FireSIGHT 系统用户指南

5.4.1 版
2015 年 1 月 22 日

思科系统公司
www.cisco.com
思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices。

目 录

第 3 章

思科 FireSIGHT 系统简介

思科 FireSIGHT® 系统是集成的网络安全和流量管理产品套件，部署在专用平台上或作为软件解决方案。

系统旨在帮助您以符合组织的安全策略（网络保护准则）的方式处理网络流量。安全策略可能还包括可接受的使用策略 (AUP)，该策略向员工提供有关其可以如何使用组织的系统的准则。

*设备*监控流量以进行分析并向管理*防御中心*® 报告。内联部署的设备会影响流量。

提示 有多种型号的设备和防御中心。受管设备包括物理和虚拟 FirePOWER 设备、用于 Blue Coat X-系列的思科 NGIPS 和 具备 FirePOWER 服务的 Cisco ASA 防火墙 (ASA FirePOWER)。防御中心还可以部署为物理或虚拟设备。如有必要，可将设备型号进一步分组为系列。系统功能通常取决于型号和许可证。

防御中心提供具有 Web 界面的集中管理控制台，可用于执行管理、分析和报告任务。物理受管设备也有一个可用于执行初始设置以及基本分析和配置任务的 Web 界面。虚拟管理设备、用于 Blue Coat X-系列的思科 NGIPS 和 ASA FirePOWER 设备没有 FireSIGHT 系统 Web 界面。对于这些设备，必须使用 CLI 执行任何无法使用管理防御中心完成的任务。

本指南将提供有关 FireSIGHT 系统的特性和功能的信息。每个章节中的说明性文本、图形和操作步骤都提供详细信息，以帮助您浏览用户界面，最大化系统性能，并对问题进行疑难解答。

以下主题向您介绍 FireSIGHT 系统，描述其关键组件，并帮助您了解如何使用本指南：

- 第 1-6 页上的防御中心简介
- 第 1-1 页上的受管设备简介
- 第 1-8 页上的 5.4.1 版 随附的防御中心和设备
- 第 1-10 页上的 FireSIGHT 系统组件
- 第 1-14 页上的文档资源
- 第 1-14 页上的文档体例
- 第 1-16 页上的 IP 地址约定

受管设备简介

网段上安装的受管设备监控流量以进行分析。被动部署的受管设备收集有关组织的资产的详细信息：主机、操作系统、应用、用户、传输的文件 （包括恶意软件）、漏洞等等。 FireSIGHT 系统将此信息关联以供您进行分析，从而可以监控用户访问的网站及其使用的应用，评估流量模式，并获得入侵和其他攻击的通知。

如果以内联方式部署，则系统可以使用*访问控制*来影响流量，借此可以精细指定如何处理进入、退出和穿越网络的流量。您收集的有关网络流量的数据和从中获取的所有信息可用于根据以下条件来过滤和控制该流量：

- 简单、轻松确定的传输层和网络层特性：源和目标、端口、协议等等
- 有关流量的最新上下文信息，包括诸如信誉、风险、业务关联性、使用的应用或访问的 URL 之类的特性
- 组织中的 Microsoft Active Directory LDAP 用户；可以向不同用户授予不同的访问级别
- 加密流量的特性；也可以解密此流量以进一步分析
- 未加密或已解密的流量包含禁止的文件、检测到的恶意软件还是入侵事件

发生适合于最大程度提高灵活性和性能的各类型的流量检查和控制。例如，基于信誉的黑名单，因为它使用简单的源和目标数据，可以在流程中提前阻止禁止的流量，而检测并阻止入侵和漏洞是最后一道防御。

除访问控制之外， 3 系列 设备上的网络管理功能还允许其在交换式和路由式环境中工作，执行网络地址转换 (NAT)，以及在配置的虚拟路由器之间构建安全虚拟专用网 (VPN) 隧道。您还可以配置旁路接口、聚合接口、快速路径规则和严格 TCP 实施。

有关详情，请参阅：

- 第 1-2 页上的 2 系列和 3 系列 受管设备
- 第 1-3 页上的 64 位虚拟受管设备
- 第 1-3 页上的适用于 Blue Coat X 系列的 Cisco NGIPS
- 第 1-3 页上的具备 FirePOWER 服务的 Cisco ASA 防火墙

2 系列和 3 系列 受管设备

3 系列设备（其中包括所有 思科 FirePOWER 7000 系列和 8000 系列设备）是专用于 FireSIGHT 系统的第三系列物理设备。3 系列设备具有各种吞吐量，但是共享大多数相同的功能。一般来说，8000 系列设备比 7000 系列功能更强大；它们还支持其他功能，如快速路径规则、链路聚合和堆叠。

请注意，防御中心和 3 系列设备均在进行品牌过渡。防御中心也称为 FireSIGHT 管理中心， 3 系列 设备也称为 FirePOWER 设备。防御中心的产品标识号可能以 FS 而不是 DC 开头。同样， 3 系列 设备的产品标识号可能以 FP 而不是 3D 开头。否则型号保持不变。例如，DC4000 和 FS4000 引用同一防御中心。

2 系列是第二系列的物理受管设备。 2 系列 设备自动具有与保护许可证关联的大多数功能：入侵检测和防御、文件控制以及基本简单网络的访问控制。此外， 3D9900 还支持快速路径规则、堆叠和分路模式。

但是，由于资源和架构限制， 2 系列设备支持保护许可证授予的有限功能集。 2 系列设备无法对存档文件内的嵌套文件执行安全智能过滤或文件控制。此外， 2 系列设备也无法执行基于地理位置的访问控制，即使使用 FireSIGHT 许可的防御中心也如此。**不能**在 2 系列设备上启用其他许可功能。

虽然思科不再发行新的 2 系列设备，但是可以将运行先前版本的系统的 2 系列设备更新或重新映像为5.4.1 版。请注意，重新映像将导致丢失设备上的几乎**所有**配置和事件数据。有关详细信息，请参阅《*FireSIGHT 系统安装指南*》。

提示 可以将特定配置和事件数据从版本 4.10.3 部署迁移到版本 5.2 部署，然后可以将后者更新为 5.4.1 版。有关详细信息，请参阅版本 5.2 的《*FireSIGHT 系统迁移指南*》。

64 位虚拟受管设备

可以使用 VMware vSphere Hypervisor 或 vCloud Director 环境将 64 位虚拟设备部署为 ESXi 主机。您也可以在所有受支持 ESXi 版本上启用 VMware Tools。有关受支持版本的列表，请参阅《*FireSIGHT 系统虚拟安装指南*》。有关 VMware Tools 的完整功能的信息，请参阅 VMware 网站 (http://www.vmware.com/)。

虚拟设备使用 e1000（1 千兆位/秒）接口，您也可以使用 VMware 客户端将默认感知和管理接口替换为 vmxnet3（10 千兆位/秒）接口。您还可以使用 VMware vSphere 客户端在虚拟防御中心上创建其他管理接口。有关详细信息，请参阅《*FireSIGHT 系统虚拟安装指南*》。

无论安装和应用了何种许可证，虚拟设备都不支持任何基于硬件的系统功能：冗余和资源共享、交换、路由等等。此外，虚拟设备没有 FireSIGHT 系统 Web 界面。

适用于 Blue Coat X 系列的 Cisco NGIPS

可以在 Blue Coat X -系列平台上安装用于 Blue Coat X-系列的思科 NGIPS。这个基于软件的设备作用类似于虚拟受管设备。无论安装和应用何种许可证，用于 Blue Coat X-系列的思科 NGIPS 都不支持以下任何 FireSIGHT 系统功能：

- 用于 Blue Coat X-系列的思科 NGIPS 不支持由恶意软件或可控性许可证授予的功能，包括高级恶意软件防护 (AMP)、应用控制、用户控制和任何系统的基于硬件的功能 （集群、堆叠、交换、路由、 VPN、 NAT 等等）。
- 无法使用用于 Blue Coat X-系列的思科 NGIPS 解密或检查加密流量（SSL 检查）。
- 无法使用用于 Blue Coat X-系列的思科 NGIPS 根据网络流量的源或目标国家/地区或大洲来过滤网络流量 （基于地理位置的访问控制）。
- 无法使用防御中心 Web 界面配置用于 Blue Coat X-系列的思科 NGIPS 接口。
- 无法使用防御中心关闭、重新启动或以其他方式管理用于 Blue Coat X-系列的思科 NGIPS 进程。
- 无法使用防御中心从用于 Blue Coat X-系列的思科 NGIPS 创建备份或将备份恢复到其中。
- 无法向用于 Blue Coat X-系列的思科 NGIPS 应用运行状况或系统策略。这包括管理时间设置。

用于 Blue Coat X-系列的思科 NGIPS 没有 Web 界面。但是，它具有 X -系列平台独有的命令行界面 (CLI)。使用此 CLI 可安装系统以及执行其他特定于平台的管理任务，例如：

- 创建虚拟设备处理器 (VAP) 组，从而利用 X -系列平台的负载均衡和冗余优势（堪比思科物理设备集群）
- 配置被动和内联感知接口，包括配置接口的最大传输单位 (MTU)
- 管理进程
- 管理时间设置，包括 NTP 设置

具备 FirePOWER 服务的 Cisco ASA 防火墙

具备 FirePOWER 服务的 Cisco ASA 防火墙（ASA FirePOWER 设备）的功能类似于受管设备。在此部署中，ASA 设备提供最重要的系统策略，并将流量传递至 FireSIGHT 系统进行访问控制、入侵检测和防御、发现以及高级恶意软件防护。

无论安装和应用何种许可证， ASA FirePOWER 设备都不支持以下任何 FireSIGHT 系统功能：

- ASA FirePOWER 设备不支持 FireSIGHT 系统的基于硬件的功能：集群、堆叠、交换，路由、VPN、 NAT 等等。但是， ASA 平台确实提供这些功能，可以使用 ASA CLI 和 ASDM 配置这些功能。有关详细信息，请参阅 ASA 文档。
- ASA FirePOWER 设备不支持 SSL 检查。
- 无法使用防御中心 Web 界面配置 ASA FirePOWER 接口。
- 无法使用防御中心关闭、重新启动或以其他方式管理 ASA FirePOWER 进程。
- 无法使用防御中心从 ASA FirePOWER 设备创建备份或将备份恢复到其中。
- 无法编写访问控制规则以使用 VLAN 标记条件与流量进行匹配。

ASA FirePOWER 设备没有 FireSIGHT Web 界面。但是，它拥有 ASA 平台特有的软件和命令行界面 (CLI)。使用这些特定于 ASA 的工具可安装系统以及执行其他特定于平台的管理任务，例如：有关详细信息，请参阅 ASA FirePOWER 模块文档。

可以将 ASA 5506-X 设备作为独立设备或受管设备进行管理。使用 ASDM 管理独立 ASA FirePOWER 模块 并使用防御中心管理受管 ASA FirePOWER 设备。当设备注册到防御中心时，无法使用 ASDM 管理 ASA FirePOWER 模块。

请注意，如果编辑 ASA FirePOWER 设备并从多情景模式切换到单情景模式（反之亦然），则设备会重命名其所有接口。**必须**重新配置所有 FireSIGHT 系统安全区域、关联规则和相关配置才能使用已更新的 ASA FirePOWER 接口名称。

注　在 SPAN 端口模式下部署 ASA FirePOWER 时，防御中心不显示 ASA 接口。

按受管设备型号汇总受支持功能

在运行 5.4.1 版时， FireSIGHT 系统设备具有各种吞吐量和功能，具体取决于型号和许可证。

请注意，防御中心和 3 系列设备均在进行品牌过渡。防御中心也称为 FireSIGHT 管理中心， 3 系列设备也称为 FirePOWER 设备。防御中心的产品标识号可能以 FS 而不是 DC 开头。同样，3 系列设备的产品标识号可能以 FP 而不是 3D 开头。否则型号保持不变。例如， DC4000 和 FS4000 引用同一防御中心。

尽管可使用任何 5.4.1 版防御中心管理所有设备所有5.4.1 版设备，但是 DC500（以及较小程度上的 DC750）支持有限的 FireSIGHT 系统功能集。有关详细信息，请参阅第 1-7 页上的按防御中心型号汇总受支持功能。

下表将系统的主要访问控制和网络管理功能与支持这些功能的受管设备以及必须启用的许可证相匹配。有关这些功能的简短描述，请参阅第 1-10 页上的 FireSIGHT 系统组件。

表 1-1　按设备型号支持的访问控制功能

特性或功能	2 系列设备	3 系列设备	ASA FirePOWER 设备	虚拟设备	X -系列设备	许可证
访问控制：基本网络控制	是	是	否， VLAN 控制	是	是	任意
访问控制：文本 URL	否	是	是	是	是	任意
访问控制：SSL 检查	否	是	否	否	否	任意
网络发现：主机、用户、应用	是	是	是	是	是	FireSIGHT
访问控制：基于地理位置的过滤	否	是	是	是	否	FireSIGHT

表 1-1　按设备型号支持的访问控制功能 （续）

特性或功能	2 系列设备	3 系列设备	ASA FirePOWER 设备	虚拟设备	X -系列设备	许可证
安全智能过滤	否	是	是	是	是	保护
入侵检测和防御 (IPS)	是	是	是	是	是	保护
文件控制：按文件类型	是	是	是	是	是	保护
文件控制：存档文件检查	否	是	是	是	是	保护
高级恶意软件防护 (AMP)	否	是	是	是	否	恶意软件
访问控制：应用控制	否	是	是	是	否	可控性
访问控制：用户控制	否	是	是	是	否	可控性
访问控制：按类别和信誉执行 URL 过滤	否	是	是	是	是	URL 过滤

表 1-2　按设备型号支持的管理和网络管理功能

特性或功能	2 系列设备	3 系列设备	ASA FirePOWER 设备	虚拟设备	X -系列设备	许可证
流量信道	否	是	否	否	否	任意
多个管理接口	否	是	否	否	否	任意
链路聚合	否	是	否	否	否	任意
FireSIGHT 系统Web 界面	有限	有限	否	否	否	任意
受限制命令行界面 (CLI)	否	是	是	是	否	任意
外部身份验证	是	是	否	否	否	任意
连接到 eStreamer 客户端	是	是	是	否	否	任意
自动应用旁路	是	是	否	是	否	任意
分路模式	3D9900	是	否	否	否	任意
快速路径规则	3D9900	8000 系列	否	否	否	任意
严格 TCP 实施	否	是	否	否	否	保护
内联集的旁路模式	是	因 NetMod/SFP 而异	否	否	否	保护
恶意软件存储包	否	是	否	否	否	恶意软件
交换、路由、交换式和路由式聚合接口	否	是	否	否	否	可控性
NAT 策略	否	是	否	否	否	可控性
设备堆叠	3D9900	3D8140 82xx 子系列 83xx 子系列	否	否	否	任意
设备集群	否	是	否	否	基于 X -系列	可控性，X -系列 除外

表 1-2　　按设备型号支持的管理和网络管理功能 （续）

特性或功能	2 系列 设备	3 系列 设备	ASA FirePOWER 设备	虚拟 设备	X -系列 设备	许可证
集群堆栈	否	3D8140 82xx 子系列 83xx 子系列	否	否	否	可控性
VPN	否	是	否	否	否	VPN

防御中心简介

防御中心为 FireSIGHT 系统部署提供集中管理控制台和数据库存储库。防御中心汇聚和关联入侵、文件、恶意软件、发现、连接和性能数据，从而评估事件对特定主机的影响并用危害表现标记主机。借助此功能，可以监控设备相互报告的信息，并评估和控制网络中发生的总体活动。防御中心还控制设备上的网络管理功能：交换、路由、 NAT、 VPN 等等。

防御中心的主要功能包括：

- 设备、许可证和策略管理
- 在表、图形和图表中显示事件和上下文信息
- 运行状况与性能监控
- 外部通知和警报
- 关联、危害表现以及实时威胁响应的补救功能
- 自定义和基于模板的报告
- 高可用性（冗余）功能（确保运行的连续性）

2 系列 和3 系列 防御中心是思科提供的具有容错功能的专用物理网络设备。您还可以使用 VMware vSphere Hypervisor 或 vCloud Director 环境将 64 位虚拟防御中心部署为 ESXi 主机。任何防御中心都可管理所有类型的设备：物理、虚拟、具备 FirePOWER 服务的 Cisco ASA 防火墙 和用于 Blue Coat X-系列的思科 NGIPS。

防御中心具有各种设备管理、事件存储、主机监控和用户监控功能。请注意，由于资源和架构限制，DC500（以及较小程度上的 DC750）支持有限的 FireSIGHT 系统功能集。

请注意，防御中心和 3 系列设备均在进行品牌过渡。防御中心也称为 FireSIGHT 管理中心，3 系列设备也称为 FirePOWER 设备。防御中心的产品标识号可能以 FS 而不是 DC 开头。同样，3 系列设备的产品标识号可能以 FP 而不是 3D 开头。否则型号保持不变。例如，DC4000 和 FS4000 引用同一防御中心。

注　尽管思科不再发行新的 2 系列防御中心，但是可以将其更新或重新映像为 5.4.1 版。请注意，重新映像将导致丢失设备上的几乎**所有**配置和事件数据。有关详细信息，请参阅《*FireSIGHT 系统安装指南*》。

按防御中心型号汇总受支持功能

在运行 5.4.1 版时，所有防御中心都具有类似的功能，主要区别在于容量和速度。防御中心型号根据其可以管理的设备数、其可以存储的事件数及其可以监控的主机和用户数而异。有关详情，请参阅：

- 第 4-1 页上的管理设备
- 第 63-14 页上的配置控制面板事件限制
- 第 65-6 页上的了解 FireSIGHT 主机和用户许可证限制

尽管可使用任何 5.4.1 版 防御中心管理所有设备所有 5.4.1 版设备，但是 DC500 （以及较小程度上的 DC750）支持有限的 FireSIGHT 系统功能集。此外，许多系统功能受**设备**许可证和型号的限制；请参阅第 1-4 页上的按受管设备型号汇总受支持功能。

DC2000 和 DC4000 将思科的统一计算系统 (UCS) 平台引入到 FireSIGHT 系统系统中。请注意，DC2000 和 DC4000 不支持使用基板管理控制器 (BMC) 上的工具的思科，如 UCS Manager 或思科集成管理控制器 (CIMC)。下表将系统的主要访问控制和网络管理功能与支持这些功能的防御中心以及必须启用的许可证相匹配。有关这些功能的简短描述，请参阅第 1-10 页上的 FireSIGHT 系统组件。

表 1-3　　按防御中心型号支持的访问控制功能

特性或功能	2 系列 防御中心	3 系列 防御中心	虚拟 防御中心	许可证
管理执行基于简单网络的访问控制的设备	是	是	是	任意
管理通过文本（手动输入）URL 执行 URL 控制的设备	是	是	是	任意
管理执行 SSL 检查的设备	是	是	是	任意
收集受管设备报告的发现数据（主机、应用和用户）并为组织创建网络映射	是	是	是	FireSIGHT
使用地理位置（国家/地区和洲）数据增强发现，并管理执行基于地理位置的访问控制的设备	DC1000、 DC3000	是	是	FireSIGHT
管理执行安全智能过滤（黑名单）的设备	DC1000、 DC3000	是	是	保护
管理入侵检测和防御 (IPS) 部署	是	是	是	保护
管理按文件类型执行简单文件控制的设备	是	是	是	保护
管理执行存档文件检查的设备	DC1000、 DC3000	是	是	保护
管理执行应用控制的设备	是	是	是	可控性
管理执行用户控制的设备	DC1000、 DC3000	是	是	可控性
管理按类别和信誉执行 URL 过滤的设备	DC1000、 DC3000	是	是	URL 过滤
管理高级恶意软件防护 (AMP) 部署并安装恶意软件存储包	DC1000、 DC3000	是	是	恶意软件

表 1-3　按防御中心型号支持的访问控制功能 （续）

特性或功能	2 系列 防御中心	3 系列 防御中心	虚拟 防御中心	许可证
接受来自 FireAMP 部署的基于终端的恶意软件 (FireAMP) 事件	是	是	是	FireAMP 订用
连接到 eStreamer、主机输入或数据库客户端	是	是	是	任意

表 1-4　按防御中心型号支持的网络管理和冗余功能

特性或功能	2 系列 防御中心	3 系列 防御中心	虚拟 防御中心	许可证
使用流量信道分隔并管理内部和外部流量	否	是	是	任意
使用多个管理接口隔离并管理不同网络上的流量	否	是	是	任意
建立防御中心冗余（高可用性）	DC1000、 DC3000	DC1500、 DC2000、 DC3500、 DC4000	否	任意
管理基于设备的冗余和资源共享 - 堆栈、集群和集群堆栈	是	是	是	可控性
管理具有因硬件而异的网络管理功能的设备：快速路径规则、严格 TCP 实施、旁路模式、分路模式、交换和路由、NAT、 VPN	是	是	是	因功能而异

5.4.1 版 随附的防御中心和设备

下表列出思科随 FireSIGHT 系统的 5.4.1 版 提供的防御中心和受管设备。

表 1-5　5.4.1 版 FireSIGHT 系统 防御中心和设备

型号/系列	系列	类型
70xx 子系列： • 3D7010/7020/7030/7050	3 系列 FirePOWER （7000 系列）	设备
71xx 子系列： • 3D7110/7120 • 3D7115/7125 • AMP7150	3 系列 FirePOWER （7000 系列）	设备
81xx 子系列： • 3D8120/8130/8140 • AMP8150	3 系列 FirePOWER （8000 系列）	设备

表 1-5　　5.4.1 版 FireSIGHT 系统 防御中心和设备 （续）

型号/系列	系列	类型
82xx 子系列： • 3D8250 • 3D8260/8270/8290	3 系列 FirePOWER （8000 系列）	设备
83xx 子系列： • 3D8350 • 3D8360/8370/8390	3 系列 FirePOWER （8000 系列）	设备
64 位虚拟设备	不适用	设备
用于 Blue Coat X-系列的思科 NGIPS	不适用	设备
ASA FirePOWER： • ASA5585-X-SSP-10 • ASA5585-X-SSP-20 • ASA5585-X-SSP-40 • ASA5585-X-SSP-60	不适用	设备
ASA FirePOWER： • ASA5506-X • ASA5512-X • ASA5515-X • ASA5525-X • ASA5545-X • ASA5555-X	不适用	设备
3 系列 防御中心： • DC750/1500/3500 • DC2000/4000	3 系列	防御中心
64 位虚拟防御中心	不适用	防御中心

请注意，防御中心和 3 系列设备均在进行品牌过渡。防御中心也称为 FireSIGHT 管理中心， 3 系列 设备也称为 FirePOWER 设备。防御中心的产品标识号可能以 FS 而不是 DC 开头。同样， 3 系列 设备的产品标识号可能以 FP 而不是 3D 开头。否则型号保持不变。例如，DC4000 和 FS4000 引用同一防御中心。

虽然思科不再发行新的 2 系列设备，但是可以将运行较老版本此系统的 2 系列设备和防御中心更新或重新映像为 5.4.1 版。请注意，重新映像将导致丢失设备上的几乎**所有**配置和事件数据。有关详细信息，请参阅《*FireSIGHT 系统安装指南*》。

提示 可以将特定配置和事件数据从版本 4.10.3 部署迁移到版本 5.2 部署，然后可以将后者更新为 5.4.1 版。有关详细信息，请参阅版本 5.2 的 《*FireSIGHT 系统迁移指南*》。

FireSIGHT 系统组件

以下主题描述 FireSIGHT 系统的一些有助于组织安全性、可接受的使用策略和流量管理策略的关键功能：

提示 很多 FireSIGHT 系统功能因设备型号、许可证和用户角色而异。本文档包含关于每个功能必需哪些 FireSIGHT 系统许可证和设备以及哪些用户角色有权完成各操作步骤的信息。有关详细信息，请参阅第 1-14 页上的文档体例。

冗余和资源共享

可以通过 FireSIGHT 系统的冗余和资源共享功能确保运行的连续性和整合多个物理设备的处理资源。

防御中心高可用性

为确保运行的连续性，可以通过 防御中心*高可用性*功能指定冗余的 DC1000、 DC1500、DC2000、DC3000、DC3500 或 DC4000 防御中心来管理设备。事件数据从受管设备流式传输至两个防御中心；两个防御中心上都保留某些配置元素。如果一个防御中心发生故障，可以使用另一个防御中心继续不间断地监控网络。

设备堆叠

*设备堆叠*允许通过将二至四台设备连接成堆叠配置以增加网段上检查的流量。建立堆叠配置时，请将每台堆叠设备的资源组合成单个共享配置。

设备集群

设备集群（有时称为设备高可用性）可用于在两个或多个3 系列 设备或堆栈之间建立网络功能和配置数据的冗余。集群两个或多个对等设备或堆栈可为策略应用、系统更新和注册建立统一的逻辑系统。通过设备集群，系统可以手动或自动进行故障切换。

大多数情况下，可以使用 (SFRP) 在不集群设备的情况下实现第 3 层冗余。 SFRP 允许设备充当指定 IP 地址的冗余网关。通过网络冗余，可以配置两台或多台设备或堆栈来提供相同的网络连接，确保网络上其他主机的连接。

使用用于 Blue Coat X-系列的思科 NGIPS 实现负载均衡

通过在 X -系列平台上的多成员 VAP 组中将用于 Blue Coat X-系列的思科 NGIPS 部署为单独的 VAP，可以利用 X -系列平台的负载均衡和冗余优势（堪比思科物理设备集群）。然后可以使用防御中心管理这些 VAP 组。有关详细信息，请参阅《*用于 Blue Coat X-系列的思科 NGIPS 安装和配置指南*》。

网络流量管理

利用 FireSIGHT 系统的网络流量管理功能可将受管设备用作贵公司网络基础设施的一部分。可以配置 3 系列设备，使其在交换式、路由式或混合式（交换路由式）环境中提供服务；执行网络地址转换 (NAT) 以及创建安全虚拟专用网络 (VPN) 通道。

交换

可以在第 2 层部署中配置 FireSIGHT 系统，使其在两个或多个网段提供数据包交换。在第 2 层部署中，在受管设备上配置交换接口和虚拟交换机作为独立的广播域。虚拟交换机根据主机的 MAC 地址来确定数据包发送的目的地。您还可以将多个物理接口组成单个逻辑链路，用于在网络中的两个终端之间提供数据包交换。终端可以是两个 FirePOWER 受管设备，也可以是连接到第三方接入交换机的 FirePOWER 受管设备。

路由

可以在第 3 层部署配置 FireSIGHT 系统，路由两个或多个接口之间的流量。在第 3 层部署中，受管设备上的路由接口和虚拟路由器配置为接收和转发流量。系统通过根据目标 IP 地址制定数据包转发决策来路由数据包。路由器根据转发条件从传出接口获取目标位置，访问控制规则指定要应用的安全策略。

配置虚拟路由器时，可以定义静态路由。此外，还可以配置路由信息协议 (RIP) 和开放式最短路径优先 (OSPF) 动态路由协议。还可以配置静态路由与 RIP 或静态路由与 OSPF 的组合。可以为所配置的每个虚拟路由器设置 DHCP 中继。

如果在使用的思科设备中同时包括虚拟交换机和虚拟路由器，可以配置关联混合接口以桥接它们之间的流量。这些实用程序将分析流量，确定流量类型和相应的响应措施（路由、交换或其他）。您还可以将多个物理接口组成单个逻辑链路，用于在网络中的两个终端之间路由流量。终端可以是两个 FirePOWER 受管设备，也可以是连接到第三方路由器的 FirePOWER 受管设备。

NAT

在第 3 层部署中，可以配置网络地址转换 (NAT)。可以将内部服务器暴露于外部网络，或者允许内部主机或服务器连接外部应用。还可以使用 IP 地址块或使用有限制的 IP 地址块和端口转换，从外部网络配置 NAT 来隐藏专用网络地址。

VPN

虚拟专用网络 (VPN) 是通过互联网或其他网络等公共资源在终端之间建立安全隧道的一种网络连接。可以配置 FireSIGHT 系统，在 3 系列设备的虚拟路由器之间建立安全 VPN 隧道。

FireSIGHT

FireSIGHT 是思科用于查看和收集有关主机、操作系统、应用、用户、文件、网络、地理位置信息和漏洞信息的发现和感知技术，为您提供网络全面信息。

可以使用防御中心的 Web 界面来查看和分析系统收集的数据。还可以使用此数据来帮助执行访问控制和修改入侵规则状态。此外，还可以根据主机的关联事件数据，对网络主机生成和跟踪危害表现信息。

访问控制

*访问控制*是一项基于策略的功能，可用于指定、检查和记录可以流经网络的流量。*访问控制策*决定系统如何处理网络上的流量。

最简单的访问控制策略指导其目标设备使用其*默认操作*处理所有流量。可以将此默认操作设置为阻止或信任所有流量而不进一步检查，或者检查入侵和发现数据的流量。

更复杂的访问控制策略可以根据安全智能数据将流量列入黑名单，以及使用*访问控制规则*对网络流量日志记录和处理实行精细控制。这些规则可以简单也可以复杂，从而使用多个条件来匹配和检查流量；可以按安全区域、网络或地理位置、 VLAN、端口、应用、所请求的 URL 和用户来控制流量。高级访问控制选项包括解密、预处理和性能。

每个访问控制规则还具有*操作*，用于确定监控、信任、阻止还是允许匹配流量。当允许流量时，可以指定系统首先使用入侵或文件策略检查该流量，以在任何漏洞、恶意软件或禁止的文件到达资产或退出网络之前对其进行阻止。

SSL 检查

*SSL 检查*是基于策略的功能，通过其可处理加密流量而不解密，或者解密加密流量以进一步进行访问控制检查。可以选择阻止不受信任加密流量的源而不解密或进一步分析流量，也可以选择不解密加密流量，而是通过访问控制对其进行检查。

为深入洞察加密流量，可以使用上传到系统的公钥证书和配对私钥来解密穿越网络的加密流量，然后通过访问控制检查解密流量，如同其从未加密一样。如果系统在分析后不阻止解密流量，则会重新加密流量，然后再将其传递到目标主机。系统可以在其处理加密连接时记录有关这些连接的详细信息。

入侵检测和防御

在允许流量发送到其目标之前，入侵检测和防御是系统的最后一道防线。*入侵策略*是由访问控制策略调用的入侵检测和防御配置的已定义集合。这些策略使用*入侵规则*和其他设置来检查流量是否存在安全违规，并且在内联部署中可以阻止或修改恶意流量。

思科随 FireSIGHT 系统提供若干入侵策略。通过使用系统提供的策略，可以利用思科漏洞研究团队 (VRT) 的经验。对于这些策略， VRT 会设置入侵和预处理器规则状态（已启用或已禁用），以及提供其他高级设置的初始配置。已启用的规则会导致系统为与规则相匹配的流量生成入侵事件或者阻止该流量。

如果系统提供的策略不完全满足组织的安全需求，自定义策略可以提高环境中系统的性能，并可提供网络上发生的恶意流量和策略违规的集中视图。通过创建和调整自定义策略，可以非常精细地配置系统如何处理和检查网络上的入侵的流量。

高级恶意软件防护和文件控制

为帮助识别和减轻恶意软件影响，FireSIGHT 系统的文件控制、网络文件轨迹和高级恶意软件防护组件可以检测、跟踪、捕获、分析并选择性阻止网络流量中文件（包括恶意软件文件和存档文件内的嵌套文件）的传输。

文件控制

*文件*控制允许受管设备检测并阻止用户通过特定应用协议上传（发送）或下载（接收）特定类型的文件。可以配置文件控制，作为全局访问控制配置的一部分；与访问控制规则关联的文件策略可以检查符合规则条件的网络流量。

基于网络的高级恶意软件防护 (AMP)

基于网络的*高级恶意软件防护* (AMP) 允许系统检查几种类型的文件中的网络流量是否存在恶意软件。设备可以将检测文件存储到其硬盘或（针对某些型号）恶意软件存储包中以供进一步分析。

无论是否存储检测到的文件，都可以将其提交给综合安全智能云，使用文件的 SHA-256 哈希值进行简单的已知性质搜索。还可以提交文件进行*动态分析*，获取威胁评分。使用此上下文信息，可以配置系统来阻止或允许特定的文件。

可以配置恶意软件防护，作为全局访问控制配置的一部分；与访问控制规则关联的文件策略可以检查符合规则条件的网络流量。

FireAMP 集成

FireAMP 是思科的企业级高级恶意软件分析和防御解决方案，可以发现、了解并阻止高级恶意软件爆发、高级持续性威胁和有针对性的攻击。

如果贵公司有订用 FireAMP，个人用户可以在计算机和移动设备（又叫做*终端*）上安装 *FireAMP 连接器*。这些轻量级代理与思科云通信，后者又与防御中心通信。

如果组织的安全策略不允许使用传统云服务器连接，则可获取并配置思科的私有内部云解决方案（FireAMP 私有云），它是一种虚拟机，充当公共思科云的压缩本地版本。

配置防御中心连接云之后，可以使用防御中心 Web 界面查看由于贵公司终端上的扫描、检测和隔离而生成的基于终端的恶意软件事件。防御中心还使用 FireAMP 数据生成和跟踪威胁对主机的影响的指示信息以及显示网络文件轨迹。

使用 *FireAMP 门户* (http://amp.sourcefire.com/) 配置 FireAMP 部署。此门户可帮助快速识别和隔离恶意软件。可以识别恶意软件爆发，跟踪它们的发展轨迹，了解其影响，并学习如何成功恢复。还可以使用 FireAMP 创建自定义防御，根据群组策略阻止执行某些应用，以及创建自定义白名单。

网络文件轨迹

网络文件轨迹功能可以跟踪网络中的文件传输路径。系统使用 SHA-256 哈希值跟踪文件；因此，要跟踪文件，系统必须执行以下一项操作：

- 计算文件的 SHA-256 哈希值并使用该值执行恶意软件云查找
- 利用防御中心与贵公司 FireAMP 订用的集成接收基于终端的威胁并隔离与该文件相关的数据

每个文件都具有相关的轨迹图，其中包含文件在一段时间内的传输轨迹视觉展示和与文件相关的其他信息。

可为网络服务、协调和服务管理功能体现出网络价值的

有几种方法可以使用应用程序编程接口 (API) 来与系统交互。有关详细信息，可以从以下任一支持站点下载更多文档：

- **Sourcefire**：(https://support.sourcefire.com/)
- **思科**：(http://www.cisco.com/cisco/web/support/index.html)

eStreamer

Event Streamer (eStreamer) 可以将几种事件数据从思科设备传输至定制开发的客户端应用。创建客户端应用后，可以将其连接到 eStreamer 服务器（防御中心或物理受管设备），启动 eStreamer 服务，并开始交换数据。

eStreamer 集成要求定制编程，但是可以向设备请求获取特定数据。如果在网络管理应用中显示网络主机数据，就可以写入一个程序来从防御中心检索主机重要性或漏洞数据并将该信息添加到显示中。

外部数据库访问

数据库访问功能可以在防御中心上使用支持 JDBC SSL 连接的第三方客户端查询几个数据库表。

可以使用 Crystal Reports、Actuate BIRT 或 JasperSoft iReport 等行业标准报告工具来设计和提交查询。也可以配置定制应用来查询思科数据。例如，可以创建 servlet 来定期报告和发现事件数据或刷新警报控制面板。

主机输入

主机输入功能允许使用脚本或命令行文件从第三方资源导入数据，从而增加网络映射中的信息。

Web 界面也提供部分主机输入功能；可以修改操作系统或应用程序协议特性，验证或阻止漏洞以及从网络映射中删除客户端与服务器端口等各种项目。

补救

该系统包含可用于创建*补救*操作的 API，在网络状况违反相关关联策略或合规白名单时，防御中心可以自动启动。这不仅可以在您无法立即处理攻击时自动减轻攻击，还可以确保系统保持符合贵公司的安全策略。除了用户自己创建的补救操作，防御中心还提供预定义的补救模块。

文档资源

FireSIGHT 系统文档包括联机帮助和 PDF 文件。可以通过以下方式访问来自 Web 界面的联机帮助：

- 点击各页面上的上下文帮助链接
- 选择 **Help > Online**

联机帮助包含关于使用防御中心或设备 Web 界面可以完成的任务的信息，包括系统管理、策略管理和事件分析。

可以在以下任一支持站点访问最新版本 PDF 文档：

- **Sourcefire**：(https://support.sourcefire.com/)
- **思科**：(http://www.cisco.com/cisco/web/support/index.html)

此类文档包括：

- 《*FireSIGHT 系统用户指南*》，其内容与联机帮助相同，但格式更便于打印
- 《*FireSIGHT 系统安装指南*》，包括有关安装思科设备的信息以及硬件规格与安全信息
- 《*FireSIGHT 系统虚拟安装指南*》，包括有关安装、管理虚拟设备和虚拟防御中心以及疑难解答的信息
- 《*用于 Blue Coat X-系列的思科 NGIPS 安装和配置指南*》，包括有关安装、管理用于 Blue Coat X-系列的思科 NGIPS 以及疑难解答的信息
- 各种 API 指南和补充材料

文档体例

本文档包含关于每个功能要求使用哪些许可证和设备型号 FireSIGHT 系统以及哪些用户有权限完成各个操作步骤的信息。有关详细信息，请参阅以下各节：

- 第 1-15 页上的许可证约定
- 第 1-15 页上的受支持设备和防御中心约定
- 第 1-16 页上的访问约定

许可证约定

各个章节开头的许可证声明指出了使用本节所述功能所要求使用的许可证，详情如下：

FireSIGHT

FireSIGHT 许可证随附于防御中心中，执行主机、应用和用户发现要求使用此许可证。防御中心上的FireSIGHT 许可证决定了利用防御中心及其受管设备可以监控多少单独的主机和用户以及可以利用多少用户来执行用户控制。

保护

保护许可证允许受管设备进行入侵检测和防御、文件控制以及安全情报过滤。

可控性

可控性许可证允许受管设备执行用户和应用控制。它还允许设备执行交换和路由（包括 DHCP 中继）、NAT，并且允许集群设备和堆栈。可控性许可证要求具备保护许可证。

URL 过滤

URL 过滤许可证允许受管设备基于受监控主机请求的 URL，使用定期更新的基于云的类别和信誉数据确定哪些流量可以流经网络。 URL 过滤许可证要求具备保护许可证。

恶意软件

恶意软件许可证允许受管设备执行基于网络的高级恶意软件防护 (AMP)，即检测、捕捉并阻止通过网络传输的文件中的恶意软件通过网络并提交这些文件进行动态分析。它还允许查看其轨迹，跟踪通过网络传输的文件。恶意软件许可证要求具备保护许可证。

VPN

许可证VPN允许在思科受管设备的虚拟路由器之间建立安全 VPN 隧道。VPN许可证要求保护和可控性许可证。

由于许可的功能通常是累加的，此文档仅提供每项功能的最高要求许可证。例如，如果功能要求 FireSIGHT、保护以及可控性许可证，则只列出可控性。

许可证声明中“或”语句表明要使用本部分描述的功能需要使用特定的许可证，但是附加许可证可以增加功能。例如，在文件策略内，有些文件规则操作要求使用保护许可证，而其他的则要求使用恶意软件许可证。因此，文件规则文档的许可证声明会列出保护或恶意软件。

请注意，由于架构和资源限制，并非所有的许可证都可应用于所有受管设备。一般而言，无法许可设备不支持的功能，请参阅第 1-4 页上的按受管设备型号汇总受支持功能。有关详细信息，请参阅第 65-1 页上的了解许可。

受支持设备和防御中心约定

每节开头的“受支持设备”声明指出了只有指定的设备系列、子系列或型号才支持相应的功能。例如，只有在 3 系列设备上才支持堆栈。如果某一节没有“受支持设备”声明，则表明所有设备都支持该功能，或该节不适用于受管设备。

有关此版本支持的平台的详细信息，请参阅第 1-6 页上的防御中心简介。

访问约定

本文档每个程序开头的“访问”声明都指出了执行此程序所要求的预定用户角色。正斜杠隔开的角色表示任何列出的角色都可执行此程序。下表定义了“访问”声明中出现的常用术语。

表 1-6　访问约定

访问术语	说明
Access Admin	用户必须具备访问控制管理员角色
管理	用户必须具备管理员角色
任何环境	用户可以是任何角色
任何角色/管理员	用户可以是任何角色，但是只有管理员角色可以不受限制地访问（例如可以查看保存为专用级别的其他用户数据）
任何安全分析师	用户可以是安全分析师角色或安全分析师（只读）角色
数据库	用户必须具备外部数据库角色
Discovery Admin	用户必须具备发现管理员角色
Intrusion Admin	用户必须具备入侵管理员角色
维护	用户必须具备维护人员角色
网络管理员	用户必须具备网络管理员角色
安全分析师	用户必须具备安全分析师角色
Security Approver	用户必须具备安全审批人角色

自定义角色的用户可以拥有不同于预定角色的权限。预定角色用于指示某个程序的访问要求时，具有相似权限的自定义角色也能访问。某些具有自定义角色的用户可以使用略有不同的菜单路径到达配置页面。例如，具有仅有入侵策略权限的自定义角色的用户通过入侵策略而非通过访问控制策略的标准路径来访问网络分析策略。有关自定义用户角色的详细信息，请参阅第 61-48 页上的管理自定义用户角色。

IP 地址约定

可以使用 IPv4 无类别域际路由选择 (CIDR) 表示法和类似的 IPv6 前缀长度表示法定义 FireSIGHT 系统很多位置的地址块。

CIDR 表示法使用网络 IP 地址结合位掩码来定义指定地址块中的 IP 地址。例如，下表列出了 CIDR 表示法中的 IPv4 地址空间。

表 1-7　CIDR 表示法语法示例

CIDR 块	CIDR 块中的 IP 地址	子网掩码	IP 地址数量
10.0.0.0/8	10.0.0.0 - 10.255.255.255	255.0.0.0	16,777,216
172.16.0.0/12	172.16.0.0 - 172.31.255.255	255.240.0.0	1,048,576
192.168.0.0/16	192.168.0.0 - 192.168.255.255	255.255.0.0	65,536

同样， IPv6 使用网络 IP 地址结合前缀长度来定义指定块中的 IP 地址。例如， 2001:db8::/32 指定的 IPv6 地址在 2001:db8:: 网络中，前缀长度为 32 位，即 2001:db8:: 至 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff。

使用 CIDR 或前缀长度表示法指定 IP 地址块时，FireSIGHT 系统只使用前缀长度指定的网络 IP 地址部分。例如，如果键入 10.1.2.3/8，则 FireSIGHT 系统使用 10.0.0.0/8。

换句话说，虽然思科建议使用 CIDR 或前缀长度表示法时采用使用标准网络 IP 地址的标准方法，但是 FireSIGHT 系统并不要求必须这么做。

登录 FireSIGHT 系统

本章详细介绍使用基于设备的网络界面以及命令行界面 (CLI) 登录和注销 FireSIGHT 系统必须执行的步骤。您还可以配置使用 LDAP 或 RADIUS 凭证的外部身份验证的用户帐户。

登录网络界面后，将指针悬停在特定区域上，*上下文菜单*功能会提供额外信息和有用的导航链接。

有关详细信息，请参阅以下各节：

登录设备

许可证：任何环境

FireSIGHT 系统防御中心具有一个可用于执行管理和分析任务的网络界面。物理受管设备也有一个可用于执行初始设置以及基本分析和配置任务的网络界面。有关浏览器要求的信息，请参阅此版本 FireSIGHT 系统的版本说明。

虚拟受管设备没有网络界面。对这些设备（和 3 系列设备），FireSIGHT 系统提供交互式 CLI，可用于执行使用设备的管理防御中心无法完成的任何任务。

用于 Blue Coat X-系列的思科 NGIPS也没有网络界面，但有一个专用于 X -系列 平台的 CLI。您可以使用该 CLI 安装来安装系统以及执行其他平台特定的管理任务。有关详细信息（包括如何登录 X -系列 平台 CLI），请参阅《*用于 Blue Coat X-系列的思科 NGIPS 安装和配置指南*》。

ASA FirePOWER 设备有自己的管理应用（ASDM 和 CSM）以及用于配置 ASA 设备的 CLI。此外，FireSIGHT 系统 带有一个交互式 CLI，可用于执行使用设备的管理防御中心无法完成的任何任务。您可以使用 ASA 专用工具来安装系统以及执行其他平台特定的管理任务。有关详细信息，请参阅 ASA 文档。

注 由于 FirePOWER 设备根据用户帐户审核用户活动，因此，请确保用户使用正确的帐户登录系统。

您必须提供用户名和密码才能访问设备的网络界面、 CLI 或外壳。登录设备后，您可以访问的功能受制于您获得的用户帐户权限。有关详细信息，请参阅第 61-40 页上的管理用户帐户。

或者，如果贵组织使用通用访问卡 (CAC) 进行身份验证，则您可以使用 CAC 凭证获得对设备网络界面的访问权。有关 CAC 身份验证和授权的详细信息，请参阅第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。

注意事项 如果多次提供不正确的凭证，您的外壳程序访问帐户可能会被锁定。如果提供了正确的凭证，但登录被拒绝，请联系系统管理员，而不要反复尝试登录。

在网络会话期间首次访问设备主页时，可以查看您上一次登录该设备的登录会话相关信息。您可以查看与您上次登录相关的以下信息：

- 登录的年、月、日和周
- 用 24 小时制表示的登录设备本地时间
- 上次用于访问设备的主机和域名

默认情况下，不活动达 1 小时之后将自动注销会话，您已配置免除会话超时的情况除外。担任管理员角色的用户可以在系统策略中更改会话超时间隔。有关详细信息，请参阅第 61-44 页上的管理用户登录设置和第 63-26 页上的配置用户界面设置。

请注意，耗时较长的某些进程可能导致网络浏览器显示指明脚本无响应的消息。如果出现这种情况，请确保允许脚本继续运行，直至完成。

注 要在设备上对系统进行全新安装（新安装或映像），您必须使用管理员 (admin) 用户帐户登录来完成初始设置流程（详见《*FireSIGHT 系统安装指南*》）。按照第 61-41 页上的添加新用户帐户所述创建其他用户帐户后，您与其他用户应使用这些帐户登录网络界面。

提示 您**必须**配置 CAC 身份验证和授权，然后网络上的用户才能使用他们的 CAC 凭证登录 CAC Login 页面。有关详细信息，请参阅第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。

要通过网络界面登录设备，请执行以下操作：

访问：任何环境

步骤 1 通过浏览器访问 `https://hostname/`，其中，*hostname* 表示设备的主机名。

随即显示“登录”页面。

步骤 2 在 **Username** 和 **Password** 字段中，键入用户名和密码。用户名区分大小写。

如果您的组织登录时使用 SecurID® 令牌，请将所用的令牌添加到您的 SecurID PIN 之后并将其用作登录密码。例如，您的 PIN 为 `1111`，SecurID 令牌是 `222222`，则请键入 `1111222222`。必须生成 SecurID PIN 后才能登录 FireSIGHT 系统。

步骤 3 点击 **Login**。

系统将显示默认开始页面。如果您为自己的用户帐户选择了自定义主页，则显示的是该自定义主页。有关详情，请参见第 71-2 页上的指定主页。

提示 如果您无法访问网络界面，请联系系统管理员修改您的帐户权限，或者用具有管理员访问权限的用户身份登录并修改帐户的权限。有关详细信息，请参阅第 61-50 页上的修改用户权限和选项。

在页面顶部显示的菜单和菜单选项取决于用户帐户的权限。但是，默认主页上的链接包括适用于各种用户帐户权限范围的选项。如果您点击的链接要求具备与您帐户已经获得的权限不同的权限，将显示以下警告消息：

```
You are attempting to view an unauthorized page.This activity has been logged.
```

在这种情况下，您可以从可用菜单选择一个不同的选项，也可以点击浏览器窗口的 **Back** 以返回到上一页。

要采用 CAC 凭证通过网络界面登录设备，请执行以下操作：

访问：任何环境

步骤 1　按照贵组织的说明插入 CAC。

步骤 2　通过浏览器访问 `https://hostname/`，其中，*hostname* 表示设备的主机名。

步骤 3　如有提示，请输入与步骤 1 中插入的 CAC 关联的 PIN。

系统接受您的 PIN。

步骤 4　如有提示，请从下拉列表中选择相应的证书。

浏览器接受选择并显示 CAC Login 页面。

步骤 5　要使用您的 CAC 凭证进行身份验证，请点击 **Continue**。

要使用用户名和密码进行身份验证，请在 **Username** 和 **Password** 字段中输入用户名和密码。用户名区分大小写。

系统将显示默认开始页面。如果您为自己的用户帐户选择了自定义主页，则显示的是该自定义主页。有关详情，请参见第 71-2 页上的指定主页。

提示　如果您无法访问网络界面，请联系系统管理员修改您的帐户权限，或者用具有管理员访问权限的用户身份登录并修改帐户的权限。有关详细信息，请参阅第 61-50 页上的修改用户权限和选项。

在页面顶部显示的菜单和菜单选项取决于用户帐户的权限。但是，默认主页上的链接包括适用于各种用户帐户权限范围的选项。如果您点击的链接要求具备与您帐户已经获得的权限不同的权限，将显示以下警告消息：

```
You are attempting to view an unauthorized page.This activity has been logged.
```

在这种情况下，您可以从可用菜单选择一个不同的选项，也可以点击浏览器窗口的 **Back** 以返回到上一页。

注　在浏览会话活动期间，**请勿**删除 CAC。如果在会话期间移除或替换 CAC，则网络浏览器会终止该会话，并且系统会注销网络界面。

要通过命令行登录3 系列 设备、虚拟设备或 ASA FirePOWER 设备，请执行以下操作：

访问：CLI 基本配置

步骤 1　对于3 系列 设备和虚拟设备，请用 *hostname* 打开设备的 SSH 连接，其中，*hostname* 表示设备的主机名。对于 ASA FirePOWER 设备，请用管理地址打开 ASA FirePOWER 模块的 SSH 连接。

系统将会显示 `login as:` 命令提示符。

步骤 2　输入用户名并按 Enter。

系统将会显示 `Password:` 提示符。

步骤 3　输入密码并按 Enter。

如果您的组织登录时使用 SecurID® 令牌，请将所用的令牌添加到您的 SecurID PIN 之后并将其用作登录密码。例如，您的 PIN 为 `1111`，SecurID 令牌是 `222222`，则请键入 `1111222222`。必须生成 SecurID PIN 后才能登录 FireSIGHT 系统。

系统先显示登录提示，然后显示 > 提示符。

您可以使用您的命令行访问权限级别允许的任何命令。有关可用的 CLI 命令的详细信息，请参阅第 D-1 页上的命令行参考。

注销设备

许可证：任何环境

不再使用网络界面时，思科建议您注销，即使您只是暂时离开网络浏览器。注销会结束您的 Web 会话并确保没有人可以凭借您的凭证使用设备。

默认情况下，不活动达 1 小时之后将自动注销会话，您已配置免除会话超时的情况除外。担任管理员角色的用户可以在系统策略中更改会话超时间隔。有关详细信息，请参阅第 61-44 页上的管理用户登录设置和第 63-26 页上的配置用户界面设置。

要注销设备，请执行以下操作：

访问：任何环境

步骤 1　点击工具栏上的 **Logout**。

使用上下文菜单

许可证：因功能而异

为方便您使用，网络界面的某些页面支持弹出上下文菜单，可供您用作快捷方式来访问 FireSIGHT 系统中的其他功能。菜单的内容取决于您访问菜单所处的*热点* - 不仅是页面，还包括具体数据。

例如，事件视图、入侵事件数据包视图、控制面板和 Context Explorer 中的 *IP 地址热点*都提供更多选项。右键点击热点，利用 IP 地址上下文菜单详细了解与该地址关联的主机，包括所有可用的 whois 和主机配置文件信息。除了不支持安全情报筛选的 DC500 防御中心之外，您还可以在安全情报全局白名单或黑名单上添加具体 IP 地址。

再如，您可以通过事件视图和控制面板中的 *SHA-256 哈希值热点*将文件的 SHA-256 哈希值添加到白名单或自定义检测列表中，或者查看要复制的完整哈希值。请注意，DC 500 防御中心也不受支持此功能。

以下列表描述了网络界面各种页面的上下文菜单中的许多可用选项。在不支持思科上下文菜单的页面或位置，将会显示适用于浏览器的常规上下文菜单。

访问控制、 SSL 和 NAT 策略编辑器

访问控制、SSL 和 NAT 策略编辑器包含每个规则的热点。您可以使用上下文菜单执行这些操作：插入新规则和类别；剪切、复制和粘贴规则；设置规则状态；以及编辑规则。

入侵规则编辑器

入侵规则编辑器包含每个入侵规则的热点。您可以使用上下文菜单执行这些任务：编辑规则；设置规则状态（包括禁用规则）；配置阈值和抑制选项；查看规则文档。

事件查看器

事件页面（下钻式页面和表视图）包含每个事件、IP 地址以及某些检测文件 SHA-256 哈希值的热点。对于大多数事件类型，您可以使用上下文菜单查看 Context Explorer 中的相关信息，也可以在新窗口中向下钻取事件信息。在事件视图中，如果事件字段包含过长的文本以至于无法全部显示，例如文件的 SHA-256 哈希值、漏洞说明或 URL，可以使用上下文菜单查看完整文本。

对于捕获的文件、文件事件和恶意软件事件，您可以使用上下文菜单向白名单或自定义检测列表添加文件或从中删除文件，下载文件的副本，查看档案文件中嵌套的文件，为嵌套文件下载父档案文件，或将文件提交至综合安全智能云进行动态分析。

对于入侵事件，您可以使用上下文菜单执行类似于在入侵规则编辑器或入侵策略中的任务：编辑触发规则；设置规则状态 （包括禁用规则）；配置阈值和抑制选项；查看规则文档。

数据包视图

入侵事件数据包视图包含 IP 地址热点。请注意，数据包视图使用左键上下文菜单而不是右键菜单。

控制面板

许多控制板构件包含用于查看 Context Explorer 中相关信息的热点。控制面板构件还包含 IP 地址和 SHA-256 值热点。

Context Explorer

Context Explorer 包含其图表、表格和图形上的热点。如果您想要以超出 Context Explorer 允许的程度更为详细地查看图表或列表的数据，您可以向下钻取相关数据的表视图。您还可以查看相关的主机、用户、应用、文件和入侵规则信息。

请注意， Context Explorer 使用左键上下文菜单，该菜单也包含 Context Explorer 独有的筛选选项及其他选项。有关详细信息，请参阅第 56-38 页上的向下钻取 Context Explorer 数据。

要访问上下文菜单，请执行以下操作：

访问：任何环境

步骤 1　在网络界面中支持热点的页面上，将指针悬停在热点上。

将会显示 `Right-click for menu` 消息（在 Context Explorer 中除外）。

步骤 2　调用上下文菜单：

- 在 Context Explorer 或数据包视图中，左键点击您的定点设备。
- 在所有其他支持热点的页面上，右键点击您的定点设备。

将会出现弹出上下文菜单，其中包含适用于热点的选项。

步骤 3　左键点击您要选择的其中一个选项的名称。

如果您使用访问控制策略编辑器或 NAT 策略编辑器，将会修改规则。否则，会根据您选择的选项打开新的浏览器窗口。

管理可重用对象

为了提高灵活性以及使网络界面更易于使用， FireSIGHT 系统允许创建命名*对象*；命名对象是将名称与值相关联的可重用配置，这样当要使用某个值时，可以使用相应的命名对象代替。

可建以下类型的对象：

- 表示 IP 地址和网络的基于网络的对象、端口/协议对、VLAN 标记、安全区域以及源/目标国家/地区（地理定位）
- 表示智能情报源和列表的基于信誉的对象，基于类别和信誉的应用过滤器和文件列表
- 非基于信誉的对象（例如 URL 类别）
- 包含您与入侵策略相关联的变量的入侵策略变量集
- 帮助处理加密流量的对象，包括密码套件、公共密钥证书和配对私有密钥以及证书可分辨名称

可以在系统网络界面中的不同位置使用这些对象，包括访问控制策略、网络分析策略、入侵策略和规则、网络发现规则、事件搜索、报告、控制面板等。

将对象分组使得可以引用带有单个配置的多个对象。可以对网络、端口、VLAN 标记、URL 和公用密钥基础结构 (PKI) 对象进行分组。

注 在大多数情况下，编辑用于策略的对象要求重新应用策略以使您的更改生效。编辑安全区域后也需要重新应用相应的设备配置。

有关详细信息，请参阅以下各节：

使用对象管理器

许可证：任何环境

可以使用对象管理器 (**Objects > Object Management**) 创建和管理对象（包括应用过滤器、变量集和安全区域）。可以将网络、端口、VLAN 标记、URL 和 PKI 对象进行分组；还可以排序、过滤和浏览对象和对象组的列表。

有关详情，请参阅：

将对象分组

许可证：任何环境

可以将网络、端口、VLAN 标记、URL 和 PKI 对象分组。系统允许在网络界面中互用对象和对象组。例如，在任何要使用端口对象的地方，也可以使用端口对象组。相同类型的对象和对象组不能具有相同的名称。

提示　要将密码套件分组，请配置密码套件列表。有关详细信息，请参阅第 3-35 页上的使用密码套件列表。

编辑用于策略的对象组 （例如，用于访问控制策略的网络对象组）后，必须重新应用策略，才能使更改生效。

删除组不会删除组中的对象，只会删除对象之间的相关性。此外，也无法删除正在使用的组。例如，无法删除用于已保存访问控制策略中的 VLAN 条件的 VLAN 标记组。

要将可重复使用对象进行分组，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　您有以下选项：

- 在要分组的 **Network**、 **Port**、 **VLAN Tag**、 **URL** 或 **Distinguished Name** 对象类型下，选择 **Object Groups**。
- 在 **PKI** 下，选择 **Internal CA Groups**、 **Trusted CA Groups**、 **Internal Cert Groups** 或 **External Cert Groups** 作为要分组的 PKI 对象。

系统显示要分组的对象类型的页面。

步骤 3　点击要分组的对象对应的 **Add** 按钮。

显示一个弹出窗口，可以在其中创建组。

步骤 4　在 **Name** 字段中为创建的组键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　选择一个或多个对象，然后点击 **Add**。

- 使用 Shift 和 Ctrl 键可选择多个对象，或者右键单击并选择 **Select All**。
- 使用过滤器字段 ( ) 可搜索要包括的现有对象，在您键入时，该字段会更新以显示匹配项目。点击搜索字段上方的重新加载图标 ( )，或点击搜索字段中的清除图标 ( ) 以清除搜索字符串。
- 如果现有对象不符合您的需要，可点击添加图标 ( ) 动态创建对象。

步骤 6　点击 **Save**。

组创建成功。

浏览、排序和过滤对象

许可证：任何环境

对象管理器每页显示 20 个对象或对象组。如果有超过 20 个任何类型的对象或对象组，请使用位于页面底部的导航链接查看其他页面。还可以转到特定页或点击刷新图标 ( ) 刷新视图。

默认情况下，页面会按名称的字母顺序列示对象和对象组。然而，也可以按显示的任何列对每种类型的对象或对象组进行排序。列标题旁边的向上 (▲) 或向下 (▼) 箭头表示页面按该列升序或降序排序。还可以按名称对页面上的对象进行过滤。对于某些对象类型，同一过滤器将按名称或值匹配。

要排序对象或对象组：

访问：管理员/访问管理员/网络管理员

步骤 1　点击列标题。要按相反方向排序，请再次点击标题。

要过滤对象或对象组：

访问：管理员/访问管理员/网络管理员

步骤 1　在 **Filter** 字段中键入搜索条件。

页面会在您键入内容时进行更新，以显示匹配的项目。可以使用以下通配符：

- 星号 [*] 匹配零或重复出现的一个字符。
- 脱字符 (^) 匹配字符串开头的内容。
- 美元符号 ($) 匹配字符串结尾的内容。

使用网络对象

许可证：任何环境

网络对象代表可单独指定或作为地址块指定的一个或多个 IP 地址。可在系统网络界面中的不同位置使用网络对象和对象组（请参阅第 3-2 页上的将对象分组），包括访问控制策略、网络变量、入侵规则、网络发现规则、事件搜索、报告，等等。

无法删除正在使用的网络对象。此外，在编辑用于访问控制策略、网络发现策略或入侵策略的网络对象后，必须重新应用策略，才能使更改生效。

要创建网络对象：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **Network** 下，选择 **Individual Objects**。

步骤 3　点击 **Add Network**。

系统将显示 Network Objects 弹出窗口。

步骤 4　在 **Name** 字段中为网络对象键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　对于要添加到网络对象的每个 IP 地址或地址块，键入其值，然后点击 **Add**。

步骤 6　点击 **Save**。

网络对象添加成功。

使用安全情报列表和源

许可证：保护

受支持的设备：任何防御中心，除了2 系列

受支持的防御中心：除 DC500 外的所有型号

安全情报功能允许根据源或目标 IP 地址对每个访问控制策略指定可以流经网络的流量。如果要将特定 IP 地址加入黑名单（即，在访问规则对流向和来自该 IP 地址的流量进行分析之前拒绝这些流量），这尤其有用。同样，可将 IP 地址添加到白名单，从而强制系统使用访问控制来处理这些 IP 地址的连接。

如果不确定是否要将特定 IP 地址添加到黑名单，可以使用“仅监控”设置，这样，系统可以使用访问控制来处理连接，但也会记录连接与黑名单的匹配情况。

默认情况下，每个访问控制策略中都包括*全局白名单*和*全局黑名单*，它们适用于所有区域。此外，在每个访问控制策略中，可以使用网络对象和对象组的组合，以及安全情报列表和源（这些都可使用安全区域进行限制）来建立独立的白名单和黑名单。

注　尽管其默认拥有所有其他的保护功能， 2 系列设备无法执行安全情报过滤。

比较源和列表

安全情报*源*是防御中心按配置的时间间隔从 HTTP 或 HTTPS 服务器下载的 IP 地址的动态集合。由于源会定期更新，因此，系统可使用最新信息来过滤网络流量。为帮助您构建黑名单，思科提供的 *Intelligence Feed*（有时称为 *Sourcefire Intelligence Feed*）代表被思科 VRT 确定为声誉不佳的 IP 地址。

防御中心下载更新的源信息时，它会自动更新其受管设备。尽管源更新可能需要几分钟才能在部署中生效，但在创建或修改源之后，或者在进行预定的源更新之后，无需重新应用访问控制策略。

注 如果要对防御中心从互联网下载源的时间进行严格控制，可禁用该源的自动更新。但是，思科建议您允许自动更新。虽然可以手动执行按需更新，但是允许系统定期下载源可获得最新、最相关的数据。

与源相比，安全情报*列表*是手动上传到防御中心的简单静态 IP 地址列表。可使用自定义列表对源以及全局白名单和黑名单进行扩充和微调。请注意，编辑自定义列表（以及编辑网络对象和从全局白名单或黑名单删除 IP 地址）后，需要重新应用访问控制策略，才能使更改生效。

格式化和已损坏源数据

源和列表源文件必须是大小不超过 500MB 的简单文本文件，每个 IP 地址或地址块占一行。注释行必须以 `#` 字符开头。列表源文件必须使用 `.txt` 扩展名。

如果防御中心下载了损坏的源或包括不可识别的 IP 地址的源，系统将继续使用旧的源数据（除非是第一次下载）。但是，如果系统可以识别源中的至少一个 IP 地址，防御中心就会使用可识别的地址更新其受管设备。

默认运行状况策略包括安全情报模块，该模块会在出现涉及安全情报过滤的一些情况（包括防御中心无法更新源，或者源损坏或不包含可识别的 IP 地址）时发出警报。

互联网访问和高可用性

系统使用 443/HTTPS 端口下载情报源，使用 443/HTTP 或 80/HTTP 端口下载自定义源或第三方源。要更新源，必须打开防御中心上的相应端口（包括入站和出站）。如果防御中心无法直接访问源站点，可使用代理服务器（请参阅第 64-8 页上的配置管理接口）。

注 防御中心在下载自定义源时**不**执行对等 SSL 证书验证，系统也不支持使用证书捆绑包或自签证书来验证远程对等设备。

虽然安全情报对象同步在高可用性部署中的防御中心之间同步，但只有主防御中心会下载更新。如果主防御中心发生故障，您不仅必须确保辅助防御中心能够访问源站点，还必须使用辅助防御中心上的网络界面将其升级为 `Active`。有关详细信息，请参阅第 4-13 页上的监控和更改高可用性状态。

管理源和列表

可以使用对象管理器的 Security Intelligence 页面创建和管理安全情报列表和源（统称为安全情报对象）。（有关创建和管理网络对象和对象组的信息，请参阅第 3-4 页上的使用网络对象。）

请注意，无法删除当前正用于已保存或已应用的访问控制策略的自定义列表或源。也不能删除全局列表，但可以移除单个 IP 地址。同样，虽然不能删除情报源，但对情报源进行编辑可以禁用或更改其更新频率。

安全情报对象快速参考

下表提供了可用于执行安全情报过滤的对象的快速参考。

表 3-1　　安全情报对象功能

容量	全局白名单或黑名单	情报源	自定义源	自定义列表	网络对象
使用方法	默认情况下在访问控制策略中	在所有访问控制策略中作为白名单或黑名单对象			
是否可以通过安全区域进行限制？	否	是	是	是	是
是否可以删除？	否	否	是，除非当前正用于已保存或已应用的访问控制策略		
对象管理器编辑功能	仅删除 IP 地址 （使用上下文菜单添加 IP 地址）	禁用或更改更新频率	完全修改	仅上传已修改列表	完全修改
修改后是否需要重新应用访问控制策略？	删除后需要重新应用 （添加 IP 地址后不需要重新应用）	否	否	是	是

有关创建管理和使用安全情报列表和源的详细信息，请参阅：

- 第 3-6 页上的使用全局白名单和黑名单
- 第 3-7 页上的使用情报源
- 第 3-8 页上的使用自定义安全情报源
- 第 3-9 页上的手动更新安全情报源
- 第 3-9 页上的使用自定义安全情报列表
- 第 13-1 页上的使用安全情报 IP 地址信誉实施黑名单

使用全局白名单和黑名单

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

在分析过程中，可以使用事件视图、 Context Explorer 或控制面板中的 IP 地址上下文菜单创建安全情报*全局黑名单*。例如，如果注意到入侵事件中的一组可路由 IP 地址涉及漏洞攻击尝试，可以立即将这些 IP 地址添加到黑名单。还可以按类似方式建立*全局白名单*。

默认情况下，每个访问控制策略中都包含系统的全局白名单和全局黑名单，它们应用于所有区域。可以为每个策略选择是否使用这些全局列表。

将 IP 地址添加到全局列表时，防御中心会自动更新其受管设备。尽管可能需要等待几分钟，更改才会在部署中生效，但向全局列表添加 IP 地址后无需重新应用访问控制策略。相反，从全局白名单或黑名单删除 IP 地址后，必须应用访问控制策略，更改才会生效。

请注意，尽管可以将子网掩码为 /0 的网络对象添加到白名单或黑名单，但这些对象中使用 `/0` 子网掩码的地址块将被忽略，并且不会基于这些地址进行白名单和黑名单过滤。安全情报源中子网掩码为 `/0` 的地址块将被忽略。如果希望监控或阻止策略所针对的所有流量，请分别使用具有 **Monitor** 或 **Block** 规则操作的访问控制规则，并使用 **Source Networks** 和 **Destination Networks** 的默认值 **any**，而不使用安全情报过滤。

由于将 IP 地址添加到全局白名单或黑名单会影响访问控制，因此必须具有以下其中一种权限或角色：

- 管理员访问权限
- 默认角色的组合：网络管理员或访问管理员，加上安全分析师和安全审批人
- 同时具有修改访问控制策略和应用访问控制策略权限的自定义角色；请参阅第 12-3 页上的使用自定义用户角色管理部署

要使用上下文菜单将 IP 地址添加到全局白名单或黑名单：

访问：管理员/自定义

步骤 1　在事件视图、数据包视图、 Context Explorer 或控制面板中，将指针悬停在某个 IP 地址热点上。

提示　在事件视图或控制面板中，请将指针悬停在某个 IP 地址上，而不是该地址左侧的主机图标 () 上。

步骤 2　调用上下文菜单：

- 在事件视图或控制面板中，右键单击。
- 在 Context Explorer 或数据包视图中，左键单击。

步骤 3　从上下文菜单中，选择 **Whitelist Now** 或 **Blacklist Now**。

有关上下文菜单中其他选项的信息，请参阅第 2-4 页上的使用上下文菜单。

步骤 4　确认要将 IP 地址添加到白名单或黑名单。

在防御中心将您所做的添加通知其受管设备后，您的部署将根据更改开始过滤流量。

从全局白名单或黑名单移除 IP 地址：

访问：管理员/网络管理员

步骤 1　在对象管理器的 Security Intelligence 页面上，点击全局白名单或黑名单旁边的编辑图标 ()。

系统将显示 Global Whitelist 或 Global Blacklist 弹出窗口。

步骤 2　点击列表中要移除的 IP 地址旁边的删除图标 ()。

要一次删除多个 IP 地址，请使用 Shift 和 Ctrl 键选择要删除的 IP 地址，然后右键单击并选择 **Delete**。

步骤 3　点击 **Save**。

更改保存成功，但必须应用访问控制策略后更改才会生效。

使用情报源

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

为了帮助您构建黑名单，思科提供了 *Intelligence Feed*（有时称为 *Sourcefire Intelligence Feed*），其中包括 VRT 确定为信誉不佳的 IP 地址的多个列表，这些列表会定期更新。情报源中的每个列表均代表一个特定类别：开放中继、已知攻击者、伪造 IP 地址（虚假）等。在访问控制策略中，可以将任何或所有类别加入到黑名单。

由于情报源会定期更新，因此系统可以使用最新信息来过滤网络流量。恶意 IP 地址是指诸如恶意软件、垃圾邮件、僵尸网络以及网络钓鱼的安全威胁，它们的出现和消失速度要快于更新和应用新策略的速度。

虽然不能删除情报源，但对情报源进行编辑可以更改其更新频率。默认情况下，源每两小时更新一次。

要修改情报源的更新频率，请执行以下操作：

访问：管理员/网络管理员

步骤 1　在对象管理器的 Security Intelligence 页面上，点击 Sourcefire Intelligence Feed 旁的编辑图标（  ）。

系统将显示 Sourcefire Security Intelligence 弹出窗口。

步骤 2　编辑 **Update Frequency**。

可选择从两小时到一周不等的时间间隔。也可以禁用源更新。

步骤 3　点击 **Save**。

已保存您的更改。

使用自定义安全情报源

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

自定义或第三方安全情报源允许您使用互联网上其他定期更新且信誉良好的白名单和黑名单来扩充情报源。也可以设置内部源；如果要使用一个源列表来更新部署中的多个防御中心，这将会很有用。

配置源时，可使用 URL 指定位置；但 URL 不能使用 Punycode 编码。默认情况下，防御中心会按照配置的时间间隔下载整个源列表，然后自动更新其受管设备。

或者，可以将系统配置为使用 md5 校验和来确定是否下载更新的源。如果校验和自防御中心上一次下载源以来没有更改，系统不需要重新下载该源。您可能希望将 md5 校验和用于内部源，尤其是那些很大的内部源。 md5 校验和必须存储在仅带有该校验和的简单文本文件中。不支持注释。

要配置安全情报源：

访问：管理员/入侵管理员

步骤 1　在对象管理器的 Security Intelligence 页面上，点击 **Add Security Intelligence**。

系统将显示 Security Intelligence 弹出窗口。

步骤 2　在 **Name** 字段中为源键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 3　从 **Type** 下拉列表中指定要配置 **Feed**。

弹出窗口将会更新以显示新的选项。

步骤 4　指定**源 URL**，或者，还可以指定 **MD5 URL**。

步骤 5　从 **Update Frequency** 选择更新频率。

可选择从两小时到一周不等的时间间隔。也可以禁用源更新。

步骤 6　点击 **Save**。

安全情报源对象创建成功。除非已禁用源更新，否则防御中心会尝试下载并验证源。现在，您可以在访问控制策略中使用该源对象。

手动更新安全情报源

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

手动更新安全情报源会更新所有源（包括情报源）。

要更新所有安全情报源：

访问：管理员/访问管理员/网络管理员

步骤 1　在对象管理器的 Security Intelligence 页面上，点击 **Update Feeds**。

步骤 2　确认要更新所有源。

系统显示确认对话框，警告您更新可能需要几分钟才能生效。

步骤 3　点击 **OK**。

防御中心下载和验证源更新后，会将任何更改通知其受管设备。您的部署开始使用更新的源过滤流量。

使用自定义安全情报列表

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

安全情报列表是手动上传到防御中心的简单静态 IP 地址和地址块列表。如果要扩充和微调单个防御中心的受管设备的源或其中一个全局列表，自定义列表很有用。

请注意，地址块的子网掩码可以是 0 到 32 之间的任意整数或 0 到 128 之间的任意整数（分别适用于 IPv4 和 IPv6）。

例如，如果信誉良好的源错误地阻止了对重要资源的访问，但整体来说该源对您的组织很有用，您可以创建仅包括分类不当的 IP 地址的自定义白名单，而不从访问控制策略的黑名单中移除该安全情报源对象。

请注意，要修改安全情报列表，必须更改源文件并上传新副本。有关详细信息，请参阅第 3-10 页上的更新安全情报列表。

要将新的安全情报列表上传到防御中心：

访问：管理员/访问管理员/网络管理员

步骤 1　在对象管理器的 Security Intelligence 页面上，点击 **Add Security Intelligence**。

系统将显示 Security Intelligence 弹出窗口。

步骤 2　在 **Name** 字段中为列表键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 3　从 **Type** 下拉列表中指定要上传 **List**。

弹出窗口将会更新以显示新的选项。

步骤 4　点击 **Browse** 浏览至列表 `.txt` 文件，然后点击 Upload。

列表上传成功。弹出窗口将显示系统在列表中查找到的 IP 地址和地址块的总数。

如果显示的数字不是您期望的值，请检查文件格式并重试。

步骤 5　点击 **Save**。

安全情报列表对象保存成功。现在，您可以在访问控制策略中使用该列表对象。

更新安全情报列表

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

要编辑安全情报列表，必须更改源文件并上传新副本。不能使用防御中心的网络界面来修改文件内容。如果您无法访问源文件，可以从防御中心下载副本。

要修改安全情报列表：

访问：管理员/访问管理员/网络管理员

步骤 1　在对象管理器的 Security Intelligence 页面上，点击要更新的列表旁边的编辑图标 ( )。

系统将显示 Security Intelligence 弹出窗口。

步骤 2　如果需要列表副本进行编辑，请点击 **Download**，然后按照浏览器的提示将列表保存为文本文件。

步骤 3　根据需要对列表进行更改。

步骤 4　在 Security Intelligence 弹出窗口中，点击 **Browse** 浏览到修改后的列表，然后点击 **Upload**。

列表上传成功。

步骤 5　点击 **Save**。

已保存您的更改。如果列表正由活动访问控制策略使用，则必须应用策略，更改才会生效。

使用端口对象

许可证：任何环境

端口对象以略有不同的方式代表不同协议：

- 对于 TCP 和 UDP，端口对象代表传输层协议（协议号括在括号内，加上一个可选的相关端口或端口范围）。例如：`TCP(6)/22`。
- 对于 ICMP 和 ICMPv6 (IPv6-ICMP)，端口对象代表互联网层协议以及可选类型和代码。例如：`ICMP(1):3:3`。
- 端口对象还可以代表不使用端口的其他协议。

请注意，思科提供已知端口的默认端口对象。可以修改或删除这些对象，但思科建议您创建自定义端口对象。

可在系统网络界面中的不同位置使用端口对象和对象组（请参阅第 3-2 页上的将对象分组），包括访问控制策略、网络发现规则、端口变量和事件搜索。例如，如果您的组织使用的自定义客户端使用特定范围的端口并导致系统生成过多误导事件，可以配置网络发现策略来排除对这些端口的监控。

不能删除正在使用的网络端口。此外，在编辑用于访问控制、网络发现或入侵策略的端口对象后，必须重新应用策略，才能使更改生效。

请注意，不能为访问控制规则中的源端口条件添加除 TCP 或 UDP 以外的任何协议。此外，在规则中设置源端口条件和目标端口条件时，不能混用传输协议。

如果要将不受支持的协议添加到用于源端口条件的端口对象组，则应用策略时使用该协议的规则不会应用于受管设备。此外，如果创建同时包含 TCP 和 UDP 端口的端口对象，然后将其添加为规则的源端口条件，则不能添加目标端口，反之亦然。

要创建端口对象：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **Port** 下，选择 **Individual Objects**。

步骤 3　点击 **Add Port**。

系统将显示 Port Objects 弹出窗口。

步骤 4　在 **Name** 字段中为端口对象键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　选择 **Protocol**。

可以快速选择 **TCP**、**UDP**、**IP**、**ICMP** 或 **IPv6-ICMP**，或者使用 **Other** 下拉列表选择其他协议或选择 **All**。

步骤 6　或者，使用 **Port** 或端口范围限制 TCP 或 UDP 端口对象。

可以指定 1 到 65535 之间的任何端口，或者指定 any 以匹配所有端口。使用连字符可指定端口范围。

步骤 7　或者，使用 **Type** 和相关 **Code**（如果适当）限制 ICMP 或 IPV6-ICMP 端口对象。

创建 ICMP 或 IPv6 ICMP 对象时，可以指定类型和代码（如适用）。有关 ICMP 类型和代码的详细信息，请参阅：

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

可以将类型设置为 any 以匹配任意类型，或者将代码设置为 any 以匹配指定类型的任意代码。

步骤 8　或者，选择 **Other** 并从下拉列表中选择协议。如果选择 **All**，请在 **Port** 字段中键入端口号。

步骤 9　点击 **Save**。

端口对象添加成功。

使用 VLAN 标记对象

许可证：任何环境

配置的每个 VLAN 标记对象代表一个 VLAN 标记或标记范围。可在系统网络界面中的不同位置使用 VLAN 标记对象和对象组（请参阅第 3-2 页上的将对象分组），包括访问控制策略和事件搜索。例如，可以编写仅适用于特定 VLAN 的访问控制规则。

不能删除正在使用的 VLAN 标记对象。此外，在编辑用于访问控制策略的 VLAN 标记对象后，必须重新应用策略，才能使更改生效。

要添加 VLAN 标记对象：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **VLAN Tag** 下，选择 **Individual Objects**。

步骤 3　点击 **Add VLAN Tag**。

系统将显示 VLAN Tag 弹出窗口。

步骤 4　在 **Name** 字段中为 VLAN 标记键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　在 **VLAN Tag** 字段中，键入 VLAN 标记的值。

可以指定 1 到 4094 之间的任何 VLAN 标记。使用连字符可指定 VLAN 标记范围。

步骤 6　点击 **Save**。

VLAN 标记对象添加成功。

使用 URL 对象

许可证：任何环境

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

配置的每个 URL 对象代表单个 URL 或 IP 地址。可在系统网络界面中的不同位置使用 URL 对象和对象组（请参阅第 3-2 页上的将对象分组），包括访问控制策略和事件搜索。例如，可以编写阻止特定网站的访问控制规则。

在创建 URL 对象时，特别是如果未将 SSL 检查配置解密或阻止已加密的流量，请记住以下要点：

- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公用密钥中的主题公用名创建该对象。此外，系统会忽略在主题公用名中的子域，因此，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

- 当使用包括 URL 条件的访问控制规则匹配网络流量时，系统会忽略加密协议（HTTP 和 HTTPS ）。换句话说，如果阻止网站，将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个应用条件细化该规则。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 `example.com` 而不是 `http://example.com/` 。

有关详细信息，请参阅第 19-1 页上的了解流量解密和第 16-7 页上的阻止 URL

不能删除正在使用的 URL 对象。此外，在编辑用于访问控制策略的 URL 对象后，必须重新应用策略，才能使更改生效。

要添加 URL记对象：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **URL** 下，选择 **Individual Objects**。

步骤 3　点击 **Add URL**。

系统将显示 URL Objects 弹出窗口。

步骤 4　在 **Name** 字段中为 URL 对象键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　键入 URL 对象的 **URL** 或 IP 地址。您**不能**在此字段中使用通配符 (*)。

步骤 6　点击 **Save**。

URL 对象添加成功。

使用应用过滤器

许可证：FireSIGHT

受支持的设备：任何防御中心，除了 2 系列

FireSIGHT 系统分析 IP 流量时，会尝试识别网络上常用的应用。应用感知是执行基于应用的访问控制的关键。系统随附适用于许多应用的检测器，而且思科经常通过系统和漏洞数据库 (VDB) 更新和添加更多检测器。您还可以创建自己的应用协议检测器，以此增强系统的检测能力。

应用过滤器根据与应用的风险、业务相关性、类型、类别和标记相关联的条件对应用进行分组；请参阅第 45-9 页上的表 45-2。创建应用协议检测器时，也必须使用这些条件来确定应用的特征。使用应用过滤器可以快速为访问控制规则创建应用条件，因为无需逐个搜索和添加应用；有关详细信息，请参阅第 16-3 页上的将流量与应用过滤器相匹配。

使用应用过滤器的另一个好处是，修改或添加新应用时，无需更新使用过滤器的访问控制规则。例如，如果配置访问控制策略阻止所有社交网络应用，并且 VDB 更新包括新的社交网络应用检测器，更新该 VDB 时就会更新该策略。虽然必须先重新应用策略，系统才可以阻止新应用，但无需更新阻止该应用的访问控制规则。

如果思科提供的应用过滤器未根据您的需求对应用分组，您可以创建自己的过滤器。用户定义的过滤器可以对思科提供的过滤器进行分组和组合。例如，您可以创建可阻止所有非常高风险、低业务相关性应用的过滤器。还可以通过手动指定单个应用程序创建过滤器，但请谨记，更新系统软件或 VDB 时，这些过滤器**不**会自动更新。

可以在访问控制规则中使用用户定义的应用过滤器，就像使用思科提供的应用过滤器一样。还可以出于以下目的使用用户定义的过滤器：

- 要使用事件查看器搜索应用；请参阅第 60-5 页上的在搜索中使用对象和应用过滤器
- 要限制报告模板中的表视图；请参阅第 57-16 页上的使用报告模板部分中的搜索
- 要过滤 Custom Analysis 控制面板构件中的应用统计信息；请参阅第 55-13 页上的配置 Custom Analysis 构件

可使用对象管理器 (**Objects > Object Management**) 创建和管理应用过滤器。请注意，还可以在向访问控制规则添加应用条件时快速创建应用过滤器。

Application Filters 列表包括思科提供的应用过滤器，您可以选择它们来构建自己的过滤器。可以使用搜索字符串来限制显示的过滤器；这对类别和标记尤其有用。

Available Applications 列表包含所选过滤器中的各个应用。还可以使用搜索字符串来限制显示的应用。

系统将同一类型的多个过滤器与 OR 操作关联。假设一个中等风险过滤器包含 100 个应用，一个高风险过滤器包含 50 个应用。如果同时选择两个过滤器，系统将显示 150 个可用的应用。

系统将不同类型的过滤器与 AND 操作关联。例如，如果选择中等风险和高风险过滤器，以及中等业务相关性和高业务相关性过滤器，系统将显示具有中等或高风险的应用，以及具有中等或高业务相关性的应用。

提示　点击信息图标 ( ) 可获得相关应用的详细信息。要显示其他信息，请点击弹出窗口中的任意互联网搜索链接。

在确定要添加到过滤器的应用后，可以逐个添加这些应用，或者，如果选择了应用过滤器，可选择 **All apps matching the filter**。可以添加多个过滤器和多个应用的任意组合，只要 Selected Applications and Filters 列表中的总项数不超过 50。

创建的应用过滤器会在对象管理器的 Application Filters 页面上列出。该页面显示组成每个过滤器的条件总数。

有关对显示的应用过滤器进行排序和过滤的信息，请参阅第 3-2 页上的使用对象管理器。请注意，不能删除正在使用的应用过滤器。此外，在编辑用于访问控制策略的应用过滤器后，必须重新应用策略，才能使更改生效。

要创建应用过滤器：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　点击 **Application Filters**。

系统将显示 Application Filters 部分。

步骤 3　点击 **Add Application Filter**。

系统将显示 Application Filters 弹出窗口。

步骤 4　在 **Name** 字段中为过滤器提供名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　或者，在 **Application Filters** 列表中使用思科提供的过滤器，以减少要添加到过滤器的应用列表中的应用数量：

- 点击每种过滤器类型旁边的箭头可展开和折叠列表。

- 右键单击某种过滤器类型并点击 **Check All** 或 **Uncheck All**。请注意，列表会指示已选择的每种类型的过滤器数目。
- 要减少显示的过滤器，请在 **Search by name** 字段中键入搜索字符串；这对类别和标记尤其有用。要清除搜索，请点击清除图标 — ✖ 。
- 要刷新过滤器列表并清除所有选定的过滤器，请点击重新加载图标 ( )。
- 要清除所有过滤器和搜索字段，请点击 **Clear All Filters**。

与所选过滤器匹配的应用将会显示在 Available Applications 列表中。该列表每次显示 100 个应用。

步骤 6　从 **Available Applications** 列表中选择要添加到过滤器的应用：

- 选择 **All apps matching the filter** 可添加满足在上一步骤中指定的限制条件的所有应用。
- 要减少显示的应用，请在 **Search by name** 字段中键入搜索字符串。要清除搜索，请点击清除图标 (✖)。
- 使用位于列表底部的页码图标可浏览可用应用的列表。
- 使用 Shift 和 Ctrl 键可选择多个应用。右键单击并选择 **Select All** 可全部选择当前显示的应用。
- 要刷新应用列表并清除所有选定的应用，请点击重新加载图标 ( )。

不能同时选择单个应用和 **All apps matching the filter**。

步骤 7　将所选应用添加到过滤器。可以点击并拖动，也可以点击 **Add to Rule**。

结果是以下项的组合：

- 所选的应用过滤器
- 所选的各个可用应用，或者 **All apps matching the filter**

最多可以将 50 个应用和过滤器添加到过滤器。要从所选应用中删除应用或过滤器，请点击相应的删除图标 ( )。还可以选择一个或多个应用和过滤器，或右键单击并选择 **Select All**，然后右键单击并选择 **Delete Selected**。

步骤 8　点击 **Save**。

应用过滤器保存成功。

使用变量集

许可证：保护

变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。还可以在入侵策略中使用变量表示规则抑制、自适应配置文件和动态规则状态中的 IP 地址。

提示　无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。

可以使用变量集对变量进行管理、自定义和分组。可以使用思科提供的默认变量集，也可以创建您自己的自定义变量集。可以在任何变量集中修改预定义默认变量，以及添加和修改用户定义的变量。

FireSIGHT 系统提供的大多数共享对象规则和标准文本规则都使用预定义的默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护的（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。

当变量更准确地反映网络环境时，规则更加有效。至少应修改默认变量集中的的默认变量，如第 3-16 页上的优化预定义默认变量中所述。通过确保变量（例如 $HOME_NET）正确地定义网络且 $HTTP_SERVERS 包括网络上的所有网络服务器，从而优化处理和监控所有相关系统的可疑活动。

要使用变量，请将变量集链接到与访问控制规则相关的入侵策略或访问控制策略的默认操作。默认情况下，默认设置集链接到访问控制策略使用的所有入侵策略。

有关详细信息，请参阅以下各节：

优化预定义默认变量

许可证：保护

默认情况下，FireSIGHT 系统提供一个默认变量集，它包含预定义默认变量。思科漏洞研究团队 (VRT) 使用规则更新来提供最新的入侵规则及其他入侵策略元素（包括默认变量）。有关详情，请参见第 66-13 页上的导入规则更新和本地规则文件。

由于思科提供的许多入侵规则使用预定义默认变量，因此，应该为这些变量设置适当的值。可以在任何或所有变量集中修改这些默认变量的值，具体取决于如何使用变量集识别网络流量。有关详情，请参见第 3-22 页上的添加和编辑变量。

注意事项 导入访问控制策略或入侵策略会以导入的默认变量覆盖默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。有关详细信息，请参阅第 A-4 页上的导入配置。

下表介绍思科提供的变量并指出通常需要修改哪些变量。要获得为网络定制自定义变量方面的帮助，请联系专业服务或支持部门。

表 3-2　　思科 提供的变量

Variable Name	说明	是否需要修改？
$AIM_SERVERS	定义已知的 AOL Instant Messenger (AIM) 服务器，并用于基于聊天的规则和查找 AIM 漏洞攻击的规则。	不需要。
$DNS_SERVERS	定义域名服务 (DNS) 服务器。如果创建专门影响 DNS 服务器的规则，可以使用 $DNS_SERVERS 变量作为目标或源 IP 地址。	在当前规则集中不需要。
$EXTERNAL_NET	定义 FireSIGHT 系统视为未受保护的网络，并在许多规则中用于定义外部网络。	需要；应该充分定义 $HOME_NET，然后避免将 $HOME_NET 作为 $EXTERNAL_NET 的值。

表 3-2　　思科（续）提供的变量

Variable Name	说明	是否需要修改？
$FILE_DATA_PORTS	定义非加密端口，用于检测网络数据流中的文件的入侵规则。	不需要。
$FTP_PORTS	定义网络上 FTP 服务器的端口，用于 FTP 服务器漏洞攻击规则。	如果 FTP 服务器使用除默认端口以外的端口，需要修改（可以在网络界面中查看默认端口）。
$GTP_PORTS	定义数据包解码器用于提取 GTP（通用分组无线业务 [GPRS] 隧道协议）PDU 中的负载的数据信道端口。	不需要。
$HOME_NET	定义相关入侵策略监控的网络，用于许多定义内部网络的规则。	需要，以便包括内部网络的 IP 地址。
$HTTP_PORTS	定义网络上 FTP 服务器的端口，用于网络服务器漏洞攻击规则。	如果网络服务器使用除默认端口以外的端口，需要修改（可以在网络界面中查看默认端口）。
$HTTP_SERVERS	定义网络上的网络服务器。用于网络服务器漏洞攻击规则。	如果运行 HTTP 服务器，需要修改。
$ORACLE_PORTS	定义网络上的 Oracle 数据库服务器端口，用于扫描针对 Oracle 数据库的攻击的规则。	如果运行 Oracle 服务器，需要修改。
$SHELLCODE_PORTS	定义希望系统对其扫描外壳代码漏洞的端口，用于检测使用外壳代码的漏洞的规则。	不需要。
$SIP_PORTS	定义网络上 SIP 服务器的端口，用于 SIP 漏洞攻击规则。	不需要。
$SIP_SERVERS	定义网络上的 SIP 服务器，用于针对 SIP 的漏洞攻击的规则。	需要；如果运行 SIP 服务器，应该充分定义 $HOME_NET，然后包括 $HOME_NET 作为 $SIP_SERVERS 的值。
$SMTP_SERVERS	定义网络上的 SMTP 服务器，用于解决针对邮件服务器的漏洞的规则。	如果运行 SMTP 服务器，需要修改。
$SNMP_SERVERS	定义网络上的 SNMP 服务器，用于扫描针对 SNMP 服务器的攻击的规则。	如果运行 SNMP 服务器，需要修改。
$SNORT_BPF	代表一个旧版的高级变量，仅当该变量存在于安装了 V5.3.0 之前的 FireSIGHT 系统软件的系统，随后软件升级到 V5.3.0 或更高版本的情况下，才会显示该变量。请参阅第 3-28 页上的了解高级变量。	不需要，只能查看或删除此变量。删除此变量后不能对其进行编辑或恢复。
$SQL_SERVERS	定义网络上的数据库服务器，用于解决针对数据库的漏洞的规则。	如果运行 SQL 服务器，需要修改。
$SSH_PORTS	定义网络上 SSH 服务器的端口，用于 SSH 服务器漏洞规则。	如果 SSH 服务器使用除默认端口以外的端口，需要修改（可以在网络界面中查看默认端口）。
$SSH_SERVERS	定义网络上的 SSH 服务器，用于解决针对 SSH 的漏洞的规则。	需要修改；如果运行 SSH 服务器，应该充分定义 $HOME_NET，然后包括 $HOME_NET 作为 $SSH_SERVERS 的值。
$TELNET_SERVERS	定义网络上的已知 Telnet 服务器，用于解决针对 Telnet 的漏洞的规则。	如果运行 Telnet 服务器，需要修改。

表 3-2　　思科 （续）提供的变量

Variable Name	说明	是否需要修改？
$USER_CONF	提供一个通用工具，让您能够配置无法通过网络界面使用的一个或多个功能。请参阅第 3-28 页上的了解高级变量。 ⚠ **注意事项** 存在冲突或重复的 $USER_CONF 配置会导致系统停止。请参阅第 3-28 页上的了解高级变量。	不需要，除非功能描述中有指示或在支持人员的指导下进行。

了解变量集

许可证：保护

将一个变量添加到任意变量集会将其添加到所有变量集；也就是说，每个变量集都是系统中当前配置的所有变量的集合。在任何变量集中，都可以添加用户定义的变量以及自定义任何变量的值。

最初， FireSIGHT 系统提供由预定义默认值组成的单个默认变量集。默认变量集中的每个变量最初设置为其默认值，对于预定义变量，该默认值是由 VRT 设置并在规则更新中提供的值。

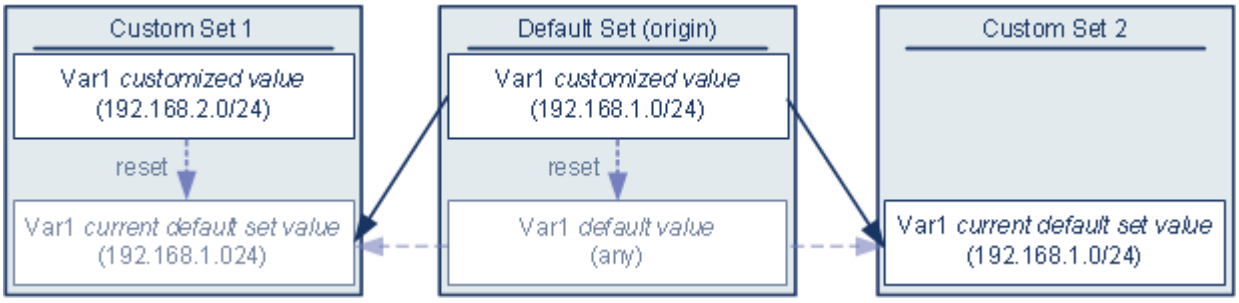
虽然可以将预定义默认变量保留为所配置的默认值，但思科建议您修改预定义变量的子集，如第 3-16 页上的优化预定义默认变量中所述。

可以仅使用默认变量集中的变量，但在许多情况下，执行以下操作可得到最大益处：添加一个或多个自定义变量集；在不同变量集中配置不同的变量值；甚至添加新变量。

使用多个变量集时务必谨记，默认变量集中任何变量的*当前值*决定所有其他变量集中该变量的*默认值*。

示例：将用户定义的变量添加到默认变量集

下图说明了将用户定义的变量 Var1 （其值为 192.168.1.0/24）添加到默认变量集时发生的变量集交互。



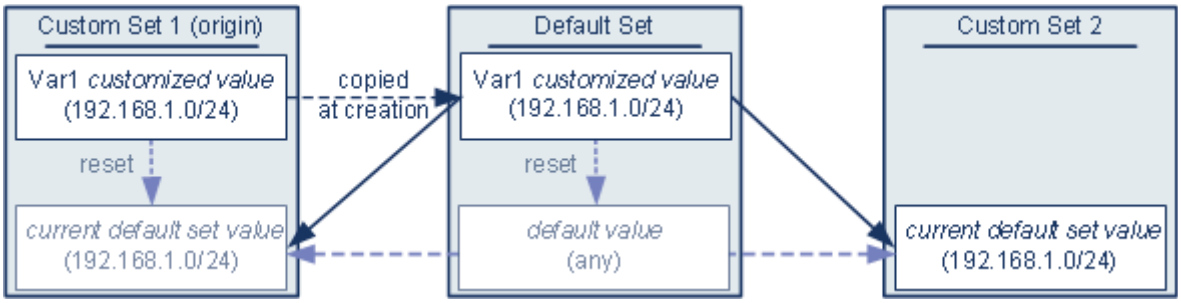
或者，可以在任何变量集中自定义 Var1 的值。在未自定义 Var1 的自定义变量集 2 中，此变量的值是 192.168.1.0/24。在自定义变量集 1 中， Var1 的自定义值 192.168.2.0/24 覆盖了默认值。重置默认变量集中某个用户定义的变量会将所有变量集中该变量的默认值重置为 any。

须注意的一点是，在本示例中，如果不更新自定义变量集 2 中的 Var1，进一步自定义或重置默认变量集中的 Var1 会导致更新自定义变量集 2 中 Var1 的默认值，从而影响与变量集相关联的所有入侵策略。

请注意，虽然在本示例中未显示，但用户定义的变量和默认变量的变量集交互是相同的，唯一不同的是重置默认变量集中的默认变量会在当前规则更新中将其值重置为由思科配置的值。

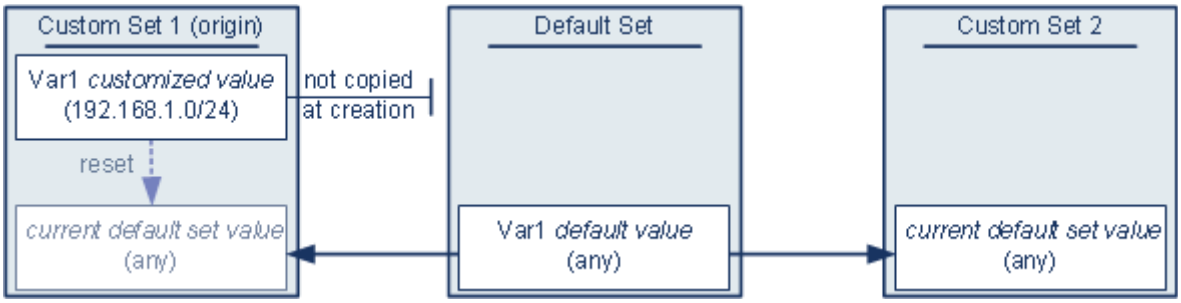
示例：将用户定义的变量到添加到自定义变量集

以下两个示例说明了将用户定义的变量添加到自定义变量集时变量集之间的交互。保存新变量时，系统会提示您选择是否将配置值用作其他变量集的默认值。在以下示例中，您选择**使用**配置值。



请注意，除了 Var1 来自自定义变量集 1 以外，本示例与以上将 Var1 添加到默认变量集的示例完全相同。将 Var1 的自定义值 192.168.1.0/24 添加到自定义变量集 1 会将该值复制到默认变量集，以作为默认值为 any 的自定义值。之后，Var1 值和交互就像之前将 Var1 添加到默认变量集一样。请记住，与前一个示例一样，进一步自定义或重置默认变量集中的 Var1 会导致更新自定义变量集 2 中 Var1 的默认值，从而影响与变量集相关联的所有入侵策略。

在下一个示例中，像前一个示例一样，将 Var1（其值为 192.168.1.0/24）添加到自定义变量集 1，但选择**不使用** Var1 的配置值作为其他变量集中的默认值。



此方法会将 Var1（其默认值为 any）添加到所有变量集。添加 Var1 后，可以在任何变量集中自定义它的值。此方法的优点是，通过最初不在默认变量集中自定义 Var1，可以降低这样的风险：在默认变量集中自定义此变量的值时，无意中更改了尚未自定义 Var1 的变量集（例如，自定义变量集 2）中的当前值。

管理变量集

许可证：保护

如果选择 Object Manager 页面 (**Objects > Object Management**) 上的 **Variable Sets**，对象管理器会列出默认变量集以及您创建的所有自定义变量集。

在一个全新安装的系统上，默认变量集仅包括思科预定义的默认变量。

每个变量集都包括思科提供的默认变量以及从任何变量集添加的所有自定义变量。请注意，可以编辑默认变量集，但不能重命名或删除默认变量集。

注意事项　导入访问控制策略或入侵策略会以导入的默认变量覆盖默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。有关详细信息，请参阅第 A-4 页上的导入配置。

下表总结了可用于管理变量集的操作。

表 3-3　变量集管理操作

要.....	您可以.....
显示变量集	选择 **Objects > Object Management**，然后选择 **Variable Set**。
按名称过滤变量集	键入名称；当您键入时，页面会刷新以显示匹配的名称。
清除名称过滤	点击过滤器字段中的清除图标 (✖)。
添加自定义变量集	点击 **Add Variable Set**。 为方便使用，新变量集包括所有当前定义的默认和自定义变量。 **注**　变量集名称可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印的标准 ASCII 字符。
编辑变量集	点击要编辑的变量集旁边的编辑图标 ( )。 **提示**　可以在变量集的行中右键单击，然后选择 **Edit**。
删除自定义变量集	点击变量集旁边的删除图标 ( )，然后点击 **Yes**。不能删除默认变量集。请注意，在删除的变量集中创建的变量不会被删除，这些变量在其他变量集中也不会受到影响。 **提示**　可以在变量集的行中右键单击，选择 **Delete**，然后点击 **Yes**。使用 Ctrl 和 Shift 键可选择多个变量集。

在配置变量集后，可以将它们链接到入侵策略。

要创建或编辑变量集：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　选择 **Variable Set**。

步骤 3　添加变量集或编辑现有变量集：

- 要添加变量集，请点击 **Add Variable Set**。
- 要编辑变量集，请点击变量集旁边的编辑图标 ( )。

系统显示新建或编辑变量集页面。在命名变量集时，可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印的标准 ASCII 字符。有关添加或编辑变量集中的变量的信息，请参阅第 3-22 页上的添加和编辑变量。

管理变量

许可证：保护

可通过新建或编辑变量页面管理变量集中的变量。所有变量集的变量页面都将变量划分到 Customized Variables 和 Default Variables 页面区域。

*默认变量*是思科提供的变量。可以自定义默认变量的值。不能重命名或删除默认变量，也不能更改其默认值。

自定义*变量*是以下其中一种变量：

- 自定义的默认变量

  编辑默认变量的值时，系统会将该变量从 Default Variables 区域转移到 Customized Variables 区域。由于默认变量集中的变量值决定自定义变量集中变量的默认值，因此，自定义默认变量集中的默认变量会修改所有其他变量集中该变量的默认值。

- 用户定义的变量

  您可以添加和删除自己的变量，在不同变量集中自定义这些变量的值，以及将自定义变量重置为默认值。重置用户定义的变量时，该变量保留在 Customized Variables 区域。

下表总结了可用于创建或编辑变量的操作。

表 3-4　　变量管理操作

要.....	**您可以.....**
显示变量页面	在变量集页面上，点击 **Add Variable Set** 创建新变量集，或者点击要编辑的变量集旁边的编辑图标 ( )。
对变量集进行命名或者描述	在 **Name** 和 **Description** 字段中输入字母数字字符串 （可包含空格和特殊字符）。 **注**　变量集名称可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印的标准 ASCII 字符。
显示变量的完整值	将指针悬停在变量旁边的 **Value** 列中的值上。 **注**　变量的值最多可包含 8192 个字符。但请记住，此限制适用于变量的扩展值的大小。如果使用一个或多个变量来定义其他变量，所有变量值的字符和空格总数不能超过 8192 个字符。
添加变量	点击 **Add**。 有关详情，请参见第 3-22 页上的添加和编辑变量。
编辑变量	点击要编辑的变量旁边的编辑图标 ( )。 有关详情，请参见第 3-22 页上的添加和编辑变量。
将已修改变量重置为默认值	点击已修改变量旁边的重置图标 ( )。如果重置图标呈灰色显示，表示当前值已经是默认值。 **提示**　将指针悬停在活动的重置图标上可显示默认值。
删除用户定义的自定义变量	点击变量集旁边的删除图标 ( )；如果在添加该变量后已保存变量集，点击 **Yes** 确认要删除变量。 不能删除默认变量，也不能删除入侵规则或其他变量使用的用户定义的变量。
保存对变量集的更改	点击 **Save**，然后，如果访问控制策略正在使用该变量集，点击 **Yes** 确认要保存更改。 由于默认变量集中的当前值决定所有其他变量集中的默认值，因此，修改或重置默认变量集中的变量会更改未对该变量默认值进行自定义的那些变量集中的该变量当前值。

要查看变量集中的变量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　选择 **Variable Set**。

步骤 3　添加变量集或编辑现有变量集：

- 要添加变量集，请点击 **Add Variable Set**。
- 要编辑变量集，请点击变量集旁边的编辑图标 ( )。

系统显示新建或编辑变量集页面。在命名变量集时，可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印的标准 ASCII 字符。

步骤 4　要添加变量或编辑现有变量：

- 要添加变量，点击 **Add**。
- 要编辑变量，点击变量旁边的编辑图标 ( )。

系统显示新建或编辑变量页面。

有关添加或编辑变量集中的变量的信息，请参阅第 3-22 页上的添加和编辑变量。

添加和编辑变量

许可证：保护

可以修改任何自定义变量集中的变量。

如果您创建自定义标准文本规则，您可能还希望添加自己的用户定义的变量，以便更准确地反映您的流量或作为快捷方式简化规则创建过程。例如，如果创建只检查“隔离区”(DMZ) 中流量的规则，可以创建名为 `$DMZ` 的变量，其值列出已暴露的服务器 IP 地址。这样，在所有为该区域编写的所有规则中都可以使用 `$DMZ` 变量。

将变量添加到变量集会将其添加到所有其他变量集。除了下述一种例外情况，变量将被添加到其他变量集作为默认值，然后可以对默认值进行自定义。

添加自定义变量集中的变量时，必须选择是否使用配置值作为默认变量集中的自定义值。

- 如果**使用**配置的值（例如，192.168.0.0/16），变量添加到默认变量集时，将会使用配置值作为自定义值，且默认值为 `any`。由于默认变量集中的当前值决定在其他变量集中的默认值，因此，其他自定义变量集中的初始默认值为配置值（在本示例中为 192.168.0.0/16）。
- 如果**不使用**配置值，变量添加到默认变量集时，只会使用默认值 `any`，因此，其他自定义变量集中的初始默认值为 `any`。

有关详情，请参见第 3-18 页上的了解变量集。

可在 New Variable 页面上向变量集添加变量，在 Edit Variable 页面上编辑现有变量。这两个页面的使用方法相同，唯一不同之处在于，编辑现有变量时不能更改变量名称或变量类型。

这两个页面均主要包括三个窗口：

- 可用项目，包括现有网络或端口变量、对象和网络对象组
- 要包括在变量定义中的网络或端口
- 要从变量定义中排除的网络或端口

可以创建或编辑两种类型的变量：

- *网络*变量指定网络流量中的主机的 IP 地址。请参阅第 3-25 页上的使用网络变量。
- *端口*变量指定网络流量中的 TCP 或 UDP 端口，包括这两种端口类型的值 any。请参阅第 3-26 页上的使用端口变量。

指定是否要添加网络或端口变量类型时，页面会刷新以列出可用项目。在列表上方的搜索字段可用于对列表施加约束，该列表在您键入时会更新。

可以选择并拖动项目列表中的可用项目，以包括或排除这些项目。还可以选择项目并点击 **Include** 或 **Exclude** 按钮。使用 Ctrl 和 Shift 键可选择多个项目。可以使用包含或排除项目列表下方的配置字段为网络变量指定文本 IP 地址和地址块，并为端口变量指定端口和端口范围。

要包含或排除的项目列表可以包括原义字符串和现有变量、对象和网络对象组（对于网络变量）的任意组合。

下表总结了可用于创建或编辑变量的操作。

表 3-5　　变量编辑操作

要.....	您可以.....
显示变量页面	在变量集页面上，点击 **Add** 添加新变量，或者点击现有变量旁边的编辑图标 ( )。
为变量命名	在 **Name** 字段中，键入一个唯一的字母数字字符串 （区分大小写，不能包含除下划线字符 (_) 以外的特殊字符）。 请注意，变量名称区分大小写；例如， var 和 Var 是不同的。
指定网络或端口变量	从 **Type** 下拉列表中选择 **Network** 或 **Port**。 有关可以如何使用和配置网络和端口变量的详细信息，请参阅第 3-25 页上的使用网络变量和第 3-26 页上的使用端口变量。
添加单个网络对象以供随后在可用网络列表中选择	从 **Type** 下拉列表中选择 **Network**，然后点击添加图标 ( )。有关使用对象管理器添加网络对象的信息，请参阅第 3-4 页上的使用网络对象。
添加单个端口对象以供随后在可用端口列表中选择	从 **Type** 下拉列表中选择 **Port**，然后点击添加图标 ( )。 虽然可以添加任何端口类型，但只有 TCP 和 UDP 端口 （包括这两种端口类型的值 any）是有效变量值，可用端口列表仅显示使用这些值类型的变量。有关使用对象管理器添加端口对象的信息，请参阅第 3-10 页上的使用端口对象。
按名称搜索可用端口或网络项目	在可用项目列表上方的搜索字段中键入名称；当您键入时，页面会刷新以显示匹配的名称。
清除名称搜索	点击 Search 字段上方的重新加载图标 ( ) 或 Search 字段中的清除图标 ( )。
区分可用项目	查找变量图标 ( )、网络对象图标 ( )、端口图标 ( ) 和对象组图标 ( ) 旁边的项目。 请注意，仅网络组可用，端口组不可用。
选择在变量定义中要包括或排除的对象	点击可用网络或端口列表中的对象；使用 Ctrl 和 Shift 键可选择多个对象。
将选定项目添加到包含或排除的网络或端口列表	拖放选定项目 或者，点击 **Include** 或 **Exclude**。 可以从可用项目列表添加网络变量、端口变量、网络对象和端口对象。还可以添加网络对象组。
将文字网络或端口添加到要包括或排除的网络或端口列表	点击以从 **Network** 或 **Port** 文字字段中移除提示符，键入网络变量的文字 IP 地址或地址块，或者键入端口变量的端口或端口范围，然后点击 **Add**。 请注意，不能输入域名或列表；要添加多个项目，请逐个添加。

表 3-5　　变量编辑操作 （续）

要.....	您可以.....
添加具有值 any 的变量	给变量命名并选择变量类型，然后在不配置值的情况下点击 **Save**。 **注**　变量名称必须是一个唯一的字母数字字符串 （区分大小写，不能包含除下划线字符 (_) 以外的特殊字符）。
从包含或排除列表删除变量或对象	点击变量旁边的删除图标 ( )。
保存新的或修改后的变量	点击 **Save**；然后，如果要添加自定义变量集中的变量，点击 **Yes** 以使用配置值作为其他变量集中的默认值，或者点击 **No** 以使用默认值 any。

有关详细信息，请参阅以下各节：

- 第 3-25 页上的使用网络变量
- 第 3-26 页上的使用端口变量

要添加或编辑变量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　选择 **Variable Set**。

步骤 3　添加变量集或编辑现有变量集：

- 要添加变量集，请点击 **Add Variable Set**。
- 要编辑现有变量集，请点击变量集旁边的编辑图标 ( )。

系统显示新建或编辑变量集页面。在命名变量集时，可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印的标准 ASCII 字符。

步骤 4　要添加新变量或编辑现有变量：

- 要添加新变量，请点击 **Add**。
- 要编辑现有变量，请点击变量旁边的编辑图标 ( )。

系统显示新建或编辑变量页面。

提示　在变量页面上，可以使用右键单击上下文菜单选择或删除项目；请参阅第 2-4 页上的使用上下文菜单。

步骤 5　如果是添加新变量：

- 在 **Name** 字段中为变量输入一个唯一名称。

  可以使用字母数字字符和下划线 (_) 字符。
- 从 **Type** 下拉列表中选择 **Network** 或 **Port** 变量类型。

步骤 6　或者，将项目从可用网络或端口列表移至包含或排除项目列表。

可以选择一个或多个项目然后执行拖放操作，或者点击 **Include** 或 **Exclude**。使用 Ctrl 和 Shift 键可选择多个项目。

提示　如果网络或端口变量的包含变量列表和排除变量列表中的地址或端口重叠，排除的地址或端口优先。

步骤 7　或者，输入一个文字值，然后点击 **Add**。

对于网络变量，可以输入单个 IP 地址或地址块。对于端口变量，可以添加单个端口或端口范围，用连字符 (-) 隔开上限和下限值。

如有需要，可重复此步骤输入多个文字值。

步骤 8　点击 **Save** 保存变量。如果是添加自定义变量集中的新变量，有以下选项可供选择：

- 点击 **Yes** 添加使用配置值作为默认变量集中的自定义值（进而也是其他自定义变量集中的默认值）的变量。
- 点击 **No** 将变量添加为默认变量集中的默认值 `any`（进而在其他自定义变量集中也使用此默认值）。

步骤 9　完成更改后，点击 **Save** 保存变量集，然后点击 **Yes**。

更改保存成功，与该变量集链接的所有访问控制策略均显示为过期状态。要使更改生效，必须将与该变量集链接的访问控制策略应用于入侵策略；请参阅第 12-13 页上的应用访问控制策略。

使用网络变量

许可证：保护

网络变量代表可用于已在入侵策略、入侵策略规则抑制、动态规则状态和自适应配置文件中启用的入侵规则中的 IP 地址。网络变量与网络对象和网络对象组的不同之处在于，网络变量特定于入侵策略和入侵规则，但可以使用网络对象和网络对象组在系统网络界面中的不同位置（包括访问控制策略、网络变量、入侵规则、网络发现规则、事件搜索和报告等）来代表 IP 地址。有关详情，请参见第 3-4 页上的使用网络对象。

可在以下配置中使用网络变量来指定网络上主机的 IP 地址：

- 入侵规则

  入侵规则 **Source IPs** 和 **Destination IPs** 报头字段可用于限制仅检查来自或发往特定 IP 地址的数据包。请参阅第 36-5 页上的在入侵规则中指定 IP 地址。

- 抑制

  在特定 IP 地址或 IP 地址范围触发入侵规则或预处理器时，源或目标入侵规则抑制中的 **Network** 字段让您能够抑制入侵事件通知。请参阅第 32-24 页上的按入侵策略配置抑制。

- 动态规则状态

  源或目标动态规则状态中的 **Network** 字段让您能够检测在给定时间段内发生过多入侵规则或预处理器规则匹配的情况。请参阅第 32-26 页上的添加动态规则状态。

- 自适应配置文件

  自适应配置文件 **Networks** 字段识别网络图（您希望在其中改进被动部署中的数据包分段和 TCP 数据流的重组）中的主机。请参阅第 30-1 页上的调整被动部署中的预处理。

在本节中所述字段中使用变量时，链接至入侵策略的变量集决定使用该入侵策略的访问控制策略处理的网络流量中的变量值。

可以将以下网络配置的任意组合添加到变量：

- 从可用网络列表中选择的网络变量、网络对象和网络对象组的任意组合

有关使用对象管理器创建单个网络对象和成组网络对象的信息，请参阅第 3-4 页上的使用网络对象。

- 从 New Variable 或 Edit Variable 页面添加的单个网络对象（这些对象随后可添加到变量以及其他现有和将来的变量）
- 文字的、单个 IP 地址或地址块

  可以通过逐个添加来列出多个文字 IP 地址和地址块。可以单独列出 IPv4 和 IPv6 地址以及地址块，或者列出它们的任意组合。指定 IPv6 地址时，可使用 RFC 4291 中定义的任意寻址约定。

在任何变量中添加的包含网络的默认值是单词 `any`，它表示任意 IPv4 或 IPv6 地址。已排除网络的默认值为 `none`，它表示无网络。还可以使用文字值指定地址 `::`，以指示包含网络列表中的任何 IPv6 地址，或排除列表中没有 IPv6 地址。

将网络添加到排除列表会使指定的地址和地址块无效。也就是说，可以匹配除了被排除的 IP 地址或地址块以外的所有 IP 地址。

例如，排除文字地址 `192.168.1.1` 会指定除 192.168.1.1 以外的所有 IP 地址，排除 `2001:db8:ca2e::fa4c` 会指定除 2001:db8:ca2e::fa4c 以外的所有 IP 地址。

使用文字网络或可用网络可以排除任意的网络组合。例如，排除文字值 `192.168.1.1` 和 `192.168.1.5` 会*包含*除 192.168.1.1 或 192.168.1.5 以外的所有 IP 地址。也就是说，系统将此解释为“**既不是** 192.168.1.1 **也不是** 192.168.1.5”，这就会匹配除括号中列出的 IP 地址以外的所有 IP 地址。

添加或编辑网络变量时，请注意以下几点：

- 在逻辑上，不能排除值 `any`，如果排除该值，将表示无地址。例如，不能将具有值 `any` 的变量添加到排除网络列表。
- 网络变量为指定的入侵规则和入侵策略功能识别流量。请注意，无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。
- 排除值必须解析为包含值的子集。例如，不能包含地址块 192.168.5.0/24 并排除 192.168.6.0/24。如果这样做，系统将会显示警告错误消息并标识出违规的变量，而且，当您排除包含值范围之外的值时，将无法保存变量集。

有关添加和编辑网络变量的信息，请参阅第 3-22 页上的添加和编辑变量。

使用端口变量

许可证：保护

端口变量代表可在入侵策略中启用的入侵规则的 **Source Port** 和 **Destination Port** 报头字段中使用的 TCP 和 UDP 端口。端口变量与端口对象和端口对象组的不同之处在于，端口变量特定于入侵规则。可以为除 TCP 和 UDP 以外的其他协议创建端口对象，还可以在系统网络界面中的不同位置使用端口对象，包括端口变量、访问控制策略、网络发现规则和事件搜索。有关详情，请参见第 3-10 页上的使用端口对象。

可以在入侵规则 **Source Port** 和 **Destination Port** 报头字段中使用端口变量来限制仅检查来自或发往特定 TCP 或 UDP 端口的数据包。

在这些字段中使用变量时，链接到与访问控制规则或策略相关的入侵策略的变量集决定应用访问控制策略的网络流量中这些变量的值。

可以将以下端口配置的任意组合添加到变量：

- 从可用端口列表中选择的端口变量和端口对象的任意组合

  请注意，可用端口列表不显示端口对象组，而且不能将这些对象组添加到变量。有关使用对象管理器创建端口对象的信息，请参阅第 3-10 页上的使用端口对象。
- 从 New Variable 或 Edit Variable 页面添加的单个端口对象 （这些对象随后可添加到变量以及其他现有和将来的变量）

仅 TCP 和 UDP 端口（包括两种端口类型的值 any）是有效的变量值。如果使用新建或编辑变量页面添加不是有效变量值的有效端口对象，对象将被添加到系统，但不会显示在可用对象列表中。使用对象管理器编辑用于变量的端口对象时，只能将其值更改为有效的变量值。

- 单个文本端口值和端口范围

  必须使用破折号 (-) 隔开端口范围。带有冒号 (:) 的端口范围表示具有向后兼容性，但不能在创建的端口变量中使用冒号。

  可以通过逐个添加来列出多个文本端口值的任意组合。

添加或编辑端口变量时，请注意以下几点：

- 在任何变量中添加的包含端口的默认值是单词 any，它表示任意端口或端口范围。已排除端口的默认值为 none，它表示无端口。

提示 要创建一个值为 any 的变量，请在不添加具体值的情况下命名并保存该变量。

- 在逻辑上，不能排除值 any，如果排除该值，将表示无端口。例如，将具有值 any 的变量添加到排除端口列表时，无法保存变量集。
- 将端口添加到排除列表会使指定端口和端口范围失效。也就是说，可以匹配除了被排除的端口或端口范围以外的所有端口。
- 排除值必须解析为包含值的子集。例如，不能包含端口范围 10-50 并排除端口 60。如果这样做，系统将会显示警告错误消息并标识出违规的变量，而且，当您排除包含值范围之外的值时，将无法保存变量集。

有关添加和编辑端口变量的信息，请参阅第 3-22 页上的添加和编辑变量。

重置变量

许可证：保护

在变量集新建或编辑变量页面上，可以将变量重置为默认值。下表总结了重置变量的基本原则。

表 3-6　　变量重置值

要重置的变量类型	所属变量集类型	重置后的值
default	default	规则更新值
用户定义的变量	default	any
默认变量或用户定义的变量	custom	当前默认变量集值（已修改或未修改）

重置自定义变量集中的变量会将其重置为该变量在默认变量集中的当前值。

相反，重置或修改默认变量集中某个变量的值总是会更新所有自定义变量集中该变量的默认值。如果重置图标呈灰色显示，表示不能重置变量，这意味着该变量在该变量集中没有自定义值。除非自定义了自定义变量集中某个变量的值，否则对默认变量集中该变量的更改会更新与该变量集链接的任何入侵策略中使用的值。

注 一种好的做法是，在修改默认变量集中的某个变量时，评估这些更改如何影响在已链接自定义变量集中使用该变量的任何入侵策略，尤其是在自定义变量集中未对该变量值进行自定义时。

将指针悬停在变量集中的重置图标 ( ) 上可查看重置值。当自定义值和重置值相同时，这表示以下其中一种情况属实：

- 您在自定义或默认变量集中，而且在其中添加了值为 `any` 的变量
- 您在自定义变量集中，在其中添加了具有显式值的变量，并且选择了使用配置值作为默认值

将变量集链接到入侵策略

许可证：保护

默认情况下， FireSIGHT 系统会将默认变量集链接到访问控制策略中使用的所有入侵策略。应用使用入侵策略的访问控制策略时，在入侵策略中已启用的入侵规则使用链接的变量集中的变量值。

修改访问控制策略中的入侵策略所使用的自定义变量集时，系统会反映该策略的状态，在 Access Control 页面上将其状态显示为过时。必须重新应用该访问控制策略，才能使变量集的更改生效。修改默认变量集时，系统会将使用入侵策略的所有访问控制策略的状态显示为过时，因此，必须重新应用所有访问控制策略才能使更改生效。

有关信息，请参阅以下各节：

- 要将除默认变量集外的其他变量集链接到访问控制规则，请参阅第 18-5 页上的配置访问控制规则以执行入侵防御中所述的步骤。
- 要将除默认变量集外的其他变量集链接到访问控制策略的默认操作，请参阅第 12-6 页上的设置对网络流量的默认处理和检查。
- 要应用访问控制策略（包括将变量集链接到入侵策略的策略），请参阅第 12-13 页上的应用访问控制策略。

了解高级变量

许可证：保护

高级变量让您能够配置通常无法通过网络界面配置的功能。 FireSIGHT 系统目前仅提供两个高级变量，因此您只能编辑 USER_CONF 高级变量。

USER_CONF

USER_CONF 提供一个通用工具，让您能够配置无法通过网络界面使用的一个或多个功能。

注意事项 请勿使用高级变量 USER_CONF 来配置入侵策略功能，除非功能描述或支持人员指示您这样做。存在冲突或重复的配置会导致系统停止。

编辑 USER_CONF 时，可以在单行中最多输入总共 4096 个字符；达到该限制后，行会自动换行。可以包含任意数量的有效说明或行，直至达到变量的最大字符长度限制（8192 个字符）或物理限制（例如磁盘空间）。在命令指令中，可以在任何完整参数之后使用反斜杠 (\) 续行符。

重置 USER_CONF 会将其清空。

SNORT_BPF

SNORT_BPF 是一个旧版的高级变量，仅当该变量存在于安装了 V5.3.0 之前的 FireSIGHT 系统软件的系统，随后软件升级到 V5.3.0 或更高版本的情况下，才会显示该变量。只能查看或删除此变量。删除此变量后不能对其进行编辑或恢复。

借助此变量，可以在流量到达系统之前对流量应用 Berkeley 数据包过滤器 (BPF)。如果 SNORT_BPF 提供访问控制规则，应使用这些规则而不是此变量来强制执行过滤。此变量仅出现在系统升级之前存在的配置中。

使用文件列表

许可证：恶意软件

受支持的设备：除 2 系列或 X -系列外的所有型号

受支持的防御中心：除 DC500 外的所有型号

如果使用基于网络的高级恶意软件防护 (AMP)，而且综合安全智能云错误地识别某个文件的性质，则可以使用 SHA-256 哈希值将该文件添加到*文件列表*，以便将来能够更好地检测该文件。根据文件列表的类型，可以执行以下操作：

- 要好像云已为文件分配了安全性质一样对其进行处理，请将文件添加到*白名单*。
- 要好像云已为文件分配了恶意软件性质一样对其进行处理，请将文件添加到*自定义检测列表*。

由于您手动指定这些文件的阻止行为，因此，系统将不会执行恶意软件云查找，即使这些文件被云识别为恶意软件。请注意，必须为文件策略中的某个规则配置 **Malware Cloud Lookup** 或 **Block Malware** 操作和匹配的文件类型，以计算文件的 SHA 值。有关详细信息，请参阅第 37-15 页上的使用文件规则。

默认情况下，每个文件策略中都包含系统的白名单和自定义检测列表。可以为每个策略选择不使用这两个列表中的任何一个或者都不使用。

注意事项 请**勿**在白名单中包含实际上是恶意软件的文件。系统不会阻止它们，即使云已为这些文件分配了恶意软件性质，或者已将它们添加到自定义检测列表。

每个文件列表最多可以包含 10000 个唯一的 SHA-256 值。要将文件添加到文件列表，可执行以下操作：

- 使用事件查看器上下文菜单添加 SHA-256 值。
- 上传文件，以便系统计算并添加文件的 SHA-256 值。
- 直接输入文件的 SHA-256 值。
- 创建并上传包含多个 SHA-256 值的逗号分隔值 (CSV) 源文件。所有非重复的 SHA-256 值都将被添加到文件列表。

将文件添加到文件列表，编辑文件列表中的 SHA-256 值或删除文件列表中的 SHA-256 值时，必须重新应用使用该列表的所有访问控制策略，更改才会生效。

由于将文件添加到文件列表会影响访问控制，因此，必须具有以下其中一种访问权限，才能管理文件列表的所有方面：

- 管理员访问权限
- 网络管理员或访问管理员访问权限（编辑文件列表）、安全审批人访问权限（重新应用访问控制策略）和安全分析师或安全分析师 (RO) 访问权限（使用 SHA-256 值从事件视图添加文件）的组合
- 具有修改访问控制策略权限和对象管理器（编辑文件列表）、应用访问控制策略（重新应用访问控制策略）和修改文件事件（使用 SHA-256 值从事件视图添加文件）权限的自定义角色；请参阅第 12-3 页上的使用自定义用户角色管理部署

有关使用文件列表的详细信息，请参阅以下主题：

将多个 SHA-256 值上传到文件列表

许可证：恶意软件

受支持的设备：除 2 系列或 X -系列外的所有型号

受支持的防御中心：除 DC500 外的所有型号

可通过上传包含 SHA-256 值和描述的列表的逗号分隔值 (CSV) 源文件将多个 SHA-256 值添加到文件列表。防御中心会验证内容并使用有效 SHA-256 值填充文件列表。

源文件必须为具有 .csv 文件扩展名的简单文本文件。所有标题必须以井号 (#) 开头；标题将被视为注释，不会上传。每个条目应包含一个 SHA-256 值，后接一段描述 （最多包含 256 个字母数字或特殊字符），并以 LF 或 CR+LF 换行字符结尾。系统将会忽略条目中的任何其他信息。

请注意：

- 从文件列表删除源文件也会从该文件列表删除所有相关的 SHA-256 哈希值。
- 如果成功上传源文件导致文件列表包含超过 10000 个不同的 SHA-256 值，则不能将多个文件上传到该文件列表。
- 上传时，系统会截去描述中超过 256 个字符的字符，仅保留前 256 个字符。如果描述包括逗号，必须使用转义字符 (\,)。如果未包含描述，将会改为使用源文件名。
- 如果文件列表包含 SHA-256 值，并且上传了包括该值的源文件，新上传的值不会修改现有 SHA-256 值。查看与 SHA-256 值相关的捕获的文件、文件事件或恶意软件事件时，所有威胁名称或描述都来源于单个 SHA-256 值。
- 系统不会在源文件中上传无效的 SHA-256 值。
- 如果多个上传的源文件包括相同 SHA-256 值的条目，系统将使用最新的值。
- 如果源文件包括相同 SHA-256 值的多个条目，系统将使用最后一个。
- 不能在对象管理器中直接编辑源文件。要进行更改，必须首先直接修改源文件，删除系统中的副本，然后上传修改后的源文件。有关详情，请参见第 3-33 页上的从文件列表下载源文件。

要将源文件上传到文件列表，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　点击 **File List**。

系统将显示 File List 部分。

步骤 3　点击要从源文件向其添加值的文件列表旁边的编辑图标 ( )。

系统将显示 File List 弹出窗口。

步骤 4　从 **Add by** 字段选择 `List of SHAs`。

弹出窗口将会更新以包括新字段。

步骤 5　或者，在 **Description** 字段中输入源文件的描述。

如果不输入描述，系统将会使用文件名。

步骤 6　点击 **Browse** 浏览到源文件，然后点击 **Upload and Add List** 添加列表。

源文件即被添加到文件列表。 SHA-256 列显示文件包含多少个 SHA-256 值。

步骤 7　点击 **Save**。

步骤 8　重新应用具有使用此文件列表的文件策略的所有访问控制策略。

应用策略后，系统不再对文件列表中的文件执行恶意软件云查找。

将单个文件上传到文件列表

许可证：恶意软件

受支持的设备：除 2 系列或 X -系列外的所有型号

受支持的防御中心：除 DC500 外的所有型号

如果希望将文件副本添加到文件列表，可以将文件上传到防御中心进行分析；系统会计算文件的 SHA-256 值并将文件添加到列表。系统不对用于 SHA-256 计算的文件大小强制实施任何限制。

要通过让防御中心计算文件的 SHA-256 值来添加文件，请执行以下操作：

访问：管理员/网络管理员

步骤 1　在对象管理器的 File List 页面上，点击要添加文件的白名单或自定义检测列表旁边的编辑图标 ( )。

系统将显示 File List 弹出窗口。

步骤 2　从 **Add by** 字段选择 **Calculate SHA**。

弹出窗口将会更新以包括新字段。

步骤 3　或者，在 **Description** 字段中输入文件的描述。

如果不输入描述，在上传时文件名将被用作描述。

步骤 4　点击 **Browse** 浏览到源文件，然后点击 **Calculate and Add SHA** 添加列表。

文件即被添加到文件列表。

步骤 5　点击 **Save**。

步骤 6　重新应用具有使用此文件列表的文件策略的所有访问控制策略。

应用策略后，系统不再对文件列表中的文件执行恶意软件云查找。

将 SHA-256 值添加到文件列表

许可证：恶意软件

受支持的设备：除 2 系列或 X -系列外的所有型号

受支持的防御中心：除 DC500 外的所有型号

可以提交文件的 SHA-256 值以将其添加到文件列表。不能添加重复的 SHA-256 值。

提示 在事件视图中右键单击某个文件或恶意软件事件，并在上下文菜单中选择 **Show Full Text**，以查看和复制该文件的完整 SHA-256 值。

要通过手动输入文件的 SHA-256 值来添加文件，请执行以下操作：

访问：管理员/网络管理员

步骤 1 在对象管理器的 File List 页面上，点击要添加文件的白名单或自定义检测列表旁边的编辑图标 ( )。

系统将显示 File List 弹出窗口。

步骤 2 从 **Add by** 字段选择 `Enter SHA Value`。

弹出窗口将会更新以包括新字段。

步骤 3 在 **Description** 字段中输入源文件的描述。

步骤 4 键入或粘贴文件的完整 **SHA-256** 值。系统不支持匹配部分值。

步骤 5 点击 **Add** 添加文件。

文件即被添加到文件列表。

步骤 6 点击 **Save**。

步骤 7 重新应用具有使用此文件列表的文件策略的所有访问控制策略。

应用策略后，系统不再对文件列表中的文件执行恶意软件云查找。

修改文件列表中的文件

许可证：恶意软件

受支持的设备：除 2 系列或 X -系列外的所有型号

受支持的防御中心：除 DC500 外的所有型号

可以编辑或删除文件列表中的各个 SHA-256 值。请注意，不能在对象管理器中直接编辑源文件。要进行更改，必须首先直接修改源文件，删除系统中的副本，然后上传修改后的源文件。有关详情，请参见第 3-33 页上的从文件列表下载源文件。要编辑文件列表中的文件，请执行以下操作：

访问：管理员/网络管理员

步骤 1 在对象管理器的 File List 页面上，点击要修改文件的白名单或自定义检测列表旁边的修改图标 ( )。

系统将显示 File List 弹出窗口。

步骤 2　点击要编辑的 SHA-256 值旁边的编辑图标 ( )。

系统将显示 Edit SHA-256 弹出窗口。

提示　也可以从列表中删除文件。点击要移除的文件旁边的删除图标 ( )。

步骤 3　更新 **SHA-256** 值或 **Description**。

步骤 4　点击 **Save**。

系统将显示 File List 弹出窗口。系统更新列表中的文件条目。

步骤 5　点击 **Save**。

步骤 6　重新应用具有使用此文件列表的文件策略的所有访问控制策略。

应用策略后，系统不再对文件列表中的文件执行恶意软件云查找。

从文件列表下载源文件

许可证：恶意软件

受支持的设备：除 2 系列或 X -系列外的所有型号

受支持的防御中心：除 DC500 外的所有型号

可以查看、下载或删除文件列表中的现有源文件条目。请注意，不能编辑已上传的源文件，必须首先删除文件列表中的源文件，再上传更新后的文件。有关上传源文件的详细信息，请参阅第 3-30 页上的将多个 SHA-256 值上传到文件列表。

与源文件相关的条目数是指不同的 SHA-256 值的数量。如果从文件列表删除某个源文件，文件列表包含的 SHA-256 条目总数将会减少至该源文件中有效条目的数量。

要下载源文件，请执行以下操作：

访问：管理员/网络管理员

步骤 1　在对象管理器的 File List 页面上，点击要下载源文件的白名单或自定义检测列表旁边的修改图标 ( )。

系统将显示 File List 弹出窗口。

步骤 2　点击要下载的源文件旁边的视图图标 ( )。

系统将显示 View SHA-256's in list 弹出窗口。

步骤 3　点击 **Download SHA List** 并按照提示保存源文件。

步骤 4　点击**关闭**。

系统将显示 File List 弹出窗口。

使用安全区域

许可证：任何环境

*安全区域*由一个或多个内联接口、被动接口、交换接口、路由接口或 ASA 接口组成，可在各种策略和配置中用于管理和分类流量。一个区域中的接口可以跨多个设备；也可以在一个设备上配置多个区域。这使得您能够将网络划分为可以应用各种策略的网段。必须将至少一个接口分配到安全区域，以根据该安全区域匹配流量，每个接口只能属于一个区域。

除了使用安全区域来对接口分组，还可以在系统网络界面中的不同位置（包括访问控制策略、网络发现规则和事件搜索）使用区域。例如，可编写仅适用于特定源或目标区域的访问控制规则，或者限制网络发现仅针对发往或来自特定区域的流量。

更新安全区域对象时，系统会保存对象的新版本。因此，如果同一安全区域中的受管设备具有不同版本的安全区域对象，您可能会记录似乎是重复的连接。如果发现重复连接报告，可以将所有受管设备更新为使用该对象的同一版本。在对象管理器中，可以编辑安全区域，移除所有受管设备，保存对象，重新添加受管设备，以及再次保存对象。然后，重新应用所有受影响的设备策略。有关应用设备策略的详细信息，请参阅第 4-22 页上的对设备应用更改。

可通过以下其中一种方式创建安全区域：

- 系统在设备注册时基于您在设备初始配置时为其选择的检测模式创建安全区域。例如，系统在被动部署中创建被动区域，在内联部署中则创建外部区域和内部区域。
- 可在配置受管设备上的接口时快速创建安全区域。
- 可以使用对象管理器 (**Objects > Object Management**) 创建安全区域。

对象管理器的 Security Zones 页面列出在受管设备上配置的区域。该页面还显示每个区域中的接口类型，您可以展开每个区域查看哪个设备上的哪个接口属于该区域。

注　安全区域中的所有接口都必须相同，也就是说，所有接口均为内联接口、被动接口、交换接口、路由接口或 ASA 接口。此外，创建安全区域后，不能更改其包含的接口类型。

如果修改 ASA 安全情景，在单情景模式与多情景模式之间切换，系统将从您的安全区域配置中移除所有接口。

不能删除正在使用的安全区域。从区域添加或移除接口后，必须对接口所在的设备重新应用设备配置。还必须重新应用使用该区域的访问控制策略和网络发现策略。

要添加安全区域，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　选择 **Security Zones**。

步骤 3　点击 **Add Security Zone**。

系统将显示 Security Zones 弹出窗口。

步骤 4　在 **Name** 字段中为区域键入名称。可以使用除大括号 ({})、管道 (|)、分号 (;) 或井号 (#) 之外的任何可打印的标准 ASCII 字符。

步骤 5　从 **Type** 选择区域的接口类型。

创建安全区域后，不能更改其类型。

步骤 6　从 **Device > Interfaces** 下拉列表中，选择包含要添加到区域的接口的设备。

步骤 7　选择一个或多个接口。

使用 Shift 和 Ctrl 键可选择多个对象。如果尚未配置受管设备上的接口，可以创建空区域，稍后再向其添加接口；跳至第 10 步。

步骤 8　点击 **Add**。

所选的接口即被添加到区域，并按设备分组。

步骤 9　重复第 6 至第 8 步，将其他设备上的接口添加到区域。

步骤 10　点击 **Save**。

安全区域添加成功。

使用密码套件列表

许可证：任何环境

受支持的设备：3 系列

密码套件列表是由多个密码套件组成的对象。每个预定义的密码套件值代表用于协商 SSL 或 TLS 加密会话的一个密码套件。可以在 SSL 规则中使用密码套件和密码套件列表根据协商 SSL 会话的客户端和服务器是否使用该加密套件来控制加密流量。如果将密码套件列表添加到 SSL 规则，使用该列表中的任何密码套件协商的 SSL 会话都匹配该规则。

注　虽然密码套件和密码套件列表在网络界面中可使用的位置相同，但不能添加、修改或删除密码套件。

不能删除正在使用的密码套件列表。此外，编辑用于 SSL 策略的密码套件列表后，必须重新应用相关的访问控制策略，更改才会生效。

要创建密码套件列表，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　选择 **Cipher Suite List**。

步骤 3　点击 **Add Cipher Suites**。

系统将显示 Cipher Suite List 弹出窗口。

步骤 4　在 **Name** 字段中为密码套件列表键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　选择一个或多个密码套件，然后点击 **Add**。

- 使用 Shift 和 Ctrl 可选择多个密码套件，或者右键单击并选择 **Select All**。
- 使用过滤器字段 ( ) 搜索要包括的现有密码套件，在您键入时，该字段会更新以显示匹配的项目。点击搜索字段上方的重新加载图标 ( )，或点击搜索字段中的清除图标 ( ) 可清除搜索字符串。

步骤 6　点击 **Save**。

密码套件列表创建成功。

使用可分辨名称对象

许可证：任何环境

受支持的设备：3 系列

每个可分辨名称对象代表所列出的公共密钥的使用者或颁发者的可分辨名称。可在 SSL 规则中使用可分辨名称对象和对象组（请参阅第 3-2 页上的将对象分组）根据协商 SSL 会话的客户端和服务器是否使用将该可分辨名称作为使用者或颁发者的服务器证书来控制加密流量。

可分辨名称对象包含公用名属性 (**CN**)。如果添加不带“CN=”的公用名称，系统会在名称前面加上“CN=”，再保存对象。

还可以添加带有下表中列出的每个属性（用逗号隔开）的一个可分辨名称。

表 3-7　　可分辨名称属性

属性	说明	允许的值
C	国家/地区代码	两个字母字符
CN	通用名称	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格
O	组织	
OU	组织单位	

可以定义一个或多个星号 (*) 作为属性中的通配符。在公用名属性中，可以为每个域名标签定义一个或多个星号。通配符仅在该标签中匹配，不过，可以使用通配符定义多个标签。请参阅下表中的示例。

表 3-8　　公用名属性通配符示例

属性	匹配	不匹配
CN=”*ample.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”exam*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*xamp*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*.example.com”	mail.example.com	example.com example.text.com ampleexam.com

表 3-8　公用名属性通配符示例

属性	匹配	不匹配
CN=”*.com”	example.com ampleexam.com	mail.example.com example.text.com
CN=”*.*.com”	mail.example.com example.text.com	example.com ampleexam.com

不能删除正在使用的可分辨名称对象。此外，编辑用于 SSL 策略的可分辨名称对象后，必须重新应用相关的访问控制策略，更改才会生效。

要添加可分辨名称对象，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **Distinguished Name** 下，选择 **Individual Objects**。

步骤 3　点击 **Add Distinguished Name**。

系统将显示 Distinguished Name 弹出窗口。

步骤 4　在 **Name** 字段中为可分辨名称对象键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　在 **DN** 字段中，键入可分辨名称或公用名称的值。您有以下选项：

- 如果添加可分辨名称，则可包括第 3-36 页上的表 3-7 中列出的每个属性（以逗号隔开）。
- 如果添加公用名，则可包括多个标签和通配符。

步骤 6　点击 **Save**。

可分辨名称对象添加成功。

使用 PKI 对象

许可证：任何环境

受支持的设备：3 系列

PKI 对象代表支持 SSL 检查部署所需的公共密钥证书和配对私有密钥。内部和可信 CA 对象包括证书颁发机构 (CA) 证书；内部 CA 对象还包括与证书配对的私有密钥。内部和外部证书对象包括服务器证书；内部证书对象还包括与证书配对的私有密钥。在 SSL 规则中使用这些对象可以解密以下各项：

- 传出流量（通过对带有内部 CA 对象的服务器证书进行重签）
- 传入流量（使用内部证书对象中的已知私有密钥）

还可以创建 SSL 规则并匹配使用以下证书加密的流量：

- 外部证书对象中的证书
- 由可信 CA 对象中的 CA 签名的证书或在 CA 的信任链中的证书

可以手动输入证书和密钥信息，上传包含这些信息的文件，在某些情况下，还可以生成新的 CA 证书和私有密钥。

在对象管理器中查看 PKI 对象列表时，系统会将证书的使用者可分辨名称显示为对象值。将指针悬停在该值上可查看证书使用者的完整可分辨名称。要查看其他证书的详细信息，请编辑 PKI 对象。

注 防御中心和受管设备在保存存储在内部 CA 对象和内部证书对象中的所有私有密钥之前，会使用随机生成的密钥对它们进行加密。如果上传受密码保护的私有密钥，设备会使用用户提供的密码对该密钥进行解密，然后用随机生成的密钥对其重新加密，再进行保存。

有关详细信息，请参阅以下各节：

- 第 3-38 页上的使用内部证书颁发机构对象
- 第 3-42 页上的使用可信证书颁发机构对象
- 第 3-44 页上的使用外部证书对象
- 第 3-45 页上的使用内部证书对象

使用内部证书颁发机构对象

许可证：任何环境

受支持的设备：3 系列

配置的每个内部证书颁发机构 (CA) 对象代表组织控制的 CA 的 CA 公共密钥证书。此类对象由对象名称、CA 证书和配对私有密钥组成。可以在 SSL 规则中使用内部 CA 对象和对象组（请参阅第 3-2 页上的将对象分组）通过使用内部 CA 对服务器证书进行重签来解密传出加密流量。

注 如果在 **Decrypt - Resign** SSL 规则中引用内部 CA 对象，且该规则与加密会话相匹配，在协商 SSL 握手时，用户的浏览器可能会警告证书不可信。要避免此问题，请将内部 CA 对象证书添加到可信根证书的客户端或域列表。

可以通过以下方式创建内部 CA 对象：

- 导入现有基于 RSA 或基于椭圆曲线的 CA 证书和私有密钥
- 生成新的基于 RSA 的自签 CA 证书和私有密钥
- 生成未签名的基于 RSA 的 CA 证书和私有密钥。使用内部 CA 对象之前，必须向另一个 CA 提交证书签名请求 (CSR) 以对证书进行签名。

创建包含签名证书的内部 CA 对象后，可以下载 CA 证书和私有密钥。系统使用用户提供的密码对下载的证书和私有密钥进行加密。

无论是系统生成还是用户创建的内部 CA 对象名称，您都只能修改其名称，但不能修改其他对象属性。

不能删除正在使用的内部 CA 对象。此外，在编辑用于 SSL 策略的内部 CA 对象后，相关联的访问控制策略已过时。必须重新应用访问控制策略，才能使更改生效。

有关详细信息，请参阅以下各节：

- 第 3-39 页上的导入 CA 证书和私有密钥
- 第 3-39 页上的生成新的 CA 证书和私有密钥
- 第 3-40 页上的获取和上传新的签名证书
- 第 3-41 页上的下载 CA 证书和私有密钥

导入 CA 证书和私有密钥

许可证：任何环境

受支持的设备：3 系列

可以通过导入 X.509 v3 RSA 证书和私有密钥来配置内部 CA 对象。可以上传采用下列其中一种受支持格式编码的文件：

- 可区别编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果私有密钥文件受密码保护，您可以提供解密密码。如果证书和密钥采用 PEM 格式编码，还可以复制并粘贴信息。

只能上传包括适当的证书或密钥信息并且相互配对的文件。系统在保存对象之前会验证文件对。

注　如果配置具有 **Decrypt - Resign** 操作的规则，除了任何配置的规则条件之外，该规则还根据引用的内部 CA 证书的加密算法类型匹配流量。例如，必须上传一个基于椭圆曲线的 CA 证书，以解密用基于椭圆曲线的算法进行加密的出站流量。有关详细信息，请参阅第 21-9 页上的解密操作：解密流量以进一步检查。

要导入内部 CA 证书和私有密钥，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **PKI** 下，选择 **Internal CAs**。

步骤 3　点击 **Import CA**。

系统将显示 Import Internal Certificate Authority 弹出窗口。

步骤 4　在 **Name** 字段中为内部 CA 对象键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6　在 **Key** 字段上方，点击 **Browse** 上传 DER、 PEM 编码的配对私有密钥文件。

步骤 7　如果上传的文件受密码保护，请选择 **Encrypted, and the password is:** 复选框并输入密码。

步骤 8　点击 **Save**。

内部 CA 对象添加成功。

生成新的 CA 证书和私有密钥

许可证：任何环境

受支持的设备：3 系列

可以通过提供识别信息生成基于 RSA 的自签 CA 证书和私有密钥来配置内部 CA 对象。下表介绍提供用来生成证书的识别信息。

表 3-9　　生成的内部 CA 属性

字段	允许的值	必填
Country Name (two-letter code)	两个字母字符	是
州或省	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*)、句点 (.) 或空格字符	no
Locality or City		
组织		
组织单位		
通用名称		

生成的 CA 证书有效期为十年。有效期起始日期为生成一周之前。

要生成自签 CA 证书，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **PKI** 下，选择 **Internal CAs**。

步骤 3　点击 **Generate CA**。

系统将显示 Generate Internal Certificate Authority 弹出窗口。

步骤 4　在 **Name** 字段中为内部 CA 对象键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　键入识别属性，如第 3-40 页上的表 3-9 中所述。

步骤 6　点击 **Generate self-signed CA**。

内部 CA 对象添加成功。

获取和上传新的签名证书

许可证：任何环境

受支持的设备：3 系列

可以通过从 CA 获取签名证书来配置内部 CA 对象。这包括两个步骤：

- 提供识别信息以配置内部 CA 对象。这会生成未签名证书和配对私有密钥，并创建向您指定的 CA 发出的证书签名请求 (CSR)。
- 在 CA 颁发签名证书后，请上传证书到内部 CA 对象，用以替换未签名证书。

仅当内部 CA 对象包含签名证书时，才能在 SSL 规则中引用该对象。

要创建未签名 CA 证书和 CSR，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **PKI** 下，选择 **Internal CAs**。

步骤 3　点击 **Generate CA**。

系统将显示 Generate Internal Certificate Authority 弹出窗口。

步骤 4　在 **Name** 字段中为内部 CA 对象键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　键入识别属性，如第 3-40 页上的表 3-9 中所述。

步骤 6　点击 **Generate CSR**。

系统将显示 Generate Internal Certificate Authority 弹出窗口。

步骤 7　复制 CSR 以将其提交到 CA。

步骤 8　点击 **OK**。

CA 对象创建成功。请注意，必须首先上传 CA 颁发的签名证书，然后才可以使用该 CA 对象。

要上传为响应 CSR 而颁发的签名证书，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **PKI** 下，选择 **Internal CAs**。

步骤 3　点击包含等待 CSR 的未签名证书的 CA 对象旁边的编辑图标 ( )。

系统将显示 Edit Internal Certificate Authority 弹出窗口。

步骤 4　点击 **Install Certificate**。

系统将显示 Install Internal Certificate Authority 弹出窗口。

步骤 5　在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6　如果上传的文件受密码保护，请选择 **Encrypted, and the password is:** 复选框并输入密码。

步骤 7　点击 **Save**。

CA 对象即包含签名证书并可在 SSL 规则中被引用。

下载 CA 证书和私有密钥

许可证：任何环境

受支持的设备：3 系列

可以通过下载包含内部 CA 对象中的证书和密钥信息的文件来备份或传输 CA 证书和配对私有密钥。

注意事项　系统始终将下载的密钥信息存储在安全的位置。

系统在保存密钥信息之前，会使用随机生成的密钥对存储在内部 CA 对象中的私有密钥进行加密。如果从内部 CA 下载证书和私有密钥，系统在创建包含证书和私有密钥信息的文件之前，会首先对这些信息进行解密。然后，您必须提供系统用于加密下载文件的密码。

注意事项 作为系统备份一部分下载的私有密钥将被解密，然后存储在未加密的备份文件中。有关详细信息，请参阅第 70-2 页上的创建备份文件。

要下载内部 CA 证书和私有密钥，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1 选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2 在 **PKI** 下，选择 **Internal CAs**。

步骤 3 点击要下载其证书和私有密钥的内部 CA 对象旁边的编辑图标 ( )。

系统将显示 Edit Internal Certificate Authority 弹出窗口。

步骤 4 单击**“下载”**。

系统将显示 Encrypt Download File 弹出窗口。

步骤 5 在 **Password** 和 **Confirm Password** 字段中键入加密密码。

步骤 6 点击 **OK**。

系统提示您保存文件。

使用可信证书颁发机构对象

许可证：任何环境

受支持的设备：3 系列

配置的每个可信证书颁发机构 (CA) 对象代表属于组织外部的可信 CA 的 CA 公共密钥证书。此类对象由对象名称和 CA 公共密钥证书组成。可以在 SSL 策略中使用外部 CA 对象和对象组 （请参阅第 3-2 页上的将对象分组）控制使用由可信 CA 或信任链中的任何 CA 签名的证书加密的流量。

创建可信 CA 对象后，可以修改名称和添加证书撤销列表 (CRL)，但不能更改其他对象属性。可添加到对象的 CRL 数量没有限制。要修改已上传到对象的 CRL，必须删除并重新创建该对象。

不能删除正在使用的可信 CA 对象。此外，在编辑用于 SSL 策略的可信 CA 对象后，相关联的访问控制策略已过时。必须重新应用访问控制策略，才能使更改生效。

有关详细信息，请参阅以下各节：

- 第 3-42 页上的添加可信 CA 对象
- 第 3-43 页上的将证书撤销列表添加到可信 CA 对象

添加可信 CA 对象

许可证：任何环境

受支持的设备：3 系列

可通过上传 X.509 v3 CA 证书来配置外部 CA 对象。可以上传采用下列其中一种受支持格式编码的文件：

- 可区别编码规则 (DER)

- 隐私增强电子邮件 (PEM)

如果文件受密码保护，必须提供解密密码。如果证书采用 PEM 格式编码，还可以复制并粘贴信息。

仅当文件包含适当的证书信息时，才可以上传 CA 证书；系统在保存对象之前会对证书进行验证。

要导入可信 CA 证书，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **PKI** 下，选择 **Trusted CAs**。

步骤 3　点击 **Add Trusted CAs**。

系统将显示 Import Trusted Certificate Authority 弹出窗口。

步骤 4　在 **Name** 字段中为可信 CA 对象键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6　如果文件受密码保护，请选择 **Encrypted, and the password is:** 复选框并输入密码。

步骤 7　点击 **OK**。

可信 CA 对象添加成功。

将证书撤销列表添加到可信 CA 对象

许可证：任何环境

受支持的设备：3 系列

可以将 CRL 上传到可信 CA 对象。如果在 SSL 策略中引用上传的可信 CA 对象，可以根据颁发会话加密证书的 CA 随后是否会撤销证书来控制加密流量。可以上传采用下列其中一种受支持格式编码的文件：

- 可区别编码规则 (DER)
- 隐私增强电子邮件 (PEM)

添加 CRL 后，可以查看已撤销证书的列表。要修改已上传到对象的 CRL，必须删除并重新创建该对象。

只能上传包含适当 CRL 的文件。可添加到可信 CA 对象的 CRL 数量没有限制。但是，每次上传 CRL 之后，必须先保存对象再添加另一个 CRL。

要上传 CRL，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **PKI** 下，选择 **Trusted CAs**。

步骤 3　点击可信 CA 对象旁边的编辑图标 ( )。

系统将显示 Edit Trusted Certificate Authority 弹出窗口。

步骤 4　点击 **Add CRL** 上传 DER 或 PEM 编码的 CRL 文件。

步骤 5　点击 **OK**。

已保存您的更改。

使用外部证书对象

许可证：任何环境

受支持的设备：3 系列

配置的每个外部证书对象代表一个不属于组织的服务器公共密钥证书。此类对象由对象名称和证书组成。可以在 SSL 规则中使用外部证书对象和对象组（请参阅第 3-2 页上的将对象分组）来控制使用服务器证书加密的流量。例如，您可以上传您信任的自签服务器证书，但不能使用可信 CA 证书进行验证。

可通过上传 X.509 v3 服务器证书来配置外部证书对象。可以上传采用下列其中一种受支持格式的文件：

- 可区别编码规则 (DER)
- 隐私增强电子邮件 (PEM)

仅当文件包含适当的服务器证书信息时，才可以上传文件；系统在保存对象之前会对文件进行验证。如果证书采用 PEM 格式编码，还可以复制并粘贴信息。

创建外部证书对象后，可以修改其名称，但不能更改其他对象属性。

不能删除正在使用的外部证书对象。此外，在编辑用于 SSL 策略的外部证书对象后，相关联的访问控制策略已过时。必须重新应用访问控制策略，才能使更改生效。

要添加外部证书对象，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **PKI** 下，选择 **External Certs**。

步骤 3　点击 **Add External Cert**。

系统将显示 Add Known External Certificate 弹出窗口。

步骤 4　在 **Name** 字段中为外部证书对象键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 服务器证书文件。

步骤 6　点击 **Save**。

内部 CA 对象添加成功。

使用内部证书对象

许可证：任何环境

受支持的设备：3 系列

配置的每个内部证书对象代表一个属于组织的服务器公共密钥证书。此类对象由对象名称、公共密钥证书和配对私有密钥组成。可以在 SSL 规则中使用内部证书对象和对象组（请参阅第 3-2 页上的将对象分组），利用已知私有密钥来解密传入到组织其中一个服务器的流量。

可以通过上传基于 X.509 v3 RSA 或基于椭圆曲线的服务器证书和配对的私有密钥来配置内部证书对象。可以上传采用下列其中一种受支持格式的文件：

- 可区别编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果文件受密码保护，必须提供解密密码。如果证书和密钥采用 PEM 格式编码，还可以复制并粘贴信息。

只能上传包括适当的证书或密钥信息并且相互配对的文件。系统在保存对象之前会验证文件对。

创建内部证书对象后，可以修改其名称，但不能更改其他对象属性。

不能删除正在使用的内部证书对象。此外，在编辑用于 SSL 策略的内部证书对象后，相关联的访问控制策略已过时。必须重新应用访问控制策略，才能使更改生效。

要添加内部证书对象，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **PKI** 下，选择 **Internal Certs**。

步骤 3　点击 **Add Internal Cert**。

系统将显示 Add Known Internal Certificate 弹出窗口。

步骤 4　为内部证书对象键入**名称**。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 服务器证书文件。

步骤 6　在 **Key** 字段上方，点击 **Browse** 上传 DER、 PEM 编码的配对私有密钥文件。

步骤 7　如果上传的私有密钥文件受密码保护，请选择 **Encrypted, and the password is:** 复选框并输入密码。

步骤 8　点击 **Save**。

内部证书对象添加成功。

使用地理定位对象

许可证：FireSIGHT

受支持的设备：3 系列、虚拟、 ASA FirePOWER

受支持的防御中心：所有 （DC500 除外）

配置的每个地理定位对象代表系统识别为受监控网络上流量的源或目标的一个或多个国家/地区或大洲。可在系统网络界面中的不同位置使用地理定位对象，包括访问控制策略、 SSL 策略和事件搜索。例如，可编写阻止流向或来自某些国家/地区的流量的访问控制规则。有关按地理位置过滤流量的信息，请参阅第 15-3 页上的按网络或地理位置控制流量。有关按地理位置过滤已加密流量的信息，请参阅第 22-3 页上的按网络或地理位置控制加密流量。

要确保使用最新信息来过滤网络流量，思科强烈建议您定期更新地理定位数据库 (GeoDB)。有关下载和安装 GeoDB 更新的信息，请参阅第 66-24 页上的更新地理定位数据库。

不能删除正在使用的地理定位对象。此外，编辑用于访问控制策略或 SSL 策略的地理定位对象后，必须重新应用该访问控制策略，才能使更改生效。

要添加地理定位对象，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Objects > Object Management**。

系统将显示 Object Management 页面。

步骤 2　选择 **Geolocation**。

系统将显示 Geolocation Objects 页面。

步骤 3　点击 **Add Geolocation**。

系统将显示 Geolocation Object 弹出窗口。

步骤 4　在 **Name** 字段中为地理定位对象键入名称。可以使用除管道 (|) 或大括号 ({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　选择要包括到地理定位对象中的国家/地区和大洲的相应复选框。

选择大洲会选择该大洲的所有国家/地区，以及 GeoDB 更新将来可能添加到该大洲下的所有国家/地区。取消选择大洲下的所有国家/地区会取消选择该大洲。可以选择国家/地区和大洲的任意组合。

步骤 6　点击 **Save**。

地理定位对象添加成功。

管理设备

防御中心是 FireSIGHT 系统中的关键组件。可以使用防御中心管理 FireSIGHT 系统组成的完整范围的设备，以及汇聚、分析和应对这些设备在网络中检测到的威胁。

通过使用防御中心管理设备，可以执行以下操作：

- 从单个位置为所有设备配置策略，从而更轻松地更改配置
- 在设备上安装各种类型的软件更新
- 向受管设备推送运行状况策略并从防御中心监控其运行状态

防御中心汇总并关联入侵事件、网络发现信息和设备性能数据，从而能够监控设备报告的相互关联的信息，以及评估网络上出现的整体活动。

有关详细信息，请参阅以下各节：

- 第 4-1 页上的管理概念介绍使用防御中心管理设备所涉及的一些功能和限制。
- 第 4-3 页上的了解管理接口介绍如何能够使用流量信道和多个管理接口改善性能或隔离不同网络上设备之间的流量。
- 第 4-6 页上的在 NAT 环境中工作介绍在网络地址转换环境中设置设备管理的原理。
- 第 4-7 页上的配置高可用性介绍如何将两个防御中心设置为高可用性对以帮助确保操作的连续性。
- 第 4-16 页上的处理设备介绍如何建立和禁用设备与防御中心之间的连接。它还说明如何添加、删除和更改受管设备的状态。
- 第 4-23 页上的管理设备组介绍如何创建设备组以及如何从组中添加和移除设备。
- 第 4-25 页上的集群设备介绍如何建立和管理两个受管设备之间的高可用性。
- 第 4-42 页上的编辑设备配置介绍可以编辑的设备属性并说明如何对其进行编辑。
- 第 4-37 页上的管理堆叠设备介绍如何创建受管设备堆栈以及如何从堆栈中移除设备。
- 第 4-52 页上的配置感应接口说明如何配置受管设备上的接口。

管理概念

可以使用防御中心管理设备行为的几乎每个方面。只需一个防御中心即可管理设备，不过也可以使用另一个防御中心作为高可用性对的一部分。后面各节说明在规划 FireSIGHT 系统部署时需要了解的一些概念：

- 第 4-2 页上的防御中心可以管理哪些内容？
- 第 4-2 页上的除策略和事件以外的其他功能
- 第 4-3 页上的使用冗余防御中心

防御中心可以管理哪些内容？

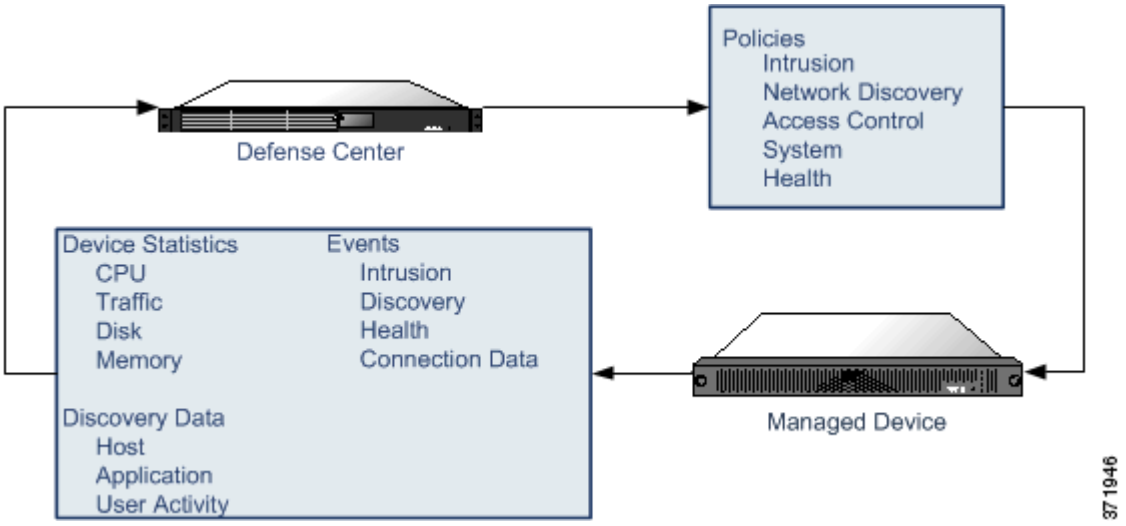
可以使用防御中心作为 FireSIGHT 系统部署中的中央管理点来管理以下设备：

- FirePOWER 受管设备
- 具备 FirePOWER 服务的 Cisco ASA 防火墙设备
- 基于软件的设备，例如虚拟设备和用于 Blue Coat X-系列的思科 NGIPS

注　思科建议使用 DC500 型号防御中心管理不超过三台设备（包括基于软件的设备）。有关 DC500 数据库限制的详细信息，请参阅数据库事件限制表。

管理设备时，信息通过 SSL 加密的安全 TCP 隧道在防御中心和该设备之间传输。

下图列出了在防御中心及其受管设备之间传输的内容。请注意，设备间发送的事件和策略的类型基于设备类型。



除策略和事件以外的其他功能

许可证：任何环境

除将策略应用到设备和从其接收事件以外，还可以在防御中心上执行其他设备相关任务。

备份设备

您**无法**创建或恢复虚拟受管设备、用于 Blue Coat X-系列的思科 NGIPS或者具备 FirePOWER 服务的 Cisco ASA 防火墙的备份文件。

当您从设备本身执行物理受管设备的备份时，**只**会备份设备配置。要备份配置数据和（可选的）统一文件，请使用管理防御中心执行设备备份。

要备份事件数据，请对管理防御中心执行备份。有关详细信息，请参阅第 70-2 页上的创建备份文件。

更新设备

思科会定期发布 FireSIGHT 系统更新，包括：

- 入侵规则更新，其中可能包含新的和已更新的入侵规则
- 漏洞数据库更新
- 地理定位更新
- 软件补丁和更新

可以使用防御中心在其管理的设备上安装更新。

使用冗余防御中心

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

可以将两个防御中心设置为高可用性对。这样可以在其中一个防御中心发生故障时确保冗余功能发挥作用。在两个防御中心之间进行共享策略和用户帐户等等。事件自动发送到两个防御中心。有关详情，请参见第 4-7 页上的配置高可用性。

了解管理接口

管理接口提供防御中心与其管理的设备之间的通信方式。在设备之间维持良好的流量控制是部署成功的关键。

在 3 系列 设备和虚拟防御中心上，您可以修改默认配置，在防御中心和/或设备上启用管理接口，从而将设备之间的流量归入两个独立的流量信道。*管理流量信道*传送所有内部流量（例如特定于设备和系统管理的设备内部流量），*事件流量信道*传送所有事件流量（例如网络事件）。当您要将流量拆分为两个信道时，请在两个设备之间创建两个连接点，以提高吞吐量，从而提高性能。您还可以启用*多个管理接口*，每个管理接口拥有一个唯一 IP 地址（IPv4 或 IPv6）和主机名，从而分离和管理流量信道，同时仍可提供更大的吞吐量。

利用多个管理接口，您还可以只使用一个防御中心隔离和管理来自不同网络的流量。使用管理接口向目标网络添加静态路由，并向单独的管理接口注册设备，以确保来自一个网络的流量与另一个网络上的流量隔离。可以在同一接口上发送两个流量信道，或者，如果有足够的附加管理接口，则既可以隔离网络流量，又可以将每个管理接口配置为仅传送一个流量信道。

管理接口通常位于设备背面。有关详细信息，请参阅《*FireSIGHT 系统安装指南*》中的“识别管理接口”一节。要进一步了解管理接口，请参阅以下各节，获取详细信息：

- 第 4-4 页上的使用单一管理接口
- 第 4-4 页上的使用多个管理接口
- 第 4-5 页上的使用流量信道
- 第 4-6 页上的使用网络路由

使用单一管理接口

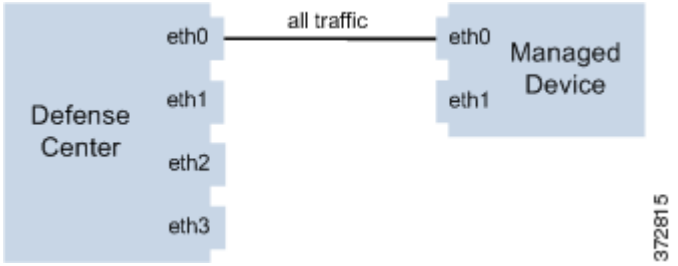
许可证：任何环境

受支持的设备：任何环境

受支持的防御中心：任何环境

当您向防御中心注册您的设备时，会建立一个传送防御中心上的管理接口和设备上的管理接口之间所有流量的通信信道。

下图显示默认的单一通信信道。一个接口传送包含管理和事件流量的通信信道。



使用多个管理接口

许可证：任何环境

受支持的设备：3 系列

受支持的防御中心：3 系列、虚拟

您可以启用并配置多个管理接口，每个接口使用唯一的 IP 地址（IPv4 或 IPv6）和（可选的）主机名，通过将每个流量信道发送至不同的管理接口提高流量吞吐量。配置较小的接口传送较少的管理流量负载，配置较大的接口传送较大的事件流量负载。您可以注册设备以分离管理接口，并为同一接口配置两个通信信道，或者使用一个专用管理接口传送由防御中心管理的所有设备的事件流量信道。

您还可以从您的防御中心上的特定管理接口创建通向不同网络上的设备的路由。当您向非默认管理接口注册不同网络上的设备时，该设备上的流量会与向默认 (`eth0`) 管理接口注册的设备上的流量隔离。有关详情，请参见第 4-6 页上的使用网络路由。

非默认管理接口的许多功能与默认管理接口相同（例如使用防御中心之间的高可用性），但以下情况除外：

- 只能在默认 (`eth0`) 管理接口上配置 DHCP。其他（`eth1` 等）接口需要唯一的静态 IP 地址和主机名。
- 当您使用一个非默认的管理接口来连接防御中心和受管设备，且这些设备被一台 NAT 设备隔开时，您必须配置两条流量信道使用同一个管理接口。
- 只能在默认管理接口上使用无人值守管理。
- 在 70xx 子系列上，您可以将流量分至两个信道并对信道进行配置，以将流量发送至防御中心上的一个或多个管理接口。但是，由于 70xx 子系列只带一个管理接口，该设备仅通过一个管理接口接收从防御中心发送来的流量。

使用流量信道

许可证：任何环境

受支持的设备：3 系列

受支持的防御中心：3 系列、虚拟

在一个管理接口上使用两个流量信道时，会在防御中心和受管设备之间创建两个连接。一个信道传送管理流量，一个信道传送事件流量，这两种流量在同一接口上单独进行传送。

以下示例显示同一接口上有两个独立流量信道的通信信道。

使用多个管理接口时，可以在两个管理接口上划分流量信道，进而可以通过添加两个接口的容量来增加流量，从而进一步提高性能。一个接口传送管理流量信道，另一个接口传送事件流量信道。如果任一接口发生故障，则所有流量重新路由到活动接口，并且连接得以维持。

下图显示了两个管理接口上的管理流量信道和事件流量信道。

可以使用专用管理接口仅传送来自多台设备的事件流量。在此配置中，每台设备分别注册到不同管理接口上以传送管理流量信道，并且防御中心上的一个管理接口传送来自所有设备的所有事件流量信道。如果任一接口发生故障，流量重新路由到活动接口，并且连接得以维持。请注意，由于所有设备的事件流量都在同一接口上传送，因此未在网络之间隔离流量。

下图显示了使用不同管理通道流量接口的两台设备共用相同的事件流量信道专用接口。

在一个管理接口上使用两个流量信道时，会在防御中心和受管设备之间创建两个连接。一个信道传送管理流量，一个信道传送事件流量，这两种流量在同一接口上单独进行传送。使用多个管理接口时，可以在两个管理接口上划分流量信道，进而可以通过添加两个接口的容量来增加流量，从而进一步提高性能。一个接口传送管理流量信道，另一个接口传送事件流量信道。如果任一接口发生故障，则所有流量重新路由到活动接口，并且连接得以维持。

还可以使用专用管理接口仅传送来自多台设备的事件流量。在此配置中，每台设备分别注册到不同管理接口上以传送管理流量信道，并且防御中心上的一个管理接口传送来自所有设备的所有事件流量信道。如果任一接口发生故障，流量重新路由到活动接口，并且连接得以维持。请注意，由于所有设备的事件流量都在同一接口上传送，因此未在网络之间隔离流量。

使用网络路由

许可证：任何环境

受支持的设备：3 系列

受支持的防御中心：3 系列、虚拟

您可以从防御中心上的特定管理接口创建通向不同网络的路由。当您从该网络向防御中心上指定的管理接口注册设备时，您将在防御中心和其他网络上的设备之间提供一个隔离连接。将两个流量信道配置为使用相同的管理接口，以确保来自该设备的流量与其他网络上的设备流量保持隔离。由于路由接口与防御中心上的所有其他接口隔离，因此，如果路由管理接口发生故障，连接会丢失。

提示 思科建议您在使用除默认 (eth0) 管理接口之外的任何管理接口注册防御中心及其设备时使用静态 IP 地址。只有默认的管理接口上才支持 DHCP。

安装防御中心后，使用网络界面配置多个管理接口。有关详细信息，请参阅《*FireSIGHT 系统用户指南*》中的“配置设备设置”。

下图显示通过为所有流量使用独立管理接口隔离网络流量的两台设备。您可以添加更多管理接口，为每台设备配置独立的管理和事件流量信道接口。

在 NAT 环境中工作

许可证：任何环境

网络地址转换 (NAT) 是一种通过路由器传输和接收网络流量的方法，其中涉及在流量通过路由器传递时重新分配源或目标 IP 地址。使用 NAT 的典型应用支持专用网络上的多个主机使用单个公共 IP 地址访问公共网络。

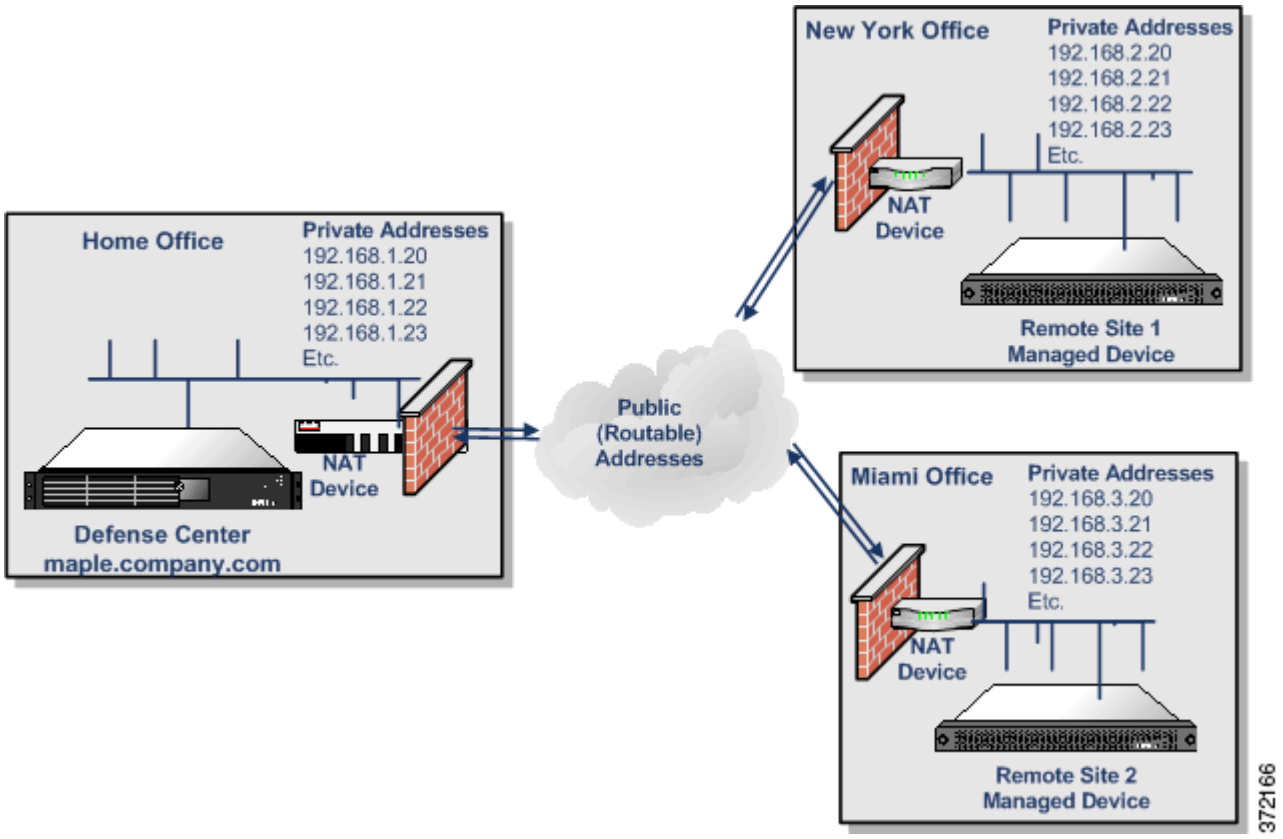
将设备添加到防御中心时，会在设备之间建立通信。建立通信所需的信息取决于环境是否使用 NAT：

- 在不使用 NAT 的环境中，需要注册密钥以及两台设备的 IP 地址或完全限定域名。
- 在使用 NAT 的环境中，需要注册密钥和唯一 NAT ID。

注　NAT ID **必须**在用于将设备注册到防御中心的所有 NAT ID 中唯一。

请注意，使用非默认管理接口连接防御中心和受管设备并且这些设备由 NAT 设备分隔时，必须配置两个流量信道使用同一管理接口。

下图显示在 NAT 环境中管理两台设备的防御中心。添加这两台设备时可以使用同一注册密钥，因为注册密钥不必唯一。但是，将设备添加到防御中心时，**必须**使用唯一 NAT ID。



配置高可用性

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

要确保操作的连续性，可通过高可用性功能指定冗余防御中心以管理设备。从受管设备到两个防御中心和某些配置元素的事件数据流在两个防御中心上均进行维护。如果一个防御中心发生故障，可以使用另一个防御中心继续不间断地监控网络。

注意事项 由于系统将某些功能限制为适用于主防御中心，因此如果该设备发生故障，则必须将辅助防御中心升级为主用设备。请参阅第 4-13 页上的监控和更改高可用性状态。

有关设置高可用性的详细信息，请参阅以下各节：

- 第 4-8 页上的使用高可用性列出实施高可用性时共享和未共享的配置。
- 第 4-11 页上的实施高可用性的准则概括要实施高可用性时必须遵循的准则。
- 第 4-12 页上的设置高可用性说明如何指定主和辅助防御中心。
- 第 4-13 页上的监控和更改高可用性状态说明如何检查链接的防御中心的状态，以及在主防御中心发生故障的情况下如何更改防御中心的角色。
- 第 4-14 页上的禁用高可用性和注销设备说明如何永久移除链接的防御中心之间的链路。
- 第 4-15 页上的暂停成对防御中心之间的通信说明如何暂停链接的防御中心之间的通信。
- 第 4-15 页上的重新启动成对防御中心之间的通信说明如何重启链接的防御中心之间的通信。

使用高可用性

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

DC1500、 DC2000、 DC3500 和 DC4000 支持高可用性配置；而 DC750 和虚拟防御中心不支持高可用性配置。思科**强烈**建议高可用性对中的两个防御中心为同一型号。**请勿**尝试在不同防御中心型号之间设置高可用性。

尽管高可用性模式中的防御中心被指定*主*和*辅助*，但是可以对任一防御中心进行策略或其他更改。但是，思科建议**仅**更改主防御中心上的配置，并将辅助防御中心保留为备份。

防御中心定期相互更新对其配置的更改，并且对一个防御中心进行的任何更改都应该在 10 分钟内应用在另一个防御中心上。（每个防御中心有一个 5 分钟的同步周期，但是，周期本身可能有长达 5 分钟的时间处于不同步的状态，因此更改会在两个 5 分钟的周期内出现。）在此 10 分钟窗口内，配置在防御中心上可能看似不同。

例如，如果在主防御中心上创建策略并将其应用到也受辅助防御中心管理的设备，则该设备可能先联系辅助防御中心，然后防御中心再相互联系。由于辅助防御中心无法识别设备所应用的策略，因此辅助防御中心会显示一个名为“unknown”的新策略，直到防御中心同步。

此外，如果在防御中心同步之间的同一窗口内对防御中心进行的策略或其他更改有冲突，则无论将防御中心指定为主设备还是辅助设备，上次进行的更改优先。

建立高可用性对之前，请注意以下先决条件：

- 确保两个防御中心均有具有“管理员”特权的名为 `admin` 的用户帐户。这些帐户必须使用同一密码。
- 请确保除 `admin` 帐户以外，两个防御中心不具有用户名相同的用户帐户。建立高可用性之前，请移除或重命名其中一个重复用户帐户。

请注意，配置为高可用性对的防御中心既无需在同一可信管理网络上，也不必在同一地理位置中。

要确保操作的连续性，高可用性对中的两个防御中心均必须能够访问互联网；请参阅第 E-1 页上的互联网访问要求。为实现特定功能，主防御中心将访问互联网，然后在同步过程中与辅助防御中心共享信息。因此，如果主防御中心发生故障，则应该将辅助防御中心升级为主用设备，如第 4-13 页上的监控和更改高可用性状态中所述。

有关在高可用对的成员之间共享或未共享哪些配置的详细信息，请参阅：

共享配置

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

高可用性对中的防御中心共享以下信息：

- 用户帐户属性、身份验证配置和自定义用户角色
- 用户帐户和用户感知的身份验证对象，以及可用于访问控制规则中的用户条件的用户和组
- 自定义控制面板
- 自定义工作流程和表
- 设备属性，如设备生成的事件存储所在的设备的主机名以及设备驻留在其中的组
- 访问控制、 SSL、网络分析、入侵、文件和网络发现策略
- 本地入侵规则
- 自定义入侵规则分类
- 网络发现策略
- 用户定义的应用协议检测器及其检测的应用
- 激活的自定义指纹
- 主机属性
- 网络发现用户反馈，包括备注和主机重要性；主机、应用和网络在网络映射中的删除；以及漏洞的禁用或修改
- 关联策略和规则、合规性白名单及流量量变曲线
- 更改记录快照和报告设置
- 入侵规则、地理定位数据库 (GeoDB) 和漏洞数据库 (VDB) 更新
- 可重用的对象，包括与以上任何配置关联的变量集

运行状况和系统策略

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

防御中心和受管设备的运行状况和系统策略在高可用性对中会进行共享。预留足够时间可确保有关运行状况策略、模块、黑名单的信息在新近激活的防御中心上同步。

注　虽然系统策略由防御中心在高可用性对中共享，但是不会自动应用这些策略。如果希望系统策略在两个防御中心上均相同，请在其同步后应用策略。

高可用性对中的防御中心共享以下系统和运行状况策略信息：

- 系统策略
- 系统策略配置（在什么位置应用什么策略）
- 运行状况策略
- 运行状况监控策略（在什么位置应用什么策略）
- 哪些设备通过系统监控列入黑名单
- 哪些设备将单个运行状况监控策略列入黑名单

关联响应

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

虽然防御中心共享关联策略、规则和响应，但是防御中心不共享关联规则及其响应之间的*关联*。这旨在违反关联策略时避免启动重复响应。

在补救可用于与关联策略关联之前，必须上传和安装任何自定义补救模块并在辅助防御中心上配置补救实例。如果主要防御中心发生故障，则不仅应该快速将关联策略与辅助防御中心上的相应响应和补救相关联，还必须使用辅助防御中心上的网络界面将其升级为主用设备以维护操作的连续性。有关详细信息，请参阅第 4-13 页上的监控和更改高可用性状态。有关关联响应的详细信息，请参阅第 51-42 页上的创建关联策略和第 54-1 页上的创建补救。

在故障后恢复主防御中心时，如果在规则或白名单与其在辅助防御中心上的响应和补救之间创建了关联，请确保移除关联，从而将仅由主防御中心生成响应和补救。

许可证

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

高可用性对中的防御中心**不**共享许可证。必须向对的每个成员添加等效许可证。有关详细信息，请参阅第 65-1 页上的了解许可。

URL 过滤和安全情报

许可证：URL 过滤或保护

受支持的设备：3 系列、虚拟、 X -系列、 ASA FirePOWER

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

URL 过滤和安全情报配置及信息在高可用性部署中的防御中心之间同步。但是，只有主防御中心会下载 URL 类别和信誉数据并更新安全情报源。

如果主防御中心发生故障，则不仅必须确保辅助防御中心可以访问 URL 过滤云和所有已配置的源站点，还必须使用辅助防御中心上的网络界面将其升级为主用设备。有关信息，请参阅第 4-13 页上的监控和更改高可用性状态。

云连接和恶意软件信息

许可证：任意或恶意软件

受支持的设备：任何设备， 2 系列或X -系列除外

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

虽然高可用性对中的防御中心共享文件策略和相关配置，但是它们既不共享综合安全智能云连接，也不共享恶意软件性质。为了确保业务连续性并确保在两个防御中心上对检测到文件的恶意软件的处置一致，主和辅助防御中心必须都有权访问云。有关详细信息，请参阅第 37-2 页上的了解恶意软件防护和文件控制。

用户代理

许可证：FireSIGHT

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

用户代理可以一次连接到最多五个防御中心。应该将代理连接到主防御中心。如果主防御中心发生故障，则必须确保任何代理都可与辅助防御中心进行通信。有关详情，请参见第 17-9 页上的使用用户代理报告 Active Directory 登录情况。

实施高可用性的准则

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

要利用高可用性，必须遵循以下部分中的准则。

主和辅助防御中心的要求

必须指定一个防御中心作为主防御中心，指定另一个作为辅助防御中心。如果设备从主用设备变为无效设备（反之亦然），它们会保留其原始主和辅助指定。

无论其指定为主还是辅助，在设置高可用性之前，均可使用策略、规则、受管设备等配置两个防御中心。

为避免混淆，请从处于其原始状态的辅助防御中心开始。即，尚未创建或修改任何策略，未创建任何新规则，先前也未使用其管理任何设备。要确保辅助防御中心处于其原始状态，请将其恢复为出厂默认设置。请注意，这还会从防御中心中删除事件和配置数据。有关详细信息，请参阅《*FireSIGHT 系统安装指南*》。

版本要求

两个防御中心均必须运行同一软件和规则更新版本。此外，此软件版本还必须与受管设备的软件版本相同或比其更高。

通信要求

默认情况下，成对的防御中心使用端口 8305/tcp 进行通信。可以按第 4-19 页上的更改管理端口中所述更改端口。

两个防御中心无需在同一网段上，但是每个防御中心必须能够相互以及与其共享的设备进行通信。即，主防御中心必须能够在辅助防御中心自己的管理接口上的 IP 地址处联系辅助防御中心，反之亦然。此外，每个防御中心必须能够联系其管理的设备，或者设备必须能够联系防御中心。

设置高可用性

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

要使用高可用性，必须将一个防御中心指定为主防御中心，将同一型号的另一个防御中心指定为辅助防御中心。有关编辑两台设备之间的远程管理通信的信息，请参阅第 4-18 页上的编辑远程管理。

注意事项　思科建议您**仅**更改主防御中心上的配置，并将辅助防御中心作为备份。

在配置高可用性之前，请确保同步要链接的防御中心之间的时间设置。有关设置时间的详细信息，请参阅第 63-24 页上的同步时间。

根据策略及其具有的自定义标准文本规则的数量，可能需要长达 10 分钟，所有规则和策略才会显示在两个防御中心上。可以查看 High Availability 页面来检查两个防御中心之间的链路的状态。还可以监控 Task Status 来查看进程何时完成。请参阅第 4-13 页上的监控和更改高可用性状态。

如果高可用性对中的其中一个防御中心必须重新映像，请先禁用高可用性链路。重新映像防御中心后，重新建立高可用性对，并且数据会从现有防御中心同步到新添加的防御中心。如果防御中心无法重新映像（例如，设备发生故障），请与技术支持部门联系。

要为两个防御中心设置高可用性，请执行以下操作：

访问：管理

步骤 1　登录要指定为辅助防御中心的防御中心。

步骤 2　选择 **System > Local > Registration**。

系统将显示 Registration 页面。

步骤 3　点击 **High Availability**。

系统将显示 High Availability 页面。

步骤 4　点击**辅助防御中心**选项。

系统将显示 Secondary 防御中心 Setup 页面。

步骤 5　在 **Primary DC Host** 文本框中键入主防御中心的主机名或 IP 地址。

注意事项　如果网络使用 DHCP 来分配 IP 地址，请确保使用主机名而不是 IP 地址。

请注意，如果管理主机不具有可路由地址，则可以将 **Primary DC Host** 字段保留为空。在此情况下，请同时使用 **Registration Key** 和 **Unique NAT ID** 字段。

步骤 6　在 **Registration Key** 文本框中键入一次性注册密钥

步骤 7　或者，在 **Unique NAT ID** 字段中，键入要用于识别主防御中心的唯一字母数字注册 ID。有关详情，请参见第 4-6 页上的在 NAT 环境中工作。

步骤 8　点击 **Register**。

系统将显示成功消息和 Peer Manager 页面，该页面上显示辅助防御中心的当前状态。

步骤 9　使用具有管理员访问权限的帐户登录到要指定为主防御中心的防御中心。

步骤 10　选择 **System > Local > Registration**。

系统将显示 Registration 页面。

步骤 11　点击 **High Availability**。

系统将显示 High Availability 页面。

步骤 12　点击 **primary 防御中心** 选项。

系统将显示 Primary 防御中心 Setup 页面。

步骤 13　在 **Primary DC Host** 文本框中键入辅助防御中心的主机名或 IP 地址。

注意事项　如果网络使用 DHCP 来分配 IP 地址，请确保使用主机名而不是 IP 地址。

步骤 14　在 **Registration Key** 文本框中键入在第 6 步中所使用的同一个一次性注册密钥。

步骤 15　如果在辅助防御中心上使用了唯一 NAT ID，请在 **Unique NAT ID** 文本框中键入第 7 步中所用的那个注册 ID。

步骤 16　点击 **Register**。

系统将显示成功消息和 Peer Manager 页面，该页面上显示主防御中心的当前状态。

监控和更改高可用性状态

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

在您确定了主要和辅助防御中心之后，您可以从高可用性对中的任一设备查看关于本地防御中心及其对等体的信息，包括：

- 对等体 IP 地址或主机名
- 对等体产品型号
- 对等体软件版本
- 对等体操作系统
- 距高可用性对的成员最后一次同步的时间
- 本地设备的角色和状态 （活动与主要，非活动与主要，非活动与辅助或活动与辅助）

如果主防御中心发生故障，也可以使用 High Availability 页面更改防御中心的角色。由于系统将以下功能限于主防御中心，因此如果该设备发生故障，则必须将辅助防御中心升级为主用设备：

- 更新 URL 类别和信誉数据；有关详细信息，请参阅第 4-10 页上的 URL 过滤和安全情报。
- 更新安全情报源；有关详细信息，请参阅第 4-10 页上的 URL 过滤和安全情报。
- 在关联规则与响应之间进行关联；有关详细信息，请参阅第 4-10 页上的关联响应。

要检查高可用性状态，请执行以下操作：

访问：管理

步骤 1　登录使用高可用性链接的其中一个防御中心。

步骤 2　选择 **System > Local > Registration**。

系统将显示 Registration 页面。

步骤 3　点击 **High Availability**。

系统将显示 High Availability 页面。

步骤 4　在 **High Availability Status** 下，可以查看有关高可用性对中防御中心的以下信息：

- 对等体 IP 地址或主机名
- 对等体产品型号
- 对等体软件版本
- 对等体操作系统
- 距高可用性对的成员最后一次同步的时间
- 本地设备的角色和状态（活动与主要，非活动与主要，非活动与辅助或活动与辅助）
- 用于在两个防御中心之间切换角色的选项

步骤 5　执行任何会影响共享功能的操作之后，两个防御中心将在 10 分钟内自动同步（每个防御中心花费 5 分钟）。例如，如果在一个防御中心上创建新策略，则会在 5 分钟内自动与另一个防御中心共享该策略。但是，如果要立即同步策略，请点击 **Synchronize**。

注　如果您从高可用性对中配置的防御中心中删除设备并计划重新添加该设备，则思科建议等待至少 5 分钟后再重新添加设备。此时间间隔确保高可用性对首先再同步。如果不等待 5 分钟，则可能需要多个同步周期才能将设备添加到两个防御中心。

步骤 6　点击 **Switch Roles** 以将本地角色从 Active 更改为 Inactive，或者从 Inactive 更改为 Active。

在 Primary 或 Secondary 指定保持不变的情况下，角色在两个对等体之间切换。

步骤 7　点击工具栏中的 **Peer Manager**。

系统将显示 Peer Manager 页面。

可以查看以下信息：

- 高可用性对中另一个防御中心的 IP 地址
- 通信链路的状态（已注册或未注册）
- 高可用性对的状态（已启用或已禁用）

有关编辑两台设备之间的远程管理通信的信息，请参阅第 4-18 页上的编辑远程管理。

禁用高可用性和注销设备

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

如果要从高可用性对中移除其中一个防御中心，则必须首先禁用其之间的高可用性链路。

要禁用高可用性对，请执行以下操作：

访问：管理

步骤 1　登录高可用性对中的其中一个防御中心。

步骤 2　选择 **System > Local > Registration**。

系统将显示 Registration 页面。

步骤 3　点击 **High Availability**。

系统将显示 High Availability 页面。

步骤 4　从 **Handle Registered Devices** 下拉列表中选择以下选项之一：

- 要使用访问此页面所通过的防御中心控制所有受管设备，请选择 **Unregister devices on the other peer**。
- 要使用另一个防御中心控制所有受管设备，请选择 **Unregister devices on this peer**。
- 要完全停止管理设备，请选择 **Unregister devices on both peers**。

步骤 5　点击 **Break High Availability**。

当出现 **Do you really want to Break High Availability?**提示时，如果您选择 **OK**，系统会根据选择禁用高可用性并从防御中心中删除任何受管设备。

可以使用其他防御中心启用高可用性，如第 4-12 页上的设置高可用性中所述。

暂停成对防御中心之间的通信

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

如果要暂时禁用高可用性，则可以禁用防御中心之间的通信信道。

要禁用高可用性对的通信信道，请执行以下操作：

访问：管理

步骤 1　点击 **Peer Manager**。

系统将显示 Peer Manager 页面。

步骤 2　点击滑块以禁用两个防御中心之间的通信信道。

有关编辑两台设备之间的远程管理通信的信息，请参阅第 4-18 页上的编辑远程管理。

重新启动成对防御中心之间的通信

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000

如果暂时禁用高可用性，则可以启用防御中心之间的通信信道以重新启动高可用性。

要启用高可用性对的通信信道，请执行以下操作：

访问：管理

步骤 1　点击 **Peer Manager**。

系统将显示 Peer Manager 页面。

步骤 2　点击滑块以启用两个防御中心之间的通信信道。

有关编辑两台设备之间的远程管理通信的信息，请参阅第 4-18 页上的编辑远程管理。

处理设备

许可证：任何环境

可以使用防御中心管理组成 FireSIGHT 系统的整个系列设备。管理设备时，会在防御中心和设备之间设置双向、SSL 加密的通信信道。防御中心 使用此信道向设备发送有关要如何分析和管理网络流量的信息。

设备评估流量时，会生成事件并使用同一信道将其发送到防御中心。

有关管理设备的详细信息，请参阅以下各节：

了解 Device Management 页面

许可证：任何环境

Device Management 页面提供可用于管理注册设备、设备集群和设备组的相关信息和选项。该页面显示防御中心上当前注册的所有设备的列表。

可以使用 **sort-by** 下拉列表根据需要将设备列表排序。设备在设备列表中按所选类别分组进行显示。可以按照以下方式排序：

- 组（即设备组）；有关详细信息，请参阅第 4-23 页上的管理设备组
- 类型（即应用到设备的许可证的类型）；有关详细信息，请参阅第 65-1 页上的许可 FireSIGHT 系统
- 型号（即由防御中心管理的设备的型号）
- 运行状况策略；有关详细信息，请参阅第 68-1 页上的使用运行状况监控
- 系统策略；有关详细信息，请参阅第 63-1 页上的管理系统策略
- 访问控制策略；有关详细信息，请参阅第 12-9 页上的管理访问控制策略

对于设备组，可以展开和折叠组中的设备列表。默认情况下，列表以折叠状态显示。

有关设备列表的详细信息，请参阅下表。

表 4-1　　设备列表字段

字段	说明
字段名称	每台设备的主机名、 IP 地址、设备型号和软件版本的列表。设备左侧的状态图标表示其当前运行状态。
许可证类型	在受管设备上启用的许可证。
健康政策	设备的当前应用的运行状况策略。可以点击运行状况策略的名称查看策略的只读版本。有关修改现有运行状况策略的信息，请参阅第 68-27 页上的编辑运行状况策略。
System Policy	设备的当前应用的系统策略。可以点击系统策略的名称查看策略的只读版本。有关详情，请参见第 63-1 页上的管理系统策略。
访问控制策略	指向当前应用的访问控制策略的链接。请参阅第 12-9 页上的管理访问控制策略。

有关详细信息，请参阅以下各节：

- 第 4-17 页上的配置远程管理
- 第 4-20 页上的将设备添加到防御中心
- 第 4-23 页上的管理设备组
- 第 4-25 页上的集群设备
- 第 4-37 页上的管理堆叠设备

配置远程管理

许可证：任何环境

必须先在两个 FireSIGHT 系统设备之间设置双向、 SSL 加密的通信信道，然后才能对两台设备进行相互管理。设备使用信道共享配置和事件信息。高可用性对等体也使用该信道，默认情况下，该信道在端口 8305/tcp 上。

必须在将受管理的设备上（即在要使用防御中心管理的设备上）配置远程管理。配置远程管理后，可以使用管理设备的网络界面将受管设备添加到部署中。

请注意，本节中的过程说明如何在 FirePOWER 物理设备上配置远程管理。

要启用两台设备之间的通信，必须提供设备相互识别的方法。 FireSIGHT 系统在允许通信时使用三个条件：

- 尝试建立通信时所使用的设备的主机名或 IP 地址

  在 NAT 环境中，即使另一设备没有可路由地址，在配置远程管理或添加受管设备时也必须提供主机名或 IP 地址。

- 长度多达 37 个字符的用于识别连接的自生成字母数字注册密钥
- 可帮助 FireSIGHT 系统在 NAT 环境中建立通信的可选唯一字母数字 NAT ID

  该 NAT ID **必须**在用于注册受管设备的所有 NAT ID 中唯一。有关详细信息，请参阅第 4-6 页上的在 NAT 环境中工作。

向防御中心注册受管设备时，可以选择向该设备应用的访问控制策略。但是，如果设备与策略不兼容，则策略应用会失败。这种不兼容有多种可能的原因，包括许可不匹配、型号限制、被动与内联问题和其他配置错误。如果初始访问控制策略应用失败，则初始网络发现策略也会应用失

败。在解决导致失败的问题后，您必须手动向设备应用访问控制和网络发现策略。有关可能导致访问控制策略应用失败的问题的详细信息，请参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

要配置本地设备的远程管理，请执行以下操作：

访问：管理

步骤 1　在要管理的设备的网络界面上，选择 **System > Local > Registration**。

系统将显示 Remote Management 页面。

注意事项　思科**强烈**建议不更改管理端口的值。如果更改端口值，还必须为部署中需要相互通信的所有设备更改端口值。有关详细信息，请参阅第 4-19 页上的更改管理端口。

步骤 2　点击 **Add Manager**。

系统将显示 Add Remote Management 页面。

步骤 3　在 **Management Host** 字段中，键入要用于管理此设备的设备的 IP 地址或主机名。

主机名是完全限定域名或通过本地 DNS 解析为有效 IP 地址的名称。

在 NAT 环境中，如果计划在添加受管设备时指定 IP 地址或主机名，则无需在此处进行指定。在此情况下，FireSIGHT 系统使用后来将提供的 NAT ID 识别受管设备的网络界面上的远程管理器。

注意事项　如果网络使用 DHCP 来分配 IP 地址，请使用主机名而不是 IP 地址。

步骤 4　在 **Registration Key** 字段中，键入要用于设置设备之间的通信的注册密钥。

步骤 5　对于 NAT 环境，请在 **Unique NAT ID** 字段中，键入要用于设置设备之间的通信的**唯一**字母数字 NAT ID。

步骤 6　点击 **Save**。

在设备确认其是否可以相互通信后，会显示 Pending Registration 状态。

步骤 7　使用管理设备的网络界面将此设备添加到部署中。

有关详细信息，请参阅第 4-20 页上的将设备添加到防御中心。

注　启用设备的远程管理时，在使用 NAT 的一些高可用性部署中，可能还需要以管理员身份添加辅助防御中心。有关详细信息，请与技术支持部门联系。

编辑远程管理

许可证：任何环境

使用以下过程编辑管理设备的主机名或 IP 地址。也可以更改管理设备的显示名称，该名称仅在 FireSIGHT 系统环境的上下文内使用。尽管可以使用主机名作为设备的显示名称，但是输入其他显示名称不会更改主机名。

请注意，不能添加运行多个主版本低于防御中心的软件的设备。例如，如果防御中心运行的是 5.4.0 版本，则可以添加运行 5.3.x 或更高版本的设备，但不能添加运行 5.2.x 版本的设备。

提示　可以点击滑块启用或禁用受管设备的管理。禁用管理会阻止防御中心和设备之间的连接，但是不会从防御中心删除设备。如果不想再管理设备，请参阅第 4-23 页上的删除设备。

要编辑远程管理，请执行以下操作：

访问：管理

步骤 1　在设备的网络界面上，选择 **System > Local > Registration**。

系统将显示 Remote Management 页面。

步骤 2　点击要为其编辑远程管理设置的管理器旁边的编辑图标 ( )。

系统将显示 Edit Remote Management 页面。

步骤 3　在 **Name** 字段中，更改管理设备的显示名称。

步骤 4　在 **Host** 字段中，更改管理设备的 IP 地址或主机名。

主机名是完全限定域名或通过本地 DNS 解析为有效 IP 地址的名称。

步骤 5　点击 **Save**。

已保存您的更改。

更改管理端口

许可证：任何环境

FireSIGHT 系统设备使用双向、SSL 加密的通信信道（默认情况下在端口 8305 上）进行通信。

尽管思科**强烈**建议保留默认设置，但如果管理端口与网络上的其他通信冲突，则可以选择其他端口。通常，在 FireSIGHT 系统安装期间对管理端口进行更改。

注意事项　如果更改管理端口，则必须为部署中需要相互通信的所有设备更改该端口。

要更改管理端口，请执行以下操作：

访问：管理

步骤 1　在设备的网络界面上，选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **Network**。

系统将显示 Network Settings 页面。

步骤 3　在 **Remote Management Port** 字段中，输入要使用的端口号。

步骤 4　点击 **Save**。

系统更改管理端口。

步骤 5　对部署中必须与此设备进行通信的每台设备重复此过程。

将设备添加到防御中心

许可证：任何环境

管理设备时，会在防御中心和设备之间设置双向、 SSL 加密的通信信道。防御中心使用此信道向设备发送有关要如何分析网络流量的信息。设备评估流量时，会生成事件并使用同一信道将其发送到防御中心。有关配置该信道的详细信息，请参阅第 4-17 页上的配置远程管理。

请注意，不能添加运行多个主版本低于防御中心的软件的设备。例如，如果防御中心运行的是 5.4 版本，则可以添加运行 5.3.x 或更高版本的设备，但不能添加运行 5.2.x 版本的设备。

使用防御中心管理设备之前，必须确保在该设备上正确配置网络设置。这通常在安装过程中完成。有关详情，请参见第 64-8 页上的配置管理接口。

请注意，如果注册了防御中心和一个使用 IPv4 的设备并要将其转换为 IPv6，则必须删除并重新注册该设备。

向防御中心注册受管设备时，可以选择向该设备应用的访问控制策略。但是，如果设备与策略不兼容，则策略应用会失败。这种不兼容有多种可能的原因，包括许可不匹配、型号限制、被动与内联问题和其他配置错误。如果初始访问控制策略应用失败，则初始网络发现策略也会应用失败。在解决导致失败的问题后，您必须手动向设备应用访问控制和网络发现策略。有关可能导致访问控制策略应用失败的问题的详细信息，请参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

注册设备集群或设备堆栈时，虽然可以选择许可证，但在设备注册时无法应用这些许可证。这确保集群或堆栈运行正确的许可证，以防止因许可证不匹配而进入降级状态。注册后，可以在 Device Management 页面的通用属性（集群）或堆栈属性（堆栈）中评估许可证。有关详细信息，请参阅第 4-27 页上的建立设备集群或第 4-39 页上的建立设备堆栈。

注册 2 系列设备时，虽然可以选择许可证，但在设备注册时不会应用您选择的任何许可证。2 系列设备自动配有保护功能，安全情报过滤除外。不能禁用这些功能，也不能向 2 系列设备应用其他许可证。

提示　要修改设备的详细配置，请点击设备旁边的编辑图标 ( )。有关详细信息，请参阅第 4-42 页上的编辑设备配置和第 4-52 页上的配置感应接口。

要向防御中心添加设备，请执行以下操作：

访问：管理员/网络管理员

步骤 1　将设备配置为由防御中心管理。

对于 FirePOWER 设备，请使用第 4-17 页上的配置远程管理中的过程。设备确认与防御中心的通信后，会显示 Pending Registration 状态。

对于虚拟设备、用于 Blue Coat X-系列的思科 NGIPS和 ASA FirePOWER 设备，请使用设备的命令行界面 (CLI) 配置远程管理。

注　在使用了网络地址转换 (NAT) 的一些高可用性部署中，可能需要以管理员身份添加辅助防御中心。有关详细信息，请与技术支持部门联系。

步骤 2　在防御中心的网络界面上，选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 3　从 **Add** 下拉菜单中，选择 **Add Device**。

系统将显示 Add Device 弹出窗口。

步骤 4　在 **Host** 字段中，键入要添加的设备的 IP 地址或主机名。

设备的主机名是完全限定域名或通过本地 DNS 解析为有效 IP 地址的名称。

请注意，在 NAT 环境中，如果在将设备配置为由防御中心管理时已经指定防御中心的 IP 地址或主机名，则可能无需指定设备的 IP 地址或主机名。有关详细信息，请参阅第 4-6 页上的在 NAT 环境中工作。

注意事项　如果网络使用 DHCP 来分配 IP 地址，请使用主机名而不是 IP 地址。

步骤 5　在 **Registration Key** 字段中，键入将设备配置为由防御中心管理时所使用的同一注册密钥。

步骤 6　或者，通过从 **Group** 下拉列表中选择设备组来将设备添加到该组。

有关设备组的详细信息，请参阅第 4-23 页上的管理设备组。

步骤 7　从 **Access Control Policy** 下拉列表中，选择要应用到设备的初始策略：

- **Default Access Control** 策略阻止所有流量进入网络。
- **Default Intrusion Prevention** 策略允许也通过 Balanced Security 和 Connectivity 入侵策略传递的所有流量。
- **Default Network Discovery** 策略允许仅通过网络发现进行检查的所有流量。
- 可以选择用户定义的任何现有的访问控制策略。

有关详细信息，请参阅第 12-9 页上的管理访问控制策略。

步骤 8　选择要应用到设备的许可证。请注意：

- 可控性、恶意软件和 URL 过滤许可证需要保护许可证。
- 不能在虚拟设备、用于 Blue Coat X-系列的思科 NGIPS或 ASA FirePOWER 设备上启用 VPN 许可证。
- 您无法在用于 Blue Coat X-系列的思科 NGIPS 上启用控制许可证。
- 虽然可在虚拟设备或 ASA FirePOWER 设备上启用可控性许可证，但这些设备不支持快速路径规则、交换、路由、堆栈或集群。
- 不能更改集群设备上的许可证设置。
- 对于堆叠设备，可以在设备编辑器的 Stack 页面上启用或禁用堆栈的许可证。
- 注册 2 系列设备时，在设备注册后未应用选择的任何许可证。2 系列设备自动配有保护功能，安全情报过滤除外。不能禁用这些功能，也不能向 2 系列设备应用其他许可证。

有关详细信息，请参阅第 65-1 页上的许可 FireSIGHT 系统。

步骤 9　如果在将设备配置为由防御中心管理时使用 NAT ID 识别设备，请展开 **Advanced** 部分并在 **Unique NAT ID** 字段中输入同一 NAT ID。

步骤 10　要允许设备将数据包传输到防御中心，请选择 **Transfer Packets** 复选框。

默认情况下，此选项启用。如果将其禁用，则完全禁止将数据包传输到 防御中心。

步骤 11　点击 **Register**。

设备将添加到防御中心。请注意，防御中心可能需要长达两分钟来验证设备的心跳并建立通信。

对设备应用更改

许可证：任何环境

在对设备、设备集群或设备堆栈的配置进行更改后，必须应用更改，然后更改才会在整个系统中生效。请注意，设备必须有未应用的更改，否则此选项保持禁用。

请注意，如果您编辑接口并重新应用设备策略， Snort 重启设备上的所有接口实例，而不仅仅重启您编辑的那些实例。

提示　可以从 Device Management 页面或从设备编辑器的 **Interfaces** 选项卡应用设备更改。

要将更改应用到设备，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要应用更改的设备旁边，点击应用图标 ( )。

步骤 3　出现提示时，点击 **Apply**。

系统将应用设备更改。

提示　或者，从 Apply Device Changes 对话框中，点击 **View Changes**。在新浏览器窗口中显示 Device Management Revision Comparison Report 页面。有关详细信息，请参阅第 4-22 页上的使用设备管理修订比较报告。

步骤 4　点击 **OK**。

将返回到 Device Management 页面。

使用设备管理修订比较报告

许可证：任何环境

通过设备管理比较报告，可以先查看已对设备进行的更改，然后再应用这些更改。报告显示当前设备配置和建议设备配置之间的全部差异。可借此机会发现任何潜在的配置错误。

要在应用设备更改之前对其进行比较，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要应用更改的设备旁边，点击应用图标 ( )。

系统将显示 Apply Device Changes 弹出窗口。请注意，设备必须有未应用的更改，否则应用图标保持禁用。

步骤 3　点击 **View Changes**。

在新窗口中显示 Device Management Revision Comparison Report 页面。

步骤 4　点击 **Previous** 和 **Next** 以滚动浏览当前设备配置和建议设备配置之间的差异。

步骤 5　或者，点击 **Comparison Report** 以生成报告的 PDF 版本。

删除设备

许可证：任何环境

如果不希望再管理设备，可以将其从防御中心中删除。删除设备会切断防御中心和设备之间的所有通信。要在以后某个日期再次管理设备，必须将其重新添加到防御中心。

注　如果您从高可用性对中配置的防御中心中删除设备并计划重新添加该设备，则思科建议您等待至少 5 分钟后再重新添加该设备。此时间间隔可以确保高可用性对重新同步，以便两个防御中心均意识到此删除。如果不等待 5 分钟，则可能需要多个同步周期才能将设备添加到两个防御中心。

要从防御中心中删除设备，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要删除的设备旁边，点击删除图标 ( )。

出现提示时，确认是否要删除设备。设备和防御中心之间的通信将会中断，并会从 Device Management 页面中删除设备。如果设备具有造成其通过 NTP 从防御中心接收时间的系统策略，则设备恢复为本地时间管理。

管理设备组

许可证：任何环境

防御中心允许将设备分组，从而可以在多台设备上轻松应用策略和安装更新。可以展开和折叠组中的设备列表。默认情况下，列表以折叠状态显示。

有关详细信息，请参阅以下各节：

- 第 4-24 页上的添加设备组
- 第 4-24 页上的编辑设备组
- 第 4-25 页上的删除设备组

添加设备组

许可证：任何环境

以下过程说明如何添加设备组，从而可以在多台设备上轻松应用策略和安装更新。

如果向组中添加堆栈或集群中的主设备，则会将两台设备均添加到该组中。如果将设备退栈或取消集群，则两台设备均保留在该组中。

要创建设备组并向其添加设备，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　从 **Add** 下拉菜单中，选择 **Add Group**。

系统将显示 Add Group 弹出窗口。

步骤 3　在 **Name** 字段中，键入组的名称。

步骤 4　在 **Available Devices** 下，选择要添加到设备组的一个或多台设备。点击的同时使用 Ctrl 或 Shift 键以选择多台设备。

步骤 5　点击 **Add** 将所选设备包含在设备组中。

步骤 6　点击 **OK**。

系统添加设备组。

编辑设备组

许可证：任何环境

可以更改驻留在任何设备组中的设备集。必须先从设备的当前组中移除该设备，然后才能将其添加到新组。

将设备移至新组不会将其策略更改为先前应用到组的策略。要更改设备的策略，必须将新策略应用到设备或设备组。

请注意，如果向组中添加堆栈或集群中的主设备，则会将两台设备均添加到该组中。如果将设备退栈或取消集群，则两台设备均保留在该组中。

要编辑设备组，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要编辑的设备组旁边，点击编辑图标 ( )。

系统将显示 Edit Group 弹出窗口。

步骤 3　或者，在 **Name** 字段中，键入组的新名称。

步骤 4　在 **Available Devices** 下，选择要添加到设备组的一个或多台设备。点击的同时使用 Ctrl 或 Shift 键以选择多台设备。

步骤 5　点击 **Add** 将所选设备包含在设备组中。

步骤 6　要从设备组中移除所选设备，请点击删除图标 ( )。

步骤 7　点击 **OK**。

系统保存对设备组的更改。

删除设备组

许可证：任何环境

如果删除包含设备的设备组，则会将组中的设备移至 Device Management 页面上的 Ungrouped 类别。这些设备并未从防御中心中删除。

要删除设备组，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要删除的设备组旁边，点击删除图标 ( )。

步骤 3　出现提示时，确认是否要删除设备组。

系统将删除设备组。

集群设备

许可证：可控性

受支持的设备：3 系列

通过设备集群（又称为设备高可用性），可以在两个对等设备或两个对等设备堆栈之间建立网络功能和配置数据的冗余。有关堆叠设备的详细信息，请参阅第 4-37 页上的管理堆叠设备。

可以通过将两个对等设备或两个对等设备堆栈集群为策略应用、系统更新和注册的单个逻辑系统来实现配置冗余。系统自动同步其他配置数据。

集群要求

设备或设备堆栈主成员必须为同一型号并具有相同的铜接口和光纤接口，然后才能配置设备集群。设备或设备堆栈还必须均运行的是相同软件并具有相同许可证。除已安装的恶意软件存储包以外，设备堆栈必须具有相同的硬件配置。例如，可以将 3D8290 与 3D8290 进行集群；在任一堆栈中，可能没有任何设备、有一台设备或所有设备都具有已安装的恶意软件存储包。如果 NAT 策略以设备为目标，则两个对等体均必须具有相同的 NAT 策略。将设备进行集群后，无法更改个别集群设备的许可证选项，但是可以更改整个集群的许可证。有关详情，请参见第 4-27 页上的建立设备集群。

注意事项 请勿尝试在设备中安装思科未提供的硬盘驱动器。安装不受支持的硬盘驱动器可能会损坏设备。恶意软件存储包套件**仅**可从思科购买，而且**仅限**用于 8000 系列设备。如果需要恶意软件存储包方面的帮助，请与技术支持部门联系。有关详细信息，请参阅《*FireSIGHT 系统恶意软件存储包指南*》。

集群故障转移和维护模式

通过设备集群，系统手动或自动故障转移。通过使其中一个集群设备或堆栈进入维护模式，可以手动触发故障转移。有关维护模式的详细信息，请参阅第 4-32 页上的使集群设备进入维护模式。

在主用设备或堆栈的运行状况受损之后、系统更新期间或具有管理员权限的用户关闭设备之后，会发生自动故障转移。在主用设备或设备堆栈经历 NMSB 故障、 NFE 故障、硬件故障、固件故障、重要流程故障、磁盘已满条件或两个堆叠设备之间链路故障之后，也会发生自动故障转移。如果备份设备或堆栈的运行状况同样受损，则系统不进行故障转移并会进入降级状态。其中一台设备或设备堆栈处于维护模式中时，系统也不进行故障转移。请注意，将堆叠电缆与活动堆栈断开连接会使该堆栈进入维护模式。关闭活动堆栈中的辅助设备也会使该堆栈进入维护模式。

注 如果活动集群成员进入维护模式并且活动角色故障切换至另一集群成员，当原活动集群成员恢复正常运行时，它不会自动恢复活动角色。

应用策略和更新

应用策略时，策略应用到设备集群而不是单个设备或堆栈。如果策略失败，则系统不将其应用到设备或堆栈。策略首先应用到主用设备或堆栈，然后应用到备份，以便集群始终有一个对等体处理网络流量。

集群设备将更新作为单个实体而不是单个设备或堆栈进行接收。启动更新后，系统先将其应用到备份设备或堆栈，随后进入维护模式，直到所有必要的流程重新启动，并且设备再次开始处理流量。然后，系统以同样的方式将更新应用到主用设备或堆栈。

在不集群设备的情况下实现冗余

大多数情况下，可以使用思科冗余协议 (SFRP) 在不集群设备的情况下实现第 3 层冗余。 SFRP 允许设备充当指定 IP 地址的冗余网关。通过网络冗余，可配置两台设备或堆栈以提供相同的网络连接，从而确保网络上其他主机的连接。有关 SFRP 的详细信息，请参阅第 7-6 页上的配置 SFRP。

根据 FireSIGHT 系统部署（被动、内联、路由式或交换机式），可确定如何配置设备高可用性。也可以一次性以多个角色部署系统。在四种部署类型中，仅被动部署要求您集群设备或堆栈以提供冗余。可以在具有或没有设备集群的情况下为其他部署类型建立网络冗余。以下各节简要概述各部署类型中的高可用性。

被动部署冗余

被动接口通常连接到中央交换机上的分接头端口，这使其能够分析流经交换机的所有流量。如果多台设备连接到同一分接器，则系统从每台设备生成事件。集群后，设备充当活动或备份设备，这使系统即使在发生故障的情况下也能分析流量，同时还可防止事件重复。

内联部署冗余

由于内联集无法控制通过其传递的数据包的路由，因此其在部署中必须始终处于活动状态。因此，冗余需要依靠外部系统才能正确路由流量。可以在具有或没有设备集群的情况下配置冗余内联集。

要部署冗余内联集，可配置网络拓扑，以便其仅允许流量通过其中一个内联集传递，同时防止循环路由。如果其中一个内联集失败，则周围的网络基础设施会检测与网关地址的连接是否丢失，并将路由调整为通过冗余集发送流量。

路由式部署冗余

IP 网络中的主机必须使用众所周知的网关地址将流量发送到不同网络。在路由式部署中建立冗余要求路由式接口共享网关地址，以便仅一个接口在任何指定时间处理该地址的流量。为此，必须在虚拟路由器上保留相等数量的 IP 地址。一个接口通告地址。如果该接口发生故障，则备份接口开始通告地址。

在非集群设备中，通过配置多个路由式接口之间共享的网关 IP 地址来使用 SFRP 建立冗余。可以在具有或没有设备集群的情况下配置 SFRP。也可以使用动态路由协议（例如 OSPF 和 RIP）建立冗余。

交换机式部署冗余

使用生成树协议 (STP) 在交换机式部署中建立冗余。 STP 是一种管理桥接网络拓扑的协议。它专门用于允许冗余链路为交换机式接口提供自动备份而不配置备份链路。交换机式部署中的设备依靠 STP 管理冗余接口之间的流量。连接到同一广播网络的两台设备根据 STP 计算的拓扑接收流量。有关启用 STP 的详细信息，请参阅第 6-6 页上的配置高级虚拟交换机设置。

注　思科强烈建议在配置计划于设备集群中部署的虚拟交换机时启用 STP。

有关将设备和堆栈进行集群的详细信息，请参阅以下各节：

- 第 4-27 页上的建立设备集群
- 第 4-29 页上的编辑设备集群
- 第 4-29 页上的配置集群中的单个设备
- 第 4-30 页上的配置集群中的单个设备堆栈
- 第 4-31 页上的在集群设备上配置接口
- 第 4-31 页上的在集群中切换活动对等体
- 第 4-32 页上的使集群设备进入维护模式
- 第 4-32 页上的替换集群堆栈中的设备
- 第 4-33 页上的建立集群状态共享
- 第 4-34 页上的对集群状态共享进行故障排除
- 第 4-37 页上的分隔集群设备
- 第 7-6 页上的配置 SFRP
- 第 4-55 页上的配置高可用性链路接口

建立设备集群

许可证：可控性

受支持的设备：3 系列

建立设备集群之前，必须满足以下先决条件：

- 在堆栈中的每台设备或每台主设备上配置接口。
- 在集群中包含的每台设备或设备堆栈主成员必须为同一型号并具有相同的铜接口或光纤接口。
- 设备或设备堆栈均必须具有正常运行状态，运行相同软件，并具有相同许可证。有关详情，请参见第 68-37 页上的使用运行状况监视器。特别是，设备不能具有会导致其进入维护模式并触发故障转移的硬件故障。

- 集群中的设备和堆栈必须匹配。必须将具有相同硬件配置的单一设备与单一设备进行集群，或者将具有相同硬件配置的设备堆栈与设备堆栈进行集群，但存在恶意软件存储包时除外。例如，可以将 3D8290 与 3D8290 进行集群；任一堆栈中无任何设备、一台设备或所有设备可能具有已安装的恶意软件存储包。有关恶意软件存储包的详细信息，请参阅《*FireSIGHT 系统恶意软件存储包指南*》。

注意事项 请勿尝试在设备中安装思科未提供的硬盘驱动器。安装不受支持的硬盘驱动器可能会损坏设备。恶意软件存储包套件**仅**可从思科购买，而且**仅限**用于 8000 系列设备。如果需要恶意软件存储包方面的帮助，请与技术支持部门联系。有关详细信息，请参阅《*FireSIGHT 系统恶意软件存储包指南*》。

- 如果 NAT 策略以设备为目标，则两个对等体均必须具有相同的 NAT 策略。

建立设备集群时，请将其中一台设备或堆栈指定为活动，将其他设备或堆栈指定为备份。系统对集群设备应用合并配置。如果存在冲突，则系统应用已指定为活动的设备或堆栈中的配置。

将设备进行集群后，无法更改个别集群设备的许可证选项，但是可以更改整个集群的许可证。有关详情，请参见第 4-29 页上的编辑设备集群。如果有需要在交换机式接口或路由式接口上设置的接口属性，则系统会建立集群，但是将其设置为处于挂起状态。配置必要的属性后，系统即完成设备集群并将其设置为处于正常状态。

建立集群对之后，系统在 Device Management 页面上将对等设备或堆栈视为单台设备。设备集群在设备列表中显示集群图标 ( )。所进行的任何配置更改都会在集群设备之间同步。 Device Management 页面显示集群中的哪台设备或堆栈处于活动状态，哪个在手动或自动故障转移后发生更改。有关手动故障转移的详细信息，请参阅第 4-32 页上的使集群设备进入维护模式。

从防御中心中移除设备集群的注册会从设备或堆栈中均移除注册。请按照移除个别受管设备的方式从防御中心中移除设备集群。有关详情，请参见第 4-23 页上的删除设备。

然后，可以在其他防御中心上注册集群。要注册集群单一设备，请向集群中的主用设备添加远程管理，然后将该设备添加到防御中心，从而增加整个集群。要注册集群堆叠设备，请向任一堆栈的主设备添加远程管理，然后将该设备添加到防御中心，从而添加整个集群。有关详情，请参见第 4-20 页上的将设备添加到防御中心。

建立设备集群后，可按照第 4-55 页上的配置高可用性链路接口中的说明配置高可用性链路接口。

要将设备或设备堆栈进行集群，请执行以下操作：

访问：管理员/网络管理员

步骤 1 选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2 从 **Add** 下拉菜单中，选择 **Add Cluster**。

系统将显示 Add Cluster 弹出窗口。

步骤 3 在 **Name** 字段中，键入集群的名称。

除以下无效字符外，可以输入字母数字字符和特殊字符：+、(、)、{、}、#、&、\、<、>、?、‘ 和 “。

步骤 4 为集群选择 **Active** 设备或堆栈。

步骤 5 为集群选择 **Backup** 设备或堆栈。

步骤 6 点击**集群**。

系统添加设备集群。由于此过程会同步系统数据，因此需要花费几分钟时间。

编辑设备集群

许可证：可控性

受支持的设备：3 系列

建立设备集群后，对设备配置进行的大多数更改还会更改整个集群的配置。

通过将指针悬停在 General 部分中状态图标的上方，可以查看集群的状态。还可以查看哪台设备或堆栈是集群中的活动对等体和备份对等体。

有关详细信息，请参阅以下各节：

- 第 4-43 页上的编辑常规设备设置
- 第 4-44 页上的启用和禁用设备许可证
- 第 4-33 页上的建立集群状态共享
- 第 4-48 页上的编辑高级设备设置

要编辑设备集群，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要编辑配置的设备集群旁边，点击编辑图标 ( )。

系统将显示 Cluster 页面。

步骤 3　按照更改单一设备配置的方式，使用 Cluster 页面上的各部分对集群配置进行更改。

配置集群中的单个设备

许可证：可控性

受支持的设备：3 系列

建立设备集群后，仍可以配置集群内每台设备的部分属性。可以完全按照更改单台设备的方式对集群设备进行更改。

有关详细信息，请参阅以下各节：

- 第 4-43 页上的编辑常规设备设置
- 第 4-45 页上的编辑设备系统设置
- 第 4-46 页上的查看设备的运行状况
- 第 4-46 页上的编辑设备管理设置

要配置集群中的单个设备，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要编辑配置的设备集群旁边，点击编辑图标 ( )。

系统将显示 Cluster 页面。

步骤 3　点击 **Devices**。

系统会显示“设备”页面。

步骤 4　从 **Selected Device** 下拉列表中，选择要修改的设备。

步骤 5　按照更改单台设备的方式，使用 Devices 页面上的各部分对单个集群设备进行更改。

配置集群中的单个设备堆栈

许可证：可控性

受支持的设备：3 系列

将堆叠式设备对集群后，系统会限制可编辑的堆栈属性。可以编辑集群堆栈中的堆栈的名称。此外，可以编辑堆栈的网络配置，如第 4-31 页上的在集群设备上配置接口中所述。

要编辑集群中的堆栈的名称，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要编辑配置的设备集群旁边，点击编辑图标 ( )。

系统将显示 Cluster 页面。

步骤 3　点击 **Stacks**。

系统将显示 Stacks 页面。

从 **Selected Device** 下拉列表中，选择要修改的堆栈。

步骤 4　点击 General 部分旁边的编辑图标 ( )。

系统将显示 General 弹出窗口。

步骤 5　在 **Name** 字段中，键入新分配的堆栈名称。

除以下无效字符外，可以输入字母数字字符和特殊字符：+、(、)、{、}、#、&、\、<、>、?、‘ 和 “。

步骤 6　点击 **Save**。

系统保存新名称。请注意，直到应用堆栈配置后更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

在集群设备上配置接口

许可证：可控性

受支持的设备：3 系列

可以在集群中的一台设备上配置接口。但是，还必须在集群中的对等设备上配置等效接口。对于集群堆栈，请在堆栈的主设备上配置相同接口。配置虚拟路由器时，请选择要在其中配置路由器的堆栈。有关详情，请参见第 7-7 页上的配置虚拟路由器。

集群设备的 Interfaces 页面包含在单个设备上找到的硬件和接口视图。有关详情，请参见第 4-52 页上的配置感应接口。

要在集群设备上配置接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要配置接口的设备集群旁边，点击编辑图标 ()。

系统将显示 Cluster 页面。

步骤 3　点击 **Interfaces**。

系统将显示 Interfaces 页面。

步骤 4　从 **Selected Device** 下拉列表中，选择要修改的设备。

步骤 5　按照在单个设备上进行配置的方式配置接口。有关详情，请参见第 4-52 页上的配置感应接口。

在集群中切换活动对等体

许可证：可控性

受支持的设备：3 系列

建立设备集群后，可以手动切换活动和备份对等设备或堆栈。

要在集群中切换活动对等体，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要更改活动对等体的设备集群旁边，点击交换机主用对等设备图标 ()。

系统将显示 Switch Active Peer 弹出窗口。

步骤 3　点击 **Yes** 将使备份设备立即成为集群中的主用设备。点击 **No** 将取消并返回到 Device Management 页面。

使集群设备进入维护模式

许可证：可控性

受支持的设备：3 系列

建立集群后，可以通过使其中一个集群设备或堆栈进入维护模式以对设备执行维护来手动触发故障转移。在维护模式中，系统以管理方式中断除管理接口以外的所有接口。维护完成后，可以重新启用设备以恢复正常运行。

注　不能同时使集群中的两个成员均进入维护模式。这样会阻止该集群检查流量。

要使集群设备进入维护模式，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要使其进入维护模式的集群设备旁边，点击切换维护模式图标 ( )。

系统将显示 Confirm Maintenance Mode 弹出窗口。

步骤 3　点击 **Yes** 确认维护模式，或者点击 **No** 取消。

步骤 4　再次点击切换维护模式图标 ( ) 使设备退出维护模式。

替换集群堆栈中的设备

许可证：可控性

受支持的设备：3 系列

使身为集群成员的堆栈进入维护模式后，可以将该堆栈中的辅助设备替换为其他设备。只能选择当前未堆叠或集群的设备。新设备必须遵循建立设备堆栈的相同准则。请参阅第 4-39 页上的建立设备堆栈。

要替换集群堆栈中的设备，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要使其进入维护模式的堆栈成员旁边，点击切换维护模式图标 ( )。

系统将显示 Confirm Maintenance Mode 弹出窗口。

步骤 3　点击 **Yes** 确认维护模式，或者点击 **No** 取消。

步骤 4　点击替换设备图标 ( )。

系统将显示 Replace Device 弹出窗口。

步骤 5　从下拉列表中选择 **Replacement Device**。

步骤 6　点击 **Replace** 替换设备，或者点击 **Cancel** 保留当前设备并返回到 Device Management 页面。

步骤 7　再次点击切换维护模式图标 ( ) 使堆栈立即退出维护模式。

无需重新应用设备配置。

建立集群状态共享

许可证：可控性

受支持的设备：3 系列

集群设备或集群堆栈可通过集群状态共享同步尽可能多的状态，以便在设备或堆栈发生故障的情况下，其他对等体可以接管而不中断流量。如果不进行状态共享，则以下功能可能无法正常执行故障转移：

- 严格 TCP 实施
- 单向访问控制规则
- 阻止持久性

不过请注意，启用状态共享会降低系统性能。

必须在两台设备或集群中的主堆叠设备上配置并启用高可用性链路接口，然后才能配置集群状态共享。 3D8250 设备需要 10G 高可用性链路，而其他型号的设备需要 1G 高可用性链路。有关详情，请参见第 4-55 页上的配置高可用性链路接口。

注　如果集群设备进行故障转移，则系统会终止主用设备上所有现有 SSL 加密的会话。即使建立集群状态共享，也必须在备份设备上重新协商这些会话。如果建立 SSL 会话的服务器支持会话重复使用，并且备份设备没有 SSL 会话 ID，则其无法重新协商会话。有关详细信息，请参阅第 4-25 页上的集群设备。

严格 TCP 执行

对域启用严格 TCP 实施时，系统会丢弃 TCP 会话中顺序混乱的所有数据包。例如，系统丢弃在未建立的连接上收到的非 SYN 数据包。通过状态共享，集群中的设备在故障转移后允许 TCP 会话继续，而不必重新建立连接，即使启用了严格 TCP 实施也如此。可以在内联集、虚拟路由器和虚拟交换机上启用严格 TCP 实施。

单向访问控制规则

如果配置了单向访问控制规则，则系统在故障转移后重新评估连接代答时，网络流量可能会与不同于预期的访问控制规则匹配。例如，请考虑是否有包含以下两种访问控制规则的策略：

```
Rule 1: Allow from 192.168.1.0/24 to 192.168.2.0/24
Rule 2: Block all
```

在未进行状态共享的情况下，如果允许的从 192.168.1.1 到 192.168.2.1 的连接在故障转移后仍处于活动状态，并且下一个数据包被视为响应数据包，则系统拒绝连接。在进行状态共享的情况下，中途代答会与现有连接匹配并继续允许代答。

阻止持久性

虽然根据访问控制规则或其他因素在第一个数据包上阻止了许多连接，但在一些情况下系统会允许通过一定数量的数据包，然后再确定是否应阻止连接。通过状态共享，系统也会立即阻止对等设备或堆栈上的连接。

建立集群状态共享时，可以配置以下选项：

启用

点击该复选框以启用状态共享。清除该复选框以禁用状态共享。

Minimum Flow Lifetime

指定系统为会话发送任何同步消息之前该会话经过的最短时间（以毫秒为单位）。可以使用从 0 到 65535 的任何整数。系统不同步未达到最低流量生命周期的任何会话，并且，仅当连接接收到数据包时系统才会同步。

Minimum Sync.Interval

指定会话的更新消息间隔的最短时间（以毫秒为单位）。可以使用从 0 到 65535 的任何整数。最小同步间隔防止在连接达到最小生命周期后以超过配置值的频率发送指定连接的同步消息。

Maximum HTTP URL Length

指定系统在集群设备之间同步的 URL 的最大字符数。可以使用从 0 到 225 的任何整数。

注　思科建议您使用默认值，除非部署有充分的理由更改这些值。减小值会提高集群对等体就绪程度，而增大值会改善性能。

要建立集群状态共享，请执行以下操作：

访问：管理员/网络管理员

步骤 1　为集群中的每台设备配置高可用性链路接口。

有关详情，请参见第 4-55 页上的配置高可用性链路接口。

步骤 2　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 3　在要编辑的设备集群旁边，点击编辑图标 ( )。

系统将显示 Cluster 页面。

步骤 4　在 **State Sharing** 部分旁边，点击编辑图标 ( )。

系统将显示 State Sharing 弹出窗口。

步骤 5　配置状态共享，如本节中先前所述。

步骤 6　点击 **OK**。

已保存您的更改。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

对集群状态共享进行故障排除

许可证：可控性

受支持的设备：3 系列

启用状态共享后，可以在 Cluster 页面的 State Sharing 部分中查看有关配置的以下信息：

- 使用的高可用性链路接口及其当前链路状态
- 用于排除问题的详细同步统计信息

状态共享统计主要是发送和接收的集群同步流量的不同方面的计数器，以及一些其他错误计数器。此外，可以查看集群中每台设备的最新系统日志。

有关可以查看的每台设备的统计以及如何能够将其用于对集群状态共享配置进行故障排除的详细信息，请参阅以下各节。

Messages Received (Unicast)

Messages received 是从集群对等体接收的集群同步消息的数量。

该值应该接近对等体发送的消息数。在活动使用期间，值可能不匹配，但应该接近。如果流量停止，则值应该变得稳定，并且接收的消息会与发送的消息匹配。

要进行故障排除，应该同时查看接收的消息数和发送的消息数，比较增加率，并确保值接近。每个对等体上的发送值应该以与反对等体上的接收值大致相同的速率递增。

如果接收的消息数停止递增或递增速度慢于对等体发送消息的速度，请与技术支持部门联系。

Packets Received

系统将多个消息批处理为单一数据包，以便减少开销。 Packets Received 计数器显示这些数据包以及设备已接收的其他控制数据包的总数。

该值应该接近对等设备发送的数据包数。在活动使用期间，值可能不匹配，但应该接近。由于接收的消息数应该接近并以与对等体发送的消息数相同的速率递增，因此接收的数据包数应具有相同行为。

要进行故障排除，应该同时查看接收的数据包数和发送的消息数，比较增加率，并确保值以相同速率增加。如果集群对等体上的发送值在递增，则设备上的接收值也应以相同速率增加。

如果接收的数据包数停止递增或递增速度慢于对等体发送消息的速度，请与技术支持部门联系。

Total Bytes Received

Total bytes received 是组成对等体接收的数据包的字节数。

该值应该接近其他对等体发送的字节数。在活动使用期间，值可能不匹配，但应该接近。

要进行故障排除，应该同时查看接收的总字节数和发送的消息数，比较增加率，并确保值以相同速率增加。如果集群对等体上的发送值在递增，则设备上的接收值也应以相同速率增加。

如果接收的字节数停止递增或递增速度慢于对等体发送消息的速度，请与技术支持部门联系。

Protocol Bytes Received

Protocol bytes received 是接收的协议开销的字节数，其中包括除会话状态同步消息的负载以外的所有内容。

该值应该接近对等体发送的字节数。在活动使用期间，值可能不匹配，但应该接近。

要进行故障排除，应该查看接收的总字节数以发现在与协议数据比较时共享的实际状态数据量。如果协议数据在所发送数据中占较大的百分比，则可以调整最小同步间隔。

如果接收的协议字节数以类似于接收的总字节数的速率递增，请与技术支持部门联系。根据接收的总字节数，接收的协议字节数应该最小。

Messages Sent

Messages sent 是发送到集群对等体的集群同步消息的数量。

此数据在与接收的消息数比较的过程中有用。在活动使用期间，值可能不匹配，但应该接近。

要进行故障排除，应该同时查看接收的消息数和发送的消息数，比较增加率，并确保值接近。

如果发送的消息数以类似于接收的总字节数的速率递增，请与技术支持部门联系。

Bytes Sent

Bytes sent 是组成发送到对等体的集群同步消息的发送的总字节数。

此数据在与接收的消息数比较的过程中有用。在活动使用期间，值可能不匹配，但应该接近。在对等体上接收的字节数应该接近，但是不大于该值。

如果接收的总字节数不是以与发送的字节数大致相同的速率递增，请与技术支持部门联系。

Tx Errors

Tx errors 是系统为要发送到集群对等体的消息分配空间时遇到的内存分配失败数。

该值在两个对等体上均应该始终为零。如果此数字不为零，或者如果数字稳定增大（表示系统遇到无法分配内存错误），请与技术支持部门联系。

Tx Overruns

Tx overruns 是系统尝试将消息放入传输队列并失败的次数。

该值在两个对等体上均应该始终为零。值不为零或稳定增大时，表示系统通过高可用性链路共享着太多无法足够快速地发送的数据。

如果高可用性链路 MTU 先前设置为低于默认值（9918 或 9922），则应该将其增大。可以更改最小流量生命周期和最小同步间隔设置，以减少通过高可用性链路共享的数据量，从而防止数字递增。

如果该值仍然存在或持续增大，请与技术支持部门联系。

Recent Logs

系统日志显示最新的集群同步消息。日志不应显示任何 ERROR 或 WARN 消息。它应保持在对等体之间可比较，如连接的插槽数相同。

但是，所显示的数据在某些实例中可能相反，例如，一个对等体报告它从另一个对等体收到连接并引用不同的 IP 地址。日志提供集群状态共享连接和连接内任何错误的全面视图。

如果日志显示 ERROR 或 WARN 消息或并未显示为纯参考性的任何消息，请与技术支持部门联系。

要查看集群状态共享统计，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要编辑的设备集群旁边，点击编辑图标 ( )。

系统将显示设备集群的 Cluster 页面。

步骤 3　在 **State Sharing** 部分中，点击查看统计图标 ( )。

系统将显示 State Sharing Statistics 弹出窗口。

步骤 4　或者，如果集群由设备堆栈组成，请选择要查看的 **Device**。

步骤 5　或者，点击 **Refresh** 以更新统计。

步骤 6　或者，点击 **View** 以查看每个集群设备的最新数据日志。

分隔集群设备

许可证：可控性

受支持的设备：3 系列

中断设备集群时，主用设备或堆栈保留完整部署功能。除非选择保持接口配置处于活动状态，在此情况下备份设备或堆栈会恢复正常操作，否则备份设备或堆栈会丢失其接口配置并故障转移到主用设备或堆栈。中断集群始终移除备份设备上被动接口的配置。中断集群后，维护模式中的任何设备都会恢复正常操作。

要分隔集群设备，请执行以下操作；

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要中断的设备集群旁边，点击中断集群图标 ( )。

系统将显示 Confirm Break 弹出窗口。

步骤 3　或者，选择复选框以移除备份设备或堆栈上的接口配置，这意味着会以管理方式断开除管理接口以外的所有接口。

步骤 4　点击 **Yes**。

系统分隔设备集群。

管理堆叠设备

许可证：任何环境

受支持的设备：3D8140、3D8200 子系列、3D8300 子系列、3D9900

可以通过在堆叠配置中使用设备来增加网段检查的流量。对于每个堆叠配置，堆栈中的所有设备都必须具有相同硬件。但是，如果堆栈不包含 3D9900，则无任何设备、某些设备或所有设备可能具有已安装的恶意软件存储包。根据以下堆叠配置，设备还必须来自同一设备子系列：

对于 2 系列和 81xx 子系列：

- 两个 3D8140
- 两个 3D9900

对于 82xx 子系列：

- 最多四个 3D8250
- 3D8260（一台主设备和一台辅助设备）
- 3D8270（一台具有 40G 容量的主设备和两台辅助设备）
- 3D8290（一台具有 40G 容量的主要设备和三台辅助设备）

对于 83xx 子系列：

- 最多四个 3D8350
- 3D8360（一台具有 40G 容量的主设备和一台辅助设备）

- 3D8370（一台具有 40G 容量的主设备和两台辅助设备）
- 3D8390（一台具有 40G 容量的主设备和三台辅助设备）

有关堆叠配置的详细信息，请参阅《*FireSIGHT 系统安装指南*》。有关恶意软件存储包的详细信息，请参阅《*FireSIGHT 系统恶意软件存储包指南*》。

注意事项 请勿尝试在设备中安装思科未提供的硬盘驱动器。安装不受支持的硬盘驱动器可能会损坏设备。恶意软件存储包套件**仅**可从思科购买，而且**仅限**用于 8000 系列设备。如果需要恶意软件存储包方面的帮助，请与技术支持部门联系。有关详细信息，请参阅《*FireSIGHT 系统恶意软件存储包指南*》。

建立堆叠配置时，请将每台堆叠设备的资源组合成单个共享配置。

将一台设备指定为*主*设备，在该设备上配置整个堆栈的接口。将其他设备指定为*辅助*设备。辅助设备当前不得感知任何流量，并且不得在任何接口上具有链路。

请以与配置单台设备相同的方式将主设备连接到要分析的网段。有关详情，请参见第 4-52 页上的配置感应接口。按照在《*FireSIGHT 系统安装指南*》中提供的堆叠设备布线说明将辅助设备连接到主设备。

堆叠配置中的所有设备都必须具有相同硬件，运行同一软件版本，并具有相同许可证。如果 NAT 策略以设备为目标，则主设备和辅助设备均必须具有同一 NAT 策略。有关详情，请参见第 11-7 页上的管理 NAT 策略。必须从防御中心将更新应用到整个堆栈。如果更新在堆栈中的一个或多台设备上失败，则堆栈进入混合版本状态。不能在混合版本状态下将策略应用到堆栈或更新堆栈。要纠正此状态，可以中断堆栈或移除具有不同版本的单个设备，更新单个设备，然后重新建立堆叠配置。在堆叠设备后，可以立即仅更改整个堆栈的许可证。

建立堆叠配置后，设备如同单个共享配置。如果主设备发生故障，则无任何流量传递到辅助设备。系统会生成指示堆叠心跳在辅助设备上发生故障的运行状况警报。有关详情，请参见第 68-1 页上的使用运行状况监控。

如果堆栈中的辅助设备发生故障，已启用可配置旁路的内联集会进入主要设备的旁路模式。对于所有其他配置，系统会继续将均衡流量加载到发生故障的辅助设备。无论是哪一种情况，系统都会生成指示链路丢失的运行状况警报。

可以在部署中按照使用单台设备的方式使用设备堆栈，但会存在几个异常。如果具有集群设备，则不能在集群对中堆叠设备集群或设备。有关详情，请参见第 4-25 页上的集群设备。也不能在设备堆栈上配置 NAT。

注 如果使用 eStreamer 将事件数据从堆叠设备流化到外部客户端应用，请从每台设备收集数据并确保以相同方式配置每台设备。 eStreamer 设置在堆叠设备之间未自动同步。

有关详细信息，请参阅以下各节：

建立设备堆栈

许可证：任何环境

受支持的设备：3D8140、3D8200 子系列、3D8300 子系列、3D9900

可以通过堆叠两个基于光纤的 3D9900、两个 3D8140 设备、最多四个 3D8250、一个 3D8260、一个 3D8270、一个 3D8290、最多四个 3D8350、一个 3D8360、一个 3D8370 或一个 3D8390 并在单个共享配置中使用其组合资源来增加网段检查的流量。开始之前，必须：

- 确定哪台设备将作为主设备
- 指定主/辅助设备关系之前正确对设备进行布线。有关布线的信息，请参阅《*FireSIGHT 系统安装指南*》。

注　如果具有集群设备，则不能在集群对中堆叠设备集群或设备。但是，可以集群设备堆栈。有关详情，请参见第 4-25 页上的集群设备。

建立设备堆栈后，系统在 Device Management 页面上将多台设备视为单台设备。设备堆栈在设备列表中显示堆栈图标 ( )。

从防御中心中移除设备堆栈的注册会从两种设备中都移除注册。请按照删除单个受管设备的方式从防御中心中删除堆叠设备；然后，可以在其他防御中心上注册堆栈。只需在新的防御中心上注册其中一个堆叠设备即可显示整个堆栈。有关详细信息，请参阅第 4-23 页上的删除设备和第 4-20 页上的将设备添加到防御中心。

建立设备堆栈后，除非中断并重新建立堆栈，否则无法更改哪些设备是主或辅助。但是，可以：

- 将辅助设备添加到由两个或三个 3D8250、一个 3D8260 或一个 3D8270 组成的现有堆栈（在一个堆栈中限制最多有四个 3D8250）
- 将辅助设备添加到由两个或三个 3D8350、一个 3D8360 或一个 3D8370 组成的现有堆栈（在一个堆栈中限制最多有四个 3D8350）

对于其他设备，堆栈中的主设备必须具有其他已布线设备的必要的堆叠网络模块。例如，如果 3D8260 中的主设备仅有单个堆叠网络模块，则无法向此堆栈中添加其他辅助设备。请以最初建立堆叠设备配置的相同方式将辅助设备添加到现有堆栈。

要建立堆叠设备配置，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　从 **Add** 下拉菜单中，选择 **Add Stack**。

系统将显示 Add Stack 弹出窗口。

步骤 3　从 **Primary** 下拉列表中，选择已为主要操作布线的设备。

注　如果编辑未作为主要设备进行布线的设备，则无法执行后面的系列步骤。

步骤 4　在 **Name** 字段中，键入堆栈的名称。除以下无效字符外，可以输入字母数字字符和特殊字符：+、(、)、 {、 }、 #、 &、 \、 <、 >、 ?、 ‘ 和 “。

步骤 5　点击 **Add** 以选择要用于组成堆栈的设备。

系统将显示 Add Secondary Connection 弹出窗口。下图显示 3D8140 的主设备的前视图。

步骤 6　从 **Slot on Primary Device** 下拉列表中，选择将主设备连接到辅助设备的堆叠网络模块。

步骤 7　从 **Secondary Device** 下拉列表中，选择已为辅助操作布线的设备。

注　堆栈中的所有设备都必须为同一硬件型号（例如，3D9900 与 3D9900、3D8140 与 3D8140，依此类推）。可以在 82xx 子系列和 83xx 子系列中堆叠总共四台设备（一台主设备和最多三台辅助设备）。

步骤 8　从 **Slot on Secondary Device** 下拉列表中，选择将辅助设备连接到主设备的堆叠网络模块。

步骤 9　点击 **Add**。

系统重新显示 Add Stack 窗口，其中包含新的辅助设备。

步骤 10　或者，如果是将辅助设备添加到由多台 3D8250、一台 3D8260、一台 3D8270 组成的现有堆栈或由多台 3D8350、一台 3D8360 或一台 3D8370 组成的现有堆栈，请重复第 5 步到第 9 步。

步骤 11　点击 **Stack**。

系统建立设备堆栈或者添加其他辅助设备。请注意，由于此过程会同步系统数据，因此需要花费几分钟时间。

编辑设备堆栈

许可证：任何环境

受支持的设备：3D8140、3D8200 子系列、3D8300 子系列、3D9900

建立设备堆栈后，对设备配置进行的大多数更改还会更改整个堆栈的配置。在设备编辑器的 Stack 页面上，可以按照与在单台设备的 Device 页面上相同的方式对堆栈配置进行更改。

可以更改堆栈的显示名称，启用和禁用许可证，查看系统和运行状况策略，配置自动应用旁路以及设置快速路径规则。

有关详细信息，请参阅以下各节：

- 第 4-43 页上的编辑常规设备设置
- 第 4-44 页上的启用和禁用设备许可证
- 第 4-48 页上的编辑高级设备设置

要编辑堆叠配置，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要编辑配置的堆叠设备旁边，点击编辑图标 ( )。

系统将显示该设备的 Stack 页面。

步骤 3　按照更改单一设备配置的方式，使用 Stack 页面上的各部分对堆叠配置进行更改。

配置堆栈中的单台设备

许可证：任何环境

受支持的设备：3D8140、3D8200 子系列、3D8300 子系列、3D9900

建立设备堆栈后，仍可以仅配置堆栈内一台设备的部分属性。在设备编辑器的 Devices 页面上，可以按照与单台设备的 Devices 页面上相同的方式对堆栈中配置的设备进行更改。

可以更改设备的显示名称，查看系统设置，关闭或重新启动设备，查看运行状况信息，以及编辑设备管理设置。

有关详细信息，请参阅以下各节：

- 第 4-43 页上的编辑常规设备设置
- 第 4-45 页上的编辑设备系统设置
- 第 4-46 页上的查看设备的运行状况
- 第 4-46 页上的编辑设备管理设置

要配置堆栈中的单个设备，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要编辑配置的堆叠设备旁边，点击编辑图标 ( )。

系统将显示该设备的 Stack 页面。

步骤 3　点击 **Devices**。

系统会显示“设备”页面。

步骤 4　从 **Selected Device** 下拉列表中，选择要修改的设备。

步骤 5　按照更改单台设备的方式，使用 Devices 页面上的各部分对单个堆叠设备进行更改。

在堆叠设备上配置接口

许可证：任何环境

受支持的设备：3D8140、3D8200 子系列、3D8300 子系列、3D9900

除管理接口以外，在堆栈中主设备的 Interfaces 页面上还可配置堆叠设备接口。可以选择堆栈中的任何设备来配置管理接口。有关详情，请参见第 64-8 页上的配置管理接口。

3 系列 堆叠设备的 Interfaces 页面包含在单个设备上找到的硬件和接口视图。3D9900 的 Interfaces 页面不包含这些视图。有关详情，请参见第 4-52 页上的配置感应接口。

要在堆叠设备上配置接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要配置接口的堆叠设备旁边，点击编辑图标 ( )。

系统将显示该设备的 Stack 页面。

步骤 3　点击 **Interfaces**。

系统将显示 Interfaces 页面。

步骤 4　从 **Selected Device** 下拉列表中，选择要修改的设备。

步骤 5　按照在单个设备上进行配置的方式配置接口。有关详情，请参见第 4-52 页上的配置感应接口。

分隔堆叠设备

许可证：任何环境

受支持的设备：3D8140、3D8200 子系列、3D8300 子系列、3D9900

如果不再需要对设备使用堆叠配置，则可以中断堆栈并分隔设备。

要分隔堆叠设备，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要中断的设备堆栈旁边，点击中断堆栈图标 ( )。

系统将显示 Confirm Break 弹出窗口。

提示　要从由三个或更多 3D8250 设备组成的堆栈中移除辅助设备而不中断堆栈，请点击从堆栈中移除图标 ( )。移除辅助设备会导致短暂中断流量检查、流量或链路状态，因为系统会重新配置堆栈以在没有额外设备的情况下运行。

步骤 3　点击 **Yes**。

系统分隔设备堆栈。

编辑设备配置

许可证：任何环境

设备编辑器的 Device 页面显示详细设备配置和信息。通过该页面，还可以对设备配置的某些部分进行更改，例如，启用和禁用许可证，关闭并重新启动设备，修改管理以及设置快速路径规则。

有关详细信息，请参阅以下各节：

- 第 4-43 页上的编辑常规设备设置
- 第 4-44 页上的启用和禁用设备许可证
- 第 4-45 页上的编辑设备系统设置
- 第 4-46 页上的查看设备的运行状况

编辑常规设备设置

许可证：任何环境

Device 选项卡的 General 部分显示以下列出的受管设备设置，您可以更改这些设置。

字段名称

为受管设备分配的名称。

Transfer Packets

表示是否已将数据包数据传输至防御中心以和事件一起存储。

要编辑常规设备设置，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要编辑分配的名称的设备旁边，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 页面。

步骤 3　点击 **Device**。

系统将显示 Device 页面。

提示　对于堆叠设备，编辑设备编辑器的 Stack 页面上堆栈的分配的设备名称。可以编辑设备编辑器的 Devices 页面上单个设备的分配的设备名称。

步骤 4　在 **General** 部分旁边，点击编辑图标 ( )。

系统将显示 General 弹出窗口。

步骤 5　在 **Name** 字段中，键入设备的新分配名称。除以下无效字符外，可以输入字母数字字符和特殊字符：+、（、）、{、}、#、&、\、<、>、?、‘ 和 “。

步骤 6　选择 **Transfer Packets** 复选框以允许数据包数据随事件一起存储在防御中心上。清除该复选框以防止受管设备随事件发送数据包数据。

步骤 7　点击 **Save**。

系统保存更改。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

启用和禁用设备许可证

许可证：任何环境

受支持的设备：3 系列、虚拟设备、 X -系列和 ASA FirePOWER

如果在防御中心上有可用的许可证，则可以启用设备上的许可证。请注意：

- 可控性、恶意软件和 URL 过滤许可证需要保护许可证。
- 不能在虚拟设备、用于 Blue Coat X-系列的思科 NGIPS或 ASA FirePOWER 设备上启用 VPN 许可证。
- 虽然可以在虚拟设备、用于 Blue Coat X-系列的思科 NGIPS或 ASA FirePOWER 设备上启用可控性许可证，但这些设备不支持快速路径规则、切换、路由、堆叠或集群。用于 Blue Coat X-系列的思科 NGIPS不支持应用或用户控制。
- 不能更改集群设备上的许可证设置。
- 由于 2 系列设备自动具有除安全情报过滤以外的保护功能，因此，既不能禁用这些功能，也不能对 2 系列设备应用其他许可证。

有关详细信息，请参阅第 65-1 页上的许可 FireSIGHT 系统。

要启用或禁用设备许可证，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要启用或禁用许可证的设备旁边，点击编辑图标 ( )。

系统将显示该设备的 **Interfaces** 选项卡。

步骤 3　点击 **Device**。

系统将显示 **Devices** 选项卡。

提示　对于堆叠设备，可以在设备编辑器的 Stack 页面上启用或禁用堆栈的许可证。

步骤 4　在 **License** 部分旁，点击编辑图标 ( )。

系统将显示 License 弹出窗口。

步骤 5　您有以下选项：

- 要启用许可证，请选择许可证名称旁边的复选框。
- 要禁用许可证，请清除许可证名称旁边的复选框。

步骤 6　点击 **Save**。

系统保存更改。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

编辑设备系统设置

许可证：任何环境

Device 选项卡的 System 部分显示只读系统信息表，如下表中所述。

表 4-2　　System 部分表字段

字段	说明
型号	受管设备的型号名称和编号。
串行	受管设备的机箱的序列号。
时间	设备的当前系统时间。
版本	受管设备上当前安装的软件版本。
策略	指向当前应用到受管设备的系统策略的链接。

也可以关闭或重新启动设备。

注　不能使用 FireSIGHT 系统用户界面关闭或重新启动 X-系列 或 ASA FirePOWER 设备。有关如何关闭各自设备的详细信息，请参阅《*用于 Blue Coat X-系列的思科 NGIPS 安装指南*》或 ASA 文档。

要关闭并重新启动受管设备，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要重新启动的设备旁边，点击编辑图标 ( )。

系统将显示该设备的 **Interfaces** 选项卡。

步骤 3　点击 **Device**。

系统将显示 **Devices** 选项卡。

提示　对于堆叠设备，关闭或重新启动设备编辑器的 Devices 页面上的单个设备。

步骤 4　要关闭设备，请点击关闭设备图标 ( )。

步骤 5　出现提示时，确认是否要关闭设备。

将返回到 Device Management 页面。

步骤 6　要重新启动设备，请点击重新启动设备图标 ( )。

步骤 7　出现提示时，确认是否要重新启动设备。

设备将会重新启动。

请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

查看设备的运行状况

许可证：任何环境

Device 选项卡的 Health 部分显示运行状况相关信息。可以查看显示受管设备的当前运行状况的图标。也可以点击该图标以导航至该设备的 Health Monitor 页面。有关详情，请参见第 68-38 页上的解释运行状况监视器状态。

可以点击 **Policy** 链接查看当前应用的运行状况策略的只读版本。有关详情，请参见第 68-27 页上的编辑运行状况策略。

也可以点击 **Blacklist** 链接转至 页面，在该页面上可以启用和禁用运行状况黑名单模块。有关详情，请参见第 68-34 页上的将运行状况策略模块列入黑名单。

编辑设备管理设置

许可证：任何环境

Device 选项卡的 Management 部分显示下列远程管理信息。

主机

设备的当前管理主机名或 IP 地址。您可以使用此设置指定管理主机名和重新生成虚拟 IP 地址。

注　有时，如果您通过其他方法编辑设备的主机名或 IP 地址（例如使用设备的 LCD 面板或 CLI），可能需要使用以下操作步骤手动更新管理防御中心上的主机名或 IP 地址。

状态

指定防御中心和受管设备之间的通信信道的状态。

提示　可以点击滑块启用或禁用受管设备的管理。禁用管理会阻止防御中心和设备之间的连接，但是**不会**从防御中心删除设备。如果不想再管理设备，请参阅第 4-23 页上的删除设备。

要修改设备管理选项，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要修改管理选项的设备旁边，点击编辑图标 ( )。

系统将显示该设备的 **Interfaces** 选项卡。

步骤 3　点击 **Device**。

系统将显示 **Devices** 选项卡。

提示　对于堆叠设备，修改设备编辑器的 Devices 页面上单个设备的管理选项。

步骤 4　在 **Management** 部分旁边，点击编辑图标 ( )。

系统将显示 Management 弹出窗口。

步骤 5　在 **Host** 字段中，输入管理主机的名称或 IP 地址。

步骤 6　点击 **Save**。

已保存您的更改。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

了解高级设备设置

许可证：任何环境

受支持的设备：因功能而异

Device 选项卡上的 Advanced 部分显示高级配置设置表，如下表所述。

表 4-3　　Advanced 部分表字段

字段	说明	支持的设备
Application Bypass	设备上 Automatic Application Bypass 的状态。	2 系列、3 系列、虚拟设备
Bypass Threshold	Automatic Application Bypass 阈值（以毫秒为单位）。	2 系列、3 系列、虚拟设备
检查本地路由器流量	设备是否检查在路由式接口上接收的以其本身为目标的流量，如 ICMP、DHCP 和 OSPF 流量。	3 系列
快速路径规则	设备上已创建的快速路径规则数。	8000 系列、3D9900

可以使用 Advanced 部分编辑其中任何设置。有关详细信息，请参阅以下各节：

- 第 4-47 页上的自动应用旁路
- 第 4-48 页上的编辑高级设备设置
- 第 4-49 页上的配置快速路径规则

自动应用旁路

许可证：任何环境

自动应用旁路 (AAB) 功能限制通过接口处理数据包所允许的时间，并在超过时间的情况下允许数据包绕开检测。该功能适用于任何部署；但在内联部署中最有价值。

通过网络的数据包延迟容限来平衡数据包处理时延。如果 Snort 中出现故障或设备配置不当导致流量处理时间超过指定阈值，则 AAB 会导致 Snort 在发生故障后的 10 分钟内重新启动，并生成故障排除数据，您可以分析这些数据以调查处理时间过长的原因。

在 5.4.1 版和更高版本中， AAB 选项的默认行为根据设备而异，如下所示：

- 3 系列：关闭
- 2 系列和虚拟设备：开启
- ASA FirePOWER：不支持
- X -系列：不支持

如果您从低于 5.3 的版本升级，则会保留现有设置。如果选择该选项，则可以更改旁路阈值。默认设置为 3000 毫秒 (ms)。有效范围为 250 ms 到 60,000 ms。

通常，在超过延迟阈值后使用入侵策略中的 Rule Latency Thresholding 通过快速路径传送数据包。Rule Latency Thresholding 不关闭引擎或生成故障排除数据。有关详细信息，请参阅第 18-10 页上的配置数据包和入侵规则延迟阈值。

注　只有在花费过量时间处理单个数据包时，才会激活 AAB。如果使用 AAB，则系统会终止所有 Snort 进程。

如果绕过了检测，则设备会生成运行状况监控警报。有关该运行状况监控警报的详细信息，请参阅第 68-37 页上的使用运行状况监视器。

有关启用自动应用旁路和设置旁路阈值的详细信息，请参阅第 4-48 页上的编辑高级设备设置。

编辑高级设备设置

许可证：任何环境

受支持的设备：因功能而异

可以使用 **Devices** 的 Advanced 部分修改 Automatic Application Bypass 和 Inspect Local Router Traffic 设置。还可以按照第 4-49 页上的配置快速路径规则中的说明配置快速路径规则。

请注意：

- 只能在 8000 系列和 3D9900 设备上配置快速路径规则。
- 只能在 3 系列设备上配置 **Inspect Local Router Traffic**。

要修改高级设备设置，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要编辑高级设备设置的设备旁边，点击编辑图标 ( )。

系统将显示该设备的 **Interfaces** 选项卡。

步骤 3　点击 **Device**。

系统将显示 **Devices** 选项卡。

提示　对于堆叠设备，编辑设备编辑器的 Stack 页面上堆栈的高级设备设置。

步骤 4　在 **Advanced** 部分旁边，点击编辑图标 ( )。

系统将显示 Advanced 弹出窗口。

步骤 5　或者，如果网络对延迟敏感，请选择 **Automatic Application Bypass**。自动应用旁路在内联部署中最有用。有关详细信息，请参阅第 4-47 页上的自动应用旁路。

步骤 6　如果 Automatic Application Bypass 选项，可以在 **Bypass Threshold** 中键入旁路阈值（以毫秒 (ms) 为单位）。默认设置为 3000 ms，并且有效范围为从 250 ms 到 60,000 ms。

步骤 7　或者，在部署为路由器时选择 **Inspect Local Router Traffic** 复选框以检查异常流量。

步骤 8　或者，配置快速路径规则。有关详细信息，请参阅第 4-49 页上的配置快速路径规则。

步骤 9　点击 **Save**。

已保存您的更改。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

配置快速路径规则

许可证：任何环境

受支持的设备：8000 系列、3D9900

可以创建快速路径规则以直接通过设备发送流量而无进一步检查。快速路径规则转移无需分析即可绕过设备的流量。快速路径规则将流量发送到快速路径（在接口外部），或者允许其继续进入设备以进行进一步分析。它们的优点在于其确定流量的正确路径的速度。由于快速路径规则在硬件层面起作用，因此其仅确定有关数据包的有限信息。

有关详细信息，请参阅以下各节：

- 第 4-49 页上的添加 IPv4 快速路径规则
- 第 4-50 页上的添加 IPv6 快速路径规则
- 第 4-52 页上的删除快速路径规则

添加 IPv4 快速路径规则

许可证：任何环境

受支持的设备：8000 系列、3D9900

快速路径规则将流量发送到快速路径（在接口外部），或者发送到设备中以进行进一步分析。可以使用以下条件选择要转移到快速路径且不检查的 IPv4 流量：

- 发起方或响应方 IP 地址或 CIDR 块
- 协议
- 发起方或响应方端口（适用于 TCP 或 UDP 协议）
- VLAN ID
- 双向选项

请注意，最外层的 ID 用于快速路径规则。

提示　要编辑现有快速路径规则，请点击规则旁边的编辑图标 ( )。

要构建或编辑 IPv4 快速路径规则，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要添加快速路径规则的设备旁边，点击编辑图标 ( )。

系统将显示该设备的 **Interfaces** 选项卡。

步骤 3　点击 **Device**。

系统将显示 **Devices** 选项卡。

步骤 4　在 **Advanced** 部分旁边，点击编辑图标 ( )。

系统将显示 Advanced 弹出窗口。

步骤 5　点击 **New IPv4 Rule** 添加快速路径规则。

系统将显示 New IPv4 Rule 弹出窗口。

步骤 6　从 **Domain** 下拉列表中，选择内联集或被动安全区域。有关详情，请参见第 5-1 页上的设置 IPS 设备。

步骤 7　在 **Initiator** 和 **Responder** 字段中使用 CIDR 表示法指定其数据包应绕过进一步分析的发起方和响应方的 IP 地址。

规则与来自指定发起方的数据包或面向指定响应方的数据包匹配。有关在 FireSIGHT 系统中使用 CIDR 表示法的信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 8　或者，从 **Protocol** 下拉列表中，选择要对其应用规则的协议，或者选择 **All** 以匹配来自列表中任何协议的流量。

步骤 9　或者，如果在第 8 步中选择 TCP 或 UDP 协议，请在 **Initiator Port** 和 **Responder Port** 字段中输入发起方和响应方端口以指定端口。

提示　可以在每个规则中输入端口号的逗号分隔列表。在 IPv4 快速路径规则中不能使用端口范围。请注意，空白端口值作为 **Any** 处理。

如果还选择 **Bidirectional** 选项，则过滤条件范围缩小为来自这些发起方端口的数据包或面向这些响应方端口的数据包。

步骤 10　或者，在 **VLAN** 字段中输入 VLAN ID。

规则仅与该 VLAN 的流量匹配。请注意，空白 VLAN 值作为 **Any** 处理。

步骤 11　或者，选择 **Bidirectional** 选项以过滤在指定发起方和响应方 IP 地址之间传播的所有流量。清除该选项以仅过滤从指定发起方 IP 地址到指定响应方 IP 地址的流量。

步骤 12　点击 **Save**。

规则添加在 Advanced 弹出窗口中的 Fast-Path Rules 下。虽然添加了规则，但是必须再次点击 **Save** 才会保存规则。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

添加 IPv6 快速路径规则

许可证：任何环境

受支持的设备：3 系列、3D9900

快速路径规则将流量发送到快速路径（在接口外部），或者发送到设备中以进行进一步分析。可以使用以下条件选择要转移到快速路径且不检查的 IPv6 流量：

- 发起方或响应方 IP 地址或地址块
- 协议
- 发起方或响应方端口（适用于 TCP 或 UDP 协议）
- VLAN ID
- 双向选项

请注意，最外层的 VLAN ID 用于快速路径规则。

提示　要编辑现有快速路径规则，请点击规则旁边的编辑图标 ( )。

要添加 IPv6 快速路径规则，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要添加快速路径规则的设备旁边，点击编辑图标 ( )。

系统将显示该设备的 **Interfaces** 选项卡。

步骤 3　点击 **Device**。

系统将显示 **Devices** 选项卡。

步骤 4　在 **Advanced** 部分旁边，点击编辑图标。

系统将显示 Advanced 弹出窗口。

步骤 5　点击 **New IPv6 Rule** 以添加快速路径规则。

系统将显示 New IPv6 Rule 弹出窗口。请注意，发起方和响应方字段固定，并且指示过滤器适用于来自任何发起方或响应方的 IPv6 数据包。

步骤 6　从 **Domain** 下拉列表中，选择内联集或被动安全区域。有关详情，请参见第 5-1 页上的设置 IPS 设备。

步骤 7　键入 IP 地址，或者使用 IPv6 前缀长度表示法在 **Initiator** 和 **Responder** 字段中为其数据包应绕过进一步分析的发起方或响应方的 IP 地址指定地址块。

规则与来自指定发起方的数据包或面向指定响应方的数据包匹配。有关在 FireSIGHT 系统中使用 IPv6 前缀长度表示法的信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 8　或者，从 **Protocol** 下拉列表中，选择要对其应用规则的协议，或者选择 **All** 以匹配来自列表中任何协议的流量。

快速路径规则仅与所选协议的数据包匹配。

步骤 9　或者，如果在第 7 步中选择 TCP 或 UDP 协议，请在 **Initiator Port** 和 **Responder Port** 字段中输入发起方和响应方端口以指定端口。

提示　可以在每个规则中输入端口号的逗号分隔列表。在 IPv6 快速路径规则中不能使用端口范围。请注意，空白端口值作为 **Any** 处理。

步骤 10　或者，在 **VLAN** 字段中输入 VLAN ID。

规则仅与该 VLAN 的流量匹配。请注意，空白 VLAN 值作为 **Any** 处理。

步骤 11　或者，选择 **Bidirectional** 以过滤在指定发起方和响应方端口之间传播的所有流量。清除该选项以指定规则仅与来自这些发起方端口的数据包或面向这些响应方端口的数据包匹配。

步骤 12　点击 **Save**。

规则添加在 Advanced 弹出窗口中的 Fast-Path Rules 下。

步骤 13　在 Advanced 弹出窗口中，点击 **Save**。

系统保存规则。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

删除快速路径规则

许可证：任何环境

受支持的设备：8000 系列、3D9900

以下过程说明如何删除任何 IPv4 或 IPv6 快速路径规则。

要删除任何快速路径规则，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要删除快速路径规则的设备旁边，点击编辑图标 ( )。

系统将显示该设备的 **Interfaces** 选项卡。

步骤 3　点击 **Device**。

系统将显示 **Devices** 选项卡。

步骤 4　在 **Advanced** 部分旁边，点击编辑图标 ( )。

系统将显示 Advanced 弹出窗口。

步骤 5　在要删除的快速路径规则旁边，点击删除图标 ( )。

步骤 6　出现提示时，确认是否要删除规则。

规则将从 Advanced 弹出窗口中被删除。

步骤 7　点击 **Save**。

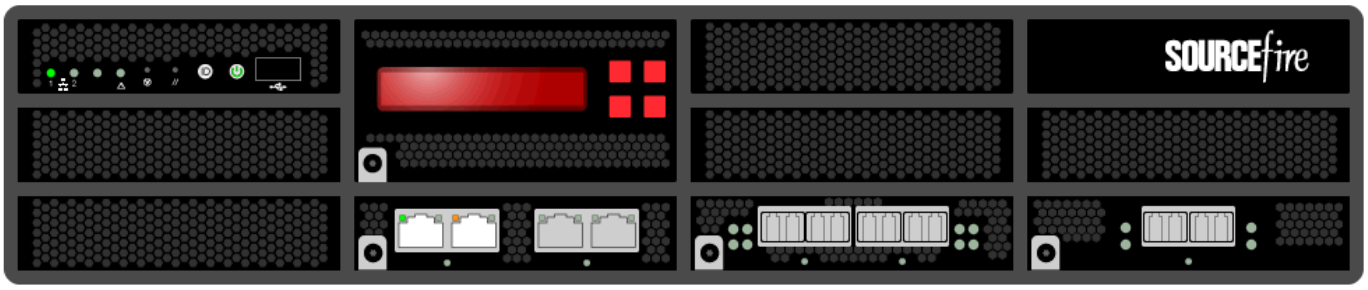
已保存您的更改。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

配置感应接口

许可证：任何环境

根据 FireSIGHT 系统部署，可以从设备编辑器的 Interfaces 页面配置受管设备的感应接口。

Interfaces 页面的顶部显示受管的 3 系列设备的物理硬件视图。 2 系列、虚拟设备、用于 Blue Coat X-系列的思科 NGIPS和 ASA FirePOWER 设备没有物理硬件视图。下图显示 3D8250 的硬件视图。



下表说明如何使用物理硬件视图。

表 4-4　使用硬件视图

要.....	您可以.....
查看网络模块的类型、部件号和序列号	将光标悬停在网络模块左下角的黑色圆圈上方。
在接口表视图中选择接口	点击接口。
打开接口编辑器	双击接口。
查看接口的名称、接口的类型、接口是否具有链路、接口的速度设置，以及接口当前是否处于旁路模式	将光标悬停在接口上方。
查看有关错误或警告的详细信息	将光标悬停在网络模块上的受影响端口上方。

位于 3 系列设备硬件视图下的接口表视图列出设备上的所有可用接口。该表包含可用来查看所有已配置的接口的可扩展式导航树。您可以点击接口旁的箭头图标以收起或展开接口，从而隐藏或查看其子部件。接口表视图中还提供了每个接口的汇总信息，如下表所述。请注意，仅 8000 系列设备会显示 MAC Address 列和 IP Address 列。有关详细信息，请参阅下表。

表 4-5　接口表视图字段

字段	说明
字段名称	每个接口类型都用指示其类型和链路状态（如适用）的唯一图标表示。您可以在工具提示中将指针悬停在名称或图标上面以查看接口类型、速度和双工模式（如果适用）。第 4-54 页上的表 4-6 对接口图标进行了说明。 这些图标使用标记规则指示接口的当前链接状态，其可能是以下三种状态之一： • 错误 () • 故障() • 不可用 () 逻辑接口具有与其父物理接口相同的链路状态。用于 Blue Coat X-系列的思科 NGIPS和 ASA FirePOWER 设备不显示链路状态。请注意，禁用的接口以半透明的图标表示。 在图标右侧显示的接口名称是自动生成的，但混合接口和 ASA FirePOWER 接口除外，那是用户定义的。请注意，对于 ASA FirePOWER 接口，系统仅显示已启用、已命名和具有链路的接口。 物理接口显示物理接口的名称。逻辑接口显示物理接口和分配的 VLAN 标记的名称。 ASA FirePOWER 接口显示安全上下文的名称和接口的名称 （如果有多个安全上下文）。如果只有一个安全上下文，则系统仅显示接口的名称。
Security Zone	已分配接口的安全区域。要添加或编辑安全区域，请点击编辑图标 ()。
Used by	已分配接口的内联集、虚拟交换机或虚拟路由器。 ASA FirePOWER 设备不显示 Used by 列。

表 4-5　接口表视图字段 （续）

字段	说明
MAC 地址	为交换式和路由式功能启用接口时，所显示的该接口的 MAC 地址。 对于虚拟设备，会显示 MAC 地址，以便可以将设备上配置的网络适配器与 Interfaces 页面上显示的接口匹配。用于 Blue Coat X-系列的思科 NGIPS和 ASA FirePOWER 设备不显示 MAC 地址。
IP 地址	分配给接口的 IP 地址。将指针悬停在 IP 地址上方以查看其处于活动还是非活动状态。非活动 IP 地址会灰显。 ASA FirePOWER 设备不显示 IP 地址。

表 4-6　接口图标类型和说明

图标	接口类型	有关详细信息，请参阅.....
	物理 - 未经配置的物理接口。	—
	被动 - 配置用于分析被动部署中的流量的感应接口。	第 5-1 页上的配置被动接口
	内联 - 配置用于处理内联部署中的流量的感应接口。	第 5-3 页上的配置内联接口
	交换 - 配置用于交换第 2 层部署中的流量的接口。	第 6-1 页上的配置交换接口
	路由 - 配置用于路由第 3 层部署中的流量的接口。	第 7-1 页上的配置路由接口
	高可用性 - 在设备集群对每个成员上配置的用作设备之间冗余通信渠道的接口，又称为高可用性链路接口。	第 4-55 页上的配置高可用性链路接口
	汇聚 - 配置为单个逻辑链路的多个物理接口。	第 8-1 页上的设置汇聚接口
	汇聚交换 - 配置为第 2 层部署中单个逻辑链路的多个物理接口。	第 8-4 页上的添加汇聚交换接口
	汇聚路由 - 配置为第 3 层部署中单个逻辑链路的多个物理接口。	第 8-6 页上的添加汇聚路由接口
	混合 - 配置用于桥接虚拟路由器和虚拟交换机之间流量的逻辑接口。	第 9-1 页上的添加逻辑混合接口
	ASA FirePOWER - 在安装了 ASA FirePOWER 模块的 ASA 设备上配置的接口。	第 4-56 页上的管理具备 FirePOWER 服务的 Cisco ASA 防火墙接口

请注意，在 FirePOWER 受管设备上最多只能配置 1024 个接口。

注　在 SPAN 端口模式中部署 ASA FirePOWER 时，防御中心不显示 ASA 接口。

有关可在设备上配置接口的不同方式的详细信息，请参阅以下各节：

- 第 4-55 页上的配置高可用性链路接口
- 第 4-56 页上的配置感应接口 MTU
- 第 4-56 页上的管理具备 FirePOWER 服务的 Cisco ASA 防火墙接口
- 第 4-57 页上的禁用接口
- 第 4-58 页上的防止连接日志记录重复
- 第 5-1 页上的设置 IPS 设备

- 第 6-1 页上的设置虚拟交换机
- 第 7-1 页上的设置虚拟路由器
- 第 8-1 页上的设置汇聚接口
- 第 9-1 页上的设置混合接口

配置高可用性链路接口

许可证：任何环境

受支持的设备：3 系列

建立设备集群后，可以将物理接口配置为高可用性 (HA) 链路接口。此链路充当用于在集群设备之间共享运行状况信息的冗余通信信道。在一台设备上配置高可用性链路接口时，在第二台设备上会自动配置接口。必须在同一广播域中配置两个高可用性链路。有关详情，请参见第 4-25 页上的集群设备。

动态 NAT 依靠动态分配 IP 地址和端口来映射到其他 IP 地址和端口。如果没有高可用性链路，则这些映射在故障转移中会丢失，导致所有已转换的连接失败，因为它们通过集群中的当前主用设备进行路由。

注意事项　更改最大传输单位 (MTU) 会中断设备流量。 MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

要配置高可用性链路接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要配置高可用性链路接口的集群设备旁边，点击编辑图标 ( )。

系统将显示该设备的 **Interfaces** 选项卡。

步骤 3　在要配置为高可用性链路接口的接口旁边，点击编辑图标 ( )。

系统将显示 Edit Interface 弹出窗口。

步骤 4　点击 **HA Link** 以显示高可用性链路选项。

步骤 5　选择 **Enabled** 复选框以允许高可用性链路接口提供链路。

如清除此复选框，则将禁用并强制性断开该接口。

步骤 6　从 **Mode** 下拉列表中，选择一个选项以指定链路模式，或者选择 **Autonegotiation** 以指定接口配置为自动协商速度和双工设置。

步骤 7　从 **MDI/MDIX** 下拉列表中，选择一个选项来指定将接口配置为 MDI（媒体依赖接口）、MDIX（媒体依赖接口的交叉）还是 Auto - MDIX。

通常， MDI/MDIX 设置为 **Auto-MDIX**，它会自动处理 MDI 和 MDIX 之间的切换以获取链路。

步骤 8　在 **MTU** 字段中，键入最大传输单位 (MTU)，它指定允许的最大数据包。

MTU 的设置范围因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

步骤 9　点击 **Save**。

已保存您的更改。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

配置感应接口 MTU

许可证：任何环境

如果更改接口或内联集上的最大传输单位 (MTU)，则以下功能可能会受影响：

- 流量检查，包括应用感知和控制、URL 过滤、入侵检测和防御以及连接日志记录
- 流量，包括交换、路由及相关功能
- 链路状态

网络流量中断的方式和持续时间取决于接口类型以及设备的配置和部署方式。

另请注意，对于用于 Blue Coat X-系列的思科 NGIPS，请使用用于 Blue Coat X-系列的思科 NGIPS CLI 配置接口 MTU。有关详细信息，请参阅《*用于 Blue Coat X-系列的思科 NGIPS 安装指南*》。

注　由于系统会自动从配置的 MTU 值中修剪 18 个字节，因此任何低于 1298 的值都不符合 1280 的最小 IPv6 MTU 设置，并且任何低于 594 的值都不符合 576 的最小 IPv4 MTU 设置。例如，系统自动将配置值 576 调整为 558。

下表列出 MTU 受管设备的配置范围。

表 4-7　　按设备划分的 MTU 范围

在此型号设备上...	MTU 范围是...
2 系列， 3D6500 和 3D9900 除外	576 到 1518（所有接口和内联集）
3D6500、 3D9900、虚拟设备	576 到 9018（所有接口和内联集）
3 系列	576 到 9234（管理接口） 576 到 10172（内联集） 576 到 9922（所有其他）

管理具备 FirePOWER 服务的 Cisco ASA 防火墙接口

许可证：保护

受支持的设备：ASA FirePOWER

编辑 ASA FirePOWER 接口时，从 FireSIGHT 防御中心只能配置接口的安全区域。有关详情，请参见第 3-34 页上的使用安全区域。

可使用特定于 ASA 的软件和 CLI 全面配置 ASA FirePOWER 接口。如果编辑 ASA FirePOWER 设备并从多情景模式切换至单情景模式（或反之），设备会重命名其所有接口。您必须重新配置所有 FireSIGHT 系统安全区域、关联规则以及相关的配置，才能使用更新的 ASA FirePOWER 接口名称。有关 ASA FirePOWER 接口配置的详细信息，请参阅 ASA 文档。

注　既不能更改 ASA FirePOWER 接口的类型，也不能从 FireSIGHT 防御中心禁用接口。

要编辑 ASA FirePOWER 接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要编辑接口的设备旁边，点击编辑图标 ( )。

系统将显示该设备的 **Interfaces** 选项卡。

步骤 3　在要编辑的接口旁边，点击编辑图标 ( )。

系统将显示 Edit Interface 弹出窗口。

步骤 4　从 **Security Zone** 下拉列表中，选择现有安全区域或选择 **New** 以添加新的安全区域。

步骤 5　点击 **Save**。

系统配置安全区域。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

禁用接口

许可证：任何环境

可以通过将接口类型设置为 **None** 禁用接口。已禁用的接口在接口列表中会灰显。

注　既不能更改 ASA FirePOWER 接口的类型，也不能从 FireSIGHT 防御中心禁用接口。

要禁用接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要禁用接口的设备旁边，点击编辑图标 ( )。

系统将显示该设备的 **Interfaces** 选项卡。

步骤 3　在要禁用的接口旁边，点击编辑图标 ( )。

系统将显示 Edit Interface 弹出窗口。

步骤 4　点击 **None**。

步骤 5　点击 **Save**。

已保存您的更改。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

防止连接日志记录重复

许可证：任何环境

更新安全区域对象时，系统会保存对象的新版本。因此，如果同一安全区域中的受管设备具有接口中配置的安全区域对象的不同修订版本，则可记录看似重复的连接。

如果发现重复连接报告，可以将所有受管设备更新为使用该对象的同一版本。

要跨设备同步安全区域对象修订版本，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

注意事项　不得将受管设备重新应用到任何设备，直到已编辑要同步的所有设备上接口的区域设置为止。

步骤 2　在要更新安全区域选择的设备旁边，点击编辑图标 ( )。

系统将显示该设备的 **Interfaces** 选项卡。

步骤 3　对于记录重复连接事件的每个接口，请将 **Security Zone** 更改为其他区域，点击 **Save**，然后将其重新更改为所需区域，并再次点击 **Save**。

步骤 4　为记录重复事件的每台设备重复第 2 步到第 3 步。

步骤 5　编辑所有设备上的所有接口后，立即将设备更改应用到所有受管设备。

设置 IPS 设备

您可以被动或内联 IPS 部署方式配置设备。在被动部署中，您可以在网络流量的带外部署系统。在内联部署中，您可以将两个端口绑定在一起，从而在网段上透明配置系统。

以下各节介绍如何在 FireSIGHT 系统中配置设备进行被动和内联部署：

了解被动 IPS 部署

许可证：保护

在被动 IPS 部署中，FireSIGHT 系统使用交换机 SPAN 或镜像端口通过网络监控流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。这可以提供网络内系统可视性，无需网络流量。如果在被动部署中进行配置，系统无法采取某些措施（例如，流量阻断和整形）。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。

注 出站流量包括流控制数据包。因此，设备上的被动接口可能根据您的配置显示出站流量并生成事件；这是预期行为。

配置被动接口

许可证：保护

您可以将受管设备的一个或多个物理端口配置为被动接口。

请注意，如果您编辑接口并重新应用设备策略， Snort 重启设备上的所有接口实例，而不仅仅重启您编辑的那些实例。

安装思科软件包时，可以将 用于 Blue Coat X-系列的思科 NGIPS 接口配置为被动或内联接口。您不能使用 FireSIGHT 系统网络接口重新配置 用于 Blue Coat X-系列的思科 NGIPS接口。有关详细信息，请参阅第 5-10 页上的为 Blue Coat X 系列接口配置思科 NGIPS。

注意事项　更改最大传输单位 (MTU) 会中断设备流量。 MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

要配置被动接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　点击要配置被动接口的设备旁的编辑图标 ( )。

系统将显示 **Interfaces** 选项卡。

步骤 3　在要配置为被动接口的接口旁边，点击编辑图标 ( )。

系统将显示 Edit Interface 弹出窗口。

步骤 4　点击 **Passive** 显示被动接口选项。

步骤 5　或者，从 **Security Zone** 下拉列表中，选择现有安全区域或选择 **New** 以添加新的安全区域。

步骤 6　选择 **Enabled** 复选框允许被动接口监控流量。

如果清除此复选框，接口将被禁用，用户将因安全原因无法对其进行访问。

步骤 7　从 **Mode** 下拉列表中，选择一个选项指定链路模式，或选择 **Autonegotiation** 指定将接口配置为自动协商速度和双工设置。请注意，模式设置仅适用于铜接口。

注　8000 系列设备上的接口不支持半双工选项。

步骤 8　从 **MDI/MDIX** 下拉列表中，选择一个选项来指定将接口配置为 MDI（媒体依赖接口）、MDIX（媒体依赖接口的交叉）还是 Auto - MDIX。请注意，MDI/MDIX 设置仅适用于铜接口。

默认情况下， MDI/MDIX 设置为 **Auto-MDIX**，自动处理 MDI 和 MDIX 之间的交换来建立链路。

步骤 9　在 **MTU** 字段中，键入最大传输单位 (MTU)，它指定允许的最大数据包。

MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

步骤 10　点击 **Save**。

被动接口配置成功。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

了解内联 IPS 部署

许可证：保护

在内联 IPS 部署中，您可以将两个端口绑定在一起，从而在网段上透明配置 FireSIGHT 系统。这使系统可以安装在任何网络环境中，而无需配置相邻网络设备。内联接口无条件接收所有流量，但是，除非已明确丢弃，否则这些接口上接收的所有流量将在内联集外重传。

配置内联接口

许可证：保护

您可以将受管设备的一个或多个物理端口配置为内联接口。在一对内联接口处理内联部署中的流量之前，必须将这对内联接口分配给内联集。

请注意，如果您编辑接口并重新应用设备策略， Snort 重启设备上的所有接口实例，而不仅仅重启您编辑的那些实例。此外，请注意，如果您将内联对中的接口设置为不同的速度或者接口协商为不同的速度，系统将向您发出警报。

安装思科软件包时，可以将 用于 Blue Coat X-系列的思科 NGIPS接口配置为被动或内联接口。您不能使用 FireSIGHT 系统网络接口重新配置 用于 Blue Coat X-系列的思科 NGIPS接口。有关详细信息，请参阅第 5-10 页上的为 Blue Coat X 系列接口配置思科 NGIPS。

注　如果将接口配置为内联接口，网络模块中的相邻端口也自动成为内联接口来完成组对。

要在虚拟设备中配置内联接口，必须使用相邻接口创建内联对

要配置内联接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　点击要配置内联接口的设备旁的编辑图标 ( )。

系统将显示 **Interfaces** 选项卡。

步骤 3　点击要配置为内联接口的接口旁的编辑图标 ( )。

系统将显示 Edit Interface 弹出窗口。

步骤 4　点击 **Inline** 显示内联接口选项。

步骤 5　或者，从 **Security Zone** 下拉列表中，选择现有安全区域或选择 **New** 以添加新的安全区域。

步骤 6　从 **Inline Set** 下拉列表中，选择现有内联集或选择 **New** 以添加新的内联集。

请注意，如果添加了新的内联集，必须在设置内联接口之后，在 Device Management 页面 (**Devices > Device Management > Inline Sets)** 配置该内联集。有关详细信息，请参阅第 5-5 页上的添加内联集。

步骤 7　选择 **Enabled** 复选框允许内联接口处理流量。

如果清除此复选框，接口将被禁用，用户将因安全原因无法对其进行访问。

步骤 8　从 **Mode** 下拉列表中，选择一个选项指定链路模式，或选择 **Autonegotiation** 指定将接口配置为自动协商速度和双工设置。请注意，模式设置仅适用于铜接口。

注　8000 系列设备上的接口不支持半双工选项。

步骤 9　从 **MDI/MDIX** 下拉列表中，选择一个选项来指定将接口配置为 MDI（媒体依赖接口）、MDIX（媒体依赖接口的交叉）还是 Auto - MDIX。请注意，MDI/MDIX 设置仅适用于铜接口。

默认情况下， MDI/MDIX 设置为 **Auto-MDIX**，自动处理 MDI 和 MDIX 之间的交换来建立链路。

步骤 10　点击 **Save**。

内联接口配置成功。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

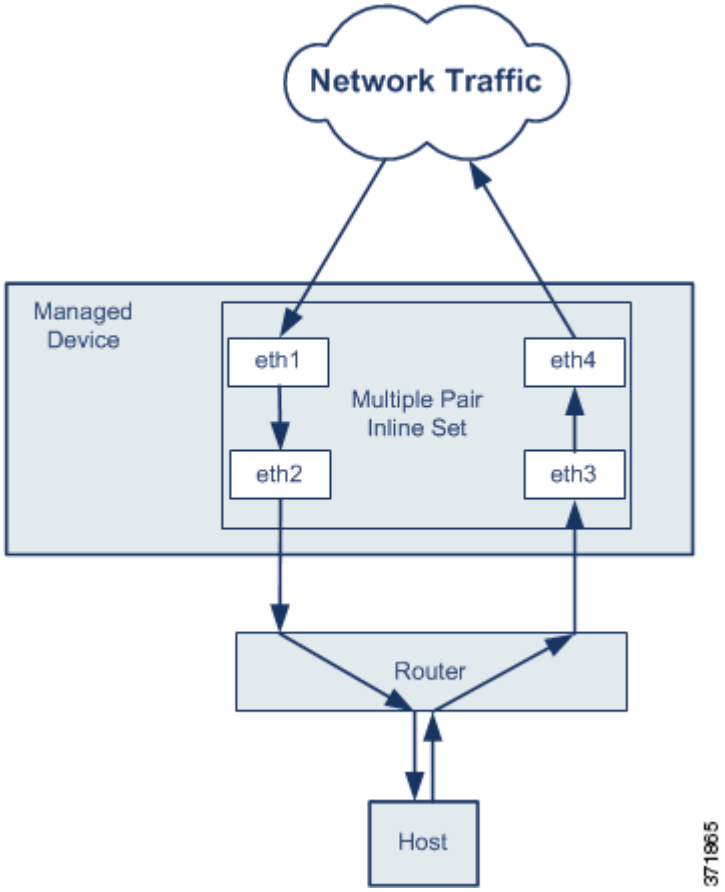
配置内联集

许可证：保护

在内嵌部署使用内联接口之前，必须配置内联集和分配内联接口对。内联集是设备上的一个或多个内联接口对的集合；一个内联接口对每次只能属于一个内联集。

您可以将受管设备上的接口配置为在您网络上的主机和外部主机之间通过不同的内联接口对路由流量，具体取决于设备流量是入站流量还是出站流量。这是*异步路由*配置。如果您部署异步路由，但一个内联集只包含一个接口对，设备可能无法正确分析网络流量，因为它可能只发现一半的流量。作为同一流量的一部分，将多个内联接口对添加到同一内联接口集允许系统识别入站和出站流量。也可以通过将接口对包括在同一安全区域中来实现此目的。

当系统从通过异步路由配置的流量生成连接事件时，事件可能识别来自同一内联接口对的入口接口和出口接口。例如，下图中的配置会生成一个连接事件，将 **eth3** 识别为入口接口，并将 **eth2** 识别为出口接口。在此配置中，这是预期行为。



注　如果将多个接口对分配到单个内联接口集，但在复制流量时遇到问题，则重新配置以帮助系统唯一地识别数据包。例如，您可以重新指定接口对以分隔内联集或修改您的安全区域。

对于有内联集的设备，在设备重新启动后，自动设置软件网桥传输数据包。如果设备正在重新启动，没有任何软件网桥在运行。如果在内联集中开启旁路模式，在设备重新启动时将变为硬件旁路模式。在这种情况下，当系统出现故障并恢复运行时，可能由于设备链路的重新协商丢失了几秒钟的数据包。但是，当 Snort 重新启动时，系统会传递流量。

注意事项　您对现有内联集的更改可能会将阻断设备的流量。更改最大传输单位 (MTU) 会中断设备的流量；一些数据包未经检测即被传输和丢弃。 MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

有关详细信息，请参阅以下各节：

查看内联集

许可证：保护

Device Management 页面的 **Inline Sets** 选项卡显示设备中配置的所有内联集的列表。请注意，您不能在虚拟设备或 用于 Blue Coat X-系列的思科 NGIPS中配置内联集进入旁路模式。内联集表视图字段表包括有关每个集的摘要信息。

表 5-1　内联集表视图字段

字段	说明
字段名称	内联集名称。
Interface Pairs	分配给内联集的所有内联接口对的列表。通过 Interfaces 选项卡禁用接口对中的任一接口时，该接口对不可用。
Bypass	配置的内联集旁路模式。

添加内联集

许可证：保护

您可以从 Device Management 页面的 **Inline Sets** 选项卡添加内联集，或者可以在配置内联接口时添加内联集。

只能将内联接口对分配给内联集。如果在受管设备上配置内联接口前要创建内联集，您可以创建一个空内联集，然后向其中添加接口。

要添加内联集，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　点击要添加内联集的设备旁的编辑图标 ( )。

系统将显示 **Interfaces** 选项卡。

步骤 3　点击 **Inline Sets**。

系统将显示 **Inline Sets** 选项卡。

步骤 4　点击 **Add Inline Set**。

系统将显示 Add Inline Set 弹出窗口。

步骤 5　在 **Name** 字段中，键入一个内联集名称。可使用字母数字字符和空格。

步骤 6　此时您有两种选择，可以将内联接口对添加到内联集中：

- 在 **Interfaces** 旁边，选择一个或多个内联接口对，然后点击添加所选的图标 ( )。使用 Ctrl 或 Shift 键选择多个内联接口对。
- 要将所有接口对添加到内联集中，请点击添加所有图标 ( )。

提示　要从内联集删除内联接口，请选择一个或多个内联接口对，并点击删除选定的图标 ( )。要从内联集删除所有接口对，请点击删除所有图标 ( )。通过 **Interfaces** 选项卡禁用接口对中的任一接口也可以删除该接口对。

步骤 7　在 **MTU** 字段中，键入最大传输单位 (MTU)，它指定允许的最大数据包。

MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

步骤 8　或者，选择 **Failsafe** 指定允许通过设备对流量进行旁路检测并继续。受管设备在内部流量缓冲区已满的情况下监控这些缓冲区和旁路检测。

请注意，只有 3 系列和 3D9900 设备支持该选项。

步骤 9　选择旁路模式，配置在接口出现故障时内联接口中的中继如何做出响应。

- 选择 **Bypass** 允许流量继续通过接口。
- 选择 **Non-Bypass** 阻断流量。

注　在旁路模式下，重新启动设备时可能会丢失一些数据包。另请注意，您不能为集群设备上的内联集、虚拟设备或 用于 Blue Coat X-系列的思科 NGIPS上的内联集、为 8000 系列设备上的非旁路网络模块，或者为 3D7115 或 3D7125 设备上的 SFP 模块配置旁路模式。

步骤 10　点击 **OK**。

内联集添加成功。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

提示　要配置内联集的高级设置（例如分路模式、链路状态传播和透明内联模式），请参阅第 5-7 页上的配置高级内联集选项。

配置高级内联集选项

许可证：保护

受支持的设备：因功能而异

在配置内联集时可以考虑使用多个选项。有关各个选项的详细信息，请参阅以下各节。

分路模式

受支持的设备：3 系列、3D9900

当您创建一个内联或带有失效开放接口集的内联时，分路模式在 3D9900 和 3 系列设备上可用。

在分路模式下，设备部署内联，但是包级流不通过设备，而是每个数据包副本发送到设备，并且网络流量不会受到干扰。由于您使用的是数据包副本而不是数据包本身，设置为丢弃的规则和使用替换关键字的规则不会影响包数据流。但是，这些类型的规则在触发时会生成入侵事件，而且入侵事件表视图显示了触发数据包会在内联部署中被丢弃。

在已部署内联的设备上使用分路模式有很多优点。例如，您可以设置设备和网络之间的布线，就像设备是内联，并分析设备生成的多种入侵事件。根据结果，您可以修改入侵策略，并添加最好地保护您的网络却不影响有效性的丢弃规则。准备部署设备内联时，您可以禁用分路模式，并开始丢弃可疑流量，而无需重新配置设备和网络之间的走线。

请注意，您不能在同一内联集中启用此选项和严格 TCP 执行选项。

传播链路状态

受支持的设备：2 系列、 3 系列

链路状态传播是旁路模式下配置的内联集的一个特性，因两对内联集都要设置跟踪状态。链路状态传播适用于铜和光纤可配置旁路接口。

在内联集的一个接口断开时，链路状态传播自动关闭内联接口对的第二个接口。当被关闭的接口恢复运行时，备用接口也自动恢复运行。换句话说，如果一个接口的链路状态更改，设备感知该更改并更新其他接口的链路状态以与其匹配。请注意，设备需要至多 4 秒传播链路状态更改。

注　触发链路状态传播时，2 系列设备（3D9900 上的除外）上配置为失效开放的光纤内联集激活硬件旁路模式。在这种情况下，相关接口卡不会自动走出旁路；您必须手动导出旁路模式。有关内联集和硬件旁路的光纤接口的详细信息，请参阅第 5-9 页上的删除配置为失效开放的光纤内联集的旁路模式。

在将路由器配置为在处于故障状态的网络设备上自动重新路由流量的弹性网络环境中，链路状态传播特别有用。

您不能在集群设备配置的内联集上禁用链路状态传播。

请注意，虚拟设备、用于 Blue Coat X-系列的思科 NGIPS和具备 FirePOWER 服务的 Cisco ASA 防火墙不支持链路状态传播。

透明内联模式

Transparent Inline Mode 选项允许设备作为“线内凸点”，这意味着不管是源地址还是目的地址，设备都将转发其看见的所有网络流量。请注意，您不能在3 系列 或 3D9900 设备上禁用此选项。

严格 TCP 执行

受支持的设备：3 系列

为最大程度地提高 TCP 的安全性，可以启用严格执行，以阻断三次握手尚未完成的连接。严格执行功能也阻止：

- 三次握手尚未完成的连接的非 SYN TCP 数据包
- TCP 连接上由发起方发出的、响应方尚未发送 SYN-ACK 数据包的非 SYN/RST 数据包
- TCP 连接上由响应方在 SYN 数据包之后、但在会话建立前发出的非 SYN-ACK/RST 数据包
- 来自发起方或响应方的已建立 TCP 连接上的 SYN 数据包

请注意， 2 系列、虚拟设备和 用于 Blue Coat X-系列的思科 NGIPS不支持此选项。此外，您不能在同一内联集中启用此选项和分路模式。

要配置高级内联集选项，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　点击要编辑内联集的设备旁的编辑图标 ( )。

系统将显示 **Interfaces** 选项卡。

步骤 3　点击 **Inline Sets**。

系统将显示 **Inline Sets** 选项卡。

步骤 4　点击要编辑的内联集旁的编辑图标 ( )。

系统将显示 Edit Inline Set 弹出窗口。

步骤 5　点击 **Advanced**。

系统将显示 **Advanced** 选项卡。

步骤 6　或者，选择 **Tap Mode** 在 3 系列和 3D9900 设备的内联接口启用分路模式。

请注意，除了 3D9900 外的虚拟设备、用于 Blue Coat X-系列的思科 NGIPS和2 系列 不支持该选项。此外，您不能在同一内联集中启用分路模式和严格的 TCP 实施。

步骤 7　或者，在 2 系列或 3 系列设备上选择 **Propagate Link State**。如果网络中的路由器能够在断开的网络设备上重新路由流量，此选项将特别有用。

您不能在集群设备配置的内联集上禁用链路状态传播。

请注意，虚拟设备和 用于 Blue Coat X-系列的思科 NGIPS不支持此选项。

步骤 8　或者，选择 **Strict TCP Enforcement** 在 3 系列设备上启用严格的 TCP 实施。

请注意， 2 系列、虚拟设备和 用于 Blue Coat X-系列的思科 NGIPS不支持此选项。此外，您不能在同一内联集中启用严格的 TCP 实施和分路模式。

步骤 9　或者，选择 **Transparent Inline Mode**。

请注意，您不能在 3 系列或 3D9900 设备上禁用此选项。

步骤 10　点击 **OK**。

已保存您的更改。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

删除配置为失效开放的光纤内联集的旁路模式

许可证：保护

受支持的设备：2 系列（除了 3D9900）

在将光纤内联集配置为失效开放的 2 系列设备上启用链路状态传播并且设备进入旁路模式时，所有网络流量通过内联集，无需进行分析。当链路恢复，配置为失效开放的大多数光纤内联集不会从旁路自动返回。您可以使用命令行工具强制内联集退出旁路模式。

此工具在将光纤内联接口配置为失效开放的内联集中工作。在将铜内联接口设置为失效开放的内联集上，不必使用该工具。

注　如果您对设备上配置为失效开放的内联集有任何问题，请联系支持人员。

要强制将设备上配置为失效开放的光纤内联集退出旁路模式，请执行以下操作：

访问：管理员/网络管理员

步骤 1　打开设备的终端窗口，并作为管理员用户登录。

步骤 2　在命令行输入以下内容：

```
sudo /var/sf/bin/unbypass_cards.sh
```

系统提示您输入密码。

步骤 3　当接口退出旁路模式，系统日志中的一则消息指示设备正在分析流量。例如：

```
光纤对已被 un_bypass 重置
```

删除内联集

许可证：保护

删除一个内联集时，分配给该集的任何内联接口都可包含在另一个集合中。接口没有删除。

要删除内联集，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　点击要删除内联集的设备旁的编辑图标 ( )。

系统将显示 **Interfaces** 选项卡。

步骤 3　点击 **Inline Sets**。

系统将显示 **Inline Sets** 选项卡。

步骤 4　点击要删除的内联集旁的编辑图标 ( )。

步骤 5　出现提示时，确认您要删除内联集。

内联集删除成功。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

为 Blue Coat X 系列接口配置思科 NGIPS

许可证：保护

受支持的设备：X -系列

在部署 用于 Blue Coat X-系列的思科 NGIPS软件包时或在软件包安装之后，您可以创建被动或内联接口。当您将 用于 Blue Coat X-系列的思科 NGIPS添加到防御中心时，这些接口都已配置。用于 Blue Coat X-系列的思科 NGIPS不支持高级配置选项。

您不能使用 FireSIGHT 系统网络接口重新配置 用于 Blue Coat X-系列的思科 NGIPS接口。要重新配置，您必须首先从防御中心删除当前的接口，然后创建新接口。有关创建和删除接口的详细信息，请参阅《*用于 Blue Coat X-系列的思科 NGIPS 安装指南*》。

要在 用于 Blue Coat X-系列的思科 NGIPS上配置接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　点击要配置的设备旁的编辑图标 ( )。

系统将显示 **Interfaces** 选项卡。请注意，链路在所有 用于 Blue Coat X-系列的思科 NGIPS接口始终显示为活动状态 ( )。

步骤 3　点击要配置的接口旁的编辑图标 ( )。

步骤 4　从 **Security Zone** 下拉列表中，选择现有安全区域或选择 **New** 以添加新的安全区域。

步骤 5　或者，对于内联接口，从 **Inline Set** 下拉列表中选择现有内联集，或者选择 **New** 添加新的内联集。

请注意，如果添加了新的内联集，必须在设置内联接口之后，在 Device Management 页面 (**Devices > Device Management > Inline Sets)** 配置该内联集。有关详细信息，请参阅第 5-5 页上的添加内联集。

步骤 6　点击 **Save**。

接口配置成功。请注意，直到通过点击菜单栏右上角的 **Apply Changes** 应用设备配置之后，您的更改才能生效。

设置虚拟交换机

可以在第二层部署配置受管设备，使它在两个或多个网络之间提供数据包交换。在第二层部署，可以在受管设备上将虚拟交换机配置为独立运行的广播域，将网络划分为多个逻辑分段。虚拟交换机根据主机的媒体访问控制 (MAC) 地址来确定在哪里发送数据包。

当配置虚拟交换机时，交换机起初会通过交换机的每个可用端口来广播数据包。随着时间的推移，交换机使用标记的回传流量了解哪些主机驻留在连接到每个端口的网络上。

虚拟交换机必须包含两个或多个交换接口来处理流量。对于每个虚拟交换机，配置作为交换接口的组端口的流量受到限制。例如，如果用四个交换接口配置虚拟交换机，通过某个广播端口发送的数据包只能通过交换机的其余三个端口转发出去。

配置物理交换接口时，必须将它分配到虚拟交换机。还可以根据需要在物理端口定义其他逻辑交换接口。在 3 系列受管设备上，可将多个物理接口组合到一个称为链路聚合组 (LAG) 的逻辑交换接口中。此单个聚合逻辑链路在两个端点之间提供更高的带宽、冗余和负载均衡。

注意事项 如果第二层部署因任何原因而失效，设备将不再传递流量。

有关配置第二层部署的详细信息，请参阅以下各节：

- 第 6-1 页上的配置交换接口
- 第 6-4 页上的配置虚拟交换机
- 第 8-1 页上的配置 LAG

配置交换接口

许可证：可控性

受支持的设备：3 系列

可以将交换接口设置成物理或逻辑配置。可以配置用于处理未标记 VLAN 流量的物理交换接口。还可以创建用于处理含指定 VLAN 标记的流量的逻辑交换接口。

在第二层部署，系统将删除在没有交换接口为其等待的外部物理接口上收到的所有流量。如果系统接收到没有 VLAN 标记的数据包且您没有为该端口配置物理交换接口，系统会删除该数据包。如果系统收到带有 VLAN 标记的数据包且您未配置逻辑交换接口，系统也会删除数据包。

系统在交换接口处理所接收的带有 VLAN 标记的流量，去除入口处最外层的 VLAN 标记，然后做出任何规则评估或转发决策。通过 VLAN 标记的逻辑交换接口离开设备的数据包将通过出口相关的 VLAN 标记封装。

请注意，如果将父物理接口更改为内联或被动接口，系统将删除所有关联的逻辑接口。

有关详细信息，请参阅以下各节：

配置物理交换接口

许可证：可控性

受支持的设备：3 系列

可以在受管设备上配置一个或多个物理端口作为交换接口。必须将物理交换接口分配到虚拟交换机，物理接口才可以处理流量。

注意事项　更改最大传输单位 (MTU) 会中断设备上的流量并造成丢包。 MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

要配置物理交换接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在需要配置交换接口的设备旁，点击编辑图标 ( )。

系统将显示 Interfaces 选项卡。

步骤 3　在需要配置为交换接口的接口旁边，点击编辑图标 ( )。

系统将显示 Edit Interface 弹出窗口。

步骤 4　点击 **Switched** 显示交换接口选项。

步骤 5　或者，从 **Security Zone** 下拉列表中，选择现有安全区域或选择 **New** 以添加新的安全区域。

步骤 6　或者，从 **Virtual Switch** 下拉列表中，选择现有虚拟交换机或选择 **New** 来添加新的虚拟交换机。

请注意，如果添加新的虚拟交换机，则在设置交换接口之后，必须在 Device Management 页面的 Virtual Switches 选项卡 (**Devices > Device Management> Virtual Switches**) 中对其进行设置。请参阅第 6-5 页上的添加虚拟交换机。

步骤 7　选择 **Enabled** 复选框，允许交换接口处理流量。

如果清除此复选框，接口将被禁用，用户将因安全原因无法对其进行访问。

步骤 8　从 **Mode** 下拉列表中，选择一个选项来指定链路模式或选择 **Autonegotiation** 来指定将该接口配置为自动协商速度和双工设置。请注意，模式设置仅适用于铜接口。

注　8000 系列设备上的接口不支持半双工选项。

步骤 9　从 **MDI/MDIX** 下拉列表中，选择一个选项来指定将接口配置为 MDI（媒体依赖接口）、MDIX（媒体依赖接口的交叉）还是 Auto - MDIX。请注意，MDI/MDIX 设置仅适用于铜接口。

默认情况下， MDI/MDIX 设置为 Auto-MDIX，自动处理 MDI 和 MDIX 之间的交换来建立链路。

步骤 10　在 **MTU** 字段中，键入最大传输单位 (MTU)，它指定允许的最大数据包。

MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

步骤 11　点击 **Save**。

物理交换接口配置成功。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

添加逻辑交换接口

许可证：可控性

受支持的设备：3 系列

对于每个物理交换接口，可以添加多个逻辑交换接口。必须将每个逻辑接口与 VLAN 标记关联，以处理物理接口接收的带有该特定标记的流量。必须指定一个逻辑交换接口作为虚拟交换机来处理流量。

注意事项　对最大传输单位 (MTU) 做出的任何更改均会中断设备的交换流量并造成丢包。

要编辑现有逻辑交换接口，请点击接口旁的编辑图标 ( )。

要添加逻辑交换接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在需要添加交换接口的设备旁，点击编辑图标 ( )。

系统将显示 Interfaces 选项卡。

步骤 3　点击 **Add Interface**。

系统将显示 Add Interface 弹出窗口。

步骤 4　点击 **Switched** 显示交换接口选项。

步骤 5　从 **Interface** 下拉列表中，选择要接收 VLAN 标记的流量的物理接口。

步骤 6　在 **VLAN Tag** 字段中，键入将分配到此接口上的入站和出站流量的标记值。该值可以是 1 到 4094 之间的任意一个整数。

步骤 7　或者，从 **Security Zone** 下拉列表中，选择现有安全区域或选择 **New** 以添加新的安全区域。

步骤 8　或者，从 Virtual Switch 下拉列表中，选择现有虚拟交换机或选择 **New** 来添加新的虚拟交换机。

请注意，如果添加新的虚拟交换机，则在设置交换接口之后，必须在 Device Management 页面 (**Devices > Device Management> Virtual Switches**) 中对其进行设置。请参阅第 6-5 页上的添加虚拟交换机。

步骤 9　选择 **Enabled** 复选框，允许交换接口处理流量。

如清除此复选框，则将禁用并强制性断开该接口。如果禁用物理接口，则会同时禁用与其相关的所有逻辑接口。

步骤 10　在 **MTU** 字段中，键入最大传输单位 (MTU)，它指定允许的最大数据包。

MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

步骤 11　点击 **Save**。

逻辑交换接口添加成功。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

注　当物理接口被禁用时，与该物理接口关联的逻辑接口也被禁用。

删除逻辑交换接口

许可证：可控性

受支持的设备：3 系列

当删除逻辑交换接口时，会从其所在的物理接口将其删除，同时会还会删除与之相关的虚拟交换机和安全区域。

要删除交换接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　选择要删除的包含交换接口的设备，并点击设备的编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　在要删除的逻辑交换接口旁，点击删除图标 ( )。

步骤 4　出现提示时，请确认要删除接口。

接口删除成功。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

配置虚拟交换机

许可证：可控性

受支持的设备：3 系列

您必须先配置虚拟交换机并为其分配交换接口，然后才能在第二层部署中使用交换接口。虚拟交换机是通过网络处理入站和出站流量的一组交换接口。

有关配置虚拟交换机的详细信息，请参阅以下各节：

- 第 6-5 页上的查看虚拟交换机
- 第 6-5 页上的添加虚拟交换机

查看虚拟交换机

许可证：可控性

受支持的设备：3 系列

Device Management 页面的 Virtual Switches 选项卡显示在设备上配置的所有虚拟交换机的列表。该页面包括每个交换机的汇总信息，如下表所述。

表 6-1　　虚拟交换机表视图字段

字段	说明
字段名称	虚拟交换机的名称。
接口	已分配到虚拟交换机的所有交换接口。已从 Interfaces 选项卡禁用的接口将不可用。
Hybrid Interface	将虚拟交换机关联到虚拟路由器的可选择配置的混合接口。
Unicast Packets	虚拟交换机的单播数据包统计信息，包括： • 接收的单播数据包 • 转发的单播数据包 （不包括主机丢包） • 无意间丢弃的单播数据包
Broadcast Packets	虚拟交换机的广播数据包统计信息，包括： • 接收的广播数据包 • 转发的广播数据包 • 无意间丢弃的广播数据包

添加虚拟交换机

许可证：可控性

受支持的设备：3 系列

可以从 Device Management 页面的 Virtual Switches 选项卡添加虚拟交换机。在配置交换接口时也可以添加交换机。

只能将交换接口分配到虚拟交换机。如果要在受管设备配置交换接口之前创建虚拟交换机，可以创建空的虚拟交换机并稍后为之添加接口。

提示　要编辑现有虚拟交换机，请点击交换机旁的编辑图标 ( )。

请注意，对现有虚拟交换机作出的更改可能会阻断设备的流量。

要添加虚拟交换机，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在需要添加虚拟交换机的设备旁，点击编辑图标 ( )。

系统将显示 Interfaces 选项卡。

步骤 3　点击 **Virtual Switches**。

系统将显示 Virtual Switches 选项卡。

步骤 4　点击 **Add Virtual Switch**。

系统将显示 Add Virtual Switch 弹出窗口。

步骤 5　在 **Name** 字段中键入交换机名称。可使用字母数字字符和空格。

步骤 6　在 **Available** 下，选择一个或多个要添加到虚拟交换机的交换接口。

提示　已从 Interfaces 选项卡中禁用的接口将不可用；添加接口后禁用接口会从配置中删除该接口。

步骤 7　点击 **Add**。

步骤 8　或者，从 **Hybrid Interface** 下拉列表中，选择将虚拟交换机联接到虚拟路由器的混合接口。有关详细信息，请参阅第 9-1 页上的设置混合接口。

步骤 9　点击 **Save**。

虚拟交换机添加成功。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

提示　要配置交换机的高级设置，例如静态 MAC 条目和生成树协议，请参阅第 6-6 页上的配置高级虚拟交换机设置。

配置高级虚拟交换机设置

许可证：可控性

受支持的设备：3 系列

添加或编辑虚拟交换机时，可以添加静态 MAC 条目，启用生成树协议 (STP)，删除桥接协议数据单元 (BPDU)，以及启用严格 TCP 执行。

随着时间的推移，虚拟交换机通过标记来自网络的回传流量来了解 MAC 地址。或者，可以手动添加静态 MAC 条目，指定驻留在特定端口的 MAC 地址。不管是否收到来自该端口的流量，MAC 地址在表中将保持静态。可以为每个虚拟交换机指定一个或多个静态 MAC 地址。

STP 是一种用来防止网络环路的网络协议。 BPDU 通过网络进行交换，并传输有关网络桥接的信息。如果网络中存在重复的链路，该协议将使用 BPDU 识别并选择最快的网络链路。如果网络链路发生故障，生成树会切换到现有的备用链路。

如果虚拟交换机在 VLAN 之间路由，类似于单臂路由， BPDU 将通过不同的逻辑交换接口进出设备，但是在同一个物理交换接口。因此， STP 确认设备为冗余网络环路，可在特定第二层部署产生问题。为了防止这种情况出现，可在域级别配置虚拟交换机，让设备在监控流量时删除 BPDU。

注　思科强烈建议在配置计划于设备集群中部署的虚拟交换机时启用 STP。

为最大程度地提高 TCP 的安全性，可以启用严格执行，以阻断三次握手尚未完成的连接。严格执行功能也阻止：

- 三次握手尚未完成的连接的非 SYN TCP 数据包
- TCP 连接上由发起方发出的、响应方尚未发送 SYN-ACK 数据包的非 SYN/RST 数据包
- TCP 连接上由响应方在 SYN 数据包之后、但在会话建立前发出的非 SYN-ACK/RST 数据包
- 来自发起方或响应方的已建立 TCP 连接上的 SYN 数据包

请注意，如果将虚拟交换机与逻辑混合接口关联，交换机使用与该逻辑混合接口关联的虚拟路由器相同的严格 TCP 执行设置。在这种情况下，不能在交换机上的指定严格 TCP 执行。

要配置高级虚拟交换机设置，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要编辑的包含虚拟交换机的设备旁，点击编辑图标 ( )。

系统将显示 Interfaces 选项卡。

步骤 3　点击 **Virtual Switches**。

系统将显示 Virtual Switches 选项卡。

步骤 4　在要编辑的虚拟交换机旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Switch 弹出窗口。

步骤 5　点击 **Advanced**。

系统将显示 Advanced 选项卡。

步骤 6　要添加静态 MAC 条目，请点击 **Add**。

系统将显示 Add Static MAC Address 弹出窗口。

步骤 7　在 **MAC Address** 字段中，使用两个十六进制数字为一组的六组数位，采用冒号分隔的标准格式键入地址（例如，01:23:45:67:89:AB）。

注　广播地址（00:00:00:00:00:00 和 FF:FF:FF:FF:FF:FF）不能作为静态 MAC 地址来添加。

步骤 8　从 **Interface** 下拉列表中，选择要分配 MAC 地址的接口。

步骤 9　点击 **Add**。

MAC 地址被添加到 Static MAC Entries 表格。

要编辑 MAC 地址，请点击编辑图标 ( )。要删除 MAC 地址，请点击删除图标 ( )。

步骤 10　或者，要启用生成树协议，请选择 **Enable Spanning Tree Protocol**。只有当虚拟交换机在多个网络接口之间传输流量时，才选择 **Enable Spanning Tree Protocol**。

无法选择 **Drop BPDUs**，除非清除**Enable Spanning Tree Protocol**。

步骤 11　或者，选择 **Strict TCP Enforcement** 来启用严格 TCP 执行。

如果将虚拟交换机与逻辑混合接口关联，则不会显示此选项，并且交换机使用与该逻辑混合接口关联的虚拟路由器相同的设置。

步骤 12　或者，选择 **Drop BPDUs**以在域级别删除 BPDU。只有当虚拟交换机通过单个物理接口在各个 VLAN 之间传输流量，才能选择 **Drop BPDUs**。

无法选择 **Enable Spanning Tree Protocol**，除非清除 **Drop BPDUs**。

步骤 13　点击 **Save**。

已保存您的更改。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

删除虚拟交换机

许可证：可控性

受支持的设备：3 系列

删除虚拟交换机时，所有分配给交换机的交换接口可以纳入另一台交换机中。

要删除虚拟交换机，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　选择要删除的包含虚拟交换机的受管设备，然后点击设备的编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Switches**。

系统将显示 Virtual Switches 选项卡。

步骤 4　在要删除的虚拟交换机旁，点击删除图标 ( )。

步骤 5　出现提示时，请确认要删除虚拟交换机。

虚拟交换机删除成功。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

设置虚拟路由器

可在第 3 层部署中配置受管设备，使其在两个或多个接口之间路由流量。必须为每个接口分配一个 IP 地址，并将这些接口分配给虚拟路由器以路由流量。在 3 系列受管设备上，可将多个物理接口分组到单个逻辑路由接口中，这称为链路聚合组 (LAG)。此单个聚合逻辑链路在两个端点之间提供更高的带宽、冗余和负载均衡。

可对系统进行配置，使其根据目标地址做出数据包转发决策，从而对数据包进行路由。配置为路由接口的接口将接收和转发第 3 层流量。路由器根据转发条件从输出接口获取目标，访问控制规则指定要应用的安全策略。

在第 3 层部署中，可定义静态路由。此外，还可以配置路由信息协议 (RIP) 和开放式最短路径优先 (OSPF) 动态路由协议。还可以配置静态路由与 RIP 或静态路由与 OSPF 的组合。

注意事项 如果第 3 层部署出于任何原因失效，则设备将不再传递流量。

有关配置第 3 层部署的详细信息，请参阅以下各节。

- 第 7-1 页上的配置路由接口
- 第 7-7 页上的配置虚拟路由器
- 第 8-1 页上的配置 LAG

配置路由接口

许可证：可控性

受支持的设备：3 系列

可使用物理或逻辑配置设置路由接口。可以配置物理路由接口，以处理未标记的 VLAN 流量。还可创建逻辑路由接口，以处理带有指定 VLAN 标记的流量。

在第 3 层部署中，如果外部物理接口上收到的流量没有等待它的路由接口，系统会将其这些流量全部丢弃。如果系统收到的数据包没有 VLAN 标记，且尚未给该端口配置物理路由接口，系统将丢弃该数据包。如果系统收到带 VLAN 标记的数据包，但尚未配置逻辑路由接口，则系统也将丢弃该数据包。

在处理交换接口上收到的带 VLAN 标记的流量时，系统会首先在入口处剥离最外层的 VLAN 标记，然后再进行任何规则评估或做出转发决策。当数据包通过带 VLAN 标记的逻辑路由接口离开设备时，系统会在出口处使用关联的 VLAN 标记对该数据包进行封装。剥离过程结束后，系统将丢弃接收到的所有带 VLAN 标记的任何流量。

请注意，如果将父物理接口更改为内联或被动接口，系统将删除所有关联的逻辑接口。

有关详细信息，请参阅以下各节：

配置物理路由接口

许可证：可控性

受支持的设备：3 系列

可将受管设备上的一个或多个物理端口配置为路由接口。必须先向虚拟路由器分配物理路由接口，然后它才能路由流量。

可向路由接口添加静态地址解析协议 (ARP) 条目。当外部主机要将流量发送到本地网络上的目标 IP 地址时，如果其需要知道该目标 IP 地址的 MAC 地址，它将发送 ARP 请求。配置静态 ARP 条目时，虚拟路由器会使用 IP 地址和关联的 MAC 地址做出响应。

请注意，针对路由接口禁用 **ICMP Enable Responses** 选项并不在所有情形下均阻止 ICMP 响应。可向访问控制策略添加规则，以丢弃目标 IP 为路由接口 IP 且协议为 ICMP 的数据包；请参阅第 15-1 页上的使用基于网络的规则控制流量。

如您在受管设备上启用 **Inspect Local Router Traffic** 选项，则该设备在数据包到达主机之前将其丢弃，从而阻止所有响应。有关检查本地路由器流量的详细信息，请参阅第 4-47 页上的了解高级设备设置。

注意事项　更改最大传输单位 (MTU) 会中断设备上的流量并造成丢包。 MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

要配置物理路由接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要为其配置路由接口的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　在要将其配置为路由接口的接口旁，点击编辑图标 ( )。

系统将显示 Edit Interface 弹出窗口。

步骤 4　点击 **Routed** 以显示路由接口选项。

步骤 5　或者，从 **Security Zone** 下拉列表中，选择现有安全区域或选择 **New** 以添加新的安全区域。

步骤 6　或者，从 **Virtual Router** 下拉列表中，选择现有虚拟路由器或选择 **New** 以添加新的虚拟路由器。

请注意，如果添加新的虚拟路由器，在完成路由接口设置后，必须在 Device Management 页面的 Virtual Routers 选项卡 **(Devices > Device Management > Virtual Routers)** 上配置该虚拟路由器。请参阅第 7-8 页上的添加虚拟路由器。

步骤 7　选择 **Enabled** 复选框，以使路由接口处理流量。

如果清除此复选框，接口将被禁用，用户将因安全原因无法对其进行访问。

步骤 8　从 **Mode** 下拉列表中，选择一个选项来指定链路模式或选择 **Autonegotiation** 来指定将该接口配置为自动协商速度和双工设置。请注意，模式设置仅适用于铜接口。

注　8000 系列设备上的接口不支持半双工选项。

步骤 9　从 **MDI/MDIX** 下拉列表中，选择一个选项来指定将接口配置为 MDI（媒体依赖接口）、MDIX（媒体依赖接口的交叉）还是 Auto - MDIX。请注意，MDI/MDIX 设置仅适用于铜接口。

通常，MDI/MDIX 会设置为 Auto-MDIX，此选项可自动处理 MDI 与 MDIX 之间的切换以获得链路。

步骤 10　在 **MTU** 字段中，键入最大传输单位 (MTU)，它指定允许的最大数据包。请注意， MTU 是第 2 层 MTU/MRU，而非第 3 层 MTU。

MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

步骤 11　在 **ICMP** 旁，选择 **Enable Responses** 复选框，以使接口对 ICMP 流量（例如 ping 和 traceroute）做出响应。

步骤 12　在 **IPv6 NDP** 旁，选择 **Enable Router Advertisement** 复选框，以使接口广播路由器通告。

步骤 13　要添加 IP 地址，请点击 **Add**。

系统将显示 Add IP Address 弹出窗口。

步骤 14　在 **Address** 字段中，使用 CIDR 表示法输入路由接口的 IP 地址和子网掩码。请注意：

- 不能添加网络和广播地址，或静态 MAC 地址 00:00:00:00:00:00 和 FF:FF:FF:FF:FF:FF。
- 无论子网掩码如何，均不能将多个相同的 IP 地址添加至虚拟路由器的接口。

步骤 15　或者，如果贵组织使用 IPv6 地址，请在 **IPv6** 字段旁，选择 **Address Autoconfiguration** 复选框，以自动设置接口的 IP 地址。

步骤 16　对于 **Type**，选择 Normal 或 SFRP。

有关 SFRP 选项，请参阅第 7-6 页上的配置 SFRP以了解详细信息。

步骤 17　点击 **OK**。

IP 地址添加成功。

要编辑 IP 地址，请点击编辑图标 ( )。要删除 IP 地址，请点击删除图标 ( )。

注　在为集群设备的路由接口添加 IP 地址时，必须向对等集群的路由接口添加相应的 IP 地址。

步骤 18　要添加静态 ARP 条目，请点击 **Add**。

系统将显示 Add Static ARP Entry 弹出窗口。

步骤 19　在 **IP Address** 字段中，键入静态 ARP 条目的 IP 地址。

步骤 20　在 **MAC Address** 字段中，键入与该 IP 地址关联的 MAC 地址。使用标准格式（即用冒号隔开的六组两位十六进制数字）输入地址（例如，01:23:45:67:89:AB）。

步骤 21　点击 **OK**。

静态 ARP 条目添加成功。

提示　要编辑静态 ARP 条目，请点击编辑图标 ( )。要删除静态 ARP 条目，请点击删除图标 ( )。

步骤 22　点击 **Save**。

物理路由接口配置成功。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

添加逻辑路由接口

许可证：可控性

受支持的设备：3 系列

对于每个物理路由接口，可添加多个逻辑路由接口。必须将每个逻辑接口与 VLAN 标记关联，以处理物理接口接收的带有该特定标记的流量。必须向虚拟路由器分配逻辑路由接口以路由流量。

请注意，针对路由接口禁用 **ICMP Enable Responses** 选项并不在所有情形下均阻止 ICMP 响应。可向访问控制策略添加规则，以丢弃目标 IP 为路由接口 IP 且协议为 ICMP 的数据包；请参阅第 15-1 页上的使用基于网络的规则控制流量。

如您在受管设备上启用 **Inspect Local Router Traffic** 选项，则该设备在数据包到达主机之前将其丢弃，从而阻止所有响应。有关检查本地路由器流量的详细信息，请参阅第 4-47 页上的了解高级设备设置。

注意事项　更改最大传输单位 (MTU) 会中断设备上的流量并造成丢包。 MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

要编辑现有路由接口，请点击接口旁的编辑图标 ( )。

要添加逻辑路由接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加路由接口的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Add Interface**。

系统将显示 Add Interface 弹出窗口。

步骤 4　点击 **Routed** 以显示路由接口选项。

步骤 5　从 **Interface**下拉列表中，选择要向其添加逻辑接口的物理接口。

步骤 6　在 **VLAN Tag** 字段中，键入将分配到此接口上的入站和出站流量的标记值。该值可以是 1 到 4094 之间的任意一个整数。

步骤 7　或者，从 **Security Zone** 下拉列表中，选择现有安全区域或选择 **New** 以添加新的安全区域。

步骤 8　或者，从 **Virtual Router** 下拉列表中，选择现有虚拟路由器或选择 **New** 以添加新的虚拟路由器。

请注意，如果添加新的虚拟路由器，在完成路由接口设置之后，必须在 Device Management 页面 **(Devices > Device Management> Virtual Routers)** 上配置该虚拟路由器。请参阅第 7-8 页上的添加虚拟路由器。

步骤 9　选择 **Enabled** 复选框，以使路由接口处理流量。

如清除此复选框，则将禁用并强制性断开该接口。如果禁用物理接口，则会同时禁用与其相关的所有逻辑接口。

步骤 10　在 **MTU** 字段中，键入最大传输单位 (MTU)，它指定允许的最大数据包。请注意， MTU 是第 2 层 MTU/MRU，而非第 3 层 MTU。

MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

步骤 11　在 **ICMP** 旁，选择 **Enable Responses** 复选框以将更新或错误消息发送给其他路由器、中间设备或主机。

步骤 12　在 **IPv6 NDP** 旁，选择 **Enable Router Advertisement** 复选框，以使接口广播路由器通告。

步骤 13　要添加 IP 地址，请点击 **Add**。

系统将显示 Add IP Address 弹出窗口。

步骤 14　在 **Address** 字段中，使用 CIDR 表示法键入 IP 地址。请注意：

- 不能添加网络和广播地址，或静态 MAC 地址 00:00:00:00:00:00 和 FF:FF:FF:FF:FF:FF。
- 无论子网掩码如何，均不能将多个相同的 IP 地址添加至虚拟路由器的接口。

步骤 15　或者，如果贵组织使用 IPv6 地址，请在 **IPv6** 字段旁，选择 **Address Autoconfiguration** 复选框，以自动设置接口的 IP 地址。

步骤 16　对于 **Type**，选择 Normal 或 SFRP。

有关 SFRP 选项，请参阅第 7-6 页上的配置 SFRP 以了解详细信息。

步骤 17　点击 **OK**。

IP 地址添加成功。

要编辑 IP 地址，请点击编辑图标 ( )。要删除 IP 地址，请点击删除图标 ( )。

注　向集群设备的路由接口添加 IP 地址时，必须向对等集群的路由接口添加相应的 IP 地址。

步骤 18　要添加静态 ARP 条目，请点击 **Add**。

系统将显示 Add Static ARP Entry 弹出窗口。

步骤 19　在 **IP Address** 字段中，键入静态 ARP 条目的 IP 地址。

步骤 20　在 **MAC Address** 字段中，键入与该 IP 地址关联的 MAC 地址。使用标准格式 （即用冒号隔开的六组两位十六进制数字）输入地址 （例如， 01:23:45:67:89:AB）。

步骤 21　点击 **OK**。

静态 ARP 条目添加成功。

提示　要编辑静态 ARP 条目，请点击编辑图标 ( )。要删除静态 ARP 条目，请点击删除图标 ( )。

步骤 22　点击 **Save**。

逻辑路由接口添加成功。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

注　当物理接口被禁用时，与该物理接口关联的逻辑接口也被禁用。

删除逻辑路由接口

许可证：可控性

受支持的设备：3 系列

删除逻辑路由接口时，会将它从其所驻留的物理接口删除，并会删除分配给它的的虚拟路由器和安全区域。

要删除路由接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要删除路由接口的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　在要删除的逻辑路由接口旁，点击删除图标 ( )。

步骤 4　出现提示时，请确认要删除接口。

接口删除成功。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

配置 SFRP

许可证：可控性

受支持的设备：3 系列

可配置思科冗余协议 (SFRP) 以实现网络冗余，从而提高设备集群或单个设备上的可用性。 SFRP 可为 IPv4 和 IPv6 地址提供网关冗余。您可在路由接口和混合接口上配置 SFRP。

在单一设备配置的各个接口必须位于相同的广播域中。您必须将至少一个此类接口指定为主用接口，并指定相同数量的备用接口。对于每个 IP 地址，系统仅支持一个主用接口和一个备用接口。如果网络连接断开，系统会自动将备用接口升级为主用接口，以保持连接的稳定性。

对于一组 SFRP 接口中的所有接口，为 SFRP 设置的选项必须相同。一个接口组中的多个 IP 地址必须处于相同的主/备状态。因此，添加或编辑 IP 地址时，为该地址设置的状态将传播至其所在组的所有地址。出于安全考虑，必须输入相应组内所有接口所共享的 **Group ID** 和 **Shared Secret** 的值。

为了在虚拟路由器上启用 SFRP IP 地址，还必须至少配置一个非 SFRP IP 地址。

对于集群设备，请指定共享密钥，系统会将其和 SFRP IP 配置一起复制至对等集群。共享密钥用于验证对等数据。

有关集群设备的详细信息，请参阅第 4-25 页上的集群设备。

要配置 SFRP，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要为其配置 SFRP 的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　在要为其配置 SFRP 的接口旁，点击编辑图标 ( )。

系统将显示 Edit Interface 弹出窗口。

步骤 4　选择要为其配置 SFRP 接口类型。

- 点击 **Routed** 以显示路由接口选项。
- 点击 **Hybrid**，系统将显示混合接口选项。

步骤 5　可在添加或编辑 IP 地址时配置 SFRP：

- 要添加 IP 地址，请点击 **Add**。
- 要编辑 IP 地址，请点击编辑图标 ( )。

系统将显示 Add IP Address 或 Edit IP Address 窗口。

步骤 6　对于 **Type**，请选择 **SFRP** 以显示 SFRP 选项。

步骤 7　在 **Group ID** 字段中，输入为 SFRP 配置的一组主用接口或备用接口的值。

步骤 8　对于 **Priority**，请选择 **Master** 或 **Backup** 以指定首选接口。

- 对于单台设备，必须在一台设备上将某一接口设置为主用接口，在另一设备上将另一接口设置为备用接口。
- 对于设备集群，在将某一接口设置为主用接口时，另一接口会自动成为备用接口。

步骤 9　在 **Shared Secret** 字段中，输入共享密钥。

对于设备集群中的群组， Shared Secret 字段会自动填充。

步骤 10　在 **Adv.Interval (seconds)** 字段中，输入第 3 层流量的路由通告间隔。

步骤 11　点击 **OK**。

IP 地址添加或编辑成功。

步骤 12　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

配置虚拟路由器

许可证：可控性

受支持的设备：3 系列

要在第 3 层部署中使用路由接口，必须首先配置虚拟路由器并向它们分配路由接口。虚拟路由器是可路由第 3 层流量的一组路由接口。

有关配置虚拟路由器的详细信息，请参阅以下各节。

查看虚拟路由器

许可证：可控性

受支持的设备：3 系列

Device Management 页面的 Virtual Routers 选项卡 **(Devices > Device Management > Virtual Routers)** 会显示已在设备上配置的所有虚拟路由器的列表。该表包含每个路由器的摘要信息，如下表所示。

表 7-1　虚拟路由器表视图字段

字段	说明
字段名称	虚拟路由器名称
接口	已分配至虚拟路由器的所有路由接口的列表。在 Interfaces 选项卡上禁用某一接口会将其移除。
协议	虚拟路由器当前使用的协议，具体为下列之一 • 静态 • 静态、 RIP • 静态、 OSPF

添加虚拟路由器

许可证：可控性

受支持的设备：3 系列

可从 Device Management 页面的 Virtual Routers 选项卡中添加虚拟路由器。也可在配置路由接口时添加路由器。

可仅将路由接口和混合接口分配至虚拟路由器。如要先创建虚拟路由器，然后再在受管设备上配置接口，则可在创建一个空虚拟路由器之后再向其添加接口。

为最大程度地提高 TCP 的安全性，可以启用严格执行，以阻断三次握手尚未完成的连接。严格执行功能也阻止：

- 三次握手尚未完成的连接的非 SYN TCP 数据包
- TCP 连接上由发起方发出的、响应方尚未发送 SYN-ACK 数据包的非 SYN/RST 数据包
- TCP 连接上由响应方在 SYN 数据包之后、但在会话建立前发出的非 SYN-ACK/RST 数据包
- 来自发起方或响应方的已建立 TCP 连接上的 SYN 数据包

请注意，如将第 3 层接口的配置更改为非第 3 层接口或从虚拟路由器上移除某一第 3 层接口，路由器可能会陷入无效状态。例如，如将它用于 DHCPv6 中，可能会导致上行和下行不匹配。对现有虚拟路由器做出的任何更改均可能导致设备上的流量中断。

提示　要编辑现有虚拟路由器，请点击路由器旁的编辑图标 ( )。

除了常规方法，还可用多种方式配置虚拟路由器。有关这些配置的详细信息，请参阅以下各节。

- 第 7-10 页上的设置 DHCP 中继
- 第 7-11 页上的设置静态路由
- 第 7-13 页上的设置动态路由

- 第 7-14 页上的设置 RIP 配置
- 第 7-19 页上的设置 OSPF 配置
- 第 7-26 页上的设置虚拟路由器过滤条件
- 第 7-28 页上的添加虚拟路由器身份验证配置文件

要添加虚拟路由器，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加虚拟路由器的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

提示　如果设备采用了集群式堆栈部署，请从 **Selected Device** 下拉列表中选择要修改的堆栈。

步骤 4　点击 **Add Virtual Router**。

系统将显示 Add Virtual Router 弹出窗口。

步骤 5　在 **Name** 字段中，键入虚拟路由器的名称。可使用字母数字字符和空格。

步骤 6　要在虚拟路由器上启用 IPv6 静态路由、OSPFv3 和 RIPng，请选择 **IPv6 Support** 复选框。要禁用这些功能，请清除此复选框。

步骤 7　或者，如果不想启用严格 TCP 执行功能，则可清除 **Strict TCP Enforcement**。

默认情况下，此选项启用。

步骤 8　在 **Interfaces** 下方， **Available** 列表包含设备上可分配至虚拟路由器上的所有已启用的第 3 层路由和混合接口。选择要分配给虚拟路由器的一个或多个接口，然后点击 **Add**。

提示　要从虚拟路由器移除路由或混合接口，请点击删除图标 ( )。在 Interfaces 选项卡上禁用已配置的接口也会将其移除。

步骤 9　点击 **Save**。

虚拟路由器添加成功。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

设置 DHCP 中继

许可证：可控性

受支持的设备：3 系列

DHCP 提供 Internet 主机的配置参数。尚未获得 IP 地址的 DHCP 客户端不能直接与广播域之外的 DHCP 服务器通信。要使 DHCP 客户端与 DHCP 服务器进行通信，可配置 DHCP 中继实例以处理客户端与服务器处于不同广播域的情况。

可以为所配置的每个虚拟路由器设置 DHCP 中继。默认情况下，此功能已禁用。可启用 DHCPv4 中继或 DHCPv6 中继。

有关详细信息，请参阅以下各节：

- 第 7-10 页上的设置 DHCPv4 中继
- 第 7-11 页上的设置 DHCPv6 中继

设置 DHCPv4 中继

许可证：可控性

受支持的设备：3 系列

以下步骤介绍如何在虚拟路由器上设置 DHCPv4 中继。

要设置 DHCPv4 中继，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要为其设置 DHCP 中继的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要为其设置 DHCP 中继的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　要为 DHCPv4 设置 DHCP 中继，请选择 **DHCPv4** 复选框。

步骤 6　在 **Servers** 字段下方，键入服务器 IP 地址。

步骤 7　点击**添加**。

IP 地址已添加至 **Servers** 字段。最多可添加四个 DHCP 服务器。

提示　要删除 DHCP 服务器，请点击服务器 IP 地址旁的删除图标 ( )。

步骤 8　在 **Max Hops** 字段中，键入范围在 1 到 255 之间的最大跳数。

步骤 9　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

设置 DHCPv6 中继

许可证：可控性

受支持的设备：3 系列

以下步骤介绍如何在虚拟路由器上设置 DHCPv6 中继。

注　不能通过在同一设备上运行的两个或多个虚拟路由器运行 DHCPv6 中继链。

要设置 DHCPv6 中继，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要为其设置 DHCP 中继的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要为其设置 DHCP 中继的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　要为 DHCPv6 设置 DHCP 中继，请选择 **DHCPv6** 复选框。

步骤 6　在 **Interfaces** 字段中，选择已分配至虚拟路由器的一个或多个接口旁的复选框。

提示　如对某一接口进行了 DHCPv6 中继配置，则无法从 Interfaces 选项卡禁用该接口。只有先清除 DHCPv6 Relay Interfaces 复选框，才能保存配置。

步骤 7　在所选接口旁，点击下拉菜单图标并选择接口是在 **Upstream**、**Downstream** 还是 **Both** 接口中继 DHCP 请求。

请注意，必须包含至少一个下行接口和一个上行接口。二者同时选择表示接口既可以下行也可以上行。

步骤 8　在 **Max Hops** 字段中，键入范围在 1 到 255 之间的 的最大跳数

步骤 9　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

设置静态路由

许可证：可控性

受支持的设备：3 系列

静态路由可供您编写有关通过路由器的流量的 IP 地址的规则。因为无需就网络的当前拓扑与其他路由器进行通信，因此它是配置虚拟路由器的路径选择的最简便方式。

有关详细信息，请参阅以下各节：

- 第 7-12 页上的了解静态路由表视图
- 第 7-12 页上的添加静态路由

了解静态路由表视图

许可证：可控性

受支持的设备：3 系列

Virtual Router 编辑器的 Static Routes 选项卡显示已在虚拟路由器上配置的所有静态路由的列表。该表包括每个路由器的摘要信息，如下表所示。

表 7-2　　静态路由表视图字段

字段	说明
启用	指定此路由当前是否已启用。
字段名称	静态路由的名称。
目标	流量将路由至的目标网络。
类型	指定为此路由执行的操作，具体为下列某项： • IP - 指定路由将数据包转发至相邻路由器的地址。 • 接口 - 指定路由将数据包转发至流量被路由到直连网络上主机时所经由的接口。 • 丢弃 - 指定静态路由丢弃数据包。
网关	目标 IP 地址（如已选择 IP 作为静态路由类型）或接口（如已选择接口作为静态路由类型）。
偏好	确定路由选择。如有多条路由到达同一目标，系统会选择优先级高的路由。

添加静态路由

许可证：可控性

受支持的设备：3 系列

以下步骤介绍如何添加静态路由。

要编辑静态路由，请点击编辑图标 ( )。要删除静态路由，请点击删除图标 ( )。

要添加静态路由，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加静态路由的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要向其添加静态路由的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　点击 **Static** 以显示静态路由选项。

步骤 6　点击 **Add Static Route**。

系统将显示 Add Static Route 弹出窗口。

步骤 7　在 **Route Name** 字段中，键入静态路由的名称。可使用字母数字字符和空格。

步骤 8　对于 **Enabled**，请选择该复选框以指定路由当前已启用。

步骤 9　在 **Preference** 字段中，键入介于 1 和 65535 之间的一个数值以确定路由选择。

如有多条路由到达同一目标，系统会选择优先级高的路由。

步骤 10　从 **Type** 下拉列表中，选择要配置的静态路由类型。

步骤 11　在 **Destination** 字段中，键入应将流量路由至的目标网络的 IP 地址。

步骤 12　在 **Gateway** 字段中，有两个选项：

- 如已选择 **IP** 作为选定的静态路由类型，请键入 IP 地址。
- 如已选择 **Interface** 作为选定的静态路由类型，请从下拉列表中选择已启用的接口。

提示　已从 Interfaces 选项卡中禁用的接口将无法使用；禁用已添加的接口会同时将其从配置中删除。

步骤 13　点击 **OK**。

静态路由添加成功。

步骤 14　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

设置动态路由

许可证：可控性

受支持的设备：3 系列

动态或自适应路由使用路由协议更改路由所经过的路径，以响应网络状况的变化。自适应旨在使尽可能多的路由保持有效状态，也就是说，在响应变化时有可到达的目标。这样，只要有其他选项可用，网络就可“绕过”故障，例如节点丢失或节点间连接断开。可配置无动态路由的路由器，也可配置路由信息协议 (RIP) 或开放最短路径优先 (OSPF) 路由协议。

有关详细信息，请参阅以下各节：

- 第 7-14 页上的设置 RIP 配置
- 第 7-19 页上的设置 OSPF 配置

设置 RIP 配置

许可证：可控性

受支持的设备：3 系列

路由信息协议 (RIP) 是一种动态路由协议，专为小型 IP 网络设计，它依靠跳数确定路由。最佳路由采用的跳数最少。 RIP 允许的最大跳数为 15。此跳数限值也限制 RIP 可支持的网络规模。

有关配置 RIP 的详细信息，请参阅以下各节。

为 RIP 配置添加接口

许可证：可控性

受支持的设备：3 系列

在配置 RIP 时，必须从要配置 RIP 的虚拟路由器上所包括的接口中选择接口。已禁用的接口无法使用。

要编辑 RIP 接口，请点击编辑图标 ( )。要删除 RIP 接口，请点击删除图标 ( )。

要为 RIP 配置添加接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加 RIP 接口的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要向其添加 RIP 接口的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　点击 **Dynamic Routing** 以显示动态路由选项。

步骤 6　点击 **RIP** 以显示 RIP 选项。

步骤 7　在 **Interfaces** 下，点击添加图标 ( )。

系统将显示 Add an Interface 弹出窗口。

步骤 8　从 **Name** 下拉列表中，选择要为其配置 RIP 的接口。

提示　已从 Interfaces 选项卡中禁用的接口将无法使用；禁用已添加的接口会同时将其从配置中删除。

步骤 9　在 **Metric** 字段中，键入接口的度量值。如有来自不同 RIP 实例的路由可用且它们都有相同的优先级，则度量值最低的路由会成为首选路由。

步骤 10　从 **Mode** 下拉列表中，选择下列选项之一。

- **Multicast** - 默认模式。在此模式下，RIP 会将整个路由表组播至位于指定地址的所有邻接路由器。
- **Broadcast** - 即使有组播模式可供使用，也会强迫 RIP 使用广播模式 （例如， RIPv1）。
- **Quiet** - RIP 不会将任何定期消息发送至该接口。
- **No Listen** - RIP 将发送消息至该接口，但不监听该接口。

步骤 11　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

配置 RIP 配置的身份验证设置

许可证：可控性

受支持的设备：3 系列

RIP 身份验证使用您在虚拟路由器上配置的某一身份验证配置文件。有关配置身份验证配置文件的详细信息，请参阅第 7-28 页上的添加虚拟路由器身份验证配置文件。

要配置 RIP 配置的身份验证设置，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加 RIP 身份验证配置文件的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要向其添加 RIP 身份验证配置文件的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　点击 **Dynamic Routing** 以显示动态路由选项。

步骤 6　点击 **RIP** 以显示 RIP 选项。

步骤 7　在 **Authentication** 下方，使用 Profile 下拉列表选择一个现有虚拟路由器身份验证配置文件或选择 **None**。

步骤 8　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

配置 RIP 配置的高级设置

许可证：可控性

受支持的设备：3 系列

可配置与影响协议行为的各种超时值和其他功能相关的高级 RIP 设置。

注意事项　如将任一高级 RIP 设置更改为错误值，将导致路由器无法与其他 RIP 路由器成功通信。

要配置 RIP 配置的高级设置，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加 RIP 高级设置的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要向其添加 RIP 高级设置的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　点击 **Dynamic Routing** 以显示动态路由选项。

步骤 6　点击 **RIP** 以显示 RIP 选项。

步骤 7　在 **Preference** 字段中，键入路由协议优先级的数值（越高越好）。相比于静态路由，系统更偏向于使用通过 RIP 获悉的路由。

步骤 8　在 **Period** 字段中，键入定期更新之间的时间间隔，单位为秒。数值越小，收敛速度越快，但网络负载也越大。

步骤 9　在 **Timeout Time** 字段中，键入指定路由存续时间的数值（单位为秒）。过了该时间，路由将视为不可达。

步骤 10　在 **Garbage Time** 字段中，键入指定路由存续时间的数值（单位为秒）。过了该时间后，路由将被丢弃。

步骤 11　在 **Infinity** 字段中，键入在收敛计算中表示无限距离的数值。该值越大，协议收敛将越慢。

步骤 12　从 **Honor** 下拉列表中，选择下列选项之一，以指定何时满足删除路由表的请求：

- **Always** - 始终满足请求
- **Neighbor** - 仅满足由直连网络上主机发送的请求
- **Never** - 始终不满足请求

步骤 13　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

添加 RIP 配置的导入过滤条件

许可证：可控性

受支持的设备：3 系列

可添加导入过滤条件，以指定在由 RIP 进入路由表时，哪些路由会被接受或拒绝。导入过滤条件的应用顺序与其在表中的出现顺序相同。

在添加导入过滤条件时，请使用在虚拟路由器上配置的过滤条件之一。有关配置过滤条件的详细信息，请参阅第 7-26 页上的设置虚拟路由器过滤条件。

提示 要编辑 RIP 导入过滤条件，请点击编辑图标 ( )。要删除 RIP 导入过滤条件，请点击删除图标 ( )。

要添加 RIP 配置的导入过滤条件，请执行以下操作：

访问：管理员/网络管理员

步骤 1 选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2 在要向其添加 RIP 虚拟路由器过滤条件的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3 点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4 在要向其添加 RIP 虚拟路由器过滤条件的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5 点击 **Dynamic Routing** 以显示动态路由选项。

步骤 6 点击 **RIP** 以显示 RIP 选项。

步骤 7 在 **Import Filters** 下方，点击添加图标 ( )。

系统将显示 Add an Import Filter 弹出窗口。

步骤 8 从 **Name** 下拉列表中，选择要作为导入过滤条件添加的过滤条件。

步骤 9 在 **Action** 旁，选择 **Accept** 或 **Reject**。

步骤 10 点击 **OK**。

导入过滤条件添加成功。

提示 要更改导入过滤条件的顺序，请根据需要点击上移 ( ) 和下移 ( ) 图标。也可在列表中上下拖动过滤条件。

步骤 11 点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

添加 RIP 配置的导出过滤条件

许可证：可控性

受支持的设备：3 系列

可添加导出过滤条件，以指定在从路由表导出至 RIP 时，哪些路由会被接受或拒绝。导出过滤条件的应用顺序与其在表中的出现顺序相同。

在添加导出过滤条件时，请使用在虚拟路由器上配置的过滤条件之一。有关配置过滤条件的详细信息，请参阅第 7-26 页上的设置虚拟路由器过滤条件。

要添加 RIP 配置的导出过滤条件，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加 RIP 虚拟路由器过滤条件的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要向其添加 RIP 虚拟路由器过滤条件的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　点击 **Dynamic Routing** 以显示动态路由选项。

步骤 6　点击 **RIP** 以显示 RIP 选项。

步骤 7　在 **Export Filters** 下方，点击添加图标 ( )。

系统将显示 Add an Export Filter 弹出窗口。

步骤 8　从 **Name** 下拉列表中，选择要作为导出过滤条件添加的过滤条件。

步骤 9　在 **Action** 旁，选择 **Accept** 或 **Reject**。

步骤 10　点击 **OK**。

导出过滤条件添加成功。

提示　要更改导出过滤条件的顺序，请根据需要点击上移 ( ) 和下移 ( ) 图标。也可在列表中上下拖动过滤条件。

步骤 11　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

设置 OSPF 配置

许可证：可控性

受支持的设备：3 系列

开放最短路径优先 (OSPF) 是一个自适应路由协议，它使用链路状态通告获取来自其他路由器的信息并向其他路由器通告路由，从而动态地确定路由。路由器会保留其与目标之间的链路信息，以做出路由决定。 OSPF 向每个路由接口分配一个开销，并将开销最低的路由视为最佳路由。

有关详细信息，请参阅以下各节：

- 第 7-19 页上的设置 OSPF 路由区域
- 第 7-24 页上的添加 OSPF 配置的导入过滤条件
- 第 7-25 页上的添加 OSPF 配置的导出过滤条件

设置 OSPF 路由区域

许可证：可控性

受支持的设备：3 系列

OSPF 网络可以构建或划分为多个路由区域，从而简化管理并优化流量和资源的使用。区域按 32 位数字识别，可简单表示为十进制数，或通常表示为基于八字节的的点十进制符号。

按照惯例，区域 0 或 0.0.0.0 代表 OSPF 网络的核心或骨干区域。可选择标识其他区域。通常，管理员会选择某一区域内主路由器的 IP 地址作为该区域的标识。每个额外区域都必须有到骨干 OSPF 区域的直接或虚拟连接。此类连接由互联的路由器维护，这些路由器称为区域边界路由器 (ABR)。 ABR 为其服务的各个区域维护单独的链路状态数据库，并为网络中的所有区域维护汇总路由。

有关设置 OSPF 区域的详细信息，请参阅以下各节：

- 第 7-19 页上的添加 OSPF 区域
- 第 7-20 页上的添加 OSPF 区域接口
- 第 7-23 页上的添加 OSPF 区域虚拟链路

添加 OSPF 区域

许可证：可控性

受支持的设备：3 系列

以下步骤介绍如何添加 OSPF 区域和配置常规设置。

要添加 OSPF 区域，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加 OSPF 常规选项的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要向其添加 OSPF 常规选项的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　点击 **Dynamic Routing** 以显示动态路由选项。

步骤 6　点击 **OSPF** 以显示 OSPF 选项。

步骤 7　在 **Areas** 下方，点击添加图标 ( )。

系统将显示 Add OSPF Area 弹出窗口。

步骤 8　在 **Area Id** 字段中，键入区域的数值。该值可以是整数或 IPv4 地址。

步骤 9　或者，选择 **Stubnet** 复选框，以指定该区域不接收自治系统之外的路由器通告，并且区域内的路由完全基于默认路由。如果清除此复选框，则该区域将成为骨干区域，否则将成为非末节区域。

系统将显示 Default Cost 字段和 Stubnet 字段。

步骤 10　在 **Default cost** 字段中，键入与该区域的默认路由相关联的开销。

步骤 11　在 **Stubnets** 下方，点击添加图标 ( )。

步骤 12　在 **IP Address** 字段中，使用 CIDR 表示法键入 IP 地址。

步骤 13　选择 **Hidden** 复选框以指明末节网络已隐藏。隐藏的末节网络不会传播到其他区域。

步骤 14　选择 **Summary** 复选框，以指定属行此末节网络子网的默认末节网络已被抑制。

步骤 15　在 **Stub cost** 字段中，输入用于确定与路由至此末节网络的开销相关联的值。

步骤 16　点击 **OK**。

末节网络添加成功。

提示　要编辑末节网络，请点击编辑图标 ( )。要删除末节网络，请点击删除图标 ( )。

步骤 17　或者，在 **Networks** 下方，点击添加图标 ( )。

步骤 18　在 **IP Address** 字段中，使用 CIDR 表示法键入网络的 IP 地址。

步骤 19　选择 **Hidden** 复选框以指明网络已隐藏。隐藏的网络不会传播到其他区域。

步骤 20　点击 **OK**。

网络添加成功。

提示　要编辑网络，请点击编辑图标 ( )。要删除网络，请点击删除图标 ( )。

步骤 21　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

添加 OSPF 区域接口

许可证：可控性

受支持的设备：3 系列

可为 OSPF 配置分配给虚拟路由器的接口子集。下表介绍了可在各个接口上指定的选项。

接口

选择要为其配置 OSPF 的接口。已从 Interfaces 选项卡中禁用的接口将无法使用

类型

从以下选项中选择 OSPF 接口的类型：

- Broadcast - 在广播网络中，泛洪和呼叫消息使用组播发送，即同一数据包会发送给所有邻居。此选项指定路由器负责同步链路状态数据库并发起网络链路状态通告。此网络类型不能用在物理上非广播多路访问 (NBMP) 网络及未编号的无适当 IP 前缀的网络上。
- Point-to-Point (PtP) - 点对点网络仅将两台路由器连接在一起。此选项不执行选举，也不会发起网络链路状态通告，因此连接起来更简单更快速。此网络类型不仅适用于物理上 PtP 的接口，同时适用于用作 PtP 链路的广播网络。此网络类型不能用于物理形态为 NBMP 的网络。
- Non-Broadcast - 在 NBMP 网络上，由于缺少组播功能，数据包被单独发送给各个邻居。类似于广播网络，此选项会指定一个路由器，该路由器在链路状态通告的传播上起着重要作用。此网络类型不能用于无编号网络。
- Autodetect - 系统根据指定的接口确定正确的类型。

成本

指定接口的输出开销。

Stub

指定接口是否应监听 OSPF 流量并发送自己的流量。

优先级

输入一个数字值，以指定用于指定路由器选举的优先级值。在每个多路访问网络上，系统会指定一个路由器和备用路由器。这些路由器在泛洪过程中有一些特殊的功能。优先级越高，在此选举中的优先级也越高。不能配置优先级为 0 的路由器。

Nonbroadcast

指定是否将 hello 数据包发给任何未定义的邻居。此交换机在所有 NBMA 网络均被忽略。

身份验证

从在虚拟路由器上配置的某一身份验证配置文件中选择此接口使用的 OSPF 身份验证配置文件，或选择 **None**。有关配置身份验证配置文件的详细信息，请参阅第 7-28 页上的添加虚拟路由器身份验证配置文件。

Hello Interval

输入发送 hello 消息的间隔，单位为秒。

Poll

键入向 NBMA 网络上某些邻居发送 hello 消息时的间隔，单位为秒。

Retrans Interval

键入重新传输未确认更新之间的间隔，单位为秒。

Retrans Delay

键入在接口上传输链路状态更新数据包时估计需要的时间，单位为秒。

Wait Time

键入路由器在开始选举和建立邻接关系之间等待的时间，单位为秒。

Dead Interval

键入当路由器未收到来自邻居的消息时，在宣告邻居崩溃之前需等待的时间，单位为秒。如已定义该值，则它会覆盖由失效计数计算而来的值。

Dead Count

键入一个数字值，该值与 问询间隔的乘积会指定当路由器未收到来自邻居的消息时，在宣告邻居崩溃之前需等待的时间，单位为秒。

要编辑 OSPF 区域接口，请点击编辑图标 ( )。要删除 OSPF 区域接口，请点击删除图标 ( )。在 Interfaces 选项卡上禁用已配置的接口也会将其删除。

注　只能选择一个接口用于 OSPF 区域。

要添加 OSPF 区域接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加 OSPF 接口的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要向其添加 OSPF 接口的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　点击 **Dynamic Routing** 以显示动态路由选项。

步骤 6　点击 **OSPF** 以显示 OSPF 选项。

步骤 7　在 **Areas** 下方，点击添加图标 ( )。

系统将显示 Add OSPF Area 弹出窗口。

步骤 8　点击 **Interfaces**。

系统将显示 Interfaces 选项卡。

步骤 9　点击添加图标 ( )。

系统将显示 Add OSPF Area Interface 弹出窗口。

步骤 10　执行第 7-20 页上的添加 OSPF 区域接口中描述的任意操作。

步骤 11　或者，在 **Neighbors** 下方，点击添加图标 ( )。

步骤 12　在 **IP address** 字段中，键入在非广播网络上从此接口接收 hello 消息的邻居的 IP 地址。

步骤 13　选择 **Eligible** 复选框以指明邻居有资格接收消息。

步骤 14　点击 **OK**。

邻居添加成功。

提示　要编辑邻居，请点击编辑图标 ( )。要删除邻居，请点击删除图标 ( )。

步骤 15　点击 **OK**。

OSPF 区域接口添加成功。

步骤 16　点击 **Save**。

OSPF 区域保存成功。

步骤 17　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

添加 OSPF 区域虚拟链路

许可证：可控性

受支持的设备：3 系列

OSPF 自治系统中的所有区域均必须与骨干区域进行物理连接。在无法实现物理连接的情况下，可以使用虚拟链路，通过非骨干区域连接到骨干区域。虚拟链路也可用于通过非骨干区域连接一个分区骨干网的两个部分。

必须至少添加两个 OSPF 区域，然后才能添加虚拟链路。

要添加 OSPF 区域虚拟链路，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加 OSPF 虚拟链路的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要向其添加 OSPF 接口的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　点击 **Dynamic Routing** 以显示动态路由选项。

步骤 6　点击 **OSPF** 以显示 OSPF 选项。

步骤 7　在 **Areas** 下方，点击添加图标 ( )。

系统将显示 Add OSPF Area 弹出窗口。

步骤 8　点击 **Vlinks**。

系统将显示 Vlinks 选项卡。

步骤 9　点击添加图标 ( )。

系统将显示 Add OSPF Area Vlink 弹出窗口。

步骤 10　在 **Router ID** 字段中，键入路由器的 IP 地址。

步骤 11　从 **Authentication**下拉列表中，选择虚拟链路将使用的身份验证配置文件。

步骤 12　在 **Hello Interval** 字段中，键入 hello 消息的发送间隔，单位为秒。

步骤 13　在 **Retrans Interval** 字段中，键入重新传输未获确认更新之间的间隔，单位为秒。

步骤 14　在 **Wait Time** 字段中，键入路由器在开始选举和建立邻接关系之间等待的时间，单位为秒。

步骤 15　在 **Dead Interval** 字段中，键入当路由器未收到来自邻居的消息时，在宣告邻居崩溃之前需等待的时间，单位为秒。如已定义该值，则它会覆盖由失效计数计算而来的值。

步骤 16　在 **Dead Count** 字段中，键入一个数字值，该值与 问询间隔的乘积会指定当路由器未收到来自邻居的消息时，在宣告邻居崩溃之前需等待的时间，单位为秒。

步骤 17　点击 **OK**。

OSPF 区域虚拟链路添加成功。

步骤 18　点击 **Save**。

OSPF 区域保存成功。

步骤 19　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

添加 OSPF 配置的导入过滤条件

许可证：可控性

受支持的设备：3 系列

可添加导入过滤条件，以指定在由 OSPF 进入路由表时，哪些路由会被接受或拒绝。导入过滤条件的应用顺序与其在表中的出现顺序相同。

在添加导入过滤条件时，请使用在虚拟路由器上配置的过滤条件之一。有关配置过滤条件的详细信息，请参阅第 7-26 页上的设置虚拟路由器过滤条件。

要添加 OSPF 配置的导入过滤条件，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加 OSPF 虚拟路由器过滤条件的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要向其添加 OSPF 虚拟路由器过滤条件的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　点击 **Dynamic Routing** 以显示动态路由选项。

步骤 6　点击 **OSPF** 以显示 OSPF 选项。

步骤 7　在 **Import Filters** 下方，点击添加图标 ( )。

系统将显示 Add Import Filter 弹出窗口。

步骤 8　从 **Name** 下拉列表中，选择要作为导入过滤条件添加的过滤条件。

步骤 9　在 **Action** 旁，选择 **Accept** 或 **Reject**。

步骤 10　点击 **OK**。

导入过滤条件添加成功。

提示　要更改导入过滤条件的顺序，请根据需要点击上移 ( ) 和下移 ( ) 图标。也可在列表中上下拖动过滤条件。

步骤 11　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

添加 OSPF 配置的导出过滤条件

许可证：可控性

受支持的设备：3 系列

可添加导出过滤条件，以指定在从路由表导出至 OSPF 时，哪些路由会被接受或拒绝。导出过滤条件的应用顺序与其在表中的出现顺序相同。

在添加导出过滤条件时，请使用在虚拟路由器上配置的过滤条件之一。有关配置过滤条件的详细信息，请参阅第 7-26 页上的设置虚拟路由器过滤条件。

要添加 OSPF 配置的导出过滤条件，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加 OSPF 虚拟路由器过滤条件的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要向其添加 OSPF 虚拟路由器过滤条件的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　点击 **Dynamic Routing** 以显示动态路由选项。

步骤 6　点击 **OSPF** 以显示 OSPF 选项。

步骤 7　在 **Export Filters** 下方，点击添加图标 ( )。

系统将显示 Add an Export Filter 弹出窗口。

步骤 8　从 **Name** 下拉列表中，选择要作为导出过滤条件添加的过滤条件。

步骤 9　在 **Action** 旁，选择 **Accept** 或 **Reject**。

步骤 10　点击 **OK**。

导出过滤条件添加成功。

提示　要更改导出过滤条件的顺序，请根据需要点击上移 (▲) 和下移 (▼) 图标。也可在列表中上下拖动过滤条件。

步骤 11　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

设置虚拟路由器过滤条件

许可证：可控性

受支持的设备：3 系列

过滤条件提供了一种匹配路由的方式，以将路由导入至虚拟路由器的路由表并将路由导出至动态协议。可创建和管理过滤条件列表。每个过滤条件都界定了特定的准则，以查找静态界定的路由或从动态协议获得的路由。

提示　要编辑虚拟路由器过滤条件，请点击编辑图标 ( )。要删除虚拟路由器过滤条件，请点击删除图标 ( )。

Virtual Router 编辑器的 Filter 选项卡显示一个表，其中列出在虚拟路由器上已配置的所有过滤条件。该表包括每种过滤条件的摘要信息，如下表所示。

表 7-3　虚拟路由器过滤条件表视图字段

字段	说明
字段名称	过滤条件名称。
协议	发起路由所依据的协议： • Static - 作为本地静态路由发起的路由。 • RIP - 由动态 RIP 配置发起的路由。 • OSPF - 由动态 OSPF 配置发起的路由。
From Router	此过滤条件尝试在路由器中匹配的路由器 IP 地址。必须为静态和 RIP 过滤条件输入此值。
Next Hop	使用此路由的数据包将被转发到的下一跳。必须为静态和 RIP 过滤条件输入此值。
Destination Type	数据包要发送到的目标类型： • 路由器 • 设备 • 丢弃
目标网络	此过滤条件尝试在路由中匹配的网络。

表 7-3　虚拟路由器过滤条件表视图字段（续）

字段	说明
OSPF Path Type	仅适用于 OSPF 协议。路径类型可是以下其中一项： • Ext-1 • Ext-2 • Inter Area • Intra Area
OSPF Router ID	仅适用于 OSPF 协议。通告该路由/网络的路由器的路由器 ID。

要添加虚拟路由器过滤条件，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加虚拟路由器过滤条件的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要向其添加虚拟路由器过滤条件的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　点击 **Filter** 以显示 Filter 选项。

步骤 6　点击 **Add Filter**。

系统将显示 Create Filter 弹出窗口。

步骤 7　在 **Name** 字段中，键入过滤器名称。只能使用字母数字字符。

步骤 8　在 **Protocol** 下方，选择 **All** 或选择适用于过滤条件的协议。

步骤 9　如已选择 All、 Static 或 RIP 作为协议，则在 **From Router** 下方，键入此过滤条件尝试在路由中匹配的路由器 IP 地址。

请注意，也可输入一个 32 位的 CIDR 数据块来表示 IPv4 地址和一个 128 位的前缀长度来表示 IPv6 地址。所有其他的地址块对于此字段都无效。

步骤 10　点击**添加**。

From Router 字段填充成功。

步骤 11　如已选择 All、 Static 或 RIP 作为协议，则在 **Next Hop** 下方，键入此过滤条件尝试在路由中匹配的网关的 IP 地址。

请注意，也可输入一个 32 位的 CIDR 数据块来表示 IPv4 地址和一个 128 位的前缀长度来表示 IPv6 地址。所有其他的地址块对于此字段都无效。

步骤 12　点击**添加**。

Next Hop 字段填充成功。

步骤 13　在 **Destination Type** 类型下方，选择适用于该过滤条件的选项。

步骤 14　在 **Destination Network** 下方，键入此过滤条件将在路由中尝试匹配的网络的 IP 地址。

步骤 15　点击**添加**。

Destination Network 字段填充成功。

步骤 16　如已选择 All 或 OSPF 作为协议，则在 **Path Type** 下方，选择适用于该过滤条件的选项。

必须至少选择一种路径类型。

步骤 17　如已选择 OSPF 作为协议，则在 **Router ID** 下方，键入用作路由/网络通告路由器的路由器 ID 的 IP 地址。

步骤 18　点击**添加**。

Router ID 字段填充成功。

步骤 19　点击 **OK**。

过滤条件添加成功。

步骤 20　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

添加虚拟路由器身份验证配置文件

许可证：可控性

受支持的设备：3 系列

可设置用于 RIP 和 OSPF 配置的身份验证配置文件。可配置简单的密码或指定共享的加密密钥。简单密码允许所有数据包携带密码的八个字节。如果接收到的数据包缺少此密码，系统会将其忽略。加密密钥可用于进行验证，它是一个根据密码生成的 16 字节长的摘要，用于附加到每个数据包上。

请注意，对于 OSPF，每个区域均可能有不同的身份验证方法。因此，可创建能在许多区域之间共享的身份验证配置文件。无法为 OSPFv3 添加身份验证。

提示　要编辑身份验证配置文件，请点击编辑图标 ( )。要删除身份验证配置文件，请点击删除图标 ( )。

要添加虚拟路由器身份验证配置文件，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要向其添加虚拟路由器身份验证配置文件的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要向其添加虚拟路由器身份验证配置文件的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Edit Virtual Router 弹出窗口。

步骤 5　点击 **Authentication Profile**。

系统将显示 Authentication Profile 选项卡。

步骤 6　点击 **Add Authentication Profile**。

系统将显示 Add Authentication Profile 弹出窗口。

步骤 7　在 **Authentication Profile Name** 字段中，键入身份验证配置文件的名称。

步骤 8　从 **Authentication Type** 下拉列表中，选择 **simple** 或 **cryptographic**。

步骤 9　在 **Password** 字段中，键入安全的密码。

步骤 10　在 **Confirm Password** 字段中，重新键入密码进行确认。

步骤 11　点击 **OK**。

身份验证配置文件添加成功。

步骤 12　点击 **Save**。

已保存您的更改。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

查看虚拟路由器统计数据

许可证：可控性

受支持的设备：3 系列

可查看每个虚拟路由器的运行时统计数据。这些统计数据显示了单播数据包、丢弃的数据包和针对 IPv4 和 IPv6 地址的不同的路由表。

要查看虚拟路由器的统计数据，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要为其查看虚拟路由器统计数据的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要为其查看虚拟路由器统计数据的虚拟路由器旁，点击编辑图标 ( )。

系统将显示 Statistics 弹出窗口。

步骤 5　点击 **OK** 关闭该窗口。

删除虚拟路由器

许可证：可控性

受支持的设备：3 系列

删除虚拟路由器之后，向其分配的所有路由接口均可纳入另一路由器中。

要删除虚拟路由器，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要为其删除虚拟路由器的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Virtual Routers**。

系统将显示 Virtual Routers 选项卡。

步骤 4　在要删除的虚拟路由器旁，点击删除图标 ( )。

步骤 5　看到提示后，请确认要删除虚拟路由器。

虚拟路由器删除成功。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

设置汇聚接口

您可以将多个物理以太网接口组合到3 系列 受管设备上的单一逻辑链路，这些设备或者在提供网络间数据包交换的第 2 层部署中配置，或者在路由接口间流量的第 3 层部署中配置。此单一汇聚逻辑链路在两个终端之间提供更高的带宽、冗余和负载均衡。

可以通过创建一个交换或路由链路汇聚组或 LAG 来创建汇聚链路。当创建汇聚组时，会创建称为汇聚接口的逻辑接口。对一个上层实体而言，LAG 看起来像单一逻辑链路，并且数据流量通过汇聚接口进行传输。通过将多条链路的带宽添加到一起，汇聚链路可增加带宽。通过负载均衡所有可用链路之间的流量，它还提供冗余。如果一条链路发生故障，系统自动负载均衡所有剩余的链路之间的流量。

LAG 中的终端可以是两台 FirePOWER 受管设备（如上图所示）或者是连接到第三方接入交换机或路由器的 FirePOWER 受管设备。两台设备无需匹配，但是必须具有相同的物理配置并且必须支持 IEEE 802.ad 链路汇聚标准。LAG 的典型部署可能是在两台受管设备之间汇聚访问链路，或者在受管设备和接入交换机或路由器之间创建点对点连接。

请注意，您不能在虚拟受管设备、具备 FirePOWER 服务的 Cisco ASA 防火墙设备或用于 Blue Coat X-系列的思科 NGIPS设备上配置聚集接口。

有关设置汇聚接口的详细信息，请参阅第 8-1 页上的配置 LAG。

配置 LAG

许可证：可控性

受支持的设备：3 系列

有两种类型的汇聚接口：交换接口和路由接口，前者是第 2 层汇聚接口，后者是第 3 层汇聚接口。通过使用链路汇聚组 (LAG) 可以实现链路汇聚。通过创建汇聚交换或路由接口，然后将一组物理接口与链路相关联，可以配置 LAG。所有物理接口必须具有相同的速度和介质。

您可以动态或静态创建汇聚链路。当静态链路汇聚不起作用时，动态链路汇聚使用链路汇聚控制协议 (LACP)，该协议是 IEEE 802.ad 链路汇聚标准的组件。 LACP 启用 LAG 任一端上的每台设备，以交换链路和系统信息，从而确定汇聚中将主动使用哪些链路。静态 LAG 配置要求您手动维护链路汇聚以及应用负载均衡和链路选择策略。

当您创建交换或路由汇聚接口时，会自动创建同一类型的链路汇聚组并进行编号。例如，当您创建第一个 LAG（交换或路由）时，此汇聚接口可以使用受管设备的 Interfaces 选项卡上的 **lag0** 标签进行识别。将物理和逻辑接口与此 LAG 相关联时，在分层树菜单中的主要 LAG 下面以嵌套方式显示这些接口。请注意，交换 LAG 只能包含交换的物理接口，路由 LAG 只能包含路由物理接口。

当配置 LAG 时，请考虑以下要求：

- FireSIGHT 系统最多支持 14 个 LAG，并为每个 LAG 接口分配一个唯一 ID，范围从 0 到 13。LAG ID 不可配置。
- 您必须在链路的两侧配置 LAG，并且必须将链路每侧的接口设置为具有相同的速率。
- 必须将每个 LAG 与最少两个、最多八个物理接口相关联。一个物理接口不能属于多个 LAG。
- 不能以任何其他操作模式将 LAG 中的物理接口用作内联或被动接口，或用作已标记流量的另一个逻辑接口的一部分。
- LAG 中的物理接口可以跨越多个 NetMod，但是不能跨越多个传感器（即，所有物理接口必须位于同一台设备上）。
- LAG 不能包含堆叠的 NetMod。

注　设备集群上不支持链路汇聚。

有关详细信息，请参阅以下各节：

- 第 8-2 页上的指定负载均衡算法
- 第 8-3 页上的指定链路选择策略
- 第 8-4 页上的配置 LACP
- 第 8-4 页上的添加汇聚交换接口
- 第 8-6 页上的添加汇聚路由接口
- 第 8-9 页上的添加逻辑汇聚接口
- 第 8-10 页上的查看汇聚接口统计数据
- 第 8-11 页上的删除汇聚接口

指定负载均衡算法

许可证：可控性

受支持的设备：3 系列

将出口负载均衡算法分配给确定如何将流量分布给 LAG 捆绑包的成员链路的 LAG。负载均衡算法基于各种数据包字段中的值作出散列决策，例如第 2 层 MAC 地址、第 3 层 IP 地址和第 4 层端口号（TCP/UDP 流量）。您选择的负载均衡算法适用于 LAG 捆绑包的所有成员链路。

配置 LAG 时，从以下选项选择支持您的部署方案的负载均衡算法：

- Destination IP
- Destination MAC
- Destination Port
- Source IP
- Source MAC
- Source Port

- Source and Destination IP
- Source and Destination MAC
- Source and Destination Port

注　您应该将 LAG 的两端配置为具有相同的负载均衡算法。必要时，较高层的算法将回退到较低层的算法（例如，对于 ICMP 流量，第 4 层算法回退到第 3 层算法）。

指定链路选择策略

许可证：可控性

受支持的设备：3 系列

链路汇聚要求每条链路的速度和介质在两个终端上均相同。由于链路属性可以动态更改，因此，链路选择策略有助于确定系统如何管理链路选择过程。最大化最高端口数的链路选择策略支持链路冗余，同时最大化总带宽的链路选择策略支持总链路速度。稳定的链路选择策略尝试将链路状态下的额外更改减到最少。

注　您应该将 LAG 的两端配置为具有相同的链路选择策略。

配置 LAG 时，从以下选项选择支持您的部署方案的链路选择策略：

- Highest Port Count — 为最高总活动端口数选择此选项，以提供更多冗余。
- Highest Total Bandwidth — 选择此选项，为汇聚链路提供最高总带宽。
- Stable — 如果您最关心链路稳定性和可靠性，请选择此选项。一旦配置 LAG 后，仅当绝对必要（例如链路故障）而不是为获得更多端口数或带宽时，活动链路才会更改。
- LACP Priority — 选择此选项，以使用 LACP 算法确定在 LAG 中哪些链路处于活动状态。如果未定义部署目标，或者 LAG 另一端的设备是非 FirePOWER 设备，则此设置是适当的。

  启用 LACP 后，基于 LACP 优先级的链路选择策略使用两种 LACP 属性：系统优先级和链路优先级，如下所述：

  – LACP 系统优先级。您在运行 LACP 的每台合作设备上配置该值，以确定哪个在链路汇聚中更优越。具有较低值的系统具有较高的系统优先级。在动态链路汇聚中，具有较高 LACP 系统优先级的系统首先设置自己一侧的成员链路的选定状态，然后具有较低优先级的系统相应设置其成员链路。可指定 0 到 65535 之间的任意数字。如果未指定值，则默认优先级是 32768。

  – LACP 链路优先级。您在属于汇聚组的每条链路上配置该值。链路优先级确定在 LAG 中的活动和备用链路。具有较低值的链路具有较高优先级。如果活动链路出现故障，则选择具有最高优先级的备用链路来替换有故障的链路。但是，如果两个或多个链路具有相同的 LACP 链路优先级，则具有最低物理端口号的链路选定为备用链路。可指定 0 到 65535 之间的任意数字。如果未指定值，则默认优先级是 32768。

LACP 是自动化支持动态链路汇聚的链路选择方法的一个主要方面。有关详细信息，请参阅第 8-4 页上的配置 LACP。

配置 LACP

许可证：可控性

受支持的设备：3 系列

链路汇聚控制协议 (LACP) 作为 IEEE 802.3ad 的组件，是交换系统和端口信息以创建和维护 LAG 捆绑包的一种方法。当启用 LACP 时，在 LAG 任一端的每台设备都使用 LACP 确定将在汇聚中主动使用哪些链路。LACP 通过在链路之间交换 LACP 数据包（或控制消息）提供可用性和冗余。它动态了解链路的功能并通知其他链路。一旦 LACP 确定正确匹配的链路，它就促进将链路组合到 LAG 中。如果链路发生故障，流量在剩余的链路继续通过。只有在 LAG 的两端都启用 LACP 才能使链路正常运行。

当启用 LACP 时，您需要为 LAG 的每一端选择一种传输方式，从而确定如何在合作设备之间交换 LACP 数据包。 LACP 模式有 2 种选项：

- Active — 选择此模式将设备置于主动协商状态，在这种状态下，设备通过发送 LACP 数据包发起与远程链路的协商。
- Passive — 选择此模式将设备置于被动协商状态，在这种状态下，设备对其接收的 LACP 数据包做出响应，但是不发起 LACP 协商。

注　这两种模式允许 LACP 在链路之间协商，以根据标准（例如端口速度）确定链路是否可以构成链路捆绑包。但是，您应避免被动-被动配置，其实质上是将 LAG 两端置于侦听模式。

LACP 有一个计时器，其定义在设备之间发送 LACP 数据包的频率。 LACP 以下面的速度交换数据包：

- 慢 - 30 秒
- 快 - 1 秒

此选项所应用的设备预期以该频率从 LAG 另一侧的合作设备接收 LACP 数据包。

注　在作为设备堆栈一部分的受管设备上配置 LAG 时，只有主设备与合作伙伴系统参与 LACP 通信。所有辅助设备将 LACP 消息转发给主设备。主设备将所有动态 LAG 修改中继给辅助设备。

添加汇聚交换接口

许可证：可控性

受支持的设备：3 系列

您可以将受管设备上的两个和八个物理端口结合起来创建交换 LAG 接口。必须将交换 LAG 接口分配给虚拟交换机，然后该接口才可以处理流量。受管设备可支持多达 14 个 LAG 接口。

注意事项　更改最大传输单位 (MTU) 会中断设备上的流量并造成丢包。 MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

要编辑现有交换 LAG 接口，请点击接口旁的编辑图标 ( )。

要配置交换 LAG 接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　点击要配置交换 LAG 接口所在设备旁的编辑图标 ( )。

系统将显示 Interfaces 选项卡。

步骤 3　从 **Add** 下拉菜单中选择 **Add Logical Interface**。

步骤 4　点击 **Switched** 显示交换 LAG 接口选项。

步骤 5　或者，从 **Security Zone** 下拉列表中，选择现有安全区域或选择 **New** 以添加新的安全区域。

步骤 6　必须从 **Virtual Switch** 下拉列表中选择现有虚拟交换机或者选择 **New** 来添加新的虚拟交换机。

注　如果添加新的虚拟交换机，则必须在设置交换接口之后，在 Device Management 页面的 Virtual Switches 选项卡 (**Devices > Device Management> Virtual Switches**) 上配置该虚拟交换机。请参阅第 6-5 页上的添加虚拟交换机。

步骤 7　选择 **Enabled** 复选框，允许交换 LAG 接口处理流量。

如果清除此复选框，接口将被禁用，用户将因安全原因无法对其进行访问。

步骤 8　从 **Mode** 下拉列表中，选择一个选项来指定链路模式或选择 **Autonegotiation** 来指定将该接口配置为自动协商速度和双工设置。请注意，模式设置仅适用于铜接口。

注　8000 系列设备上的接口不支持半双工选项。当链路自动协商速度时，根据相同的速度设置为 LAG 选择所有活动链路。

步骤 9　从 **MDI/MDIX** 下拉列表中，选择一个选项来指定将接口配置为 MDI（媒体依赖接口）、MDIX（媒体依赖接口的交叉）还是 Auto - MDIX。请注意，MDI/MDIX 设置仅适用于铜接口。

默认情况下， MDI/MDIX 设置为 Auto-MDIX，自动处理 MDI 和 MDIX 之间的交换来建立链路。

步骤 10　在 **MTU** 字段中，键入最大传输单位 (MTU)，它指定允许的最大数据包。

MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

步骤 11　在 **Link Aggregation** 下，有两个选项可用于选择要添加到 LAG 捆绑包的物理接口：

- 选择 **Available Interfaces** 旁的一个或多个接口，然后点击添加选定项图标 ( )。使用 **Ctrl** 或 **Shift** 键选择多个物理接口。
- 要将所有接口对添加到 LAG 捆绑包中，请点击添加所有项图标 ( )。

提示　要从 LAG 捆绑包移除物理接口，请选择一个或多个物理接口，并点击移除选定项图标 ( )。要从 LAG 捆绑包移除所有物理接口，请点击移除所有项图标 ( )。从 Interfaces 选项卡删除 LAG 接口也会移除接口。

步骤 12　从 **Load-Balancing Algorithm** 下拉列表中选择支持您的部署方案的选项。有关详情，请参见第 8-2 页上的指定负载均衡算法。

步骤 13　从 **Link Selection Policy** 下拉列表中选择支持您的部署方案的选项：Highest Port Count（冗余）、Highest Total Bandwidth（速度）、Stable（维护链路状态下没有额外更改）或者 LACP Priority（自动链路汇聚）。

如果选择 **LACP Priority**，则需要为 **System Priority** 分配一个值。然后，需要点击 **Configure Interface Priority** 链路为 LAG 中的每个接口分配一个优先级值。可指定 0 到 65535 之间的任意数字。如果未指定值，则默认优先级是 32768。有关详情，请参见第 8-3 页上的指定链路选择策略。

注　在 FireSIGHT 系统设备与第三方网络设备之间配置汇聚接口时，请选择 **LACP Priority**。

步骤 14　从 **Tunnel Level** 下拉列表中选择支持您的部署方案的选项（可以是 **Inner** 或 **Outer**）。

请注意，在配置第 3 层负载均衡时，隧道级别仅适用于 IPv4 流量。外部隧道始终用于第 2 层和 IPv6 流量。如果没有显式设置 **Tunnel Level**，则默认值为 **Outer**。

步骤 15　在 **LACP** 下，选择 **Enabled** 复选框，允许交换 LAG 接口使用链路汇聚控制协议处理流量。有关详情，请参见第 8-4 页上的配置 LACP。

如果清除此复选框，则 LAG 接口成为静态配置，并且 FireSIGHT 系统将使用为汇聚选定的所有物理接口。

步骤 16　选择 **Rate** 单选按钮，设置确定从合作设备接收 LACP 控制消息的频率。

- 选择 **Slow**，以每隔 30 秒钟接收数据包。
- 选择 **Fast**，以每隔 1 秒钟接收数据包。

步骤 17　选择 **Mode** 单选按钮，以建立设备的侦听模式。

- 选择 **Active** 发起与远程链路的协商，方式是将 LACP 数据包发送给合作设备。
- 选择 **Passive** 对接收到的 LACP 数据包做出响应。

步骤 18　点击 **Save**。

交换 LAG 接口配置成功。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 4-22 页上的对设备应用更改。

添加汇聚路由接口

许可证：可控性

受支持的设备：3 系列

您可以将受管设备上的两个和八个物理端口结合起来创建路由 LAG 接口。必须先向虚拟路由器分配路由 LAG 接口，然后其才能路由流量。受管设备可支持多达 14 个 LAG 接口。

可向路由 LAG 接口添加静态地址解析协议 (ARP) 条目。当外部主机要将流量发送到本地网络上的目标 IP 地址时，如果其需要知道该目标 IP 地址的 MAC 地址，它将发送 ARP 请求。配置静态 ARP 条目时，虚拟路由器会使用 IP 地址和关联的 MAC 地址做出响应。

请注意，为路由 LAG 接口禁用 **ICMP Enable Responses** 选项不会在所有情景下都阻止 ICMP 响应。可向访问控制策略添加规则，以丢弃目标 IP 为路由接口 IP 且协议为 ICMP 的数据包；请参阅第 15-1 页上的使用基于网络的规则控制流量。

如您在受管设备上启用 **Inspect Local Router Traffic** 选项，则该设备在数据包到达主机之前将其丢弃，从而阻止所有响应。有关检查本地路由器流量的详细信息，请参阅第 4-47 页上的了解高级设备设置。

注意事项　更改最大传输单位 (MTU) 会中断设备上的流量并造成丢包。 MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

要编辑现有路由 LAG 接口，请点击接口旁的编辑图标 ( )。

要配置路由 LAG 接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　点击要配置路由 LAG 接口所在设备旁的编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　从 **Add** 下拉菜单中选择 **Add Logical Interface**。

步骤 4　点击 **Routed** 以显示路由 LAG 接口选项。

步骤 5　或者，从 **Security Zone** 下拉列表中，选择现有安全区域或选择 **New** 以添加新的安全区域。

步骤 6　必须从 **Virtual Router** 下拉列表中选择现有虚拟路由器或选择 **New** 以添加新的虚拟路由器。

注　如果添加新的虚拟路由器，则必须在设置路由接口后，在 Device Management 页面的 Virtual Routers 选项卡 **(Devices > Device Management > Virtual Routers)** 上配置该虚拟路由器。请参阅第 7-8 页上的添加虚拟路由器。

步骤 7　选择 **Enabled** 复选框，以允许路由 LAG 接口处理流量。

如果清除此复选框，接口将被禁用，用户将因安全原因无法对其进行访问。

步骤 8　从 **Mode** 下拉列表中选择一个选项来指定链路模式，或者选择 **Autonegotiation** 来指定将 LAG 接口配置为自动协商速度和双工设置。请注意，模式设置仅适用于铜接口。

注　8000 系列设备上的接口不支持半双工选项。当链路自动协商速度时，根据相同的速度设置为 LAG 选择所有活动链路。

步骤 9　从 **MDI/MDIX** 下拉列表中选择一个选项来指定是为 MDI（介质相关接口）、MDIX（介质相关接口交叉）还是 Auto-MDIX 配置 LAG 接口。请注意，MDI/MDIX 设置仅适用于铜接口。

通常， MDI/MDIX 会设置为 Auto-MDIX，此选项可自动处理 MDI 与 MDIX 之间的切换以获得链路。

步骤 10　在 **MTU** 字段中，键入最大传输单位 (MTU)，它指定允许的最大数据包。请注意， MTU 是第 2 层 MTU/MRU，而非第 3 层 MTU。

MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

步骤 11　选择 **ICMP** 旁的 **Enable Responses** 复选框，以使 LAG 接口可以对 ICMP 流量（例如 ping 和 traceroute）做出响应。

步骤 12　选择 **IPv6 NDP** 旁的 **Enable Router Advertisement** 复选框，以使 LAG 接口可以广播路由通告。

步骤 13　要添加 IP 地址，请点击 **Add**。

系统将显示 Add IP Address 弹出窗口。

步骤 14　在 **Address** 字段中，使用 CIDR 表示法键入路由 LAG 接口的 IP 地址和子网掩码。请注意：

- 不能添加网络和广播地址，或静态 MAC 地址 00:00:00:00:00:00 和 FF:FF:FF:FF:FF:FF。
- 无论子网掩码如何，均不能将多个相同的 IP 地址添加至虚拟路由器的接口。

步骤 15　或者，如果贵组织使用 IPv6 地址，请选择 **IPv6** 字段旁的 **Address Autoconfiguration** 复选框，以自动设置 LAG 接口的 IP 地址。

步骤 16　对于 **Type**，选择 Normal 或 SFRP。

有关 SFRP 选项，请参阅第 7-6 页上的配置 SFRP 以了解详细信息。

步骤 17　点击 **OK**。

IP 地址添加成功。

要编辑 IP 地址，请点击编辑图标 ( )。要删除 IP 地址，请点击删除图标 ( )。

注　在为集群设备的路由接口添加 IP 地址时，必须向对等集群的路由接口添加相应的 IP 地址。

步骤 18　要添加静态 ARP 条目，请点击 **Add**。

系统将显示 Add Static ARP Entry 弹出窗口。

步骤 19　在 **IP Address** 字段中，键入静态 ARP 条目的 IP 地址。

步骤 20　在 **MAC Address** 字段中，键入与该 IP 地址关联的 MAC 地址。使用标准格式 （即用冒号隔开的六组两位十六进制数字）输入地址 （例如， 01:23:45:67:89:AB）。

步骤 21　点击 **OK**。

静态 ARP 条目添加成功。

提示　要编辑静态 ARP 条目，请点击编辑图标 ( )。要删除静态 ARP 条目，请点击删除图标 ( )。

步骤 22　在 **Link Aggregation** 下，有两个选项可用于选择要添加到 LAG 捆绑包的物理接口：

- 选择 **Available Interfaces** 旁的一个或多个接口，然后点击添加选定项图标 ( )。使用 **Ctrl** 或 **Shift** 键选择多个物理接口。
- 要将所有接口对添加到 LAG 捆绑包中，请点击添加所有项图标 ( )。

提示　要从 LAG 捆绑包移除物理接口，请选择一个或多个物理接口，并点击移除选定项图标 ( )。要从 LAG 捆绑包移除所有物理接口，请点击移除所有项图标 ( )。从 Interfaces 选项卡删除 LAG 接口也会移除接口。

步骤 23　从 **Load-Balancing Algorithm** 下拉列表中选择支持您的部署方案的选项。有关详情，请参见第 8-2 页上的指定负载均衡算法。

步骤 24　从 **Link Selection Policy** 下拉列表中选择支持您的部署方案的选项：Highest Port Count（冗余）、Highest Total Bandwidth（速度）、Stable（维护链路状态下没有额外更改）或者 LACP Priority（自动链路汇聚）。

如果选择 **LACP Priority**，则需要为 **System Priority** 分配一个值。然后，需要点击 **Configure Interface Priority** 链路为 LAG 中的每个接口分配一个优先级值。可指定 0 到 65535 之间的任意数字。如果未指定值，则默认优先级是 32768。有关详情，请参见第 8-3 页上的指定链路选择策略。

注　在 FireSIGHT 系统设备与第三方网络设备之间配置汇聚接口时，请选择 **LACP Priority**。

步骤 25　从 **Tunnel Level** 下拉列表中选择支持您的部署方案的选项（可以是 **Inner** 或 **Outer**）。

请注意，在配置第 3 层负载均衡时，隧道级别仅适用于 IPv4 流量。外部隧道始终用于第 2 层和 IPv6 流量。如果没有显式设置 **Tunnel Level**，则默认值为 **Outer**。

步骤 26　在 **LACP** 下，选择 **Enabled** 复选框，允许交换 LAG 接口使用链路汇聚控制协议处理流量。有关详情，请参见第 8-4 页上的配置 LACP。

如果清除此复选框，LAG 接口成为静态配置，并且 FireSIGHT 系统会将所有物理接口用于汇聚。

步骤 27　选择 **Rate** 单选按钮，设置确定从合作设备接收 LACP 控制消息的频率。

- 选择 **Slow**，以每隔 30 秒钟接收数据包。
- 选择 **Fast**，以每隔 1 秒钟接收数据包。

步骤 28　选择 **Mode** 单选按钮，以建立设备的侦听模式。

- 选择 **Active** 发起与远程链路的协商，方式是将 LACP 数据包发送给合作设备。
- 选择 **Passive** 对接收到的 LACP 数据包做出响应。

步骤 29　点击 **Save**。

路由 LAG 接口配置成功。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

添加逻辑汇聚接口

许可证：可控性

受支持的设备：3 系列

对于每个交换或路由汇聚接口，均可添加多个逻辑接口。必须将每个逻辑 LAG 接口与 VLAN 标记相关联，以处理 LAG 接口接收的带有该特定标记的流量。将逻辑接口添加到交换或路由汇聚接口的方式与将逻辑接口添加到物理交换或路由接口的方式相同。

注　当创建 LAG 接口时，默认情况下也会创建“未加标记的”逻辑接口。该逻辑接口用 **lag*n.0*** 标签进行识别，其中 ***n*** 是 0 到 13 之间的一个整数。每个 LAG 至少需要一个这样的逻辑接口才起作用。您可以将额外的逻辑接口与任何 LAG 相关联以处理 VLAN 标记的流量。每个额外逻辑接口都需要唯一的 VLAN 标记。 FireSIGHT 系统支持范围在 1 到 4094 之间的 VLAN 标记。

您也可以在逻辑路由接口上配置 SFRP。有关详情，请参见第 7-6 页上的配置 SFRP。

请注意，为逻辑路由接口禁用 **ICMP Enable Responses** 选项不会在所有情景下都阻止 ICMP 响应。可向访问控制策略添加规则，以丢弃目标 IP 为路由接口 IP 且协议为 ICMP 的数据包；请参阅第 15-1 页上的使用基于网络的规则控制流量。

如您在受管设备上启用 **Inspect Local Router Traffic** 选项，则该设备在数据包到达主机之前将其丢弃，从而阻止所有响应。有关检查本地路由器流量的详细信息，请参阅第 4-47 页上的了解高级设备设置。

注意事项　如果更改最大传输单位 (MTU)，则将中断设备上已路由或已交换的流量，并丢弃数据包。 MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

要编辑现有逻辑 LAG 接口，请点击接口旁的编辑图标 ( )。

要添加逻辑 LAG 接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　点击要添加逻辑 LAG 接口所在设备旁的编辑图标 ( )。

系统将显示 Interfaces 选项卡。

步骤 3　从 **Add** 下拉菜单中，选择 **Add Logical Interface**。

系统将显示 Add Interface 弹出窗口。

步骤 4　点击 **Switched** 显示交换接口选项，或者选择 **Routed** 显示路由接口选项。

当为 LAG 创建逻辑接口时，您从 **Interface** 下拉列表中选择可用的 LAG。汇聚接口用 **lag*n*** 标签进行识别，其中 ***n*** 是 0 到 13 之间的一个整数。

有关将逻辑接口添加到交换接口的详细信息，请参阅第 6-3 页上的添加逻辑交换接口。

有关将逻辑接口添加到路由接口的详细信息，请参阅第 7-4 页上的添加逻辑路由接口。

注　当汇聚接口被禁用时，与汇聚接口关联的逻辑接口也被禁用。

查看汇聚接口统计数据

许可证：可控性

受支持的设备：3 系列

您可以查看每个汇聚接口的协议和流量统计数据。统计数据显示 LACP 协议信息，例如 LACP 密钥和合作伙伴信息、接收的数据包、数据包发射器和丢弃的数据包。每个成员接口均可进一步优化统计数据，以按每端口显示流量和链路信息。

汇聚接口信息还通过预定义的控制面板构件提供给控制面板。 Current Interface Status 构件显示设备上所有接口的状态：已启用或未使用。 Interface Traffic 构件显示设备接口上在控制面板时间范围内的接收流量速率 (Rx) 和传输流量速率 (Tx)。请参阅第 55-6 页上的了解预定义构件。

要查看汇聚接口统计数据，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　点击要查看逻辑汇聚接口统计数据所在设备旁的编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击要查看接口统计数据所在接口旁的视图图标 ( )。

系统将显示 Statistics 弹出窗口。

步骤 4　点击 **OK** 关闭该窗口。

删除汇聚接口

许可证：可控性

受支持的设备：3 系列

以下操作步骤说明如何删除汇聚接口。

要删除汇聚接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　点击要删除汇聚接口所在设备旁的编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击要删除的汇聚接口旁的删除图标 ( )。

此汇聚接口可以使用 ***lagn*** 标签进行识别，其中 ***n*** 可以是 0 到 13 之间的一个整数。

步骤 4　当出现提示时，请确认要删除汇聚接口。

接口删除成功。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

设置混合接口

在使 FireSIGHT 系统在虚拟路由器与虚拟交换机之间桥接流量的受管设备上，可配置逻辑混合接口。如果虚拟交换机接口收到的 IP 流量发送至关联混合逻辑接口的 MAC 地址，则系统将其作为第 3 层流量处理，并根据目标 IP 地址对该流量进行路由或做出响应。如果系统收到任何其他流量，则将其作为第 2 层流量处理，并对其进行适当交换。您不能在虚拟受管设备或用于 Blue Coat X-系列的思科 NGIPS上配置逻辑混合接口。

有关设置混合接口的详细信息，请参阅第 9-1 页上的添加逻辑混合接口。

添加逻辑混合接口

许可证：可控性

受支持的设备：3 系列

如要桥接第 2 层和第 3 层之间的流量，您必须将逻辑混合接口与虚拟路由器和虚拟交换机相关联。您只能将单个混合接口与虚拟交换机关联。但是，您能将多个混合接口与虚拟路由器关联。

您也可以在逻辑混合接口上配置 SFRP。有关详情，请参见第 7-6 页上的配置 SFRP。

请注意，禁用混合接口的 **ICMP Enable Responses** 选项并不会阻止所有情形下的 ICMP 响应。您可向访问控制策略添加规则，在目标 IP 为混合接口 IP 且协议为 ICMP 时丢弃数据包；请参阅第 15-1 页上的使用基于网络的规则控制流量。

如您在受管设备上启用 **Inspect Local Router Traffic** 选项，则该设备在数据包到达主机之前将其丢弃，从而阻止所有响应。有关检查本地路由器流量的详细信息，请参阅第 4-47 页上的了解高级设备设置。

注意事项 如果更改最大传输单位 (MTU)，则将中断设备上已路由或已交换的流量，并丢弃数据包。 MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

要编辑现有混合接口，请点击接口旁的编辑图标 ( )。

要添加逻辑混合接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1 选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2 在要向其添加混合接口的设备旁，点击编辑图标 ( )。

系统将显示 Interfaces 选项卡。

步骤 3　从 **Add** 下拉菜单中，选择 **Add Logical Interface**。

系统将显示 Add Interface 弹出窗口。

步骤 4　点击 **Hybrid**，系统将显示混合接口选项。

步骤 5　在 **Name** 字段中，键入接口名称。可使用字母数字字符和空格。

步骤 6　从 **Virtual Router** 下拉列表中选择一个现有虚拟路由器，选择 **None**，或选择 **New** 以添加新虚拟路由器。

请注意，如果添加新虚拟路由器，在完成混合接口设置之后，必须在 Device Management 页面 **(Devices > Device Management> Virtual Routers)** 上配置该虚拟路由器。请参阅第 7-8 页上的添加虚拟路由器。

步骤 7　从 **Virtual Router** 下拉列表中选择一个现有虚拟交换机，选择 **None**，或选择 **New** 以添加新虚拟交换机。

请注意，如果添加新虚拟交换机，在完成混合接口设置之后，必须在 Device Management 页面 **(Devices > Device Management> Virtual Switches)** 上配置该虚拟交换机。请参阅第 6-5 页上的添加虚拟交换机。

步骤 8　选择 **Enabled** 复选框，以使混合接口处理流量。

如清除此复选框，则将禁用并强制性断开该接口。

步骤 9　在 **MTU** 字段中，键入最大传输单位 (MTU)，它指定允许的最大数据包。

MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。有关详情，请参见第 4-56 页上的配置感应接口 MTU。

步骤 10　在 **ICMP** 旁，选择 **Enable Responses** 复选框，以使接口对 ICMP 流量（例如 ping 和 traceroute）做出响应。

步骤 11　在 **IPv6 NDP** 旁，选择 **Enable Router Advertisement** 复选框，以使接口广播路由器通告。

只有添加了 IPv6 地址，才能选择此选项。

步骤 12　要添加 IP 地址，请点击 **Add**。

系统将显示 Add IP Address 弹出窗口。

步骤 13　在 **Address** 字段中，键入 IP 地址和子网掩码。请注意：

- 不能添加网络和广播地址，或静态 MAC 地址 00:00:00:00:00:00 和 FF:FF:FF:FF:FF:FF。
- 无论子网掩码如何，均不能将多个相同的 IP 地址添加至虚拟路由器的接口。

步骤 14　或者，如果您有 IPv6 地址，请在 **IPv6** 字段旁边，选择 **Address Autoconfiguration** 复选框，以自动设置接口的 IP 地址。

步骤 15　对于 **Type**，选择 Normal 或 SFRP。

有关 SFRP 选项，请参阅第 7-6 页上的配置 SFRP 以了解详细信息。

步骤 16　点击 **OK**。

IP 地址添加成功。

提示　要编辑 IP 地址，请点击编辑图标 ( )。要删除 IP 地址，请点击删除图标 ( )。

步骤 17　点击 **Save**。

逻辑混合接口添加成功。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

删除逻辑混合接口

许可证：可控性

受支持的设备：3 系列

以下步骤说明如何删除逻辑混合接口。

要删除混合接口，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要从其中删除混合接口的设备旁，点击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　在要删除的逻辑混合接口旁，点击删除图标 ( )。

步骤 4　出现提示时，请确认要删除接口。

接口删除成功。请注意，只有应用设备配置，更改才会生效；请参阅第 4-22 页上的对设备应用更改。

使用网关 VPN

虚拟专用网络 (VPN) 是一种网络连接，通过诸如 Internet 或其他网络之类公共资源在终端之间建立安全隧道。可将 FireSIGHT 系统配置为在思科受管设备的虚拟路由器之间构建的安全 VPN 隧道。系统利用互联网协议安全 (IPSec) 协议套件建立隧道。

在思科 VPN 部署中，只有思科受管设备可用作终端。不支持第三方终端。

建立 VPN 连接之后，本地网关后台的主机可通过安全 VPN 隧道连接至远程网关后台的主机。连接包括两个网关的 IP 地址和主机名、网关后台的子网以及供两个网关互相进行身份验证的共享密钥。

各 VPN 终端利用 Internet 密钥交换 (IKE) 版本 1 或版本 2 协议相互进行身份验证，为隧道创建安全关联。系统使用 IPSec 身份验证标头 (AH) 协议或 IPSec 封装安全载荷 (ESP) 协议验证进入隧道的数据。除具有与 AH 相同的功能之外， ESP 协议还可以对数据加密。

如果部署中有访问控制策略，系统在通过访问控制前不会发送 VPN 流量。此外，在隧道关闭时，系统不向公共资源发送隧道流量。

为了配置和应用 VPN 部署，必须在每个目标受管设备上启用 VPN 许可证。此外， VPN 功能仅适用于 3 系列设备。

有关创建和管理 VPN 部署的详细信息，请参阅以下各节：

了解 IPSec

IPSec 协议套件定义如何在 ESP 或 AH 安全协议中散列、加密和封装通过 VPN 隧道的 IP 数据包。FireSIGHT 系统使用安全关联 (SA) 的散列算法和加密密钥，安全关联 (SA) 通过 Internet 密钥交换 (IKE) 协议在两个网关之间建立。

安全关联 (SA) 在两台设备之间建立共享安全属性并使 VPN 终端支持安全通信。 SA 可使两个 VPN 终端处理相关参数，确保在两终端之间建立 VPN 隧道。

系统在协商 IPSec 连接的初始阶段，采用 Internet 安全关联与密钥管理协议 (ISAKMP) 在终端建立 VPN 并实现已验证的密钥交换。 IKE 协议驻留在 ISAKMP 之内。有关 IKE 协议的详细信息，请参阅第 10-2 页上的了解 IKE。

AH 安全协议为数据包标头和数据提供保护，但不能对其进行加密。 ESP 为数据包提供加密和保护，但不能保护最外层的 IP 标头。在许多情况下，并不需要此保护，由于 ESP 具有加密功能，大多数 VPN 部署更频繁地使用 ESP，较少使用 AH。由于 VPN 仅在隧道模式运行，因此，在 ESP 协议中，系统从第 3 层向上对整个数据包进行加密和身份验证。在隧道模式下， ESP 可对数据进行加密，并具有 AH 的加密功能。

了解 IKE

FireSIGHT 系统使用 IKE 协议对两个网关共同进行身份验证，并为隧道协商 SA。此流程包含两个阶段。

IKE 阶段 1 通过使用 Diffie - Hellman 密钥交换建立一个安全的经验证通信信道，生成一个预共享密钥对 IKE 通信进行进一步加密。此协商促成一个双向的 ISAKMP 安全关联。系统允许您使用预共享密钥执行身份验证。阶段 1 在主模式中运行，力图在协商期间保护所有数据，同时保护对等体的身份。

在 IKE 阶段 2 中，IKE 对等体使用在阶段 1 中建立的安全隧道代表 IPSec 协商安全关联。此协商促成至少两个单向的安全关联，一个为入站关联，一个为出站关联。

了解 VPN 部署

VPN 部署指定纳入 VPN 的终端和网络及其如何互相连接。配置 VPN 部署之后，可将其应用于受管设备或由另一防御中心管理的设备。

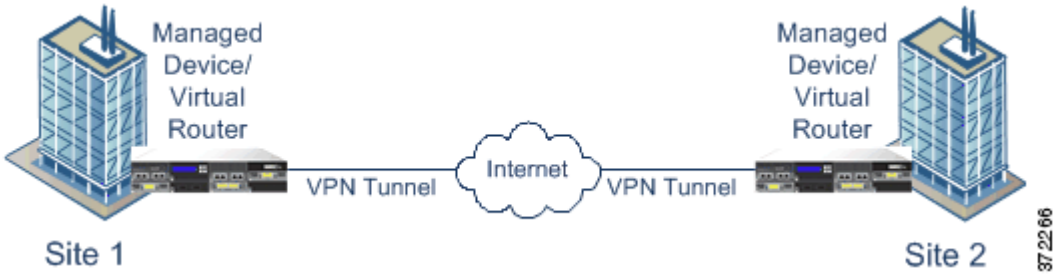
系统支持三类 VPN 部署：点对点、星型和网格。有关这些 VPN 部署的详细信息，请参阅以下各节：

- 第 10-2 页上的了解点对点 VPN 部署
- 第 10-2 页上的了解星型 VPN 部署
- 第 10-3 页上的了解网格 VPN 部署

了解点对点 VPN 部署

在点对点 VPN 部署中，两个终端彼此直接通信。将两个终端配置为对等设备，任一台设备均可启动安全连接。在此配置中，每台设备必须为支持 VPN 的受管设备。

以下图表显示了一个典型点对点 VPN 部署。



有关详情，请参见第 10-5 页上的配置点对点 VPN 部署。

了解星型 VPN 部署

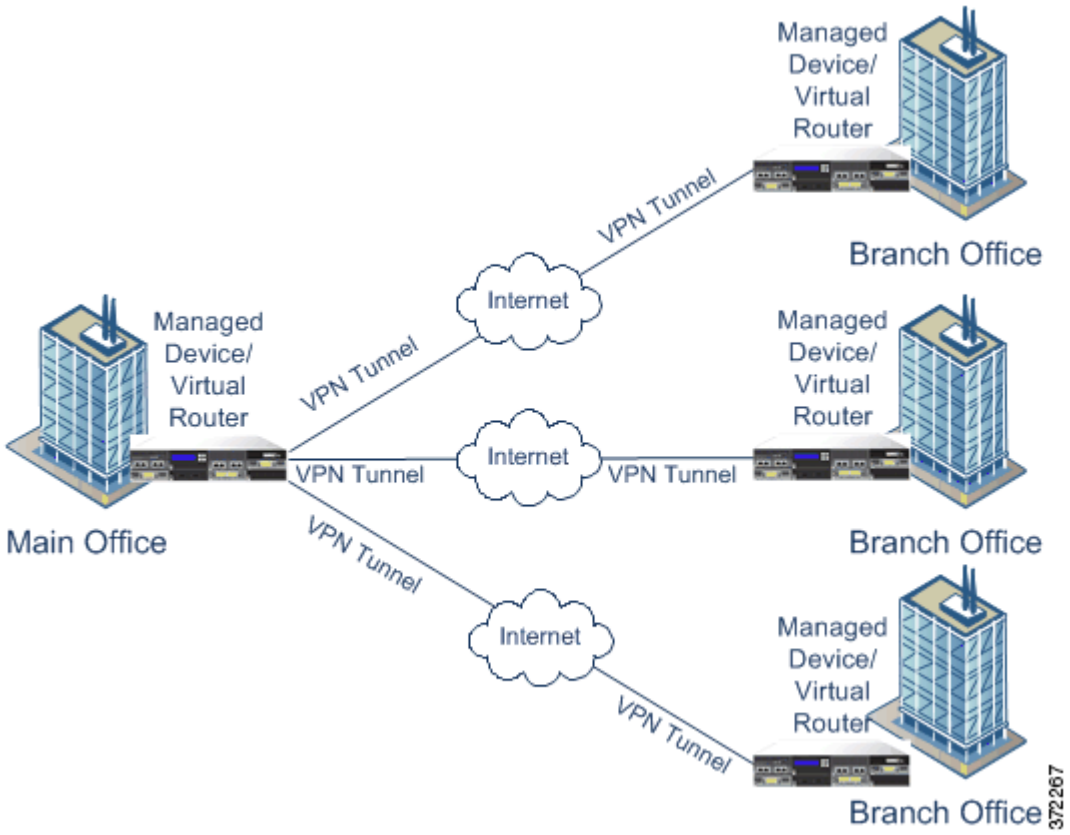
在星型 VPN 部署中，中央终端（集线器节点）建立与多个远程终端（叶节点）的安全连接。集线器节点与每个叶节点之间的每条连接均为独立 VPN 隧道。任何叶节点后台的主机均可通过集线器节点相互通信。

星型部署通常代表通过互联网或其他第三方网络建立安全连接，将公司总部和分公司相连的 VPN。星型 VPN 部署为所有员工提供对公司网络的受控访问权。

在典型星型部署中，集线器节点位于总部。叶节点位于分支机构并发起大部分流量。每个节点均必须属于支持 VPN 的受管设备。

请注意，星型部署仅支持 IKE 第 2 版。

以下图表显示了一个典型的星型 VPN 部署。

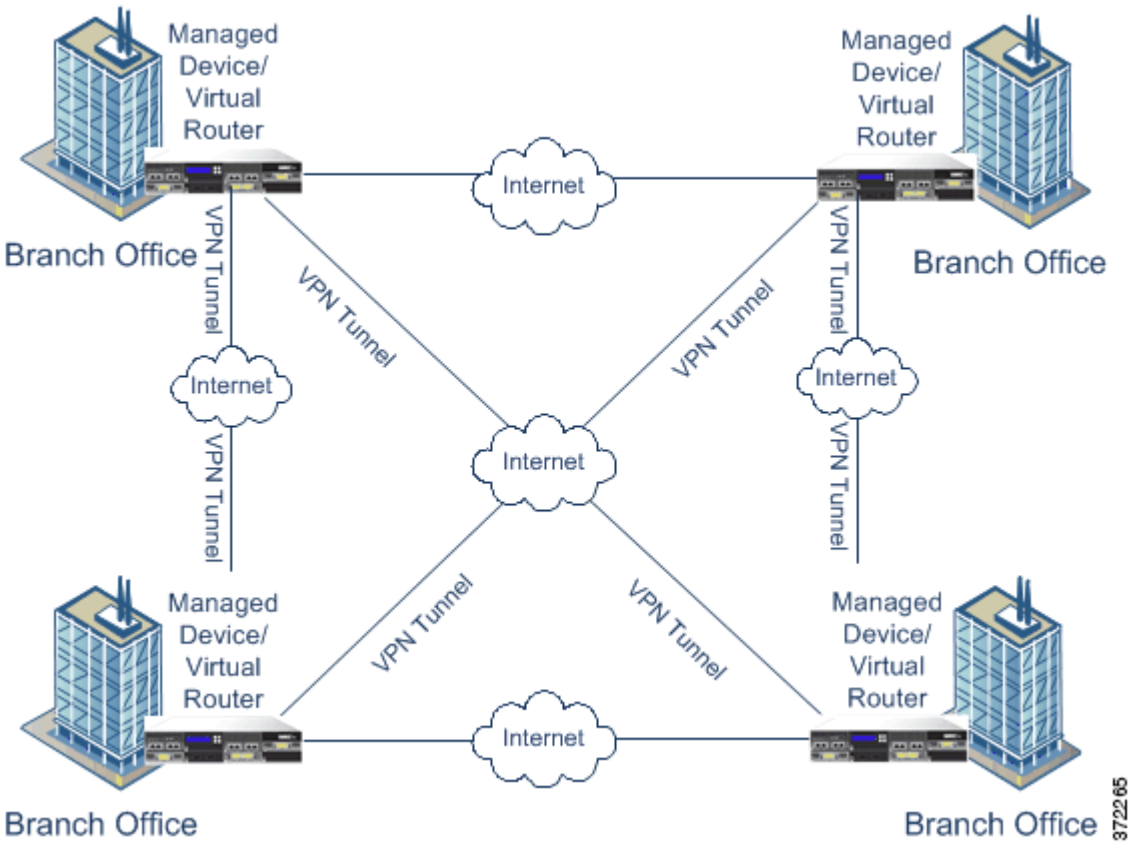


有关详情，请参见第 10-7 页上的配置星型 VPN 部署。

了解网格 VPN 部署

在网格 VPN 部署中，所有终端均可通过单一 VPN 隧道与每个其他终端进行通信。网格部署可保证冗余，以便当一个终端发生故障时，其余终端仍可以互相通网格部署提供冗余节点信。此类部署通常代表连接一组分散式分公司地点的 VPN。在此配置中，所部署的支持 VPN 的受管设备数量取决于所需的冗余级别。每个终端均必须属于支持 VPN 的受管设备。

以下图表显示了典型的网格 VPN 部署。



有关详情，请参见第 10-9 页上的配置网格 VPN 部署。

管理 VPN 部署

许可证：VPN

受支持的设备：3 系列

在 VPN 页面 (**Devices > VPN**) 上，可按名称和部署中所含的终端查看所有当前 VPN 部署。通过此页选项，可查看 VPN 部署的状态、新建部署、应用部署以及编辑或删除部署。

注意事项　向防御中心注册设备时，如果选择默认访问控制策略，则默认访问控制规则将拦截所有流量。如在设备上配置 VPN 部署，部署将失败。

请注意，向防御中心注册设备时，已应用的 VPN 部署将在注册期间同步至防御中心。

下表介绍了可在 VPN 页面上执行的部署管理操作。

表 10-1　　VPN 部署管理操作

要.....	您可以.....
新建 VPN 部署	点击 **Add**。有关详情，请参见第 10-5 页上的配置 VPN 部署。
修改现有 VPN 部署中的设置	点击编辑图标 ( )。有关详情，请参见第 10-5 页上的配置 VPN 部署。
查看现有 VPN 部署的状态	点击状态图标。有关详情，请参见第 10-13 页上的查看 VPN 部署状态。
将 VPN 部署应用于部署中的所有目标设备	点击应用图标 ( )。有关详情，请参见第 10-13 页上的应用 VPN 部署。
删除 VPN 部署	点击删除图标 ( )，然后点击 **Yes**，或在决定不删除部署时，点击 **No**。

配置 VPN 部署

许可证：VPN

受支持的设备：3 系列

新建 VPN 部署时，必须至少为其提供一个唯一名称、指定部署类型并指定预共享密钥。有三类部署可供选择，每类部署均包含一组 VPN 隧道：

- 点对点 (PTP) 部署在两个终端之间建立 VPN 隧道。
- 星型部署建立一组 VPN 隧道连接一个集线器终端与一组叶终端。
- 网格部署在一组终端当中建立一组 VPN 隧道。

在思科 VPN 部署中，只有思科受管设备可用作终端。不支持第三方终端。

必须为 VPN 身份验证定义一个预共享密钥。可指定一个默认密钥，用于在部署中生成的所有 VPN 连接。对于点对点部署，可为每个终端对指定一个预共享密钥。

有关创建每类 VPN 部署的详细信息，请参阅以下各节:

- 第 10-5 页上的配置点对点 VPN 部署
- 第 10-7 页上的配置星型 VPN 部署
- 第 10-9 页上的配置网格 VPN 部署

配置点对点 VPN 部署

许可证：VPN

受支持的设备：3 系列

配置点对点 VPN 部署时，先定义一组终端对，然后在每个终端对的两个节点之间创建 VPN。有关详细信息，请参阅第 10-2 页上的了解点对点 VPN 部署。

以下列表描述了在部署中可以指定的选项。

字段名称

为部署提供一个唯一名称。

类型

点击 **PTP** 表明正在配置点对点部署。

Pre-shared Key

定义一个用于身份验证的唯一预共享密钥。系统会将该密钥用于部署中的所有 VPN，除非为每个终端对指定一个预共享密钥。

设备

可选择一台受管设备，包括设备堆栈或集群，作为部署的终端。对于思科受管设备（不受正在使用的防御中心管理），请选择 **Other**，然后为此终端指定一个 IP 地址。

Virtual Router

如已选定一台受管设备作为终端，请选择一个当前应用于所选设备的虚拟路由器。不能为多个终端选择相同虚拟路由器。

接口

如已选定一台受管设备作为终端，请选择一个已分配给所选虚拟路由器的路由接口。

IP地址

- 如已选定一台受管设备作为终端，请选择一个已分配给所选路由接口的 IP 地址。
- 如果此受管设备为设备集群，则只能从 SFRP IP 地址列表中选择。
- 如已选定一台不受防御中心管理的受管设备，请为终端指定一个 IP 地址。

Protected Networks

在部署中指定已加密的网络。为每个网络输入带 CIDR 块的子网。 IKE 版本 1 仅支持一个受保护的网络。

请注意，VPN 终端不能有相同的 IP 地址，并且 VPN 终端对中的受保护网络不能重叠。如果一个终端的受保护网络列表包含一个或多个 IPv4 或 IPv6 条目，另一个终端的受保护网络必须至少包含一个相同类型的条目（即 IPv4 或 IPv6）。否则，另一个终端的 IP 地址必须为相同类型，且不得与受保护网络中的条目重叠。（对于 IPv4，使用 /32 CIDR 地址块；对于 IPv6 使用 /128 CIDR 地址块）。如果以上两种检查均失败，则此终端对无效。

Internal IP

如果终端驻留在带网络地址转换的防火墙后面，请选择此复选框。

Public IP

如已选择 **Internal IP**，请指定防火墙的公用 IP 地址。如果终端为响应方，必须指定此值。

Public IKE Port

如已选择 **Internal IP**，请为防火墙上要端口转发至到内部终端的 UDP 端口指定一个介于 1 与 65535 之间的数值。如果终端为响应方，且防火墙上正在转发的端口不是 500 或 4500，必须指定此值。

Use Deployment Key

选择此复选框，可使用为部署定义的预共享密钥。清除此复选框，可为此终端对指定用于 VPN 身份验证的预共享密钥。

Pre-shared Key

如已清除 **Use Deployment Key** 复选框，请在此字段中指定一个预共享密钥。

提示　要编辑现有点对点部署，请点击部署旁边的编辑图标 ( )。在最初保存部署之后，不能编辑部署类型。两个用户不应同时编辑同一部署；然而，请注意，网络界面不会阻止同时编辑。

要配置点对点 VPN 部署，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > VPN**。

系统将显示 VPN 页面。

步骤 2　点击 **Add**。

系统将显示 Create New VPN Deployment 弹出窗口。

步骤 3　为部署提供一个唯一**名称**。

可使用所有可打印字符，包括空格和特殊字符。

步骤 4　确保 **PTP** 已选作 **Type**。

步骤 5　为部署提供一个唯一的 **Pre-shared Key**。

步骤 6　点击 **Node Pairs** 旁边的添加图标 ( )。

系统将显示 Add New Endpoint Pair 弹出窗口。

步骤 7　配置 VPN 部署，如本节前面所述。

步骤 8　点击 **Node A** 下方的 **Protected Networks** 旁边的添加图标 ( )。

系统将显示 Add Network 弹出窗口。

步骤 9　为受保护网络键入一个 CIDR 块。

步骤 10　点击 **OK**。

受保护网络添加成功。

步骤 11　针对 **Node B** 重复第 10 步至第 8 步。

步骤 12　点击 **Save**。

终端对已添加至部署中，系统再次显示 Create New VPN Deployment 弹出窗口。

步骤 13　点击 **Save** 完成部署配置，系统再次显示 VPN 页面。

请注意，只有应用部署才能使其生效；请参阅第 10-13 页上的应用 VPN 部署。

配置星型 VPN 部署

许可证：VPN

受支持的设备：3 系列

配置星型 VPN 部署时，需定义一个集线器节点终端和一组叶节点终端。必须定义集线器节点终端和至少一个叶节点终端才能配置部署。有关详细信息，请参阅第 10-2 页上的了解星型 VPN 部署。

以下列表描述了在部署中可以指定的选项。

字段名称

为部署提供一个唯一名称。

类型

单击 **Star** 指定正在配置星型部署。

Pre-shared Key

定义一个用于身份验证的唯一预共享密钥。

设备

可选择一台受管设备，包括设备堆栈或集群，作为部署的终端。对于思科受管设备（不受正在使用的防御中心管理），请选择 **Other**，然后为此终端指定一个 IP 地址。

Virtual Router

如已选定一台受管设备作为终端，请选择一个当前应用于所选设备的虚拟路由器。不能为多个终端选择相同虚拟路由器。

接口

如已选定一台受管设备作为终端，请选择一个已分配给所选虚拟路由器的路由接口。

IP地址

- 如已选定一台受管设备作为终端，请选择一个已分配给所选路由接口的 IP 地址。
- 如果此受管设备为设备集群，则只能从 SFRP IP 地址列表中选择。
- 如已选定一台不受防御中心管理的受管设备，请为终端指定一个 IP 地址。

Protected Networks

在部署中指定已加密的网络。为每个网络输入带 CIDR 块的子网。

请注意，VPN 终端不能有相同的 IP 地址，并且 VPN 终端对中的受保护网络不能重叠。如果一个终端的受保护网络列表包含一个或多个 IPv4 或 IPv6 条目，另一个终端的受保护网络必须至少包含一个相同类型的条目（即 IPv4 或 IPv6）。否则，另一个终端的 IP 地址必须为相同类型，且不得与受保护网络中的条目重叠。（对于 IPv4，使用 /32 CIDR 地址块；对于 IPv6 使用 /128 CIDR 地址块）。如果以上两种检查均失败，则此终端对无效。

Internal IP

如果终端驻留在带网络地址转换的防火墙后面，请选择此复选框。

Public IP

如已选择 **Internal IP**，请指定防火墙的公用 IP 地址。如果终端为响应方，必须指定此值。

Public IKE Port

如已选择 **Internal IP**，请为防火墙上要端口转发至到内部终端的 UDP 端口指定一个介于 1 与 65535 之间的数值。如果终端为响应方，且防火墙上正在转发的端口不是 500 或 4500，必须指定此值。

提示 要编辑现有星形部署，请点击部署旁边的编辑图标 ( )。在最初保存部署之后，不能编辑部署类型。要更改部署类型，必须删除部署并新建一个部署。两个用户不应同时编辑同一部署；然而，请注意，网络界面不会阻止同时编辑。

要配置星型部署，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > VPN**。

系统将显示 VPN 页面。

步骤 2　点击 **Add**。

系统将显示 Create New VPN Deployment 弹出窗口。

步骤 3　为部署提供一个唯一**名称**。

可使用所有可打印字符，包括空格和特殊字符。

步骤 4　点击 **Star** 以指定 **Type**。

步骤 5　为部署提供一个唯一的 **Pre-shared Key**。

步骤 6　点击 **Hub Node** 旁边的添加图标 ( )。

系统将显示 Add Hub Node 弹出窗口。

步骤 7　配置 VPN 部署，如本节前面所述。

步骤 8　点击 **Protected Networks** 旁边的添加图标 ( )。

系统将显示 Add Network 弹出窗口。

步骤 9　为受保护网络键入 IP 地址。

步骤 10　点击 **OK**。

受保护网络添加成功。

步骤 11　点击 **Save**。

集线器节点已添加至部署，系统再次显示 Create New VPN Deployment 弹出窗口。

步骤 12　点击 **Leaf Nodes** 旁边的添加图标 ( )。

系统将显示 Add Leaf Node 弹出窗口。

步骤 13　重复第 7 步至第 10 步完成叶节点，该节点具有与集线器节点相同的选项。

步骤 14　点击 **Save**。

叶节点已添加至部署，系统再次显示 Create New VPN Deployment 弹出窗口。

步骤 15　点击 **Save** 完成部署配置，系统再次显示 VPN 页面。

请注意，只有应用部署才能使其生效；请参阅第 10-13 页上的应用 VPN 部署。

配置网格 VPN 部署

许可证：VPN

受支持的设备：3 系列

配置网格 VPN 部署时，需定义一组 VPN 以连接一组特定终端的任何两点。有关详细信息，请参阅第 10-3 页上的了解网格 VPN 部署。

以下列表描述了在部署中可以指定的选项。

字段名称

为部署提供一个唯一名称。

类型

点击 **Mesh** 指定正在配置网格部署。

Pre-shared Key

定义一个用于身份验证的唯一预共享密钥。

设备

可选择一台受管设备，包括设备堆栈或集群，作为部署的终端。对于思科受管设备（不受正在使用的防御中心管理），请选择 **Other**，然后为此终端指定一个 IP 地址。

Virtual Router

如已选定一台受管设备作为终端，请选择一个当前应用于所选设备的虚拟路由器。不能为多个终端选择相同虚拟路由器。

接口

如已选定一台受管设备作为终端，请选择一个已分配给所选虚拟路由器的路由接口。

IP地址

- 如已选定一台受管设备作为终端，请选择一个已分配给所选路由接口的 IP 地址。
- 如果此受管设备为设备集群，则只能从 SFRP IP 地址列表中选择。
- 如已选定一台不受防御中心管理的受管设备，请为终端指定一个 IP 地址。

Protected Networks

在部署中指定已加密的网络。为每个网络输入带 CIDR 块的子网。 IKE 版本 1 仅支持一个受保护的网络。

请注意，VPN 终端不能有相同的 IP 地址，并且 VPN 终端对中的受保护网络不能重叠。如果一个终端的受保护网络列表包含一个或多个 IPv4 或 IPv6 条目，另一个终端的受保护网络必须至少包含一个相同类型的条目（即 IPv4 或 IPv6）。否则，另一个终端的 IP 地址必须为相同类型，且不得与受保护网络中的条目重叠。（对于 IPv4，使用 /32 CIDR 地址块；对于 IPv6 使用 /128 CIDR 地址块）。如果以上两种检查均失败，则此终端对无效。

Internal IP

如果终端驻留在带网络地址转换的防火墙后面，请选择此复选框。

Public IP

如已选择 **Internal IP**，请指定防火墙的公用 IP 地址。如果终端为响应方，必须指定此值。

Public IKE Port

如已选择 **Internal IP**，请为防火墙上要端口转发至到内部终端的 UDP 端口指定一个介于 1 与 65535 之间的数值。如果终端为响应方，且防火墙上正在转发的端口不是 500 或 4500，必须指定此值。

提示　要编辑现有网格部署，请点击此部署旁边的编辑图标 ( )。在最初保存部署之后，不能编辑部署类型。要更改部署类型，必须删除部署并新建一个部署。两个用户不应同时编辑同一部署；然而，请注意，网络界面不会阻止同时编辑。

要配置网格 VPN 部署，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > VPN**。

系统将显示 VPN 页面。

步骤 2　点击 **Add**。

系统将显示 Create New VPN Deployment 弹出窗口。

步骤 3　为部署提供一个唯一**名称**。

可使用所有可打印字符，包括空格和特殊字符。

步骤 4　点击 **Mesh** 以指定 **Type**。

步骤 5　为部署提供一个唯一的 **Pre-shared Key**。

步骤 6　点击 **Nodes** 旁边的添加图标 ( )。

系统将显示 Add Endpoint 弹出窗口。

步骤 7　配置 VPN 部署，如本节前面所述。

步骤 8　点击 **Protected Networks** 旁边的添加图标 ( )。

系统将显示 Add Network 弹出窗口。

步骤 9　为受保护网络键入一个 CIDR 块。

步骤 10　点击 **OK**。

受保护网络添加成功。

步骤 11　点击 **Save**。

终端已添加至部署，系统再次显示 Create New VPN Deployment 弹出窗口。

步骤 12　重复第 6 步至第 11 步，添加更多终端。

步骤 13　点击 **Save** 完成部署，系统再次显示 VPN 页面。

请注意，只有应用部署才能使其生效；请参阅第 10-13 页上的应用 VPN 部署。

配置高级 VPN 部署设置

许可证：VPN

受支持的设备：3 系列

VPN 部署包含可在部署的 VPN 中共享的一些常见设置。每个 VPN 均可使用默认设置，也可覆盖这些默认设置。高级设置通常只需要很少的修改或者不需要修改，不通用于各个部署。

以下列表描述了在部署中可指定的高级选项。

Other Algorithm Allowed

选择此复选框可对算法列表中未列出、但远程对等体拟用的算法启用自动协商。

Algorithm

在部署中指定第一阶段和第二阶段算法方案以保护数据。为两个阶段选择 **Cipher**、**Hash** 和 Diffie - Hellman (**DH**) 组身份验证消息。

IKE Life Time

指定一个数值并为最大 IKE SA 重新协商间隔选择一个时间单位。可以指定最短 15 分钟和最长 30 天。

IKE v2

选择此复选框，可指定系统使用 IKE 版本 2。此版本支持星型部署和多个受保护网络。

Life Time

指定一个数值并为最大 SA 重新协商间隔选择一个时间单位。可以指定最短 5 分钟和最长 24 小时。

Life Packets

指定在 IPsec SA 到期前可通过其传输的数据包的数量。可以使用 0 到 18446744073709551615 之间的任意整数。

Life Bytes

指定在 IPsec SA 到期前可通过其传输的字节数。可以使用 0 到 18446744073709551615 之间的任意整数。

AH

选择此复选框，可指定系统使用身份验证报头安全协议，以保护数据。清除此复选框，可使用加密服务有效载荷 (ESP) 协议。有关何时使用每个协议的指南，请参阅第 10-1 页上的了解 IPSec。

要配置高级 VPN 部署设置，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > VPN**。

系统将显示 VPN 页面。

步骤 2　点击 **Add**。

系统将显示 Create New VPN Deployment 弹出窗口。

步骤 3　点击 **Advanced** 选项卡。

步骤 4　配置高级设置，如本节前面所述。

步骤 5　点击 **Algorithms** 旁边的添加图标 ( )。

系统将显示 Add IKE Algorithm Proposal 弹出窗口。

步骤 6　为两个阶段选择 **Cipher**、 **Hash** 和 Diffie - Hellman (**DH**) 组身份验证消息。

步骤 7　点击 **OK**。

IKE 算法方案添加成功。

步骤 8　点击 **Save**。

更改已保存，系统将显示 VPN 页面。

请注意，只有应用部署才能使其生效；请参阅第 10-13 页上的应用 VPN 部署。

应用 VPN 部署

许可证：VPN

受支持的设备：3 系列

在配置 VPN 部署或对 其做出任何更改之后，必须将此部署应用于一台或多台设备，以实施为此部署指定的设置。

要应用 VPN 部署，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > VPN**。

系统将显示 VPN 页面。

步骤 2　点击要应用的 VPN 部署旁边的应用图标 ( )。

步骤 3　提示时点击 **Yes**。

VPN 部署应用成功。

提示　或者，从 Apply VPN Deployment 对话框，点击 **View Changes**。 VPN Comparison View 页面在一个新的浏览器窗口中显示。有关详细信息，请参阅第 10-16 页上的使用 VPN 部署对比视图。

步骤 4　点击 **OK**。

系统返回 VPN 页面。

查看 VPN 部署状态

许可证：VPN

受支持的设备：3 系列

配置 VPN 部署之后，可查看已配置的 VPN 隧道的状态。 VPN 页面将针对每个已应用 VPN 部署显示状态图标：

- ( ) 图标表示所有 VPN 终端均已启用。
- ( ) 图标表示所有 VPN 终端均已关闭。
- ( ) 图标表示部分终端已启用，部分终端已关闭。

可点击状态图标，以查看部署状态及部署中终端的基本信息，如终端名称和 IP 地址。 VPN 状态每分钟更新一次，或在发生状态变化时更新，例如终端关闭或启用。

要查看 VPN 状态，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > VPN**。

系统将显示 VPN 页面。

步骤 2　点击要查看其状态的部署旁边的 VPN 状态图标。

系统将显示 VPN Status 弹出窗口。

步骤 3　点击 **OK** 返回 VPN 页面。

查看 VPN 统计数据和日志

许可证：VPN

受支持的设备：3 系列

配置 VPN 部署之后，可查看有关横越已配置 VPN 隧道的统计数据。此外，还可查看每个终端的最新 VPN 系统和 IKE 日志。

系统将显示以下统计信息。

终端

到路由接口的设备路径和指定为 VPN 终端的 IP 地址。

状态

VPN 连接处于启用还是禁用状态。

协议

用于加密的协议， ESP 或 AH。

Packets Received

在 IPsec SA 协商期间， VPN 隧道接收的每接口数据包数量。

已转发数据包

在 IPsec SA 协商期间， VPN 隧道传输的每接口数据包数量。

已接收字节

在 IPsec SA 协商期间， VPN 隧道收到的每接口字节数。

已转发字节

在 IPsec SA 协商期间， VPN 隧道传输的每个接口字节数。

创建时间

VPN 连接的创建日期和时间。

上次使用时间

用户上次启动 VPN 连接的时间。

NAT 遍历

如果显示 Yes，至少一个 VPN 终端驻留在带有网络地址转换的设备之后。

IKE 状态

IKE SA 的状态：正在连接，已建立，正在删除或正在销毁。

IKE 事件

IKE SA 事件：重新身份验证或密钥更新。

IKE 事件时间

下一个事件应发生的时间（秒）。

IKE 算法

VPN 部署在使用的 IKE 算法。

IPSec 状态

IPSec SA 的状态：在安装、已安装、在更新、密钥更新、删除和销毁。

IPSec 事件

IPSec SA 事件进行密钥更新时的通知。

IPSec 事件时间

距离下一个事件发生的秒数。

IPSec 算法

VPN 部署在使用的 IPSec 算法。

要查看 VPN 统计信息，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > VPN**。

系统将显示 VPN 页面。

步骤 2　点击要在其中查看 VPN 统计信息的部署旁边的 VPN 状态图标。

系统将显示 VPN Status 弹出窗口。

步骤 3　点击视图统计信息图标 ()。

系统将显示 VPN Statistics 弹出窗口。

步骤 4　或者，点击 **Refresh** 更新 VPN 统计信息。

步骤 5　或者，点击 **View Recent Log** 查看每个终端的最新数据日志。

要查看集群设备和堆栈设备的日志，可选择主用设备/主设备或备用/辅助设备的链路。

使用 VPN 部署对比视图

许可证：VPN

受支持的设备：3 系列

在 VPN 部署对比视图中，可先查看对部署已做出的更改，然后再应用这类更改。报告显示当前部署与拟用部署之间的所有差异。可借此机会发现任何潜在的配置错误。

对比视图以并排格式显示两种部署，并在对比视图的左右两侧的标题栏中用名称标识每个部署。上次修改时间和最近一次做出修改的用户会与部署名称一起显示。

两个部署之间的差异已高亮显示：

- 蓝色指明高亮显示的设置在两个部署中不同，并以红色文本标明差异。
- 绿色指明高亮显示的设置只出现其中一个部署中。

您可以执行下表中的任何操作。

表 10-2　　VPN 部署对比视图操作

要.....	您可以.....
逐一浏览更改	点击标题栏上方的 **Previous** 或 **Next**。 在左右两侧之间以双箭头图标 ( ) 为中心移动， **Difference** 数字调整为识别您正在查看哪个差异。
生成部署对比报告	点击 **Comparison Report**。 部署对比报告创建一个 PDF 文档，仅列出两个策略之间的差异。

使用 NAT 策略

网络地址转换 (NAT) 策略决定系统如何借助网络地址转换实现路由。可以配置一个或多个 NAT 策略，然后将其应用于一个或多个受管设备。目前，只能为每个设备应用一个策略。

可以将 NAT 规则添加到策略来控制系统如何处理网络地址转换。每个规则包含用于识别要转换的特定流量的一组条件。可以创建以下类型的规则：

- 静态（提供对目标网络或者端口和协议的一对一转换）
- 动态 IP（转换多对多源网络，但保留端口和协议）
- 动态 IP 和端口（转换多对一或多对多的源网络、端口和协议）

在检查动态转换之前，系统会将流量与静态转换进行匹配，然后，按顺序将流量与动态 NAT 规则进行匹配；由最先匹配的规则处理流量。有关详细信息，请参阅第 11-5 页上的在 NAT 策略中整理规则。

如果在部署中有访问控制策略，系统会在流量通过访问控制后才对其进行转换。

要在设备上配置并应用 NAT 策略，必须在每个目标受管设备都有已启用的可控性许可证。此外，只能将 NAT 策略应用于配置了虚拟路由器或混合接口的 3 系列设备。

配置和部署了 NAT 策略后，可以使用目标受理设备的命令行界面 (CLI) 对部署进行故障排除。CLI 显示三种类型的 NAT 信息：配置、规则定义和活动转换。有关详细信息，请参阅第 D-1 页上的命令行参考。

有关创建和管理 NAT 策略的详细信息，请参阅以下各节：

规划和实施 NAT 策略

许可证：任何环境

可以用不同的方法配置 NAT 策略来管理特定的网络需求。本节提供有关可用于部署 NAT 策略的一些方法的信息。

注意事项　在集群配置中，如果 NAT 转换影响的所有网络都是专用网络，只能在集群设备上选择静态 NAT 规则的具体对等接口。不能将此配置用于会影响公共网络与专用网络之间流量的静态 NAT 规则。

可以配置 NAT 来将内部服务器开放到外部网络。在此配置中，可定义从外部 IP 地址转换为内部 IP 地址的静态转换，以便系统从网络外部访问内部服务器。发送到服务器的流量以外部 IP 地址或 IP 地址和端口为目标，并转换为内部 IP 地址或 IP 地址和端口。从服务器返回的流量重新转换为外部地址。

可以配置 NAT 以允许内部主机或服务器连接到外部应用。在此配置中，可定义从内部地址转换为外部地址的静态转换。这样的定义允许内部主机或服务器向预期内部主机或服务器有特定 IP 地址和端口的外部应用发起连接。因此，系统无法动态分配内部主机或服务器的地址。

通过使用 IP 地址块，可以配置 NAT 隐藏来自外部网络的专用网络地址。如果要对内部网络地址进行模糊处理，且具有足够的外部 IP 地址来满足内部网络需求，这样做将会很有用。在此配置中，可创建动态转换，以自动将任何传出流量的源 IP 地址转换为来自外部目标 IP 地址的未使用的 IP 地址。

可以使用有限的 IP 地址块和端口转换来配置 NAT，以隐藏来自外部网络的专有网络地址。如果要对内部网络地址进行模糊处理，但并没有足够的外部 IP 地址来满足内部网络需求，这样做将会很有用。在此配置中，可创建动态转换，以自动将传出流量的源 IP 地址和端口转换为来自外部目标 IP 地址的未使用的 IP 地址。

配置 NAT 策略

许可证：可控性

受支持的设备：3 系列

要配置 NAT 策略，必须为策略提供一个唯一的名称，以及识别要应用策略的设备（又称为*目标*）。还可以添加、编辑、删除、启用和禁用 NAT 规则。创建或修改 NAT 策略后，可以将策略应用于全部或部分目标设备。

可以将 NAT 策略应用于设备集群（包括集群堆叠），就像应用于独立设备一样。但是，可以对单独集群设备或整个集群上的接口定义静态 NAT 规则，并在源区域使用这些接口。对于动态规则，只可以在源或目标区域使用整个集群的接口。

注意事项　在集群配置中，如果 NAT 转换影响的所有网络都是专用网络，只能在集群设备上选择静态 NAT 规则的具体对等接口。不能将此配置用于会影响公共网络与专用网络之间流量的静态 NAT 规则。

如果在没有建立 HA 链路接口的设备集群上配置动态 NAT，两个集群设备将会分配动态 NAT 条目，系统将无法同步这两台设备之间的条目。有关详细信息，请参阅第 4-55 页上的配置高可用性链路接口。

可以将 NAT 策略应用于设备堆叠，就像应用于独立设备一样。如果从包含在 NAT 策略中的设备建立设备堆叠，且这些设备具有与作为堆叠成员的辅助设备的接口关联的规则，则辅助设备的接口将保留在 NAT 策略中。可以保存并应用包含接口的策略，但规则不提供任何转换。有关详细信息，请参阅第 4-37 页上的管理堆叠设备。

下表总结了在 NAT 策略的 Edit 页面可执行的配置操作。

表 11-1　NAT 策略配置操作

要.....	您可以.....
修改策略的名称或说明	点击 **Name** 或 **Description** 字段，根据需要删除字符，然后键入新的名称或说明。
管理策略目标	在第 11-3 页上的管理 NAT 策略目标中查找详细信息。
保存策略更改	点击 **Save**。
保存并应用策略	点击 **Save and Apply**。有关详细信息，请参阅第 11-12 页上的应用 NAT 策略。
取消策略更改	点击 **Cancel**，然后点击 **OK**（如果进行了更改）。
将规则添加到策略	点击 **Add Rule**。有关详细信息，请参阅第 11-14 页上的创建和编辑 NAT 规则。 **提示**　还可以右键单击现有规则并选择 **Insert new rule**。
编辑现有规则。	点击要编辑的规则旁边的编辑图标 ( )。有关详细信息，请参阅第 11-14 页上的创建和编辑 NAT 规则。 **提示**　还可以右键单击要编辑的规则并选择 **Edit**。
删除规则	点击要删除的规则旁边的删除图标 ( )，然后点击 **OK**。 **提示**　要删除一个或多个选定的规则，可以右键单击选定规则行的空白区域，选择 **Delete**，然后点击 **OK**。
启用或禁用现有规则	右键单击选定的规则，选择 **State**，然后选择 **Disable** 或 **Enable**。被禁用的规则在规则名称下方呈灰色显示并带有相应的标记 (`disabled`)。
显示特定规则属性的配置页面	在规则行上点击条件列中的名称、值或图标。例如，点击 **Source Networks** 列中的名称或值可显示所选规则的 Source Network 页面。有关详细信息，请参阅第 11-21 页上的处理 NAT 规则中不同类型的条件。

管理 NAT 策略目标

许可证：可控性

受支持的设备：3 系列

应用 NAT 策略之前，必须确定要应用策略的受管设备（包括设备堆叠、集群或组）。创建或编辑策略时，可以确定要应用策略的受管设备。可以搜索一系列可用的设备、堆叠和集群，并将其添加到选定设备列表。还可以拖放选定的设备，或者使用两个列表之间的按钮添加设备。

请注意，不能以运行不同版本 FireSIGHT 系统的堆叠设备作为目标（例如，如果其中一台设备的升级失败）。有关详细信息，请参阅第 4-37 页上的管理堆叠设备。

下表总结了管理目标设备时可执行的操作。

表 11-2　目标设备管理操作

要.....	您可以.....
搜索可用设备、堆叠和集群的列表	在搜索字段中点击，然后键入搜索字符串。设备列表会在您键入内容时进行更新，以显示匹配的设备名称。
清除对可用设备的搜索	在搜索字段中点击清除图标 ( )。

表 11-2　目标设备管理操作（续）

要.....	您可以.....
选择要添加到所选目标列表的可用设备、堆叠或集群	点击要添加的设备的名称；使用 Ctrl 和 Shift 键可选择多台设备。 **提示**　还可以右键单击一个可用设备，然后点击 **Select All**。
添加选定的设备、堆叠或集群	点击 **Add to Policy**。 **提示**　还可以将选定的设备、堆叠或集群拖放到选定设备列表。
从 Selected Devices 列表删除单台设备、堆叠或集群	点击要删除的设备旁边的删除图标 ( )。 **提示**　还可以右键单击要编辑的设备并选择 **Delete**。
从 Selected Devices 列表删除多台设备	使用 Ctrl 和 Shift 键选择多台设备，右键单击以突出显示某个选定设备的行，然后点击 **Delete Selected**。
保存配置	点击 **Save**。
放弃配置而不保存更改	点击 **Cancel**。

以下步骤说明如何配置 NAT 策略来管理目标设备。有关编辑 NAT 策略的完整步骤，请参阅第 11-8 页上的编辑 NAT 策略。

要在 NAT 策略中管理目标设备，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > NAT**。

系统将显示 NAT 页面。

步骤 2　点击要配置的 NAT 策略旁边的编辑图标 ( )。

系统将显示 NAT Policy Editor 页面。

步骤 3　点击 **Targets** 选项卡。

系统将显示 Targets 页面

步骤 4　或者，点击 Available Devices 列表上方的 **Search** 提示，然后键入名称。

列表会在您键入内容时进行更新，以显示匹配的设备。可以点击清除图标 (✖) 来清除列表。

步骤 5　点击要添加的设备、堆叠、集群或设备组。使用 Ctrl 和 Shift 键可选择多台设备。

提示　还可以右键单击一个可用设备，然后点击 **Select All**。

步骤 6　点击 **Add to Policy**。

所选设备添加成功。

提示　还可以通过拖放来添加设备。

步骤 7　如有需要，可以点击删除图标 ( ) 删除选定设备列表中的设备；或者，使用 Ctrl 和 Shift 键选择多台设备，右键单击，然后选择 **Delete Selected**。

步骤 8　点击 **Save** 保存配置，或点击 **Cancel** 放弃配置。

在 NAT 策略中整理规则

许可证：任何环境

NAT 策略的 Edit 页面分别列出了静态 NAT 规则和动态 NAT 规则。系统按名称的字母顺序对静态规则进行排序，显示顺序不能更改。不能创建具有相同的匹配值的静态规则。系统会先检查匹配的静态转换，再检查所有动态转换。

动态规则按数字顺序处理。每个动态规则的数字位置显示在规则旁边的页面左侧。可以移动或插入动态规则，也可以更改规则顺序。例如，如果将动态规则 10 移动到动态规则 3 下方，规则 10 将会变成规则 4，而且所有后续编号将会相应地增大。

动态规则的位置很重要，因为系统会按策略的 Edit 页面中显示的规则数字顺序将数据包与动态规则进行比较。如果某个数据包符合某个动态规则的所有条件，系统会将该规则的条件应用于该数据包，并忽略该数据包的所有后续规则。

如有需要，还可以在添加或编辑动态规则时指定动态规则的数字位置。还可以在增加新的动态规则之前突出显示某个动态规则，以将新规则插入到突出显示的规则下方。请参阅第 11-14 页上的创建和编辑 NAT 规则。

可以通过点击规则行的空白区域来选择一个或多个动态规则。可以将选定的动态规则拖放到新位置，从而更改移动的规则及其后续规则的位置。

可以剪切或复制选定的规则，并将其粘贴到现有规则的上方或下方。静态规则只能粘贴到静态转换列表中，动态规则只能粘贴到动态转换列表中。还可以删除选定的规则，并将新规则插入到现有规则列表中的任何位置。

注　静态规则可以复制但不能剪切。

可以显示解释性警告，用以识别由于被前置规则抢占而绝对不会匹配的规则。

如果在部署中有访问控制策略，系统会在流量通过访问控制后才对其进行转换。

下表总结了可用于整理规则的操作。

表 11-3　NAT 规则整理操作

要.....	您可以.....
选择规则	点击规则行的空白区域。使用 Ctrl 或 Shift 键可选择多个规则。选定的规则将会突出显示。
清除选定的规则	点击页面右下方重新加载图标 ( )。要清除单个规则，请按住 Ctrl 键并点击规则行的空白区域。
剪切或复制选定的规则	右键单击选定规则行的空白区域，然后选择 **Cut** 或 **Copy**。 **提示**　静态规则可以复制但不能剪切。

表 11-3　NAT 规则整理操作（续）

要.....	您可以.....
将剪切或复制的规则粘贴到规则列表中	右键单击要在其中粘贴选定规则的规则行的空白区域，然后选择 **Paste above** 或 **Paste below**。 **提示**　静态规则只能粘贴到静态转换列表中，动态规则只能粘贴到动态转换列表中。
移动选定的规则	将选定的规则拖放到新位置下方（拖动规则时，指针上方显示的蓝色横线即表示新位置）。
删除规则	点击要删除的规则旁边的删除图标 ( )，然后点击 **OK**。 **提示**　还可以右键单击选定规则行的空白区域，选择 **Delete**，然后点击 **OK** 删除一个或多个选定的规则。
显示警告	点击 **Show Warnings**；请参阅第 11-6 页上的处理 NAT 规则警告和错误。

处理 NAT 规则警告和错误

许可证：任何环境

NAT 规则的条件可以抢占来自匹配流量的后续规则。任何类型的规则条件都可以抢占后续规则。

规则还会抢占所有配置条件都相同的完全一样的后续规则。只要任何一个条件不同，后续规则都不会被抢占。

下表总结了可用于显示和清除警告的操作。

表 11-4　被抢占规则的警告操作

要.....	您可以.....
显示警告	点击 **Show Warnings**。页面即会更新，每个被抢占的规则旁边都显示警告图标 ( )。
显示规则警告	将指针悬停在相应规则旁边的警告图标 ( ) 上。系统将显示一条消息，指明哪个规则抢占了该规则。
清除警告	点击 **Hide Warnings**。页面即会刷新，警告消失。 **提示**　任何刷新页面的操作 （例如，添加或编辑规则，或者单击重新加载图标 ( )）也会清除警告。

如果创建了导致 NAT 策略应用失败的规则，该规则旁边将会显示错误图标 ( )。如果静态规则中存在冲突，或者编辑策略中使用的但当前使策略无效的网络对象，将会出现错误。例如，如果将网络对象更改为只使用 IPv6 地址，并且使用该对象的规则不再有任何有效网络，但该规则要求至少有一个网络，将会出现错误。错误图标自动显示；无需点击 **Show Warnings**。

管理 NAT 策略

许可证：可控性

受支持的设备：3 系列

在 NAT 策略页面 (**Devices > NAT**)，可以按名称查看所有当前的 NAT 策略以及策略的可选说明和以下状态信息：

- 如果策略在目标设备上是最新的，以绿色文本显示
- 如果策略在目标设备上是过时的，以红色文本显示

可以使用该页面上的选项来比较策略，创建新策略，将策略应用于目标设备，复制策略，查看列出每个策略中最近保存的设置的报告，以及编辑策略。

注　不能删除已应用于受理设备的 NAT 策略，即使策略已过时。如果要从受管设备删除已应用的 NAT 规则，必须应用不带有任何规则的 NAT 策略。

下表介绍了可在 NAT 策略页面上执行的策略管理操作。

表 11-5　NAT 策略管理操作

要.....	您可以.....
创建新的 NAT 策略	点击 **New Policy**。有关详细信息，请参阅第 11-7 页上的创建 NAT 策略。
修改现有 NAT 策略的设置	点击编辑图标 ( )。有关详细信息，请参阅第 11-8 页上的编辑 NAT 策略。
将 NAT 策略应用于作为策略目标的所有设备	点击策略应用图标 ( )。有关详细信息，请参阅第 11-12 页上的应用 NAT 策略。
复制 NAT 策略	点击复制图标 ( )。有关详细信息，请参阅第 11-9 页上的复制 NAT 策略。
查看列出 NAT 策略的当前配置设置的 PDF 报告	点击报告图标 ( )。有关详细信息，请参阅第 11-9 页上的查看 NAT 策略报告。
比较 NAT 策略	点击 **Compare Policies**。有关详细信息，请参阅第 11-10 页上的比较两个 NAT 策略。
删除 NAT 策略	点击删除图标 ( )，然后点击 **OK**；如果决定不删除策略，点击 **Cancel**。当系统提示是否继续时，还会告知您是否有其他用户在策略中有未保存的更改。 **注**　将 NAT 策略应用于受理设备后，就不能从设备删除策略。如果要从受管设备删除已应用的 NAT 规则，必须应用不带有任何规则的 NAT 策略。也不能删除上一次应用于任何目标设备的策略，即使该策略已过时。要完全删除该策略，必须向目标应用其他策略。

创建 NAT 策略

许可证：可控性

受支持的设备：3 系列

创建新的 NAT 策略时，必须至少为其提供一个唯一的名称。虽然在创建策略过程中不需要识别策略目标，但必须执行这个步骤后才能应用策略；请参阅第 11-3 页上的管理 NAT 策略目标。如果将不带有规则的 NAT 策略应用于某台设备，系统会从该设备删除所有 NAT 规则。

要创建 NAT 策略，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > NAT**。

系统将显示 NAT 页面。

步骤 2　点击 **New Policy**。

系统将显示 New NAT Policy 弹出窗口。

步骤 3　在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

可使用所有可打印字符，包括空格和特殊字符。

步骤 4　在 **Available Devices** 中选择要应用策略的设备。

使用 Ctrl 和 Shift 键可选择多台设备，或者右键单击以选择 **Select All**。要减少显示的设备，请在 **Search** 字段中键入搜索字符串。要清除搜索，请点击清除图标 (✖)。

步骤 5　添加**选定的设备**。也可以点击并拖动，或者点击 **Add to Policy**。

步骤 6　点击 **Save**。

系统将显示 NAT 策略的 Edit 页面。有关配置新政策（包括添加规则）的信息，请参阅第 11-8 页上的编辑 NAT 策略。请注意，策略在应用后才会生效；请参阅第 11-12 页上的应用 NAT 策略。

编辑 NAT 策略

许可证：可控性

受支持的设备：3 系列

可以在 NAT 策略的 Edit 页面配置策略。有关详细信息，请参阅第 11-2 页上的配置 NAT 策略。

更改配置时，会有消息提示您有未保存的更改。要保留更改，必须在退出 NAT 策略的 Edit 页面之前保存策略。如果在未保存更改的情况下退出 Edit 页面，系统会提醒您有未保存的更改；可以放弃更改并退出策略，或者返回到 Edit 页面。

为了保护会话隐私，在策略 Edit 页面进入不活动超过 60 分钟后，系统会放弃对策略所做的更改，并返回到 NAT 页面。在进入不活动状态超过 30 分钟后，会显示一条消息，并定期进行更新以提供距离放弃更改的分钟数。页面上的任何活动都会重置计时器。

当您尝试在两个浏览器窗口中编辑同一个策略时，系统会询问您要执行以下何种操作：在新窗口中恢复编辑；放弃在原始窗口中所做的更改并继续在新窗口中进行编辑；取消第二个窗口并返回到策略 Edit 页面。

如果多个用户同时编辑同一个策略，策略 Edit 页面中将会对每个用户显示一条消息，用以指出未保存更改的其他用户。当有用户尝试保存更改时，系统会提醒他们这样做会覆盖其他用户所做的更改。如果多个用户保存同一个策略，系统会保留最后的更改。

如果将某个接口的类型更改为不适用于以具有该接口的设备为目标的 NAT 策略的类型，策略会将该接口标记为“已删除”。在 NAT 策略中点击 **Save** 会自动从策略删除接口。

要编辑 NAT 策略，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > NAT**。

系统将显示 NAT 页面。

步骤 2　点击要配置的 NAT 策略旁边的编辑图标 ( )。

系统将显示 NAT 策略的 Edit 页面。

步骤 3　要配置策略，请执行第 11-2 页上的配置 NAT 策略中所述的任何操作。

步骤 4　保存或放弃配置。有以下选项可供选择：

- 要保存更改并继续编辑，请点击 **Save**。
- 要保存更改并应用策略，请点击 **Save and Apply**。请参阅第 11-12 页上的应用 NAT 策略。所做的更改在应用策略后才会生效。
- 要放弃更改，请点击 **Cancel**；如果出现提示，点击 **OK**。更改被放弃并显示 NAT 页面。

复制 NAT 策略

许可证：可控性

受支持的设备：3 系列

可以复制和重命名 NAT 策略。复制的策略包含所有规则和配置。

要复制 NAT 策略，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > NAT**。

系统将显示 NAT 页面。

步骤 2　点击要配置的 NAT 策略旁边的复制图标 ( )。

系统将显示 Copy NAT Policy 弹出窗口。

步骤 3　在 **Name** 字段中输入唯一的策略名称。

可以使用任何可打印字符（包括空格和特殊字符）。

步骤 4　点击 **OK**。

复制的内容将按名称的字母顺序显示在 NAT 页面中。

查看 NAT 策略报告

许可证：可控性

受支持的设备：3 系列

NAT 策略报告是在特定时间点对策略和规则配置的记录。报告可用于审核或检查当前配置。

提示　还可以生成 NAT 比较报告，用以将某个策略与当前应用的策略或其他策略作比较 有关详细信息，请参阅第 11-10 页上的比较两个 NAT 策略。

NAT 策略报告包含下表所述的各个部分。

表 11-6　NAT 策略报告的组成部分

项	说明
标题页	指明策略报告的名称、策略上次修改的日期和时间以及上次修改策略的用户的名称。
目录	说明报告的内容。
策略信息	提供策略的名称和说明、上次修改策略的用户的名称以及策略上次修改的日期和时间 请参阅第 11-8 页上的编辑 NAT 策略。
设备目标	列出作为策略目标的受管设备。请参阅第 11-3 页上的管理 NAT 策略目标。
规则	提供策略中每个规则的规则类型和条件。请参阅第 11-14 页上的创建和编辑 NAT 规则。
引用对象	提供策略中使用的所有具体对象和组对象的名称及配置，按作为对象配置依据的条件的类型（区域、网络和端口）显示。

要查看 NAT 策略报告，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > NAT**。

系统将显示 NAT 页面。

步骤 2　点击要生成报告的策略旁的报告图标 ( )。生成 NAT 策略报告之前，请记住要保存所有更改；报告中只会显示已保存的更改。

系统将会生成报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

比较两个 NAT 策略

许可证：可控性

受支持的设备：3 系列

要查看策略更改，可以检查两个 NAT 策略之间的区别。可以比较任意两个策略，也可以将当前应用的策略与另一策略进行比较。在进行比较后，或者生成 PDF 报告来记录两个策略之间的差异。

有两个可以用来比较策略的工具：

- 比较视图仅会以并排格式显示两个策略之间的差异。每个策略的名称将会显示在比较视图左侧和右侧的标题栏中，当选择 **Running Configuration** 时除外，在这种情况下，空白栏代表当前的活动策略。

  可以使用此工具来在网络界面中查看和导航两个策略（在其差异突出显示的情况下）。

- 比较报告会以类似策略报告的格式（但采用 PDF 格式）创建仅有两个策略之间的差异的记录。

  可以使用此工具来保存、复制、打印和共享策略比较，供未来检查使用。

有关了解和使用策略比较工具的详细信息，请参阅以下各节：

- 第 11-11 页上的使用 NAT 策略比较视图
- 第 11-11 页上的使用 NAT 策略比较报告

使用 NAT 策略比较视图

许可证：可控性

受支持的设备：3 系列

比较视图会以并排格式显示两个策略，每个策略由比较视图左侧和右侧标题栏中的名称确定。比较运行配置之外的两个策略时，最后修改的时间和最后修改的用户将会随策略名称显示。

两个策略之间的差异将会突出显示：

- 蓝色指示突出显示的设置在两个策略中不同，不同之处以红色文本标注。
- 绿色指示突出显示的设置在一个策略中存在，但在另一个策略中不存在。

您可以执行下表中的任何操作。

表 11-7　NAT 策略比较视图操作

要.....	您可以.....
逐一浏览更改	点击标题栏上方的 **Previous** 或 **Next**。 在左右两侧之间以双箭头图标 (◂▸) 为中心移动， **Difference** 数字调整为识别您正在查看哪个差异。
生成新的策略比较视图	点击 **New Comparison**。 系统将显示 **Select Comparison** 窗口。有关详细信息，请参阅第 11-11 页上的使用 NAT 策略比较报告。
生成策略比较报告	点击 **Comparison Report**。 策略比较报告将会创建仅列出两个策略之间的差异的 PDF 文档。

使用 NAT 策略比较报告

许可证：可控性

受支持的设备：3 系列

NAT 策略比较报告记录策略比较视图中识别出的两个 NAT 策略之间或者某个策略与当前应用的策略之间的差异，其文件格式为 PDF。可以使用此报告来进一步检查两个策略配置之间差异，以及保存和分发比较结果。

对于您能够访问的任何策略，都可以通过比较视图生成 NAT 策略比较报告。在生成策略报告前，切记保存所有更改，只有已保存的更改会在报告中显示。

策略比较报告的格式与策略报告的格式相同，两者的唯一不同之处是：策略报告包含策略中的所有配置，而策略比较报告仅列出策略之间不同的配置。NAT 策略比较报告包含NAT 策略报告的组成部分表所述的各个部分。

要比较两个 NAT 策略，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > NAT**。

系统将显示 NAT 页面。

步骤 2　点击 **Compare Policies**。

系统将显示 Select Comparison 窗口。

步骤 3　从 **Compare Against** 下拉列表中选择要进行比较的类型：

- 要比较两个不同的策略，请选择 **Other Policy**。

  页面将会刷新，并显示 Policy A 和 Policy B 下拉列表。
- 要比较两个不同的版本，请选择 **Other Revision**。

  页面即会刷新并显示 Policy、 Revision A 和 Revision B 下拉列表。
- 要将另一策略与当前活动的策略进行比较，请选择 **Running Configuration**。

  页面将会刷新，并会显示 Target/Running Configuration A 和 Policy B 下拉列表。

步骤 4　根据您选择的比较类型，有以下选项可供选择：

- 如果您比较两个不同的策略，请从 **Policy A** 和 **Policy B** 下拉列表中选择要比较的策略。
- 如果要比较两个不同的版本，请选择策略，然后从 **Revision A** 和 **Revision B** 下拉列表选择要比较的版本。
- 如果与另一策略比较运行配置，请从 **Policy B** 下拉列表中选择另一个策略。

步骤 5　点击 **OK** 显示策略比较视图。

系统将显示比较视图。

步骤 6　如有需要，点击 **Comparison Report** 以生成 NAT 策略比较报告。

即会显示 NAT 策略比较报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

应用 NAT 策略

许可证：可控性

受支持的设备：3 系列

更改 NAT 策略后，必须将其应用于一个或多台设备，才能在设备监控的网络上实施配置更改。必须先将要应用策略的设备设置为目标设备，然后才可以应用策略。请参阅第 11-3 页上的管理 NAT 策略目标。

应用 NAT 策略时，请谨记以下几点：

- 可以在防御中心配置和维护多个 NAT 策略，但是，一次只能将一个策略应用于某台设备。
- 可以将两个不同的 NAT 策略于两个不同的设备，即使这两台设备都是多个策略的目标。
- 不能将 NAT 策略应用于运行不同版本 FireSIGHT 系统的堆叠设备（例如，如果其中一台设备的升级失败）。有关详细信息，请参阅第 4-37 页上的管理堆叠设备。
- 不能应用其应用状态为“待处理”的新 NAT 策略。
- 如果应用会影响 NAT 策略中接口的设备配置，系统会对该设备重新应用 NAT 策略（包括接口更改）。但是，策略在 DC 中保持不变，并且接口显示错误图标 ( )。

注　应用空的 NAT 策略会删除设备上的所有 NAT 规则。

有关详细信息，请参阅以下各节：

- 第 11-13 页上的应用完整的 NAT 策略说明如何使用快速应用选项来应用 NAT 策略。
- 第 11-13 页上的应用选定的策略配置说明如何在 NAT 策略中选择和应用配置。

应用完整的 NAT 策略

许可证：可控性

受支持的设备：3 系列

可以随时应用 NAT 策略。应用某个 NAT 策略，会同时将所有相关的规则配置、对象和策略更改应用于作为该策略的目标的设备。借助弹出窗口，可以作为一次快速应用操作同时应用所有更改。

要快速应用完整的 NAT 策略，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > NAT**。

系统将显示 NAT 页面。

步骤 2　点击要应用的策略旁的应用图标 ( )。

系统将显示 Apply NAT Rules 弹出窗口。

另外，可以点击策略 Edit 页面上的 **Save and Apply**；请参阅第 11-8 页上的编辑 NAT 策略。

步骤 3　点击 **Apply All**。

策略应用任务将会排入队列。点击 **OK** 返回到 NAT 页面。

提示　可以在 Task Status 页面（**System > Monitoring > Task Status**）上监控策略应用任务的进度

应用选定的策略配置

许可证：可控性

受支持的设备：3 系列

可以使用详细策略应用页面来将更改应用于 NAT 策略以及任何指定的目标设备。该详细页面列出被每个策略作为目标的设备，并为 NAT 策略提供设备列。可以指定是否要将更改应用于每个过时目标设备的 NAT 策略。

要应用选定的 NAT 策略配置，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > NAT**。

系统将显示 NAT 页面。

步骤 2　点击要应用的策略旁的应用图标 ( )。

系统将显示 Apply NAT Rules 弹出窗口。

另外，可以点击策略 Edit 页面上的 **Save and Apply**；请参阅第 11-8 页上的编辑 NAT 策略。

步骤 3　点击 **Details**。

系统将显示详细的 Apply NAT Rules 弹出窗口。

提示　也可以从 NAT 页面 (**Devices > NAT**) 打开该弹出窗口，具体操作是，在相应策略的 **Status** 列中点击过时消息。

步骤 4　选择或清除设备名称旁边的 **NAT policy** 复选框，以指定是否将 NAT 策略应用于目标设备。

步骤 5　点击 **Apply Selected Configurations**。

策略应用任务将会排入队列。点击 **OK** 返回到 NAT 页面。

提示　可以在 Task Status 页面（**System > Monitoring > Task Status**）上监控策略应用任务的进度

创建和编辑 NAT 规则

许可证：可控性

受支持的设备：3 系列

简单来说， NAT 规则是一组具有如下作用的配置和条件：

- 限定网络流量
- 指定那些符合资格的流量如何转换

可以在现有 NAT 策略中创建和编辑 NAT 规则。每个规则只属于一个策略。

用于添加或编辑规则的网络界面是类似的。在页面顶部指定规则的名称、状态、类型和位置（如果是动态规则）。在页面左侧使用选项卡建立条件；每种条件都有自己的选项卡。

以下列表总结了 NAT 规则的可配置组成部分。

字段名称

为每个规则提供唯一的名称。对于静态 NAT 规则，请使用最多 22 个字符。对于动态 NAT 规则，请使用最多 30 个字符。可以使用可打印字符，包括空格和特殊字符，但冒号 (:) 除外。

Rule State

默认情况下，规则处于启用状态。系统不使用已禁用的规则来评估要转换的网络流量。查看 NAT 策略中的规则列表时，已禁用的规则呈灰色显示，但这些规则仍可以修改。

类型

规则的类型决定系统如何处理与规则条件相匹配的流量。创建和编辑 NAT 规则时，可配置的组成部分因规则类型而异。

有关规则类型以及它们如何影响转换和流量的详细信息，请参阅第 11-15 页上的了解的 NAT 规则类型。

位置（仅适用于动态规则）

NAT 策略中的动态规则带有编号（从 1 开始）。系统按编号自上而下的顺序将流量与 NAT 规则进行匹配。

向策略添加规则时，可以使用规则编码作为参考点，通过将其置于特定规则**之上**或**之下**来确定它的位置。编辑现有规则时，可以通过类似的做法**移动**规则。有关详细信息，请参阅第 11-5 页上的在 NAT 策略中整理规则。

条件

规则条件确定要转换的特定流量。条件可以通过多个属性（包括安全区域、网络和传输协议端口）的任意组合来匹配流量。

有关添加条件的详细信息，请参阅第 11-17 页上的了解 NAT 规则条件和条件机制和第 11-21 页上的处理 NAT 规则中不同类型的条件。

要创建或编辑 NAT 规则，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > NAT**。

系统将显示 NAT 页面。

步骤 2　点击要向其添加规则的 NAT 策略旁边的编辑图标 ( )。

系统将显示 NAT 策略的 Edit 页面。

步骤 3　要添加新规则或编辑现有规则：

- 要添加新规则，请点击 **Add Rule**。
- 要编辑现有规则，请点击要编辑的规则旁边的编辑图标 ( )。

系统将显示 Add Rule 或 Editing Rule 页面。

提示　可以使用右键单击显示的上下文菜单进行多项规则创建和管理操作；请参阅第 2-4 页上的使用上下文菜单。也可以通过拖放规则来改变规则的顺序。

步骤 4　如本节前面所述配置规则组成部分。可以配置以下内容或接受默认设置：

- 您必须在 **Name** 中提供唯一的规则名称。
- 指定规则是否为 **Enabled**。
- 在 **Type** 中选择规则类型。
- 指定规则位置（仅适用于动态规则）。
- 配置规则的条件。

  静态规则必须包括原始目标网络。

  动态规则必须包含转换后的源网络。

步骤 5　点击 **Add** 或 **Save**。

已保存您的更改。必须应用 NAT 策略来使更改生效；请参阅第 11-12 页上的应用 NAT 策略。

了解的 NAT 规则类型

许可证：任何环境

每个 NAT 规则都有具有如下作用的相关类型：

- 限定网络流量
- 指定那些符合资格的流量如何转换

以下列表总结了 NAT 规则类型。

静态

静态规则提供对目标网络或者端口和协议的一对一转换。配置静态转换时，可以配置源区域、目标网络和目标端口。不能配置目标区域或源网络。

必须指定原始目标网络。对于目标网络，只能选择包含单个 IP 地址的网络对象和组，或者输入代表单个 IP 地址的文字 IP 地址。只能指定一个原始目标网络和一个转换后的目标网络。

如有需要，可以指定一个原始目标端口和一个转换后的目标端口。在指定原始目标端口之前，必须指定原始目标网络。此外，必须满足以下条件才能指定转换后的目标端口：已经指定原始目标端口，且转换后的值与原始值的协议相匹配。

注意事项　对于集群设备上的静态 NAT 规则，如果所有受 NAT 转换影响的网络都是专用网络，则仅选择单个对等接口。**不**能将此配置用于会影响公共网络与专用网络之间流量的静态 NAT 规则。

仅动态 IP

“仅动态 IP”规则转换多对多源网络，但保留端口和协议。配置“仅动态 IP”转换时，可以配置区域、源网络、原始目标网络和原始目标端口。不能配置转换后的目标网络或转换后的目标端口。

必须至少指定一个转换后的源网络。如果转换后的源网络值的数量少于原始源网络的数量，系统将会显示针对的警告，指出在所有原始地址匹配之前可能用完转换后的地址。

如果有多个规则具有与同一个数据包相匹配的规则，优先级较低的规则将会变成死规则，这意味着，这些规则绝不会被触发。系统还会显示针对死规则的警告。可以查看工具提示来确定哪个规则取代了死规则。

注　可以保存和应用包含死规则的策略，但此类规则无法提供任何转换。

在某些情况下，您可能希望以较大的范围创建带有有限范围前置规则的规则。例如：

```
规则 1：匹配地址 A 和端口 A/转换为地址 B
规则 2：匹配地址 A/转换为地址 C
```

在本示例中，与某些数据包匹配的规则 1 也与规则 2 相匹配。因此，规则 2 并没有完全死亡。

或者，可以仅指定原始目标端口。不能指定转换后的目标端口。

动态 IP + 端口

“动态 IP 和端口”规则转换多对一或多对多的源网络、端口和协议。配置“动态 IP 和端口”转换时，可以配置区域、源网络、原始目标网络和原始目标端口。不能配置转换后的目标网络或转换后的目标端口。

必须至少指定一个转换后的源网络。如果有多个规则具有与同一个数据包相匹配的规则，优先级较低的规则将会变成死规则，这意味着，这些规则绝不会被触发。系统还会显示针对死规则的警告。可以查看工具提示来确定哪个规则取代了死规则。

注　可以保存和应用包含死规则的策略，但此类规则无法提供任何转换。

或者，可以仅指定原始目标端口。不能指定转换后的目标端口。

注　如果创建动态 IP 和端口规则，并且系统传递没有使用接口的流量，流量不发生转换。例如，来自匹配源网络的 IP 地址的 ping (ICMP) 不会映射，因为 ICMP 不使用端口。

下表总结了可以根据指定的 NAT 规则类型配置的 NAT 规则条件类型：

表 11-8　每种 NAT 规则类型可用的 NAT 规则条件类型

情况	静态	动态 （仅 IP 或 IP+ 端口）
源区域	可选	可选
目标区域	不允许	可选
原始源网络	不允许	可选
转换后的源网络	不允许	**必填**
原始目标网络	**必填**	可选
转换后的目标网络	可选；仅单个地址	不允许
原始目标端口	可选；仅限单个端口，且仅在定义了原始目标网络的情况下才可用	可选
转换后的目标端口	可选；仅限单个端口，且仅在定义了原始目标端口的情况下才可用	不允许

了解 NAT 规则条件和条件机制

许可证：任何环境

可以向 NAT 规则添加条件来识别与规则匹配的流量的类型。对于每种条件类型，从可用条件列表中选择要添加到规则的条件。如果适用，可使用条件过滤器来限制可用的条件。可用条件和选定条件的列表可以短至只包含一个条件，也可以长达多页。可以搜索可用条件，并仅显示那些与您在列表中键入的名称或值相匹配的条件（该列表会根据键入的内容同步更新）。

根据条件类型，可用条件列表可以同时包含思科直接提供的条件和使用 FireSIGHT 系统的其他功能配置的条件，包括使用对象管理器 (**Objects > Object Management**) 创建的对象、直接从各个条件页面创建的对象和文字条件。

有关指定规则情况的信息，请参阅以下各节：

- 第 11-18 页上的了解 NAT 规则条件定义不同类型的规则条件。
- 第 11-18 页上的向 NAT 规则添加条件介绍用于选择和添加规则条件的控件。
- 第 11-20 页上的搜索 NAT 规则条件列表说明如何搜索可用条件，并仅显示那些与您在列表中键入的名称或值相匹配的条件（该列表会根据键入的内容同步更新）。
- 第 11-20 页上的向 NAT 规则添加文字条件说明如何将文字条件添加到规则。
- 第 11-21 页上的在 NAT 规则条件中使用对象说明如何从相关条件类型的配置页面将各个对象添加到系统。

了解 NAT 规则条件

许可证：任何环境

可以设置 NAT 规则来匹配满足下表所述的任何条件的流量：

表 11-9　　NAT 规则条件类型

情况	说明	支持的防御中心。	支持的设备
区域	一种包含一个或多个路由接口的配置，允许应用 NAT 策略。区域提供用于对源接口和目标接口上的流量进行分类的机制；您可以向规则添加源区域条件和目标区域条件。有关使用对象管理器创建区域的信息，请参阅第 3-34 页上的使用安全区域。	任何环境	3 系列
网络	单个 IP 地址、CIDR 块和前缀长度的任意组合，明确指定或使用网络对象和组（请参阅第 3-4 页上的使用网络对象）。可以向 NAT 规则添加源网络条件和目标网络条件。	任何环境	3 系列
目标端口	传输协议端口，包括基于传输协议创建的单个端口对象和端口对象组。有关使用对象管理器创建单个传输协议对象和成组传输协议对象的信息，请参阅第 3-10 页上的使用端口对象。	任何环境	3 系列

向 NAT 规则添加条件

许可证：任何环境

对于每种条件，向 NAT 规则添加条件的操作基本相同。在可用条件列表左侧选择条件，然后将所选条件添加到右侧的一个或两个选定条件列表中。

对于所有条件类型，要选择一个或多个可用条件，可通过点击来突出显示要选择的条件。可以点击两种列表之间的按钮将所选的可用条件添加到选定条件列表，也可以将所选的可用条件拖放到选定条件列表。

最多可以将同一类型的 50 个条件添加到选定条件列表。例如，最多可以添加 50 个源区域条件、50 个目标区域条件和 50 个源网络条件，等等，直至达到设备的上限。

下表介绍了可用于选择并向规则添加条件的操作。

表 11-10　　向 NAT 规则添加条件

要.....	您可以.....
选择要添加到选定条件列表的可用条件	点击可用条件；使用 Ctrl 和 Shift 键可选择多个条件。
选择所有列出的可用条件	右键单击任何可用条件的行，然后点击 **Select All**。
搜索可用条件或过滤器	在 **Search** 字段中点击，然后键入搜索字符串。有关详细信息，请参阅第 11-20 页上的搜索 NAT 规则条件列表。
在搜索可用条件或过滤器时清除搜索	点击 Search 字段上方的重新加载图标 ( ) 或 Search 字段中的清除图标 ( )。
将可用条件列表中的选定区域条件添加到选定源条件或目标条件的列表	点击 **Add to Source** 或 **Add to Destination**。有关详细信息，请参阅第 11-21 页上的向 NAT 规则添加区域条件。

表 11-10　向 NAT 规则添加条件 （续）

要.....	您可以.....
将可用条件列表中的选定网络条件和端口条件添加到选定原始条件或转换后条件的列表	点击 **Add to Original** 或 **Add to Translated**。有关详细信息，请参阅第 11-23 页上的将源网络条件添加到动态 NAT 规则、第 11-24 页上的将目标网络条件添加到 NAT 规则或第 11-25 页上的向 NAT 规则添加端口条件。
将选定的可用条件拖放到选定条件列表	点击选定的条件，然后将其拖放到选定条件列表。
使用文字字段将文字条件添加到选定条件列表	点击以从文字字段中删除提示，键入文字条件，然后点击 **Add**。网络条件提供一个用于添加文字条件的字段。
使用下拉列表将文字条件添加到选定条件列表	从下拉列表中选择条件，然后点击 **Add**。端口条件提供一个用于添加文字条件的下拉列表。有关详细信息，请参阅第 11-25 页上的向 NAT 规则添加端口条件。
添加具体对象或条件过滤器以供在可用条件列表中选择	点击添加图标 ( )。有关使用对象管理器添加对象的信息，请参阅第 3-1 页上的管理可重用对象。
从选定条件列表中删除单个条件	点击要删除的条件旁边的删除图标 ( )。
从选定条件列表中删除条件	右键单击以突出显示所选条件的行，然后点击 **Delete**。
从选定条件列表中删除多个条件	使用 Shift 和 Ctrl 键选择多个条件；或者右键单击并选择 **Select All**；接着，右键单击以显示所选条件的行，然后点击 **Delete Selected**。

在相关条件页面和策略 Edit 页面上，将指针悬停在单个对象上显示该对象的内容，将指针悬停在某个组对象上可显示该组中各个对象的编号。

以下基本步骤说明如何将条件添加到新规则。有关添加和修改规则的完整说明，请参阅第 11-14 页上的创建和编辑 NAT 规则。

要将可用条件添加到选定条件列表，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > NAT**。

系统将显示 NAT 页面。

步骤 2　点击要修改的 NAT 策略旁边的编辑图标 ( )。

系统将显示策略 Edit 页面。

步骤 3　点击 **Add Rule**。

系统将显示 Add Rule 页面。

步骤 4　点击要添加到规则的条件类型的选项卡。

系统将显示所选条件类型的条件页面。

步骤 5　执行向 NAT 规则添加条件表中列出的任何可用操作。

步骤 6　点击 **Add** 保存配置。

规则添加成功，系统将显示策略 Edit 页面。

搜索 NAT 规则条件列表

许可证：任何环境

可以过滤可用的 NAT 规则条件列表来限制列表中显示的项目数量。列表会在您键入内容时进行更新，以显示匹配的项目。

如有需要，可以搜索对象名称以及为对象配置的值。例如，如果有一个名为 `Texas Office` 的网络对象，该对象配置了 `192.168.3.0/24` 这个值，且该对象包含在组对象 `US Offices` 中，则可以键入部分或完整的搜索字符串（例如 `Tex`）或者键入某个值（例如 `3`）来显示这两个对象。

以下基本步骤说明如何在新规则中过滤列表。有关添加和修改规则的完整说明，请参阅第 11-14 页上的创建和编辑 NAT 规则。

要搜索可用条件列表，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > NAT**。

系统将显示 NAT 页面。

步骤 2　点击要修改的 NAT 策略旁边的编辑图标 ( )。

系统将显示策略 Edit 页面。

步骤 3　点击 **Add Rule**。

系统将显示 Add Rule 页面。

步骤 4　要搜索列表，在搜索字段中点击以清除提示，然后输入搜索字符串。

列表会在您键入内容时进行更新以显示匹配的项目，清除列表图标 (✖) 显示在搜索字段中。列表更新，如果搜索字符串没有匹配的结果，将不会列出任何项目。

步骤 5　如有需要，点击 **Search** 字段上方的重新加载图标 ( )，或者点击 **Search** 字段中的清除图标 (✖) 以清除搜索字符串。

显示完整列表。

步骤 6　点击 **Add** 保存配置。

规则添加成功，系统将显示策略 Edit 页面。

向 NAT 规则添加文字条件

许可证：任何环境

可以向以下条件类型的原始条件列表和转换后条件列表添加文字值。

- 网络
- 端口

对于网络条件，可在原始条件列表或转换后条件列表下方的配置字段中键入文字值。

对于端口条件，可从下拉列表中选择协议。协议为 `All` 或者 `TCP` 或 `UDP` 时，可在配置字段中键入端口号。

每个相关条件页面都提供添加文字值所需的控件。如果在配置字段中键入的值是无效的，将会显示为红色文本，直至被识别为是有效值。键入的值被识别为有效值后，将会变为蓝色文本。识别到有效值后，呈灰色显示的 **Add** 按钮将会激活。添加的文字值立即显示在选定条件列表中。

有关添加每种类型的文字值的具体详细信息，请参阅以下各节：

- 第 11-23 页上的将源网络条件添加到动态 NAT 规则
- 第 11-24 页上的将目标网络条件添加到 NAT 规则
- 第 11-25 页上的向 NAT 规则添加端口条件

在 NAT 规则条件中使用对象

许可证：任何环境

在对象管理器 (**Objects > Object Management**) 中创建的对象会立即显示在相关的可用 NAT 规则条件列表中以供选择。有关信息，请参阅第 3-1 页上的管理可重用对象。

还可以通过 NAT 策略快速创建对象。相关条件页面上的控件提供对于在对象管理器中使用的相同配置控件的访问权限。

快速创建的各个对象会立即显示在可用对象列表中。可以将创建的对象添加到当前规则以及其他现有和将来的规则。在相关条件页面和策略 Edit 页面上，将指针悬停在单个对象上显示该对象的内容，将指针悬停在某个组对象上可显示该组中各个对象的编号。

处理 NAT 规则中不同类型的条件

许可证：任何环境

可以将流量与一个或多个规则条件进行匹配。有关详细信息，请参阅以下各节：

- 第 11-21 页上的向 NAT 规则添加区域条件说明如何根据用对象管理器创建的安全区域来匹配流量。
- 第 11-23 页上的将源网络条件添加到动态 NAT 规则和第 11-24 页上的将目标网络条件添加到 NAT 规则说明根据通过 IP 地址或地址块来匹配流量。
- 第 11-25 页上的向 NAT 规则添加端口条件说明如何根据指定的传输协议端口来匹配流量。

向 NAT 规则添加区域条件

许可证：任何环境

系统的安全区域包括受管设备的接口。添加到 NAT 规则的区域使规则以网络上在这些区域中有路由接口或混合接口的设备为目标。只能将带有路由接口或混合接口的安全区域添加为 NAT 规则条件。有关使用对象管理器创建安全区域的信息，请参阅第 3-34 页上的使用安全区域。

可以将当前已分配给虚拟路由器的区域或独立接口添加到 NAT 规则。如果有未应用配置的设备，Zones 页面中可用区域列表的顶部会显示警告图标 (⚠)，表明仅显示已应用的区域和接口。可以点击区域旁边的箭头图标 (▷) 来折叠或展开区域，以隐藏或查看其接口。

如果接口在集群设备上，可用区域列表将会显示该接口的一个额外分支，集群其他接口则显示为集群中主用设备的主接口的子项。也可以单击箭头图标 (▷) 来折叠或展开集群设备接口，以隐藏或查看其接口。

注　可以保存和应用带有被禁用接口的策略，但规则无法提供任何转换，直至接口被启用。

右侧列出的两个条目是供 NAT 规则用于匹配用途的源区域和目标区域。如果规则配置了值，当您编辑规则时，这些列表将显示现有值。如果源区域列表为空，规则将会匹配*来自*任何区域或接口的流量。如果目标区域列表为空，规则将会匹配*流向*任何区域或接口的流量。

对于带有绝不会在目标设备上触发的区域组合的规则，系统会显示警告。

注　可以保存和应用带有这种区域组合的策略，但规则不提供任何转换。

可以通过选择区域中的某个项目或选择独立接口来添加各个接口。如果要向其添加接口的区域未添加到源区域列表或目标区域列表，则只能在该区域中添加接口。这些单独选定的接口不受区域更改的影响，即使您删除并将其添加到不同的区域。在接口是集群的主成员的情况下，如果要配置动态规则，只可以将主接口添加到源区域列表或目标区域列表。对于静态规则，可以将各个集群成员接口添加到源区域列表。对于未添加子接口的主集群接口，只能将它添加到列表；如果未添加主接口，只能添加单个集群接口。

如果添加区域，规则会使用与添加的区域关联的所有接口。如果从区域添加或删除接口，规则不会使用区域的更新版本，直至设备配置重新应用于接口所在的设备。

注　在静态 NAT 规则中，只能添加源区域。在动态 NAT 规则中，可添加源区域和目标区域。

以下步骤说明如何在添加或编辑 NAT 规则时添加源区域条件和目标区域条件。有关更多详细信息，请参阅第 11-17 页上的了解 NAT 规则条件和条件机制。

要将区域条件添加到 NAT 规则，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择规则 Edit 页面上的 **Zones** 选项卡。

系统将显示 Zones 页面。

步骤 2　如有需要，点击 **Available Zones** 列表上方的 **Search by name** 提示，然后键入名称或值。

列表会在您键入内容时进行更新，以显示匹配的条件。有关详细信息，请参阅第 11-20 页上的搜索 NAT 规则条件列表。

步骤 3　在 **Available Zones** 列表中点击所需的区域或接口。使用 Shift 和 Ctrl 键可选择多个条件，或者右键单击并选择 **Select All**。

选定的条件将会突出显示。

步骤 4　有以下选项可供选择：

- 要根据源区域匹配流量，请点击 **Add to Source**。
- 要根据目标区域匹配流量，请点击 **Add to Destination**。

或者，可以将所选条件拖放到 **Source Zones** 或 **Destination Zones** 列表中。

所选条件添加成功。请注意，虽然可以将被禁用的接口添加到 NAT 规则，但规则不提供任何转换。

注　只能将源区域添加到静态 NAT 规则。

步骤 5　保存或继续编辑规则。

必须应用 NAT 策略来使更改生效；请参阅第 11-12 页上的应用 NAT 策略。

将源网络条件添加到动态 NAT 规则

许可证：任何环境

可以配置数据包源 IP 地址的匹配值和转换值。如果原始源网络未配置，任何源 IP 地址都会匹配动态 NAT 规则。请注意，不能配置静态 NAT 规则的源网络。如果数据包与 NAT 规则相匹配，系统会使用转换后源网络的值来为源 IP 地址分配新值。对于动态规则，则必须配置至少有一个值的转换后源网络。

注意事项　如果更改或删除正被 NAT 规则使用的网络对象或对象组，可能导致规则无效。

可以将以下任何类型的源网络条件添加到动态 NAT 规则：

- 使用对象管理器创建的单个网络对象和成组网络对象

  有关使用对象管理器创建单个网络对象和成组网络对象的信息，请参阅第 3-4 页上的使用网络对象。

- 从 Source Network 条件页面添加的单个网络对象（这些对象随后可添加到当前规则以及其他现有和将来的规则）

  有关详细信息，请参阅第 11-21 页上的在 NAT 规则条件中使用对象。

- 单个文字 IP 地址、地址范围或地址块

  有关详细信息，请参阅第 11-20 页上的向 NAT 规则添加文字条件。

以下步骤说明如何在添加或编辑动态 NAT 规则时添加源网络条件。有关更多详细信息，请参阅第 11-17 页上的了解 NAT 规则条件和条件机制。

要将网络条件添加到动态 NAT 规则，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择规则 Edit 页面上的 **Source Networks** 选项卡。

系统将显示 Source Network 页面。

步骤 2　如有需要，点击 **Available Networks** 列表上方的 **Search by name or value** 提示，然后键入名称或值。

列表会在您键入内容时进行更新，以显示匹配的条件。有关详细信息，请参阅第 11-20 页上的搜索 NAT 规则条件列表。

步骤 3　在 **Available Networks** 列表中点击要添加的条件。使用 Shift 和 Ctrl 键可选择多个条件，或者右键单击并选择 **Select All**。

选定的条件将会突出显示。

步骤 4　有以下选项可供选择：

- 要根据原始源网络匹配流量，请点击 **Add to Original**。
- 要为与转换后源网络匹配的流量指定转换值，请点击 **Add to Translated**。

或者，可以将选定的条件拖放到 **Original Source Network** 或 **Translated Source Network** 网络列表。

所选条件添加成功。

步骤 5　或者，点击 **Available Networks** 列表上方的 ( ) 图标添加单个网络对象。

可以向每个网络对象添加多个 IP 地址、 CIDR 块和前缀长度。

然后，可以根据需要选择添加的对象。有关详细信息，请参阅第 3-4 页上的使用网络对象和第 11-21 页上的在 NAT 规则条件中使用对象。

步骤 6　或者，点击 **Original Source Network** 或 **Translated Source Network** 列表下方的 **Enter an IP address** 提示；然后键入 IP 地址、地址范围或地址块并单击 **Add**。

按以下格式添加地址范围：低位 IP 地址-高位 IP 地址。例如：`179.13.1.1-179.13.1.10`。

列表更新以显示输入的条目。有关详细信息，请参阅第 11-20 页上的向 NAT 规则添加文字条件。

步骤 7　保存或继续编辑规则。

注　在更新在已应用策略中使用的动态规则中的网络条件时，系统将使用现有转换地址池丢弃任何网络会话。

必须应用 NAT 策略来使更改生效；请参阅第 11-12 页上的应用 NAT 策略。

将目标网络条件添加到 NAT 规则

许可证：任何环境

可以配置数据包目标 IP 地址的匹配值和转换值。请注意，不能为动态 NAT 规则配置转换后目标网络。

由于静态 NAT 规则是一对一转换，因此，**Available Networks** 列表仅包含只有一个 IP 地址的网络对象和网络对象组。对于静态转换，只能将一个对象或文字值添加到 **Original Destination Network** 或 **Translated Destination Network** 列表。

注意事项　如果更改或删除正被 NAT 规则使用的网络对象或对象组，可能导致规则无效。

可以将以下任何类型的目标网络条件添加到 NAT 规则：

- 使用对象管理器创建的单个网络对象和成组网络对象

  有关使用对象管理器创建单个网络对象和成组网络对象的信息，请参阅第 3-4 页上的使用网络对象。

- 从 Destination Network 条件页面添加的单个网络对象（这些对象随后可添加到当前规则以及其他现有和将来的规则）

  有关详细信息，请参阅第 11-21 页上的在 NAT 规则条件中使用对象。

- 单个文字 IP 地址、地址范围或地址块

  对于静态 NAT 规则，只能添加带子网掩码 `/32` 的 CIDR，并且只能在列表中不能已存在值的情况下添加。

  有关详细信息，请参阅第 11-20 页上的向 NAT 规则添加文字条件。

以下步骤说明如何在添加或编辑 NAT 规则时添加目标网络条件。有关更多详细信息，请参阅第 11-17 页上的了解 NAT 规则条件和条件机制。

要将目标网络条件添加到 NAT 规则，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择规则 Edit 页面上的 **Destination Network** 选项卡。

系统将显示Destination Network 页面。

步骤 2　如有需要，点击 **Available Networks** 列表上方的 **Search by name or value** 提示，然后键入名称或值。

列表会在您键入内容时进行更新，以显示匹配的条件。有关详细信息，请参阅第 11-20 页上的搜索 NAT 规则条件列表。

步骤 3　在 **Available Networks** 列表中点击要添加的条件。使用 Shift 和 Ctrl 键可选择多个条件，或者右键单击并选择 **Select All**。

选定的条件将会突出显示。

步骤 4　有以下选项可供选择：

- 要根据原始目标网络匹配流量，请点击 **Add to Original**。
- 要为与转换后目标网络匹配的流量指定转换值，请点击 **Add to Translated**。

或者，可以将选定的条件拖放到 **Original Destination Network** 或 **Translated Destination Network** 网络列表。

所选条件添加成功。

步骤 5　或者，点击 **Available Networks** 列表上方的 ( ) 图标添加单个网络对象。

对于动态规则，可以向每个网络对象添加多个 IP 地址、 CIDR 块和前缀长度。对于静态规则，只能添加一个 IP 地址。然后，可以根据需要选择添加的对象。有关详细信息，请参阅第 3-4 页上的使用网络对象和第 11-21 页上的在 NAT 规则条件中使用对象。

步骤 6　或者，点击 **Original Destination Network** 或 **Translated Destination Network** 列表下方的 **Enter an IP address** 提示，然后键入 IP 地址、地址范围或地址块并单击 **Add**。

列表更新以显示输入的条目。有关详细信息，请参阅第 11-20 页上的向 NAT 规则添加文字条件。

步骤 7　保存或继续编辑规则。

注　在更新在已应用策略中使用的动态规则中的网络条件时，系统将使用现有转换地址池丢弃任何网络会话。

必须应用 NAT 策略来使更改生效；请参阅第 11-12 页上的应用 NAT 策略。

向 NAT 规则添加端口条件

许可证：任何环境

可以根据原始目标端口、转换后目标端口和用于转换的传输协议将端口条件添加到与网络流量匹配的规则。如果未配置原始端口，任何目标端口都会匹配该规则。如果数据包与 NAT 值相匹配，并且转换后目标端口已配置，系统会将端口转换为该值。请注意，对于动态规则，只能指定原始目标端口。对于静态规则，可以定义转换后目标端口，但前提是，转换后目标端口所带有的对象与原始目标端口对象或文字值使用相同的协议。

对于静态规则，系统会将目标端口与原始目标端口列表中端口对象或文字对象的值进行匹配；对于动态规则，会将目标端口与多个值进行匹配。

由于静态 NAT 规则是一对一转换，因此，**Available Ports** 列表仅包含只有一个端口的端口对象和端口对象组。对于静态转换，只能将一个对象或文字值添加到 **Original Port** 或 **Translated Port** 列表。

对于动态规则，可以添加一系列端口。例如，在指定原始目标端口时，可以添加 `1000-1100` 作为文字值。

注意事项　如果更改或删除正被 NAT 规则使用的对象或对象组，可能导致规则无效。

可以将以下任何类型的端口条件添加到 NAT 规则：

- 使用对象管理器创建的单个端口对象和成组端口对象

  有关使用对象管理器创建单个端口对象和成组端口对象的信息，请参阅第 3-10 页上的使用端口对象。
- 从 Destination Ports 条件页面添加的单个网络对象（这些对象随后可添加到当前规则以及其他现有和将来的规则）

  有关详细信息，请参阅第 11-21 页上的在 NAT 规则条件中使用对象。
- 文字端口值，由 TCP、UDP、All（TCP 和 UDP）传输协议和一个端口组成

  有关详细信息，请参阅第 11-20 页上的向 NAT 规则添加文字条件。

以下步骤说明如何在添加或编辑 NAT 规则时添加端口条件。有关更多详细信息，请参阅第 11-17 页上的了解 NAT 规则条件和条件机制。

要将端口条件添加到 NAT 规则，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择规则 Edit 页面上的 **Destination Port** 选项卡。

系统将显示Destination Port 页面。

步骤 2　如有需要，点击 **Available Ports** 列表上方的 **Search by name or value** 提示，然后键入名称或值。

列表会在您键入内容时进行更新，以显示匹配的条件。有关详细信息，请参阅第 11-20 页上的搜索 NAT 规则条件列表。

步骤 3　在 **Available Ports** 列表中点击要添加的条件。使用 Shift 和 Ctrl 键可选择多个条件，或者右键单击选择所有条件。请注意，最多可以添加 50 个条件。

选定的条件将会突出显示。

步骤 4　有以下选项可供选择：

- 点击 **Add to Original** 将所选端口添加到 Original Ports 列表。
- 点击 **Add to Translated** 将所选端口添加到 Translated Ports 列表。
- 将可用端口拖放到列表。

步骤 5　或者，如果要创建并添加单个端口对象，请点击 **Available Ports** 列表上方的添加 ( ) 图标。

可以在添加的每个端口对象中确定单个端口或端口范围。然后，可以选择添加的对象作为规则的条件。有关详细信息，请参阅第 11-21 页上的在 NAT 规则条件中使用对象。

对于静态规则，只能使用带有单个端口的端口对象。

步骤 6　或者，如果要添加文字端口，请从 **Original Port** 或 **Translated Port** 列表下方的 **Protocol** 下拉列表选择条目。

输入端口，然后点击 **Add**。可以指定 0 至 65535 的端口号。对于动态规则，可以指定单个端口或端口范围。

列表更新以显示所选的内容。有关详细信息，请参阅第 11-20 页上的向 NAT 规则添加文字条件。

所选条件添加成功

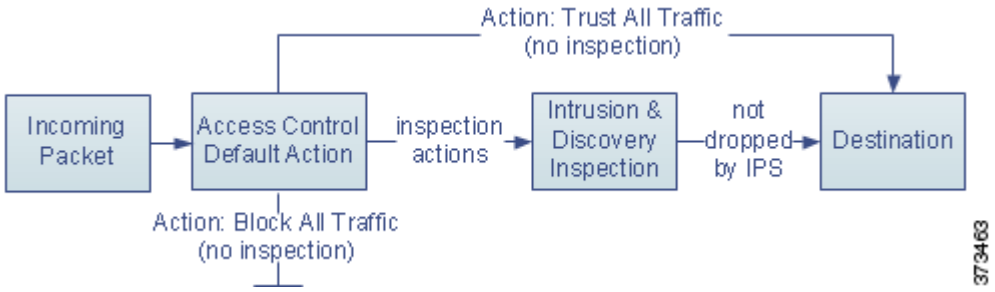
步骤 7　保存或继续编辑规则。

必须应用 NAT 策略来使更改生效；请参阅第 11-12 页上的应用 NAT 策略。

访问控制策略入门

*访问控制策略*确定系统如何处理网络上的非快速路径流量。可以配置一个或多个访问控制策略，然后应用于一个或多个受管设备。目前，只能为每个设备应用一个策略。

最简单的访问控制策略指导其目标设备使用其*默认操作*处理所有流量。可以将此默认操作设置为阻止或信任所有流量而不进一步检查，或者检查流量中是否存在入侵和发现数据。



请注意，只有内联部署的设备才能影响流量的流动。将配置为阻止或修改流量的访问控制策略应用于被动部署的设备会出现意外结果。在某些情况下，系统会阻止将内联配置应用于被动部署的设备。

本章说明如何创建和应用简单访问控制策略。它还包含有关管理访问控制策略的基本信息：编辑、更新、比较等等。有关详情，请参阅：

更复杂的访问控制策略可以根据安全情报数据将流量列入黑名单，以及使用*访问控制规则*对网络流量日志记录和处理实行精细控制。这些规则可能很简单，也可能很复杂，使用多个条件来匹配和检查流量。高级访问控制策略选项控制解密、预处理、性能和其他一般首选项。

在创建基本访问控制策略后，请参阅以下章节以获取有关根据部署定制该策略的详细信息：

- 第 13-1 页上的使用安全情报 IP 地址信誉实施黑名单说明如何根据最新信誉情报将连接立即列入黑名单（阻止）。
- 第 19-1 页上的了解流量解密说明如何使用 SSL 策略阻止加密流量而不对其进行检查，或者选择在解密流量后将其传递到访问控制规则。
- 第 23-1 页上的了解网络分析和入侵策略说明网络分析和入侵策略作为系统的入侵检测和防御功能的一部分如何预处理并检查数据包。
- 第 14-1 页上的使用访问控制规则调整流量说明访问控制规则如何提供跨多个受管设备处理网络流量的精细方法。
- 第 18-1 页上的使用入侵和文件策略控制流量说明了入侵和文件策略如何通过检测并（可选）阻止入侵、受禁文件和恶意软件，在允许流量流向其目标之前提供最后一道防线。

访问控制许可证和角色要求

虽然无论防御中心上的许可证如何都可创建访问控制策略，但是许多功能要求在应用策略之前启用相应的许可证。此外，某些功能仅在特定型号上可用。

另请注意，可用的访问控制相关功能和操作取决于用户角色。系统包含为各种管理员和分析师设计的预定义用户角色，并且可以使用专用访问权限创建自定义用户角色。

有关详情，请参阅：

- 第 12-2 页上的访问控制的许可证和型号要求
- 第 12-3 页上的使用自定义用户角色管理部署

访问控制的许可证和型号要求

尽管无论防御中心上的许可证如何，都可以创建访问控制策略，但在访问控制的某些方面时，要求在应用策略之前先启用目标设备上的特定许可功能。此外，某些功能仅在特定型号上可用。

警告图标和确认对话框指定部署不支持的功能。有关详细信息，请将指针悬停在警告图标上方并参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

下表说明应用访问控制策略的许可证和设备型号要求。请注意， 2 系列设备自动启用大多数保护功能，无需特意启用保护。

表 12-1　　访问控制的许可证和型号要求

要应用以下访问控制策略...	许可证	支持的防御中心	支持的设备
根据区域、网络、 VLAN 或端口执行访问控制 使用文本 URL 和 URL 对象执行 URL 过滤	任意	任意	任意，以下除外： • 2 系列设备无法执行 URL 过滤 • ASA FirePOWER 设备无法执行 VLAN 过滤
执行 SSL 检查；请参阅第 12-3 页上的表 12-2	任意	任意，不同在于 DC500 限用于网络、应用和 SSL 相关控制	3 系列

表 12-1　访问控制的许可证和型号要求 （续）

要应用以下访问控制策略...	许可证	支持的防御中心	支持的设备
使用地理位置数据执行访问控制（源或目标国家/地区或大洲）	FireSIGHT	任意， DC500 除外	3 系列 虚拟 ASA FirePOWER
执行入侵检测与防御、文件控制或者安全情报过滤	保护	任意	任意，不同在于 2 系列设备无法执行安全情报过滤
执行高级恶意软件防护，即基于网络的恶意软件检测与阻止	恶意软件	任意， DC500 除外	任意， 2 系列或 X -系列除外
执行用户或应用控制	可控性	任意，不同在于 DC500 无法执行用户控制	任意， 2 系列或 X -系列除外
使用类别和信誉数据执行 URL 过滤	URL 过滤	任意， DC500 除外	任意， 2 系列除外

下表说明为应用通过调用 SSL 策略来执行 SSL 检查的访问控制策略而必须具有的许可证。

表 12-2　SSL 检查的许可证和型号要求

要应用以下 SSL 策略...	许可证	支持的防御中心	支持的设备
根据区域、网络、 VLAN、端口或 SSL 相关条件处理加密流量	任意	任意	3 系列
使用地理位置数据处理加密流量	FireSIGHT	任意， DC500 除外	3 系列
使用应用或用户条件处理加密流量	控制	任意，不同在于 DC500 无法执行用户控制	3 系列
使用 URL 类别和信誉数据过滤加密流量	URL 过滤	任意， DC500 除外	3 系列

使用自定义用户角色管理部署

许可证：因功能而异

如第 61-48 页上的管理自定义用户角色中所述，可以创建具有特殊化访问权限的自定义用户角色。自定义用户角色可以具有任何基于菜单的权限集和系统权限集，并且可能完全是原始的或基于预定义用户角色。访问控制相关功能的自定义角色决定用户是否可以查看、修改和应用访问控制、入侵和文件策略，以及是否可以在 Administrator Rules 或 Root Rules 类别中插入或修改规则。

下表展现了五个决定 FireSIGHT 系统用户如何与访问控制功能交互的示例自定义角色。该表以在创建自定义用户角色时的显示顺序，列出了每个自定义角色需要的权限。

表 12-3　示例访问控制自定义角色

自定义角色权限	Access Control & SSL Editor	Intrusion & Network Analysis Editor	File Policy Editor	Policy Applier (All)	Intrusion Policy Applier
Access Control	是	否	否	是	是
Access Control List	是	否	否	是	是
Modify Access Control Policy	是	否	否	否	否
Apply Intrusion Policies	否	否	否	是	是

表 12-3　　示例访问控制自定义角色 （续）

自定义角色权限	Access Control & SSL Editor	Intrusion & Network Analysis Editor	File Policy Editor	Policy Applier (All)	Intrusion Policy Applier
Apply Access Control Policies	否	否	否	是	否
Intrusion（还授予网络分析权限）	否	是	否	否	否
Intrusion Policy	否	是	否	否	否
Modify Intrusion Policy	否	是	否	否	否
File Policy	否	否	是	否	否
Modify File Policy	否	否	是	否	否
SSL	是	否	否	否	否
Modify SSL Policy	是	否	否	否	否
Apply SSL Policy	否	否	否	是	否

请注意，如果 FireSIGHT 系统用户帐户的角色限制为 Intrusion Policy 或 Modify Intrusion Policy，则可以创建和编辑网络分析及入侵策略。

系统根据用户可以应用完整访问控制策略（包括入侵策略）、仅入侵策略还是无法应用任一策略来以不同方式呈现 Web 界面。例如，上表中的 Intrusion Policies Appliers 可以查看访问控制策略和应用入侵策略，但无法编辑任一策略。他们既无法应用访问控制策略，也无法查看文件或 SSL 策略。在此情况下，在 Web 界面中：

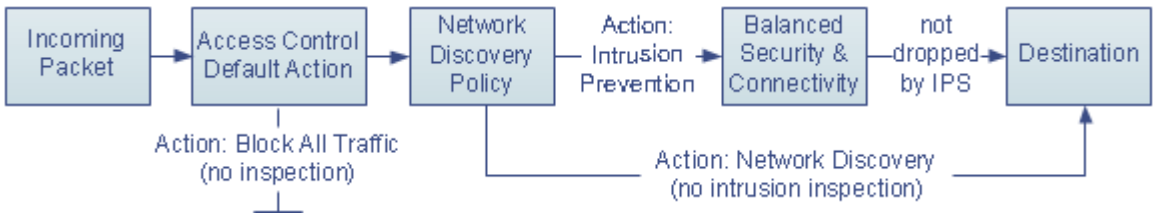
- Access Control Policy 页面上不显示编辑图标 ( )
- Access Control Policy 页面上不显示删除图标 ( )
- 快速应用弹出窗口仅应用入侵策略
- 详细应用弹出窗口中的访问控制策略复选框已禁用

创建基本访问控制策略

许可证：任何环境

创建新访问控制策略时，必须为其提供唯一名称并指定默认操作。此时，默认操作确定策略的目标设备如何处理所有非快速路径流量；稍后将会添加影响流量的其他配置。尽管在创建时不要求识别策略目标，但是必须先执行此步骤，然后才能应用策略。

创建新策略时，可以将默认操作设置为阻止所有流量而不进一步检查，或者检查入侵和发现数据的流量，如下图所示。



提示　首次创建访问控制策略时，不能选择信任流量作为默认操作。如果要在默认情况下信任所有流量，请在创建策略后更改默认操作。

使用 Access Control Policy 页面 (**Policies > Access Control**) 创建新访问控制策略和管理现有访问控制策略。根据是否将设备注册到防御中心以及注册方式，两个预定义访问控制策略中的任一策略可能会显示并已应用于设备：

- Default Access Control 策略阻止所有流量而不进一步检查。
- Default Intrusion Prevention 策略允许所有流量，但是还会使用 Balanced Security and Connectivity 入侵策略和默认入侵变量集进行检查。

可以使用和修改其中任一访问控制策略。请注意，这些默认策略均未启用日志记录。

要创建访问控制策略，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

提示　您还可以从此防御中心复制现有策略或从另一个防御中心导入策略。要复制策略，请点击复制图标 ( )。要导入策略，请参阅第 A-1 页上的导入和导出配置。

步骤 2　点击 **New Policy**。

系统将显示 New Access Control Policy 弹出窗口。

步骤 3　在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

可以使用所有的可打印字符，包括空格和特殊字符，井号 (#)、分号 (;) 或大括号 ({}) 除外。名称必须包含至少一个非空格字符。

步骤 4　指定初始 **Default Action**：

- **Block all traffic** 使用默认操作 **Access Control: Block All Traffic** 创建策略。
- **Intrusion Prevention** 使用默认操作 **Intrusion Prevention: Balanced Security and Connectivity** 创建策略。
- **Network Discovery** 使用默认操作 **Network Discovery Only** 创建策略。

有关选择初始默认操作以及今后如何对其进行更改的指导，请参阅第 12-6 页上的设置对网络流量的默认处理和检查。

步骤 5　在 **Available Devices** 中选择要应用策略的设备。

使用 Ctrl 和 Shift 键可选择多台设备，或者右键单击以选择 **Select All**。要减少显示的设备，请在 **Search** 字段中键入搜索字符串。如果跳过添加目标设备，请参阅第 12-8 页上的为访问控制策略设置目标设备以获取有关稍后添加这些设备的信息。

步骤 6　点击 **Add to Policy** 添加所选设备。

您也可以拖放所选对象。

步骤 7　点击 **Save**。

系统将显示访问控制策略编辑器。有关配置新策略的信息，请参阅第 12-10 页上的编辑访问控制策略。请注意，策略在应用后才会生效；请参阅第 12-13 页上的应用访问控制策略。

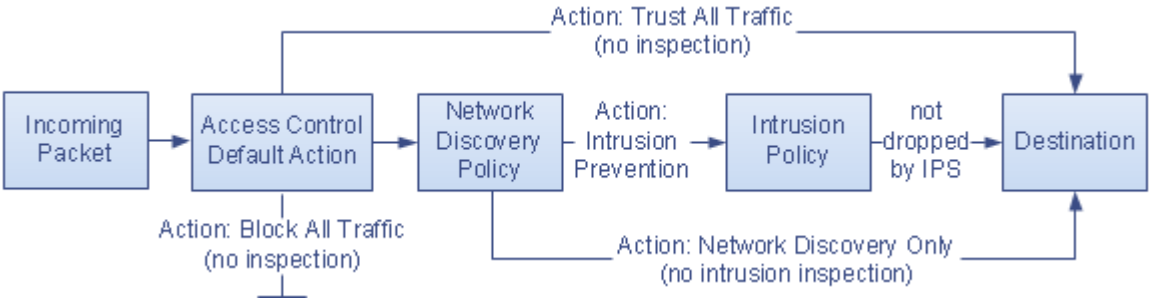
设置对网络流量的默认处理和检查

许可证：任何环境

在创建访问控制策略时，必须选择默认操作。访问控制策略的默认操作决定系统如何处理如下流量：

- 未被安全情报列入黑名单
- 未被 SSL 检查阻止（仅限加密流量）
- 不与策略中的任何规则相匹配（Monitor 规则除外，该规则匹配并记录但不处理或检查流量）

因此，当应用的访问控制策略不包含任何访问控制规则或安全情报配置，并且不调用 SSL 策略来处理加密流量时，默认操作确定如何处理网络上的*所有*流量。可以阻止或信任所有流量而不进一步检查，或者检查入侵和发现数据的流量。下图中显示选项。

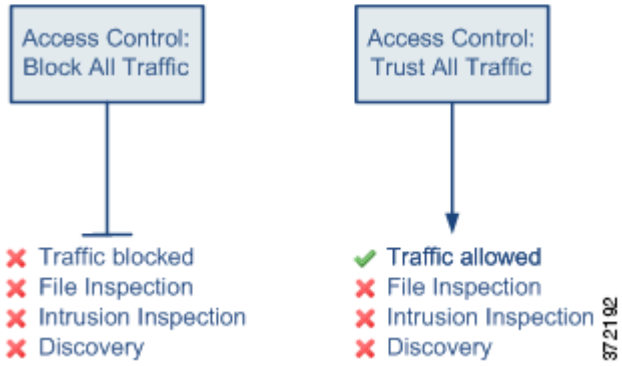


下表描述不同的默认操作如何处理流量，并列出可对由每个默认操作处理的流量执行的检查类型。请注意，**不能**对由默认操作处理的流量执行文件或恶意软件检查。有关详细信息，请参阅第 18-1 页上的使用入侵和文件策略控制流量。

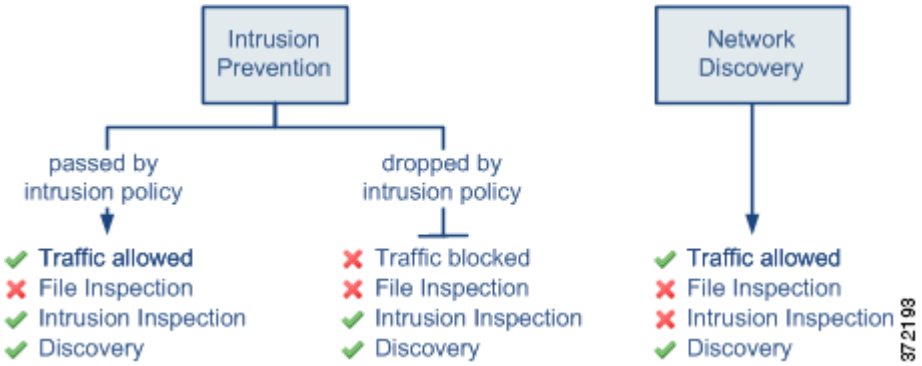
表 12-4　访问控制策略默认操作

默认操作	对流量的影响	检查类型和策略
Access Control: Block All Traffic	阻止，无需进一步检查	无
Access Control: Trust All Traffic	信任（允许到达其最终目标而不进一步检查）	无
Intrusion Prevention	允许，只要其是由指定的入侵策略传递即可 （需要保护）	入侵，使用指定的入侵策略和关联变量集，以及发现、使用网络发现策略
Network Discovery Only	允许	仅发现，使用网络发现策略

下图说明 **Block All Traffic** 和 **Trust All Traffic** 默认操作。



下图说明 **Intrusion Prevention** 和 **Network Discovery Only** 默认操作。



提示　**Network Discovery Only** 的目的是在仅发现部署中提高性能。如果您仅对入侵检测和防御感兴趣，则不同的配置可以禁用发现。有关详细信息，包括必须遵循的其他准则，请参阅第 12-17 页上的 IPS 或仅发现性能注意事项。

首次创建访问控制策略时，默认情况下已禁用由默认操作处理的日志记录连接。如果选择用于执行入侵检测的默认操作，系统会自动将默认入侵变量集与选择的入侵策略相关联。创建策略后，可以更改其中任一选项以及默认操作本身。

要更改访问控制策略的默认操作及相关选项，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Default Action**。

- 如要阻止所有流量，选择 **Access Control: Block All Traffic**。
- 如要信任所有流量，选择 **Access Control: Trust All Traffic**。

- 如要允许所有流量，并用网络发现对其进行检查，选择 **Network Discovery Only**。
- 如要同时使用网络发现和入侵策略检查所有流量，选择一项入侵策略，所有入侵策略都以标签 **Intrusion Prevention** 开头。记住，入侵策略可以阻止流量。

注意事项　请勿使用 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 4　如果选择 **Intrusion Prevention** 默认操作，请点击变量图标 ( ) 更改与所选入侵策略关联的变量集。

在显示的弹出窗口中，选择新变量集，然后点击 **OK**。您还可以通过点击编辑图标 ( ) 在新窗口中编辑所选变量集。如果不更改此变量集，系统将使用默认变量集。有关详细信息，请参阅第 3-15 页上的使用变量集。

步骤 5　点击日志记录图标 ( ) 更改由默认操作处理的连接的日志记录选项。

根据默认操作，可以在其开头和/或结尾记录匹配连接。可以将连接记录到防御中心数据库、外部系统日志 (syslog) 或 SNMP 陷阱服务器。有关详细信息，请参阅第 38-15 页上的记录访问控制默认操作处理的连接。

为访问控制策略设置目标设备

许可证：任何环境

必须先识别要应用访问控制策略的受管设备，然后才能应用该策略。可以在创建策略时识别要为其应用策略的设备，也可以稍后添加这些设备。

下表总结了管理目标设备时可执行的操作。

表 12-5　目标设备管理操作

要.....	您可以.....
搜索可用设备列表	在搜索字段中点击，然后键入搜索字符串。设备列表会在您键入内容时进行更新，以显示匹配的设备名称。
清除对可用设备的搜索	在搜索字段中点击清除图标 ( )。
选择可以添加至选定目标列表的可用设备	点击要添加的设备的名称；使用 Ctrl 和 Shift 键可选择多台设备。还可以右键单击一个可用设备，然后点击 **Select All**。
添加选定设备	点击 **Add to Policy** 或拖放到所选设备列表中。
从 Selected Devices 列表中删除单个设备	点击设备旁边的删除图标 ( )，或者右键单击设备，然后选择 **Delete**。
从 Selected Devices 列表删除多台设备	使用 Ctrl 和 Shift 键选择多台设备，右键单击以突出显示某个选定设备的行，然后点击 **Delete Selected**。

请注意，不能以运行不同系统版本的堆叠设备作为目标（例如，如果其中一台设备的升级失败）。可以将设备堆栈作为目标，但不能以堆栈内的单个设备为目标。有关详情，请参见第 4-37 页上的管理堆叠设备。

要在访问控制策略中管理目标设备，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　点击设备目标链接，然后点击 **Manage Targets**。

屏幕上将会显示 Manage Device Targets 弹出窗口。

步骤 4　制定目标联系人列表。

使用第 12-8 页上的表 12-5 中汇总的操作。

步骤 5　点击 **OK**。

系统会将配置添加到策略中并显示访问控制策略编辑器。

管理访问控制策略

许可证：任何环境

在 Access Control Policy 页面 (**Policies > Access Control**) 上，可以查看当前自定义访问控制策略，并在适当情况下查看以下信息：

- 使用每个访问控制策略检查流量的设备的数量，包括有关策略仅应用于其某些目标还是应用于该策略当前未锁定为目标的设备的信息
- 其中每个策略过期的目标设备的数量，以及有关当前在编辑每个策略的人员（如果有）的信息

除创建的自定义策略之外，系统还可提供三种自定义策略：Default Access Control、 Default Intrusion Prevention 和 Default Network Discovery。系统根据在设备初始配置期间为其选择的检测模式，在初始设备注册期间创建这些策略。可以编辑并使用这些系统提供的自定义策略。请注意，设备的检测模式不是一个以后可以更改的设置；它只是您在设置期间选择的一个选项，用于帮助系统定制该设备的初始配置。

通过 Access Control Policy 页面上的选项，可以采取下表中的操作。

表 12-6　访问控制策略管理操作

要.....	您可以.....	请参阅.....
创建新的访问控制策略	点击 **New Policy**。	第 12-4 页上的创建基本访问控制策略
编辑现有访问控制策略。	点击编辑图标 ( )。	第 12-10 页上的编辑访问控制策略
将访问控制策略重新应用于受管设备	点击应用图标 ( )。	第 12-13 页上的应用访问控制策略
导出要在另一个防御中心上导入的访问控制策略	点击导出图标 ( )	第 A-1 页上的导出配置

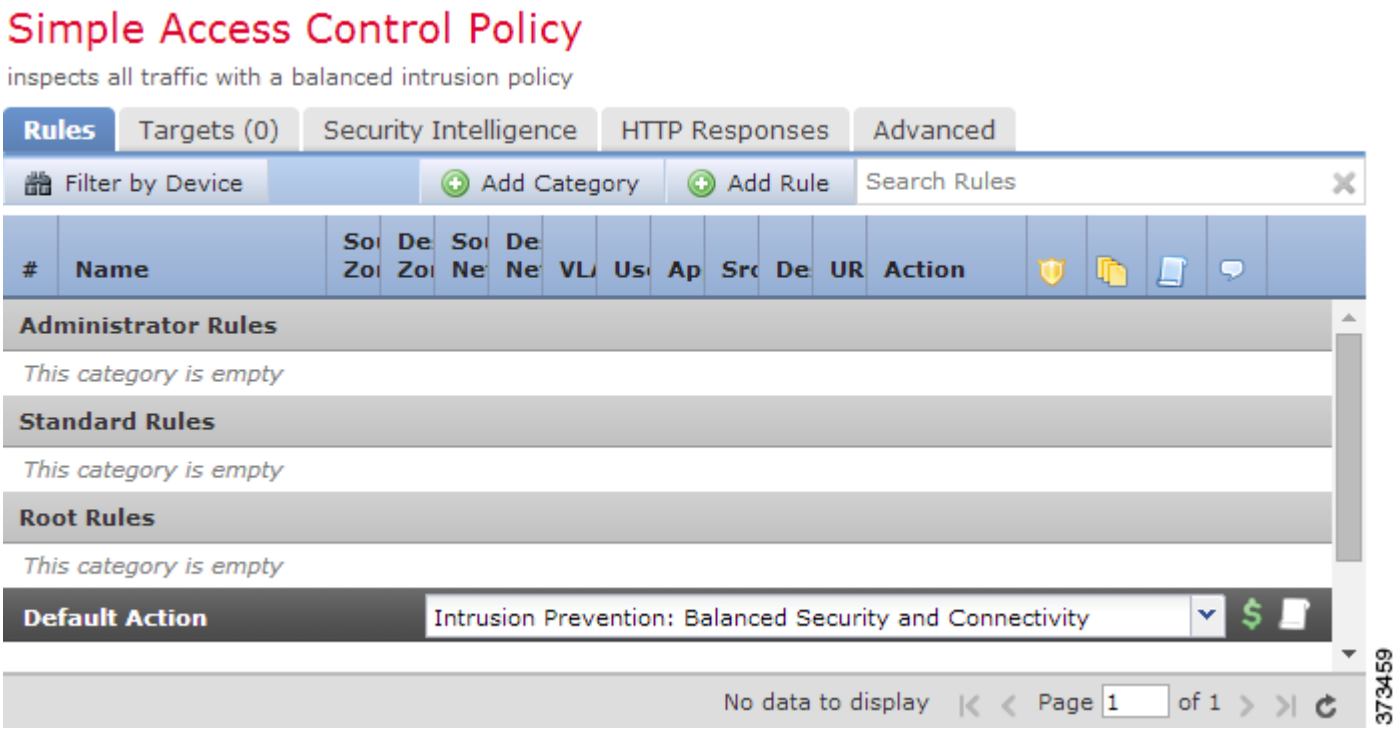
表 12-6　访问控制策略管理操作 （续）

要.....	您可以.....	请参阅.....
查看在访问控制策略中列出当前配置设置的 PDF 报告	点击报告图标 ( )。	第 12-21 页上的生成当前访问控制设置报告
比较访问控制策略	点击 **Compare Policies**。	第 12-22 页上的比较访问控制策略
删除访问控制策略	点击删除图标 ( )，然后确认要删除策略。不能删除已应用或当前正在应用的访问控制策略。	

编辑访问控制策略

许可证：任何环境

首次创建新的访问控制策略时，会显示访问控制策略编辑器且焦点在 Rules 选项卡上。下图显示新创建的策略。由于新策略还没有规则或其他配置，因此默认操作处理*所有*流量。在此情况下，默认操作使用系统提供的 Balanced Security and Connectivity 入侵策略检查未加密流量，然后才允许其到达其最终目标。请注意，默认情况下，系统对加密负载禁用文件和入侵检查。



使用访问控制策略编辑器可添加和组织规则，指定将会使用策略的设备，等等。以下列表提供有关可以更改的策略配置的信息。

名称和描述

要更改策略的名称和描述，请点击相应的字段并键入新的名称或描述。

目标

在您可以应用访问控制策略之前，请使用 Targets 选项卡识别受管设备，包括要应用策略的设备组。有关详细信息，请参阅第 12-8 页上的为访问控制策略设置目标设备。

安全智能

安全情报是抵御恶意互联网内容的第一道防线。通过此功能可根据最新信誉情报立即将连接列入黑名单（阻止）。要确保连续访问重要资源，可以使用自定义白名单覆盖黑名单。此流量过滤发生在任何其他基于策略的检测、分析或流量处理（包括规则和默认操作）**之前**。有关详细信息，请参阅第 13-1 页上的使用安全情报 IP 地址信誉实施黑名单。

规则

规则提供了一种精细的网络流量处理方法。系统已对访问控制策略中的规则进行编号，从 1 开始。系统会用升序的规则号码以从上到下的顺序将流量匹配到访问控制规则中。

在大多数情况下，系统根据*第一个*访问控制规则（规则的*所有*条件都与流量相匹配）处理网络流量。这些条件包括安全区域、网络或地理位置、VLAN、端口、应用、所请求的 URL 或用户。条件可以简单也可以复杂；其使用通常取决于某些许可证和设备型号。

使用 Rules 选项卡可添加、分类、启用、禁用、过滤和以其他方式管理规则。有关详细信息，请参阅第 14-1 页上的使用访问控制规则调整流量。

默认操作

默认操作确定系统如何处理未被安全情报列入黑名单且与任何访问控制规则均不匹配的流量。使用默认操作可以阻止或信任所有流量而不进一步检查，或者检查入侵和发现数据的流量。您还可以选择自定义变量集（如果已创建），并启用或禁用由默认操作处理的连接的日志记录。

有关详细信息，请参阅第 12-6 页上的设置对网络流量的默认处理和检查和第 38-13 页上的根据访问控制处理记录连接。

HTTP 响应

可以指定当系统阻止用户的网站请求时该用户在浏览器中查看的内容 - 显示通用的系统提供的响应页面，或者输入自定义 HTML。您还可以显示以下页面：对用户进行警告，但也允许其点击按钮以继续操作或者刷新该页面以加载原先请求的站点。有关详细信息，请参阅第 16-15 页上的显示被阻止 URL 的自定义网页。

高级访问控制选项

高级访问控制策略设置通常只需要进行很小的修改或不需要修改。默认设置适用于大多数的部署。可以修改的高级设置包括：

- 在防御中心数据库中为用户请求的每个 URL 存储的字符数；请参阅第 38-16 页上的记录在连接中检测到的 URL
- 在用户绕过初始阻止后重新阻止网站之前的时间长度；请参阅第 16-14 页上的为被阻止网站设置用户旁路超时
- 用于监控、解密、阻止或允许使用安全套接字层 (SSL) 或传输层安全 (TLS) 加密的应用层协议流量的 SSL 策略；请参阅第 20-8 页上的使用访问控制应用解密设置
- 在策略应用期间允许流量检查或对安全连接禁用流量检查；请参阅第 12-13 页上的应用访问控制策略
- 允许根据网络、区域和 VLAN 定制许多预处理选项以及设置默认入侵检测行为的网络分析和入侵策略设置；请参阅第 25-1 页上的自定义流量预处理
- 全局应用于所有网络、区域和 VLAN （其中会应用访问控制策略）的高级传输和网络预处理器设置；请参阅第 29-1 页上的配置高级传输/网络设置

- 用于根据网络的主机操作系统改进被动部署中数据包片段和 TCP 数据流的重组的自适应配置文件；请参阅第 30-1 页上的调整被动部署中的预处理
- 入侵检测、文件控制、文件存储、动态分析和高级恶意软件防护的性能选项；请参阅第 18-7 页上的调整的入侵防御性能和第 18-17 页上的调整文件和恶意软件检查性能和存储

当您编辑访问控制策略时，会有一条消息指明您有未保存的更改。要保留更改，必须在退出策略编辑器之前保存策略。如果尝试退出策略编辑器而不保存更改，系统会提醒您有未保存的更改；您可以废弃更改并退出策略，或者返回到策略编辑器。

为保护您会话的隐私，在策略编辑器上不执行操作超过 60 分钟后，系统将丢弃对您策略做出的更改，您将返回 Access Control Policy 页面。无活动时间的前 30 分钟过后，屏幕上将会显示一条消息，并会定期更新以提供更改被放弃前的剩余分钟数。在页面上进行任何操作都会取消定时器。

当尝试在两个浏览器窗口中编辑同一策略时，系统会提示您执行以下哪种操作：在新窗口中恢复编辑，废弃原始窗口中的更改并继续在新窗口中编辑；或者取消第二个窗口并返回到策略编辑器。

当多个用户并发编辑同一策略时，策略编辑器上每个用户的对应消息表明其他用户有未保存的更改。任何尝试保存其更改的用户都会获得其更改将会覆盖其他用户的更改的提醒。当多个用户保存相同的策略时，最后保存的更改将会保留。

要编辑访问控制策略，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　编辑策略。采取以上汇总的任何操作。

步骤 4　保存或废弃配置：

- 要保存更改并继续编辑，请点击 **Save**。
- 要保存更改并应用策略，请点击 **Save and Apply**。请参阅第 12-13 页上的应用访问控制策略。
- 要放弃更改，请点击 **Cancel**；如果出现提示，点击 **OK**。

了解过期策略警告

许可证：任何环境

在 Access Control Policy 页面 (**Policies > Access Control**) 上，过期策略用红色状态文本标记，指示其需要策略更新的目标设备的数量。

在几乎每种情况下，只要更改访问控制策略，便必须将其重新应用以使更改生效。如果访问控制策略调用其他策略或依靠其他配置，则更改这些策略或配置也要求重新应用访问控制策略（或者，对于入侵策略更改，可以仅重新应用入侵策略）。

要求重新应用策略的配置更改包括：

- 修改访问控制策略本身：对访问控制规则、默认操作、策略目标、安全情报过滤、高级选项（包括 NAP 规则）等等的任何更改。
- 更改访问控制策略调用的任何策略：SSL 策略、网络分析策略、入侵策略和文件策略。

- 更改访问控制策略中使用的任何可重用对象或配置，或其调用的策略：网络、端口、 VLAN 标记、 URL 和地理定位对象；安全情报列表和源；应用过滤器或检测器；入侵策略变量集；文件列表；解密相关对象、安全区域等等。
- 更新系统软件、入侵规则或漏洞数据库 (VDB)。

请记住，可以从 Web 界面中的多个位置更改其中某些配置。例如，可以使用对象管理器 (**Objects > Object Management**) 修改安全区域，但是修改设备配置 (**Devices > Device Management**) 中的接口类型还会修改区域并要求重新应用策略。

请注意，以下更新**不**要求重新应用策略：

- 使用上下文菜单自动对安全情报源进行更新和对安全情报全局黑名单或白名单进行添加
- 自动更新 URL 过滤数据
- 计划的地理定位数据库 (GeoDB) 更新

要确定访问控制或入侵策略过期的原因，请使用比较查看器。

要确定访问控制策略过期的原因，请执行以下操作：

访问：管理员/安全审批者

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。过期的策略会用红色状态文本标记，表明其需要策略更新的目标设备的数量。

步骤 2　点击过期策略的策略状态。

系统将显示详细的 Apply Access Control Policy 弹出窗口。

步骤 3　点击您感兴趣的已更改部分旁的 **Out-of-date**。

在新窗口中显示策略比较报告。有关详细信息，请参阅第 12-22 页上的比较访问控制策略和第 31-9 页上的比较两个入侵策略或版本。

步骤 4　或者，重新应用策略。

请参阅下一节应用访问控制策略。

应用访问控制策略

许可证：任何环境

在更改访问控制策略后，必须将策略应用于一个或多个目标设备，以对设备监控的网络实施更改。尽管可以应用访问控制策略及其关联入侵策略的任意组合，但是应用访问控制策略会自动应用所有关联 SSL、网络分析和文件策略。无法独立应用这些策略。

注意事项

在高级选项卡选中 **Inspect Traffic During Policy Apply** 选项后，将不允许在策略应用期间因连接的简短中断而使任何未检查的流量通过。如果相比于已检查的流量，您更注重连接，请取消选中 **Inspect Traffic During Policy Apply** 选项以在无中断的情况下允许未检查的流量。在 3D7010、3D7020 和 3D7030 受管设备上，应用访问控制策略最多可能需要五分钟时间。为尽量减少不便，请在更改窗口期间应用访问控制策略或保持选中 **Inspect Traffic During Policy Apply** 选项。

当 Snort® 进程重新启动时，会发生流量中断；例如，在防御中心应用升级后将新版本 Snort 推送至受管设备的访问控制策略时，在包含共享对象规则的规则导入后首次应用策略时，以及在某些情况下安装 VDB 更新时，该进程会重新启动。如果通过高级选项卡选中 **Inspect Traffic During Policy Apply**，则系统在策略应用期间会继续检查流量。

提示 如果在使用内联部署的 用于 Blue Coat X-系列的思科 NGIPS，而且配置了多 VAP 的 VAP 组以实现负载均衡和冗余性，可以从负载均衡列表移除受影响的 VAP，直到设备重新启动，然后将其恢复，从而避免处理暂停。

请注意，只有内联部署的设备才能影响流量的流动。将配置为阻止或修改流量的访问控制策略应用于被动部署的设备会出现意外结果。例如，由于受阻止连接在被动部署中未实际受阻止，因此系统可能会为每个受阻止连接报告多个连接开始事件。

在某些情况下，系统会阻止将内联配置应用于被动部署的设备，包括分路模式下的内联设备。例如，在被动部署中，您不能应用会引用以下 SSL 策略的访问控制策略：阻止加密流量，或配置为对已解密流量重新签名。此外，被动部署也不支持解密使用短 Diffie-Hellman (DHE) 或椭圆曲线 Diffie-Hellman (ECDHE) 密码套件加密的流量。

应用访问控制策略时，请另外谨记以下要点：

- 某些功能对许可证、最低系统版本或设备型号都有具体要求。有关详细信息，请参阅第 12-2 页上的访问控制的许可证和型号要求，以及您在受管设备上运行的系统版本的版本说明。如果访问控制策略需要许可证通过最近应用的设备配置启用，系统会将访问控制策略应用排入队列，直到设备配置完成应用。
- 不能将访问控制策略应用于运行不同版本的系统的堆叠设备（例如，如果其中一个设备的升级失败）。
- 应用访问控制策略时，系统会将所有规则一起评估并创建一组目标设备用于评估网络流量的扩展条件。弹出窗口可能会警告您已超过目标设备支持的访问控制规则或入侵策略的最大数量。此最大值取决于多个因素，包括设备上的物理内存和处理器数量。 .在具有较少计算资源的设备上，请注意，有限内存可能要求在整个访问控制策略中选择少至三个入侵策略。有关详细信息，请参阅第 12-19 页上的简化规则以提高性能。
- 如果执行的是应用控制，则必须为用作访问控制或 SSL 规则中的条件的每个应用启用至少一个检测器。如果没有为应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。
- 导入入侵规则更新时，可以在导入完成后自动重新应用访问控制和入侵策略。借此可以使用最新的入侵规则和高级设置，以及预处理器规则和预处理器设置。如果允许规则更新修改系统提供的基本策略，则这种方法尤其有用。请注意，规则更新还可修改访问控制策略中高级预处理和性能选项的默认值。有关详细信息，请参阅第 66-13 页上的导入规则更新和本地规则文件。

有关详细信息，请参阅以下各节：

- 第 12-15 页上的应用完整的策略说明如何使用快速应用选项来应用访问控制策略，以及所有关联的 SSL、网络分析、入侵和文件策略。
- 第 12-15 页上的应用所选策略配置说明如何应用特定访问控制策略配置，包括单独入侵策略。

应用完整的策略

许可证：任何环境

受支持的设备：

您可以随时将访问控制策略应用于其目标设备。应用访问控制策略还会应用任何与当前运行的策略不同的关联策略：

- SSL 策略
- 网络分析策略
- 入侵策略
- 文件策略

弹出窗口将会允许您以单一的快速应用操作的形式同时应用所有的策略。使用快速应用选项时，不会应用未更改的策略。

快速应用弹出窗口上的应用按钮标签可能会有不同，具体取决于是否允许应用访问控制策略、入侵策略或二者；请参阅第 12-3 页上的使用自定义用户角色管理部署。

要快速应用完整的访问控制策略，请执行以下操作：

访问：管理员/安全审批者

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要应用的策略旁的应用图标 ( )。

系统将显示 Apply Access Control Policy 弹出窗口。

或者，可以在编辑策略时点击 **Save and Apply**；请参阅第 12-10 页上的编辑访问控制策略。

步骤 3　点击 **Apply All**。

请注意， **Inspect Traffic During Policy Apply** 选项在默认情况下处于选中状态，并在策略应用期间允许流量检查。如果相比于流量检查，您更注重连接，请通过高级选项卡取消选中此选项。

策略应用任务将会排入队列。点击 **OK** 返回到 Access Control Policy 页面。可以在 Task Status 页面 (**System > Monitoring > Task Status**) 上监控策略应用任务的进度。

应用所选策略配置

许可证：任何环境

可以使用详细的策略应用页面将更改应用于访问控制策略和任何关联入侵策略。详细页面列出了策略针对的每个设备，并提供了按设备分类的访问控制策略列和按设备分类的关联入侵策略列。对于每个目标设备，可以指定将更改应用于访问控制策略、应用于单独或以组合形式的关联入侵策略，还是同时应用于两者。

在以下的任一情况下，必须同时应用访问控制策略和关联的入侵策略：

- 当访问控制策略将会是首次应用至设备时
- 当入侵策略是新添加至访问控制策略时

在这两种情况下，访问控制策略和入侵策略的状态都会链接，即必须同时应用或同时不应用。

请注意，无论应用何种入侵策略，应用访问控制策略都会自动应用与该策略的目标设备上当前运行的 SSL、网络分析和文件策略不同的所有关联策略。无法独立应用这些策略。

访问控制策略列

Access Control Policy 列提供了指示是否应用访问控制策略的复选框。

提示 尽管可以在应用任务仍处于任务队列，即应用任务尚未完成时重新应用策略，但是这样做没有任何的好处。

状态消息会指示策略目前是最新的，还是已过期。当策略已过期时，可以方便地在新的浏览器窗口中显示该策略与当前运行策略的比较。比较不会包含访问控制策略关联的入侵策略的差异。

入侵策略列

Intrusion Policies 列提供用于指示是否将访问控制策略关联的入侵策略应用至设备的一个或多个复选框。单个灰色的复选框指示所有关联的入侵策略与当前运行的策略一致，在这种情况下，复选框会被清除且无法选取。无法应用未改变的入侵策略，仅发生改变的入侵策略会被列出，这些策略可以单独选择。当相同的入侵策略与策略中的多个规则关联时，对于每个设备，入侵策略将仅会列出一次。

入侵策略的复选框会被选取，当访问控制策略和入侵策略必须同时应用时，如上所述，在以下的任一情况下，复选框会变灰且无法更改：

- 当访问控制策略将会是首次应用至设备时
- 当入侵策略是新添加至访问控制策略时

状态消息会指示入侵策略目前是最新的，还是已过期。当入侵策略与列出的设备上当前运行的入侵策略不一致时，该入侵策略已过期。设备上的一致入侵策略是最新的。当策略已过期时，可以方便地在新的浏览器窗口中显示该策略与当前运行策略的比较。

要应用选定的访问控制策略配置，请执行以下操作：

访问：管理员/安全审批者

步骤 1 选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2 点击要应用的策略旁的应用图标 ( )。

系统将显示 Apply Access Control Policy 弹出窗口。

或者，可以在编辑策略时点击 **Save and Apply**；请参阅第 12-10 页上的编辑访问控制策略。

步骤 3 点击 **Details**。

系统将显示详细的 Apply Access Control Policy 弹出窗口。请注意，您还可以通过在策略的 **Status** 列中点击过期消息来从 Access Control Policy 页面 (**Policies > Access Control**) 打开弹出窗口。

步骤 4 选取或清除设备名称旁的访问控制策略复选框，从而指定是否将访问控制策略应用至目标设备。

步骤 5 选取或清除设备名称旁的入侵策略复选框，从而指定是否将入侵策略应用至目标设备。

步骤 6 点击 **Apply Selected Configurations**。

策略应用任务将会排入队列。点击 **OK** 返回到 Access Control Policy 页面。

请注意，弹出窗口可能会警告您已超过设备支持的入侵策略的最大数量。您必须重新评估访问控制策略并整合入侵策略。在关联入侵策略（包括默认操作）的数量处于最大值范围内之前，无法应用访问控制策略。

请注意， **Inspect Traffic During Policy Apply** 选项在默认情况下处于选中状态，并在策略应用期间允许流量检查。如果相比于流量检查，您更注重连接，请通过高级选项卡取消选中此选项。

可以在 Task Status 页面 (**System > Monitoring > Task Status**) 上监控策略应用任务的进度

IPS 或仅发现性能注意事项

许可证：FireSIGHT 或保护

FireSIGHT 许可证随提供防御中心，通过该许可证可执行主机、应用和用户发现。通过发现数据，系统可以创建完整、最新的网路配置文件。在对受管设备应用保护许可证的情况下，系统可以充当入侵检测和防御系统 (IPS)。您可以分析入侵和漏洞的网络流量，或者丢弃有问题的数据包。

将发现和 IPS 组合可提供网络活动情景并允许您利用许多功能，包括：

- 影响标志和危害指示，可以告诉您哪些主机易受特定漏洞、攻击或某种恶意软件的攻击
- 自适应配置文件和 FireSIGHT 建议，允许您根据目标主机以不同方式检查流量
- 关联，允许您根据受影响主机以不同方式响应入侵（和其他事件）

但是，如果组织对于仅执行 IPS 或仅执行发现感兴趣，则有一些配置可以优化系统的性能，如以下各节中所述：

- 第 12-17 页上的优化仅网络发现部署
- 第 12-18 页上的在没有发现的情况下执行入侵检测和防御

优化仅网络发现部署

许可证：FireSIGHT

通过*发现*功能，可以监控网络流量并确定网络上主机（包括网络设备）的数量和类型，以及这些主机上的操作系统、活动应用和开放式端口。您还可以配置受管设备和 User Agent 以监控网络上的用户活动。可以使用发现数据执行流量量变分析，评估网络合规性和对策略违规作出响应。

在基本部署中（仅包含发现和简单、基于网络的访问控制），可以通过在配置设备的访问控制策略时遵循一些重要准则来提高该设备的性能。

注 必须应用访问控制策略，即使该策略只是简单地允许所有流量也必须应用。网络发现策略**只**能检查访问控制策略允许通过的流量。

首先，确保访问控制策略不要求复杂的处理并仅使用简单、基于网络的条件处理网络流量。必须实施以下**所有**准则；错误配置其中任何一个选项都会消除性能优势：

- 请**勿**使用安全情报功能。从策略的安全情报配置中移除任何已填充的全局白名单或黑名单。
- 请**勿**包含具有 Monitor 或 Interactive Block 操作的访问控制规则。仅使用 Allow、Trust 和 Block 规则。请记住，可以通过发现检查允许的流量，但无法检查受信任和受阻止的流量。
- 请**勿**包含具有基于应用、用户、 URL 或地理位置的网络条件的访问控制规则，即使设备相应地获得许可也如此。仅使用简单的基于网络的条件：区域、 IP 地址、 VLAN 标记和端口。
- 请**勿**包含执行文件、恶意软件或入侵检查的访问控制规则，即使设备相应地获得许可也如此。换句话说，请勿将文件策略或入侵策略与任何访问控制规则相关联。

- 确保访问控制策略的默认入侵策略设置为 **No Rules Active**；请参阅第 25-1 页上的设置用于访问控制的默认入侵策略。
- 选择 **Network Discovery Only** 作为策略的默认操作。请**勿**为执行入侵检查的策略选择默认操作。

请注意，除基于地理位置的访问控制之外，上述选项至少需要保护许可证。如果仅有 FireSIGHT 许可证，则系统会使用这些功能阻止应用访问控制策略。

在配置并应用访问控制策略后，可以配置并应用网络发现策略，它指定系统为发现数据检查的网段、端口和区域，以及是否在网段、端口和区域上发现了主机、应用和用户。

在没有发现的情况下执行入侵检测和防御

许可证：保护

通过入侵检测和防御功能，可以分析入侵和漏洞的网络流量，或者丢弃有问题的数据包。如果要执行入侵检查，但不需要利用发现数据，可以通过禁用发现来提高设备的性能。

注　如果执行的是应用、用户或 URL 控制，则**无法**禁用发现以获取性能优势。虽然可以防止系统存储发现数据，但是系统**必须**收集并检查该数据才能实施这些功能。

要禁用发现，请实施以下**所有**准则；错误配置任何准则都会消除性能优势：

- 在访问控制策略中，请**勿**包含具有基于应用、用户、 URL 或地理位置的网络条件的规则，即使设备相应地获得许可也如此。仅使用简单的基于网络的条件：区域、 IP 地址、 VLAN 标记和端口。
- 从网络发现策略中删除所有规则。

在依次应用访问控制策略和网络发现策略后，会在目标设备上停止新的发现。系统根据您在网络发现策略中指定的超时期逐渐删除网络映射中的信息。或者，可以立即清除所有发现数据，请参阅第 B-1 页上的从数据库清除发现数据。

对访问控制策略和规则进行故障排除

许可证：任何环境

正确配置访问控制策略（尤其是创建访问控制规则并对其排序）是一项复杂任务。但是，该任务对于构建有效的部署至关重要。如果不认真规划策略，则规则可能会取代其他规则或包含无效配置。规则和其他策略设置均可能需要额外的许可证。

为帮助确保系统按预期处理流量，访问控制策略接口具有功能强大的反馈系统。访问控制策略和规则编辑器的图标标记警告和错误，如访问控制错误图标表中所述。将指针悬停在图标上方可阅读警告、错误或信息文本。

提示　在访问控制策略编辑器中，点击 **Show Warnings** 可显示弹出窗口，其中会列出策略的所有警告。

此外，系统还会在应用时就可能会影响流量分析和流动的任何问题向您发出警告。

表 12-7　访问控制错误图标

图标	说明	详细信息
	错误	如果规则或配置存在错误，则更正错误之前无法应用策略，即便禁用任何受影响的规则也是如此。
	警告	可以应用显示规则或其他警告的访问控制策略。但是，以警告标记的错误配置不起作用。 例如，您可以应用这样包含被取代的规则，或者因为配置不当（使用空对象组的条件、不匹配任何应用的应用过滤器、在没有启用云通信的情况下配置 URL 条件等）而无法匹配流量的规则的策略。这些规则不评估流量。如果禁用存在警告的规则，警告图标将会消失。如果在没有纠正潜在问题的情况下启用规则，警告图标将会再次显示。 又例如，许多功能需要特定许可或设备型号。访问控制策略只能成功应用于合格的目标设备。
	信息	信息图标传达有关可能会影响流量的配置的实用信息。这些问题不会阻止您应用策略。 例如，如果执行的是应用控制或 URL 过滤，则系统可以跳过将连接的前几个数据包与某些访问控制规则相匹配，直至系统识别该连接中的应用或网络流量为止。借此可以建立连接，从而能够识别应用和 HTTP 请求。有关详细信息，请参阅第 16-6 页上的对应用控制的限制和第 16-12 页上的对 URL 检测和阻止的限制。

正确配置访问控制策略和规则还可以减少处理网络流量所需的资源。创建复杂规则、调用许多不同的入侵策略和对规则错误排序都可能会影响性能。

有关详情，请参阅：

- 第 12-2 页上的访问控制许可证和角色要求
- 第 12-19 页上的简化规则以提高性能
- 第 12-20 页上的了解规则取代和无效配置警告
- 第 12-21 页上的将规则排序以提高和避免取代

简化规则以提高性能

复杂的访问控制策略和规则会运用大量资源。应用访问控制策略时，系统会将所有规则一起评估并创建一组目标设备用于评估网络流量的扩展条件。弹出窗口可能会警告您已超过目标设备支持的访问控制规则或入侵策略的最大数量。此最大值取决于多个因素，包括设备上的物理内存和处理器数量。

简化访问控制规则

以下准则可帮助简化访问控制规则并提高性能：

- 在构造规则时，请在条件中尽可能少地使用单独元素。例如，在网络条件中，使用 IP 地址块而不是单独的 IP 地址。在端口条件中，使用端口范围。使用应用过滤器及 URL 类别和信誉执行应用控制和 URL 过滤，使用 LDAP 用户组执行用户控制。

  请注意，将元素组成后来在访问控制规则条件中使用的对象不会提高性能。例如，相比于在条件中逐个包含 50 个单独 IP 地址，使用包含这些 IP 地址的网络对象仅为您提供组织而非性能优势。
- 请尽可能按安全区域限制规则。如果设备的接口不在区域限制规则中的其中一个区域内，则该规则不影响该设备上的性能。
- 不要过度配置规则。如果一个条件足以匹配要处理的流量，请勿使用两个条件。

避免入侵策略和变量集激增

可用于在访问控制策略中检查流量的唯一入侵策略的数量取决于设备上的资源和策略的复杂性：可以将一个入侵策略与每个 Allow 和 Interactive Block 规则相关联，还可与默认操作相关联。每一唯一的入侵策略和变量集对计为一个策略。

如果超过了设备支持的入侵策略数量，请重新评估您的访问控制策略。您可能希望整合入侵策略或变量集，从而能够将单个入侵策略/变量集对与多个访问控制规则相关联。

查看选择的策略数以及这些策略在访问控制策略中的以下每个位置中使用的变量集的数量：Advanced 访问控制策略设置中的 **Intrusion Policy used before Access Control rule is determined** 选项、访问控制策略的默认操作以及策略中任何访问控制规则的检查设置。

了解规则取代和无效配置警告

许可证：任何环境

正确配置访问控制规则（以及高级部署中的网络分析规则）并将其排序对于构建有效的部署至关重要。在访问控制策略中，访问控制规则会取代其他规则或包含无效配置。同样，使用访问控制策略的高级设置配置的网络分析规则可能具有相同的问题。系统使用警告和错误图标标记这些问题。

了解规则取代警告

访问控制规则的条件会取代匹配流量的后续规则。例如：

```
规则 1：允许管理用户
规则 2：允许管理用户
```

以上的第二个规则永远不会阻止流量，因为第一个规则已允许流量。

任何类型的规则条件都可以取代后续规则。例如，以下的第一个规则中的 VLAN 范围包含第二个规则中的 VLAN，因此第一个规则将取代第二个规则：

```
规则 1：允许 VLAN 22-33
规则 2：阻止 VLAN 27
```

在以下示例中，规则 1 匹配所有 VLAN，因为没有配置 VLAN，因此规则 1 会取代尝试匹配 VLAN 2 的规则 2：

```
规则 1：允许源网络 10.4.0.0/16
规则 2：允许源网络 10.4.0.0/16，VLAN 2
```

规则还会取代所有配置条件都相同的完全一样的后续规则。例如：

```
规则 1：允许 VLAN 1 URL www.example.com
规则 2：允许 VLAN 1 URL www.example.com
```

如果任意条件不同，后续规则不会被取代。例如：

```
规则 1：允许 VLAN 1 URL www.example.com
规则 2：允许 VLAN 2 URL www.example.com
```

了解无效配置警告

因为访问控制策略所依赖的外部设置可能会变化，有效的访问控制策略可能会变得无效。请看以下示例：

- 执行 URL 过滤的规则可可能在您将没有 URL 过滤许可证的设备锁定为目标之前是有效的。这时，错误图标会显示在规则旁，无法将策略应用至该设备，直到编辑或删除规则、重新设置策略目标或者启用适当的许可证。
- 如果将端口组添加到规则中的源端口，然后将端口组更改为包含 ICMP 端口，则规则变为无效，并且在其旁边会显示警告图标。您仍然可以应用策略，但是，规则将对网络流量无效。
- 如果向规则中添加用户，然后将 LDAP 用户感知设置更改为排除该用户，则该规则将无效，因为用户不再是访问受控的用户。

将规则排序以提高和避免取代

许可证：任何环境

系统已对访问控制策略中的规则进行编号，从 1 开始。系统通过对规则编号进行升序排序来自上而下地将流量与规则进行匹配。除 Monitor 规则之外，流量匹配的第一个规则即是处理该流量的规则。

适当的访问控制规则顺序可减少处理网络流量所需的资源并防止规则取代。虽然创建的规则对于每个组织和部署都是唯一的，但在对可以优化性能同时满足需求的规则进行排序时，要遵循一些通用准则。

按重要性从高到低对规则进行排序

首先，必须对规则进行排序，以满足组织的需求。将必须应用于所有流量的优先级规则放置在策略顶部附近。例如，如果要检查来自单个用户的流量中是否存在入侵（使用 Allow 规则），但是信任部门中的所有其他用户（使用 Trust 规则），请按此顺序放置两个访问控制规则。

从特定到通用对规则进行排序

可以通过将特定规则（即精确定义其处理的流量的规则）放置在前来提高性能。这一点也非常重要，因为具有广泛条件的规则可以匹配许多不同类型的流量，并可以取代更为靠后、更为具体的规则。

假设有这样一个场景：您希望阻止大部分社交网站，但是允许访问其他特定网站。例如，您可能希望图形设计者能够访问 Creative Commons Flickr 和 deviantART 内容，但无法访问其他站点，例如 Facebook 或 Google+。应按如下对规则进行排序：

```
规则 1：对"Design"LDAP 用户组允许 Flickr、deviantART
规则 2：阻止社交网络
```

如果调转规则顺序：

```
规则 1：阻止社交网络
规则 2：对"Design"LDAP 用户组允许 Flickr、deviantART
```

第一个规则阻止所有社交流量，包括 Flickr 和 deviantART。由于没有流量与第二个规则相匹配，因此设计者无法访问您希望可供其访问的内容。

将检查流量的规则放置在后

由于发现、入侵、文件和恶意软件检查需要处理资源，因此将不检查流量的规则（Trust、Block）放置在检查流量的规则（Allow、Interactive Block）之前可以提高性能。这是因为 Trust 和 Block 规则可以转移系统可能会以其他方式检查的流量。在所有其他因素均平等的前提下，也就是说，假设有一组规则，其中的任一条规则都不比其他规则更为关键，且取代不是问题，请考虑按以下顺序放置这些规则：

- Monitor 规则，记录匹配连接但不对流量采取其他操作
- Trust 和 Block 规则，处理流量而不进一步检查
- Allow 和 Interactive Block 规则，不进一步检查流量
- Allow 和 Interactive Block 规则，选择性检查流量中是否存在恶意软件和/或入侵

生成当前访问控制设置报告

许可证：任何环境

访问控制策略报告是特定时间点的策略和规则配置的记录。您可以使用包含以下信息的报告进行审计或检查当前配置。

表 12-8　访问控制策略报告的各个章节

项	说明
策略信息	提供策略的名称和说明、上次修改策略的用户的名称以及策略上次修改的日期和时间
设备目标	列出作为策略目标的受管设备。
HTTP 阻止响应 HTTP 交互阻止响应	提供使用策略阻止网站时向用户显示的页面有关的详细信息。
安全智能	提供有关策略的安全情报白名单和黑名单的详细信息。
默认操作	列出默认操作和关联变量集（如果有）。
规则	列出策略中的每个访问控制规则，并提供有关其配置的详细信息。
高级设置	有关策略的高级设置的详细信息，包括： • 用于预处理访问控制策略的流量的网络分析策略，以及全局预处理选项 • 被动部署的自适应配置文件设置 • 用于检测文件、恶意软件和入侵的性能设置 • 其他策略范围设置
引用对象	提供有关访问控制策略引用的可重用对象的详细信息，包括 SSL 策略使用的入侵策略变量集和对象。

还可以生成访问控制比较报告，该报告将一个策略与当前应用的策略或另一策略进行比较。有关详细信息，请参阅第 12-22 页上的比较访问控制策略。

要查看访问控制策略报告，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要生成报告的策略旁的报告图标 ( )。在生成访问控制策略报告前，切记保存所有更改，只有已保存的更改会在报告中显示。

系统将会生成报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

比较访问控制策略

许可证：任何环境

如要审阅策略更改以便符合组织的标准或提高系统性能，可以检查两个访问控制策略之间的差异。可以比较任意两个策略，也可以将当前应用的策略与另一策略进行比较。在进行比较后，或者生成 PDF 报告来记录两个策略之间的差异。

有两个可以用来比较策略的工具：

- 比较视图仅会以并排格式显示两个策略之间的差异。每个策略的名称将会显示在比较视图左侧和右侧的标题栏中，当选择 **Running Configuration** 时除外，在这种情况下，空白栏代表当前的活动策略。

  可以使用此工具来在 Web 界面中查看和导航两个策略（在其差异突出显示的情况下）。

- 比较报告会以类似策略报告的格式（但采用 PDF 格式）创建仅有两个策略之间的差异的记录。

  可以使用此工具来保存、复制、打印和共享策略比较，供未来检查使用。

如需了解和使用策略比较工具的更多相关信息，请参阅：

- 第 12-23 页上的使用访问控制策略比较视图
- 第 12-23 页上的使用访问控制策略比较报告

使用访问控制策略比较视图

许可证：任何环境

比较视图会以并排格式显示两个策略，每个策略由比较视图左侧和右侧标题栏中的名称确定。比较运行配置之外的两个策略时，最后修改的时间和最后修改的用户将会随策略名称显示。

两个策略之间的差异将会突出显示：

- 蓝色指示突出显示的设置在两个策略中不同，不同之处以红色文本标注。
- 绿色指示突出显示的设置在一个策略中存在，但在另一个策略中不存在。

您可以执行下表中的任何操作。

表 12-9　　访问控制策略比较视图操作

要.....	您可以.....
逐一浏览更改	点击标题栏上方的 **Previous** 或 **Next**。 在左右两侧之间以双箭头图标 (◂▸) 为中心移动，**Difference** 数字调整为识别您正在查看哪个差异。
生成新的策略比较视图	点击 **New Comparison**。 系统将显示 **Select Comparison** 窗口。有关详情，请参见第 12-23 页上的使用访问控制策略比较报告。
生成策略比较报告	点击 **Comparison Report**。 策略比较报告将会创建仅列出两个策略之间的差异的 PDF 文档。

使用访问控制策略比较报告

许可证：任何环境

访问控制策略比较报告是策略比较视图确定的两个访问控制策略或者一个策略和当前应用的策略之间的所有差异的记录，以 PDF 格式提供。可以使用此报告来进一步检查两个策略配置之间差异，以及保存和分发比较结果。

对于可以访问的所有策略，都可以通过比较视图生成访问控制策略比较报告。在生成策略报告前，切记保存所有更改，只有已保存的更改会在报告中显示。

策略比较报告的格式与策略报告相同，有一处例外：策略报告包含策略中的所有配置，而策略比较报告仅列出策略之间的那些不同配置。访问控制策略比较报告包含第 12-22 页上的表 12-8中描述的部分。

提示 可以使用类似的操作步骤比较 SSL、网络分析、入侵、文件、系统或运行状况策略。

要比较两个访问控制策略，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1 选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2 点击 **Compare Policies**。

系统将显示 Select Comparison 窗口。

步骤 3 从 **Compare Against** 下拉列表中选择要进行比较的类型：

- 要比较两个不同的策略，请选择 **Other Policy**。

  页面将会刷新，并显示 Policy A 和 Policy B 下拉列表。
- 要将另一策略与当前活动的策略进行比较，请选择 **Running Configuration**。

  页面将会刷新，并会显示 Target/Running Configuration A 和 Policy B 下拉列表。

步骤 4 根据您选择的比较类型，有以下选项可供选择：

- 如果您比较两个不同的策略，请从 Policy A 和 Policy B 下拉列表中选择要比较的策略。
- 如果您将正运行的配置与另一策略进行比较，请从 Policy B 下拉列表中选择第二个策略。

步骤 5 点击 **OK** 显示策略比较视图。

系统将显示比较视图。

步骤 6 或者点击 **Comparison Report** 生成访问控制策略比较报告。

屏幕上将会显示访问控制策略比较报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

使用安全情报 IP 地址信誉实施黑名单

作为防御恶意互联网内容的第一道防线，FireSIGHT 系统包括安全情报功能，可供您根据最新声誉情报立即将连接列出黑入单（阻止），再也无需资源更密集型深入分析。安全情报过滤要求具备保护许可证，支持除 2 系列之外的所有受管设备。

安全情报通过阻止具有已知不良声誉的 IP 地址的往返流量而发挥作用。这种流量过滤发生于任何其他基于策略的检查、分析或流量处理**之前**（但是其确实发生于快速路径等硬件级别处理之后）。

请注意，您可以通过 IP 地址手动限制流量来创建可执行与安全情报过滤类似的功能的访问控制规则。但是，访问控制规则范围更广泛，配置更为复杂，并且无法使用动态源自动更新。

被安全情报列入黑名单的流量会被立即阻止，因此其将不接受任何进一步检测 — 既不检查其是否存在入侵、漏洞、恶意软件等，也不检测其是否存在网络发现。或者，在被动部署中建议选择使用安全情报过滤的仅监控设置。这使系统能够分析本应被列入黑名单的连接，但也将匹配项记录至黑名单并生成连接结束安全情报事件。

注意事项 对于3 系列设备所处理的流量，系统将先处理某些“信任”规则，然后才处理访问控制策略的安全情报黑名单，这样会允许列入黑名单的流量未经检查就通过。有关详细信息，请参阅第 14-10 页上的借助 3 系列设备信任或阻止流量的限制。

为了您的方便，思科提供*情报源*（有时称为 *Sourcefire 情报源*），它包括由 VRT 确定具有不良声誉且定期更新的多个 IP 地址集合组成。情报源会跟踪开放式中继、已知攻击者、伪造的 IP 地址（虚假地址）等等。您还可自定义功能以满足贵组织的独特需求，例如：

- **第三方源** — 使用第三方声誉源补充情报源，系统可以像更新思科源一样自动更新第三方声誉源
- **自定义黑名单** — 系统允许您以多种方式根据自己的需求将特定 IP 地址手动列入黑名单
- **按安全区域实施黑名单** — 为提高性能，您可能想要锁定实施目标，例如将垃圾邮件黑名单限定于处理邮件流量的区域
- **监控，而不是列入黑名单** — 在被动部署中及对于其实施之前的源测试尤为有用；只监控违规会话，而不阻止它们，从而生成连接结束事件
- **列入白名单以消除误报** — 当黑名单范围太大或不正确阻止想要允许的流量（例如，重要资源）时，可使用自定义白名单覆盖黑名单

有关配置访问控制策略以执行安全情报过滤和查看此过滤功能生成的事件数据的详细信息，请参阅以下章节：

- 第 13-2 页上的选择安全情报战略
- 第 13-3 页上的建立安全情报白名单和黑名单
- 第 38-9 页上的记录安全情报（黑名单）决策
- 第 39-1 页上的使用连接与安全情报数据

选择安全情报战略

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

构建黑名单最简易的方式是使用情报源，该情报源跟踪已知为开放中继、已知攻击者、伪造 IP 地址（虚假地址）的 IP 地址。因为情报源定期更新，使用它可确保系统使用最新信息来过滤网络流量。恶意 IP 地址是指诸如恶意软件、垃圾邮件、僵尸网络以及网络钓鱼的安全威胁，它们的出现和消失速度要快于更新和应用新策略的速度。

为扩大情报源，可以使用自定义或第三方 IP 地址列表和源来执行安全情报过滤，其中：

- *list* 是 IP 地址的静态列表，可以将其上传至防御中心
- *feed*是防御中心定期从互联网下载的 IP 地址的动态列表；情报源是一种特殊的源

如需有关配置安全情报列表和源的详细信息，包括高可用性和互联网访问要求，请参阅第 3-4 页上的使用安全情报列表和源。

使用安全情报全局黑名单

在分析过程中，可以通过在事件视图、情景管理器或控制面板中选择任何 IP 地址来构建*全局黑名单*。例如，如果注意到入侵事件中的一组可路由 IP 地址涉及漏洞攻击尝试，可以立即将这些 IP 地址添加到黑名单。在所有访问控制策略中，防御中心使用此全局黑名单（和相关的*全局白名单*）来执行安全情报过滤。如需管理这些全局列表的相关信息，请参阅第 3-6 页上的使用全局白名单和黑名单。

注 尽管全局黑名单（或全局白名单；请见下文）的源更新和增添会在整个部署中自动实施更改，但对安全情报对象做出的任何其他更改均需要重新应用访问控制策略。有关详细信息，请参阅第 3-6 页上的表 3-1。

使用网络对象

最后，构建黑名单的一种简便方式为使用代表 IP 地址、 IP 地址块或 IP 地址集合的*网络对象或网络对象组*。如需创建和修改网络对象的相关信息，请参阅第 3-4 页上的使用网络对象。

使用安全情报白名单

除了黑名单，每个访问控制策略还有关联的白名单，也可以使用安全情报对象来进行填充。策略的白名单可以覆盖其黑名单。即系统使用访问控制规则评估已列入白名单的源或目标 IP 地址的流量，即便 IP 地址也被列入黑名单。通常，如果黑名单仍然有用，但范围又太过广泛，错误地阻止您想要检查的流量，则可以使用白名单。

例如，如果可信源不当地阻止了对重要资源的访问，但其整体而言对您的组织有用，可以仅将不当分类的 IP 地址列入白名单，而不是从黑名单移除整个源。

通过安全区域实施安全情报过滤

为提高精细度，可以根据连接中的源或目标 IP 地址是否位于特定安全区域来实施安全情报过滤。

要扩展以上的白名单示例，可以将不当分类的 IP 地址列入白名单，但随后使用组织中需要访问 IP 地址的人员所使用的安全区域限制白名单对象。这样，只有有业务需要的人员才可以访问列入白名单的 IP 地址。再如，您可以使用第三方垃圾邮件源将邮件服务器安全区域上的流量列入黑名单。

监控连接而不将其列入黑名单

如果您不确定是否想要将特殊 IP 地址或地址集列入黑名单，则可使用“仅监控”设置，该设置允许系统将匹配连接传递给访问控制规则，但也将匹配项记录到黑名单并生成连接结束安全情报事件。请注意，无法将全局黑名单设置为仅监控。有关详细信息，请参阅：

考虑一下这样的情况，在使用第三方源实施阻止之前，想要先对该源进行测试。当将源设置为仅监控时，系统允许已被阻止的连接，以便系统能对其进行进一步的分析，但是也会记录这些连接中的每一个连接，以供进行评估。

在被动部署中，为提高性能，思科 建议始终采用仅监控的设置。被动部署的受管设备无法影响流量；与将系统配置为阻止流量相比，没有任何优势。此外，因为阻止的连接实际上在被动部署中并未被阻止，因此，系统可能针对每条已阻止连接报告多个连接开始事件。

建立安全情报白名单和黑名单

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

要构建白名单和黑名单，可用网络对象和组的任何组合以及安全情报源和列表填充它们，您可按安全区域对所有这些进行限制。

默认情况下，访问控制策略使用防御中心的应用于任何区域的全局白名单和黑名单。这些列表由分析师填充，分析师可以使用上下文菜单快速添加各个 IP 地址。可以为每个策略选择是否使用这些全局列表。

注　您不能将使用已填充全局白名单或黑名单的访问控制策略应用于 2 系列 设备（或没有保护许可的其他设备）。如果您向任一全局列表添加了 IP 地址，则**必须**先从策略的安全情报配置中移除非空列表，然后才能应用该策略。有关详细信息，请参阅第 3-6 页上的使用全局白名单和黑名单。

在构建白名单和黑名单后，可以记录列入黑名单的连接。也可以将个别列入黑名单的对象（包括源和列表）设置为仅监控。这使得系统可以使用访问控制处理涉及列入黑名单的 IP 地址的连接，但也将连接的匹配项记录至黑名单。

可以使用访问控制策略中的 Security Intelligence 选项卡来配置白名单、黑名单和日志记录选项。该页面列出了可以在白名单或黑名单中使用的可用对象以及可以用于限制列入白名单和黑名单的对象的可用区域。每种类型的对象或区域用不同的图标区分。标有思科图标 (思科) 的对象代表情报源中的不同类别。思科

在黑名单中，设置为阻止的对象标有阻止图标 ( )，而仅监控的对象标有监控图标 ( )。因为白名单会覆盖黑名单，如果您向两个列表添加相同的对象，系统会显示带删除线的已列入黑名单对象。

最多可以向白名单和黑名单添加总计 255 个对象。即白名单中的对象数量加上黑名单中的对象数量不能超过 255。

请注意，尽管可以将子网掩码为 /0 的网络对象添加到白名单或黑名单，但这些对象中使用 /0 子网掩码的地址块将被忽略，并且不会根据这些地址进行白名单和黑名单过滤。安全情报源中子网掩码为 /0 的地址块也将被忽略。如果想要监控或阻止策略已锁定为目标的所有流量，请分别使用包含 **Monitor** 或 **Block** 规则操作的访问控制规则，并使用 **Source Networks** 和 **Destination Networks** 的默认值 **any**，而不使用安全情报过滤。

要构建访问控制策略的安全情报白名单和黑名单，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Security Intelligence** 选项卡。

屏幕上将会显示访问控制策略的安全情报设置。

步骤 4　或者点击日志记录图标 ( ) 来记录已列入黑名单的连接。

必须先启用日志记录，才可以将已列入黑名单的对象设置为仅监控。有关详细信息，请参阅第 38-9 页上的记录安全情报 （黑名单）决策。

步骤 5　通过选择一个或多个**可用对象**开始构建白名单和黑名单。

使用 Shift 和 Ctrl 键可选择多个对象，或者右键单击并选择 **Select All**。

提示　可以搜索需要包含的现有对象，如果没有现有对象符合组织的需求，也可以动态创建对象。有关详细信息，请参阅第 13-5 页上的搜索添加至白名单或黑名单的对象和第 13-5 页上的创建添加至白名单或黑名单的对象。

步骤 6　也可以通过选择**可用区域**来按区域限制选定对象。

默认情况下，对象不会受到限制，即它们拥有取值为 `Any` 的区域。请注意，可以用仅一个区域进行限制，而不是使用 **Any**。如要在多个区域上实施对象的安全情报过滤，对于每个区域，都必须将对象分别添加至白名单或黑名单。此外，全局白名单或黑名单无法通过区域进行限制。

步骤 7　点击 **Add to Whitelist** 或 **Add to Blacklist**。

还可以点击并拖动选定对象至任一列表。

您选择的对象已添加到黑名单或白名单。

提示　要从列表中移除对象，请点击其删除图标 ( )。可以使用 Shift 和 Ctrl 键来选择多个对象，或者右键单击并 **Select All**，然后右键单击并选择 **Delete Selected**。如果您在删除全局列表，则必须确认您的选择。请注意，从白名单或黑名单移除的对象不会从防御中心台删除。

步骤 8　重复第 5 步至第 7 步，直到完成将对象添加至白名单和黑名单。

步骤 9　也可以通过右键单击 **Blacklist** 下的对象，然后选择 **Monitor-only (do not block)**，将列入黑名单的对象设置为仅监控。

在被动部署中，思科建议将所有已列入黑名单的对象设置为仅监控。然而，请注意，无法将全局黑名单设置为仅监控。

步骤 10　点击 **Save**。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

搜索添加至白名单或黑名单的对象

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

如果有多个网络对象、组、源和列表，可以使用搜索功能来限制要添加至黑名单或白名单的对象。

要搜索添加至白名单或黑名单的对象，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在 **Search by name or value** 字段中键入您的查询内容。

在键入字符串时， Available Objects 列表将会更新，从而显示匹配项。要清除搜索字符串，请点击搜索字段上方的重新载入图标 ( )，或点击搜索字段中的清除图标 ( )。

可以搜索为这些对象配置的网络对象名称以及值。例如，如果有一个名为 `Texas Office` 的网络对象，该对象配置了 `192.168.3.0/24` 这个值，且该对象包含在组对象 `US Offices` 中，则可以键入部分或完整的搜索字符串（例如 `Tex`）或者键入某个值（例如 `3`）来显示这两个对象。

创建添加至白名单或黑名单的对象

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

编辑访问控制策略时，可以即时创建对象以便在其白名单和黑名单中使用：可以是网络对象或者安全情报列表或源。请注意，对网络对象进行分组或创建网络对象组时，必须使用对象管理器。

要创建添加至白名单或黑名单的对象，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　点击添加图标 ( )，然后选择要创建的对象的类型：

- 选择 **Add IP List**，以便创建安全情报列表或源；请参阅第 3-4 页上的使用安全情报列表和源。
- 选择 **Add Network Object**，以便添加网络对象；请参阅第 3-4 页上的使用网络对象。

使用访问控制规则调整流量

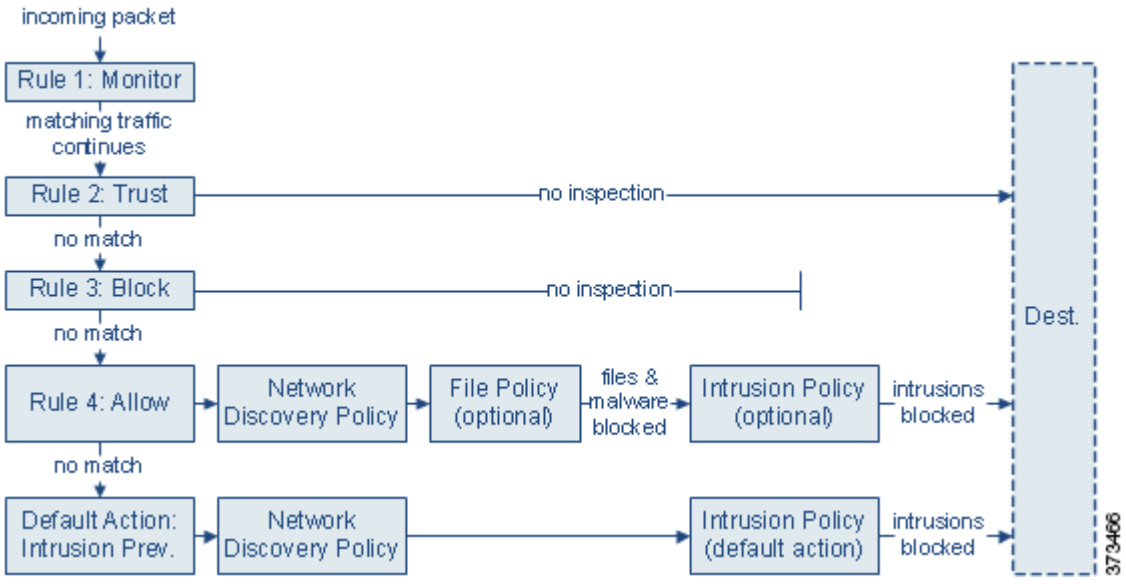
在访问控制策略中，*访问控制规则*提供在多台受管设备之间处理网络流量的精细方法。

注 基于硬件的快速路径规则、基于安全情报的流量过滤以及一些解码和预处理发生在通过访问控制规则评估网络流量**之前**。您还可以配置 *SSL 检查*功能，以在访问控制规则评估加密流量之前阻止或解密该流量。

系统按您指定的顺序将流量与访问控制规则相匹配。在大多数情况下，系统根据*所有*规则条件匹配流量的*第一个*访问控制规则处理网络流量。条件可以简单，也可以复杂；可通过安全区域、网络或地理位置、 VLAN、端口、应用、请求的 URL 和用户控制流量。

每个规则也有*操作*，确定是否监控、信任、阻止或允许匹配的流量。当允许流量时，指定系统使用入侵或文件策略先检查流量，以在漏洞、恶意软件或禁止的文件到达您的资产或退出网络之前予以阻止。但是，在系统信任或阻止流量之后，**不**执行进一步检查。

以下场景汇总了内联入侵防御部署中访问控制规则评估流量的方式。



在此情景中，流量评估如下：

- **规则 1：Monitor** 第一次评估流量。 Monitor 规则跟踪和记录网络流量，但不影响流量。系统继续根据其他规则匹配流量，以确定允许其通过，还是拒绝。

- **规则 2：Trust** 继续评估流量。允许匹配的流量传至目标，无需进一步检查。不匹配的流量继续根据下一规则进行评估。
- **规则 3：Block** 第三次评估流量。匹配的流量被阻止，无需进一步检查。不匹配的流量继续根据最终规则进行评估。
- **规则 4：Allow** 是最终规则。对于此规则，允许匹配的流量；但检测和阻止流量内禁止的文件、恶意软件、入侵和漏洞。允许其他非禁止、非恶意流量到达目标。请注意，您可能有其他只执行文件检查、只执行入侵检查或者两类检查都不执行的 Allow 规则。
- **默认操纵**处理不匹配任何规则的所有流量。在这种情况下，默认操作在允许非恶意的流量通过之前先执行入侵防御。在不同的部署中，您可能有默认操作可以信任或阻止所有流量，而无需进一步检查。（您不能对默认操作处理的流量进行文件或恶意软件检查。）

无论是使用访问控制规则还是默认操作，您允许的流量都自动可用于根据网络发现策略检查主机、应用和用户数据。尽管可以增强或禁用发现功能，但不能明确启用该功能。但是，允许流量不会自动确保收集发现数据。系统仅对涉及 IP 地址的连接执行发现功能，根据网络发现策略明确监控这些 IP 地址；此外，对于加密会话，应用发现受到限制。有关详细信息，请参阅第 45-1 页上的网络发现简介。

请注意，当 SSL 检查配置允许加密流量通过时或者如果您不配置 SSL 检查，则访问控制规则处理加密流量。但是，某些访问控制规则条件需要未加密流量，因此，加密流量可能匹配的规则更少。此外，默认情况下，系统禁用加密负载的入侵和文件检查。当加密连接匹配已配置入侵和文件检查的访问控制规则时，这有助于减少误报和提高性能。有关详细信息，请参阅第 19-1 页上的了解流量解密和第 27-60 页上的使用 SSL 预处理器。

有关访问控制规则的详细信息，请参阅：

- 第 14-2 页上的创建和编辑访问控制规则
- 第 14-11 页上的管理策略中的访问控制规则
- 第 12-18 页上的对访问控制策略和规则进行故障排除

创建和编辑访问控制规则

许可证：任何环境

在访问控制策略中，访问控制规则提供在多台受管设备之间处理网络流量的精细方法。除了其唯一名称之外，每个访问控制规则都具有以下基本组件：

State

默认情况下，规则处于启用状态。如果您禁用某规则，系统将不用它来评估网络流量并停止为该规则生成警告和错误。

Position

系统已对访问控制策略中的规则进行编号，从 1 开始。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

Conditions

条件指定规则处理的特定流量。条件可以根据安全区域、网络或地址位置、 VLAN、端口、应用、请求的 URL 或用户匹配流量。条件可以简单，也可以复杂；条件的使用通常取决于目标设备许可证和模式。

Action

规则操作确定系统如何处理匹配的流量。您可以监控、信任、阻止或允许（执行或无需执行进一步检查）匹配的流量。请注意，系统**不会**对受信任或被阻止的流量执行检查。

Inspection

访问控制规则的检查选项管理系统如何检查和阻止您意外允许的恶意流量。当允许流量使用规则时，您可以指定系统使用入侵或文件策略先检查流量，以在漏洞、恶意软件或禁止的文件到达您的资产或退出网络之前予以阻止。

Logging

规则的日志记录设置管理系统保存其处理流量的记录。您可以记录匹配规则的流量。一般来说，您可以在连接开始和/或结束时记录会话。您可以将连接记录到防御中心数据库，以及系统日志 (syslog) 或 SNMP 陷阱服务器中。

备注

每次保存对访问控制规则所做的更改时，您都可以添加一个注释。

使用访问控制规则编辑器添加和编辑访问控制规则；通过访问控制策略编辑器的 Rules 选项卡访问规则编辑器。在规则编辑器中，您可以：

- 配置基本属性，例如在编辑器上部区域的规则的名称、状态、位置和操作。
- 使用编辑器下部左侧的选项卡添加条件。
- 使用下部右侧的选项卡配置检查和日志记录选项，还可以向规则添加注释。为了方便，无论您在查看哪个选项卡，编辑器都列出规则的检查和日志记录选项。

注 正确创建和订购访问控制规则是一项复杂的任务，但却是构建有效部署的一项基本任务。如果没有认真计划策略，则规则可以抢占其他规则、需要其他许可证或包含无效的配置。为帮助确保系统按预期处理流量，访问控制策略接口具有规则的强大警告和错误反馈系统。有关详细信息，请参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

要创建或修改访问控制规则，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1 选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2 点击要添加规则的访问控制策略旁边的编辑图标 ( )。

系统将显示策略页面，侧重 Rules 选项卡。

步骤 3 您有以下选项：

- 要添加新规则，请点击 **Add Rule**。
- 要编辑现有规则，请点击要编辑的规则旁边的编辑图标 ( )。

系统将显示访问控制规则编辑器。

步骤 4 在 **Name** 中键入规则名称。

每台设备必须有一个唯一的名称。最多可以使用 30 个可打印字符，包括空格和特殊字符，但 (:) 除外。

步骤 5 配置规则组件，如上面的总结所述。可以配置以下内容或接受默认设置：

- 指定规则是否为 **Enabled**。
- 指定规则位置；请参阅第 14-4 页上的指定规则的评估顺序。
- 在 **Action** 中选择规则操作；请参阅第 14-6 页上的使用规则操作确定流量处理和检查。
- 配置规则的条件；请参阅第 14-5 页上的使用条件指定规则处理的流量。

- 对于 Allow 和 Interactive Block 规则，配置规则的 **Inspection** 选项；请参阅第 18-1 页上的使用入侵和文件策略控制流量。
- 在 **Logging** 中指定日志记录选项；请参阅 第 38-1 页上的记录网络流量中的连接。
- 在 **Comments** 中添加注释；请参阅第 14-11 页上的将注释添加到规则中。

步骤 6　点击 **Save** 保存该规则。

规则成功保存。您可以点击删除图标 ( ) 删除该规则。您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

指定规则的评估顺序

许可证：任何环境

首次创建访问控制规则时，使用规则编辑器中的 **Insert** 下拉列表指定该规则的位置。系统已对访问控制策略中的规则进行编号，从 1 开始。系统会用升序的规则号码以从上到下的顺序将流量匹配到访问控制规则中。

在大多数情况下，系统根据*所有*规则条件匹配流量的*第一个*访问控制规则处理网络流量。除了 Monitor 规则（记录流量，但不影响流量）之外，系统在流量匹配一个规则后，**不再**继续根据其他低优先级规则评估流量。

提示　正确的访问控制规则顺序降低处理网络流量所需的资源，并防止规则抢占。尽管您创建的规则对于每个组织和部署来说都是唯一的，但是排序规则时需要遵循几个基本原则，才可优化性能，同时满足您的需求。有关详细信息，请参阅第 12-21 页上的将规则排序以提高和避免取代。

除了按照编号排序规则之外，还可按类别对规则进行分组。默认情况下，系统提供三个类别：管理员、标准和根。您可以添加自定义类别，但是不能删除思科提供的类别或更改类别的顺序。有关更改现有规则的位置或类别的信息，请参阅第 14-14 页上的更改规则的位置或类别。

要在编辑或创建规则时将规则添加到类别，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在访问控制规则编辑器中，从 **Insert** 下拉列表中选择 **Into Category**，然后选择要使用的类别。

保存规则时，系统将其置于该类别的最后位置。

要在编辑或创建规则时按号码定位规则，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在访问控制规则编辑器中，从 **Insert** 下拉列表中选择 **above rule** 或 **below rule**，然后键入合适的规则编号。

当保存规则时，规则已置于您指定的位置。

使用条件指定规则处理的流量

许可证：因功能而异

受支持的设备：因功能而异

受支持的防御中心：因功能而异

访问控制规则的条件确定该规则处理的流量类型。条件可以简单，也可以复杂；可通过安全区域、网络或地理位置、 VLAN、端口、应用、请求的 URL 和用户控制流量。

向访问控制规则中添加条件时，请记住以下几点：

- 每个规则可以配置多个条件。为使规则应用于流量，流量必须匹配规则中的**所有**条件。例如，您可以使用单个规则为特定主机（区域或网络条件）执行 URL 过滤（URL 条件）。
- 为规则中的每个条件最多可以添加 50 个标准。匹配**所有**条件的标准的流量满足该条件。例如，您可以使用单个规则为最多 50 个用户和组执行用户控制。

请注意，您可以根据源和目标限制区域和网络条件，使用最多 50 个源和最多 50 个目标标准。如果将源和目标标准添加到区域或网络条件，匹配的流量必须源自指定源区域/网络之一**并**通过目标区域/网络之一流出。换句话说，系统借助 OR 运算将同一类型的多个条件标准连接在一起，并且借助 AND 运算将多个条件类型连接在一起。例如，如果规则条件如下：

```
Source Networks: 10.0.0.0/8, 192.168.0.0/16
Application Category: peer to peer
```

规则将匹配来自其中一个私有 IPv4 网络的一台主机的 P2P 应用流量 - 数据包必须源自一个 **OR** 其他源网络， **AND** 表示 P2P 应用流量。以下两个连接触发此规则：

```
10.42.0.105 to anywhere, using LimeWire
192.168.42.105 to anywhere, using Kazaa
```

如果不为规则配置特定条件，系统将不基于此标准匹配流量。例如，无论会话中使用的应用如何，具有网络条件但不具有应用条件的规则根据数据流源或目标评估流量。

注　应用访问控制策略时，系统评估其所有规则并创建一个扩展标准集，目标设备该扩展标准集评估网络流量。复杂的访问控制策略和规则可控制大量资源。有关简化访问控制规则的提示和提高性能的其他方法，请参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

当添加或编辑访问控制规则时，使用规则编辑器下部左侧的选项卡添加和编辑规则条件。下表总结了可以添加的条件类型。

表 14-1　访问控制规则条件类型

这些条件.....	匹配流量.....	详细信息
Zones	通过特定安全区域的一个接口进入或离开设备	安全区域是根据部署和安全策略划分的一个或多个接口的逻辑分组。区域中的接口可能分布于多台设备上。要构建区域条件，请参阅第 15-2 页上的通过安全区域控制流量。
Networks	按照其源或目标 IP 地址、国家/地区或大洲	可以明确指定 IP 地址或地址块。利用地理定位功能还可以根据源或目标国家/地区或大洲控制流量。要构建网络条件，请参阅第 15-3 页上的按网络或地理位置控制流量。
VLAN Tags	按照 VLAN 进行标记	系统使用最内部的 VLAN 标记来按照 VLAN 识别数据包。要构建 VLAN 条件，请参阅第 15-5 页上的控制 VLAN 流量。

表 14-1　访问控制规则条件类型 （续）

这些条件.....	匹配流量.....	详细信息
Ports	按照其源端口或目标端口	对于 TCP 和 UDP 而言，您可以基于传输层协议控制流量。对于 ICMP 和 ICMPv6 (IPv6-ICMP) 而言，您可以基于其互联网层协议加上可选类型和代码控制流量。您还可以利用未使用端口的其他协议，使用端口状态来控制流量。要构建端口条件，请参阅第 15-6 页上的通过端口和 ICMP 代码控制流量。
Applications	按照会话中检测到的应用	您可以控制对单个应用的访问，或根据基本特征过滤访问：键入、风险、业务相关性、类别和标记 。要构建应用条件，请参阅第 16-2 页上的控制应用流量。
URLs	按照会话中请求的 URL	您可以限制网络中的用户可以单独访问或基于 URL 的一般分类和风险水平进行访问的网站。要构建 URL 条件，请参阅第 16-7 页上的阻止 URL。
Users	按照会话中涉及的用户	根据登录受监控会话所涉及的主机的 LDAP 用户，可以控制流量。可以根据从 Microsoft Active Directory 服务器检索的单个用户或组控制流量。要构建用户条件，请参阅第 17-1 页上的按照用户控制流量。

请注意，虽然可使用任意许可证创建访问控制规则，但某些规则条件需要您先启用访问控制策略目标设备上的特定许可功能，然后才可以应用策略。有关详细信息，请参阅第 12-2 页上的访问控制的许可证和型号要求。

使用规则操作确定流量处理和检查

许可证：任何环境

每个访问控制规则具有为匹配的流量确定以下内容的*操作*：

- 处理 — 首先，规则操作管理系统是否会监控、信任、阻止或允许匹配规则条件的流量
- 检查 - 利用某些规则操作，可以在正确许可的条件下通过进一步检查匹配的流量，然后才允许流量通过
- 日志记录 - 该规则操作确定何时以及如何记录有关匹配的流量的详细信息

访问控制策略的*默认操作*处理不满足任何非“监控”访问控制规则条件的流量；请参阅第 12-6 页上的设置对网络流量的默认处理和检查。

请记住，只有内联部署的设备才可以阻止或修改流量。被动部署或在轻触模式下部署的设备可以分析和记录，但是不影响流量。有关规则操作的详细信息以及规则操作如何影响流量处理、检查和日志记录，请参阅以下各节：

- 第 14-7 页上的 Monitor 操作：延迟操作并确保日志记录
- 第 14-7 页上的 Trust 操作：未经检查通过流量
- 第 14-7 页上的阻止操作：未经检查阻止流量
- 第 14-8 页上的交互式阻止操作：允许用户绕过网站拦截
- 第 14-9 页上的 Allow 操作：允许和检查流量
- 第 14-10 页上的借助 3 系列设备信任或阻止流量的限制
- 第 18-1 页上的使用入侵和文件策略控制流量
- 第 38-13 页上的根据访问控制处理记录连接

Monitor 操作：延迟操作并确保日志记录

许可证：任何环境

Monitor 操作不影响流量；匹配的流量既不会被立即允许，也不会被立即拒绝。相反，系统会根据其他规则匹配流量，以确定允许还是拒绝该流量。所匹配的第一个非 Monitor 规则确定流量和任何进一步的检查。如果没有其他匹配的规则，系统使用默认操作。

由于 Monitor 规则的主要目的是跟踪网络流量，因此系统会自动记录监控流量的连接结束事件。即，即使流量不匹配其他规则，且您不对默认操作进行日志记录，系统也会记录连接。有关详细信息，请参阅第 38-5 页上的了解受监控连接的记录。

注　如果本地约束的流量与第 3 层部署中的 Monitor 规则相匹配，则该流量可能绕过检查。为确保对流量进行检查，在路由流量的受管设备的高级设备设置中启用 **Inspect Local Router Traffic**。有关详细信息，请参阅第 4-47 页上的了解高级设备设置。

Trust 操作：未经检查通过流量

许可证：任何环境

Trust 操作允许任何类型的流量通过，无需进一步检查。

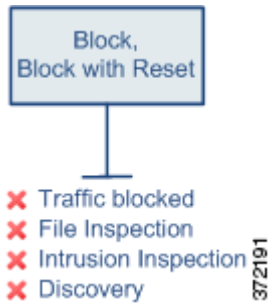
您可以在连接开始和结束时记录受信任的网络流量。请注意，根据检测连接的设备型号，系统记录 Trust 规则处理的 TCP 连接的方式有所不同。有关详细信息，请参阅第 38-6 页上的了解受信任连接的记录。

注意事项　对于3 系列 设备处理的流量，系统首先处理某些 Trust 规则，然后才处理访问控制规则的安全情报黑名单，该黑名单可以允许列入黑名单的流量未经检查就通过。有关详细信息，请参阅第 14-10 页上的借助 3 系列设备信任或阻止流量的限制。

阻止操作：未经检查阻止流量

许可证：任何环境

Block 和 **Block with reset** 操作拒绝任何类型的流量，无需进一步检查。 Block with reset 规则也会重置连接。



对于未加密的 HTTP 流量，当系统阻止网络请求时，您可以使用解释连接被拒绝的自定义页面覆盖默认的浏览器或服务器页面。系统将此自定义页面称为 *HTTP 响应页面*；请参阅第 16-15 页上的显示被阻止 URL 的自定义网页。

对于已解密和加密的 (HTTPS) 流量， Interactive Block 规则阻止无交互的匹配连接，并且系统**不**显示响应页面。

请注意，系统不显示某些被成功阻止的流量的已配置响应页面，这些流量由3 系列 设备进行处理。相反，请求禁止的 URL 的用户将连接重置或超时。有关详细信息，请参阅第 14-10 页上的借助 3 系列设备信任或阻止流量的限制。

您可以仅记录连接开始时被阻止的网络流量。请注意，仅内联部署的设备才可以阻止流量。因为被阻止的连接实际上在被动部署中并未被阻止，所以系统可能针对每个被阻止的连接报告多个连接开始事件。有关详细信息，请参阅第 38-6 页上的了解受阻和交互式受阻连接的记录。

注意事项 在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件使数据库不堪重负。对 Block 规则启用日志记录之前，考虑此规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口的流量。

交互式阻止操作：允许用户绕过网站拦截

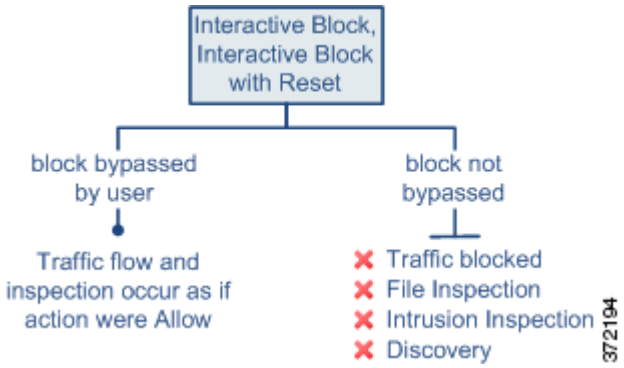
许可证：任何环境

对于未加密的 HTTP 流量，**Interactive Block** 和 **Interactive Block with reset** 使用户有机会通过点击可定制的警告页面（称为 *HTTP 响应页面*绕过网站拦截。 Interactive Block with reset 规则也可以重置连接。

注 对于已解密和加密的 (HTTPS) 流量，Interactive Block 规则阻止无交互的匹配连接，并且系统**不**显示响应页面。有关配置 SSL 检查功能以解密流量的信息，请参阅第 19-1 页上的了解流量解密。

对于所有交互式阻止的流量，系统的处理、检查和日志记录取决于用户是否绕过拦截：

- 如果用户不（或无法）绕过拦截，该规则模拟 Block 规则。匹配的流量不经进一步检查即被拒绝，并且您可以只记录连接的开始。这些连接开始事件有 `Interactive Block` 或 `Interactive Block with Reset` 操作。
- 如果用户绕过拦截，该规则模拟 Allow 规则。因此，您可以将任一类型的 Interactive Block 规则与文件和入侵策略关联，以检查此用户允许的流量。系统也可以使用网络发现检查它，您可以记录连接开始和结束事件。这些连接事件有 `Allow` 的操作。



Allow 操作：允许和检查流量

许可证：任何环境

Allow 操作允许匹配的流量通过。当您允许流量时，可以使用关联的入侵或文件策略（或两者）进一步检查和阻止未加密或解密的网络流量：

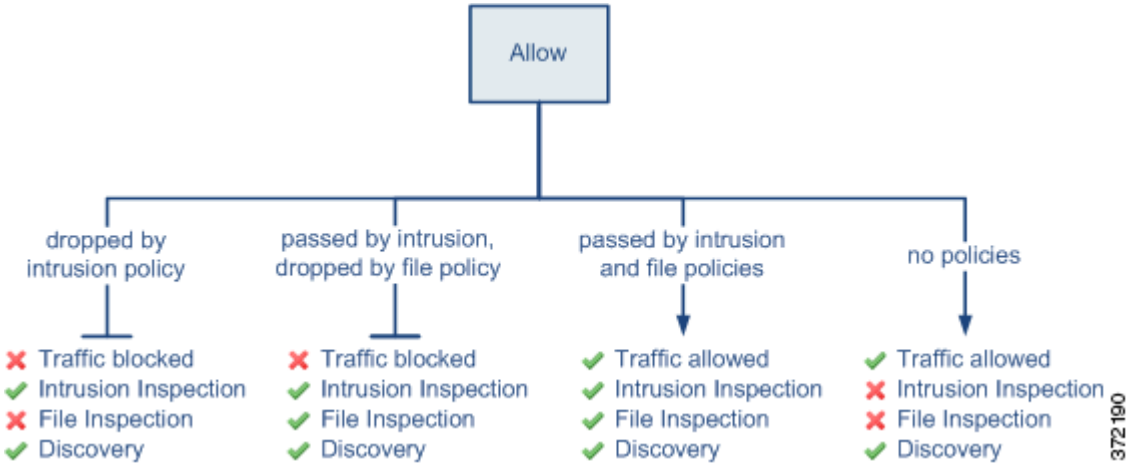
- 借助保护许可证，您可以使用入侵策略，根据入侵检测和防御配置分析网络流量，或者丢弃恶意数据包。
- 借助保护许可证，还可以使用文件策略执行文件控制。借助文件控制，可以检测和阻止用户通过特定应用协议上传（发送）或下载（接收）特定类型的文件。
- 借助恶意软件许可证，您还可以使用文件策略执行基于网络的高级恶意软件防护 (AMP)。基于网络的 AMP 可以检查文件中的恶意软件，或者阻止检测到的恶意软件。

有关如何将入侵或文件策略与访问控制规则相关联的指导，请参阅第 18-1 页上的使用入侵和文件策略控制流量。

下图说明在满足 Allow 规则（或用户忽略的 Interactive Block 规则；请参阅第 14-8 页上的交互式阻止操作：允许用户绕过网站拦截）条件的流量中进行的检查类型。请注意，文件检查会在入侵检查之前发生；被阻止文件不会进行入侵相关漏洞检测。

为简单起见，该图显示入侵和文件策略均与访问控制规则相匹配（或都不匹配）的情况下的流量。但是，可以单独配置其中一个策略。如果没有文件策略，流量将由入侵策略确定；如果没有入侵策略，流量将由文件策略确定。

不管入侵或文件策略会检测还是丢弃流量，系统都可以使用网络发现功能进行检查。但是，允许流量不会自动确保发现检查。系统仅对涉及 IP 地址的连接执行发现功能，根据网络发现策略明确监控这些 IP 地址；此外，对于加密会话，应用发现受到限制。有关详细信息，请参阅第 45-1 页上的网络发现简介。



您可以在连接开始和结束时记录允许的网络流量。

借助 3 系列设备信任或阻止流量的限制

许可证：任何环境

受支持的设备：3 系列

当您将访问控制策略应用到 3 系列设备时，系统可能*改进*满足具体标准的访问控制规则。已改进规则利用 3 系列设备上的专用硬件立即转向或阻止不需要深度数据包检测的流量。它们的优点在于其确定流量的正确路径的速度。

由于此评估发生在硬件级别，因此系统只能通过改进规则来使用有限信息快速处理连接。 3 系列设备对满足以下所有标准的规则进行改进：

- 具有 **Trust**、 **Block** 或 **Block with reset** 操作
- 仅使用简单的、基于网络的条件：安全区域、 IP 地址、 VLAN 标记和端口
- 置于**所有**其他访问控制规则（无论操作如何）之上，这些规则执行深度数据包检测，即，具有应用、URL、用户或基于地理定位的条件
- 也置于**所有** Monitor 规则之上

因此，已改进为提高性能的规则最可能是简单的 Trust 或 Block 规则，这些规则置于靠近访问控制规则 （具有小编号的规则）顶部的位置或者置于仅使用简单的、基于网络的规则的策略中。但是，通过规则改进获得的性能优势会带来某些意外行为。

抢占安全情报

在处理访问控制策略的安全情报黑名单之前，系统首先处理已改进的规则。这意味着已改进的 Trust 规则能够允许列入黑名单的流量未经检查就通过 3 系列设备。有关安全情报的详细信息，请参阅第 13-1 页上的使用安全情报 IP 地址信誉实施黑名单。

防止显示 HTTP 响应页面

即使系统成功阻止流量，已改进的 Block 规则阻止的网络流量也不会导致系统向用户显示已配置的 HTTP 响应页面。相反，请求禁止的 URL 的用户将连接重置或超时。有关配置响应页面的详细信息，请参阅第 16-15 页上的显示被阻止 URL 的自定义网页。

IPv6 流量处理

系统可以检查 IPv4 和 IPv6 流量。IPv6 检查包括 4in6、6in4、6to4 和 6in6 隧道方案；当 UDP 报头指定端口 3544 时，还包括 Teredo 隧道。当使用访问控制规则和 IP 地址条件评估流量时，在大多数情况下，3 系列设备匹配您根据最内部数据包报头中的 IP 地址指定的 IP 地址。

但是，无论 IPv6 流量是否已传输，以及 IPv6 报头是最内部还是最外部，已改进规则都使用**最外部**报头中的 IP 地址评估该流量。换句话说，当已改进规则评估已传输的流量时，只有 4in4 流量使用最内部报头与访问控制规则标准进行匹配。

例如，请考虑这样一个场景：您正使用 3 系列设备检查通过 IPv4 网络发送的 6in4 已传输流量。您创建简单的、基于网络的访问控制规则，该规则阻止流入或流出特定 IPv6 地址的流量。如果系统因为规则在访问控制策略中的位置而改进规则，则规则不起作用。这是因为，系统将传输的数据包的最外部 IPv4 报头与永远不会触发的 IPv6 规则条件相匹配。系统使用后续的访问控制规则或策略的默认操作处理流量，就好像规则不存在。

将注释添加到规则中

许可证：任何环境

当创建或编辑访问控制规则时，您可以添加注释。例如，您可为其他用户汇总整体配置，或者当您变更规则和更改的原因时进行记录。您可以显示规则的所有注释列表，以及添加每条注释的用户以及添加注释的日期。

提示　要在保存访问控制规则时提示（或强制）FireSIGHT 系统用户输入注释，请参阅第 63-7 页上的配置访问控制策略首选项。

当保存规则时，自从上次保存操作以来做出的所有注释都变为只读。

要将注释添加到规则，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在访问控制规则编辑器中，选择 **Comments** 选项卡。

系统将显示 Comments 页面。

步骤 2　点击 **New Comment**。

系统将显示 New Comment 弹出窗口。

步骤 3　键入您的注释，然后点击 **OK**。

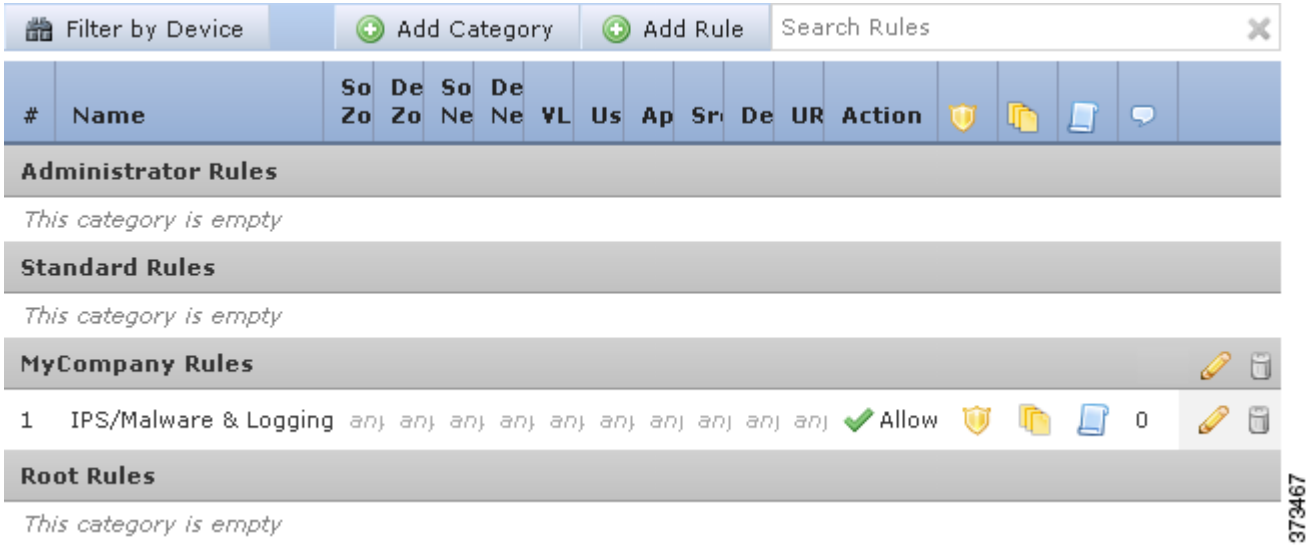
您的注释成功保存。您可以编辑或删除此注释，直到您保存规则为止。

步骤 4　保存或继续编辑规则。

管理策略中的访问控制规则

许可证：任何环境

如下图所示，访问控制策略编辑器的 Rules 选项卡允许您添加、编辑、搜索、移动、启用、禁用、删除和以其他方式管理策略中的访问控制规则。



对于每个规则，策略编辑器显示其名称、条件概要、规则操作以及传达规则检查和日志记录选项的图标。其他图标表示注释、警告、错误和其他重要信息，如下表所述。被禁用的规则在规则名称下方呈灰色显示并带有相应的标记 (disabled)。

表 14-2　　了解访问控制策略编辑器

图标	说明	您可以.....
	入侵检测	点击活动（黄色）检查图标编辑规则的检查选项；请参阅第 18-1 页上的使用入侵和文件策略控制流量。如果图标为非活动状态（白色），则没有为该规则选择此类型的策略。
	文件和恶意软件检查	
	日志记录	点击活动（蓝色）日志记录图标编辑规则的日志记录选项；请参阅第 38-13 页上的根据访问控制处理记录连接。如果图标为非活动状态（白色），则已为该规则禁用连接日志记录。
	注释	点击注释列中的数字向规则添加注释；请参阅第 14-11 页上的将注释添加到规则中。数字指示规则已包含的注释数。
	警告	将鼠标指针悬停在图标上，可以阅读警告、错误或信息文本；请参阅第 12-18 页上的对访问控制策略和规则进行故障排除。
	错误	
	信息	

有关管理控制规则的信息，请参阅：

- 第 14-2 页上的创建和编辑访问控制规则
- 第 14-13 页上的搜索访问控制规则
- 第 14-13 页上的按受影响设备显示规则
- 第 14-14 页上的启用和禁用规则
- 第 14-14 页上的更改规则的位置或类别

搜索访问控制规则

许可证：任何环境

可以使用字母数字字符串（包括空格和可打印的特殊字符）在访问控制规则列表中搜索匹配值。搜索会检查规则名称和已添加至规则的任意规则条件。对于规则条件，搜索会匹配可以为每个条件类型（区域、网络、应用程序等）添加的任意名称或值。这包括各个对象名称或值、组对象名称、组内的各个对象名称或值以及文本值。

可以使用部分或完整的搜索字符串。对于每个匹配规则，匹配值列将会突出显示。例如，如果在所有或部分规则上搜索字符串 `100Bao`，已添加 100Bao 应用程序的每个规则的 Applications 列都会突出显示。如果有名为 100Bao 的规则，则 Name 和 Applications 列都会突出显示。

可以导航至每个上一个或下一个匹配规则。状态消息会显示当前的匹配项以及匹配项的总数量。

匹配可能会出现在多页规则列表的任意页面上。当第一个匹配项不在第一个页面上时，屏幕上将会显示第一个匹配项所在的页面。当您处于最后一个匹配项时，选择下一匹配项会使您到达第一个匹配项，当处于第一个匹配项时，选择上一匹配项会到达最后一个匹配项。

要搜索规则，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在想要搜索的策略的访问控制策略编辑器中，点击 **Search Rules** 提示信息，键入搜索字符串，然后按 Enter 键。还可以使用 Tab 键或点击空白页面区域来发起搜索。

带有匹配值的规则列会被突出显示，其突出显示方式与指示的（第一个）匹配项不同。

步骤 2　查找您感兴趣的规则：

- 要在匹配规则之间导航，可以点击下一匹配项 (▼) 或上一匹配项 (▲) 图标。
- 要刷新页面并清除搜索字符串和所有突出显示的内容，请点击清除图标 (✖)。

按受影响设备显示规则

许可证：任何环境

可以过滤在访问控制策略中列出的访问控制规则，以便仅显示用来管理一个或多个指定设备的流量的规则。

要确定影响设备的规则，系统使用访问控制规则的区域条件。安全区域是接口的逻辑分组，因此，如果区域条件包括接口，处理流量的接口所在的设备受该规则影响。没有区域条件的规则适用于所有区域，因此适用于每台设备。

请注意，如果添加了新的规则，或者编辑并保存现有的规则，则过滤条件被清除。

要按设备或设备组过滤规则，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要过滤其规则的策略的访问控制规则编辑器中，点击规则列表上面的 **Filter by Device** 。

屏幕上将会显示 Filter by Device 弹出窗口。如果向策略添加了设备或设备组，屏幕上将会显示目标设备和设备组的列表。

步骤 2　选择一个或多个复选框，以仅显示应用至这些设备或组的规则。另外，可以选择 **All** 复选框，以重置和显示所有的规则。

步骤 3　点击 **OK**。

页面将会更新，从而显示针对选择的设备和设备组的规则，并且隐藏针对未选择的设备和设备组的规则。

启用和禁用规则

许可证：任何环境

创建访问控制规则时，默认情况下启用规则。如果您禁用某规则，系统将不用该规则来评估网络流量并停止为该规则生成警告和错误。在查看访问控制策略中的规则列表时，禁用的规则会呈灰色显示，不过，您仍然可以修改它们。请注意，您还可以使用规则编辑器启用或禁用访问控制规则；请参阅第 14-2 页上的创建和编辑访问控制规则。

要更改访问控制规则的状态，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在策略（包含要启用或禁用的规则）的访问控制策略编辑器中，右键点击此规则并选择规则状态：

- 要启用非活动规则，请选择 **State > Enable**。
- 要禁用活动规则，请选择 **State > Disable**。

步骤 2　点击 **Save** 保存策略。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

更改规则的位置或类别

许可证：任何环境

为帮助您组织访问控制规则，每个访问控制策略都有三个系统提供的规则类别：管理员规则、标准规则和根规则。尽管可以创建自定义类别，但不能移动、删除或重命名这些类别。

默认情况下，允许修改访问控制策略的任何预定义用户角色还允许您在规则类别内部和之间移动和修改访问控制规则。但是，可以创建自定义角色来限制用户移动和修改规则。

有关详细信息，请参阅：

- 第 14-14 页上的移动规则
- 第 14-15 页上的添加新的规则类别

移动规则

许可证：任何环境

正确的访问控制规则顺序降低处理网络流量所需的资源，并防止规则抢占。默认情况下，允许修改访问控制策略的任何预定义用户角色还允许您在规则类别内部和之间移动访问控制规则。但是，可以创建自定义角色来限制用户移动系统提供的类别中的规则。

以下步骤说明如何使用访问控制策略编辑器一次移动一个或多个规则。还可以使用规则编辑器移动单个访问控制规则；请参阅第 14-2 页上的创建和编辑访问控制规则。

要移动规则，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在策略（包含要移动的规则）的访问控制策略编辑器中，通过点击每个规则的空白区域来选择规则。使用 Ctrl 和 Shift 键选择多个规则。

您选择的规则突出显示。

步骤 2　移动规则。可以剪切、粘贴或拖放规则。

要将规则剪切并粘贴到新位置，请右键点击选定的规则并选择 **Cut**。然后，在想要粘贴所剪切规则的位置旁，右键单击规则的空白区域并选择 **Paste above** 或 **Paste below**。请注意，您不能复制和粘贴两个不同的访问控制策略之间的访问控制规则。

步骤 3　点击 **Save** 保存策略。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

添加新的规则类别

许可证：任何环境

为帮助您组织访问控制规则，每个访问控制策略都有三个系统提供的规则类别：管理员规则、标准规则和根规则。尽管在标准规则和根规则之间创建自定义类，但是不能移动、删除或重命名这些类别。

添加自定义类别允许进一步组织规则，而无需创建额外的策略。可以重命名和删除添加的类别。不能移动这些类别，但可以将规则移入其中以及从中移出。

尽管可以创建自定义规则，这些规则限制用户移动和修改系统提供的类别中的规则，但是可以修改访问控制策略的所有用户都可以向自定义类别中添加规则，并无限制地修改类别中的规则。

要添加新的类别，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要添加规则类别的策略的访问控制策略编辑器中，点击 Add Category。

提示　如果您的策略已经包含规则，则可以点击现有规则所在行的空白区域，先设置新类别的位置，然后才能添加。还可以右键点击现有规则并选择 **Insert new rule**。

屏幕上将会显示 Add Category 弹出窗口。

步骤 2　键入唯一的类别**名称**。

可以输入字母数字名称，包括空格和特殊的可打印字符，最多可有 30 个字符。

步骤 3　有以下选项可供选择：

- 要将新的类别定位至紧靠现有类别上方的位置，请从第一个 **Insert** 下拉列表中选择 **above Category**，然后从第二个下拉列表选择您想要在其上定位规则的类别。
- 如要将新的类别规则定位至现有规则之下，从下拉列表选择 **below rule**，然后输入现有规则编号。仅当策略中存在至少一个规则时，该选项才有效。
- 如要将规则定位至现有规则之上，从下拉列表选择 **above rule**，然后输入现有规则编号。仅当策略中存在至少一个规则时，该选项才有效。

步骤 4　点击 **OK**。

您的类别成功添加。您可以点击自定义类别旁边的编辑图标 ( ) 编辑其名称，或者点击删除图标 ( ) 删除此类别。删除的类别中的规则将会添加至以上类别。

步骤 5　点击 **Save** 保存策略。

使用基于网络的规则控制流量

*访问控制策略*中的*访问控制规则*对网络流量日志记录和处理进行精细控制。基于网络的条件可供您使用以下一个或多个条件管理哪些流量可以穿越您的网络：

- 源和目标安全区域
- 源和目标 IP 地址或地理位置
- 数据包的最内部的 VLAN 标记
- 源端口和目标端口，还包括传输层协议和 ICMP 代码选项

您可以将基于网络的条件相互组合及与其他类型的条件组合来创建访问控制规则。这些访问控制规则可能很简单，也可能很复杂，使用多个条件匹配和检查流量。有关访问控制规则的详细信息，请参阅第 14-1 页上的使用访问控制规则调整流量。

注 基于硬件的快速路径规则、基于安全情报的流量过滤以及一些解码和预处理在访问控制规则评估网络流量**之前**发生。您还可以配置 *SSL 检查*功能在访问控制规则对已加密的流量进行评估之前阻止或解密它。

您可以使用任何 FireSIGHT 系统设备和任何许可证执行大多数基于网络的访问控制，然而基于地理定位的访问控制要求 FireSIGHT 许可证并且在许多 2 系列设备上不受支持，在 用于 Blue Coat X-系列的思科 NGIPS设备上也不受支持。此外， ASA FirePOWER 设备不支持通过 VLAN 进行访问控制。

表 15-1 基于网络的访问控制规则的许可证和模型要求

要求	VLAN 标记	地理定位控制	所有其他基于网络的控制
许可证	任何环境	FireSIGHT	任何环境
设备	任何设备，除了 ASA FirePOWER	3 系列 虚拟 ASA FirePOWER	任何环境
防御中心	任何环境	除 DC500 外的所有型号	任何环境

有关构建基于网络的访问控制规则的信息，请参阅：

- 第 15-2 页上的通过安全区域控制流量
- 第 15-3 页上的按网络或地理位置控制流量
- 第 15-5 页上的控制 VLAN 流量
- 第 15-6 页上的通过端口和 ICMP 代码控制流量

通过安全区域控制流量

许可证：任何环境

访问控制规则中的区域条件可供您按流量的源和目标安全区域控制流量。*安全区域*是一个或多个接口的组合，这些接口可能位于多台设备上。您在设备的初始设置期间选择的选项，称为其*检测模式*，确定系统最初如何配置设备的接口以及这些接口是否属于安全区域。

一个简单的示例就是，当您注册带**内联**检测模式的设备时，防御中心创建两个区域：内部和外部，并将设备上的第一对接口分配到这些区域。连接到网络内侧的主机表示受保护资产。

为了扩展此情景，您可以部署其他相同配置的设备（由同一防御中心管理）以保护多个不同位置的类似资源。就像第一台设备一样，每台这些设备均保护其内部安全区域中的资产。

提示　您不需要将所有内部（或外部）接口组合到单个区域中。选择对您的部署和安全策略有意义的组合方式。有关创建区域的详细信息，请参阅第 3-34 页上的使用安全区域。

在此部署中，您可能决定尽管您希望这些主机可以不受限制地访问互联网，但是也想要通过检查传入流量是否存在入侵和恶意软件来保护它们。

要使用访问控制实现此目标，请配置包含区域条件的访问控制规则，其中 **Destination Zone** 设置为 **Internal**。此简单访问控制规则与从内部区域中任何接口离开设备的流量相匹配。

要确保系统检查匹配流量是否存在入侵和恶意软件，请选择 **Allow** 规则操作，然后将该规则与入侵和文件策略相关联。有关详细信息，请参阅第 14-6 页上的使用规则操作确定流量处理和检查和第 18-1 页上的使用入侵和文件策略控制流量。

如果要构建更为复杂的规则，可向单个区域条件中的每个**源区域**和**目标区域**最多可添加 50 个区域。

- 要与从一个区域中的接口*离开*设备的流量相匹配，请将该区域添加到**目标区域**。

  由于以被动方式部署的设备不会传输流量，因此，在**目标区域**条件中不能使用由被动接口组成的区域。
- 要与从一个区域中的接口*进入*设备的流量想匹配，请将该区域添加到**源区域**。
- 如果同时向一条规则添加源区域和目标区域条件，则匹配流量必须源自其中一个指定源区域**并**通过其中一个目标区域流出。

请注意，正如一个区域中的所有接口必须为相同类型（全部为内联、全部为被动、全部已交换或全部已路由），访问控制规则的区域条件中使用的全部区域必须为同一类型。也就是说，您不能编写与源自或流出不同类型区域的流量相匹配的单条规则。

构建区域条件时，警告图标指明无效的配置。有关详细信息，请将鼠标指针悬停在图标上方并参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

要按区域控制流量，请执行以下步骤：

访问：管理员/访问管理员/网络管理员

步骤 1　在将您想要按区域控制流量所处设备锁定为目标的访问控制策略中，新建访问控制规则或编辑现有规则。

有关详细说明，请参阅第 14-2 页上的创建和编辑访问控制规则。

步骤 2　在规则编辑器中，选择 Zones 选项卡。

系统将显示 Zones 选项卡。

步骤 3　查找并选择您要从 **Available Zones** 添加的用户和组。

要搜索需要添加的区域，请点击 **Available Zones** 列表上方的 **Search by name** 提示，然后键入区域名称。列表会在您键入内容时进行更新，以显示匹配区域。

点击以选择区域。要选择多个区域，请使用 Shift 和 Ctrl 键，或右键单击并选择 **Select All**。

步骤 4　点击 **Add to Source** 或 **Add to Destination**，以将选定区域添加至适当列表。

您也可以拖放选定的区域。

步骤 5　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

按网络或地理位置控制流量

许可证：因功能而异

受支持的设备：因功能而异

受支持的防御中心：因功能而异

访问控制规则中的网络条件可供您按流量的源和目标 IP 地址控制流量。您还可以：

- 明确指定要控制的流量的源和目标 IP 地址，或者
- 使用地理位置功能，该功能将 IP 地址与地理位置关联，以便根据流量的源或目标国家/地区或大陆控制流量

在构建基于网络的访问控制规则条件时，可以手动指定 IP 地址和地理位置。另外，您可以使用网络和地理位置*对象*配置网络条件，这些对象可重复使用，可以将名称与一个或多个 IP 地址、地址块、国家/地区、大陆等相关联。

提示　创建网络或地理位置对象后，您不仅可将其用于构建访问控制规则，还可以在系统的 Web 界面的各个其他位置将其用于代表 IP 地址。您可以使用对象管理器来创建这些对象；您也可以在配置访问控制规则时动态创建网络对象。有关详细信息，请参阅第 3-1 页上的管理可重用对象。

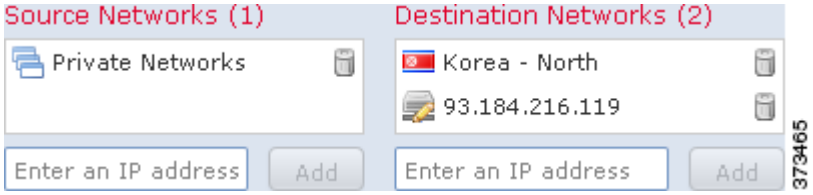
请注意，如果您要编写按地理位置控制流量的规则，请确保使用最新地理定位数据过滤您的流量，思科**强烈**建议您定期更新防御中心上的地理定位数据库 (GeoDB)；请参阅第 66-24 页上的更新地理定位数据库。

此外，请注意，尽管您可以使用任何 FireSIGHT 系统设备和任何许可证执行简单的基于 IP 地址的访问控制，然而基于地理定位的访问控制需要 FireSIGHT 许可证并且在许多 2 系列设备上不受支持，在 用于 Blue Coat X-系列的思科 NGIPS设备上也不受支持。

表 15-2　网络条件许可证和模型要求

要求	地理定位控制	IP 地址控制
许可证	FireSIGHT	任何环境
设备	3 系列、虚拟、 ASA FirePOWER	任何环境
防御中心	除 DC500 外的所有型号	任何环境

下图显示的网络条件与阻止源自您的内部网络并尝试访问位于朝鲜或 93.184.216.119 (example.com) 的连接的访问控制规则相对应。



在此示例中，称为专用网络的网络对象组（包括 IPv4 和 IPv6 专用网络网络对象，未显示）表示您的内部网络。此示例还手动指定了 example.com IP 地址，并使用系统提供的朝鲜地理定位对象代表朝鲜 IP 地址。

在单一网络条件中，您可以向每个 **Source Networks** 和 **Destination Networks** 最多添加 50 项，而且可以混用基于网络和基于地理定位的配置。

- 要与*源自* IP 地址或地理位置的流量相匹配，请配置 **Source Networks**。
- 要与*流向* IP 地址或地理位置的流量相匹配，请配置 **Destination Networks**。

如果同时向一条规则添加源网络条件和目标网络条件，则匹配流量必须源自其中一个指定 IP 地址**并**流向其中一个目标 IP 地址。

构建网络条件时，警告图标指明无效的配置。有关详细信息，请将鼠标指针悬停在图标上方并参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

要按网络或地理位置控制流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在将您想要按网络控制流量所处设备锁定为目标的访问控制策略中，新建访问控制规则或编辑现有规则。

有关详细说明，请参阅第 14-2 页上的创建和编辑访问控制规则。

步骤 2　在规则编辑器中，选择 Networks 选项卡。

系统将显示 Networks 选项卡。

步骤 3　查找并选择您要从 **Available Networks** 添加的网络，如下所述：

- 单击 Networks 选项卡显示要添加的网络对象和组；单击 Geolocation 选项卡显示地理定位对象。
- 要动态添加网络对象，以便随后可将其添加到条件，请点击 **Available Networks** 列表上方的添加图标 ( )；请参阅第 3-4 页上的使用网络对象。
- 要搜索需要添加的网络或地理定位对象，请选择相应的选项卡，点击 **Available Networks** 列表上方的 **Search by name or value** 提示，然后键入对象名称或其中一个对象组件的值。列表会在您键入内容时进行更新，以显示匹配对象。

要选择一个对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键，或右键单击并选择 **Select All**。

步骤 4　点击 **Add to Source** 或 **Add to Destination** 将选定对象添加到适当列表。

您也可以拖放选定的对象。

步骤 5　添加要手动指定的任何源或目标 IP 地址或地址块。

点击 **Source Networks** 或 **Destination Networks** 列表下方的 **Enter an IP address** 提示；然后键入一个 IP 地址或地址块并点击 **Add**。

步骤 6　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

控制 VLAN 流量

许可证：任何环境

受支持的设备：任何防御中心，除了ASA FirePOWER

访问控制规则中的 VLAN 条件可供您控制具有 VLAN 标记的流量。系统使用最内部的 VLAN 标记来通过 VLAN 识别数据包。

在构建基于 VLAN 的访问控制规则条件时，可以手动指定 VLAN 标记。或者，您可以使用 VLAN 标记 *objects* 配置 VLAN 条件，这些对象可重复使用并将名称与一个或多个 VLAN 对象相关联。

提示　创建 VLAN 标记对象后，您不仅可将其用于构建访问控制规则，还可以在系统的网络接口中的各个其他位置将其用于代表 VLAN 标记。可以使用对象管理器创建 VLAN 标记对象或在配置访问控制规则时动态创建该对象。有关详细信息，请参阅第 3-12 页上的使用 VLAN 标记对象。

下图显示访问控制规则的 VLAN 标记条件，该规则与面向公众的 VLAN （由 VLAN 标记对象组表示）以及手动添加的 VLAN 42 上的流量相匹配。

在单个 VLAN 标记条件中，最多可向 **Selected VLAN Tags** 添加 50 项。在构建 VLAN 标记条件时，警告图标指明无效的配置。有关详细信息，请将鼠标指针悬停在图标上方并参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

要按 VLAN 标记控制流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在将您想要按 VLAN 标记控制流量所处设备锁定为目标的访问控制策略中，新建访问控制规则或编辑现有规则。

有关详细说明，请参阅第 14-2 页上的创建和编辑访问控制规则。

步骤 2　在规则编辑器中，选择 VLAN Tags 选项卡。

系统将显示 VLAN Tags 选项卡。

步骤 3　查找并选择您要从 **Available VLAN Tags** 添加的 VLAN，如下所述：

- 要动态添加 VLAN 标记，以便随后可将其添加到条件，请点击 Available VLAN Tags 列表上方的添加图标 ()；请参阅 。第 3-12 页上的使用 VLAN 标记对象
- 要搜索需要添加的 VLAN 标记对象和组，请单击 **Available VLAN Tags** 列表上方的 **Search by name or value** 提示，然后键入对象的名称或对象中的一个 VLAN 标记的值。列表会在您键入内容时进行更新，以显示匹配对象。

要选择一个对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键，或右键单击并选择 **Select All**。

步骤 4　点击 **Add to Rule** 将选定的对象添加到 **Selected VLAN Tags** 列表。

您也可以拖放选定的对象。

步骤 5　添加要手动指定的任何 VLAN 标记。

或者，点击 **Selected VLAN Tags** 列表下方的 **Enter a VLAN Tag** 提示，然后键入一个 VLAN 标记或范围，最后点击 **Add**。可以指定介于 1 和 4094 之间的任何 VLAN 标记；使用连字符指定 VLAN 标记的范围。

步骤 6　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

通过端口和 ICMP 代码控制流量

许可证：任何环境

访问控制规则中的网络条件可供您按流量的源和目标端口控制流量。在此情景中，“端口”是指下列其中一项：

- 对于 TCP 和 UDP，您可以根据传输层协议控制流量。系统使用括号内的协议号以及可选的关联端口或端口范围表示此配置。例如：TCP(6)/22。
- 对于 ICMP 和 ICMPv6 (IPv6-ICMP)，您可以根据流量的互联网层协议外加可选的类型和代码控制流量。例如：ICMP(1):3:3。
- 您可以使用未使用端口的其他协议控制流量。

在构建基于端口的访问控制规则条件时，可以手动指定端口。此外，您可以使用端口 *objects* 配置端口条件，这些对象可重复使用，可将名称与一个或多个端口相关联。

提示　创建端口对象后，您不仅可将其用于构建访问控制规则，还可以在系统的网络接口中的各个其他位置将其用于代表端口。您可以使用对象管理器创建端口对象，也可以在配置访问控制规则时动态创建端口对象。有关详细信息，请参阅第 3-10 页上的使用端口对象。

在单一网络条件中，您可以向每个 **Selected Source Ports** 和 **Selected Destination Ports** 列表最多添加 50 项：

- 要与*源自*端口的流量相匹配，请配置 **Selected Source Ports**。

  如果仅将源端口添加至条件，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为源端口条件。
- 要与*流向*端口的流量相匹配，请配置 **Destination Ports**。

  如果仅将目标端口添加至条件，则可以添加使用不同传输协议的端口。

- 要与即源自特定 **Selected Source Ports** 又流向特定 **Selected Destination Ports** 的流量相匹配，请同时配置二者。

  如果同时将源和目标端口添加至条件，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

在构建端口条件时请记住以下要点：

- 当您添加类型设置为 0 的目标 ICMP 端口或类型设置为 129 的目标 ICMPv6 端口时，访问控制规则仅与主动提供的回应回复相匹配。为应答 ICMP 回应请求而发送的 ICMP 回应回复被忽略。为使某个规则匹配任何 ICMP 回应，请使用 ICMP 类型 8 或 ICMPv6 类型 128。
- 当您将 GRE (47) 协议用作目标端口条件时，只能将基于网络的其他条件添加至访问控制规则，即区域和网络以及 VLAN 标记条件。如果您添加基于声誉或用户的条件，则无法保存规则。

构建端口条件时，警告图标指明无效的配置。例如，您可以使用对象管理器来编辑正在使用的端口对象，以使使用这些对象组的规则变得无效。有关详细信息，请将鼠标指针悬停在图标上方并参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

要按端口控制流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在将您想要按端口控制流量所处设备锁定为目标的访问控制策略中，新建访问控制规则或编辑现有规则。

有关详细说明，请参阅第 14-2 页上的创建和编辑访问控制规则。

步骤 2　在规则编辑器中，选择 Ports 选项卡。

系统将显示 Ports 选项卡。

步骤 3　查找并选择您要从 **Available Ports** 添加的端口，如下所述：

- 要动态添加您随后可以添加至条件的端口对象，请点击 Available Ports 列表上方的添加图标（  ）；请参阅第 3-10 页上的使用端口对象。
- 要搜索需要添加的端口对象和组，请点击 **Available Ports** 列表上方的 **Search by name or value** 提示，然后键入对象名称或对象中某一端口的值。列表会在您键入内容时进行更新，以显示匹配对象。例如，如果键入 80，防御中心显示思科提供的 HTTP 端口对象。

  要选择一个对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键，或右键单击并选择 **Select All**。

步骤 4　点击 **Add to Source** 或 **Add to Destination** 将选定对象添加到适当列表。

您也可以拖放选定的对象。

步骤 5　添加要手动指定的任何源或目标端口。

- 对于源端口，请从 **Selected Source Ports** 列表下方的 **Protocol** 下拉列表中选择 **TCP** 或 **UDP**。然后，输入一个**端口**。您可以为单个端口指定从 0 到 65535 之间的一个值。
- 对于目标端口，请从 **Selected Destination Ports** 列表下方的 **Protocol** 下拉列表中选择一个协议（包括表示所有协议的 **All**）。您还可以在键入未显示在列表中的未分配协议的编号。

  如果选择 **ICMP** 或 **IPv6 ICMP**，系统将显示弹出窗口，可以在其中选择类型和相关代码。有关 ICMP 类型和代码的详细信息，请参阅 http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml 和 http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml。

  如果您不想指定协议，或者，如果指定 TCP 或 UDP，请输入一个**端口**。您可以为单个端口指定从 0 到 65535 之间的一个值。

点击 **Add**。请注意，防御中心不会将会导致无效配置的端口添加至规则条件。

步骤 6　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

使用基于信誉的规则控制流量

*访问控制策略*中的*访问控制规则*对网络流量日志记录和处理实行精细控制。 k traffic logging and handling.访问控制规则中的基于信誉的条件允许通过情景化网络流量并在适当情况下对其进行限制来管理哪些流量可以穿越网络。访问控制规则监管以下类型的基于信誉的控制：

- 通过应用条件可执行*应用控制*，它不仅根据单独的应用还根据应用的基本类型（类型、风险、业务关联性和标记）来控制应用流量。
- 通过 URL 条件可执行 *URL 过滤*，它根据单独的网站以及网站的系统分配的类别和信誉来控制网络流量。

可以将基于信誉的条件相互组合并与其他类型的条件组合，以创建访问控制规则。这些访问控制规则可以简单也可以复杂，从而使用多个条件来匹配和检查流量。有关访问控制规则的详细信息，请参阅第 14-1 页上的使用访问控制规则调整流量。

注 基于硬件的快速路径规则、基于安全情报的流量过滤以及一些解码和预处理发生在访问控制规则评估网络流量**之前**。您也可以配置 *SSL 检查*功能来阻止或解密加密流量，然后再由访问控制规则评估该流量。

基于信誉的访问控制需要以下许可证、设备和防御中心。

表 16-1 基于信誉的访问控制规则的许可证和型号要求

要求	应用控制	URL 过滤（类别 和信誉）	URL 过滤（手动）
许可证	可控性	URL 过滤	任意
设备	任意，2 系列 或 X -系列除外	任何设备，除了 2 系列	任何设备，除了 2 系列
防御中心s	任意	除 DC500 外的所有型号	任何环境

有关向访问控制规则中添加基于信誉的条件的信息，请参阅：

- 第 16-2 页上的控制应用流量
- 第 16-7 页上的阻止 URL

FireSIGHT 系统可执行其他类型的基于信誉的控制，但是您没有使用访问控制规则配置这些类型。有关详情，请参阅：

- 第 13-1 页上的使用安全情报 IP 地址信誉实施黑名单说明如何根据连接的源或目标的信誉（作为第一道防线）限制流量。
- 第 18-7 页上的调整的入侵防御性能说明如何检测、跟踪、存储、分析和阻止恶意软件以及其他类型的禁止文件的传输。

控制应用流量

许可证：可控性

受支持的设备：任意，2 系列或 X -系列除外

FireSIGHT 系统在分析 IP 流量时，可以识别网络上的常用应用并将其分类。系统使用此基于发现的*应用感知*功能使您可以控制网络上的应用流量。

了解应用控制

通过访问控制规则中的应用条件，可以执行此*应用控制*。在单个访问控制规则中，有多种方法可以指定要控制其流量的应用：

- 可以选择单独的应用，包括自定义应用。
- 可以使用系统提供的*应用过滤器*，此类过滤器是根据应用的基本特性（类型、风险、业务关联性、类别和标记）组织的应用的命名集合。
- 可以创建并使用自定义应用过滤器，此类过滤器以选择的任何方式对应用（包括自定义应用）进行分组。

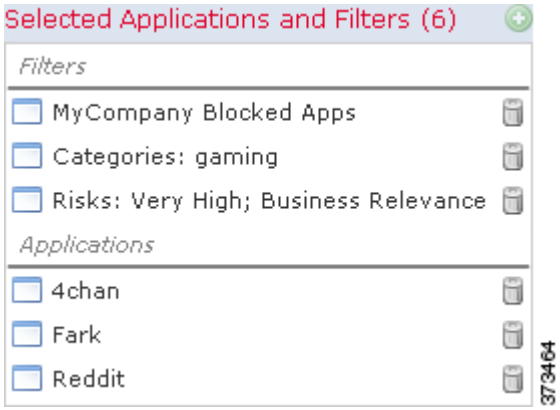
通过应用过滤器，可以快速创建访问控制规则的应用条件。它们会简化策略创建和管理，并保证系统将按预期控制网络流量。例如，可以创建识别并阻止所有高风险、低业务关联性的应用的访问控制规则。如果用户尝试使用这些应用之一，则会阻止会话。

此外，思科通过系统和漏洞数据库 (VDB) 更新频繁更新和添加其他检测器。您还可以创建自己的检测器并向其检测的应用分配特性（风险、关联性等等）。通过根据应用特性使用过滤器，可以确保系统使用最新的检测器来监控应用流量。

构建应用条件

为使流量将访问控制规则与应用条件相匹配，流量必须与向 **Selected Applications and Filters** 列表中添加的其中一个过滤器或应用相匹配。

下图显示用于阻止以下内容的访问控制规则的应用条件：MyCompany 的自定义应用组、具有高风险和低业务关联性的所有应用、游戏应用以及一些单独选定的应用。



在单个应用条件中，可以向 **Selected Applications and Filters** 列表中添加最多 50 项。以下每个内容计为一项：

- **Application Filters** 列表中的一个或多个过滤器（单独或以自定义组合形式）此项表示按特性分组的应用集。

- 通过保存 **Available Applications** 列表中的应用搜索创建的过滤器。此项表示按子字符串匹配分组的应用集。
- **Available Applications** 列表中的单独应用。

在 Web 界面中，添加到条件的过滤器会在上方列出并与单独添加的应用分隔开来。

请注意，当应用访问控制策略时，对于具有应用条件的每个规则，系统会生成要匹配的唯一应用的列表。换句话说，可以使用重叠过滤器和单独指定的应用确保完整覆盖。

注　对于加密流量，系统可以仅使用标记为 **SSL Protocol** 的应用来识别和过滤流量。只能在未加密或已解密的流量中检测到没有此标记的应用。此外，系统还会将**解密流量**标记分配给系统只能在解密流量中检测到（在加密或未加密流量中无法检测到）的应用。有关在系统将加密流量与访问控制规则相匹配之前使用 SSL 检查功能解密或阻止该流量的信息，请参阅第 19-1 页上的了解流量解密。

有关详细信息，请参阅以下各节：

将流量与应用过滤器相匹配

许可证：可控性

受支持的设备：任意， 2 系列 或 X -系列除外

当在访问控制策略中构建应用条件时，请使用 **Application Filters** 列表创建按特性分组的要匹配其流量的应用集。

为方便起见，系统使用第 45-9 页上的表 45-2中描述的条件将其检测的每个应用特性化。可以使用这些条件作为过滤器或创建过滤器的自定义组合来执行应用控制。

请注意，过滤访问控制规则中的应用的机制与使用对象管理器创建可重用、自定义应用过滤器的机制相同；请参阅第 3-13 页上的使用应用过滤器。您还可以将在访问控制规则中动态创建的许多过滤器另存为新的可重用过滤器。无法保存包含其他用户创建的过滤器的过滤器，因为不能嵌套用户创建的过滤器。

了解过滤器的组合方式

选择过滤器时（单独或以组合形式），**Available Applications** 列表会更新为仅显示满足条件的应用。可以选择组合形式的系统提供的过滤器，但是不能选择自定义过滤器。

系统将同一类型的多个过滤器与 OR 操作关联。例如，如果您在 Risks 类型下选择 Medium 和 High 过滤器，则产生的过滤器为：

```
Risk: Medium OR High
```

如果 Medium 过滤器包含 110 个应用，而 High 过滤器包含 82 个应用，则系统将在 **Available Applications** 列表中显示全部 192 个应用。

系统将不同类型的过滤器与 AND 操作关联。例如，如果您选择 Risks 类型下的 Medium 和 High 过滤器，以及 Business Relevance 类型项下的 Medium 和 High 过滤器，则所产生的过滤器为：

```
Risk: Medium OR High
和
Business Relevance: Medium OR High
```

在此情况下，系统仅显示 Medium 或 High Risk 类型和 Medium 或 High Business Relevance 类型中均包含的那些应用。

查找并选择过滤器

要选择过滤器，请点击过滤器类型旁边的箭头将其展开，然后选择或清除要显示或隐藏其应用的每个过滤器旁边的复选框。您还可以右键单击提供的过滤器类型（**Risks**、**Business Relevance**、**Types**、**Categories** 或 **Tags**），然后选择 **Check All** 或 **Uncheck All**。

要搜索过滤器，请点击 **Available Filters** 列表上方的 **Search by name** 提示，然后键入名称。列表会在您键入内容时进行更新，以显示匹配过滤器。

选择过滤器完成后，使用 **Available Applications** 列表将这些过滤器添加到规则中；请参阅第 16-4 页上的匹配来自单独应用的流量。

匹配来自单独应用的流量

许可证：可控性

受支持的设备：任意， 2 系列或 X -系列除外

在访问控制规则中构建应用条件时，请使用 **Available Applications** 列表选择要匹配其流量的应用。

浏览应用列表

首次开始构建条件时，列表不受限制，并会显示系统检测的每个应用（一次 100 个）：

- 要翻页浏览应用，请点击列表下方的箭头。
- 要显示包含有关应用特性的摘要信息的弹出窗口以及可以跟随的互联网搜索链接，请点击应用旁边的信息图标 ( )。

查找要匹配的应用

为帮助查找要匹配的应用，可以通过以下方式限制 **Available Applications** 列表：

- 要搜索应用，请点击列表上方的 **Search by name** 提示，然后键入名称。列表会在您键入内容时进行更新，以显示匹配应用。
- 要通过应用过滤器来限制应用，请使用 **Application Filters** 列表（请参阅第 16-3 页上的将流量与应用过滤器相匹配）。**Available Applications** 列表在您应用过滤器时进行更新。为方便起见，系统使用解锁图标 ( ) 标记系统只能在解密流量中识别（在加密或未加密流量中无法识别）的应用。

一旦限制，在 **Available Applications** 列表的顶部便会显示 **All apps matching the filter** 选项。通过此选项，可以一次性将受限制列表中的所有应用都添加到 **Selected Applications and Filters** 列表。

注　如果在 Application Filters 列表中选择一个或多个过滤器，并且还搜索 **Available Applications** 列表，则您的选择和搜索过滤的 **Available Applications** 列表会使用 AND 运算进行组合。也就是说，**All apps matching the filter** 条件包含 **Available Applications** 列表中当前显示的所有单独条件以及在 **Available Applications** 列表上方输入的搜索字符串。

在条件中选择要匹配的单个应用

找到要匹配的应用后，请点击选定该应用。要选择多个应用，请使用 Shift 和 Ctrl 键，或者右键单击并选择 **Select All** 以选择当前受限制视图中的所有应用。

在单个应用条件中，可以通过逐个选择应用来匹配最多 50 个应用；要添加 50 个以上的应用，必须创建多个访问控制规则或使用过滤器对应用进行分组。

选择与条件的过滤器相匹配的所有应用

一旦通过搜索或使用 **Application Filters** 列表中的过滤器进行限制， **Available Applications** 列表的顶部便会显示 **All apps matching the filter** 选项。

通过此选项，可以一次性将受限制 **Available Applications** 列表中的整个应用集添加到 **Selected Applications and Filters** 列表。与逐个添加应用相比，无论组成此应用集的单独应用的数量如何，添加此应用集都仅计为最多 50 项中的一项。

以此方式构建应用条件时，添加到 **Selected Applications and Filters** 列表的过滤器的名称是过滤器中表示的过滤器类型加上每个类型的最多三个过滤器的名称的并置。超过三个相同类型的过滤器后面会加上省略号 (.....)。例如，以下过滤器名称在 Risks 类型下包含两个过滤器，在 Business Relevance 下包括四个过滤器：

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

您使用 **All apps matching the filter** 添加的过滤器中未呈现的过滤器类型不包含在所添加的过滤器名称中。将指针悬停在 **Selected Applications and Filters** 列表中的过滤器名称上方时显示的说明文本指示这些过滤器类型设置为 *any*；也就是说，这些过滤器类型不限制过滤器，因此，这些过滤器类型允许任意值。

可以向应用条件中添加 **All apps matching the filter** 的多个实例，其中每个实例在 **Selected Applications and Filters** 列表中计为单独一项。例如，可以将所有高风险应用添加为一项，清除选择，然后将所有低业务关联性应用添加为另一项。此应用条件与高风险或具有低业务关联性的应用相匹配。

向访问控制规则中添加应用条件

许可证：可控性

受支持的设备：任意， 2 系列或 X -系列除外

为使流量将访问控制规则与应用条件相匹配，流量必须与向 **Selected Applications and Filters** 列表中添加的其中一个过滤器或应用相匹配。

每个条件可以添加最多 50 项，并且添加到条件中的过滤器会在上方列出并与单独添加的应用分隔开来。构建应用条件时，警告图标指示无效配置。有关详细信息，请将指针悬停在图标上方并参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

要控制应用流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在面向要按应用控制流量的设备的访问控制策略中，创建新访问控制规则或编辑现有规则。

有关详细说明，请参阅第 14-2 页上的创建和编辑访问控制规则。

步骤 2　在规则编辑器中，选择 Applications 选项卡。

系统将显示 Applications 选项卡。

步骤 3　或者，使用过滤器限制 **Available Applications** 列表中显示的应用列表。

在 **Application Filters** 列表中选择一个或多个过滤器。有关详细信息，请参阅第 16-3 页上的将流量与应用过滤器相匹配。

步骤 4　从 **Available Applications** 列表中查找并选择要添加的应用。

可以搜索并选择单独应用，或者，当列表受限制时，搜索并选择 **All apps matching the filter**。解锁图标 () 标记系统只能在解密流量中识别（在加密或未加密流量中无法识别）的应用。有关详细信息，请参阅第 16-4 页上的匹配来自单独应用的流量。

步骤 5　点击 **Add to Rule** 将所选应用添加到 **Selected Applications and Filters** 列表。

您也可以拖放所选应用和过滤器。过滤器会显示在标题 *Filters* 下，应用显示在标题 *Applications* 下。

提示　在将其他过滤器添加到此应用条件中之前，请点击 **Clear All Filters** 清除现有选择。

步骤 6　或者，点击 **Selected Applications and Filters** 列表上方的添加图标 ( ) 以保存由列表中当前的所有单独应用和过滤器组成的自定义过滤器。

使用对象管理器在动态创建的过滤器上对此进行管理；请参阅第 3-13 页上的使用应用过滤器。请注意，无法保存包含其他用户创建的过滤器的过滤器，因为不能嵌套用户创建的过滤器。

步骤 7　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

对应用控制的限制

许可证：可控性

受支持的设备：任意， 2 系列或 X -系列除外

执行应用控制时，请记住以下要点。

应用识别的速度

系统在以下情况之前无法执行应用控制：

- 在客户端和服务器之间建立受监控连接，并且
- 系统识别会话中的应用

此识别应在 3 到 5 个数据包内发生，或者在 SSL 握手中的服务器证书交换（如果流量已加密）后发生。如果第一批数据包中的其中之一与包含应用条件的访问控制规则中的所有其他条件匹配，但是识别未完成，则访问控制策略允许数据包通过。此行为允许建立连接，以便可以识别应用。为方便起见，受影响规则以信息图标 ( ) 标记。

允许的数据包通过访问控制策略的*默认*入侵策略（既不是*默认操作*入侵策略也不是近乎匹配规则的入侵策略）进行检查。有关详细信息，请参阅第 25-1 页上的设置用于访问控制的默认入侵策略。

在系统完成其识别后，系统会将访问控制规则操作以及任何关联入侵策略与文件策略应用于与其应用条件匹配的剩余会话流量。

处理加密流量

系统可以识别和过滤通过使用 StartTLS（如 SMTPS、POPS、FTPS、TelnetS 和 IMAPS）进行加密的未加密应用流量。此外，它还可以根据 TLS 客户端问询消息中的服务器名称指示或服务器证书主题可分辨名称值来识别某些加密应用。

这些应用标记为 **SSL Protocol**。只能在未加密或已解密的流量中检测到没有此标记的应用。有关在系统将加密流量与访问控制规则相匹配之前使用 SSL 检查功能解密或阻止该流量的信息，请参阅第 19-1 页上的了解流量解密。

处理无负载的应用流量数据包

系统将默认策略操作应用于在识别了应用的连接中没有负载的数据包。

处理推荐流量

要创建用于处理 Web 服务器所推荐的流量 （如广告流量）的规则，请为被推荐应用而非推荐应用添加条件.有关详细信息，请参阅第 45-12 页上的特殊注意事项：被推荐网络应用。

自动启用应用检测器

必须为策略中的每个应用规则条件启用至少一个检测器（请参阅第 46-24 页上的激活和停用检测器）。如果没有为应用启用检测器，则系统自动为该应用启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。

控制使用多种协议的应用流量 (Skype)

系统可以检测多个类型的 Skype 应用流量。构建用于控制 Skype 流量的应用条件时，请从 **Application Filters** 列表中选择 **Skype** 标记，而非选择单独应用。这确保系统可以相同方式检测和控制所有 Skype 流量。有关详细信息，请参阅第 16-3 页上的将流量与应用过滤器相匹配。

阻止 URL

许可证：因功能而异

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：因功能而异

通过访问控制规则的 URL 条件，可以限制网络上用户能够访问的网站。此功能称为 *URL 过滤*。有两种方法可以使用访问控制来指定要阻止（或者反过来，允许）的 URL：

- 通过任意许可证，可以手动指定单独 URL 或 URL 组来实现对网络流量的精细、自定义控制。
- 通过 URL 过滤许可证，还可以根据 URL 的一般分类或*类别*以及风险级别或*信誉*控制对网站的访问。系统在连接日志、入侵事件和应用详细信息中显示此类别和信誉数据。

注 要查看事件中的 URL 类别和信誉信息，必须使用 URL 条件至少创建一个访问控制规则。

当阻止网站时，可以允许用户浏览器的默认行为，也可以显示通用系统提供的页面或自定义页面。您还可以为用户提供机会，通过点击浏览警告页面来绕过网站阻止。

处理加密网络流量

如果配置 SSL 检查（请参阅第 19-1 页上的了解流量解密）来解密加密流量，则访问控制规则会评估解密流量，如同其未加密一样。但是，如果 SSL 检查配置允许加密连接在未解密的情况下通过，或者如果不配置 SSL 检查，则访问控制规则会评估加密流量。

使用具有 URL 条件的访问控制规则评估网络流量时，系统根据用于将流量加密的公钥证书中的主题公用名来匹配 HTTPS 流量。此外，系统还会忽略主题公用名中的子域，因此在手动过滤 HTTPS URL 时请勿包含子域信息。例如，使用 `example.com` 而不是 `www.example.com`。

此外，系统还会忽略加密协议（HTTP 和 HTTPS）。对于手动 URL 条件和基于信誉的 URL 条件均会发生此情况。换句话说，访问控制规则以相同方式处理发送到以下网站的流量：

- http://example.com/
- https://example.com/

要配置仅匹配 HTTP 或 HTTPS 流量的访问控制规则，请向规则中添加应用条件。例如，可以通过构造两个访问控制规则（每个规则具有应用和 URL 条件）来允许对某个站点进行 HTTP 访问，同时禁止 HTTP 访问。

第一个规则允许 HTTPS 流量到达网站：

```
Action: Allow
Application: HTTPS
URL: example.com
```

第二个规则阻止对同一网站进行 HTTP 访问：

```
Action: Block
Application: HTTP
URL: example.com
```

注 默认情况下，系统一检测到要将会话加密的意图便会禁用加密负载的入侵和文件检查。这在加密连接与配置有入侵和文件检查的访问控制规则相匹配时有助于减少误报和提高性能。有关详细信息，请参阅第 27-60 页上的使用 SSL 预处理器。

虽然可以使用具有任意许可证的非 2 系列设备手动阻止 URL，但是基于类别和信誉的 URL 过滤需要 URL 过滤许可证，并且在 DC500 上不受支持。

表 16-2　URL 过滤的许可证和型号要求

要求	基于类别和信誉	手动
许可证一致	URL 过滤	任何环境
设备	任何设备，除了 2 系列	任何设备，除了 2 系列
防御中心s	除 DC500 外的所有型号	任何环境

有关详情，请参阅：

- 第 16-8 页上的执行基于信誉的 URL 阻止
- 第 16-10 页上的执行手动 URL 阻止
- 第 16-12 页上的对 URL 检测和阻止的限制
- 第 16-13 页上的允许用户绕过 URL 阻止
- 第 16-15 页上的显示被阻止 URL 的自定义网页

执行基于信誉的 URL 阻止

许可证：URL 过滤

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

通过 URL 过滤许可证，可以根据所请求的 URL 的类别和信誉（FireSIGHT 系统从思科云获取）控制用户对网站的访问：

- URL *类别*是 URL 一般分类。例如， ebay.com 属于 **Auctions** 类别，而 monster.com 属于 **Job Search** 类别。 URL 可以属于多个类别。
- URL *信誉*代表可能出于违背组织的安全策略而使用 URL 的可能性。 URL 的风险范围可从 **High Risk** （1 级）到 **Well known** （5 级）。

注 **必须**先启用与思科云的通信，然后具有基于类别和信誉的 URL 条件的访问控制规则才会生效。这允许 防御中心检索 URL 数据。有关详细信息，请参阅第 64-25 页上的启用云通信。

基于信誉的 URL 阻止的优点

通过 URL 类别和信誉，可以快速创建访问控制规则的 URL 条件。例如，可以创建用于识别和阻止 **Abused Drugs** 类别中所有 **High Risk** URL 的访问控制规则。如果用户尝试浏览至具有该类别和信誉组合的任何 URL，则会阻止会话。

使用思科云中的类别和信誉数据还会简化策略创建和管理。它保证系统将按预期控制网络流量。最后，由于云使用新 URL 以及现有 URL 的新的类别和风险连续更新，因此可以确保系统使用最新信息来过滤所请求的 URL。代表安全威胁，例如恶意软件、垃圾邮件、僵尸网络和网络钓鱼，的恶意网站出现和消失的速度可能比您更新和应用新策略的速度要快。

下面提供了一些示例：

- 如果规则阻止所有游戏站点，当新的域名注册并分类为 **Gaming** 时，系统可以自动阻止这些站点。
- 如果规则阻止所有恶意软件站点，并且博客页面受到恶意软件感染，则云可以将 URL 从 **Blog** 重新分类为 **Malware**，这样系统即可阻止该站点。
- 如果规则阻止高风险的社交网站，并且某人在其包含指向恶意负载的链接的简档页面发布链接，则云可以将该页面的信誉从 **Benign sites** 更改为 **High Risk**，这样系统即可将阻止该网站。

请注意，如果云不知道 URL 的类别或信誉，或者，如果 防御中心无法联系云，则该 URL **不会**触发具有基于类别和信誉的 URL 条件的访问控制规则。在这种情况下，您将无法手动对该 URL 指定类别或信誉。

构建 URL 条件

下图显示阻止以下内容的访问控制规则的 URL 条件：所有恶意软件站点、所有高风险站点和所有非良性社交网站。它还会阻止 URL 对象表示的单个站点 example.com。

在单个 URL 条件中，可以向 **Selected URLs** 添加最多 50 项以进行匹配。每个 URL 类别（或者按信誉进行限定）计为一项。请注意，也可以在 URL 条件中使用文本 URL 和 URL 对象，但是不能使用信誉来限定这些项。有关详细信息，请参阅第 16-10 页上的执行手动 URL 阻止。

下表总结如何构建以上显示的条件。请注意，不能使用信誉来限定文本 URL 或 URL 对象。

表 16-3　　示例：构建 URL 条件

要阻止...	请选择以下类别或 URL 对象...	和此信誉...
恶意软件站点（无论信誉如何）	Malware Sites	Any
具有高风险（1 级）的任何 URL	Any	1 - High Risk
风险大于良性（1 至 3 级）的社交站点	Social Network	3 - Benign sites with security risks
example.com	名为 example.com 的 URL 对象	无

构建 URL 条件时，警告图标指示无效配置。有关详细信息，请将指针悬停在图标上方并参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

要使用类别和信誉数据按所请求的 URL 控制流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在面向要按 URL 控制流量的设备的访问控制策略中，创建新访问控制规则或编辑现有规则。

有关详细说明，请参阅第 14-2 页上的创建和编辑访问控制规则。

步骤 2　在规则编辑器中，选择 URLs 选项卡。

系统将显示 URLs 选项卡。

步骤 3　从 **Categories and URLs** 列表中查找并选择要添加的 URL 的类别。要匹配网络流量（无论类别如何），请选择 **Any** 类别。

要搜索将添加的类别，请点击 **Categories and URLs** 列表上方的 **Search by name or value** 提示，然后键入类别名称。列表会在您键入内容时进行更新，以显示匹配类别。

要选择类别，请点击该类别。要选择多个类别，请使用 Shift 和 Ctrl 键。

提示　虽然可以右键单击并**选择所有**类别，但是以此方式添加所有类别会超过 SSL 规则的最大值限制（50 项）。请改用 **Any**。

步骤 4　或者，也可以通过点击 **Reputations** 列表中的信誉级别来限定类别选择。如果不指定信誉级别，则系统默认为 **Any**，表示所有级别。

只能选择一个信誉级别。选择信誉级别时，访问控制规则根据其用途而表现不同行为：

- 如果规则阻止或监控 Web 访问（规则操作为 **Block**、**Block with reset**、**Interactive Block**、**Interactive Block with reset** 或 **Monitor**），则选择信誉级别还将选择严重性高于该级别的所有信誉。例如，如果将规则配置为阻止或监控 **Suspicious sites**（2 级），则系统还会自动阻止或监控 **High Risk**（1 级）站点。
- 如果规则根据信任还是进一步检查流量（规则操作为 **Allow** 或 **Trust**）来允许 Web 访问，则选择信誉级别还将选择严重性低于该级别的所有信誉。例如，如果您将规则配置为允许 **Benign sites**（第 4 级），系统还会自动允许 **Well known**（第 5 级）站点。

如果更改规则的规则操作，系统根据上述几点自动更改 URL 条件中的信誉级别。

步骤 5　点击 **Add to Rule** 或拖放所选项以将其添加到 **Selected URLs** 列表。

步骤 6　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

执行手动 URL 阻止

许可证：任何环境

受支持的设备：任何防御中心，除了 2 系列

要按类别和信誉补充或选择性覆盖 URL 过滤，可以通过手动指定单独 URL 或 URL 组来控制网络流量。借此可以实现对允许和阻止的网络流量的精细、自定义控制。您也可以在没有特殊许可证的情况下执行此类型的 URL 过滤。

要在访问控制规则中手动指定将允许或阻止的 URL，可以键入单个文本 URL。或者，可以使用 URL 对象配置 URL 条件，这些条件可重用，并会将名称与 URL 或 IP 地址关联。

提示 创建 URL 对象后，不仅可以将其用于构建访问控制规则，还可以在系统 Web 接口中的各种其他位置表示 URL。可以使用对象管理器创建这些对象，也可以在配置访问控制规则时动态创建 URL 对象。有关详细信息，请参阅第 3-12 页上的使用 URL 对象。

在 URL 条件中手动指定 URL

虽然手动输入可以提供对允许或阻止的网络流量的精确控制，但是不能使用信誉来限定手动指定的 URL。此外，还必须确保规则不会产生意外结果。要确定网络流量是否与 URL 条件相匹配，系统执行简单的子字符串匹配。如果 URL 对象或手动键入的 URL 的值与受监控主机所请求的 URL 的任何部分相匹配，则符合访问控制规则的 URL 条件。

因此，当在 URL 条件中（包括在 URL 对象中）手动指定 URL 时，请仔细考虑可能受影响的其他流量。例如，如果您允许到 example.com 的所有流量，用户可以浏览的 URL 将包括：

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

又例如，请考虑要明确阻止 ign.com（游戏站点）的场景。但是，子字符串匹配意味着阻止 *ign.com* 也会阻止 veris*ign.com*，这可能并非您的意愿。

手动阻止加密网络流量

请注意，当 SSL 检查配置允许加密流量通过时，或者如果没有配置 SSL 检查，则访问控制规则会处理加密流量；请参阅第 19-1 页上的了解流量解密。访问控制规则中的 URL 条件：

- 忽略网络流量的加密协议（HTTP 与 HTTPS）

  例如，访问控制规则以相同方式处理发送到 http://example.com/ 的流量和发送到 https://example.com/ 的流量。要配置仅匹配 HTTP 或 HTTPS 流量的访问控制规则，请向规则中添加应用条件。有关详细信息，请参阅第 16-7 页上的阻止 URL。

- 根据用于加密流量的公钥证书中的主题公用名与 HTTPS 流量匹配，此外忽略主题公用名中的子域

  手动过滤 HTTPS 流量时，请勿包含子域信息。

构建 URL 条件时，警告图标指示无效配置。有关详细信息，请将指针悬停在图标上方并参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

要通过手动指定将允许或阻止的 URL 来控制网络流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1 在面向要按 URL 控制流量的设备的访问控制策略中，创建新访问控制规则或编辑现有规则。

有关详细说明，请参阅第 14-2 页上的创建和编辑访问控制规则。

步骤 2 在规则编辑器中，选择 URLs 选项卡。

系统将显示 URLs 选项卡。

步骤 3 从 **Categories and URLs** 列表中查找并选择要添加的 URL 对象和组。

- 要动态添加 URL 对象（之后可以添加到条件中），请点击 **Categories and URLs** 列表上方的添加图标 ( )；请参阅第 3-12 页上的使用 URL 对象。

- 要搜索将添加的 URL 对象和组，请点击 **Categories and URLs** 列表上方的 **Search by name or value** 提示，然后键入对象的名称或者对象中 URL 或 IP 地址的值。列表会在您键入内容时进行更新，以显示匹配对象。

要选择对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键。虽然可以右键单击并**选择所有** URL 对象和类别，但是以此方式添加 URL 会超过访问控制规则的最大值 （50 项）。

步骤 4　点击 **Add to Rule** 以将选定项添加到 **Selected URLs** 列表中。

您也可以拖放选定项。

步骤 5　添加要手动指定的所有文本 URL。**不能**在此字段中使用通配符 (*)。

点击 **Selected URLs** 列表下方的 **Enter URL** 提示；然后键入 URL 或 IP 地址并点击 **Add**。

步骤 6　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

对 URL 检测和阻止的限制

许可证：任何环境

受支持的设备：任何防御中心，除了 2 系列

执行 URL 检测和阻止时，请谨记以下要点。

URL 识别的速度

系统在以前情况之前无法过滤 URL：

- 在客户端和服务器之间建立受监控连接
- 系统识别会话中的 HTTP 或 HTTPS 应用
- 系统识别所请求的 URL（面向加密会话，来自客户端问询消息或服务器证书）

此识别应在 3 到 5 个数据包内发生，或者在 SSL 握手中的服务器证书交换（如果流量已加密）后发生。如果第一批数据包中的其中之一与包含 URL 条件的访问控制规则中的所有其他条件匹配，但是识别未完成，则访问控制规则允许数据包通过。此行为允许建立连接，以便可以识别 URL。为方便起见，受影响规则以信息图标 ( ) 标记。

允许的数据包通过访问控制策略的*默认*入侵策略（既不是*默认操作*入侵策略也不是近乎匹配规则的入侵策略）进行检查。有关详细信息，请参阅第 25-1 页上的设置用于访问控制的默认入侵策略。

在系统完成其识别后，系统会将访问控制规则操作以及任何关联入侵与文件策略应用于与其 URL 条件匹配的剩余会话流量。

处理加密网络流量

在使用具有 URL 条件的访问控制规则评估加密网络流量时，系统：

- 忽略加密协议；如果访问控制规则具有 URL 条件但不具有指定该协议的应用条件，则该规则与 HTTPS 和 HTTP 流量均匹配
- 根据用于加密流量的公钥证书中的主题公用名与 HTTPS 流量匹配，并且忽略主题公用名中的子域
- 不显示 HTTP 响应页面，即使已配置该页面也如此

HTTP 响应页面

当网络流量在以下情况下时，不会显示 HTTP 响应页面：

- 会话现在或曾经加密
- 因访问控制规则提升而受 3 系列 设备阻止
- 如果系统直至连接已建立并允许传递若干数据包后才能识别连接中的所请求 URL，如上所述

有关详细信息，请参阅第 16-15 页上的显示被阻止 URL 的自定义网页。

在 URL 中搜索查询参数

系统不使用 URL 中的搜索查询参数来匹配 URL 条件。例如，考虑这样一个场景：您阻止所有购物流量。在这种情况下，使用网络搜索来搜索 amazon.com 不会被阻止，但是，浏览 amazon.com 则会被阻止。

允许用户绕过 URL 阻止

许可证：任何环境

受支持的设备：任何防御中心，除了 2 系列

使用访问控制规则阻止用户的 HTTP Web 请求时，将规则操作设置为 **Interactive Block** 或 **Interactive Block with reset** 可为该用户提供机会，通过点击浏览警告 *HTTP 响应页面*来绕过阻止。可以显示通用系统提供的响应页面，也可以输入自定义 HTML。

默认情况下，系统允许用户绕过阻止 10 分钟（600 秒），而在后续访问时不显示警告页面。可以将持续时间设置为长达一年，也可以强制用户每次都绕过阻止。

如果用户不绕过阻止，则会拒绝匹配流量而不进一步检查；您还可以重置连接。另一方面，如果用户绕过阻止，则系统允许流量。允许此流量意味着可以继续检查未加密负载来查找入侵、恶意软件和禁止文件以及发现数据。请注意，用户在绕过阻止后可能必须刷新才能加载未加载的页面元素。

请注意，将交互式 HTTP 响应页面与为 Block 规则配置的响应页面分开进行配置。例如，可以向在无交互情况下其会话被阻止的用户显示系统提供的页面，但是向可以点击以继续操作的用户显示自定义页面。有关详细信息，请参阅第 16-15 页上的显示被阻止 URL 的自定义网页。

请注意，在以下情况下，即使会话与 Interactive Block 规则相匹配，也不会显示响应页面，并且会阻止流量而不交互：

- 如果会话曾经或现在处于加密状态；这包括系统解密的会话
- 在已建立连接并允许其传递若干数据包，从而系统可以其包含的所请求 URL 和应用详细信息之后；请参阅第 12-18 页上的对访问控制策略和规则进行故障排除

提示 要在访问控制策略中快速禁用对所有规则的交互式阻止，请既不要显示系统提供的页面，也不要显示自定义页面。这会导致系统在无交互情况下阻止与 Interactive Block 规则匹配的所有连接。

要允许用户绕过网站阻止，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1 创建将网络流量与 URL 条件匹配的访问控制规则。

请参阅第 16-8 页上的执行基于信誉的 URL 阻止和第 16-10 页上的执行手动 URL 阻止。

步骤 2 确保访问控制规则操作为 **Interactive Block** 或 **Interactive Block with reset**。

请参阅第 14-6 页上的使用规则操作确定流量处理和检查。

步骤 3 假设用户将绕过阻止并相应地选择规则的检查和日志记录选项。与 Allow 规则一样：

- 可以将任一类型的 Interactive Block 规则与文件和入侵策略关联。系统也可以使用发现来检查此用户允许的流量。有关详细信息，请参阅第 18-1 页上的使用入侵和文件策略控制流量。
- 以交互方式阻止的流量的日志记录选项与允许流量的日志记录选项相同，但请记住，如果用户不绕过交互阻止，系统仅会记录连接开始事件。

  请注意，在系统最初警告用户时，它会使用 Interactive Block 或 Interactive Block with reset 操作标记任何已记录的连接开始事件。如果用户绕过阻止，则为会话记录的其他连接事件具有 Allow 操作。有关详细信息，请参阅第 38-13 页上的根据访问控制处理记录连接。

步骤 4　或者，设置用户绕过阻止后且系统再次显示警告页面前所耗用的时间量。

请参阅第 16-14 页上的为被阻止网站设置用户旁路超时。

步骤 5　或者，创建并使用要显示的自定义页面来允许用户绕过阻止。

请参阅第 16-15 页上的显示被阻止 URL 的自定义网页。

为被阻止网站设置用户旁路超时

许可证：任何环境

默认情况下，系统允许用户绕过交互式阻止 10 分钟（600 秒），而在后续访问时不显示警告页面。可以将持续时间设置为长达一年，或者设置为零以强制用户每次都绕过阻止。此设置适用于策略中的每条 Interactive Block 规则。不能每条规则都设置限制。

要定制用户旁路到期之前的时间长度，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

屏幕上将会显示访问控制策略的高级设置。

步骤 4　点击 General Settings 旁边的编辑图标 ( )。

系统将显示 General Settings 弹出窗口。

步骤 5　在 **Allow an Interactive Block to bypass blocking for (seconds)** 字段中，键入用户旁路到期之前必须经过的秒数。

可以指定从零到 31536000（一年）的任意秒数。指定零会强制用户每次都绕过阻止。

步骤 6　点击 **OK**。

屏幕上将会显示访问控制策略的高级设置。

步骤 7　点击 **Save**。

必须应用访问控制策略，使更改生效。有关详细信息，请参阅第 12-13 页上的应用访问控制策略。

显示被阻止 URL 的自定义网页

许可证：任何环境

受支持的设备：任何防御中心，除了 2 系列

当系统阻止用户的 HTTP Web 请求时，该用户在浏览器中看到的内容取决于如何使用访问控制规则的操作来阻止会话。您应该选择：

- **Block** 或 **Block with reset** 以拒绝连接。被阻止的会话将会超时；采用了“阻止并重置”配置的连接会被系统重置。然而，对于两种阻止操作，都可以使用说明连接已被拒绝的自定义页面来替代默认的浏览器或服务器页面。系统将此自定义页面称为 *HTTP response page*。
- **Interactive Block** 或 **Interactive Block with reset**（如果要显示*交互式 HTTP 响应页面*来警告页面，但又允许其点击按钮以继续操作或者刷新页面以加载最初请求的站点）。在跳过响应页面后，用户可能必需进行刷新，才能加载未加载的页面元素。

可以显示通用系统提供的响应页面，也可以输入自定义 HTML。当输入自定义文本时，计数器将会显示已使用的字符的数量。

在每个访问控制策略中，您将交互式 HTTP 响应页面与用于在无交互情况下阻止流量（也就是说，使用 Block 规则）的响应页面分开配置。例如，可以向在无交互情况下其会话被阻止的用户显示系统提供的页面，但是向可以点击以继续操作的用户显示自定义页面。

HTTP 响应页面向用户的可靠显示取决于页面的网络配置、流量负载和大小。如果构建自定义响应页面，请记住，较小的页面更可能成功显示。

请注意，当网络流量被阻止时，将不会显示响应页面：

- 通过安全情报黑名单
- 并且会话原先已加密；这包括 SSL 检查功能阻止的加密连接，以及与 Block 或 Interactive Block 访问控制规则匹配的解密和加密流量
- 因访问控制规则提升而受 3 系列设备阻止；请参阅第 14-10 页上的借助 3 系列设备信任或阻止流量的限制
- 在已建立连接并允许其传递若干数据包，从而系统可以其包含的所请求 URL 和应用详细信息之后；请参阅第 12-18 页上的对访问控制策略和规则进行故障排除

要配置 HTTP 响应页面，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　编辑以监控网络流量的设备为目标的访问控制策略。

有关详细信息，请参阅第 12-10 页上的编辑访问控制策略。

步骤 2　选择 HTTP Responses 选项卡。

屏幕上将会显示访问控制策略的 HTTP 响应页面设置。

步骤 3　对于 **Block Response Page** 和 **Interactive Block Response Page**，从下拉列表选择响应。对于每个页面，有以下选项可供选择：

- 要使用通用响应，请选择 **System-provided**。可以点击视图图标 ()，以便查看该页面的 HTML 代码。
- 如要创建自定义响应，选择 **Custom**。

  系统将显示一个弹出窗口，其中预先填充有系统提供的可以替换或修改的代码。完成时，保存更改。请注意，可以通过点击编辑图标 () 来编辑自定义页面。

- 如要禁止系统显示 HTTP 响应页面，可以选择 **None**。请注意，为交互阻止的会话选择此选项可防止用户点击以继续操作；系统会在无交互的情况下阻止会话。

步骤 4　点击 **Save**。

必须应用访问控制策略，使更改生效。有关详细信息，请参阅第 12-13 页上的应用访问控制策略。

按照用户控制流量

*访问控制策略*中的*访问控制规则*对网络流量日志记录和处理进行精细控制。访问控制规则的用户条件可供您执行*用户控制* - 通过根据登录主机的 LDAP 用户限制流量来管理哪些流量可以穿越网络。

用户控制通过将*访问受控的用户*与 IP 地址相关联来实现。部署的代理监控指定用户登录和注销主机或因其他原因用 Active Directory 凭证进行身份验证。例如，贵组织可能使用依赖于 Active Directory 进行集中身份验证的服务或应用。。

要使流量与具有用户条件的访问控制规则相匹配，必须将受监控会话中的源或目标主机的 IP 地址与登录的访问受控的用户相关联。您可以根据单个用户或这些用户所属的组来控制流量。

您可以将用户条件相互组合及与其他类型的条件组合来创建访问控制规则。这些访问控制规则可能很简单，也可能很复杂，使用多个条件匹配和检查流量。有关访问控制规则的详细信息，请参阅第 14-1 页上的使用访问控制规则调整流量。

注 基于硬件的快速路径规则、基于安全情报的流量过滤以及一些解码和预处理在访问控制规则评估网络流量**之前**发生。您还可以配置 *SSL 检查*功能在访问控制规则对已加密的流量进行评估之前阻止或解密它。

用户控制需要可控性许可证并且仅受 LDAP 用户和组（访问受控用户）支持，使用监控 Microsoft Active Directory 服务器的用户代理报告的登录和注销记录。

但是，只要有 FireSIGHT 许可证，您仍然可以利用*用户感知*，这是用户控制的基础。通过用户感知，您可以查看代理报告的用户活动以及*非访问受控用户*的其他活动，当受管设备检查允许的流量是否存在发现数据时，系统可以检测到这些活动。系统可以识别通过各种协议的登录尝试：AIM、IMAP、LDAP、Oracle、POP3、SIP、FTP、HTTP 和 MDNS。

要为系统报告的用户活动添加情景，您可以查询您的部署中的 LDAP 服务器，不仅可以检索访问受控用户的元数据，而且可以检索一些非访问受控用户的元数据：用户发现检测到的 POP3 和 IMAP 用户以及由用户发现或用户代理检测其活动的 LDAP 用户。

用户感知功能可使所有部署类型确定“谁”在执行“什么操作”。例如，您可以确定：

- 谁正在尝试未授权访问具有高主机重要性的服务器
- 谁正在耗用异常大量的带宽
- 谁尚未应用关键操作系统更新
- 谁正在使用即时消息软件或 P2P 文件共享应用，而这样做是违反公司的 IT 策略的
- 谁拥有作为影响程度为 Vulnerable（级别 1：红色）的入侵事件的目标的主机（需要保护）
- 谁发起了内部攻击或端口扫描（需要保护）

借助这些信息，可以采用有针对性的方法降低风险，以及采取措施防止中断他人的活动。用户控制增强了阻止 LDAP 用户和用户活动的能力。用户感知和控制功能相结合，可显著提高审核控制并提高合规性。有关详细信息，请参阅第 45-3 页上的了解用户数据收集。

下表列出了对用户感知和控制的要求 有关用户代理的最新详细信息，请参阅《*用户代理配置指南*》。

表 17-1　　用户感知和控制要求

要求	用户感知	用户控制
许可证一致	FireSIGHT	可控性
设备	任何环境	任何设备， 2 系列或X -系列除外
防御中心s	任何环境	除 DC500 外的所有型号
用户代理	在运行以下一种系统的 Windows 计算机上安装 2.2 版本的用户代理，其中防御中心和您想要监控的 Microsoft Active Directory 服务器之间可进行往返 TCP/IP 访问。 • Windows Vista、Windows 7 或 Windows 8 • Windows Server 2003、2008 或 2012 您还必须安装 Microsoft .NET Framework V4.0 客户端配置文件和 Microsoft SQL Server Compact (SQL CE) V3.5。	
用于用户元数据检索的 LDAP 服务器	以下项之一，其中可从防御中心进行 TCP/IP 访问： • 在 Windows Server 2003 和 Windows Server 2008 中运行的 Microsoft Active Directory（用户控制需要） • 在 Windows Server 2003 和 Windows Server 2008 上运行的 Oracle Directory Server Enterprise Edition 7.0（仅用于用户感知） • 在 Linux 上运行的 OpenLDAP（仅用于用户感知） 这些服务器支持用户代理的实时监控以及定期轮询，不支持实时监控的 Windows Server 2003 除外。	

有关详情，请参阅：

- 第 17-2 页上的向访问控制规则添加用户条件
- 第 17-4 页上的检索访问受控用户和 LDAP 用户元数据
- 第 17-9 页上的使用用户代理报告 Active Directory 登录情况

向访问控制规则添加用户条件

许可证：可控性

受支持的设备：任何设备， 2 系列或 X -系列除外

受支持的防御中心：除 DC500 外的所有型号

FireSIGHT 系统的用户控制功能通过将访问受控的用户与主机 IP 地址相关联来发挥作用。部署的用户代理监控指定用户用 Microsoft Active Directory 凭证进行身份验证。要使流量将访问控制规则与用户条件进行匹配，受监控会话中的源或目标主机的 IP 地址必须与已登录的受控访问用户关联。

在您可以执行用户控制之前，您必须：

- 在防御中心与 Microsoft Active Directory 服务器之间配置连接；请参阅第 17-4 页上的检索访问受控用户和 LDAP 用户元数据。
- 在 Microsoft Windows 计算机上安装用户代理，其中可对 Active Directory 服务器进行 TCP/IP 访问；请参阅第 17-9 页上的使用用户代理报告 Active Directory 登录情况。

注意事项 如果您配置大量要监控的用户组，或者，如果您有非常多的用户映射到网络中的主机，由于内存限制，系统可能会丢弃基于用户组的用户映射。因此，基于用户组的访问控制规则可能无法如预期那样触发。

在单一用户条件中，最多只能将 50 个用户和组添加到 **Selected Users**。带有用户组的条件与该组任何成员（包括任何子组的成员，个别排除的用户和排除的子组的成员除外）的往返流量相匹配。

注 系统必须在该组中检测到至少一个用户的活动，然后您才能使用组条件执行用户控制。此初始连接**不是**由与其匹配的访问控制规则进行处理，而是由与其匹配的下一个规则或访问控制策略默认操作进行处理。

构建用户条件时，警告图标表示无效配置。有关详细信息，请将鼠标悬停在图标上方并参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

要控制用户流量：

访问：管理员/访问管理员/网络管理员

步骤 1 在针对您要通过 LDAP 用户或组控制流量所在设备的访问控制策略中，新建访问控制规则或编辑现有规则。

有关详细说明，请参阅第 14-2 页上的创建和编辑访问控制规则。

步骤 2 在规则编辑器中，选择 Users 选项卡。

系统将显示 Users 选项卡。

步骤 3 查找并选择您要从 **Available Users** 列表中添加的用户和组。

用户和组用不同图标标记。要搜索需要添加的用户和组，请点击 **Available Users** 列表上方的 **Search by name or value** 提示，然后键入用户或组的名称。列表会在您键入内容时进行更新，以显示匹配项。

要选择一项，请点击该项。要选择多项，请使用 Shift 和 Ctrl 键，或右键单击并选择 **Select All**。

步骤 4 点击 **Add to Rule**，将选定的用户和组添加到 **Selected Users** 列表。

您也可以拖放选定的用户和组。

步骤 5 保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

检索访问受控用户和 LDAP 用户元数据

许可证：FireSIGHT或可控性

受支持的设备：因功能而异

受支持的防御中心：因功能而异

如果要执行用户控制（即，编写包含用户条件的访问控制规则），必须配置 防御中心与贵组织的至少一个 Microsoft Active Directory 服务器之间的连接。防御中心定期和自动查询 LDAP 服务器以更新访问受控用户的元数据，访问受控用户指您要通过用户代理监控其活动的以及您在限制流量时可以用作条件的用户和组。防御中心还可以检索用户代理已报告其活动的非访问受控用户的元数据。或者，可执行按需查询。

如果您未在执行用户控制，则可以查询其他类型的 LDAP 服务器，以获取用户感知数据 —— 与由用户发现检测其活动而不是由用户代理报告其活动的 POP3 和 IMAP 用户以及 LDAP 用户的相关联的元数据。系统使用 POP3 和 IMAP 登录中的邮件地址与 Active Directory、OpenLDAP 或 Oracle Directory Server Enterprise Edition 服务器上的 LDAP 用户相关联。在这种情况下，防御中心定期查询 LDAP 服务器，获取上一次查询之后系统检测到其活动的用户的新的和更新的元数据。

有关详情，请参阅：

- 第 17-4 页上的连接 LDAP 服务器以实现用户感知和控制
- 第 17-8 页上的按需更新用户控制参数
- 第 17-8 页上的暂停与 LDAP 服务器的通信

连接 LDAP 服务器以实现用户感知和控制

许可证：FireSIGHT或可控性

受支持的设备：因功能而异

受支持的防御中心：因功能而异

防御中心与贵组织的 LDAP 服务器之间的连接可以：

- 指定要通过用户代理监控其活动以及您在使用访问控制规则限制流量时可用作条件的访问受控用户和组。
- 可供您查询服务器上有关访问受控用户和一些非访问受控用户的元数据：通过用户发现检测到的 POP3 和 IMAP 用户，以及通过用户发现或用户代理检测到其活动的 LDAP 用户。

这些连接或*用户感知对象*，为 LDAP 服务器指定连接设置和身份验证过滤器设置。它们类似于您配置用于管理 FireSIGHT 系统网络界面的外部身份验证的身份验证对象；请参阅第 61-5 页上的管理身份验证对象。

要执行用户控制，您**必须**连接到 Microsoft Active Directory LDAP 服务器。如果您只是希望检索 LDAP 用户元数据，则系统支持连接其他类型的 LDAP 服务器；请参阅第 17-2 页上的表 17-1。

当系统检测到用户活动时，系统会向防御中心用户数据库，也称为用户身份数据库，添加该用户的记录。防御中心定期查询 LDAP 服务器，获取自上次查询之后检测到其活动的新的和更新的用户的元数据。对于已存在于数据库中的用户，如果其元数据在过去 12 小时里未更新，则系统会为其更新元数据。系统检测到新用户登录后，防御中心更新用户元数据可能需要几分钟时间。

系统使用 POP3 和 IMAP 登录中的邮件地址与 LDAP 服务器上的用户关联。例如，如果受管设备检测到某个用户使用与某个 LDAP 用户相同的邮件地址登录 POP3，则系统会将 LDAP 用户的元数据与该用户关联。

注　即使您从 LDAP 服务器移除系统检测到的用户，防御中心也**不会**从其用户数据库中移除这些用户；您必须手动删除。但是，在防御中心下一次更新访问受控用户列表时， LDAP 更改**会**反映在访问控制规则中。

下表列出了可与受监控用户关联的 LDAP 元数据。请注意，要成功从 LDAP 服务器检索用户元数据，服务器**必须**使用表中列出的 LDAP 字段名称。如果在 LDAP 服务器上重命名该字段，防御中心将无法使用该字段中的信息来填充其数据库。

表 17-2　将 LDAP 字段映射到思科字段

元数据	防御中心	Active Directory	Oracle Directory Server	OpenLDAP
LDAP 用户名	用户名	samaccountname	cn uid	cn uid
first name	名字	givenname	givenname	givenname
last name	姓氏	sn	sn	sn
email address	电子邮件	邮件 userprincipalname（如果 mail 没有值）	邮件	邮件
department	部门	department distinguishedname（如果 department 没有值）	department	ou
电话号码	电话	telephonenumber	不适用	telephonenumber

请与您的 LDAP 管理员密切合作，确保 LDAP 服务器配置正确并且您可以连接这些服务器并获取在创建 LDAP 连接时必须提供的信息。

服务器类型、 IP 地址和端口

必须指定服务器类型、IP 地址或主机名以及用于主 LDAP 服务器的端口（如有需要，还可以指定用于备份 LDAP 服务器的端口）。要执行用户控制，您**必须**使用 Microsoft Active Directory 服务器。

LDAP 特定参数

在防御中心搜索 LDAP 服务器以检索身份验证服务器上的用户信息时，其需要该搜索的起点。可以通过提供基本识别名称（或*基础 DN*）来指定要搜索的*命名空间*或目录树。通常，基础 DN 具有指示公司领域和运营单位的基础结构。例如，Example 公司的 Security 部门的基础 DN 可能为 `ou=security,dc=example,dc=com`。请注意，识别主服务器之后，可以从该服务器自动检索可用基础 DN 列表并选择相应的基础 DN。

必须为对于您要检索的用户信息具有适当权限的用户提供用户凭证。请记住，您指定的用户识别名称对于目录服务器的目录信息树必须是唯一的。

还可以为 LDAP 连接指定加密方法。请注意，如果使用证书进行身份验证，证书中 LDAP 服务器的名称**必须**与在防御中心网络界面中指定的主机名相匹配。例如，如果在配置 LDAP 连接时使用 `10.10.10.250`，而不是证书中的 `computer1.example.com`，连接将会失败。

最后，必须指定超时持续时间，超过该时间后，尝试联系无响应 LDAP 服务器的行为将会回滚为备份连接。

用户和组访问控制参数

要执行用户控制，请指定要在访问控制规则中用作条件的组。

包含某个组即会自动包含该组的所有成员（包括任何子组的成员）。但是，如果要在访问控制规则中使用子组，必须明确包含要使用的子组。还可排除组和单个用户。排除某个组将会排除该组的所有成员，即使用户是包含的组的成员。

可在访问控制中使用的最大用户数取决于 FireSIGHT 许可证。选择要包含的用户和组时，请确保用户总数小于 FireSIGHT 用户许可证数量。如果访问控制参数范围太宽泛，防御中心会尽可能获取有关更多用户的信息，并报告无法在任务队列中检索的用户数。

注　如果没有指定要包含的任何组，系统将会检索与您提供的 LDAP 参数匹配的所有组的用户数据。出于性能方面的考虑，思科建议您仅明确包含代表要在访问控制中使用的用户的组。请注意，**不能**包含用户或域用户组。

还必须指定防御中心查询 LDAP 服务器以获取要在访问控制中使用的新用户的频率。

在创建 LDAP 连接后，点击删除图标 ( ) 并确认选择，即可将其删除。要修改 LDAP 连接，请点击编辑图标 ( )。启用连接后，防御中心下一次查询 LDAP 服务器时您所保存的更改会生效。

要为用户感知和用户控制创建 LDAP 连接，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Users**。

系统将显示 Users Policy 页面。

步骤 2　点击 **Add LDAP Connection**。

系统将显示 Create User Awareness Authentication Object 页面。

步骤 3　在 **Name** 和 **Description** 字段中为对象键入名称和描述。

步骤 4　从 **Server Type** 中选择 LDAP 服务器类型。

如果需要执行用户控制，**必须**使用 Microsoft Active Directory 服务器。

注　代理无法向防御中心发送以 $ 字符结尾的 Active Directory 用户名。如果您要监控这些用户，则必须移除最后的 $ 字符。

步骤 5　**IP Address** 或 **Host Name** 中为主 LDAP 服务器指定 IP 地址或主机名（如有需要，也可以为备份 LDAP 服务器指定这两项）。

步骤 6　在 **Port** 中指定 LDAP 服务器用于身份验证流量的端口。

步骤 7　在 **Base DN** 中为要访问的 LDAP 目录指定基础 DN。

例如，要对示例公司的安全组织中的名称进行身份验证，请键入 `ou=security,dc=example,dc=com`。

提示　要获取完整的可用域列表，请点击 **Fetch DNs**，并从下拉列表中选择相应的基本识别名称。

步骤 8　在 **User Name** 和 **Password** 字段中指定要用于验证 LDAP 目录的访问权限的识别用户名和密码。确认密码。

例如，如果您在连接到某个 OpenLDAP 服务器，该服务器上的用户对象属性为 `uid`，且示例公司安全部门的管理员对象的 `NetworkAdmin` 的值为 `uid`，请键入 `uid=NetworkAdmin,ou=security,dc=example,dc=com`。

步骤 9　在 **Encryption** 中选择加密方法。如果使用加密，可以在 **SSL Certificate** 中添加 SSL 证书。

证书中的主机名**必须**与在第 5 步中指定的 LDAP 服务器的主机名相匹配。

步骤 10　在 **Timeout** 中指定超时持续时间（以秒为单位），超过该时间后，尝试联系无响应 LDAP 服务器的行为将会回滚为备份连接。

步骤 11　或者，在指定对象的用户感知设置之前，点击 **Test** 测试连接。

步骤 12　您有两种选择，具体取决于在第 4 步中选择的 LDAP 服务器的类型。

- 如果要连接到 Active Directory 服务器，可启用 **User/Group Access Control Parameters**，以指定要在访问控制中使用的用户。继续执行下一步。
- 如果您在连接任何其他类型的服务器，或者不想执行用户控制，请跳至第 17 步。

步骤 13　点击 **Fetch Groups**，以使用提供的 LDAP 参数填充可用组列表。

步骤 14　通过使用左箭头和右箭头按钮包含和排除组，从而指定要在访问控制中使用的用户。

包含某个组即会自动包含该组的所有成员（包括任何子组的成员）。但是，如果要在访问控制规则中使用子组，必须明确包含要使用的子组。排除某个组将会排除该组的所有成员，即使用户是包含的组的成员。

步骤 15　在 **User Exclusions** 中指定任何特定用户排除。

排除用户可防止您将用户作为条件编写访问控制规则。使用逗号分隔多个用户。还可以在此字段中使用星号 (*) 作为通配符。

步骤 16　指定您想要查询 LDAP 服务器以获取新用户和组信息的频率。

默认情况下，防御中心每天午夜查询一次服务器：

- 使用 **Start At** 下拉列表指定希望查询发生的时间。**0** 代表午夜，**1** 代表凌晨 1 点，等等。
- 使用 **Update Interval** 下拉列表指定查询服务器的频率（以小时为单位）。

步骤 17　点击 **Save**。

如果添加或更改了用户和组访问控制参数，请确认是否要应用所做的更改。对象保存成功，系统再次显示 Users Policy 页面。

步骤 18　点击您刚刚创建的连接旁的滑块，启用该连接。

如果要启用连接并且连接具有用户和组访问控制参数，请选择是否希望立即查询 LDAP 服务器以获取用户和组信息。请注意，如果不立即查询 LDAP 服务器，则会在预定时间发生查询。您可以监控任务队列中任何查询的进度 (**System > Monitoring > Task Status**)。

按需更新用户控制参数

许可证：可控性

受支持的设备：任何设备， 2 系列或 X -系列除外

受支持的防御中心：除 DC500 外的所有型号

如果更改 LDAP 连接中的用户和组访问控制参数，或者如果更改 LDAP 服务器上的用户或组且您想要更改立即可用于用户控制，则可强制防御中心从 Active Directory 服务器执行按需用户数据检索。

防御中心可从服务器检索的最大用户数取决于 FireSIGHT 许可证。如果 LDAP 连接中的访问控制参数范围太宽泛，防御中心会尽可能获取有关更多用户的信息，并报告无法在任务队列中检索的用户数。

要执行按需用户数据检索，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Users**。

系统将显示 Users Policy 页面。

步骤 2　在要用于查询 LDAP 服务器的 LDAP 连接旁边，点击下载图标 ( )。

查询开始。可在任务队列 (**System > Monitoring > Task Status**) 中监控查询进度。

暂停与 LDAP 服务器的通信

许可证：FireSIGHT 或可控性

受支持的设备：因功能而异

受支持的防御中心：因功能而异

只有已启用的 LDAP 连接才允许防御中心查询 LDAP 服务器。要停止查询，可以暂时禁用 LDAP 连接，而无需删除这些连接。

当您重新启用用于访问控制的 LDAP 连接时，可以强制防御中心立即查询服务器获取更新的用户和组信息，或者也可以等到预定的首次查询出现。

要禁用或重新启用 LDAP 连接：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Users**。

系统将显示 Users Policy 页面。

步骤 2　点击您刚刚创建的连接旁的滑块，暂停或重新启用该连接。

如在重新启用连接并且连接具有用户和组访问控制参数，请选择是否想要立即查询 LDAP 服务器以获取用户和组信息。如果不立即查询 LDAP 服务器，查询将会在预定时间发生。您可以监控任务队列中任何查询的进度 (**System > Monitoring > Task Status**)。

使用用户代理报告 Active Directory 登录情况

许可证：FireSIGHT

在 Microsoft Windows 计算机上部署的用户代理可以监控 Microsoft Active Directory 服务器，然后在贵组织的 LDAP 用户登录和注销主机时通知防御中心，或者由于其他原因用 Active Directory 凭证进行身份验证。例如，您的组织可能使用依赖 Active Directory 进行集中身份验证的服务或应用。

代理报告的信息不仅可以用作贵组织中用户活动的记录，而且可以作为用户控制的基础。要使流量与具有用户条件的访问控制规则相匹配，必须将受监控会话中的源或目标主机的 IP 地址与登录的访问受控的用户相关联。您可以根据单个用户或这些用户所属的组来控制流量。

注　如果要执行用户控制，**必须**安装并使用用户代理。但是，用户代理只报告与 Active Directory 身份验证相关的用户活动。通过用户感知，您可以查看代理报告的所有用户活动，以及在受管设备允许的网络流量中检测到的其他活动。系统使用发现功能识别通过各种协议的登录尝试：AIM、IMAP、LDAP、Oracle、POP3、SIP、FTP、HTTP 和 MDNS。有关详细信息，请参阅第 45-3 页上的了解用户数据收集。

要通过用户代理检索 LDAP 用户身份验证记录以进行用户感知或控制，请首先将每个防御中心配置为允许从代理进行连接。在高可用性部署中，请在主要防御中心和辅助防御中心上启用代理通信。用户代理可以一次连接到最多五个防御中心。您在防御中心上启用用户代理通信之后，可以在 Windows 计算机上安装代理；请参阅第 17-2 页上的表 17-1。

最后，请将用户代理配置为从 Microsoft Active Directory 服务器接收数据并将信息报告给防御中心。您也可以将代理配置为从报告中排除特定用户名和 IP 地址，以及将状态消息记录到本地事件日志或 Windows 应用日志中。用户代理状态监控器运行状况模块监控与防御中心连接的代理；请参阅第 68-25 页上的配置用户代理状态监控。

要配置防御中心以连接到用户代理，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Users**。

系统将显示 Users Policy 页面。

步骤 2　单击 **Add User Agent**。

系统将显示 Add User Agent 弹出窗口。

步骤 3　为代理键入一个**名称**。

步骤 4　键入您计划安装代理的计算机的 **主机名或地址**。**必须**使用 IPv4 地址；若使用 IPv6 地址，您将无法配置防御中心连接到用户代理。

步骤 5　单击 **Add User Agent**。

防御中心即可以连接到您所指定的计算机上的用户代理。要删除连接，请点击删除图标 ( ) 并确认您要删除该连接。

步骤 6　在您指定的计算机上安装用户代理。将其配置为从 Microsoft Active Directory 服务器接收数据并将信息报告给防御中心。

有关最新详细信息，请参阅《*用户代理配置指南*》。

使用入侵和文件策略控制流量

入侵策略和文件策略在 FireSIGHT 系统中共同发挥作用，作为允许流量到达其目的地之前的最后一道防线。

- **入侵策略**监管系统的入侵防御功能；请参阅第 23-1 页上的了解网络分析和入侵策略。
- **文件策略**监管系统的基于网络的文件控制和高级恶意软件防护 (AMP) 功能；请参阅第 37-8 页上的了解和创建文件策略。

基于硬件的快速路径、基于安全情报的流量过滤（黑名单）、基于 SSL 检查的决策以及流量解码和预处理均发生在检查网络流量是否存在入侵、受禁文件和恶意软件之前。访问控制规则和访问控制默认操作确定哪些流量由入侵策略和文件策略进行检查。

通过将入侵策略或文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略和/或文件策略检测流量。

注 默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与配置了入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。有关详细信息，请参阅第 19-1 页上的了解流量解密和第 27-60 页上的使用 SSL 预处理器。

入侵防御和 AMP 要求您在自己的访问控制策略目标设备上启用特定许可功能，如下表所述。

表 18-1 入侵和文件检查的许可证和型号要求

功能	说明	许可证	支持的防御中心	支持的设备
入侵防御	检测和（可选）阻止入侵和漏洞	保护	任何环境	任何环境
文件控制	检测和（可选）阻止文件类型传输	保护	任何环境	任何环境
高级恶意软件防护 (AMP)	检测、存储、跟踪和（可选）阻止恶意软件传输 将捕获的文件提交到思科云进行恶意软件分析	恶意软件	除 DC500 外的所有型号	除 2 系列或 X -系列外的所有型号

如果贵组织有订用 FireAMP，则防御中心还可以接收来自思科云的基于终端的恶意软件检测数据。防御中心呈现这些数据以及系统生成的基于网络的任何文件和恶意软件数据。除您的 FireAMP订阅外，导入FireAMP数据无需许可证。有关详细信息，请参阅第 37-21 页上的为 FireAMP 处理云连接。

有关检测流量中是否存在入侵、受禁文件和恶意软件的详细信息，请参阅：

- 第 18-2 页上的检查允许的流量中是否存在入侵和恶意软件
- 第 18-7 页上的调整的入侵防御性能
- 第 18-17 页上的调整文件和恶意软件检查性能和存储

检查允许的流量中是否存在入侵和恶意软件

许可证：保护或恶意软件

受支持的设备：因功能而异

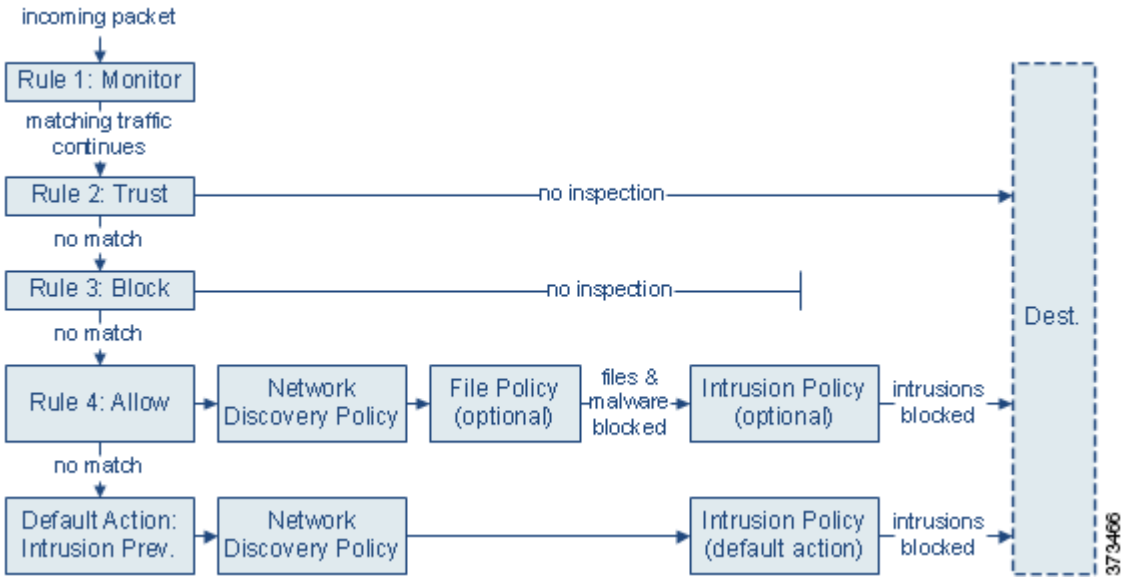
受支持的防御中心：因功能而异

入侵和文件策略监管系统的入侵防御、文件控制和 AMP 功能，是允许流量到达其目的地之前的最后一道防线。基于硬件的快速路径规则、基于安全情报的流量过滤、SSL 检查决策（包括解密）、解码和预处理以及访问控制规则选择均发生在入侵和文件检测**之前**。

访问控制规则为跨多个受管设备处理网络流量提供了精细方法。通过将入侵策略或文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略和/或文件策略检测流量。访问控制规则条件可能很简单，也可能很复杂；您可以通过安全区域、网络或地理位置、 VLAN、端口、应用、请求的 URL 和用户控制流量。

系统按您指定的顺序将流量与访问控制规则相匹配。在大多数情况下，系统会按照其*所有*条件均与流量相匹配的*第一条*访问控制规则处理网络流量。访问控制规则的*操作*确定系统如何处理匹配流量。您可以（不一定需要进一步检测）监控、信任、阻止或允许匹配流量；请参阅第 14-6 页上的使用规则操作确定流量处理和检查。

下图显示一个内联入侵防御和 AMP 部署中的流量，它受包含四种不同类型访问控制规则和默认操作的访问控制策略监管。



在上面的情景中，策略中的前三条访问控制规则 — Monitor、Trust 和 Block — 无法检查匹配的流量。 Monitor 规则跟踪和记录但不检查网络流量，因此，系统继续将流量与其他规则进行匹配以确定是允许还是拒绝该流量。 Trust 和 Block 规则处理匹配流量，无需任何何类型的进一步检查，不匹配的流量继续进入下一条访问控制规则。

策略中的第四个也是最后一条规则（Allow 规则）按照以下顺序调用各种其他策略以检查和处理匹配的流量：

- **发现：网络发现策略 —** 首先，网络发现策略检查流量是否存在发现数据。发现是被动分析，并不影响流量的流动。尽管不显式启用发现，但您可以增强或禁用它。但是，允许流量不会自动保证发现数据收集。系统仅对涉及网络发现策略显式监控的 IP 地址的连接进行发现。有关详细信息，请参阅第 45-1 页上的网络发现简介。
- **高级恶意软件防护和文件控制：文件策略 —** 在流量由发现检查之后，系统检查其中是否存在受禁文件和恶意软件。基于网络的 AMP 检测和阻止（可选）许多类型文件中的的恶意软件，包括 PDF、Microsoft Office 文档和其他文件。如果贵组织不仅要阻止传输恶意软件文件，还要阻止特定类型的所有文件（无论文件是否包含恶意软件），则 *file control* 可供您监控网络流量中特定文件类型的传输，然后阻止或允许文件。
- **入侵防御：入侵策略 —** 在文件检查之后，系统可以检查流量中是否存在入侵和漏洞。入侵策略根据模式检查已解码数据包中是否存在攻击，并且可以阻止或修改恶意流量。入侵策略与*变量集*配对，可供您使用指定值准确反映您的网络环境。
- **目的地 —** 通过上述所有检查的流量将传递到其目的地。

请注意，Interactive Block 规则（未显示在图中）具有与 Allow 规则相同的检查选项。因此，您可以在用户通过点击警告页面绕过已阻止网页时检查流量是否存在恶意内容。有关详细信息，请参阅第 14-8 页上的交互式阻止操作：允许用户绕过网站拦截。

不与策略中任何非监控访问控制规则相匹配的流量由默认操作来处理。在这种情况下，默认操作是入侵防御操作，只要流量由您指定的入侵策略进行传递，它就允许流量到达其最终目的地。在不同部署中，您可能具有信任或阻止所有流量而无需进一步检查的默认操作；请参阅第 12-6 页上的表 12-4。请注意，系统可能检测默认操作允许的流量是否存在发现数据和入侵，而不是检测其是否存在受禁文件或恶意软件。您**无法**将文件策略与访问控制默认操作相关联。

注 有时，当访问控制策略分析某条连接时，系统必须处理该连接中的头几个数据包，**从而让其通过**，然后才能确定哪个访问控制规则（如有）将处理流量。因此，这些数据包不会未经检测就到达其目的地，您可以使用称为默认入侵策略的入侵策略对其进行检测并生成入侵事件。有关详细信息，请参阅第 25-1 页上的设置用于访问控制的默认入侵策略。

有关上述情景的更多信息以及如何将文件和入侵策略与访问控制规则和访问控制默认操作相关联的说明，请参阅：

- 第 18-3 页上的了解文件和入侵检查顺序
- 第 18-5 页上的配置访问控制规则执行 AMP 或文件控制
- 第 18-5 页上的配置访问控制规则以执行入侵防御
- 第 12-6 页上的设置对网络流量的默认处理和检查

了解文件和入侵检查顺序

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

第 18-2 页上的检查允许的流量中是否存在入侵和恶意软件中的情景显示了每种类型的一条访问控制规则，包括同时与文件策略和入侵规则相关联的 Allow 规则。在您的访问控制策略中，您可以将多个 Allow 和 Interactive Block 规则与不同的入侵和文件策略相关联，以使检查配置文件匹配各种流量类型。

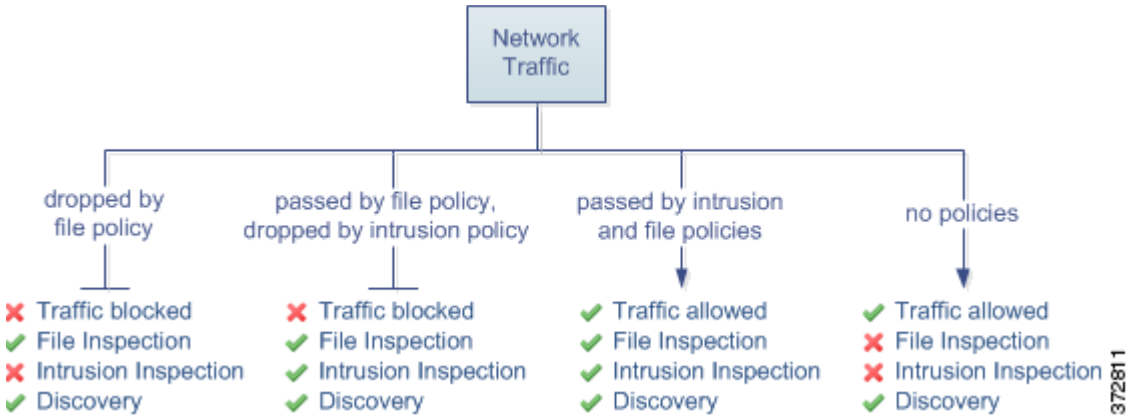
注　可检测 Intrusion Prevention 或 Network Discovery Only 默认操作允许的流量是否存在发现数据和入侵，但不能检测其是否存在受禁文件或恶意软件。您**无法**将文件策略与访问控制默认操作相关联。

您不需要在同一规则中同时执行文件和入侵检查。对于匹配 Allow 或 Interactive Block 规则的连接：

- 若没有文件策略，流量流动由入侵策略决定
- 若没有入侵策略，流量流动由文件策略决定
- 若以上两者都没有，仅由网络发现检查允许的流量

提示　系统不会对受信任的流量执行任何种类的检查。虽然没有使用入侵或文件策略配置 Allow 规则可以放行流量，就像 Trust 规则那样，但 Allow 规则让您可以对匹配的流量执行发现。

下图说明对符合 Allow 或用户绕过的 Interactive Block 访问控制规则的条件的流量执行的检查类型。为简单起见，该图显示入侵策略和/或文件策略与单个访问控制规则关联的情况的流量。



对由访问控制规则处理的任何单条连接，文件检测均发生在入侵检测之前。也就是说，系统不检测文件策略所阻止的文件是否存在入侵。在文件检测中，基于类型的简单阻止优先于恶意软件检测和阻止。

例如，请考虑按照访问控制规则中所定义通常要允许特定网络流量的情况。但是，作为预防措施，您希望阻止下载可执行文件，检查恶意软件的已下载的 PDF 并阻止找到的所有实例，然后对流量执行入侵检查。

您可以使用与自己想要暂时允许通过的流量的特征相匹配的规则创建访问控制策略，然后将其与入侵策略和文件策略相关联。文件策略阻止所有可执行文件的下载，也可检查和阻止包含恶意软件的 PDF：

- 首先，系统根据文件策略中指定的简单类型匹配阻止所有可执行文件的下载。由于这些文件会被立即阻止，因此，其既不接受恶意软件云查找也不接受入侵检测。
- 接着，系统对下载到网络主机的 PDF 执行恶意软件云查找。具有恶意软件文件性质的任何 PDF 均被阻止，且不接受入侵检测。
- 最后，系统使用与访问控制规则关联的入侵策略检查任何剩余流量，包括文件策略未阻止的文件。

注　文件在会话中得以检测和阻止之前，来自该会话的数据包均可能接受入侵检查。

配置访问控制规则执行 AMP 或文件控制

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

访问控制策略可能有多个与文件策略相关联的访问控制规则。您可以为任何 Allow 或 Interactive Block 访问控制规则配置文件检测，这样，您就可在网络中不同类型的流量到达其最终目的地之前，将不同的文件和恶意软件检测配置文件与其匹配。

当系统根据文件策略中的设置检测到受禁文件（包括恶意软件）时，会自动将事件记录到防御中心数据库中。如果您不想记录文件或恶意软件事件，则可按每条访问控制规则禁用此日志记录功能。将文件策略与访问控制规则相关联之后，清除访问控制规则编辑器 Logging 选项卡上的 **Log Files** 复选框。有关详细信息，请参阅第 38-7 页上的为允许的连接禁用文件和恶意软件事件日志记录。

无论调用访问控制规则的日志记录配置如何，系统均会将关联连接的末端记录到防御中心数据库；请参阅第 38-3 页上的与文件和恶意软件事件关联的连接。

要将文件策略与访问控制规则相关联，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要使用访问控制规则配置 AMP 或文件控制所在的访问控制策略旁的编辑图标 ( )。

步骤 3　新建一条规则或编辑现有规则；请参阅第 14-2 页上的创建和编辑访问控制规则。

系统将显示访问控制规则编辑器。

步骤 4　确保规则操作设置为 **Allow**、 **Interactive Block** 或 **Interactive Block with reset**。

步骤 5　选择 Inspection 选项卡。

系统将显示 Inspection 选项卡。

步骤 6　选择 **File Policy** 检测与访问控制规则相匹配的流量，或选择 **None** 禁用匹配流量的文件检测。

可以点击显示的编辑图标 ( )，在新浏览器选项卡中编辑策略；请参阅第 37-14 页上的创建文件策略。

步骤 7　点击 **Add** 保存规则。

您的规则保存成功。只有保存和应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

配置访问控制规则以执行入侵防御

许可证：保护

访问控制策略可能有多个与入侵策略相关联的访问控制规则。您可以为任何 Allow 或 Interactive Block 访问控制规则配置文件检测，这样，您就可在网络中不同类型的流量到达最终目的地之前，使不同的入侵检测配置文件与其匹配。

只要系统使用入侵策略来评估流量，它便会使用关联的*变量集*。变量集中的变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。您还可以使用入侵策略中的变量表示规则抑制和动态规则状态中的 IP 地址。

提示 即使您使用系统提供的入侵策略，思科**仍强烈**建议您配置系统的入侵变量以准确反映您的网络环境。至少，修改默认变量集中的默认变量；请参阅第 3-16 页上的优化预定义默认变量。

请注意，您在单个访问控制策略中可以使用的唯一入侵策略的数量取决于目标设备型号；设备的功能越强大，处理的策略就越多。每个唯一的入侵策略和变量集**对均**视为一个策略。虽然您可以将不同的入侵策略-变量集对与每条 Allow 和 Interactive Block（以及默认操作）相关联，但是，如果目标设备没有足够的资源可按照配置执行检测，则无法应用访问控制策略。有关详细信息，请参阅第 12-19 页上的简化规则以提高性能。

了解系统提供的和自定义的入侵策略

思科通过 FireSIGHT 系统提供多种入侵策略。通过使用系统提供的入侵策略，您可以借鉴思科漏洞研究团队 (VRT) 的经验。对于这些策略，VRT 设置入侵和预处理程序规则状态，并提供高级设置的初始配置。您可以按原样使用系统提供的策略，也可以将其作为基础构建自定义策略。构建自定义策略可以提高系统在环境中的性能，并且可以更密切监控在网络上发生的恶意流量和违反策略的情况。

除了您创建的自定义策略之外，系统还提供两种自定义策略：初始内联策略和初始被动策略。这两个入侵策略都使用“平衡式安全性和连接性”入侵策略作为其基本策略。两者之间的唯一区别在于其 **Drop When Inline** 设置，该设置在内联策略中启用丢弃行为，在被动策略中禁用丢弃行为。有关详细信息，请参阅第 23-6 页上的比较系统提供的策略与自定义策略。

连接和入侵事件日志记录

当访问控制规则调用的入侵策略检测入侵并生成入侵事件时，它将此事件保存到防御中心数据库。无论访问控制规则采用何种日志记录配置，系统都会将发生入侵的连接结束自动记录到防御中心数据库，请参阅第 38-3 页上的与入侵关联的连接（自动）。

要将入侵策略与访问控制规则相关联，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1 选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2 点击想要使用访问控制规则配置入侵检测所在的访问控制策略旁的编辑图标 ( )。

步骤 3 新建一条规则或编辑现有规则；请参阅第 14-2 页上的创建和编辑访问控制规则。

系统将显示访问控制规则编辑器。

步骤 4 确保规则操作设置为 **Allow**、**Interactive Block** 或 **Interactive Block with reset**。

步骤 5 选择 Inspection 选项卡。

系统将显示 Inspection 选项卡。

步骤 6 选择系统提供的入侵策略或自定义**入侵策略**，或选择 **None** 禁用对与访问控制规则相匹配的流量进行的入侵检测。

如果选择自定义入侵策略，则可点击显示的编辑图标 ( )，在新浏览器选项卡中编辑该策略；请参阅第 31-4 页上的编辑入侵策略。

注意事项　请勿选择 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 7　或者，请更改与入侵策略关联的**变量集**。

可以点击显示的编辑图标 ( )，在新浏览器选项卡中编辑变量集；请参阅第 3-15 页上的使用变量集。

步骤 8　点击 **Save** 以保存规则。

您的规则保存成功。只有保存和应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

调整的入侵防御性能

许可证：保护

思科提供了多项功能，用于提高系统在分析流量中入侵企图时的性能。您可以为每个访问控制策略配置这些性能设置，它们适用于该父访问控制策略调用的所有入侵策略。

有关详情，请参阅：

- 第 18-7 页上的限制入侵模式匹配介绍如何指定事件队列中允许的数据包数量，以及如何针对将重新构造为较大数据流的数据包启用或禁用检查。
- 第 18-8 页上的覆盖入侵规则的正则表达式限制介绍如何覆盖有关 Perl 兼容正则表达式 (PCRE) 的默认匹配和递归限制。
- 第 18-9 页上的限制每个数据包生成的入侵事件数介绍如何配置规则处理事件队列的设置。
- 第 18-10 页上的配置数据包和入侵规则延迟阈值介绍在需要通过数据包和规则延迟阈值将设备延迟维护在可接受水平时如何平衡安全性。
- 第 18-16 页上的配置入侵性能统计数据日志记录介绍如何配置受管设备的基本性能监控和报告参数。

限制入侵模式匹配

许可证：保护

您可以指定事件队列中允许的数据包数量。您还可以在数据流重组之前和之后启用或禁用检查将重建为较大数据流的数据包。

要配置事件队列设置，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 **Pattern Matching Limits** 选项卡。

步骤 5　可修改以下选项：

- 在 **Maximum Pattern States to Analyze Per Packet** 字段中，键入要排队的最多事件数。
- 要在数据流重组之前和之后对将重建为更大数据流的数据包进行检查，请选择 **Disable Content Checks on Traffic Subject to Future Reassembly**。重组前后的检查需要更多的处理开销，可能会导致性能下降。
- 要禁用在数据流重组之前和之后对将重建为更大数据流的数据包进行的检查，请清除选择 **Disable Content Checks on Traffic Subject to Future Reassembly**。禁用检查会减少数据流插件检查的处理开销，并可提高性能。

步骤 6　点击 **OK**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

覆盖入侵规则的正则表达式限制

许可证：保护

对于入侵规则中用于检查数据包负载内容的 PCRE，可覆盖其默认的匹配和递归限制。有关在入侵规则中使用 `pcre` 关键字的详细信息，请参阅第 36-32 页上的使用 PCRE 搜索内容。默认限制可确保最低水平的性能。覆盖这些限制可能会提高安全性，但也会因允许根据低效的正则表达式对数据包进行评估而严重影响性能。

注意事项　除非在撰写入侵规则方面很有经验，并且了解衰减模式的影响，否则，不要覆盖默认的 PCRE 限制。

下表介绍在覆盖默认限制时可配置的选项。

表 18-2　正则表达式约束选项

选项	说明
Match Limit State	指定是否覆盖 **Match Limit**。您有以下选项： • 选择 **Default**，以使用为 **Match Limit** 配置的值 • 选择 **Unlimited**，以允许进行次数不限的尝试 • 选择 **Custom**，为 **Match Limit** 指定 1 或更大的值，或指定 0 以彻底禁用 PCRE 匹配评估
Match Limit	指定在与 PCRE 正则表达式中定义的模式进行匹配时的尝试次数。

表 18-2　正则表达式约束选项（续）

选项	说明
Match Recursion Limit State	指定是否覆盖 **Match Recursion Limit**。您有以下选项： • 选择 **Default**，以使用为 **Match Recursion Limit** 配置的值 • 选择 **Unlimited**，以允许进行次数不限的递归 • 选择 **Custom**，为 **Match Recursion Limit** 指定 1 或更大的值，或指定 0 以彻底禁用 PCRE 递归 注意：为使 **Match Recursion Limit** 具有意义，其值必须小于 **Match Limit**。
Match Recursion Limit	指定在根据数据包静载荷对 PCRE 正则表达式进行评估时的递归次数。

要配置 PCRE 覆盖，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 Regular Expression Limits 选项卡。

步骤 5　可以修改正则表达式约束选项表中的任一选项。

步骤 6　点击 **OK**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

限制每个数据包生成的入侵事件数

许可证：保护

当规则引擎根据规则评估流量时，它会将针对给定的数据包或数据包流生成的事件放在事件队列中，然后将队列顶部的事件报告至用户界面。可选择使规则引擎在生成多个事件时为每个数据包或数据包流记录多个事件。记录这些事件之后，就可收集除已报告事件之外的相关信息。配置此选项时，可指定队列中可放置的事件数量及要记录的事件的数量，并可选择队列中事件顺序的确定条件。

下表介绍在确定为每个数据包或数据流记录的事件数量时可配置的选项。

表 18-3　　入侵事件记录限制选项

选项	说明
Maximum Events Stored Per Packet	为给定数据包或数据包流可存储的最多事件数量。
Maximum Events Logged Per Packet	为给定数据包或数据包流记录的事件数量。此值不能超过 **Maximum Events Stored Per Packet** 值。
Prioritize Event Logging By	该值用于确定事件队列中事件排序方法。排序最高的事件通过用户界面进行报告。有以下选项可供选择： • `priority`，此选项按事件的优先级对队列中的事件进行排序。 • `content_length`，此选项按识别出的最长匹配内容对事件进行排序。当事件按内容长度排序时，规则事件始终优先于解码器和预处理程序事件。

要配置为每个数据包或数据包流记录的事件数量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 **Intrusion Event Logging Limits** 选项卡。

步骤 5　可以修改入侵事件记录限制选项表中的任一选项。

步骤 6　点击 **OK**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

配置数据包和入侵规则延迟阈值

许可证：保护

您可在需要通过数据包和规则延迟阈值将设备延迟维护在可接受水平时平衡安全性。有关详细信息，请参阅：

- 第 18-11 页上的了解数据包延迟阈值设置
- 第 18-12 页上的配置数据包延迟阈值设置
- 第 18-13 页上的要禁用数据包延迟阈值，请执行以下操作：
- 第 18-15 页上的配置规则延迟阈值

了解数据包延迟阈值设置

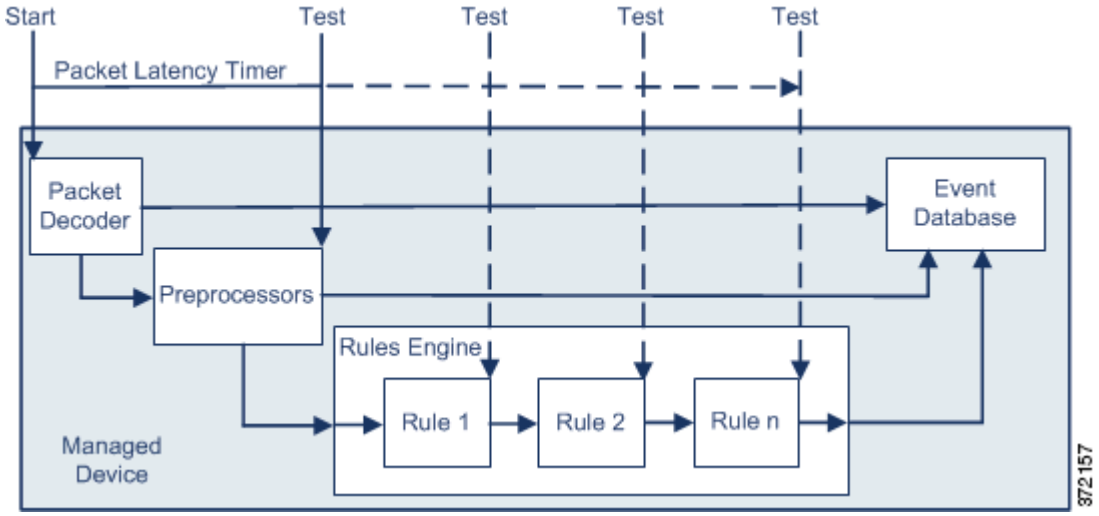
许可证：保护

可在需要将设备延迟保持在可接受水平时平衡安全性，只需启用数据包延迟阈值。数据包延迟阈值用于度量适用的解码器、预处理程序和规则在处理数据包时所需的总时间，并在处理时间超过可配置阈值时停止对数据包的检查。

数据包延迟阈值度量所需时间，而不仅是处理时间，目的是为了更准确地反映规则在处理数据包时实际所需的时间。然而，延迟阈值功能是基于软件实现的延迟管理功能，并不能实施严格的定时功能。

延迟阈值的得失分别为：实现性能和延迟优势的同时，也会导致未经检查的数据包可能包含攻击。但是，数据包延迟阈值提供的工具可用于平衡安全性与连接性。

当解码器开始处理时，每个数据包的计时器开始计时。计时器会持续计时，直到数据包的所有处理工作结束或处理时间在计时测试点超过阈值。



如上图所示，数据包延迟计时在以下测试点测试：

- 在所有解码器和预处理程序的处理完成之后且在规则处理开始之前
- 在每条规则的处理之后

如果处理时间在任何测试点超出阈值，数据包检测将停止。

提示 总的数据包处理时间不包括常规的 TCP 数据流或 IP 分片重组时间。

对于由处理数据包的解码器、预处理程序或规则所触发的事件，数据包延迟阈值不会对其产生影响。只有当数据包已完全处理完毕，或当数据包处理因超过了延迟阈值而终止时（以先出现者为准），任何适用的解码器、预处理程序或规则才会触发事件。如果丢弃规则在内联部署中检测到入侵，则丢弃规则将触发事件并将数据包丢弃。

注 只有当数据包的处理因超出数据包延迟阈值而停止后，才会根据规则评估数据包。本可触发事件的规则无法触发该事件，同时，丢弃规则无法丢弃该数据包。

有关丢弃规则的详细信息，请参阅第 32-18 页上的设置规则状态。

数据包延迟阈值功能对被动式部署和内嵌式部署的性能均有提升作用，并且可以停止检测需要大量处理时间的数据包，从而降低延迟。例如，这些性能优势可以在以下情形中发挥出来：

- 对于被动和内联式部署，多个规则依序检查一个数据包需要过长的时间
- 对于内联式部署，网络性能不佳（例如，当有人下载超大文件时）期间，数据包处理变慢。

在被动式部署中，停止数据包的处理可能无助于恢复网络性能，这是因为，只不过转至处理下一数据包而已。

配置数据包延迟阈值设置

许可证：保护

默认情况下系统提供的 Balanced Security and Connectivity 入侵策略已启用基于延迟的性能设置。下表介绍了在配置数据包延迟阈值时可设置的选项。

表 18-4　　数据包延迟阈值 选项

选项	说明
Threshold (microseconds)	指定数据包检查停止的时间，单位为微秒。有关所建议的最小阈值设置，请参阅最小数据包延迟阈值设置表。

可启用规则 134:3，这样，当系统因超过数据包延迟阈值而停止检查数据包时可生成事件。有关详细信息，请参阅第 41-7 页上的查看入侵事件和第 32-18 页上的设置规则状态。

很多因素影响系统性能和数据包延迟，如 CPU 速度、数据速率、数据包大小和协议类型。因此，思科建议您使用下表中的阈值设置，直到您计算出了适合自己的网络环境的设置。

表 18-5　　最小数据包延迟阈值设置

针对此数据速率...	将阈值（微秒）设置为至少...
1 Gbps	100
100 Mbps	250
5 Mbps	1000

计算设置时请确定：

- 每秒的平均数据包数
- 每个数据包所需的平均微秒数

将网络中每个数据包所需的平均微秒数乘以一个较大的安全因子，以确保不必要地中止数据包检查。

例如，最小数据包延迟阈值设置表建议 1 G 环境中的最小数据包延迟阈值应为 100 微秒。此建议的最小阈值所依据的测试数据为每秒平均 250,000 个数据包，即每微秒 0.25 个数据包，或每个数据包用时 4 微秒。乘以因子 25 即得出建议的最小阈值 100 微秒。

要配置数据包延迟阈值，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Latency-Based Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 Packet Handling 选项卡。

提示　默认情况下，系统将启用数据包延迟阈值。要完全禁用延迟阈值，请清除 **Enable** 复选框。

步骤 5　有关所建议的最小**阈值**设置，请参阅最小数据包延迟阈值设置表。

步骤 6　点击 **OK**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

要禁用数据包延迟阈值，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Latency-Based Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 Packet Handling 选项卡。

步骤 5　有关所建议的最小**阈值**设置，请参阅最小数据包延迟阈值设置表。

步骤 6　点击 **OK**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

了解规则延迟阈值

许可证：保护

可在需要将设备延迟保持在可接受水平时平衡安全性，只需启用规则延迟阈值。规则延迟阈值功能可以衡量每个规则处理各个数据包所花费的时间、将超过阈值的规则及一系列相关规则暂停指定的时间（如果处理时间连续超过规则延迟阈值一定次数 [可配置]），以及在暂停到期后恢复规则。

规则延迟阈值度量所需时间，而不仅是处理时间，目的是为了更准确地反映规则在处理数据包时实际所需的时间。然而，延迟阈值功能是基于软件实现的延迟管理功能，并不能实施严格的定时功能。

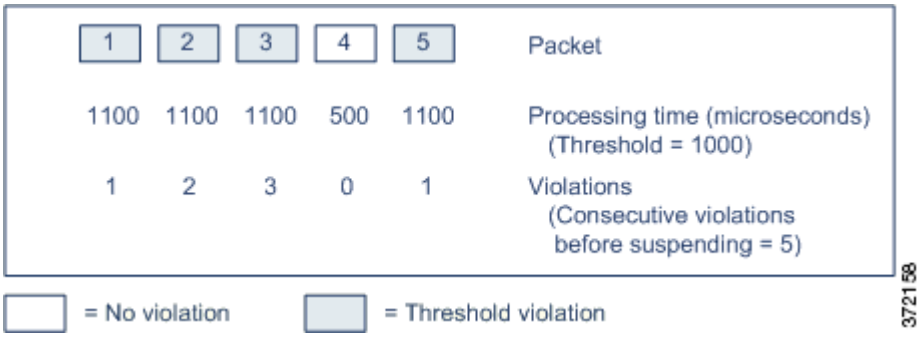
延迟阈值的得失分别为：实现性能和延迟优势的同时，也会导致未经检查的数据包可能包含攻击。但是，规则延迟阈值提供的工具可用于平衡安全性与连接性。

计时器测量每次根据一组规则处理数据包所用的处理时间。任何时候，只要规则处理时间超出指定的规则延迟阈值，系统就会递增计数器的计数。如果连续超出阈值的次数达到了指定的数值，系统就会执行下列操作：

- 按指定的期限暂停规则
- 触发事件以指明规则已暂停
- 暂停时间到期时重新启用规则
- 触发事件以指明规则已重新启用

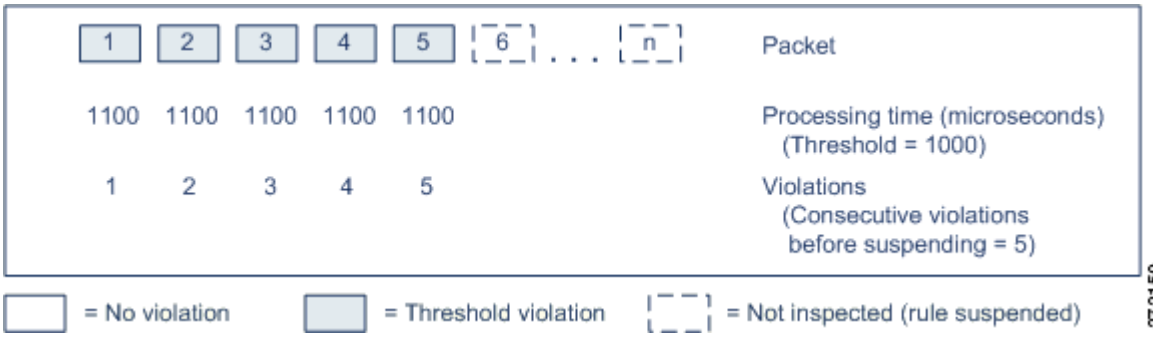
当该组规则已暂停时，或当规则违规次数非连续时，系统会将计数器清零。如在暂停规则前允许一定次数的连续违规，则将忽略对性能的影响无足轻重的偶发性违规，转而专注于反复超出规则延迟阈值的规则所造成的更大影响。

以下示例显示了未导致规则暂停的 5 次连续规则处理时间。



在以上示例中，处理前三个数据包中各个数据包的所需时间超出 1000 微秒的规则延迟阈值，每次违规时违规计数器均将递增 1 次计数。第四个数据包的处理时间未超出阈值，因此违规计数器重置为 0。第五个数据包的处理时间超出阈值，因此违规计数器从 1 开始重新计数。

以下示例显示了导致规则暂停的 5 次连续规则处理时间。



在第二个示例中，处理五个数据包中每个数据包所需的时间均超出 1000 微秒的规则延迟阈值。由于每个数据包的规则处理时间是 1100 微秒，超出 1000 微秒阈值的次数到达指定的连续 5 次，因此该组规则被暂停。在暂停时间到期前，任何后续的数据包（在图中表示为数据包 6 至 n）均不会根据暂停的规则得以检查。如果重新启用规则后收到了更多的数据包，违规计数器从 0 开始重新计数。

规则延迟阈值对数据包处理规则所触发的入侵事件无影响。无论规则处理时间是否超出阈值，规则都会因数据包中检测到的任何入侵而触发事件。如果检测到入侵的规则是内联部署中的丢弃规则，则将丢弃数据包。当丢弃规则检测到数据包中存在将导致暂停规则的入侵时，丢弃规则将触发入侵事件，数据包将被丢弃，该规则和所有相关规则均被暂停。有关丢弃规则的详细信息，请参阅第 32-18 页上的设置规则状态。

注　系统不会根据已暂停的规则对数据包进行评估。本可触发事件的已暂停规则无法触发该事件，同时，丢弃规则无法丢弃该数据包。

通过暂停在处理数据包时耗时最长的规则，规则延迟阈值可提高被动和内联部署模式下的系统性能，并缩短内联部署中的延迟。在可配置的时间到期之前，系统不会根据被暂停的规则对数据包再次进行评估，从而留出时间让过载设备进行恢复。例如，这些性能优势可以在以下情形中发挥出来：

- 匆忙写就、大量未经测试的规则需要过长的处理时间
- 网络性能不佳期间（例如，当有人下载超大文件时），数据包检查变慢。

配置规则延迟阈值

许可证：保护

可修改规则延迟阈值、已暂停规则的暂停时间以及暂停规则前必须连续超出阈值的次数。

如果规则处理数据包时所用时间超过 **Consecutive Threshold Violations Before Suspending Rule** 所指定的连续次数的**阈值**，则规则延迟阈值就会按 **Suspension Time** 指定的时间暂停规则。

可启用规则 134:1，当规则已暂停时生成事件；并启用规则 134:2，在启用已暂停规则时生成事件。有关详细信息，请参阅第 41-7 页上的查看入侵事件和第 32-18 页上的设置规则状态。

下表进一步介绍在配置规则延迟阈值时可设置的选项。

表 18-6　规则延迟阈值选项

选项	说明
阈值	指定规则在检查数据包时不应超出的时间，单位为微秒。有关所建议的最小阈值设置，请参阅最小规则延迟阈值设置表。
暂停规则前连续超出阈值的次数	指定在暂停规则之前，规则可按超过为 **Threshold** 设置的时间检查数据包的连续次数。
Suspension Time	指定暂停一组规则前需经过的秒数。

许多因素影响系统性能，如 CPU 速度、数据速率、数据包大小和协议类型。因此，思科建议您使用下表中的阈值设置，直到您计算出了适合自己的网络环境的设置。

表 18-7　最小规则延迟阈值设置

针对此数据速率...	将阈值（微秒）设置为至少...
1 Gbps	500
100 Mbps	1250
5 Mbps	5000 年

计算设置时请确定：

- 每秒的平均数据包数
- 每个数据包所需的平均微秒数

将网络中每个数据包所需的平均微秒数乘以一个较大的安全因子，以确保不必要地中断规则检查。

要配置规则延迟阈值，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Latency-Based Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 Rule Handling 选项卡。

步骤 5　可以配置规则延迟阈值选项表中的任一选项。

有关所建议的最小**阈值**设置，请参阅最小规则延迟阈值设置表。

步骤 6　点击 **OK**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

配置入侵性能统计数据日志记录

许可证：保护

可配置指定设备如何监控和报告其自身性能的基本参数。这样，就可通过配置以下选项，指定系统更新设备上的性能统计数据的时间间隔：

Sample time (seconds) and Minimum number of packets

当过了所指定的性能统计数据更新之间的秒数时，系统验证其已分析的数据包是否到达指定数量。如果到达，则系统更新性能统计数据。否则，系统等待，直到其分析的数据包到达指定的数量。

Troubleshooting Options: Log Session/Protocol Distribution

支持部门可能要求您在故障排除调用期间记录协议分布、数据包长度和端口统计信息。

注意事项　更改此故障排除选项的设置将会影响性能，只能在支持部门的指导下完成该更改。

Troubleshooting Options: Summary

支持部门可能要求您在故障排除调用期间将系统配置为仅在 Snort® 进程关闭或重新启动时计算性能统计数据。要启用此选项，也必须启用 **Log Session/Protocol Distribution** 故障排除选项。

注意事项　更改此故障排除选项的设置将会影响性能，只能在支持部门的指导下完成该更改。

要配置基本的性能统计数据参数，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 Performance Statistics 选项卡。

步骤 5　如前所述修改 **Sample time** 或 **Minimum number of packets**。

步骤 6　或者，展开 **Troubleshoot Options** 部分并修改这些选项（仅当支持部门要求这样做时）

步骤 7　点击 **OK**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

调整文件和恶意软件检查性能和存储

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

如果使用文件策略执行文件控制、文件存储、动态分析或者恶意软件检测或拦截，则可以设置下表中列出的选项。记住，提高文件大小会影响系统的性能。

表 18-8　　高级访问控制的文件和恶意软件检测选项

字段	说明	默认值	范围	备注
限制进行文件类型检测时检查的字节的数量	指定执行文件类型检测时检查的字节的数量。	1460 字节，或者 TCP 数据包的最大分段大小	0 - 4294967295 (4GB)	设置为 0 可移除限制。 在大多数情况下，系统可以使用第一个数据包确定常见的文件类型。
对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）	禁止系统存储大于特定大小的文件，对文件进行查阅综合安全智能云或阻止文件（如果已添加至自定义检测列表）。	10485760 (10MB)	0 - 4294967295 (4GB)	设置为 0 可移除限制。 该值必须大于或等于**可存储的最大文件大小（字节）**和**用于动态分析测试的最大文件大小（字节）**。
允许文件，如果用于阻止恶意软件的云查找耗时超过（秒）	指定进行恶意软件云查找时，没有缓存的处置，系统将会保持匹配**阻止恶意软件**规则的文件的最后一个字节的时长。如果该时间过去，系统没有获得处置，文件将会通过。不可用的处置不会被缓存。	2 秒	0 - 30 秒	尽管该选项接受最长 30 秒的值，思科 建议使用默认值，以避免因为连接故障而阻止流量。如未联系支持部门，**请勿**将此选项设置为 0。

表 18-8　高级访问控制的文件和恶意软件检测选项（续）

字段	说明	默认值	范围	备注
可存储的最小文件大小（字节）	指定使用文件规则，系统可以存储的最小文件大小。	6144 (6KB)	0 - 10485760 (10MB)	设置为 0 可以禁用文件存储。 此字段的值必须小于或等于**可存储的最大文件大小（字节）**和**对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）**。
可存储的最大文件大小（字节）	指定使用文件规则，系统可以存储的最大文件大小。	1048576 (1MB)	0 - 10485760 (10MB)	设置为 0 可以禁用文件存储。 此字段的值必须大于或等于**可存储的最小文件大小（字节）**，并小于或等于**对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）**。
用于动态分析测试的最小文件大小（字节）	指定系统可以提交至云以供动态分析的最小文件大小。	6144 (6KB)	6144 (6KB) - 2097152 (2MB)	此字段的值必须小于或等于**用于动态分析测试的最大文件大小（字节）**和**对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）**。 系统会检查云以更新可以提交的最小文件大小（一天不超过一次）。如果新的最小值大于当前值，当前值会更新为新的最小值，而且策略会标记为过期。
用于动态分析测试的大小文件大小（字节）	指定系统可以提交至云以供动态分析的最大文件大小。	1048576 (1MB)	6144 (6KB) - 2097152 (2MB)	此字段的值必须大于或等于**用于动态分析测试的最小文件大小（字节）**，并小于或等于**对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）**。 系统会检查云以更新可以提交的最大文件大小（一天不超过一次）。如果新的最大值小于当前值，当前值会更新为新的最大值，而且策略会标记为过期。

请注意，由于既不能对 DC500 使用恶意软件许可证，也不能在 2 系列设备或 用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此无法使用这些设备捕获、存储或阻止个别文件，分析存档文件的内容，提交文件供动态分析，或查看为其执行恶意软件云查找的文件的文件轨迹。

要配置文件和恶意软件检查性能和存储，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Files and Malware Settings** 旁边的编辑图标 ( )。

系统将显示 Files and Malware Settings 弹出窗口。

步骤 5　可以设置高级访问控制的文件和恶意软件检测选项表中的任一选项。

步骤 6　点击 **OK**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

了解流量解密

默认情况下，系统无法检查采用安全套接字层 (SSL) 或传输层安全 (TLS) 协议加密的流量。作为访问控制的一部分， *SSL 检查*功能可供您阻止已加密流量而不进行检查，或者使用访问控制检查已加密或解密的流量。系统在处理已加密会话时会记录流量的详细信息。检查已加密流量与分析已加密会话数据双管齐下，可以更好地了解和控制网络中的已加密应用和流量。

如果系统检测通过 TCP 连接进行的 SSL 或 TLS 握手，则它将确定是否能解密检测到的流量。如果不能，则将应用已配置的操作：

- 阻止已加密流量并选择性重置 TCP 连接
- 不解密已加密的流量

请注意，当 SSL 检查配置允许已加密流量通过或者您不配置 SSL 检查时，访问控制规则处理已加密流量。但是，某些访问控制规则条件需要未加密流量，因此，已加密流量可能匹配的规则更少。此外，默认情况下，系统禁用已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。有关详细信息，请参阅第 14-2 页上的创建和编辑访问控制规则和第 27-60 页上的使用 SSL 预处理器。

如果系统能够解密流量，则它将阻止流量而不进行进一步检查、使用访问控制评估未解密流量或使用以下方法之一解密该流量：

- 采用已知的私钥解密。在外部主机启动与网络上某台服务器的 SSL 握手时，系统将交换的服务器证书与之前上载至设备的服务器证书相匹配。然后使用上载的私钥解密流量。
- 通过重签服务器证书进行解密。在网络上的某台主机启动与外部服务器的 SSL 握手时，系统将使用之前上载的证书颁发机构 (CA) 证书重签交换的服务器证书。然后使用上载的私钥解密流量。

已解密流量将接受与最初未加密流量相同的流量处理和分析：基于网络、信誉和用户的访问控制，入侵检测和防御，高级恶意软件防护以及发现。如果系统在分析已解密流量后未阻止该流量，则会重新对其加密，然后再将其传递到目标主机。

注 某些 SSL 检查操作（例如，阻止流量和解密出站流量）会修改流量。以内联方式部署的设备可以执行这些操作。被动部署或分路模式中的设备不会影响流量。但是，这些设备仍然可以解密入站流量；详细信息请参阅第 19-5 页上的示例：在被动部署中解密流量。

有关详细信息，请参阅以下各节：

- 第 19-2 页上的 SSL 检查要求
- 第 19-4 页上的分析 SSL 检查设备部署

SSL 检查要求

许可证：因功能而异

受支持的设备：3 系列

仅某些设备型号支持 SSL 检查。除了您的配置设置和许可证之外，如何在网络中部署设备也会影响到您控制和解密已加密流量时可以采取的操作。

配置 SSL 检查时可用的功能和操作取决于您的用户角色。系统包括专门为各种管理员和分析师设计的预定义用户角色，您可以创建具有特殊访问权限的自定义用户角色。

SSL 检查需要公钥证书和配对的私钥才能执行某些功能。您必须将证书和配对的私钥上载到防御中心以根据加密会话特性解密和控制流量。

有关详细信息，请参阅以下各节：

部署支持 SSL 检查的设备

许可证：任何环境

受支持的设备：3 系列

SSL 检查需要 3 系列设备。

用内联、路由式、交换式或混合接口配置和部署的设备可以修改流量。这些设备可以监控、阻止、允许和解密入站和出站流量。

用被动或内联（分路模式）接口配置和部署的设备无法影响流量。这些设备只能监控、允许和解密入站流量。请注意，被动部署不支持解密采用瞬时 Diffie-Hellman (DHE) 或椭圆曲线 Diffie-Hellman (ECDHE) 密码套件加密的流量。

请审查您的映射操作列表、现有网络部署和总体要求以确定是否有一种或其他类型的部署更适合贵组织。有关详细信息，请参阅第 19-4 页上的分析 SSL 检查设备部署。

确定 SSL 检查必需的许可证

许可证：因功能而异

视乎您的许可证，您可以使用一组条件确定如何处理已加密流量。尽管无论防御中心上的许可证如何您均可创建 SSL 策略，但 SSL 检查的某些方面要求在应用策略之前先启用目标设备上的特定许可功能。防御中心使用警告图标 (⚠) 和确认对话框来指定您部署的不受支持的功能。有关详细信息，请将指针悬停在警告图标上方。

作为访问控制策略的一部分，您将 SSL 策略应用于受管设备，访问控制策略将检查由 SSL 策略解密的流量。有关访问控制许可的详细信息，请参阅第 12-2 页上的访问控制许可证和角色要求。

下表说明作为访问控制策略的一部分应用 SSL 策略的许可证要求。

表 19-1　SSL 检查的许可证和型号要求

要应用具有以下功能的 SSL 策略...	许可证	支持的防御中心	支持的设备
根据区域、网络、VLAN、端口或 SSL 相关条件处理已加密的流量	任何环境	任何环境	3 系列
使用地理定位数据处理已加密的流量	FireSIGHT	除 DC500 外的所有型号	3 系列
使用应用或用户条件处理已加密的流量	可控性	除 DC500 外的所有型号都无法执行用户控制	3 系列
使用 URL 类别和信誉数据过滤已加密的流量	URL 过滤	除 DC500 外的所有型号	3 系列

使用自定义用户角色管理您的 SSL 检查部署

许可证：任何环境

如第 61-48 页上的管理自定义用户角色中所述，可以创建具有特殊化访问权限的自定义用户角色。自定义用户角色可以具有任何基于菜单的权限集和系统权限集，并且可能完全是原始的或基于预定义用户角色。下表说明确定用户是否有权限配置和部署 SSL 检查的角色权限：

表 19-2　SSL 检查相关用户角色权限

用户权限	说明
对象管理员	允许您创建、修改和删除与 SSL 检查相关的对象
SSL	允许您生成 SSL 策略的报告并比较 SSL 策略或策略版本
修改 SSL 策略	允许您查看、创建、修改和删除 SSL 策略，以及创建、修改和删除不属于 Administrator Rules 或 Root RulesSSL 类别的 SSL 规则
修改 Administrator Rules	允许您创建、修改和删除 Administrator Rules 类别中的 SSL 规则
修改 Root Rules	允许您创建、修改和删除 Root Rules 类别中的 SSL 规则
应用 SSL 策略	当您应用访问控制策略之后，允许您应用与其关联的 SSL 策略
访问控制列表	允许您查看访问控制策略的列表
修改访问控制策略	允许您将 SSL 策略与访问控制策略相关联
应用访问控制策略	允许您应用与 SSL 策略关联的访问控制策略

有关详细信息，请参阅第 12-2 页上的访问控制许可证和角色要求。

收集配置 SSL 规则的必备信息

许可证：功能相关

SSL 检查依赖于大量支持公钥基础架构 (PKI) 信息。考虑贵组织的流量模式以确定可配置的匹配规则条件。收集下表列出的信息：

表 19-3　　SSL 规则条件必备信息

要匹配…	收集…
检测到的服务器证书，包括自签的服务器证书	服务器证书
受信任的服务器证书	CA 证书
检测到的服务器证书主体或颁发机构	服务器证书主体 DN 或颁发机构 DN

有关详细信息，请参阅第 22-1 页上的使用 SSL 规则调整流量解密。

决定是否不解密、阻止、监控或解密作为您匹配规则之依据的已加密流量。将这些决策映射至 SSL 规则操作、无法解密的流量操作和 SSL 策略默认操作。要解密流量，请参阅下表：

表 19-4　　SSL 解密必备条件

要解密…	收集...
您控制的服务器的入站流量	服务器证书文件和配对的私钥文件
外部服务器的出站流量	CA 证书文件和配对的私钥文件 还可以生成 CA 证书和私钥。

有关详细信息，请参阅第 21-7 页上的使用规则操作确定加密流量处理和检查。

在您收集此信息后，请将其上载到系统并配置可重复使用的对象。有关详细信息，请参阅第 3-1 页上的管理可重用对象。

分析 SSL 检查设备部署

许可证：功能相关

受支持的设备：3 系列

本小节提供了若干情景，在其中 Life Insurance Example, Inc. life insurance company (LifeIns) 对已加密流量使用 SSL 检查以帮助审核其流程。根据其业务流程， LifeIns 计划部署：

- 被动部署中的一台 3 系列受管设备，供客户服务部门使用
- 内联部署中的一台 3 系列受管设备，供保险部门使用
- 用于管理上述两台设备的一台防御中心

客户服务业务流程

LifeIns 为客户创建了面向客户的网站。LifeIns 通过其网站和邮件接收来自潜在客户的有关保单的已加密问题和请求。 LifeIns 的客户服务部门在 24 小时内处理并返回请求的信息。客户服务部门希望扩展其传入联络指标收集 LifeIns 已为客户服务部门建立内部审核机制。

LifeIns 还在线接收已加密的应用。客户服务部门在将案例文件发送到保险部门之前，在 24 小时内处理申请。客户服务部门过滤出通过在线表单发送的所有明显错误的申请，这将消耗他们不少时间。

保险业务流程

LifeIns 的保险员在线向 Medical Repository Example， LLC medical data repository （MedRepo ）提交已加密的医疗信息请求。 MedRepo 在 72 小时内审查该请求并将已加密记录传输到 LifeIns。保险员随后签署接受申请并提交保单和费率决定。保险部门希望扩展其指标收集。

最近，未知源总是发送欺骗响应到 LifeIns。虽然 LifeIns 的保险员接受过正确使用互联网的培训，但 LifeIns 的 IT 部门首先要分析采用医疗响应形式的所有已加密流量，然后要阻止所有欺骗尝试。

LifeIns 对初级保险员提供六个月的培训。最近，这些保险员错误地向 MedRepo 的客户服务部门提交了已加密的医疗法规请求。作为回应， MedRepo 多次向 LifeIns 提出投诉。 LifeIns 计划延长这些新保险员的培训期，并且审核保险员对 MedRepo 提交的请求。

有关详细信息，请参阅以下各节：

- 第 19-5 页上的示例：在被动部署中解密流量
- 第 19-9 页上的示例：在内联部署中解密流量

示例：在被动部署中解密流量

许可证：功能相关

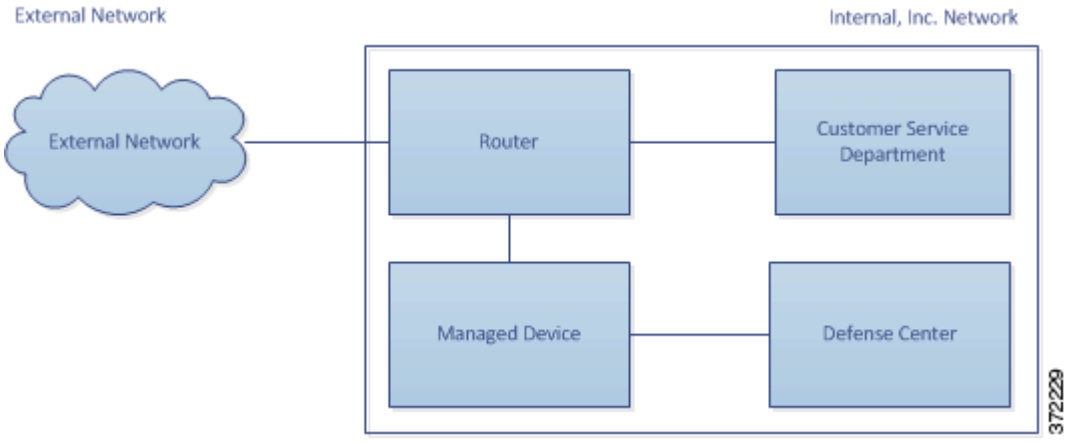
受支持的设备：3 系列

LifeIns 的业务要求客户服务部门必须：

- 在 24 小时内处理所有请求和申请
- 改善其传入联系指标收集流程
- 标识并丢弃传入错误申请

客户服务部门无需额外的审核。

LifeIns 计划以被动方式部署客户服务部门的受管设备。下图说明 LifeIns 的被动部署。



来自外部网络的流量进入 LifeIns 的路由器。该路由器将流量路由到客户服务部门并将流量的副本镜像到受管设备进行检查。

在管理防御中心上，具有访问控制和 SSL 编辑器自定义角色的用户配置 SSL 检查完成以下任务：

- 记录发送到客户服务部门的所有已加密流量
- 解密使用在线申请表发送到客户服务部门的已加密流量
- 不解密发送到客户服务部门的所有其他已加密流量，包括使用在线请求表发送的流量

用户也可以配置访问控制以检查已加密的申请表流量是否存在虚假的申请数据，并在检测到虚假数据时予以记录。

在以下情景中，用户向客户服务部门提交在线表单。用户的浏览器建立与服务器的 TCP 连接，然后启动 SSL 握手。受管设备接收该流量的副本。客户端和服务器完成 SSL 握手，建立已加密会话。系统根据握手和连接详情记录连接并对已加密流量的副本执行操作。

有关详细信息，请参阅以下部分：

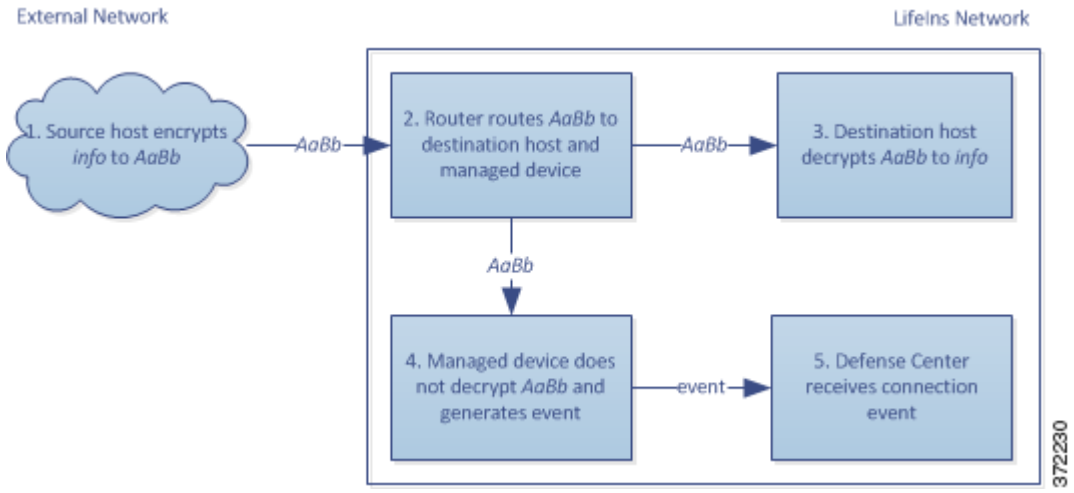
- 第 19-6 页上的在被动部署中监控已加密的流量
- 第 19-7 页上的不解密被动部署中的已加密流量
- 第 19-7 页上的在被动部署中使用私钥检查已加密的流量

在被动部署中监控已加密的流量

许可证：任何环境

受支持的设备：3 系列

对于发送到客户服务部门的所有 SSL 加密流量，系统均记录连接。下图说明监控已加密流量的系统。



发生接下来的步骤：

1. 用户提交纯文本请求 (`info`)。客户端加密此 (`AaBb`) 并将已加密流量发送到客户服务部门。
2. LifeIns 的路由器接收已加密流量并将其路由到客户服务部门服务器。它还将副本镜像到受管设备。
3. 客户服务部门服务器接收已加密的信息请求 (`AaBb`) 并将其解密为纯文本 (`info`)。
4. 受管设备不解密流量。

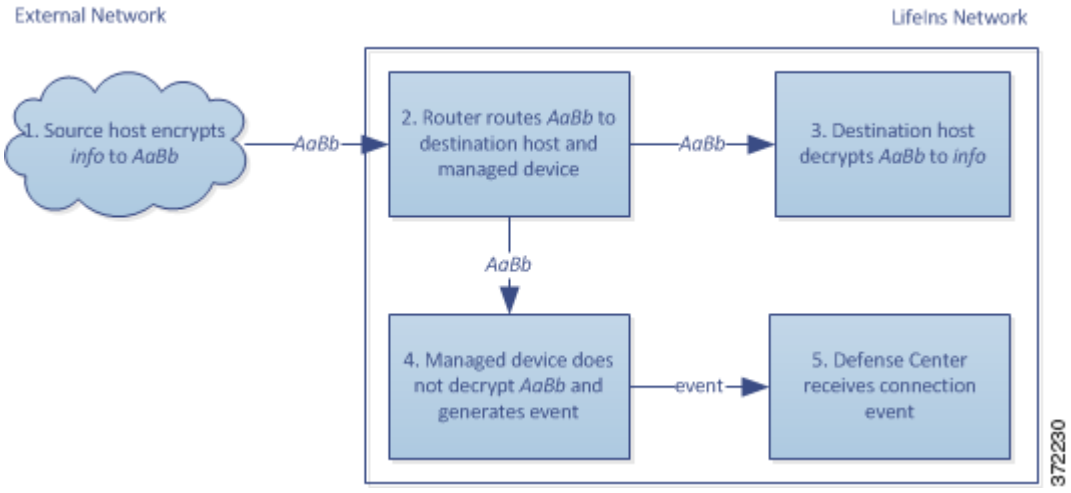
   访问控制策略继续处理已加密的流量并允许其通过。设备在会话结束后生成连接事件。
5. 防御中心 接收连接事件。

不解密被动部署中的已加密流量

许可证：任何环境

受支持的设备：3 系列

对于包含有关保单的请求的所有 SSL 加密流量，系统允许该流量通过而不解密它，并记录连接。下图说明允许已加密流量通过而无需进一步检查的系统。



发生接下来的步骤：

1. 用户提交纯文本请求 (`info`)。客户端加密此 (`AaBb`) 并将已加密流量发送到客户服务部门。
2. LifeIns 的路由器接收已加密流量并将其路由到客户服务部门服务器。它还将副本镜像到受管设备。
3. 客户服务部门服务器接收已加密的信息请求 (`AaBb`) 并将其解密为纯文本 (`info`)。
4. 受管设备不解密流量。

   访问控制策略继续处理已加密的流量并允许其通过。设备在会话结束后生成连接事件。
5. 防御中心 接收连接事件。

在被动部署中使用私钥检查已加密的流量

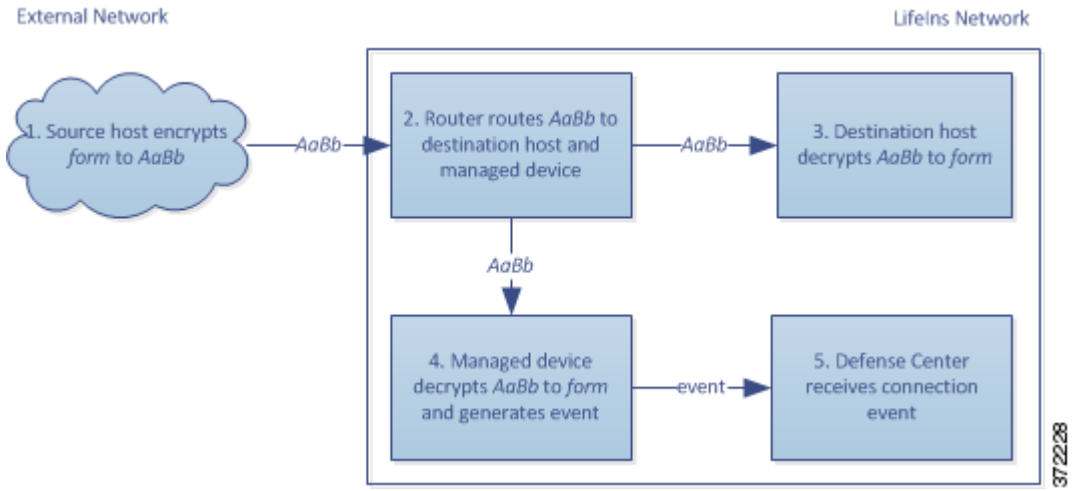
许可证：任何环境

受支持的设备：3 系列

对于包含申请表单数据的所有 SSL 加密流量，系统均解密该流量加密并记录连接。

注　在被动部署中，如果流量采用 DHE 或 ECDHE 密码套件加密，则您无法使用已知私钥解密该流量。

对于包含合法的申请表信息的流量，系统将记录连接。下图说明使用已知私钥进行的流量解密。

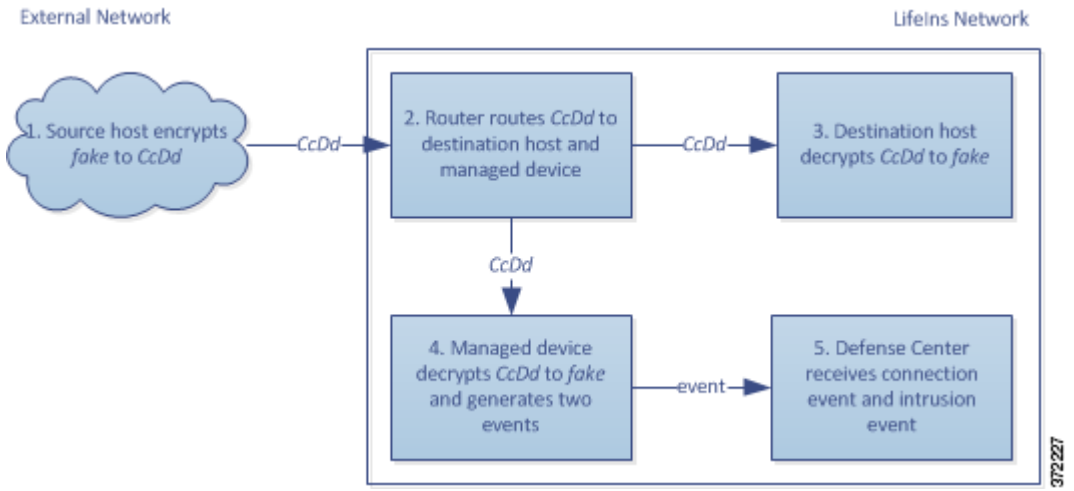


发生接下来的步骤：

1. 用户提交纯文本请求 (`form`)。客户端加密此 (`AaBb`) 并将已加密流量发送到客户服务部门。
2. LifeIns 的路由器接收已加密流量并将其路由到客户服务部门服务器。它还将副本镜像到受管设备。
3. 客户服务部门服务器接收已加密信息请求 (`AaBb`) 并将其解密为纯文本 (`form`)。
4. 受管设备使用通过上载的已知私钥获取的会话密钥将该已加密流量解密为纯文本 (`form`)。

   访问控制策略继续处理已解密的流量且不查找虚假的申请信息。设备在会话结束后生成连接事件。
5. 防御中心接收包含有关已加密和解密流量的信息的连接事件。

相反，如果已解密流量包含虚假申请数据，则系统记录连接和虚假数据。下图说明使用已知私钥对包含虚假申请数据的入站流量进行解密的系统。



发生接下来的步骤：

1. 用户提交纯文本请求 (`fake`)。客户端加密此 (`CcDd`) 并将已加密流量发送到客户服务部门。
2. LifeIns 的路由器接收已加密流量并将其路由到客户服务部门服务器。它还将副本镜像到受管设备。
3. 客户服务部门服务器接收已加密的信息请求 (`CcDd`) 并将其解密为纯文本 (`fake`)。
4. 受管设备使用通过上载的已知私钥获取的会话密钥将此已加密流量解密为纯文本 (`fake`)。

   访问控制策略继续处理已解密的流量并查找虚假的申请信息。设备生成入侵事件。设备在会话结束后生成连接事件。
5. 防御中心接收包含有关已加密和解密流量的信息的连接事件，以及虚假申请数据的入侵事件。

示例：在内联部署中解密流量

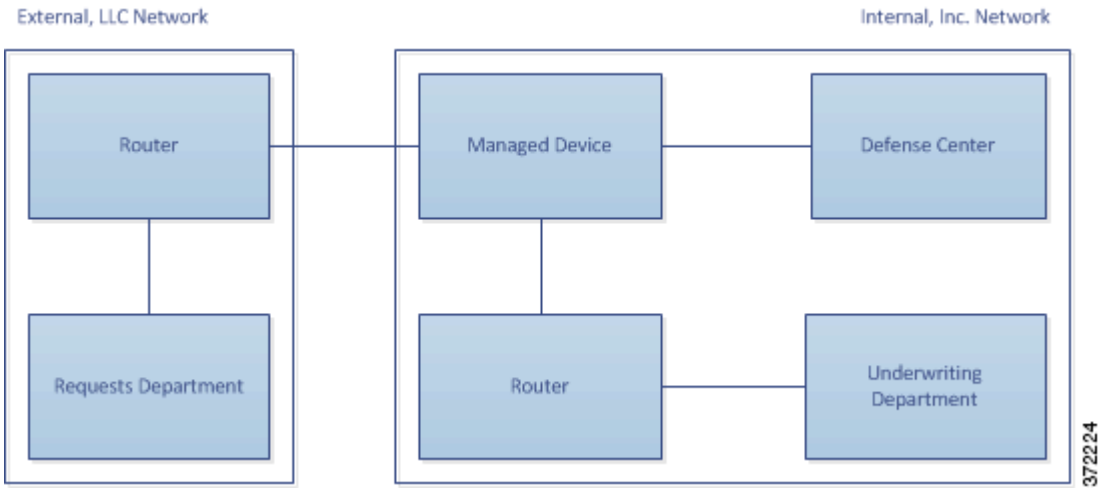
许可证：功能相关

受支持的设备：3 系列

LifeIns 的业务要求规定保险部门必须：

- 审核新的和初级保险员，确认其提交给 MedRepo 的信息请求符合所有适用的法规
- 改善其保险指标收集流程
- 检查似乎来自 MedRepo 的所有请求，然后丢弃所有欺骗尝试
- 丢弃从保险部门发送到 MedRepo 客户服务部门的所有不当法规请求
- 不审核高级保险员

LifeIns 计划在内联部署中部署一台设备供保险部门使用。下图说明 LifeIns 的内联部署。



来自 MedRepo 网络的流量进入 LifeIns 的路由器。该路由器将流量路由到 LifeIns 的网络。受管设备接收流量，将允许的流量传递到 LifeIns 的路由器，并向管理防御中心发送事件。 LifeIns 的路由器将流量路由到目标主机。

在管理防御中心上，具有访问控制和 SSL 编辑器自定义角色的用户配置 SSL 检查完成以下任务：

- 记录发送到保险部门的所有已加密流量
- 阻止从 LifeIns 的保险部门错误发送到 MedRepo 客户服务部门的所有已加密流量

- 解密从 MedRepo 发送到 LifeIns 的保险部门以及从 LifeIns 的初级保险员发送到 MedRepo 的请求部门的所有已加密流量
- 不解密从高级保险员发送的已加密流量

用户还可以将访问控制配置为使用自定义入侵策略检查已解密的流量，并且：

- 如果已解密流量包含欺骗尝试，则将其阻止并记录欺骗尝试
- 阻止包含不符合法规的信息的已解密流量，并记录不当信息
- 允许所有其他的已加密和已解密流量

系统在将允许的已解密流量发送到目标主机之前对其重新加密。

在以下情景中，用户在线向远程服务器提交信息。用户的浏览器建立与服务器的 TCP 连接，然后启动 SSL 握手。受管设备接收此流量；系统基于握手和连接详情记录连接并对流量执行相应操作。如果系统阻止流量，则也会关闭 TCP 连接。否则，客户端和服务器完成 SSL 握手，从而建立已加密会话。

有关详细信息，请参阅以下部分：

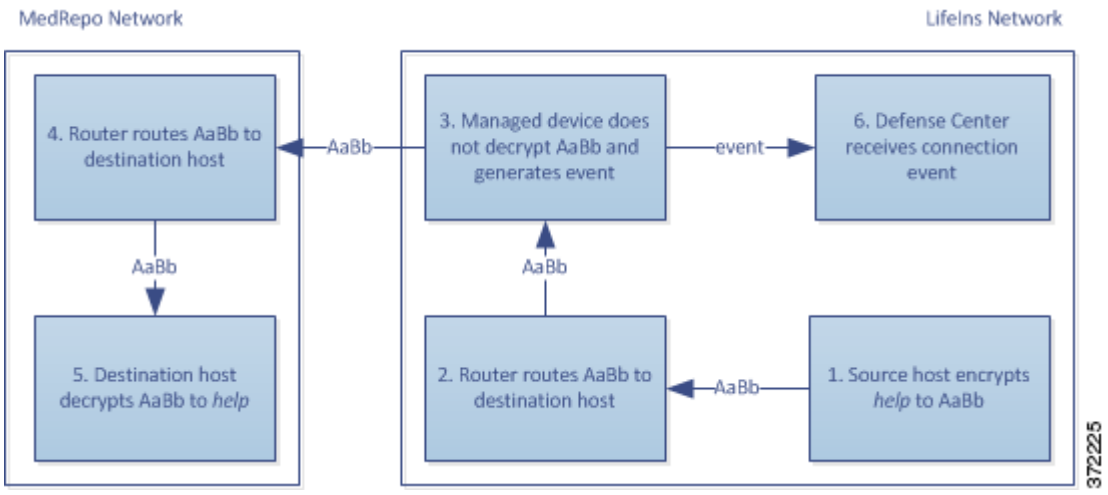
- 第 19-10 页上的在内联部署中监控已加密的流量
- 第 19-11 页上的在内联部署中允许特定用户的已加密流量
- 第 19-12 页上的在内联部署中阻止已加密的流量
- 第 19-12 页上的在内联部署中使用私钥检查已加密的流量
- 第 19-14 页上的在内联部署中使用重签证书检查特定用户的已加密流量

在内联部署中监控已加密的流量

许可证：任何环境

受支持的设备：3 系列

对于发往保险部门或从其发出的所有 SSL 加密流量，系统将记录连接。下图说明监控已加密流量的系统。



发生接下来的步骤：

1. 用户提交纯文本请求 (`help`)。客户端加密此 (`AaBb`) 并将已加密流量发送到 MedRepo 的请求部门服务器。
2. LifeIns 的路由器接收已加密流量并将其路由到请求部门服务器。
3. 受管设备不解密流量。

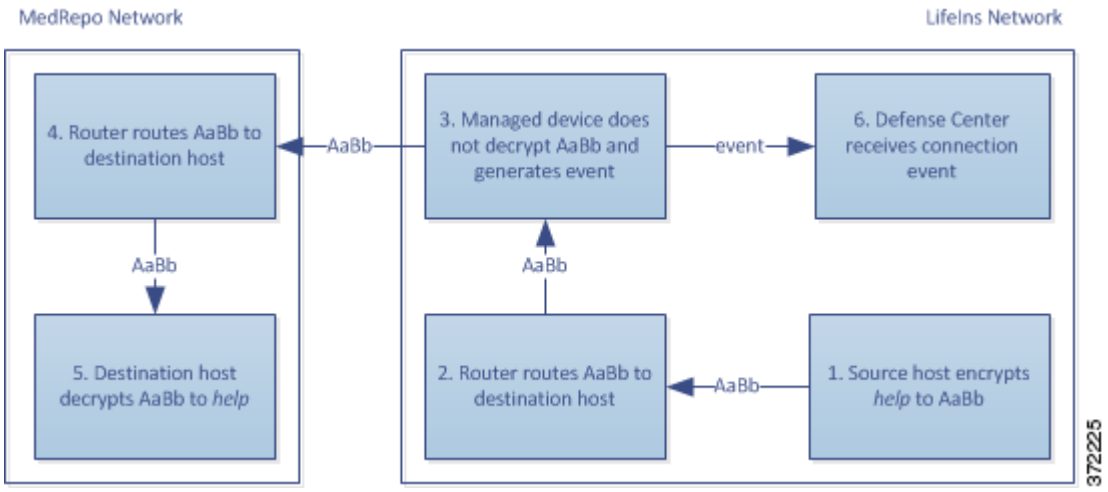
   访问控制策略继续处理已加密流量并允许其通过，然后在会话结束后生成连接事件。
4. 外部路由器接收流量并将其路由到请求部门服务器。
5. 保险部门服务器接收已加密的信息请求 (`AaBb`) 并将其解密为纯文本 (`help`)。
6. 防御中心 接收连接事件。

在内联部署中允许特定用户的已加密流量

许可证：可控性

受支持的设备：3 系列

对于来自高级保险员的所有 SSL 加密流量，系统均允许该流量通过而不进行解密，并记录连接。下图显示允许已加密流量通过的系统。



发生接下来的步骤：

1. 用户提交纯文本请求 (`help`)。客户端加密此 (`AaBb`) 并将已加密流量发送到 MedRepo 的请求部门服务器。
2. LifeIns 的路由器接收已加密流量并将其路由到请求部门服务器。
3. 受管设备不解密此流量。

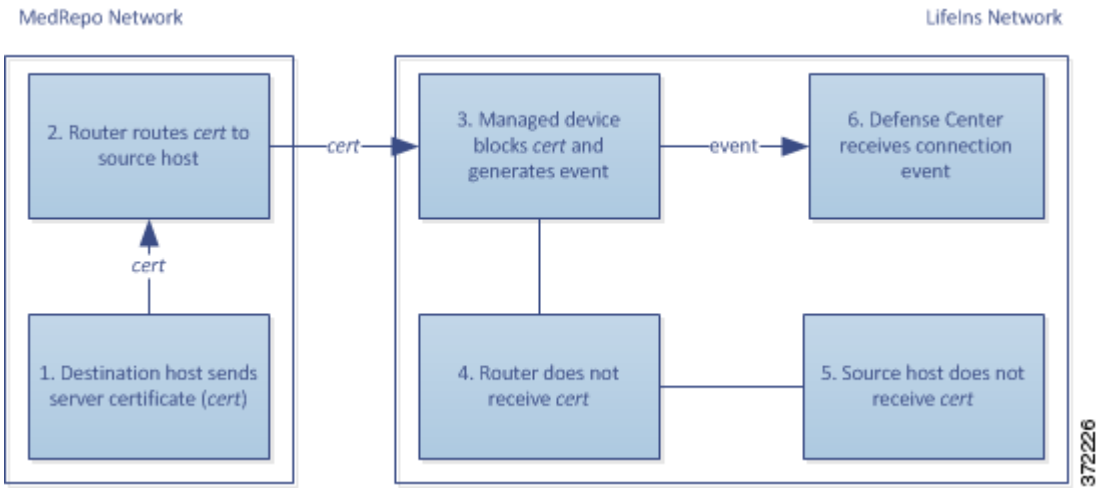
   访问控制策略继续处理已加密流量并允许其通过，然后在会话结束后生成连接事件。
4. 外部路由器接收流量并将其路由到请求部门服务器。
5. 请求部门服务器接收已加密的信息请求 (`AaBb`) 并将其解密为纯文本 (`help`)。
6. 防御中心 接收连接事件。

在内联部署中阻止已加密的流量

许可证：任何环境

受支持的设备：3 系列

对于从 LifeIns 的保险部门错误发送到 MedRepo 的客户服务部门的所有 SMTPS 邮件流量，系统在 SSL 握手期间均阻止该流量不进行进一步检查，并记录连接。下图说明阻止已加密流量的系统。



发生接下来的步骤：

1. 客户服务部门服务器从客户端浏览器收到建立 SSL 握手的请求后，客户服务部门服务器向 LifeIns 保险员发送服务器证书 (`cert`) 作为 SSL 握手的下一步。
2. MedRepo 的路由器接收证书并将其路由到 LifeIns 保险员。
3. 受管设备阻止流量并且不执行进一步检查，然后终止 TCP 连接。设备生成连接事件。
4. 内部路由器不会接收阻止的流量。
5. 保险员不会接收阻止的流量。
6. 防御中心 接收连接事件。

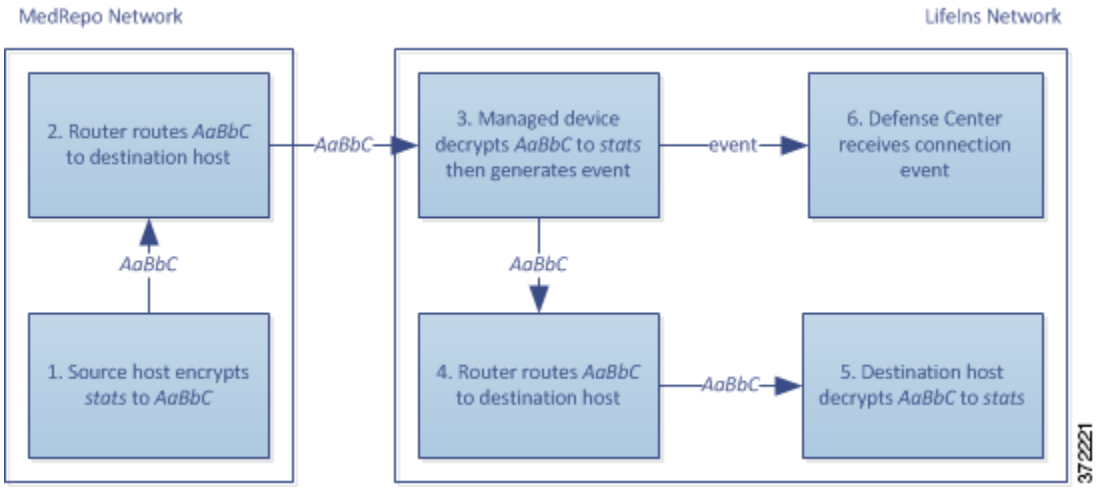
在内联部署中使用私钥检查已加密的流量

许可证：任何环境

受支持的设备：3 系列

对于从 MedRepo 发送到 LifeIns 保险部门的所有 SSL 加密流量，系统将使用上载的服务器私钥来获取会话密钥，然后解密流量并记录连接。合法流量将被允许通过并在发送到保险部门之前重新加密。

下图说明使用已知私钥解密已加密流量，然后使用访问控制检查流量并允许已解密流量的系统。

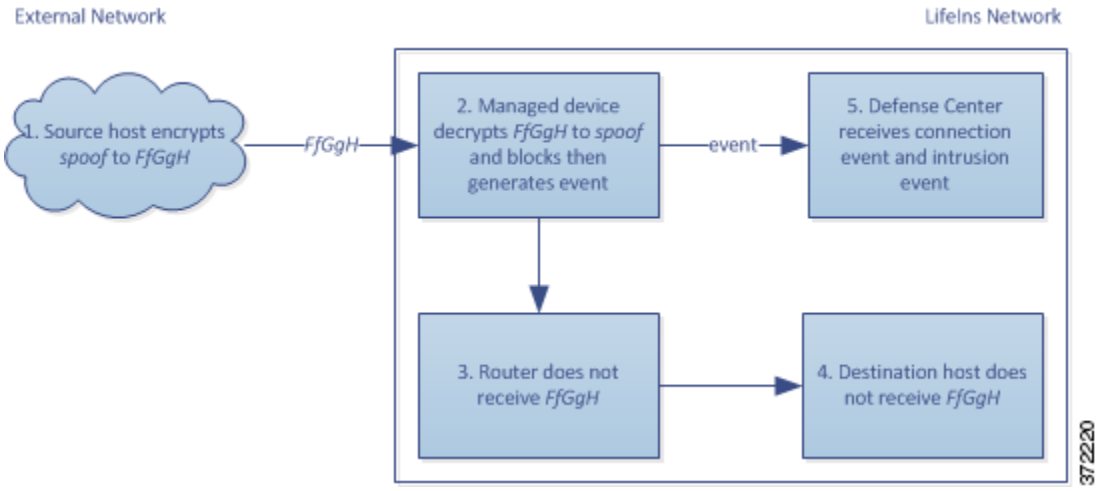


发生接下来的步骤：

1. 用户提交纯文本请求 (stats)。客户端加密此 (AaBbC) 并将已加密流量发送到保险部门服务器。
2. 外部路由器接收流量并将其路由到保险部门服务器。
3. 受管设备使用通过上载的已知私钥获取的会话密钥将此流量解密为纯文本 (stats)。

   访问控制策略继续使用自定义入侵策略处理已解密的流量，且不查找欺骗尝试。设备传输已加密流量 (AaBbC)，然后在会话结束后生成连接事件。
4. 内部路由器接收流量并将其路由到保险部门服务器。
5. 保险部门服务器接收已加密信息 (AaBbC) 并将其解密为纯文本 (stats)。
6. 防御中心接收到包含有关已加密和解密流量的信息的连接事件。

相反，实际为欺骗尝试的任何已解密流量将被丢弃。系统记录连接和欺骗尝试。下图表说明使用已知私钥解密已加密流量，然后使用访问控制策略检查流量并阻止已解密流量的系统。



发生接下来的步骤：

1. 用户提交纯文本请求 (`spoof`)，将流量修改为像是来自 MedRepo, LLC。客户端加密此 (`FfGgH`) 并将已加密流量发送到保险部门服务器。
2. 受管设备使用通过上载的已知私钥获取的会话密钥将此流量解密为纯文本 (`spoof`)。

   访问控制策略继续使用自定义入侵策略处理已解密的流量，且查找欺骗尝试。设备阻止流量，然后生成入侵事件。设备在会话结束后生成连接事件。
3. 内部路由器不会接收阻止的流量。
4. 保险部门服务器不会接收阻止的流量。
5. 防御中心接收包含有关已加密和解密流量的信息的连接事件，以及欺骗尝试的入侵事件。

在内联部署中使用重签证书检查特定用户的已加密流量

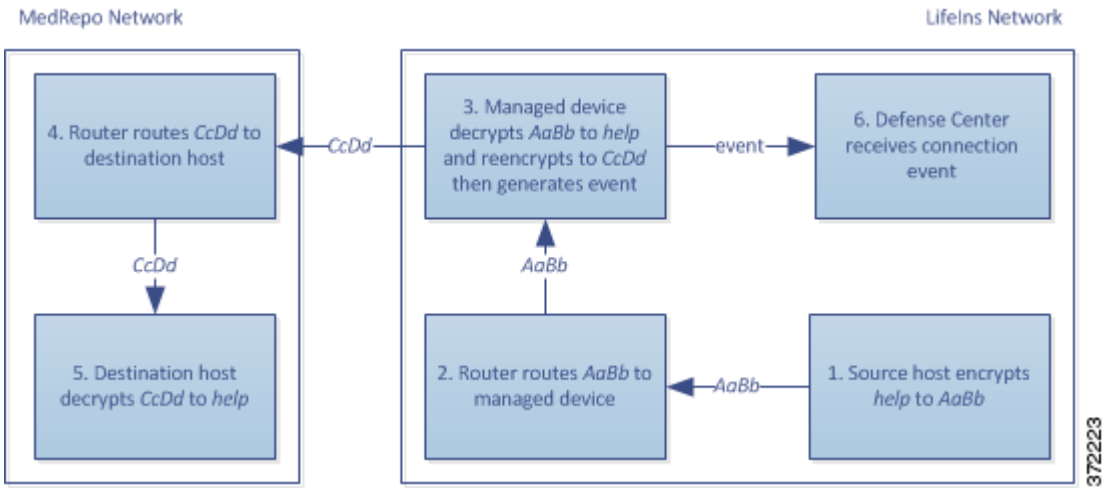
许可证：可控性

受支持的设备：3 系列

对于从新保险员和初级保险员向 MedRepo 请求部门发送的所有 SSL 加密流量，系统将使用重签服务器证书来获取会话密钥，然后解密流量并记录连接。合法流量将被允许通过并在发送到 MedRepo 之前重新加密。

注　当在内联部署中通过重签服务器证书解密流量时，设备作为中间人。它创建两个 SSL 会话，一个是客户端与受管设备之间的会话，一个是受管设备与服务器之间的会话。因此，每个会话包含不同的加密会话详细信息。

下图说明使用重签服务器证书和私钥解密已加密流量，然后使用访问控制检查流量并阻止已解密流量的系统。



发生接下来的步骤：

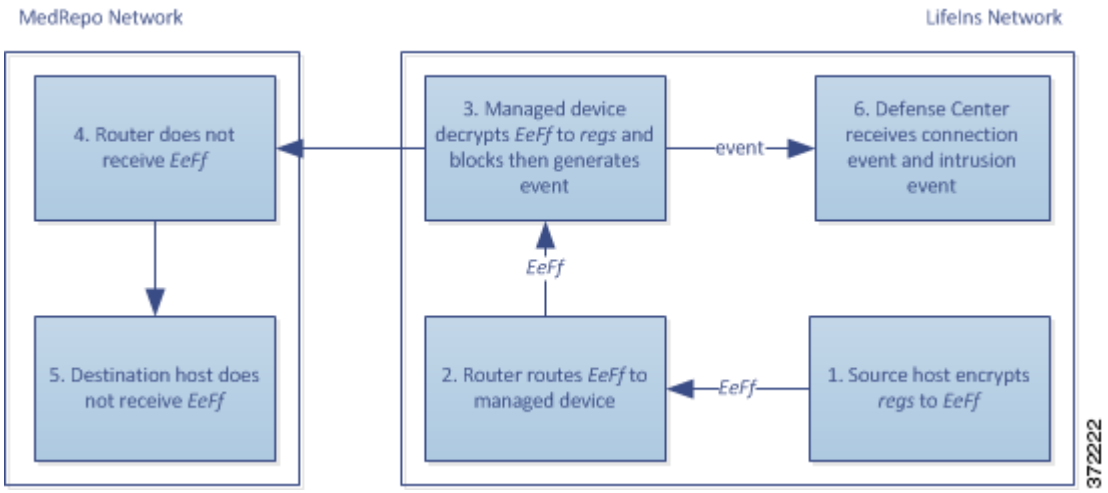
1. 用户提交纯文本请求 (`help`)。客户端加密此 (`AaBb`) 并将已加密流量发送到请求部门服务器。
2. 内部路由器接收流量并将其路由到请求部门服务器。

3. 受管设备使用通过重签服务器证书获取的会话密钥和私钥将此流量解密为纯文本 (help)。

   访问控制策略继续使用自定义入侵策略处理已解密的流量，且不查找不当请求。设备重新加密流量 (CcDd)，允许其通过。设备在会话结束后生成连接事件。
4. 外部路由器接收流量并将其路由到请求部门服务器。
5. 请求部门服务器接收已加密信息 (CcDd) 并将其解密为纯文本 (help)。
6. 防御中心接收到包含有关已加密和解密流量的信息的连接事件。

注 使用重签服务器证书加密的流量会导致浏览器警告，指出证书不受信任。要避免此问题，请将 CA 证书添加到组织的域根受信任证书存储或客户端受信任证书存储。

相反，包含不符合法规要求的任何已解密流量均将被丢弃。系统记录连接和不符信息。下图说明使用重签服务器证书和私钥解密已加密流量，然后使用访问控制策略检查流量并阻止已解密流量的系统。



发生接下来的步骤：

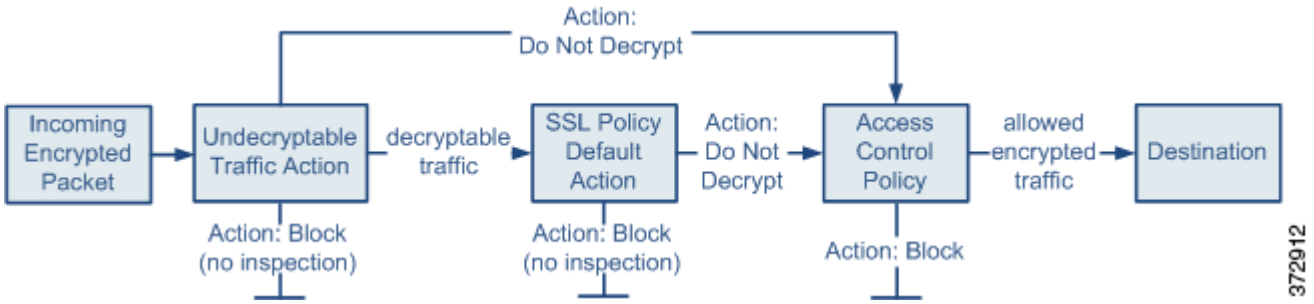
1. 用户提交不符合法规要求的纯文本请求 (regs)。客户端加密此 (EeFf) 并将已加密流量发送到请求部门服务器。
2. 内部路由器接收流量并将其路由到请求部门服务器。
3. 受管设备使用通过重签服务器证书获取的会话密钥和私钥将此流量解密为纯文本 (regs)。

   访问控制策略继续使用自定义入侵策略处理已解密流量并查找不当请求。设备阻止流量，然后生成入侵事件。设备在会话结束后生成连接事件。
4. 外部路由器不会接收阻止的流量。
5. 请求部门服务器不会接收阻止的流量。
6. 防御中心接收到包含有关已加密和解密流量的信息的连接事件，以及不当请求的入侵事件。

SSL 策略使用入门

*SSL 策略*决定系统如何处理网络上的加密流量。可以配置一个或多个 SSL 策略。您将 SSL 策略与访问控制策略相关联，然后将访问控制策略应用于受管设备。当设备检测到 TCP 握手时，访问控制策略首先处理并检查流量。如果它随后识别出通过 TCP 连接建立的 SSL 加密会话，则 SSL 策略将接管、处理和解密已加密的流量。您当前可以将一个 SSL 策略应用于 3 系列设备。

最简单的 SSL 策略如下图所示，它引导其应用所在设备使用单个默认操作处理已加密的流量。可将默认操作设置为阻止可解密流量，无需进一步检查，或者使用访问控制检查未解密的可解密流量。然后系统可以允许或阻止已加密的流量。如果设备检测到无法解密的流量，它会阻止该流量，无需进一步检查或不对其进行解密，而是使用访问控制对其进行检查。



本章介绍如何创建和应用简单 SSL 策略。本章还包含有关管理 SSL 策略的基本信息：编辑、更新和比较等。有关详细信息，请参阅：

- 第 20-2 页上的创建基本 SSL 策略
- 第 20-6 页上的编辑 SSL 策略
- 第 20-8 页上的使用访问控制应用解密设置
- 第 20-9 页上的生成当前流量解密设置的报告
- 第 20-10 页上的比较 SSL 策略

更为复杂的 SSL 策略可通过不同的操作处理不同类型无法解密的流量，根据证书颁发机构 (CA) 是否颁发或信任加密证书而控制流量，以及使用 SSL 规则对已加密流量的日志记录和处理进行精细控制。这些规则可能很简单，也可能很复杂，使用多个条件匹配和检查已加密的流量。在创建基本的 SSL 策略后，有关根据您的部署对其进行定制的详细信息，请参阅以下章节：

- 第 3-1 页上的管理可重用对象介绍如何配置可重复使用的公钥基础架构 (PKI) 对象和其他 SSL 检查相关对象增强对已加密流量的控制并解密流量。
- 第 38-1 页上的记录网络流量中的连接介绍如何配置已加密流量（无论是否可解密）的日志记录。
- 第 20-8 页上的使用访问控制应用解密设置介绍如何将 SSL 策略与访问控制策略相关联。

- 第 12-1 页上的访问控制策略入门介绍如何将访问控制策略应用于设备。
- 第 14-1 页上的使用访问控制规则调整流量介绍如何配置访问控制规则以检查已解密的流量。
- 第 21-1 页上的 SSL 规则入门介绍如何配置 SSL 规则以处理和记录已加密的流量。
- 第 22-1 页上的使用 SSL 规则调整流量解密介绍如何配置 SSL 规则条件以更好地匹配特定已加密流量。

创建基本 SSL 策略

许可证：任何环境

受支持的设备：3 系列

新建 SSL 策略时，必须至少提供一个唯一名称并指定策略默认操作。选择新策略的默认操作时，有以下的选项：

- **Do not decrypt** 创建具有 Do not decrypt 默认操作的策略。
- **Block** 创建具有 Block 默认操作的策略。
- **Block with reset** 创建具有 Block with reset 默认操作的策略。

创建 SSL 策略后，可以修改默认操作。如需选择默认操作方面的指导，请参阅第 20-3 页上的为已加密流量设置默认处理和检查。

新的 SSL 策略还包含系统无法解密的流量的默认操作：它或者继承您刚刚为无法解密的流量选择的默认操作，阻止该流量，或者不解密该流量并使用访问控制对其进行检查。创建 SSL 策略后，可以修改无法解密的流量操作。有关选择无法解密的流量操作的指导，请参阅第 20-4 页上的为无法解密的流量设置默认处理

在 SSL 策略页面 (**Policies > SSL**) 上，您可以按名称（带有可选说明）查看所有当前 SSL 策略。此页上的选项可供您比较策略、新建策略、复制策略、查看列出了每个策略中最近保存的所有设置的报告、编辑策略或删除策略。

提示 您可以从部署中的其他防御中心导出或向其导入 SSL 策略。有关详细信息，请参阅第 A-1 页上的导入和导出配置。

下表介绍了可在 SSL 策略页面上执行的策略管理操作。

表 20-1　SSL 策略管理操作

要.....	您可以.....
新建 SSL 策略	点击 **New Policy**。有关详细信息，请参阅第 20-2 页上的创建基本 SSL 策略。
修改现有 SSL 策略中的设置	点击编辑图标 ( )。有关详细信息，请参阅第 20-6 页上的编辑 SSL 策略。
比较 SSL 策略	点击 **Compare Policies**。有关详细信息，请参阅第 20-10 页上的比较 SSL 策略。
复制 SSL 策略	点击复制图标 ( )。有关编辑已复制策略的详细信息，请参阅第 20-6 页上的编辑 SSL 策略。
查看列出了 SSL 策略中当前配置设置的 PDF 报告	点击报告图标 ( )。有关详细信息，请参阅第 20-9 页上的生成当前流量解密设置的报告。
删除 SSL 策略	点击删除图标 （ ），然后点击 **OK**。当系统提示是否继续时，还会告知您是否有其他用户在策略中有未保存的更改。

要创建 SSL 策略，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > SSL**。

系统将显示 SSL Policy 页面。

步骤 2　点击 **New Policy**。

系统将显示 New SSL Policy 弹出窗口。

步骤 3　在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

可以使用所有的可打印字符，包括空格和特殊字符，。

步骤 4　指定 **Default Action**。

请注意，创建 SSL 策略后，可以修改选定的默认操作。有关详细信息，请参阅第 20-3 页上的为已加密流量设置默认处理和检查。

步骤 5　点击 **Save**。

系统将显示 SSL Policy Editor 页面。有关详细信息，请参阅第 20-6 页上的编辑 SSL 策略。

为已加密流量设置默认处理和检查

许可证：任何环境

受支持的设备：3 系列

SSL 策略的默认操作确定系统如何处理与策略中任何非监控规则不匹配的无法解密的已加密流量。当您应用不包含任何 SSL 规则的 SSL 策略时，默认操作确定如何处理网络上的所有无法解密的流量。有关系统如何处理无法解密的已加密流量的详细信息，请参阅第 20-4 页上的为无法解密的流量设置默认处理。

下表列出了可选择的默认操作，以及它们对已加密流量的影响。请注意，对于默认操作阻止的已加密流量，系统不会执行任何类型的检查。

表 20-2　　SSL 策略默认操作

默认操作	对已加密流量的影响
阻止	阻止 SSL 会话，无需进一步检查
阻止并重置	阻止 SSL 会话并且无需进一步检查，然后重置 TCP 连接
不解密	使用访问控制检查已加密的流量

首次创建 SSL 策略时，默认情况下将禁用记录默认操作所处理的连接。在创建策略后，可以修改此设置以及默认操作本身。

以下操作步骤解释在编辑策略时如何为 SSL 策略设置默认操作。有关编辑 SSL 策略的完整操作步骤，请参阅第 20-6 页上的编辑 SSL 策略。

要设置 SSL 策略的默认操作，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > SSL**。

系统将显示 SSL Policy 页面。

步骤 2　点击要配置的 SSL 策略旁的编辑图标 ( )。

系统将显示 SSL 策略编辑器。

步骤 3　选择 **Default Action**。有关详细信息，请参阅SSL 策略默认操作表。

步骤 4　如第 38-11 页上的记录可用 SSL 规则解密的连接所述，配置默认操作的日志记录选项。

步骤 5　点击 **Save**。

系统将显示 SSL Policy Editor 页面。有关详细信息，请参阅第 20-6 页上的编辑 SSL 策略。

为无法解密的流量设置默认处理

许可证：任何环境

受支持的设备：3 系列

您可以在 SSL 策略级别设置无法解密的流量操作以处理系统无法解密或检查的某些类型的已加密流量。当您应用不包含任何 SSL 规则的 SSL 策略时，无法解密的流量操作确定如何处理网络上的所有无法解密的已加密流量。

视乎无法解密的流量类型，您可以选择：

- 阻止连接
- 阻止连接，然后重置连接
- 使用访问控制检查已加密的流量
- 继承 SSL 策略的默认操作

下表介绍了无法解密的流量类型：

表 20-3　　无法解密的流量类型

类型	说明	默认操作	可执行的操作
压缩的会话	此 SSL 会话应用数据压缩方法。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
SSLv2 会话	此会话使用 SSL V2 加密。 请注意，如果客户端 hello 消息为 SSL 2.0，并且已传输流量的剩余部分为 SSL 3.0，则流量可解密。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作

表 20-3　无法解密的流量类型

类型	说明	默认操作	可执行的操作
未知密码套件	系统无法识别该密码套件。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
不受支持的密码套件	系统不支持根据检测到的密码套件进行解密。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
会话无法缓存	SSL 会话已启用会话重复使用，客户端和服务器使用会话标识符重新建立了该会话，并且系统未缓存该会话标识符。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
握手错误	在 SSL 握手协商时出错。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
解密错误	在流量解密时出错。	阻止	阻止 阻止并重置

首次创建 SSL 策略时，默认情况下将禁用记录默认操作所处理的连接。由于默认操作的日志记录设置也适用于无法解密的流量处理，默认情况下也将禁用记录无法解密的流量操作所处理的连接。有关配置默认日志记录的详细信息，请参阅第 38-11 页上的记录可用 SSL 规则解密的连接。

注　如果在客户端与受管设备之间放置 HTTP 代理，且使用 CONNECT HTTP 方法在客户端与和服务器之前建立隧道化 SSL 连接，则系统将无法解密流量。**Handshake Errors** 无法解密的操作确定系统如何处理此流量。有关详细信息，请参阅第 21-9 页上的解密操作：解密流量以进一步检查。

要为无法解密的流量设置默认处理，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > SSL**。

系统将显示 SSL Policy 页面。

步骤 2　点击要配置的 SSL 策略旁的编辑图标 ( )。

系统将显示 SSL 策略编辑器。

步骤 3　选择 **Undecryptable Actions** 选项卡。

系统将显示 Undecryptable Actions 选项卡。

步骤 4　对于每个字段，选择要对无法解密的流量类型执行的操作，或者，是否要应用 SSL 策略的默认操作。有关详细信息，请参阅 SSL 策略默认操作表。

步骤 5　点击 **Save**，以保存更改。

您必须应用关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

编辑 SSL 策略

许可证：任何环境

受支持的设备：3 系列

在 SSL 策略编辑器上，可以配置策略和排列 SSL 规则。要配置 SSL 策略，必须为策略提供唯一的名称并指定默认操作。您还可以：

- 添加、编辑、删除、启用和禁用 SSL 规则
- 添加受信任 CA 证书
- 确定系统无法解密的已加密流量的处理
- 记录由默认操作和无法解密的流量操作处理的流量

在创建或修改 SSL 策略后，可以将其与访问控制策略关联，然后应用该访问控制策略。还可以创建自定义用户角色，这些角色允许将不同的权限分配给不同的用户，以供配置、组织和应用策略。

下表总结了在 SSL 策略编辑器中可执行的配置操作。

表 20-4　　SSL 策略配置操作

要.....	**您可以.....**
修改策略的名称或说明	点击名称或描述字段，视需要删除任意字符，然后键入新的名称或描述。
设置默认操作	在第 20-3 页上的为已加密流量设置默认处理和检查中查找详细信息。
设置无法解密的流量的默认处理	在第 20-4 页上的为无法解密的流量设置默认处理中查找详细信息。
记录默认操作和无法解密的流量操作的连接	在第 38-11 页上的记录可用 SSL 规则解密的连接中查找详细信息。
添加受信任 CA 证书	在第 22-20 页上的信任外部证书颁发机构中查找详细信息。
将不同的权限分配给不同的用户	在第 19-3 页上的使用自定义用户角色管理您的 SSL 检查部署中查找详细信息。
保存策略更改	点击 **Save**。
取消策略更改	点击 **Cancel**，然后点击 **OK**（如果进行了更改）。
将规则添加到策略	点击 **Add Rule**。有关详细信息，请参阅第 21-4 页上的了解和创建 SSL 规则。 **提示**　还可以右键单击规则的行的空白区域，并选择 **Insert new rule**。
编辑现有规则。	点击要编辑的规则旁的编辑图标 ( )。有关详细信息，请参阅第 21-4 页上的了解和创建 SSL 规则。 **提示**　还可以右键单击要编辑的规则并选择 **Edit**。
删除规则	点击要删除的规则旁边的删除图标 ( )，然后点击 **OK**。 **提示**　还可以右键单击选定规则行的空白区域，选择 **Delete**，然后点击 **OK** 删除一个或多个选定的规则。

表 20-4　SSL 策略配置操作（续）

要.....	您可以.....
启用或禁用现有规则	右键单击选定的规则，选择 **State**，然后选择 **Disable** 或 **Enable**。被禁用的规则在规则名称下方呈灰色显示并带有相应的标记 (`disabled`)。
显示特定规则属性的配置页面	在规则行上点击条件列中的名称、值或图标。例如，点击 **Source Networks** 列中的名称或值，以便显示选定规则的 Networks 页面。有关详细信息，请参阅第 22-1 页上的使用 SSL 规则调整流量解密。

更改配置时，会有消息提示您有未保存的更改。要保留更改，在退出策略编辑器前，必须保存策略。如果未保存更改就尝试退出策略编辑器，则系统会提醒您有未保存的更改；您可以放弃更改并退出策略，或者返回到策略编辑器。

为保护会话隐私，在策略编辑器上 60 分钟未执行任何操作之后，将放弃对策略做出的更改，且将返回 SSL Policy 页面。无活动时间的前 30 分钟过后，屏幕上将会显示一条消息，并会定期更新以提供更改被放弃前的剩余分钟数。在页面上进行任何操作都会取消定时器。

当您尝试在两个浏览器窗口中编辑同一策略时，系统会询问您要执行以下何种操作：在新窗口中恢复编辑；放弃在原始窗口中所做的更改并继续在新窗口中进行编辑；取消第二个窗口并返回到策略编辑器。

当多个用户并发地编辑同一策略时，策略编辑器上将显示一条消息，指明尚未保存更改的共他用户。当有用户尝试保存更改时，系统会提醒他们其更改会覆盖其他用户所做的更改。当多个用户保存相同的策略时，最后保存的更改将会保留。

要编辑 SSL 策略，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > SSL**。

系统将显示 SSL Policy 页面。

步骤 2　点击要配置的 SSL 策略旁的编辑图标 ( )。

系统将显示 SSL Policy Editor页面。

步骤 3　有以下选项可供选择：

- 要配置策略，可以采取 SSL 策略配置操作表中概述的任何操作。
- 要排列策略中的规则，您可以执行第 21-10 页上的管理策略中的 SSL 规则中所述的任何操作。

步骤 4　保存或放弃配置。有以下选项可供选择：

- 要保存更改并继续编辑，请点击 **Save**。
- 要放弃更改，请点击 **Cancel**；如果出现提示，点击 **OK**。

  系统将放弃更改并显示 SSL Policy 页面。

使用访问控制应用解密设置

许可证：任何环境

受支持的设备：3 系列

在对 SSL 策略做出任何更改之后，必须应用与其关联的访问控制策略。有关详细信息，请参阅第 12-13 页上的应用访问控制策略。

应用 SSL 策略时，请谨记以下几点：

- 不能删除已应用或正在应用的 SSL 策略。
- 应用访问控制策略会自动应用关联的 SSL 策略。无法独立应用 SSL 策略。

注 在被动部署中，系统无法影响流量。如果您尝试应用的访问控制策略引用了将阻止已加密流量或通过重新签署服务器证书而被配置为解密流量的 SSL 策略，则系统将显示警告。此外，被动部署不支持解密采用瞬时 Diffie-Hellman (DHE) 或椭圆曲线 Diffie-Hellman (ECDHE) 密码套件加密的流量。

要将 SSL 策略与访问控制策略相关联，请执行以下操作：

访问：管理员/安全审批者

步骤 1 选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2 点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3 选择 **Advanced** 选项卡。

屏幕上将会显示访问控制策略的高级设置。

步骤 4 点击 General Settings 旁的编辑图标 ( )。

系统将显示 General Settings 弹出窗口。

步骤 5 从 **SSL Policy to use for inspecting encrypted connections** 下拉列表中选择 SSL 策略。

步骤 6 点击 **OK**。

屏幕上将会显示访问控制策略的高级设置。

步骤 7 点击 **Save**，以保存更改。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

生成当前流量解密设置的报告

许可证：任何环境

SSL 策略报告是对特定时间点的策略和规则配置的记录。报告可用于审核或检查当前配置。

提示 还可以生成 SSL 比较报告，用以将某个策略与当前应用的策略或其他策略作比较。有关详细信息，请参阅第 20-10 页上的比较 SSL 策略。

SSL 策略报告包含下表所述的各个部分。

表 20-5　　SSL 策略报告部分

部分	说明
标题页	确定策略报告的名称、策略最后修改的日期与时间以及进行修改的用户。
目录	说明报告的内容。
策略信息	提供策略的名称和说明、上次修改策略的用户的名称以及策略上次修改的日期和时间
默认操作	提供默认操作。
默认日志记录	提供默认连接日志记录设置。
规则	按规则类别提供策略中的每个规则的规则操作和条件。
受信任 CA 证书	提供自动受信任的 CA 证书（如果检测到的流量使用这些证书或信任链中的其他证书进行加密）。
无法解密的操作	提供对系统检测到的无法解密的流量类型执行的操作。
引用的对象	按配置对象所依据的条件类型 （网络、 VLAN 标记等），提供策略中使用的所有个别对象和对象组的名称和配置。

要查看 SSL 策略报告，请执行以下操作：

访问：管理员/访问管理员/网络管理员/安全审批人

步骤 1　选择 **Policies > SSL**。

系统将显示 SSL Policy 页面。

步骤 2　点击要生成报告的策略旁的报告图标 ( )。生成 SSL 策略报告之前，请记住要保存所有更改；报告中只会显示已保存的更改。

系统将会生成报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

比较 SSL 策略

许可证：任何环境

要查看策略更改是否符合贵组织的标准或优化系统性能，可以检查这两个 SSL 策略之间的区别。可以比较任意两个策略，也可以将当前应用的策略与另一策略进行比较。在进行比较后，或者生成 PDF 报告来记录两个策略之间的差异。

有两个可以用来比较策略的工具：

- 比较视图仅会以并排格式显示两个策略之间的差异。每个策略的名称将会显示在比较视图左侧和右侧的标题栏中，当选择 **Running Configuration** 时除外，在这种情况下，空白栏代表当前的活动策略。

  可以使用此工具来在 Web 界面中查看和导航两个策略（在其差异突出显示的情况下）。

- 比较报告会以类似策略报告的格式（但采用 PDF 格式）创建仅有两个策略之间的差异的记录。

  可以使用此工具来保存、复制、打印和共享策略比较，供未来检查使用。

如需了解和使用策略比较工具的更多相关信息，请参阅：

- 第 20-10 页上的使用 SSL 策略比较视图
- 第 20-11 页上的使用 SSL 策略比较报告

使用 SSL 策略比较视图

许可证：任何环境

比较视图会以并排格式显示两个策略，每个策略由比较视图左侧和右侧标题栏中的名称确定。比较运行配置之外的两个策略时，最后修改的时间和最后修改的用户将会随策略名称显示。两个策略之间的差异将会突出显示：

- 蓝色指示突出显示的设置在两个策略中不同，不同之处以红色文本标注。
- 绿色指示突出显示的设置在一个策略中存在，但在另一个策略中不存在。

您可以执行下表中的任何操作。

表 20-6　　SSL 策略比较视图操作

要.....	您可以.....
逐一浏览更改	点击标题栏上方的 **Previous** 或 **Next**。 在左右两侧之间以双箭头图标 (◂▸) 为中心移动， **Difference** 数字调整为识别您正在查看哪个差异。
生成新的策略比较视图	点击 **New Comparison**。 系统将显示 **Select Comparison** 窗口。有关详细信息，请参阅第 20-11 页上的使用 SSL 策略比较报告。
生成策略比较报告	点击 **Comparison Report**。 策略比较报告将会创建仅列出两个策略之间的差异的 PDF 文档。

使用 SSL 策略比较报告

许可证：任何环境

SSL 策略比较报告是策略比较视图中识别出的两个 SSL 策略之间或者某个策略与当前应用的策略之间所有差异的记录，其文件格式为 PDF。可以使用此报告来进一步检查两个策略配置之间差异，以及保存和分发比较结果。

对于您能够访问的任何策略，都可以通过比较视图生成 SSL 策略比较报告。在生成策略报告前，切记保存所有更改，只有已保存的更改会在报告中显示。

策略比较报告的格式与策略报告相同，有一处例外：策略报告包含策略中的所有配置，而策略比较报告仅列出策略之间的那些不同配置。SSL 策略比较报告包含第 20-9 页上的生成当前流量解密设置的报告中描述的部分。

提示　您可以使用类似的操作步骤比较访问控制、网络分析、入侵、文件、系统或运行状况策略。

要比较两个 SSL 策略，请执行以下操作：

访问：管理员/访问管理员/网络管理员/安全审批人

步骤 1　选择 **Policies > SSL**。

系统将显示 SSL 策略。

步骤 2　点击 **Compare Policies**。

系统将显示 Select Comparison 窗口。

步骤 3　从 **Compare Against** 下拉列表中选择要进行比较的类型：

- 要比较两个不同的策略，请选择 **Other Policy**。

  页面将会刷新，并显示 Policy A 和 Policy B 下拉列表。
- 要将另一策略与当前活动的策略进行比较，请选择 **Running Configuration**。

  页面将会刷新，并会显示 Target/Running Configuration A 和 Policy B 下拉列表。

步骤 4　根据您选择的比较类型，有以下选项可供选择：

- 如果您比较两个不同的策略，请从 Policy A 和 Policy B 下拉列表中选择要比较的策略。
- 如果您将正运行的配置与另一策略进行比较，请从 Policy B 下拉列表中选择第二个策略。

步骤 5　点击 **OK** 显示策略比较视图。

系统将显示比较视图。

步骤 6　或者，点击 **Comparison Report** 以生成 SSL 策略比较报告。

系统将显示 SSL 策略比较报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

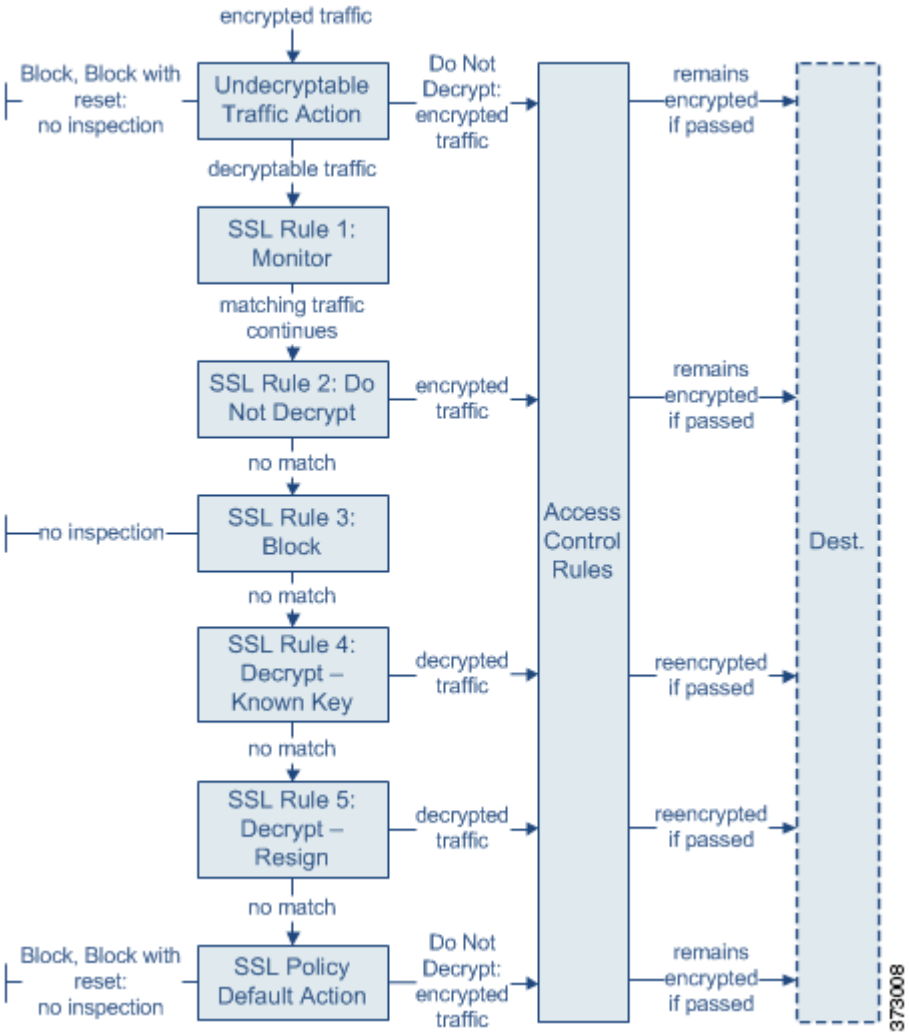
SSL 规则入门

在 SSL 策略中， *SSL 规则*提供一种精细的方法来跨多台受管设备处理加密流量：阻止流量而不进一步检查；不解密流量并通过访问控制对其进行检查；或者解密流量以进行访问控制分析。

系统会按照您所指定的顺序将流量与 SSL 规则相匹配。在大多数情况下，系统根据*第一个* SSL 规则（使用规则的*所有*条件来匹配流量）处理加密流量。条件可以简单也可以复杂；可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书可分辨名称、证书状态、密码套件或加密协议版本来控制流量。

每个规则也包含*操作*，用于确定在解密匹配流量后通过访问控制对匹配流量进行的选择性处理：监控、阻止或检查。请注意，系统**不会**进一步检查其阻止的加密流量，而是会通过访问控制来检查加密流量和无法解密的流量。但是，某些访问控制规则条件需要未加密流量，因此，加密流量可能匹配的规则更少。此外，默认情况下，系统禁用加密负载的入侵和文件检测。

下述场景概括说明了 SSL 规则在内联部署中处理流量的方式。



在此场景中，按如下方式评估流量：

- 第一， **Undecryptable Traffic Action** 评估加密流量。对于系统无法解密的流量，系统会将其阻止而不进一步检查，或者使其通过以进行访问控制检查。不匹配的加密流量继续根据下一规则进行评估。
- 第二，使用 **SSL Rule 1: Monitor** 评估加密流量。 Monitor 规则跟踪和记录加密流量，但不对流量做出任何影响。系统继续将流量与其他规则进行匹配，以确定允许还是拒绝该流量。
- 第三，使用 **SSL Rule 2: Do Not Decrypt** 评估加密流量。匹配流量未解密；系统通过访问控制检查此流量，但不执行文件或入侵检测。不匹配的流量继续根据下一规则进行评估。
- 第四，使用 **SSL Rule 3: Block** 评估加密流量。匹配流量被阻止而不进一步检查。不匹配的流量继续根据下一规则进行评估。
- 第五，使用 **SSL Rule 4: Decrypt - Known Key** 评估加密流量。系统使用您上传的私钥对传入网络的匹配流量进行解密。然后，根据访问控制规则评估解密流量。访问控制规则以相同方式处理已解密和未加密的流量。作为此额外检查的结果，系统可以阻止流量。所有剩余流量将被重新加密，才会被传输到目标。与 SSL 规则不匹配的流量继续根据下一规则进行评估。

- **SSL Rule 5: Decrypt - Resign** 是最终规则。如果流量与此规则相匹配，则系统使用已上传的 CA 证书对服务器证书重新签名，然后充当中间人解密流量。然后，根据访问控制规则评估解密流量。访问控制规则以相同方式处理已解密和未加密的流量。作为此额外检查的结果，系统可以阻止流量。所有剩余流量将被重新加密，才会被传输到目标。与 SSL 规则不匹配的流量继续根据下一规则进行评估。
- **SSL Policy Default Action** 处理所有不与任何 SSL 规则相匹配的流量。默认操作为以下两种方式之一：阻止加密流量，且不进一步检查；不解密流量而允许传输，以进行访问控制检查。

有关详细信息，请参阅以下各节：

- 第 21-3 页上的配置支持检查信息
- 第 21-4 页上的了解和创建 SSL 规则
- 第 21-10 页上的管理策略中的 SSL 规则

配置支持检查信息

许可证：任何环境

您必须创建可重用公共密钥基础设施 (PKI) 对象才能基于加密会话特性控制加密流量并解密加密流量。可以在将受信任证书颁发机构 (CA) 证书上传到 SSL 策略并创建 SSL 规则条件，以及在此过程中创建关联对象时随时添加此信息。不过，提前配置这些对象可降低不正确创建对象的几率。

使用证书和配对密钥解密加密流量

如果通过上传用于会话加密的服务器证书和私钥来配置内部证书对象，则系统可以解密传入的加密流量。如果在包含 **Decrypt - Known Key** 操作的 SSL 规则中引用该对象并且流量与该规则相匹配，则系统会使用上传的私钥来解密会话。

如果通过上传 CA 证书和私钥来配置内部 CA 对象，则系统还可以解密传出流量。如果在包含 **Decrypt - Resign** 操作的 SSL 规则中引用该对象并且流量与该规则相匹配，则系统会对传递到客户端浏览器的服务器证书重新签名，然后充当中间人来解密会话。

有关详细信息，请参阅：

- 第 3-45 页上的使用内部证书对象
- 第 3-38 页上的使用内部证书颁发机构对象

根据加密会话特性控制流量

系统可以根据用于协商会话的密码套件或服务器证书来控制加密流量。您可以从多个不同的可重用对象中选择一个进行配置，并在 SSL 规则条件中参照该对象来匹配流量。下表介绍可以配置的不同类型的可重用对象：

如果配置.....	可以根据是否存在以下内容控制加密流量.....
包含一个或多个密码套件的密码套件列表	用于协商加密会话的密码套件与密码套件列表中的密码套件相匹配
受信任 CA 对象（通过上传组织信任的 CA 证书）	受信任 CA 根据以下情况来确定是否信任用于加密会话的服务器证书： • CA 直接颁发证书 • CA 向颁发服务器证书的中间 CA 颁发证书
外部证书对象（通过上传服务器证书）	用于加密会话的服务器证书与上传的服务器证书相匹配
包含证书主题或颁发者可分辨名称的可分辨名称对象	用于加密会话的证书上的主题或颁发者通用名称、国家/地区、组织或组织单位与已配置的可分辨名称相匹配

有关详细信息，请参阅：

- 第 3-35 页上的使用密码套件列表
- 第 3-42 页上的使用可信证书颁发机构对象
- 第 3-44 页上的使用外部证书对象
- 第 3-36 页上的使用可分辨名称对象

了解和创建 SSL 规则

许可证：任何环境

受支持的设备：3 系列

在 SSL 策略中，SSL 规则提供在多台受管设备之间处理网络流量的精细方法。除了其唯一名称之外，每个 SSL 规则都具有以下基本组件。

State

默认情况下，规则处于启用状态。如果您禁用某规则，系统将不用它来评估网络流量并停止为该规则生成警告和错误。

Position

SSL 策略中的规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

Conditions

条件指定规则处理的特定流量。条件可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书主题或颁发者、证书状态、密码套件或加密协议版本来匹配流量。条件可以简单也可以复杂；条件的使用可取决于目标设备许可证。

Action

规则操作确定系统如何处理匹配的流量。您可以对匹配的流量执行监控、信任、阻止或解密操作。解密的流量会受到进一步检查。请注意，系统不对被阻止或受信任加密流量执行检查。

Logging

规则的日志记录设置管理系统保存其处理流量的记录。可以保留与规则相匹配的流量的记录。您可以在系统阻止加密会话或允许其未经检查便通过（取决于 SSL 策略中的设置）时记录连接。无论系统稍后如何处理或检查流量，您都可以强制系统记录其解密的连接，以通过访问控制规则进一步检查。您可以将连接记录到防御中心数据库，以及系统日志 (syslog) 或 SNMP 陷阱服务器中。

提示 正确创建 SSL 规则并将其排序是一项复杂的任务，但却是构建有效部署的一项重要任务。如果不仔细规划策略，规则会彼此争抢优先级、需要其他许可证，或者包含无效的配置。为帮助确保系统按预期处理流量， SSL 策略接口具有面向规则的功能强大的警告和错误反馈系统。有关详细信息，请参阅第 21-14 页上的对 SSL 规则进行故障排除。

要创建或修改 SSL 规则，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > SSL**。

系统将显示 SSL Policy 页面。

步骤 2　点击要添加规则的 SSL 策略旁边的编辑图标 ( )。

系统将显示 SSL 策略编辑器，并停留在 Rules 选项卡。

步骤 3　您有以下选项：

- 要添加新规则，请点击 **Add Rule**。
- 要编辑现有规则，请点击要编辑的规则旁边的编辑图标 ( )。

系统将显示 SSL 规则编辑器。

步骤 4　在 **Name** 中键入规则的名称。

每个规则必须有唯一的名称。最多可以使用 30 个可打印字符，包括空格和特殊字符，但 (:) 除外。

步骤 5　配置规则组件，如上面的总结所述。可以配置以下内容或接受默认设置：

- 指定规则是否为 **Enabled**。
- 指定规则位置；请参阅第 21-5 页上的指定 SSL 规则的评估顺序。
- 在 **Action** 中选择规则操作；请参阅第 21-7 页上的使用规则操作确定加密流量处理和检查。
- 配置规则的条件；请参阅第 21-6 页上的使用条件指定规则处理的加密流量。
- 在 **Logging** 中指定日志记录选项；请参阅 第 38-11 页上的记录可用 SSL 规则解密的连接。

步骤 6　点击 **Save** 保存该规则。

要使更改生效，必须应用与 SSL 策略关联的访问控制策略；请参阅第 12-13 页上的应用访问控制策略。

指定 SSL 规则的评估顺序

许可证：任何环境

受支持的设备：3 系列

首次创建 SSL 规则时，请使用规则编辑器中的 **Insert** 下拉列表指定该规则的位置。SSL 策略中的 SSL 规则从 1 开始进行编号。系统将按照规则编号的升序顺序，自上而下将流量与 SSL 规则相匹配。

在大多数情况下，系统根据*第一个* SSL 规则（其中*所有*规则的条件都与流量相匹配）处理网络流量。除 Monitor 规则（记录流量，但不对流量做出任何影响）外，当流量与某个规则进行匹配后，系统将**不再**继续根据其他较低优先级规则评估该流量。

提示　正确的 SSL 规则顺序可减少处理网络流量所需的资源，并防止规则争抢。虽然创建的规则对于每个组织和部署而言都是唯一的，但在对可以优化性能的规则进行排序并仍然满足需求时，可以遵循一些通用准则。有关详细信息，请参阅第 21-16 页上的对 SSL 规则进行排序以提高性能和避免争抢。

除了按照编号排序规则之外，还可按类别对规则进行分组。默认情况下，系统提供三个类别：管理员、标准和根。您可以添加自定义类别，但是不能删除系统提供的类别或更改类别的顺序。有关更改现有规则的位置或类别的信息，请参阅第 21-12 页上的更改 SSL 规则的位置或类别。

要在编辑或创建规则时将规则添加到类别，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在 SSL 规则编辑器中，从 **Insert** 下拉列表中选择 **Into Category**，然后选择要使用的类别。

保存规则时，系统将其置于该类别的最后位置。

要在编辑或创建规则时按编号定位规则，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在 SSL 规则编辑器中，从 **Insert** 下拉列表中选择 **above rule** 或 **below rule**，然后键入相应的规则编号。

当保存规则时，规则已置于您指定的位置。

使用条件指定规则处理的加密流量

许可证：因功能而异

受支持的设备：3 系列

SSL 规则的条件识别该规则处理的加密流量的类型。条件可以简单也可以复杂，并且可以指定每个规则有多个条件类型。仅当流量满足规则中的所有条件时，该规则才适用于此流量。

如果不为规则配置特定条件，系统将不基于此标准匹配流量。例如，无论会话 SSL 或 TLS 版本如何，具有证书条件但不具有版本条件的规则根据用于协商会话的服务器证书来评估流量。

当添加或编辑 SSL 规则时，请使用规则编辑器下部左侧的选项卡添加和编辑规则条件。下表介绍可以向 SSL 规则中添加的条件。

表 21-1　SSL 规则条件类型

此条件.....	与加密流量相匹配.....	详细信息
Zones	通过特定安全区域的一个接口进入或离开设备	安全区域是根据部署和安全策略划分的一个或多个接口的逻辑分组。区域中的接口可能分布于多台设备上。要构建区域条件，请参阅第 22-2 页上的按网络区域控制加密流量。
Networks	按照其源或目标 IP 地址、国家/地区或大洲	可以明确指定 IP 地址。利用地理定位功能还可以根据源或目标国家/地区或大洲控制流量。要构建网络条件，请参阅第 22-3 页上的按网络或地理位置控制加密流量。
VLAN Tags	按照 VLAN 进行标记	系统使用最内部的 VLAN 标记来按照 VLAN 识别数据包。要构建 VLAN 连接，请参阅第 22-5 页上的控制加密 VLAN 流量。
Ports	按照其源端口或目标端口	可以根据 TCP 端口控制加密流量。要构建端口条件，请参阅第 22-6 页上的按端口控制加密流量。

表 21-1　SSL 规则条件类型（续）

此条件.....	与加密流量相匹配.....	详细信息
Users	按照会话中涉及的用户	根据登录到加密、受监控会话中涉及的主机的 LDAP 用户，可以控制加密流量。可以根据从 Microsoft Active Directory 服务器检索的个人用户或组控制流量。要构建用户条件，请参阅第 22-7 页上的根据用户控制加密流量。
Applications	按照会话中检测到的应用	可以控制对加密会话中单个应用的访问，或者根据基本特性（类型、风险、业务相关性和类别）过滤访问。要构建应用条件，请参阅第 22-9 页上的根据应用控制加密流量。
Categories	按会话中请求的 URL（根据证书主题可分辨名称）	可以根据 URL 的通用分类和风险级别限制网络上的用户可以访问的网站。要构建 URL 条件，请参阅第 22-13 页上的按 URL 类别和信誉控制加密流量。
Distinguished Names	按用于协商加密会话的服务器证书的主题或颁发者可分辨名称	可以根据颁发服务器证书的 CA 或服务器证书持有者来控制加密流量。要构建可分辨名称条件，请参阅第 22-17 页上的按证书可分辨名称控制加密流量。
Certificates	按用于协商加密会话的服务器证书	可以根据为协商加密会话而传递到用户浏览器的服务器证书来控制加密流量。要构建证书条件，请参阅第 22-20 页上的按证书状态控制加密流量。
Certificate Status	按用于协商加密会话的服务器证书的属性	可以根据服务器证书的状态来控制加密流量。要构建证书状态条件，请参阅第 22-20 页上的按证书状态控制加密流量。
Cipher Suites	按用于协商加密会话的密码套件	可以根据由服务器选择用于协商加密会话的密码套件来控制加密流量。要构建密码套件条件，请参阅第 22-24 页上的按密码套件控制加密流量。
Versions	按用于加密会话的 SSL 或 TLS 的版本	可以根据用于加密会话的 SSL 或 TLS 的版本来控制加密流量。要构建版本条件，请参阅第 22-25 页上的按加密协议版本控制流量。

请注意，虽然您可以使用 3 系列设备控制和检查加密流量，但是使用检测到的应用、URL 类别或用户来控制流量需要其他许可证。此外，过于复杂的规则会消耗过多资源，在某些情况下还会阻止您应用策略。有关详细信息，请参阅第 21-14 页上的对 SSL 规则进行故障排除。

使用规则操作确定加密流量处理和检查

许可证：任何环境

受支持的设备：3 系列

每个 SSL 规则都具有对匹配的加密流量确定以下处理的关联操作：

- 处理 - 首先，规则操作管理系统是监控、信任、阻止还是解密与规则条件匹配的加密流量
- 日志记录 - 规则操作确定何时以及如何记录有关匹配的加密流量的详细信息。

SSL 检查配置会处理、检查并记录解密流量：

- SSL 策略的无法解密的操作处理系统无法解密的流量；请参阅第 20-4 页上的为无法解密的流量设置默认处理。
- 策略的默认操作处理不满足任何非 Monitor SSL 规则的条件的流量；请参阅第 20-3 页上的为已加密流量设置默认处理和检查。

当系统阻止或信任加密会话时，可以记录连接事件。无论系统稍后如何处理或检查流量，您都可以强制系统记录其解密的连接，以通过访问控制规则进一步检查。加密会话的连接日志包含有关加密的详细信息，例如用于加密该会话的证书。只能记录连接结束事件，但是：

- 对于被阻止连接 (Block、Block with reset)，系统立即结束会话并生成事件
- 对于受信任连接 (Do not decrypt)，系统在会话结束时生成事件

有关规则操作及其如何影响处理和日志记录的详细信息，请参阅以下各节：

- 第 21-8 页上的 Monitor 操作：延迟操作并确保日志记录
- 第 21-8 页上的不解密操作：通过加密流量而不检查
- 第 21-8 页上的阻止操作：阻止加密流量而不检查
- 第 21-9 页上的解密操作：解密流量以进一步检查
- 第 21-10 页上的管理策略中的 SSL 规则

Monitor 操作：延迟操作并确保日志记录

许可证：任何环境

受支持的设备：3 系列

Monitor 操作不影响加密流量；既不会立即允许也不会拒绝匹配流量。相反，系统会根据其他规则（如果有）来匹配流量，以确定信任、阻止还是解密该流量。所匹配的第一个非 Monitor 规则确定流量和任何进一步的检查。如果没有其他匹配的规则，系统使用默认操作。

由于 Monitor 规则的主要目的是跟踪网络流量，因此系统会自动记录监控流量的连接结束事件。即是说，无论后续处理连接的规则或默认操作的日志记录配置如何，系统都始终会将连接结束事件记录到防御中心数据库。换句话说，如果数据包匹配 Monitor 规则，即使数据包不匹配其他规则，并且您不对默认操作进行日志记录，系统也始终记录该连接。

不解密操作：通过加密流量而不检查

许可证：任何环境

受支持的设备：3 系列

Do not decrypt 操作使加密流量通过，以通过访问控制策略的规则和默认操作进行评估。由于某些访问控制规则条件需要未加密的流量，因此该流量可能与较少的规则相匹配。系统无法对加密流量执行深入检查，例如入侵或文件检查。

阻止操作：阻止加密流量而不检查

许可证：任何环境

受支持的设备：3 系列

Block 和 **Block with reset** 操作类似于访问控制规则操作 Block 和 Block with reset。这些操作防止客户端和服务器建立 SSL 加密会话并允许加密流量通过。 Block with reset 规则也会重置连接。

请注意，系统不会显示被阻止加密流量的已配置响应页面。相反，请求禁止 URL 的用户需要重置其连接，否则连接会超时。有关详情，请参见第 16-15 页上的显示被阻止 URL 的自定义网页。

提示 请注意，在被动或内联（触点模式）部署中不能使用 Block 或 Block with reset 操作，因为设备不是直接检查流量。如果创建具有 Block 或 Block with reset 操作的规则，该规则在安全区域条件内包含被动或内联（触点模式）接口，则策略编辑器在该规则旁边显示警告图标 ( )。

解密操作：解密流量以进一步检查

许可证：任何环境

受支持的设备：3 系列

Decrypt - Known Key 和 **Decrypt - Resign** 操作会对加密流量进行解密。系统通过访问控制来检查解密流量。访问控制规则以相同方式处理已解密和未加密的流量，您可以检查该流量来获得发现数据，并检测和阻止入侵、禁止的文件及恶意软件。系统在将允许的流量传递到其目标之前会将其重新加密。

当配置 **Decrypt - Known Key** 操作时，可以将一个或多个服务器证书和配对私钥与该操作相关联。如果流量与规则相匹配，并且用于加密流量的证书与操作的关联证书相匹配，则系统会使用相应的私钥获取会话加密和解密密钥。由于您必须有权访问私钥，此操作最适合于解密传入到组织控制的服务器的流量。

同样，可以将一个证书颁发机构证书和私钥与 **Decrypt - Resign** 操作相关联。如果流量与此规则相匹配，则系统会使用 CA 证书对服务器证书重新签名，然后充当中间人。它会创建两个 SSL 会话，一个介于客户端和受管设备之间，一个介于受管设备和服务器之间。每个会话包含不同的加密会话详细信息，并且允许系统解密并重新加密流量。此操作更适用于传出流量，因为证书的私钥会替换为您控制用于获取会话密钥的私钥。

对服务器证书重新签名涉及将证书的公钥替换为 CA 证书公钥，或者替换整个证书。通常，如果替换整个服务器证书，则在建立 SSL 连接时，客户端浏览器会发出警告，表明证书未由受信任机构签名。但是，如果客户端浏览器信任策略中的 CA，则浏览器不发出表明证书不可信的警告。如果原始服务器证书是自签名证书，系统会更换整个证书，并且信任重新签名的 CA，但是用户浏览器不发出表明证书是自签名的警告。在这种情况下，仅替换服务器证书公钥会导致客户端浏览器确实发出表明证书是自签名的警告。

如果配置具有 **Decrypt - Resign** 操作的规则，则除任何已配置的规则条件外，该规则会根据所引用的内部 CA 证书的签名算法类型来匹配流量。由于您将一个 CA 证书与 **Decrypt - Resign** 操作相关联，因此无法创建用来解密使用不同签名算法加密的多种类型的传出流量的 SSL 规则。此外，添加到规则中的任何外部证书对象和密码套件都必须与关联的 CA 证书加密算法类型相匹配。

例如，仅当操作引用基于椭圆曲线 (EC) 的 CA 证书时，使用 EC 算法加密的传出流量才会与 **Decrypt - Resign** 规则相匹配；如果要创建证书和密码套件规则条件，必须将基于 EC 的外部证书和密码套件添加到该规则。同样，引用基于 RSA 的 CA 证书的 **Decrypt - Resign** 规则仅与使用 RSA 算法加密的传出流量相匹配；使用 EC 算法加密的传出流量与该规则不匹配，即使所有其他已配置的规则条件都匹配也如此。

请注意：

- 如果用于建立 SSL 连接的密码套件应用 Diffie-Hellman 短时 (DHE) 或椭圆曲线 Diffie-Hellman 短时 (ECDHE) 密钥交换算法，则在被动部署中无法使用 **Decrypt - Known Key** 操作。如果 SSL 策略面向具有被动或内联（触点模式）接口的设备，并且包含具有密码套件条件（含有 DHE 或 ECDHE 密码套件）的 **Decrypt - Known Key** 规则，则系统会在该规则旁边显示信息图标 ( )。如果以后向包含被动或内联（触点模式）接口的 SSL 规则中添加区域条件，系统会显示警告图标 ( )。

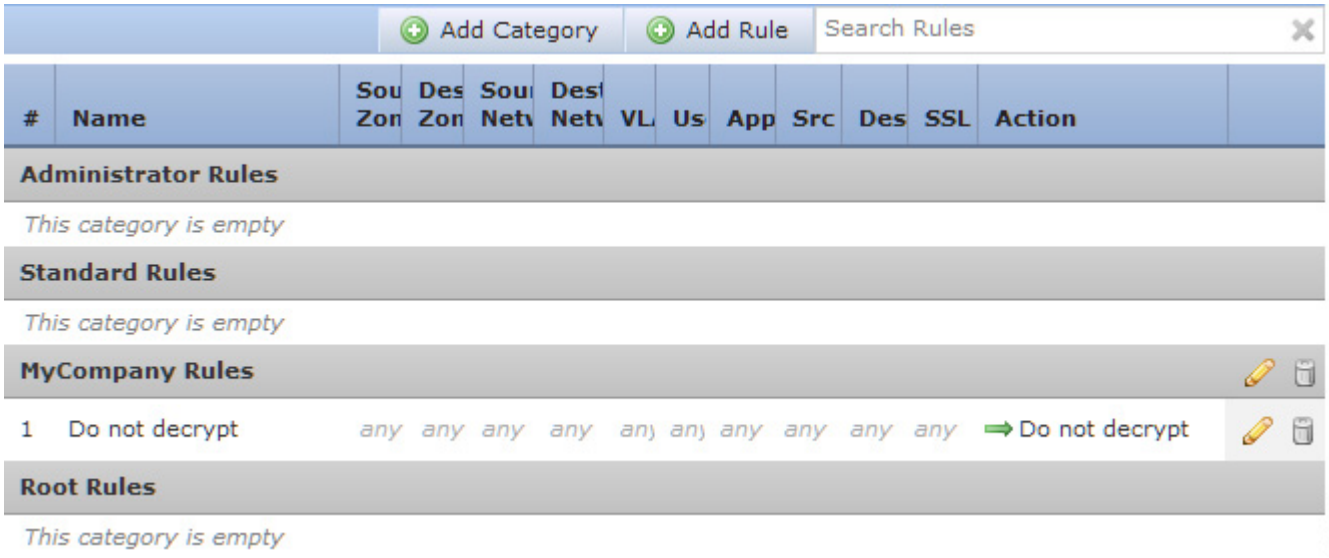
- 在被动或内联（触点模式）部署中无法使用 **Decrypt - Resign** 操作，因为设备不会直接检查流量。如果创建具有 **Decrypt - Resign** 操作的规则，该规则在安全区域中包含被动或内联（触点模式）接口，则策略编辑器在该规则旁边显示警告图标 ( )。如果 SSL 策略面向具有被动或内联（触点模式）接口的设备，并且包含 **Decrypt - Resign** 规则，则系统在该规则旁边显示信息图标 ( )。如果以后向包含被动或内联（触点模式）接口的 SSL 规则中添加区域条件，系统会显示警告图标 ( )。如果将包含 Decrypt - Resign 规则的 SSL 策略应用于具有被动或内联（触点模式）接口的设备，则与该规则相匹配的任何 SSL 会话都会失败。
- 如果客户端不信任用于对服务器证书重新签名的 CA，则会警告用户不应信任该证书。为避免此情况，请将 CA 证书导入到客户端信任的 CA 库。或者，如果组织具有专用 PKI，则可以颁发由根 CA（自动受组织中的所有客户端信任）签名的中级 CA 证书，然后将该 CA 证书上传到设备。
- 系统无法解密使用匿名密码套件加密的流量。如果向 **Cipher Suite** 条件中添加匿名密码套件，则在 SSL 规则中无法使用 **Decrypt - Resign** 或 **Decrypt - Known Key** 操作。
- 如果 HTTP 代理位于客户端和受管设备之间，并且客户端和服务器使用 CONNECT HTTP 方法建立隧道化 SSL 连接，则系统无法解密流量。 **Handshake Errors** 无法解密操作将决定系统如何处理此流量。有关详情，请参见第 20-4 页上的为无法解密的流量设置默认处理。
- 创建具有 **Decrypt - Known Key** 操作的 SSL 规则时，无法使用 **Distinguished Name** 或 **Certificate** 条件进行匹配。此限制基于这样一种假设：如果此规则与流量相匹配，则证书、主题 DN 和颁发者 DN 已经与规则的关联证书相匹配。有关详细信息，请参阅第 21-7 页上的使用规则操作确定加密流量处理和检查。
- 如果创建内部 CA 对象并选择生成证书签名请求 (CSR)，那么在将签名证书上传到对象之前，会无法对 **Decrypt - Resign** 操作使用此 CA。有关详细信息，请参阅第 3-40 页上的获取和上传新的签名证书。
- 如果配置具有 **Decrypt - Resign** 操作的规则，并且不匹配一个或多个外部证书对象或密码套件的签名算法类型，则策略编辑器在该规则旁边显示信息图标 ( )。如果不匹配所有外部证书对象或所有密码套件的签名算法类型，则策略在该规则旁边显示警告图标 ( )，并且无法应用与 SSL 策略相关联的访问控制策略。有关详细信息，请参阅第 22-19 页上的按证书控制加密流量和第 22-24 页上的按密码套件控制加密流量。
- 如果解密流量与具有 **Interactive Block** 或 **Interactive Block with reset** 操作的访问控制规则相匹配，则系统阻止匹配的连接而不交互，并且系统**不**显示响应页面。
- 如果启用内联规范化预处理器中的 **Normalize Excess Payload** 选项，则预处理器在规范化解密流量时，可能会丢弃数据包并将其替换为修整过的数据包。这不会结束 SSL 会话。如果允许流量，则修整过的数据包会作为 SSL 会话的一部分加密。有关此选项的详细信息，请参阅第 29-6 页上的规范化内联流量。

管理策略中的 SSL 规则

许可证：任何环境

受支持的设备：3 系列

通过 SSL 策略编辑器的 Rules 选项卡 （如下图所示），可以添加、编辑、搜索、移动、启用、禁用、删除和以其他方式管理策略中的 SSL 规则。



对于每个规则，策略编辑器会显示其名称和条件摘要，以及规则操作。图标表示警告、错误和其他重要信息。已禁用的规则会显示为灰色，而且规则名称下方会带有 (disabled) 标记。有关图标的详细信息，请参阅第 21-14 页上的对 SSL 规则进行故障排除。

有关管理 SSL 规则的信息，请参阅：

- 第 21-11 页上的搜索 SSL 规则
- 第 21-12 页上的启用和禁用 SSL 规则
- 第 21-12 页上的更改 SSL 规则的位置或类别

搜索 SSL 规则

许可证：任何环境

受支持的设备：3 系列

可以使用字母数字字符串 （包括空格和可打印的特殊字符）在 SSL 规则列表中搜索匹配值。搜索会检查规则名称和已添加至规则的任意规则条件。对于规则条件，搜索会匹配可以为每个条件类型 （区域、网络、应用程序等）添加的任意名称或值。这包括各个对象名称或值、组对象名称、组内的各个对象名称或值以及文本值。

可以使用部分或完整的搜索字符串。对于每个匹配规则，匹配值列将会突出显示。例如，如果在所有或部分规则上搜索字符串 100Bao，已添加 100Bao 应用程序的每个规则的 Applications 列都会突出显示。如果您还具有名为 100Bao 的规则，则 Name 和 Applications 列均会突出显示。

可以导航至每个上一个或下一个匹配规则。状态消息会显示当前的匹配项以及匹配项的总数量。

匹配可能会出现在多页规则列表的任意页面上。当第一个匹配项不在第一个页面上时，屏幕上将会显示第一个匹配项所在的页面。当您处于最后一个匹配项时，选择下一匹配项会使您到达第一个匹配项，当处于第一个匹配项时，选择上一匹配项会到达最后一个匹配项。

要搜索规则，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要搜索的策略的 SSL 策略编辑器中，点击 **Search Rules** 提示，键入搜索字符串，然后按 Enter 键。还可以使用 Tab 键或点击空白页面区域来发起搜索。

带有匹配值的规则列会被突出显示，其突出显示方式与指示的 （第一个）匹配项不同。

步骤 2　查找您感兴趣的规则：

- 要在匹配规则之间导航，可以点击下一匹配项 (▼) 或上一匹配项 (▲) 图标。
- 要刷新页面并清除搜索字符串和所有突出显示内容，请点击清除图标 (✖)。

启用和禁用 SSL 规则

许可证：任何环境

受支持的设备：3 系列

SSL 规则在创建时，默认会处于启用状态。如果禁用规则，则系统不使用其评估网络流量，并会停止为该规则生成警告和错误。查看 SSL 策略中的规则列表时，已禁用的规则会灰显，但仍然可以对其进行修改。请注意，也可使用规则编辑器启用或禁用 SSL 规则；请参阅第 21-4 页上的了解和创建 SSL 规则。

要更改 SSL 规则的状态，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　如果要启用或禁用规则，在包含该规则的策略的 SSL 策略编辑器中，右键单击规则，然后选择规则状态：

- 要启用非活动规则，请选择 **State > Enable**。
- 要禁用活动规则，请选择 **State > Disable**。

步骤 2　点击 **Save** 保存策略。

要使更改生效，必须应用与 SSL 策略关联的访问控制策略；请参阅第 12-13 页上的应用访问控制策略。

更改 SSL 规则的位置或类别

许可证：任何环境

受支持的设备：3 系列

为帮助组织 SSL 规则，每个 SSL 策略都具有三个系统提供的规则类别：Administrator Rules、Standard Rules 和 Root Rules。尽管可以创建自定义类别，但不能移动、删除或重命名这些类别。

默认情况下，任何允许您修改 SSL 策略的预定义用户角色也允许您在规则类别内部或之间移动和修改 SSL 规则。但是，可以创建自定义角色来限制用户移动和修改规则。

有关详情，请参阅：

- 第 21-13 页上的移动 SSL 规则
- 第 21-13 页上的添加新 SSL 规则类别

移动 SSL 规则

许可证：任何环境

受支持的设备：3 系列

正确的 SSL 规则顺序可减少处理网络流量所需的资源，并防止规则争抢。默认情况下，如果预定义用户角色可以修改 SSL 策略，则也能够在规则类别内部或之间移动 SSL 规则。但是，可以创建自定义角色来限制用户移动系统提供的类别中的规则。

以下步骤说明如何使用 SSL 策略编辑器一次移动一个或多个规则。您也可以使用规则编辑器移动单个 SSL 规则；请参阅第 21-4 页上的了解和创建 SSL 规则。

要移动规则，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　如果要移动规则，在包含该规则的策略的 SSL 策略编辑器中，点击每个规则的空白区域来选择规则。使用 Ctrl 和 Shift 键选择多个规则。

您选择的规则突出显示。

步骤 2　移动规则。可以剪切和粘贴或拖放规则。

要将规则剪切并粘贴到新位置，请右键点击选定的规则并选择 **Cut**。然后，在想要粘贴所剪切规则的位置旁，右键单击规则的空白区域并选择 **Paste above** 或 **Paste below**。请注意，不能在两个不同的 SSL 策略之间复制并粘贴 SSL 规则。

步骤 3　点击 **Save** 保存策略。

要使更改生效，必须应用与 SSL 策略关联的访问控制策略；请参阅第 12-13 页上的应用访问控制策略。

添加新 SSL 规则类别

许可证：任何环境

受支持的设备：3 系列

为帮助组织 SSL 规则，每个 SSL 策略都具有三个系统提供的规则类别：Administrator Rules、Standard Rules 和 Root Rules。尽管在标准规则和根规则之间创建自定义类，但是不能移动、删除或重命名这些类别。

添加自定义类别允许进一步组织规则，而无需创建额外的策略。可以重命名和删除添加的类别。不能移动这些类别，但可以将规则移入其中以及从中移出。

可以根据添加到角色中的用户权限，创建限制用户在系统提供的类别中移动和修改规则的自定义角色。有关详细信息，请参阅第 61-52 页上的用户帐户权限。

要添加新的类别，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　如果要移动规则，在包含该规则的策略的 SSL 策略编辑器中，点击 **Add Category**。

提示　如果您的策略已经包含规则，则可以点击现有规则所在行的空白区域，先设置新类别的位置，然后才能添加。还可以右键点击现有规则并选择 **Insert new rule**。

系统将显示 Add Category 弹出窗口。

步骤 2　键入唯一的类别**名称**。

可以输入字母数字名称，包括空格和特殊的可打印字符，最多可有 30 个字符。

步骤 3　有以下选项可供选择：

- 要将新的类别放置在现有类别的正上方，请从第一个 **Insert** 下拉列表中选择 **above Category**，然后从第二个下拉列表中选择您想要在其上放置规则的类别。
- 要将新类别规则放置在现有规则之下，请从下拉列表中选择 **below rule**，然后输入现有规则编号。仅当策略中存在至少一个规则时，该选项才有效。
- 要将规则放置在现有规则之上，请从下拉列表中选择 **above rule**，然后输入现有规则编号。仅当策略中存在至少一个规则时，此选项才有效该选项仅当策略中存在至少一个规则时有效。

步骤 4　点击 **OK**。

新类别将添加到系统。您可以点击自定义类别旁边的编辑图标 ( ) 编辑其名称，或者点击删除图标 ( ) 删除此类别。删除的类别中的规则将会添加至以上类别。

步骤 5　点击 **Save** 保存策略。

对 SSL 规则进行故障排除

许可证：任何环境

受支持的设备：3 系列

正确创建 SSL 规则并将其排序是一项复杂的任务，但却是构建有效部署的一项重要任务。如果不仔细规划策略，规则会彼此争抢优先级、需要其他许可证，或者包含无效的配置。为帮助确保系统按预期处理流量， SSL 策略接口具有功能强大的规则警告和错误反馈系统。

对于每个规则，策略编辑器中的图标标记警告和错误，如下表中所述。将鼠标指针悬停在图标上，可以阅读警告、错误或信息文本。

表 21-2　　SSL 错误图标

图标	说明	详细信息
⚠	警告	根据问题，可以应用将显示规则或其他警告的 SSL 策略。在这些情况下，配置错误的设置将不会生效。例如，争抢的规则绝不会评估流量。但是，如果警告图标标记许可错误或模式不匹配，则无法应用策略，直至更正问题为止。 如果禁用存在警告的规则，警告图标将会消失。如果在没有纠正潜在问题的情况下启用规则，警告图标将会再次显示。

表 21-2　SSL 错误图标 （续）

图标	说明	详细信息
	错误	如果规则或其他 SSL 策略配置存在错误，则无法应用策略，直至更正问题为止。
	信息	信息图标传达有关可能影响流量的配置的有用信息。这些问题较小，并且不会阻止您应用策略。

正确配置 SSL 规则还可以减少处理网络流量所需的资源。创建复杂规则和对规则进行错误排序会影响性能。

有关详情，请参阅：

- 第 21-15 页上的了解 SSL 规则警告和错误
- 第 21-15 页上的了解规则争抢和无效配置警告
- 第 21-16 页上的对 SSL 规则进行排序以提高性能和避免争抢

了解 SSL 规则警告和错误

许可证：因功能而异

受支持的设备：3 系列

虽然您可以使用任何许可证创建 SSL 规则，但是某些规则条件和检查选项要求您在目标设备上启用特定许可功能。您不能将使用许可功能的策略应用于未经许可的设备。系统使用警告图标和确认对话框来指定未经许可的功能。有关详细信息，请将指针悬停在警告图标上方。

下表说明您必须具有才能使用 SSL 规则的许可证。

表 21-3　SSL 规则的许可证要求

要使用规则.....	许可证	支持的防御中心	支持的设备
包括区域、网络、 VLAN、端口、证书、 DN、证书状态、密码套件或版本条件	任何环境	任何环境	3 系列
包括使用地理定位数据的网络条件	FireSIGHT	除 DC500 外的所有型号	3 系列
包括应用或用户条件	可控性	除无法执行用户控制的 DC500 外的所有型号	3 系列
包括使用 URL 类别和信誉数据的类别条件	URL 过滤	除 DC500 外的所有型号	3 系列

了解规则争抢和无效配置警告

许可证：任何环境

受支持的设备：3 系列

对 SSL 规则正确进行配置和排序对于构建有效的部署至关重要。在 SSL 策略中，SSL 规则可以争抢其他规则或包含无效配置。系统使用警告和错误图标来标记这些问题。

了解规则争抢警告

SSL 规则的条件可能从匹配流量争抢后续规则。例如：

```
Rule 1: do not decrypt Administrators
Rule 2: block Administrators
```

以上的第二个规则永远不会阻止流量，因为第一个规则已允许流量。

任何类型的规则条件都可以争抢后续规则。例如，以下的第一个规则中的 VLAN 范围包含第二个规则中的 VLAN，因此第一个规则将争抢第二个规则：

```
Rule 1: do not decrypt VLAN 22-33
Rule 2: block VLAN 27
```

在以下示例中， Rule 1 匹配所有 VLAN，因为没有配置 VLAN，因此 Rule 1 会争抢尝试匹配 VLAN 2 的 Rule 2：

```
Rule 1: do not decrypt Source Network 10.4.0.2/16
Rule 2: do not decrypt Source Network 10.4.0.2/16, VLAN 2
```

规则还会争抢所有配置条件都相同的完全一样的后续规则。例如：

```
Rule 1: do not decrypt VLAN 1 URL www.example.com
Rule 2: do not decrypt VLAN 1 URL www.example.com
```

如果任何条件不同，则不会争抢后续规则。例如：

```
Rule 1: do not decrypt VLAN 1 URL www.example.com
Rule 2: do not decrypt VLAN 2 URL www.example.com
```

了解无效配置警告

因为 SSL 策略所依赖的外部设置可能会变化，因此原先有效的 SSL 策略可能会变得无效。请考虑以下示例：

- 包含 URL 类别条件的规则可能有效，直至定位到没有 URL 过滤许可证的设备为止。此时，在规则旁边会显示错误图标，并且您无法将策略应用于该设备，直至编辑或删除该规则、重新设置策略目标或者启用适当的许可证为止。
- 如果创建 Decrypt-Resign 规则，然后向区域条件中添加具有被动接口的安全区域，则系统会在该规则旁边显示警告图标。由于无法通过在被动部署中对证书重新签名来解密流量，因此规则不会生效，直至从规则中移除被动接口或更改规则操作为止。
- 如果向规则中添加用户，然后更改 LDAP 用户感知设置以排除该用户，则该规则将不生效，因为用户不再是受访问控制的用户。

对 SSL 规则进行排序以提高性能和避免争抢

许可证：任何环境

受支持的设备：3 系列

SSL 策略中的规则从 1 开始进行编号。系统按升序规则编号自上而下将流量与规则相匹配。除 Monitor 规则以外，流量匹配的第一个规则是处理该流量的规则。

正确的 SSL 规则顺序可减少处理网络流量所需的资源，并防止规则争抢。虽然创建的规则对于每个组织和部署而言都是唯一的，但在对可以优化性能的规则进行排序并仍然满足需求时，可以遵循一些通用准则。

按重要性从高到低对规则进行排序

首先，必须对规则进行排序以满足组织的需求。将必须应用于所有流量的优先级规则放置在靠近策略顶部的位置。例如，如果要将来自单个用户的传出流量解密以进一步分析 （使用 Decrypt-Resign 规则），但是不解密来自部门中所有其他用户的流量 （使用 Do not decrypt 规则），请按该顺序放置这两个 SSL 规则。

从特定到通用对规则进行排序

可以通过将特定规则 （即，狭义定义其处理的流量的规则）放置在前来提高性能。这也非常重要，因为具有广泛条件的规则可匹配许多不同类型的流量，并且以后可以争抢更具体的规则。

请考虑以下场景，其中受信任 CA （好 CA ）错误地将 CA 证书颁发给恶意实体 （坏 CA），但是尚未撤销该证书。您希望阻止使用由不受信任 CA 颁发的证书加密的流量，但是以其他方式允许受信任 CA 的信任链中的流量。您应上传 CA 证书和所有中间 CA 证书，然后按如下方式对规则进行排序：

```
Rule 1: Block issuer CN=www.badca.com
Rule 2: Do not decrypt issuer CN=www.goodca.com
```

如果颠倒规则顺序：

```
Rule 1: Do not decrypt issuer CN=www.goodca.com
Rule 2: Block issuer CN=www.badca.com
```

第一个规则与受好 CA 信任的所有流量相匹配，包括受坏 CA 信任的流量 由于流量不曾与第二个规则相匹配，因此可能会允许而非阻止恶意流量。

将用于解密流量的规则放置在后

由于流量解密需要处理资源，因此将不解密流量的规则 （Do not decrypt、 Block）放置在解密流量的规则 （Decrypt-Known Key、 Decrypt-Resign）之前可提高性能。这是因为流量解密会运用大量资源。此外， Block 规则可以转移系统可能以其他方式解密或检查的流量。所有其他因素等同，也就是说，假如在某个规则集中，没有更重要的规则且争抢不会造成问题，请考虑按以下顺序放置这些规则：

- 记录匹配连接但不对流量采取任何其他操作的 Monitor 规则
- 阻止流量而不进一步检查的 Block 规则
- 不解密加密流量的 Do not decrypt 规则
- 使用已知私钥解密传入流量的 Decrypt-Known Key 规则
- 通过对服务器证书重新签名来解密传出流量的 Decrypt-Resign 规则

配置 SSL 检查以提高性能

许可证：任何环境

受支持的设备：3 系列

复杂 SSL 策略和规则会运用大量资源。当应用 SSL 策略时，系统会将所有规则共同进行评估，并创建目标设备用于评估网络流量的扩展标准集。弹出窗口可能会警告已超过目标设备支持的最大 SSL 规则数。此最大值取决于因素的数量，包括设备上的物理内存和处理器数量。

简化规则

以下准则可帮助您简化 SSL 规则并提高性能：

- 在构造规则时，请尽可能少地使用条件中的单独元素。例如，在网络条件中，使用 IP 地址块而不是单个 IP 地址。在端口条件中，使用端口范围。使用应用过滤器和 URL 类别及信誉可执行应用控制和 URL 过滤，使用 LDAP 用户组可执行用户控制。

  请注意，将元素结合到之后会在 SSL 规则条件中使用的对象中，将不会提高性能。例如，与在条件中逐个包含 50 个单独 IP 地址相比，使用包含这些 IP 地址的网络对象仅提供组织优势而非性能优势。
- 请尽可能按安全区域来限制规则。如果设备的接口不在某一区域限制规则中的其中一个区域内，则该规则不影响该设备上的性能。
- 不过度配置规则。如果一个条件足以匹配要处理的流量，请勿使用两个条件。

配置流量解密

当配置流量解密时，请记住以下准则：

- 流量解密需要处理资源来解密流量以及通过访问控制检查该流量。创建注重于小范围的解密规则 （相比于广泛的解密规则）可减少系统解密的流量，从而减少解密流量所需的处理资源。请尽可能阻止或选择不解密加密流量，而不是解密后使用访问控制规则允许或阻止流量。
- 如果将证书状态条件配置为根据根颁发者 CA 信任流量，请将根 CA 证书和根 CA 的信任链中的所有中间 CA 证书上传到 SSL 策略。可以在不解密的情况下允许受信任 CA 的信任链中的所有流量，而不是不必要地将其解密。

使用 SSL 规则调整流量解密

基本 SSL 规则将其规则操作应用于由设备检查的所有加密流量。为更好地控制和解密加密流量，可以配置规则条件来处理和记录特定类型的流量。每个 SSL 规则可包含 0 个、 1 个或多个规则条件；仅当流量与该 SSL 规则中的每个条件匹配时，规则才会匹配流量。

注 当流量匹配规则时，设备对流量应用配置规则操作。当连接结束时，设备会记录流量 （如果配置为执行此操作）。有关详细信息，请参阅第 21-7 页上的使用规则操作确定加密流量处理和检查和第 38-11 页上的记录已加密连接。

每个规则条件允许指定要与其相匹配的流量的一个或多个属性；这些属性包括下列各项的详细信息：

- 流量，包括其流经的安全区域、 IP 地址和端口、源或目标国家/地区以及源或目标 VLAN
- 与检测到的 IP 地址关联的用户
- 流量负载，包括流量中检测到的应用
- 连接加密，包括用于加密连接的 SSL/TLS 协议版本和密码套件及服务器证书
- 服务器证书的可分辨名称中指定的 URL 的类别和信誉

有关详细信息，请参阅以下各节：

- 第 38-11 页上的记录可用 SSL 规则解密的连接
- 第 22-1 页上的使用基于网络的条件控制加密流量
- 第 22-8 页上的按信誉控制加密流量
- 第 22-16 页上的根据加密属性控制流量

使用基于网络的条件控制加密流量

许可证：任何环境

受支持的设备：3 系列

*SSL 策略*中的 SSL *规则*对加密流量日志记录和处理实行精细控制。通过基于网络的条件，可以使用以下一个或多个标准管理哪些加密流量可穿越网络：

- 源和目标安全区域
- 源和目标 IP 地址或地理位置
- 数据包最内部的 VLAN 标记
- 源和目标端口

可以将基于网络的条件相互结合以及与其他类型的条件结合来创建 SSL 规则。这些规则可以简单也可以复杂，使用多个条件来匹配和检查流量。有关 SSL 规则的详细信息，请参阅第 21-1 页上的SSL 规则入门。

有关详细信息，请参阅以下各节：

按网络区域控制加密流量

许可证：任何环境

受支持的设备：3 系列

通过 SSL 规则中的区域条件，可以按加密流量的源和目标安全区域对其进行控制。

*安全区域*是一个或多个接口的分组，可位于多个设备之间。在设备的初始设置期间选择的选项（称为其*检测模式*）确定系统最初如何配置设备的接口，以及这些接口是否属于安全区域。

简答举例来说，当您使用 **Inline** 检测模式注册设备时，防御中心会创建两个区域：Internal 和 External，并将设备上的第一对接口分配到这些区域。连接到 Internal 侧的网络的主机表示受保护资产。

要扩展此场景，可以部署其他配置相同的设备 （由同一防御中心管理）来保护若干不同位置中的类似资源。与第一个设备类似，这些设备中的每个设备都会保护其 Internal 安全区域中的资产。

提示 无需将所有内部 （或外部）接口都分组到单个区域中。请选择适合您的部署和安全策略的分组。有关创建区域的详细信息，请参阅第 3-34 页上的使用安全区域。

在此部署中，您可以决定，尽管希望这些主机可以不受限制地访问互联网，但是想要通过解密并检查传入加密流量来保护这些主机。

要通过 SSL 检查实现此目的，请配置具有将 **Destination Zone** 设置为 **Internal** 的区域条件的 SSL 规则。此简单 SSL 规则与从 Internal 区域中的任何接口传出设备的流量相匹配。

如果要构建更复杂的规则，可以在单个区域条件中向 **Sources Zones** 和 **Destination Zones** 各添加最多 50 个区域：

- 要匹配从区域中的某个接口*传出*设备的加密流量，请将该区域添加到 **Destination Zones**。

  由于被动部署的设备不传输流量，因此无法在 **Destination Zone** 条件中使用由被动接口组成的区域。
- 要匹配从区域中的某个接口*传入*设备的加密流量，请将该区域添加到 **Source Zone**。

如果要向规则中同时添加源和目标区域条件，则匹配流量必须源于其中一个指定的源区域，**并且**通过其中一个目标区域流出。

请注意，如同区域中的所有接口都必须为相同类型 （全都为内联、全都为被动、全都为交换或全都为路由）一样， SSL 规则的区域条件中使用的所有区域也都必须为相同类型。也就是说，不能编写与出入不同类型的区域的加密流量相匹配的单一规则。

警告图标指示无效配置，例如不包含接口的区域。有关详细信息，请将鼠标指针悬停在图标上方。

要按区域控制加密流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要按区域控制加密流量的 SSL 策略中，创建新 SSL 规则或编辑现有规则。

有关详细说明，请参阅第 21-4 页上的了解和创建 SSL 规则。

步骤 2　在 SSL 规则编辑器中，选择 Zones 选项卡。

系统将显示 Zones 选项卡。

步骤 3　从 **Available Zones** 中查找并选择要添加的区域。

要搜索将添加的区域，请点击 **Available Zones** 列表上方的 **Search by name** 提示，然后键入区域名称。列表会在您键入内容时进行更新，以显示匹配区域。

点击选择区域。要选择多个区域，请使用 Shift 和 Ctrl 键，或者右键单击，然后选择 **Select All**。

步骤 4　点击 **Add to Source** 或 **Add to Destination** 将所选区域添加到相应的列表。

您也可以拖放所选区域。

步骤 5　保存或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

按网络或地理位置控制加密流量

许可证：任何环境

受支持的设备：3 系列

通过 SSL 规则中的网络条件，可以按加密流量的源和目标 IP 地址对其进行控制和解密。可以执行以下任一操作：

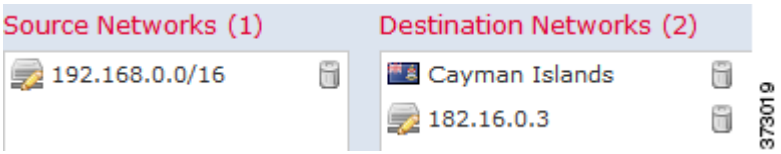
- 明确指定要控制的加密流量的源和目标 IP 地址，或者
- 使用地理定位功能 （将 IP 地址与地理位置相关联）根据加密流量的源或目标国家/地区或大洲对其进行控制

构建基于网络的 SSL 规则条件时，可以手动指定 IP 地址和地理位置。或者，也可以使用网络和地理定位*对象*配置网络条件，这些对象可重用，并会将名称与一个或多个 IP 地址、地址块、国家/地区、大洲等相关联。

提示　在创建网络或地理定位对象之后，不仅可以使用其构建 SSL 规则，还可以表示系统 Web 界面中各种其他位置的 IP 地址。可以使用对象管理器创建这些对象；也可以在配置 SSL 规则时即时创建网络对象。有关详细信息，请参阅第 3-1 页上的管理可重用对象。

请注意，如果要编写按地理位置控制流量的规则，以确保使用最新地理定位数据过滤流量，思科**强烈**建议定期更新防御中心上的地理定位数据库 (GeoDB)；请参阅第 66-24 页上的更新地理定位数据库。

下图显示 SSL 规则的网络条件，该规则阻止源于内部网络并尝试访问位于开曼群岛或 182.16.0.3 处一家离岸控股公司服务器上的资源的加密连接。



该示例手动指定离岸控股公司的服务器 IP 地址，并使用系统提供的开曼群岛地理定位对象表示开曼群岛 IP 地址。

可以在单一网络条件中向 **Source Networks** 和 **Destination Networks** 各添加最多 50 项，并且可以混合基于网络和基于地理定位的配置：

- 要与*来自* IP 地址或地理位置的加密流量相匹配，请配置 **Source Networks**。
- 要与*到* IP 地址或地理位置的加密流量相匹配，请配置 **Destination Networks**。

如果向规则中同时添加源和目标网络条件，则匹配的加密流量必须源于其中一个指定的 IP 地址，**并且**是发往其中一个目标 IP 地址。

在构建网络条件时，警告图标指示无效配置。有关详细信息，请将鼠标指针悬停在图标上方。

要按网络或地理位置控制流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要按网络控制加密流量的 SSL 策略中，创建新 SSL 规则或编辑现有规则。

有关详细说明，请参阅第 21-4 页上的了解和创建 SSL 规则。

步骤 2　在 SSL 规则编辑器中，选择 Networks 选项卡。

系统将显示 Networks 选项卡。

步骤 3　从 **Available Networks** 中查找并选择要添加的网络，如下所示：

- 点击 Networks 选项卡可以显示要添加的网络对象和组；点击 Geolocation 选项卡可以显示地理定位对象。
- 要即时添加可随后添加到条件中的网络对象，请点击 Available Networks 列表上方的添加图标 ( )；请参阅第 3-4 页上的使用网络对象。
- 要搜索将添加的网络或地理定位对象，请选择相应的选项卡，点击 **Available Networks** 列表上方的 **Search by name or value** 提示，然后键入对象名称或对象的其中一个组件的值。列表会在您键入内容时进行更新，以显示匹配对象。

要选择一个对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键，或者右键单击，然后选择 **Select All**。

步骤 4　点击 **Add to Source** 或 **Add to Destination** 将所选对象添加到相应的列表。

您也可以拖放所选对象。

步骤 5　添加要手动指定的所有源或目标 IP 地址或地址块。

点击 **Source Networks** 或 **Destination Networks** 列表下方的 **Enter an IP address** 提示；然后键入 IP 地址或地址块并点击 **Add**。

步骤 6　保存或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

控制加密 VLAN 流量

许可证：任何环境

受支持的设备：3 系列

通过 SSL 规则中的 VLAN 条件，可以控制 VLAN 标记的流量。系统使用最内部的 VLAN 标记来按照 VLAN 识别数据包。

在构建基于 VLAN 的 SSL 规则条件时，可以手动指定从 1 到 4094 的 VLAN 标记。或者，也可以使用 VLAN 标记*对象*配置 VLAN 条件，这些对象可重用，并会将名称与一个或多个 VLAN 标记相关联。

提示　在创建 VLAN 标记对象之后，不仅可以使用其构建 SSL 规则，还可以表示系统 Web 界面中各种其他位置的 VLAN 标记。可以使用对象管理器创建 VLAN 标记对象，也可以在配置访问控制规则时即时创建这些对象。有关详细信息，请参阅第 3-12 页上的使用 VLAN 标记对象。

下图显示 SSL 规则的 VLAN 标记条件，该规则与面向公众的 VLAN （以 VLAN 标记对象组表示）以及手动添加的 VLAN 42 上的加密流量相匹配。

在单个 VLAN 标记条件中可以向 **Selected VLAN Tags** 添加最多 50 项。在构建 VLAN 标记条件时，警告图标指示无效配置。有关详细信息，请将鼠标指针悬停在图标上方。

要按 VLAN 标记控制流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要按 VALN 标记控制流量的 SSL 策略中，创建新的 SSL 规则或编辑现有规则。

有关详细说明，请参阅第 21-4 页上的了解和创建 SSL 规则。

步骤 2　在 SSL 规则编辑器中，选择 VLAN Tags 选项卡。

系统将显示 VLAN Tags 选项卡。

步骤 3　从 **Available VLAN Tags** 中查找并选择要添加的 VLAN，如下所示：

- 要即时添加可随后添加到条件中的 VLAN 标记，请点击 Available VLAN Tags 列表上方的添加图标 ( )；请参阅第 3-12 页上的使用 VLAN 标记对象。
- 要搜索将添加的 VLAN 标记对象和组，请点击 **Available VLAN Tags** 列表上方的 **Search by name or value** 提示，然后键入对象的名称或对象中 VLAN 标记的值。列表会在您键入内容时进行更新，以显示匹配对象。

要选择一个对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键，或者右键单击，然后选择 **Select All**。

步骤 4　点击 **Add to Rule** 或将选定对象添加到 **Selected VLAN Tags** 列表。

您也可以拖放所选对象。

步骤 5　添加要手动指定的任何 VLAN 标记。

点击 **Selected VLAN Tags** 列表下方的 **Enter a VLAN Tag** 提示，然后键入 VLAN 标记或范围并点击 **Add**。可以指定从 1 到 4094 的任何 VLAN 标记；使用连字符可指定 VLAN 标记的范围。

步骤 6　保存或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

按端口控制加密流量

许可证：任何环境

受支持的设备：3 系列

通过 SSL 规则中的端口条件，可以按加密流量的源和目标 TCP 端口对其进行控制。在构建基于端口的 SSL 规则条件时，可以手动指定 TCP 端口。或者，也可以使用端口*对象*配置端口条件，这些对象可重用，并可以将名称与一个或多个端口相关联。

提示　在创建端口对象之后，不仅可以使用其构建 SSL 规则，还可以表示系统 Web 界面中各种其他位置的端口。可以使用对象管理器创建端口对象，也可以在配置 SSL 规则时即时创建这些对象。有关详细信息，请参阅第 3-10 页上的使用端口对象。

在单一网络条件中，可以向 **Selected Source Ports** 和 **Selected Destination Ports** 列表各添加最多 50 项：

- 要与*来自* TCP 端口的加密流量相匹配，请配置 **Selected Source Ports**。
- 要与*传到* TCP 端口的加密流量相匹配，请配置 **Selected Destination Ports**。
- 要与源自 TCP **Selected Source Ports** *和*发往 TCP **Selected Destination Ports** 的加密流量都匹配，请同时配置两者。

只能使用 TCP 端口配置 **Selected Source Ports** 和 **Selected Destination Ports** 列表。包含非 TCP 端口的端口对象在 **Available Ports** 列表中灰显。

在构建端口条件时，警告图标指示无效配置。例如，可以使用对象管理器编辑使用中的端口对象，以便使用这些对象组的规则变为无效。有关详细信息，请将鼠标指针悬停在图标上方。

要按端口控制流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要按 TCP 端口控制加密流量的 SSL 策略中，创建新的 SSL 规则或编辑现有规则。

有关详细说明，请参阅第 21-4 页上的了解和创建 SSL 规则。

步骤 2　在 SSL 规则编辑器中，选择 Ports 选项卡。

系统将显示 Ports 选项卡。

步骤 3　从 **Available Ports** 中查找并选择要添加的 TCP 端口，如下所示：

- 要即时添加可随后添加到条件中的 TCP 端口对象，请点击 Available Ports 列表上方的添加图标 ( )；请参阅第 3-10 页上的使用端口对象。

- 要搜索将添加的基于 TCP 的端口对象和组，请点击 **Available Ports** 列表上方的 **Search by name or value** 提示，然后键入对象的名称或对象中端口的值。列表会在您键入内容时进行更新，以显示匹配对象。例如，如果键入 443，防御中心将显示系统提供的 HTTPS 端口对象。

要选择基于 TCP 的端口对象，请点击该对象。要选择多个基于 TCP 的端口对象，请使用 Shift 和 Ctrl 键，或者右键单击，然后选择 **Select All**。如果对象包含不是基于 TCP 的端口，则无法将其添加到端口条件中。

步骤 4　点击 **Add to Source** 或 **Add to Destination** 将所选对象添加到相应的列表。

您也可以拖放所选对象。

步骤 5　在 **Selected Source Ports** 或 **Selected Destination Ports** 列表下输入**端口**，以手动指定源或目标端口。您可以使用 0 到 65535 范围中的一个值指定单一端口。

步骤 6　点击 **Add**。

请注意，防御中心不会向导致配置无效的规则条件中添加端口。

步骤 7　保存或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

根据用户控制加密流量

许可证：可控性

受支持的设备：3 系列

您可以将 SSL 规则配置为与从 Microsoft Active Directory 服务器检索到的用户的流量相匹配。通过 SSL 规则中的用户条件，可以根据登录到主机的 LDAP 用户限制流量，从而执行*用户控制*，以管理哪些流量可以穿越网络。

用户控制的工作原理是将*受访问控制的用户*与 IP 地址相关联。当指定的用户登录和注销主机或因其他原因使用 Active Directory 凭证进行身份验证时，已部署的代理监控这些用户。例如，您的组织可以使用依赖于 Active Directory 的服务或应用进行集中身份验证。

为使流量与具有用户条件的 SSL 规则相匹配，受监控会话中的源或目标主机的 IP 地址必须与已登录的受访问控制的用户相关联。可以根据个人用户或这些用户所属的组来控制流量。

可以将用户条件相互结合以及与其他类型的条件结合来创建 SSL 规则。这些规则可以简单也可以复杂，使用多个条件来匹配和检查流量。有关 SSL 规则的详细信息，请参阅第 21-4 页上的了解和创建 SSL 规则。

用户控制需要可控性许可证，并且仅支持用于 LDAP 用户和组 （*受访问控制的用户*），使用由监控 Microsoft Active Directory 服务器的用户代理报告的登录和注销记录。

在编写具有用户条件的 SSL 规则之前，必须在防御中心和您的组织的至少一个 Microsoft Active Directory 服务器之间配置连接。该配置 （称为身份验证对象）包含服务器的连接设置和身份验证过滤器设置。它还指定可在用户条件中使用的用户。有关详细信息，请参阅第 17-4 页上的检索访问受控用户和 LDAP 用户元数据。

此外，您还必须安装用户代理。在用户对活动目录证书进行验证时，代理监控这些用户，并将用户登录记录发送至防御中心。这些记录将用户与 IP 地址相关联，从而使具有用户条件的 SSL 规则得以触发。有关详细信息，请参阅第 17-9 页上的使用用户代理报告 Active Directory 登录情况。

要按用户控制加密流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要按用户控制加密流量的 SSL 策略中，创建新的 SSL 规则或编辑现有规则。

有关详细说明，请参阅第 21-4 页上的了解和创建 SSL 规则。

步骤 2　在 SSL 规则编辑器中，选择 Users 选项卡。

系统将显示 Users 选项卡。

步骤 3　要搜索将添加的用户，请点击 **Available Users** 列表上方的 **Search by name or value** 提示，然后键入用户名。列表会在您键入内容时进行更新，以显示匹配用户。

要选择用户，请点击该用户。要选择多个用户，请使用 Shift 和 Ctrl 键，或者右键单击，然后选择 **Select All**。

步骤 4　点击 **Add to Rule** 或将所选用户添加到 **Selected Users** 列表中。

您也可以拖放所选用户。

步骤 5　保存或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

按信誉控制加密流量

许可证：可控性或URL 过滤

受支持的设备：3 系列

SSL 规则中基于信誉的条件允许您通过将网络流量情景化并对其进行适当限制，来管理哪些加密流量可以穿越网络。 SSL 规则监管以下类型的基于信誉的控制：

- 应用条件允许您执行*应用控制*，不仅根据单个应用还根据应用的基本特性 （类型、风险、业务相关性和类别）来控制应用流量。
- URL 条件允许您根据网站的分配的类别和信誉来控制网络流量。

可以将基于信誉的条件相互结合以及与其他类型的条件结合来创建 SSL 规则。这些规则可以简单也可以复杂，使用多个条件来匹配和检查流量。

基于信誉的 SSL 检查需要以下许可证、设备和防御中心。

表 22-1　　基于信誉的 SSL 规则的许可证和设备要求

要求	应用控制	URL 过滤 （类别 和信誉）
许可证	可控性	URL 过滤
设备	3 系列	3 系列
防御中心	3 系列、虚拟设备	3 系列、虚拟设备

有关详细信息，请参阅以下各节：

- 第 22-9 页上的根据应用控制加密流量
- 第 22-13 页上的按 URL 类别和信誉控制加密流量

根据应用控制加密流量

许可证：可控性

受支持的设备：3 系列

当 FireSIGHT 系统分析加密 IP 流量时，它可以在解密加密会话之前识别和分类网络上常用的加密应用。系统使用此基于发现的*应用感知*功能，允许您控制网络上的加密应用流量。

SSL 规则中的应用条件允许您执行此*应用控制*。在单个 SSL 规则中，有多种方法可以指定要控制其流量的应用：

- 可以选择单个应用，包括自定义应用。
- 可以使用系统提供的*应用过滤器*，此类过滤器是根据应用的基本特性 （类型、风险、业务相关性和类别）组织的命名应用集。
- 您可以创建和使用自定义应用过滤器，其以您选择的任何方式将应用 （包括自定义应用）进行分组。

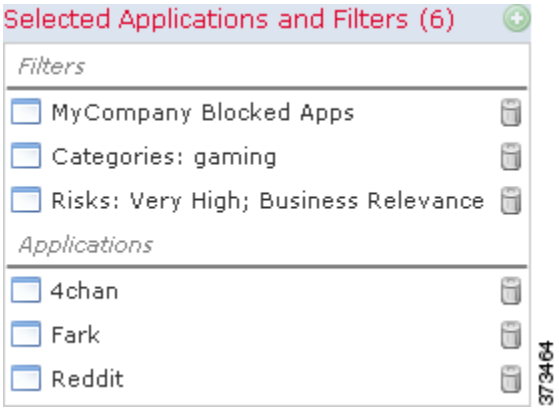
注 使用访问控制规则过滤应用流量时，可以使用应用标记作为标准 进行过滤。但是，因为没有好处，不能使用应用标记过滤加密流量。系统在加密流量中可以检测的所有应用都标记为 **SSL Protocol**；只能在未加密或已解密的流量中检测到没有此标记的应用。

通过应用过滤器，可以快速创建 SSL 规则的应用条件。这些条件简化策略创建和管理，并保证系统将按预期控制网络流量。例如，可以创建会识别并解密加密流量中的所有高风险、低业务相关性应用的 SSL 规则。如果用户尝试使用这些应用之一，则会通过访问控制来解密和检查会话。

此外，思科还通过系统和漏洞数据库 (VDB) 更新频繁更新和添加其他检测器。您还可以创建自己的检测器并向其检测的应用分配特性 （风险、相关性等）。通过根据应用特性使用过滤器，可以确保系统使用最新检测器监控应用流量。

为使流量与具有应用条件的 SSL 规则相匹配，流量必须与向 **Selected Applications and Filters** 列表中添加的其中一个过滤器或应用相匹配。

下图显示用于解密以下自定义应用组的 SSL 规则的应用条件：MyCompany 的应用，具有高风险和低业务相关性的所有应用、游戏应用以及单独选择的一些应用。



在单个应用条件中，可以向 **Selected Applications and Filters** 列表中添加最多 50 项。以下每个内容计为一项：

- **Application Filters** 列表中的一个或多个过滤器 （单独或以自定义组合形式）。此项表示按特性分组的应用集。

- 通过保存 **Available Applications** 列表中应用的搜索创建的过滤器。此项表示按子字符串匹配分组的应用集。
- **Available Applications** 列表中的单个应用。

在 Web 界面中，添加到条件的过滤器会在上方列出并与单独添加的应用分别列出。

请注意，当应用 SSL 策略时，对于具有应用条件的每个规则，系统生成要匹配的唯一应用的列表。换句话说，可以使用重叠过滤器和单独指定的应用确保完整覆盖。

有关详细信息，请参阅以下各节：

- 第 22-10 页上的将加密流量与应用过滤器相匹配
- 第 22-11 页上的匹配来自单个应用的流量
- 第 22-12 页上的向 SSL 规则中添加应用条件
- 第 22-13 页上的对加密应用控制的限制

将加密流量与应用过滤器相匹配

许可证：可控性

受支持的设备：3 系列

在 SSL 规则中构建应用条件时，使用 **Application Filters** 列表可创建要匹配其流量的按特性分组的应用集。

为方便起见，系统使用第 45-9 页上的了解应用检测中介绍的标准将其检测的每个应用特性化。可以使用这些标准作为过滤器或创建过滤器的自定义组合来执行应用控制。

请注意，过滤 SSL 规则中的应用的机制与使用对象管理器创建可重用、自定义应用过滤器的机制相同；请参阅第 3-13 页上的使用应用过滤器。您还可以将在访问控制规则中即时创建的许多过滤器另存为新的可重用过滤器。不能保存包含另一个用户创建的过滤器的过滤器，因为无法嵌套用户创建的过滤器。

了解过滤器的组合方式

选择过滤器时（单独或以组合形式），**Available Applications** 列表会更新为仅显示符合标准的应用。可以选择组合形式的系统提供的过滤器，但是不能选择自定义过滤器。

系统将同一类型的多个过滤器与 OR 操作关联。例如，如果您在 Risks 类型下选择 Medium 和 High 过滤器，则产生的过滤器为：

```
Risk: Medium OR High
```

如果 Medium 过滤器包含 110 个应用，而 High 过滤器包含 82 个应用，则系统将在 **Available Applications** 列表中显示全部 192 个应用。

系统将不同类型的过滤器与 AND 操作关联。例如，如果您选择 Risks 类型下的 Medium 和 High 过滤器，以及 Business Relevance 类型项下的 Medium 和 High 过滤器，则所产生的过滤器为：

```
Risk: Medium OR High
```

和

```
Business Relevance: Medium OR High
```

在此情况下，系统仅显示 Medium Risk 或 High Risk 类型以及 Medium Business Relevance 或 High Business Relevance 类型中均包含的那些应用。

查找并选择过滤器

要选择过滤器，请点击过滤器类型旁边的箭头将其展开，然后选择或清除要显示或隐藏其应用的每个过滤器旁边的复选框。您还可以右键单击思科提供的过滤器类型（**Risks**、**Business Relevance**、**Types** 或 **Categories**），然后选择 **Check All** 或 **Uncheck All**。

要搜索过滤器，请点击 **Available Filters** 列表上方的 **Search by name** 提示，然后键入名称。列表会在您键入内容时进行更新，以显示匹配的过滤器。

选择过滤器完成后，使用 **Available Applications** 列表将这些过滤器添加到规则中；请参阅第 22-11 页上的匹配来自单个应用的流量。

匹配来自单个应用的流量

许可证：可控性

受支持的设备：3 系列

在 SSL 规则中构建应用条件时，请使用 **Available Applications** 列表选择要匹配其流量的应用。

浏览应用列表

首次开始构建条件时，列表不受限制，并会显示系统检测的每个应用 （一次 100 个）：

- 要翻页浏览应用，请点击列表下方的箭头。
- 要显示包含有关应用特性的摘要信息的弹出窗口以及可以跟随的互联网搜索链接，请点击应用旁边的信息图标 ( )。

查找要匹配的应用

为帮助查找要匹配的应用，可以通过以下方式限制 **Available Applications** 列表：

- 要搜索应用，请点击列表上方的 **Search by name** 提示，然后键入名称。列表会在您键入内容时进行更新，以显示匹配的应用。
- 要通过应用过滤器来限制应用，请使用 **Application Filters** 列表 （请参阅第 22-10 页上的将加密流量与应用过滤器相匹配）。 **Available Applications** 列表在您应用过滤器时进行更新。

一旦限制，在 **Available Applications** 列表的顶部便会显示 **All apps matching the filter** 选项。通过此选项，可以一次性将受限制列表中的所有应用都添加到 **Selected Applications and Filters** 列表中。

注　如果在 Application Filters 列表中选择一个或多个过滤器，并且还搜索 **Available Applications** 列表，则您的选择和搜索过滤的 **Available Applications** 列表会使用 AND 运算进行组合。也就是说，**All apps matching the filter** 条件包含 **Available Applications** 列表中当前显示的所有单个条件以及在 **Available Applications** 列表上方输入的搜索字符串。

在条件中选择要匹配的单个应用

查找要匹配的应用后，请点击以选定该应用。要选择多个应用，请使用 Shift 和 Ctrl 键，或者右键单击并选择 **Select All** 以选择当前受限制视图中的所有应用。

在单个应用条件中，可以通过逐个选择应用来匹配最多 50 个应用；要添加 50 个以上的应用，必须创建多个 SSL 规则或使用过滤器对应用进行分组。

选择与条件的过滤器相匹配的所有应用

一旦通过搜索或使用 **Application Filters** 列表中的过滤器进行限制， **Available Applications** 列表的顶部就会显示 **All apps matching the filter** 选项。

通过此选项，可以一次性将受限制 **Available Applications** 列表中的整个应用集添加到 **Selected Applications and Filters** 列表中。与逐个添加应用相比，无论组成此应用集的单个应用的数量如何，添加此应用集都仅计为一项，而不是最多 50 项。

以此方式构建应用条件时，添加到 **Selected Applications and Filters** 列表的过滤器的名称是过滤器中表示的过滤器类型加上每个类型的最多三个过滤器的名称的并置。相同类型的过滤器如果超过三个，后面会加上省略号 (...)。例如，以下过滤器名称在 Risks 类型下包含两个过滤器，在 Business Relevance 下包括四个过滤器：

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

您使用 **All apps matching the filter** 添加的过滤器中未呈现的过滤器类型不包含在所添加的过滤器名称中。将鼠标指针悬停在 **Selected Applications and Filters** 列表中的过滤器名称上方时显示的说明文本指示这些过滤器类型设置为 *any*；也就是说，这些过滤器类型不限制过滤器，因此，这些过滤器类型允许使用任意值。

可以向应用条件中添加 **All apps matching the filter** 的多个实例，其中每个实例在 **Selected Applications and Filters** 列表中计为单独一项。例如，可以将所有高风险应用添加为一项，清除选择，然后将所有低业务相关性应用添加为另一项。此应用条件与具有高风险或低业务相关性的应用相匹配。

向 SSL 规则中添加应用条件

许可证：可控性

受支持的设备：3 系列

为使加密流量与具有应用条件的 SSL 规则相匹配，流量必须与向 **Selected Applications and Filters** 列表中添加的其中一个过滤器或应用相匹配。

每个条件可以添加最多 50 项，并且添加到条件中的过滤器会在上方列出并与单独添加的应用分隔开来。构建应用条件时，警告图标指示无效配置。有关详细信息，请将鼠标指针悬停在图标上方。

要控制加密应用流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要按应用控制流量的 SSL 策略中，创建新的 SSL 规则或编辑现有规则。

有关详细说明，请参阅第 21-4 页上的了解和创建 SSL 规则。

步骤 2　在 SSL 规则编辑器中，选择 Applications 选项卡。

系统将显示 Applications 选项卡。

步骤 3　或者，使用过滤器限制 **Available Applications** 列表中显示的应用列表。

在 **Application Filters** 列表中选择一个或多个过滤器。有关详细信息，请参阅第 22-10 页上的将加密流量与应用过滤器相匹配。

步骤 4　从 **Available Applications** 列表中查找并选择要添加的应用。

可以搜索并选择单个应用，或者，当列表受限制时，搜索并选择 **All apps matching the filter**。有关详细信息，请参阅第 22-11 页上的匹配来自单个应用的流量。

步骤 5　点击 **Add to Rule** 将所选应用添加到 **Selected Applications and Filters** 列表。

您也可以拖放所选应用和过滤器。过滤器会显示在标题 *Filters* 下，应用显示在标题 *Applications* 下。

提示　在将另一个过滤器添加到此应用条件中之前，请点击 **Clear All Filters** 清除现有选择。

步骤 6　保存或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

对加密应用控制的限制

许可证：可控性

受支持的设备：3 系列

执行应用控制时，请记住以下要点。

加密应用识别

系统可以识别使用 StartTLS 进行加密的未加密应用。这包括诸如 SMTPS、 POPS、 FTPS、 TelnetS 和 IMAPS 之类的应用。此外，它还可以根据 TLS 客户端问询消息中的服务器名称指示或服务器证书主题可分辨名称值来识别某些加密应用。

应用识别的速度

系统在以下情况之前无法对加密流量执行应用控制：

- 在客户端和服务器之间建立加密连接，并且
- 系统识别加密会话中的应用

此识别发生在服务器证书交换之后。如果在握手期间交换的流量与包含应用条件的 SSL 规则中的所有其他条件相匹配，但是识别未完成，则 SSL 策略允许数据包通过。此行为允许完成握手，以便可以识别应用。为方便起见，受影响规则使用信息图标 ( ) 进行标记。

在系统完成其识别后，系统将 SSL 规则操作应用于与其应用条件相匹配的剩余会话流量。

自动启用应用检测器

必须为策略中的每个应用规则条件启用至少一个检测器 （请参阅第 46-24 页上的激活和停用检测器）。如果没有为应用启用检测器，则系统自动为该应用启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。

按 URL 类别和信誉控制加密流量

许可证：URL 过滤

受支持的设备：3 系列

通过 SSL 规则中的 URL 条件，可以处理和解密网络上用户可访问的加密网站流量。系统根据 SSL 握手期间传递的信息检测所请求的 URL。通过 URL 过滤许可证，可以根据 URL 的一般分类或*类别*和风险级别或*信誉*来控制对网站的访问。

注 可以通过定义可分辨名称 SSL 规则条件来处理和解密发送到特定 URL 的流量。证书的主题可分辨名称中的公用名属性包含站点的 URL。有关详细信息，请参阅第 22-17 页上的按证书可分辨名称控制加密流量。

有关详情，请参阅：

- 第 22-14 页上的执行基于信誉的 URL 阻止
- 第 22-16 页上的对 URL 检测和阻止的限制

执行基于信誉的 URL 阻止

许可证：URL 过滤

受支持的设备：3 系列

通过 URL 过滤许可证，可以根据所请求的 URL 的类别和信誉来控制用户对网站的访问：

- URL *类别*是 URL 一般分类。例如， ebay.com 属于 **Auctions** 类别，而 monster.com 属于 **Job Search** 类别。 URL 可以属于多个类别。
- URL *信誉*代表可能出于违背组织的安全策略而使用 URL 的可能性。 URL 的风险范围可从 **High Risk** （1 级）到 **Well Known** （5 级）。

通过FireSIGHT 系统从思科云获取的 URL 类别和信誉，可以快速为 SSL 规则创建 URL 条件。例如，可以创建用于识别并阻止 **Abused Drugs** 类别中所有 **High risk** URL 的 SSL 规则。如果用户尝试通过加密连接浏览至具有该类别和信誉组合的任何 URL，则会阻止此会话。

注　**必须**先启用与思科云的通信，然后具有基于类别和信誉的 URL 条件的 SSL 规则才能生效。这样，防御中心可以检索 URL 数据。有关详细信息，请参阅第 64-25 页上的启用云通信。

使用思科云中的类别和信誉数据可简化策略创建和管理。它保证系统按预期控制加密网络流量。最后，由于云会使用新 URL 以及现有 URL 的新类别和风险持续更新，因此可以确保系统使用最新信息来过滤所请求的 URL。代表安全威胁，例如恶意软件、垃圾邮件、僵尸网络和网络钓鱼，的恶意网站出现和消失的速度可能比您更新和应用新策略的速度要快。

例如：

- 如果规则阻止所有游戏站点，当新的域名注册并分类为 **Gaming** 时，系统可以自动阻止这些站点。
- 如果规则阻止所有恶意软件，并且博客页面被恶意软件感染，则该云可以将 URL 从 **Blog** 重新分类为 **Malware**，这样系统就可以阻止该站点。
- 如果规则阻止高风险的社交网站，并且，某人在包含指向恶意负载的链接的配置文件页面发布链接，则该云可以将该页面的信誉从 **Benign sites** 更改为 **High risk**，这样系统就可以阻止它。

请注意，如果云不知道 URL 的类别或信誉，或者如果防御中心无法与云联系，则该 URL **不会**触发具有基于类别和信誉的 URL 条件的 SSL 规则。不能手动向 URL 分配类别或信誉。

下图显示用于阻止以下内容的访问控制规则的 URL 条件：所有恶意软件站点、所有高风险站点以及所有非良性社交网站。

提示　如果解密流量，然后通过访问控制阻止该流量，则可以为用户提供通过点击浏览警告页面来绕过阻止的机会。有关详情，请参见第 14-8 页上的交互式阻止操作：允许用户绕过网站拦截。

可以在单个 URL 条件中添加最多 50 个要匹配的 **Selected Categories**。每个 URL 类别（可以选择按信誉进行限定）计为一项。

下表总结如何构建以上显示的条件。请注意，不能使用信誉限定文本 URL 或 URL 对象。

表 22-2　　示例：构建 URL 条件

要阻止.....	请选择此类别或 URL 对象.....	和该信誉.....
恶意软件站点，无论信誉如何	Malware Sites	Any
具有高风险 （1 级）的任何 URL	Any	1 - High Risk
风险大于良性 （1 至 3 级）的社交网站	Social Network	3 - Benign sites with security risks

构建 URL 条件时，警告图标指示无效配置。有关详细信息，请将鼠标指针悬停在图标上方并参阅第 12-18 页上的对访问控制策略和规则进行故障排除。

要使用类别和信誉数据按所请求的 URL 控制流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要按 URL 控制加密流量的 SSL 策略中，创建新的 SSL 规则或编辑现有规则。

有关详细说明，请参阅第 21-4 页上的了解和创建 SSL 规则。

步骤 2　在 SSL 规则编辑器中，选择 Categories 选项卡。

系统将显示 Categories 选项卡。

步骤 3　从 **Categories** 列表中查找并选择要添加的 URL 的类别。要匹配加密网络流量 （无论类别如何），请选择 **Any** 类别。

要搜索将添加的类别，请点击 **Categories** 列表上方的 **Search by name or value** 提示，然后键入类别名称。列表会在您键入内容时进行更新，以显示匹配类别。

要选择类别，请点击该类别。要选择多个类别，请使用 Shift 和 Ctrl 键。

提示　虽然可以右键单击并选择 **Select All** 来选择所有类别，但是以此方式添加所有类别会超过 SSL 规则的 50 项最大限制值。请改用 **Any**。

步骤 4　或者，也可以通过点击 **Reputations** 列表中的信誉级别来限定类别选择。如果不指定信誉级别，则系统默认为 **Any**，表示所有级别。

只能选择一个信誉级别。选择信誉级别时， SSL 规则根据其用途而表现不同行为：

- 如果规则阻止 Web 访问或解密流量（规则操作为 **Block**、 **Block with reset**、 **Decrypt - Known Key**、 **Decrypt - Resign** 或 **Monitor**），则选择信誉级别还将选择严重性高于该级别的所有信誉。例如，如果将规则配置为阻止 **Suspicious sites** （2 级），则系统还会自动阻止 **High Risk** （1 级）站点。
- 如果规则根据访问控制允许 Web 访问 （规则操作为 **Do not decrypt**），则选择信誉级别还将选择严重性低于该级别的所有信誉。例如，如果您将规则配置为允许 **Benign sites** （4 级），系统还会自动允许 **Well known** （5 级）站点。

如果更改规则的规则操作，系统根据上述几点自动更改 URL 条件中的信誉级别。

步骤 5　点击 **Add to Rule** 或将所选项添加到 **Selected Categories** 列表。

您也可以拖放所选项。

步骤 6　保存或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

对 URL 检测和阻止的限制

许可证：URL 过滤

受支持的设备：3 系列

执行 URL 检测和阻止时，请记住以下要点。

URL 识别的速度

系统在以下情况之前无法将 URL 分类：

- 在客户端和服务器之间建立受监控连接
- 系统识别会话中的 HTTPS 应用
- 系统从客户端问询消息或服务器证书中识别所请求的 URL

此识别发生在服务器证书交换之后。如果在握手期间交换的流量与包含 URL 条件的 SSL 规则中的所有其他条件相匹配，但是识别未完成，则 SSL 策略允许数据包通过。此行为允许建立连接，以便可以识别 URL。为方便起见，受影响规则使用信息图标 ( ) 进行标记。

在系统完成其识别后，系统会将 SSL 规则操作应用于与其 URL 条件相匹配的剩余会话流量。

URL 中的搜索查询参数

系统不使用 URL 中的搜索查询参数来匹配 URL 条件。例如，考虑这样一个场景：您阻止所有购物流量。在这种情况下，使用网络搜索来搜索 amazon.com 不会被阻止，但是，浏览 amazon.com 则会被阻止。

根据加密属性控制流量

许可证：任何环境

受支持的设备：3 系列

您可以创建根据解密连接特性来处理和加密加密流量的 SSL 规则。可以检测用于加密会话的协议版本或密码套件，并相应地处理流量。您还可以根据以下证书特性检测服务器证书和处理流量：

- 服务器证书本身
- 证书颁发者 （是不是颁发 CA，或者证书是不是自签名的）
- 证书持有者
- 各种证书状态，例如证书是否有效或者是否被发放 CA 撤销

要检测规则、证书颁发者或证书持有者中的多个密码套件，可以创建可重用密码套件列表和可分辨名称对象并将其添加到规则中。要检测服务器证书和某些证书状态，必须为规则创建外部证书和外部 CA 对象。

有关详细信息，请参阅以下各节：

- 第 22-17 页上的按证书可分辨名称控制加密流量
- 第 22-19 页上的按证书控制加密流量
- 第 22-20 页上的按证书状态控制加密流量
- 第 22-24 页上的按密码套件控制加密流量
- 第 22-25 页上的按加密协议版本控制流量

按证书可分辨名称控制加密流量

许可证：任何环境

受支持的设备：3 系列

通过 SSL 规则中的可分辨名称，可以根据颁发服务器证书的 CA 或证书持有者来处理和检查加密流量。根据颁发者可分辨名称，可以根据颁发站点服务器证书的 CA 处理流量。

当配置规则条件时，可以手动指定文本值，引用可分辨名称对象，或者引用包含多个对象的可分辨名称组。

注　如果还选择 **Decrypt - Known Key** 操作，则无法配置可分辨名称条件。由于该操作要求选择服务器证书来解密流量，因此证书已经与流量相匹配。有关详情，请参见第 21-9 页上的解密操作：解密流量以进一步检查。

可以在单个证书状态规则条件中根据多个主题和颁发者可分辨名称进行匹配，只需匹配一个公用名或可分辨名称即可与规则相匹配。

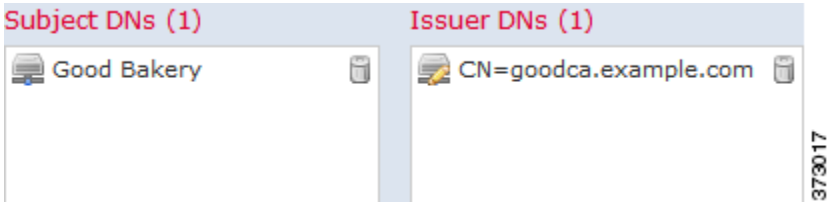
如果手动添加可分辨名称，则其可以包含公用名属性 (**CN**)。如果添加不带 CN= 的公用名，则系统在保存对象之前会在该名称之前预置 CN=。

您还可以添加具有下表中列出的各属性之一的可分辨名称 （以逗号分隔）。

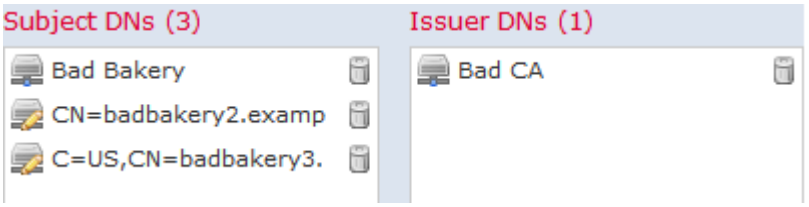
表 22-3　　可分辨名称属性

属性	说明	允许的值
C	国家/地区代码	两个字母字符
CN	公用名	最多 64 个字母数字、反斜杠 (\)、连字符 (-)、引号 (")、星号 (*)、句点 (.) 或空格字符
O	组织	
OU	组织单位	

下图说明用于搜索向 goodbakery.example.com 颁发或由 goodca.example.com 颁发的证书的可分辨名称规则条件。根据访问控制，允许通过这些证书加密的流量。



下图说明用于搜索向 badbakery.example.com 和关联域颁发的证书或由 badca.example.com 颁发的证书的可分辨名称规则条件。通过这些证书加密的流量使用重新签名的证书进行解密。



在单个 DN 条件中，可以向 **Subject DNs** 添加最多 50 个文本值和可分辨名称对象，并向 **Issuer DNs** 添加最多 50 个文本值和可分辨名称对象。

系统提供的 DN 对象组 Sourcefire Undecryptable Sites 包含系统无法解密其流量的网站。可以向 DN 条件中添加该组来阻止或不解密出入于这些网站的流量，而不会浪费系统资源尝试解密该流量。可以修改组中的单个条目。不能删除该组。系统更新可以修改此列表中的条目，但是，系统会保留用户更改。

要根据证书主题或颁发者可分辨名称检查加密流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要按证书主题或颁发者可分辨名称控制加密流量的 SSL 策略中，创建新的 SSL 规则或编辑现有规则。

有关详细说明，请参阅第 21-4 页上的了解和创建 SSL 规则。

步骤 2　在 SSL 规则编辑器中，选择 DN 选项卡。

系统将显示 DN 选项卡。

步骤 3　从 **Available DNs** 中查找并选择要添加的可分辨名称，如下所示：

- 要即时添加可随后添加到条件中的可分辨名称对象，请点击 **Available DNs** 列表上方的添加图标 ( )；请参阅第 3-36 页上的使用可分辨名称对象。
- 要搜索将添加的可分辨名称对象和组，请点击 **Available DNs** 列表上方的 **Search by name or value** 提示，然后键入对象的名称或对象中的值。列表会在您键入内容时进行更新，以显示匹配对象。

要选择一个对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键，或者右键单击，然后选择 **Select All**。

步骤 4　您有以下选项：

- 点击 **Add to Subject** 将所选对象添加到 **Subject DNs** 列表中。
- 点击 **Add to Issuer** 将所选对象添加到 **Issuer DNs** 列表中。

您也可以拖放所选对象。

步骤 5　添加要手动指定的所有文本公用名或可分辨名称。

点击 **Subject DNs** 或 **Issuer DNs** 列表下方的 **Enter DN or CN** 提示，然后键入公用名或可分辨名称并点击 **Add**。

步骤 6　添加或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

按证书控制加密流量

许可证：任何环境

受支持的设备：3 系列

通过 SSL 规则中的证书条件，可以根据用于对加密流量进行加密的服务器证书来处理和检查该流量。可以配置具有一个或多个证书的条件；如果证书与该条件的任何证书相匹配，则流量与规则相匹配。

构建基于证书的 SSL 规则条件时，可以上传服务器证书；将证书另存为外部证书*对象*，该对象可重用并会将名称与服务器证书相关联。或者，可以使用现有外部证书对象和对象组来配置证书条件。

可以根据以下证书可分辨名称特性在外部证书对象或对象组所基于的规则条件中搜索 **Available Certificates** 字段：

- 主题或颁发者公用名 (CN)
- 主题或颁发者组织 (O)
- 主题或颁发者组织单位 (OU)

您可以选择根据单个证书规则条件中的多个证书进行匹配；如果用于加密流量的证书与上传的任何证书相匹配，则加密流量与规则相匹配。

在单个证书条件中，可以向 **Selected Certificates** 添加最多 50 个外部证书对象和外部证书对象组。

请注意：

- 如果还选择 **Decrypt - Known Key** 操作，则无法配置证书条件。由于该操作要求选择服务器证书来解密流量，因此结果是证书已经与流量相匹配。有关详情，请参见第 21-9 页上的解密操作：解密流量以进一步检查。
- 如果使用外部证书对象配置证书条件，则添加到密码套件条件中的任何密码套件或与 **Decrypt - Resign** 操作相关联的内部 CA 对象必须与外部证书的签名算法类型相匹配。例如，如果规则的证书条件引用基于 EC 的服务器证书，则添加的任何密码套件或与 **Decrypt - Resign** 操作相关联的 CA 证书也必须基于 EC。如果在此情况下签名算法类型不匹配，则策略编辑器会在规则旁边显示警告图标。有关详细信息，请参阅第 22-24 页上的按密码套件控制加密流量和第 21-9 页上的解密操作：解密流量以进一步检查。

要根据服务器证书检查加密流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要根据服务器证书控制加密流量的 SSL 策略中，创建新的 SSL 规则或编辑现有规则。

有关详细说明，请参阅第 21-4 页上的了解和创建 SSL 规则。

步骤 2　在 SSL 规则编辑器中，选择 Certificate 选项卡。

系统将显示 Certificate 选项卡。

步骤 3　从 **Available Certificates** 中查找并选择要添加的服务器证书，如下所示：

- 要即时添加可随后添加到条件中的外部证书对象，请点击 **Available Certificates** 列表上方的添加图标 ( )；请参阅第 3-44 页上的使用外部证书对象。
- 要搜索将添加的证书对象和组，请点击 **Available Certificates** 列表上方的 **Search by name or value** 提示，然后键入对象的名称或对象中的值。列表会在您键入内容时进行更新，以显示匹配对象。

要选择一个对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键，或者右键单击，然后选择 **Select All**。

步骤 4　点击 **Add to Rule** 将所选对象添加到 **Subject Certificates** 列表中。

您也可以拖放所选对象。

步骤 5　添加或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

按证书状态控制加密流量

许可证：任何环境

受支持的设备：3 系列

通过 SSL 规则中的证书状态条件，可以根据用于加密流量的服务器证书的状态（包括证书是否有效、已撤销、已到期、尚未生效、自签名或由受信任 CA 签名）来处理和检查加密流量。

检查颁发或撤销证书的 CA 是否要求将根 CA 证书和中间 CA 证书以及关联的 CRL 作为对象进行上传。然后，将这些受信任 CA 对象添加到 SSL 策略的受信任 CA 证书列表。

对于配置的每个证书状态 SSL 规则条件，可以根据给定状态存在还是缺失来匹配流量。可以在一个规则条件中选择若干状态，如果证书与任何所选状态相匹配，则规则与流量相匹配。

有关详情，请参阅：

- 第 22-20 页上的信任外部证书颁发机构
- 第 22-21 页上的按证书状态匹配流量

信任外部证书颁发机构

许可证：任何环境

受支持的设备：3 系列

您可以通过向 SSL 策略中添加根 CA 证书和中间 CA 证书来信任 CA，然后使用这些受信任 CA 验证用于加密流量的服务器证书。已验证的服务器证书包括由受信任 CA 签名的证书。

如果受信任 CA 证书包含上传的证书撤销列表 (CRL)，则还可以验证受信任 CA 是否已撤销加密证书。有关详情，请参见第 3-43 页上的将证书撤销列表添加到可信 CA 对象。

将受信任 CA 证书添加到 SSL 策略后，可以将具有各种证书状态条件的 SSL 规则配置为根据此流量进行匹配。有关详细信息，请参阅第 3-42 页上的使用可信证书颁发机构对象和第 22-20 页上的按证书状态控制加密流量。

提示　将根 CA 的信任链链中的所有证书都上传到受信任 CA 证书列表中，包括根 CA 证书和所有中间 CA 证书。否则，更难以检测由中间 CA 颁发的受信任证书。

创建 SSL 策略时，系统使用默认 Trusted CA 对象组 Sourcefire Trusted Authorities 填充 Trusted CA Certificates 选项卡。可以修改组中的单个条目，并且选择是否在 SSL 策略中包含该组。不能删除该组。系统更新可以修改此列表中的条目，但会保留用户更改。有关详情，请参见第 20-2 页上的创建基本 SSL 策略。

要向策略中添加受信任 CA，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > SSL**。

系统将显示 SSL Policy 页面。

步骤 2　点击要配置的 SSL 策略旁边的编辑图标 ( )。

系统将显示 SSL 策略编辑器。

步骤 3　选择 **Trusted CA Certificates** 选项卡。

系统将显示 Trusted CA Certificates 页面。

步骤 4　从 **Available Trusted CAs** 中查找并选择要添加的受信任 CA，如下所示：

- 要即时添加可随后添加到条件中的受信任 CA 对象，请点击 **Available Trusted CAs** 列表上方的添加图标 ( )；请参阅第 3-42 页上的使用可信证书颁发机构对象。
- 要搜索将添加的受信任 CA 对象和组，请点击 **Available Trusted CAs** 列表上方的 **Search by name or value** 提示，然后键入对象的名称或对象中的值。列表会在您键入内容时进行更新，以显示匹配对象。

要选择一个对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键，或者右键单击，然后选择 **Select All**。

步骤 5　点击 **Add to Rule** 将所选对象添加到 **Selected Trusted CAs** 列表中。

您也可以拖放所选对象。

步骤 6　添加或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

按证书状态匹配流量

许可证：任何环境

受支持的设备：3 系列

根据证书状态规则条件配置，您可以根据用于加密流量的服务器证书的状态来匹配加密流量。您能够：

- 检查服务器证书状态
- 检查证书是否没有状态
- 跳过检查证书状态存在还是缺失

可以选择根据单个证书状态规则条件中多个证书状态的存在或缺失进行匹配；证书只需匹配其中一个标准即可与规则相匹配。

下表介绍系统如何根据加密服务器证书的状态评估加密流量。

表 22-4　证书状态规则条件标准

状态检查	状态设置为 Yes	状态设置为 No
已撤销	策略信任颁发服务器证书的 CA，并且上传到策略的 CA 证书包含用于撤销服务器证书的 CRL。	策略信任颁发服务器证书的 CA，并且上传到策略的 CA 证书不包含用于撤销证书的 CRL。
自签名	检测到的服务器证书包含相同的主题和颁发者可分辨名称。	检测到的服务器证书包含不同的主题和颁发者可分辨名称。
有效	以下所有情况都成立： • 策略信任颁发证书的 CA • 签名有效 • 颁发者有效 • 策略的受信任 CA 未撤销证书 • 当前日期介于证书的 Valid From 和 Valid To 日期之间	至少以下情况之一成立： • 策略不信任颁发证书的 CA • 签名无效 • 颁发者无效 • 策略中的受信任 CA 已撤销证书 • 当前日期在证书的 Valid From 日期之前 • 当前日期在证书的 Valid To 日期之后
签名无效	无法根据证书的内容正确验证证书的签名。	根据证书的内容正确验证证书的签名。
颁发者无效	颁发者 CA 证书未存储在策略的受信任 CA 证书列表中。	颁发者 CA 证书存储在策略的受信任 CA 证书列表中。
已到期	当前日期在证书的 Valid To 日期之后。	当前日期在证书的 Valid To 日期之前或当日。
尚未生效	当前日期在证书的 Valid From 日期之前。	当前日期在证书的 Valid From 日期之后或当日。

请考虑以下示例。组织信任 Verified Authority 证书颁发机构。组织不信任 Spammer Authority 证书颁发机构。系统管理员将 Verified Authority 证书和由 Verified Authority 颁发的中间 CA 证书上传到系统。由于 Verified Authority 已撤销其以前颁发的证书，因此系统管理员上传该 Verified Authority 分发的 CRL。

下图说明用于检查有效证书、由 Verified Authority 颁发的证书、不在 CRL 上的证书以及仍在 Valid From 和 Valid To 日期内的证书的证书状态规则条件。受配置原因的影响，未通过访问控制来解密和检查使用这些证书加密的流量。

下图说明用于检查状态是否缺失的证书状态规则条件。在此情况下，由于配置原因，它与使用尚未到期的证书加密的流量相匹配并监控该流量。

下图说明根据若干状态的存在或缺失进行匹配的证书状态规则条件。由于配置原因，如果规则与使用由无效用户颁发的证书、自签名证书、无效证书或已到期证书加密的传入流量相匹配，则该规则使用已知密钥来解密流量。

请注意，即使证书可能匹配多个状态，但是规则仅对流量执行一次操作。

要按服务器证书状态检查加密流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要根据服务器证书状态控制加密流量的 SSL 策略中，创建新的 SSL 规则或编辑现有规则。

有关详细说明，请参阅第 21-4 页上的了解和创建 SSL 规则。

步骤 2　在 SSL 规则编辑器中，选择 Cert Status 选项卡。

系统将显示 Cert Status 选项卡。

步骤 3　对于每个证书状态，具有以下选项：

- 选择 **Yes** 可根据该证书状态是否存在进行匹配。
- 选择 **No** 可根据该证书状态是否缺失进行匹配。
- 选择 **Do Not Match** 将不匹配该证书状态。

步骤 4　添加或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

按密码套件控制加密流量

许可证：任何环境

受支持的设备：3 系列

通过 SSL 规则中的密码套件条件，可以根据用于协商加密会话的密码套件来处理和检查加密流量。思科提供可向密码套件规则条件中添加的预定义密码套件。您还可以添加包含多个密码套件的密码套件列表对象。有关密码套件列表的详细信息，请参阅第 3-35 页上的使用密码套件列表。

注　不能添加新的密码套件。不能修改和删除预定义密码套件。

在单个密码套件条件中，可以向 **Selected Cipher Suites** 添加最多 50 个密码套件和密码套件列表。

请注意：

- 如果添加部署不支持的密码套件，则无法应用与 SSL 策略相关联的访问控制策略。例如，被动部署不支持使用任何短 Diffie-Hellman (DHE) 或短椭圆曲线 Diffie-Hellman (ECDHE) 密码套件来解密流量。使用这些密码套件创建规则将会阻止应用访问控制策略。
- 如果使用密码套件配置密码套件条件，则添加到证书条件中的任何外部证书对象或与 **Decrypt - Resign** 操作相关联的内部 CA 对象必须与密码套件的签名算法类型相匹配。例如，如果规则的密码套件条件引用基于 EC 的密码套件，则添加的任何服务器证书或与 **Decrypt - Resign** 操作相关联的 CA 证书也必须基于 EC。如果在此情况下签名算法类型不匹配，则策略编辑器会在规则旁边显示警告图标。有关详细信息，请参阅第 22-24 页上的按密码套件控制加密流量和第 21-9 页上的解密操作：解密流量以进一步检查。
- 系统无法解密使用匿名密码套件加密的流量。如果向 **Cipher Suite** 条件中添加匿名密码套件，则在 SSL 规则中无法使用 **Decrypt - Resign** 或 **Decrypt - Known Key** 操作。

要按密码套件检查加密流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要按密码套件控制加密流量的 SSL 策略中，创建新的 SSL 规则或编辑现有规则。

有关详细说明，请参阅第 21-4 页上的了解和创建 SSL 规则。

步骤 2　在 SSL 规则编辑器中，选择 Cipher Suite 选项卡。

系统将显示 Cipher Suite 选项卡。

步骤 3　从 **Available Cipher Suites** 查找并选择要添加的密码套件，如下所示：

- 要即时添加可随后添加到条件中的密码套件列表，请点击 **Available Cipher Suites** 列表上方的添加图标 ( )；请参阅第 3-35 页上的使用密码套件列表。
- 要搜索将添加的密码套件和列表，请点击 **Available Cipher Suites** 列表上方的 **Search by name or value** 提示，然后键入密码套件的名称或密码套件中的值。列表会在您键入内容时进行更新，以显示匹配的密码套件。

要选择密码套件，请点击该密码套件。要选择多个密码套件，请使用 Shift 和 Ctrl 键，或者右键单击，然后选择 **Select All**。

步骤 4　点击 **Add to Rule** 将所选密码套件添加到 **Selected Cipher Suites** 列表。

您也可以拖放所选密码套件。

步骤 5　添加或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

按加密协议版本控制流量

许可证：任何环境

受支持的设备：3 系列

通过 SSL 规则中的会话条件，可以根据用于加密流量的 SSL 或 TLS 版本来检查加密流量。可以选择根据使用 SSL V3.0 或 TLS V1.0、V1.1 或 V1.2 加密的流量进行匹配。默认情况下，在创建规则时会选择所有协议版本；如果选择多个版本，则与任何所选版本相匹配的加密流量都与该规则相匹配。保存规则条件时，必须至少选择一个协议版本。

注　可以在版本规则条件中选择 SSL V2.0；系统不支持解密使用 SSL V2.0 加密的流量。可以配置无法解密的操作来允许或阻止此流量而不进一步检查。有关详细信息，请参阅第 38-11 页上的记录可用 SSL 规则解密的连接。

要按 SSL 或 TLS 版本检查加密流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在要按加密协议版本控制加密流量的 SSL 策略中，创建新的 SSL 规则或编辑现有规则。

有关详细说明，请参阅第 21-4 页上的了解和创建 SSL 规则。

步骤 2　在 SSL 规则编辑器中，选择 Version 选项卡。

系统将显示 Version 选项卡。

步骤 3　选择要与其匹配的协议版本：**SSL v3.0**、**TLS v1.0**、**TLS v1.1** 或 **TLS v1.2**。

步骤 4　添加或继续编辑规则。

必须应用与 SSL 策略关联的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

了解网络分析和入侵策略

网络分析和入侵策略作为 FireSIGHT 系统的 入侵检测和防御功能的一部分，共同发挥作用。术语*入侵检测*通常指被动分析网络流量以寻找潜在入侵，并存储攻击数据用于安全分析的过程。术语*入侵防御*包括入侵检测的概念，但是增加了在恶意流量流经网络时对其进行拦截或更改的能力。

在入侵防御部署中，当系统检查数据包时：

- **网络分析策略**监管如何对流量进行*解码*和*预处理*，以便进一步评估，尤其是针对可能预示入侵企图的异常流量。
- **入侵策略**使用*入侵和预处理程序规则*（有时统称为*入侵规则*）根据模式检查已解码的数据包中是否存在攻击。入侵策略与*变量集*配对，允许您使用指定值准确反映您的网络环境。

网络分析和入侵策略由父访问控制策略在不同时间调用。在系统分析流量期间，网络分析 （解码和预处理）阶段发生在入侵防御 （其他预处理和入侵规则）阶段之前并且独立进行。网络分析和入侵策略共同提供广泛和深入的数据包检测。它们可以帮助您检测、警告和防止可能威胁主机及其数据的可用性、完整性和保密性的网络流量。

FireSIGHT 系统 附有若干名称类似的网络分析和入侵策略 （例如， Balanced Security and Connectivity），它们互为补充并且相互配合。通过系统提供的策略，您可以利用思科漏洞研究团队 (VRT) 的经验。对于这些策略，VRT 设置入侵和预处理程序规则状态，并提供预处理程序和其他高级设置的初始配置。

您还可以创建自定义网络分析和入侵策略。您可以调整自定义策略中的设置，以对您最重要的方式检查流量，从而能够提高受管设备的性能以及您有效响应其生成的事件的能力。

您可在网络界面中使用相似的策略编辑器创建、编辑、保存和管理网络分析和入侵策略。在您编辑任一类型的策略时，导航面板显示在网络界面的左侧；右侧显示各种配置页面。

本章简要概述网络分析和入侵策略监管的配置类型，说明策略如何协作以检查流量和生成策略违例记录，以及提供有关对策略编辑器进行导航的基本信息。本章还说明使用自定义策略与系统提供的策略的优点和局限性。有关详细信息，请参阅以下各节：

- 第 23-2 页上的了解策略如何检查流量是否存在入侵
- 第 23-6 页上的比较系统提供的策略与自定义策略
- 第 23-12 页上的使用导航面板
- 第 23-13 页上的解决冲突和提交策略更改

要自定义入侵部署，请参阅以下内容来获取后续步骤：

- 第 3-15 页上的使用变量集说明如何配置系统的入侵变量以准确反映您的网络环境。即使您不使用自定义策略，思科**也强烈**建议您修改默认变量集中的默认变量。高级用户可创建和使用自定义变量集，以将其与一个或多个自定义入侵策略配对。
- 第 31-1 页上的入侵策略入门介绍如何创建和编辑简单的自定义入侵策略。

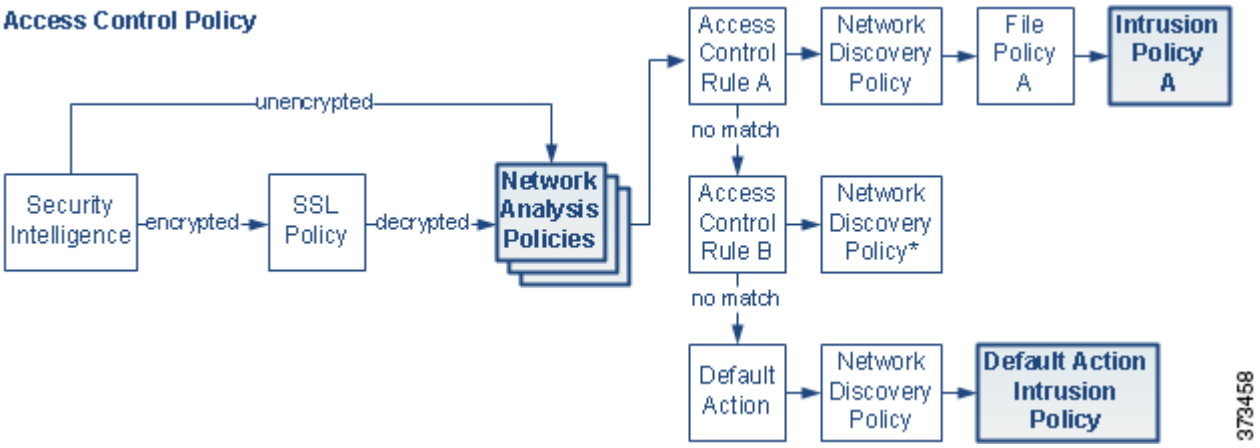
- 第 18-1 页上的使用入侵和文件策略控制流量说明如何配置系统通过将入侵策略与父访问控制策略相关联使用入侵策略仅检查您感兴趣的流量。还说明了如何配置高级入侵策略性能选项。
- 第 29-1 页上的配置高级传输/网络设置说明如何配置全局适用于由访问控制策略的目标设备处理的所有流量的高级传输和网络预处理程序设置。您可以在访问控制策略而不是网络分析或入侵策略中配置这些高级设置。
- 第 26-1 页上的网络分析策略使用入门介绍如何创建和编辑简单的自定义网络分析策略。
- 第 25-2 页上的使用网络分析策略自定义预处理介绍如何更改默认网络分析策略。对于高级用户，本节还说明了如何分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 定制预处理。
- 第 24-1 页上的在网络分析或入侵策略中使用层说明在大型组织或复杂部署中，如何使用称为策略*层*的构建块来更有效地管理多个网络分析或入侵策略。

了解策略如何检查流量是否存在入侵

许可证：保护

作为访问控制部署的一部分，系统将对流量进行分析，在此期间网络分析 （解码和预处理）阶段发生在入侵防御 （入侵规则和高级设置）阶段之前并且独立进行。

下图以简化方式显示内联入侵防御和高级恶意软件防护 (AMP) 部署中的流量分析顺序。它说明访问控制策略如何调用其他策略检查流量，以及按何种顺序调用这些策略。网络分析和入侵策略选择阶段突出显示。



在内联部署中，系统可以阻止流量，而不在图示过程中的几乎任何步骤进一步检查。安全智能、SSL 策略、网络分析策略、文件策略和入侵策略均可以丢弃或修改流量。只有网络发现策略 （被动检查的数据包）无法影响流量的流动。

同样，在进程的每个步骤中，数据包都可能导致系统生成事件。入侵和预处理程序事件 （有时统称为*入侵事件*）指示数据包或其内容可能表示安全风险。

提示 当您的 SSL 配置允许已加密流量通过，或者您未配置 SSL 检查时，此图未反映访问控制规则处理已加密流量。默认情况下，系统禁用对加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。有关详细信息，请参阅第 19-1 页上的了解流量解密和第 27-60 页上的使用 SSL 预处理器。

请注意，对于单条连接，尽管系统会选择先网络分析策略再选择访问控制策略（如图所示），但在选择访问控制规则之后还是会进行一些预处理（特别是应用层预处理）。这**不会**影响您如何在自定义网络分析策略中配置预处理。

有关详情，请参阅：

- 第 23-3 页上的解码、规范化和预处理：网络分析策略
- 第 23-4 页上的访问控制规则：入侵策略选择
- 第 23-5 页上的入侵检查：入侵策略、规则和变量集
- 第 23-6 页上的生成入侵事件

解码、规范化和预处理：网络分析策略

许可证：保护

如果没有解码和预处理，则系统无法适当评估流量是否存在入侵，因为协议差异使得无法进行模式匹配。如第 23-2 页上的了解策略如何检查流量是否存在入侵中的示意图所示，网络分析策略监管这些流量处理任务：

- 在流量由安全情报过滤**之后**
- 在已加密会话由可选 SSL 策略解密**之后**
- 在流量可以由文件或入侵策略检查**之前**

网络分析策略分阶段监管数据包处理。系统首先通过前三个 TCP/IP 层解码数据包，然后继续规范化、预处理和检测协议异常：

- 数据包解码器将数据包报头和负载转换为可由预处理程序并在以后由规则引擎轻松使用的格式。TCP/IP 栈的各层依次解码，从数据链路层开始并继续到网络层和传输层。数据包解码器还会检测数据包报头中的各种异常行为。有关详细信息，请参阅第 29-14 页上的了解数据包解码。
- 在内联部署中，内联规范化预处理程序重新格式化（规范化）流量，以尽量降低攻击者逃避检测的可能性。它会准备数据包以供其他预处理程序和入侵规则进行检查，并且帮助确保系统处理的数据包与网络上主机接收的数据包相同。有关详细信息，请参阅第 29-6 页上的规范化内联流量。

提示 在被动部署中，思科建议您在访问控制策略级别配置自适应配置文件，而非在网络分析级别配置内联规范化。有关详细信息，请参阅第 30-1 页上的调整被动部署中的预处理。

- 各种网络层和传输层预处理程序检测利用 IP 分段的攻击，执行校验和验证，以及执行 TCP 和 UDP 会话预处理；请参阅第 29-1 页上的配置传输和网络层预处理。

  请注意，一些高级传输和网络预处理程序设置全局适用于由访问控制策略的目标设备处理的所有流量。您在一个访问控制策略而非网络分析策略中配置这些高级设置；请参阅第 29-1 页上的配置高级传输/网络设置。
- 各种应用层协议解码器将特定类型的数据包数据规范化为入侵规则引擎可以分析的格式。规范化应用层协议编码后，系统就可将相同的内容相关的入侵规则有效地应用于数据以不同方式表示的数据包，并获得有意义的结果。有关详细信息，请参阅第 27-1 页上的使用应用层预处理器。

- Modbus 和 DNP3 SCADA 预处理程序检测异常流量并向入侵规则提供数据。监控与数据采集 (SCADA) 协议可监视和控制工业、基础设施以及工厂流程 （例如制造、生产、水处理、配电、机场和运输系统等）并从中获取数据。有关详细信息，请参阅第 28-1 页上的配置 SCADA 预处理。
- 通过若干预处理程序，可以检测特定威胁，如 Back Orifice、端口扫描、 SYN 泛洪和其他基于速率的攻击；请参阅第 34-1 页上的检测特定威胁。

  请注意，您配置敏感数据预处理程序，它会检测入侵策略中的敏感数据，如 ASCII 文本形式的信用卡号与社会保障号；请参阅第 34-17 页上的检测敏感数据。

在新建的访问控制策略中，一个默认网络分析策略监管对同一父访问控制策略调用的*所有*入侵策略的*所有*流量的预处理。最初，系统使用 Balanced Security and Connectivity 网络分析策略作为默认值，但是，可以将其更改为另一个系统提供的网络分析策略或自定义网络分析策略。在更复杂的部署中，高级用户可以分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 定制流量预处理选项。有关详细信息，请参阅第 23-6 页上的比较系统提供的策略与自定义策略。

访问控制规则：入侵策略选择

许可证：保护

在初始预处理后，访问控制规则 （如果存在）会评估流量。在大多数情况下，数据包匹配的第一条访问控制规则处理该流量；您可以监控、信任、阻止或允许匹配流量。

当使用访问控制规则允许流量时，系统可能按该顺序检查流量是否存在发现数据、恶意软件、受禁文件和入侵。不与任何访问控制规则匹配的流量由访问控制策略的默认操作进行处理，该操作还检查是否存在发现数据和入侵。

注　所有数据包 （**无论**哪个网络分析策略对其进行预处理）均与配置的访问控制规则相匹配，因此可能会由上而下受到入侵策略的检查。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

第 23-2 页上的了解策略如何检查流量是否存在入侵中的图显示通过内联入侵防御和 AMP 部署中的某台设备的流量，如下所述：

- Access Control Rule A 允许匹配流量通过。然后该流量由网络发现策略检查是否存在发现数据，由 File Policy A 检查是否存在受禁文件和恶意软件，最后由 Intrusion Policy A 检查是否存在入侵。
- Access Control Rule B 也允许匹配流量通过。但是，在此情景中，未检查流量是否存在入侵（或文件或恶意软件），因此没有与规则关联的入侵或文件策略。请注意，默认情况下，您允许通过的流量将由网络发现策略进行检查；您不需要配置此检查。
- 在此情景中，访问控制策略的默认操作允许匹配流量通过。然后该流量将依次由网络发现策略和入侵策略进行检查。当您将入侵策略与访问控制规则或默认操作相关联时，您可以 （但不是必须）使用不同的入侵策略。

图中的示例不包括任何阻止或信任规则，因为系统不检查已阻止或信任的流量。有关详细信息，请参阅第 14-6 页上的使用规则操作确定流量处理和检查和第 12-6 页上的设置对网络流量的默认处理和检查。

入侵检查：入侵策略、规则和变量集

许可证：保护

可使用入侵防御作为系统在允许流量到达目的地之前的最后一道防线。入侵策略监管系统如何检查流量是否存在安全违规，并且在内联部署中可以阻止或修改恶意流量。入侵策略的主要功能是管理启用哪些入侵和预处理程序规则及其如何配置。

入侵和预处理程序规则

入侵规则是一组指定的关键字和参数，用于检测企图利用网络漏洞的行为；系统使用入侵规则分析网络流量以检查其是否符合规则中的条件。系统将数据包与每条规则中指定的条件进行比较，如果数据包数据符合规则中指定的所有条件，则触发此规则。

系统包括 VRT 创建的以下类型的规则：

- *共享对象入侵规则*，该规则已编译，无法修改（诸如源和目标端口和 IP 地址等规则头信息除外）
- *标准文本入侵规则*，该规则可以保存并修改为规则的新自定义实例。
- *预处理程序规则*，这些是与网络分析策略中的预处理程序和数据包解码器检测选项相关联的规则。预处理程序规则不能复制或编辑。默认情况下，大多数预处理程序规则均已禁用；您必须将其启用才能使用预处理程序生成事件，并在内联部署中丢弃有问题的数据包。

当系统根据入侵策略处理数据包时，首先由规则优化程序根据以下标准对子集中的所有已激活规则进行分类：传输层、应用协议、来自或发往受保护网络等。然后，入侵规则引擎选择适当的规则子集应用于每个数据包。最后，多规则搜索引擎执行三种不同类型的搜索以确定流量是否与规则相匹配：

- 协议字段搜索在应用协议的特定字段中查找匹配项。
- 一般内容搜索在数据包负载中查找 ASCII 或二进制字节匹配项。
- 数据包异常搜索查找没有包含特定内容而是违反既定协议的数据包报头和负载。

在自定义入侵策略中，可通过启用和禁用规则，以及撰写和添加您自己的标准文本规则来调整检测。还可以遵从 FireSIGHT 建议，将在您的网络中检测到的操作系统、服务器和客户端应用协议与为了保护这些资产而特别编写的规则相关联。

变量集

每当系统使用入侵策略评估流量时，它使用相关的*变量集*。变量集中的大多数变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。还可以在入侵策略中使用变量表示规则抑制和动态规则状态中的 IP 地址。

默认情况下，系统提供一个默认变量集，它包含预定义默认变量。系统提供的大多数共享对象规则和标准文本规则均使用这些预定义默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护的（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。

提示 即使您使用系统提供的入侵策略，思科也**强烈**建议修改默认变量集中的关键默认变量。当使用准确反映网络环境的变量时，处理会得以优化，并且系统可以监控相关系统是否存在可疑活动。高级用户可创建和使用自定义变量集，以将其与一个或多个自定义入侵策略配对。有关详细信息，请参阅第 3-16 页上的优化预定义默认变量。

生成入侵事件

许可证：保护

当系统识别可能的入侵时，它会生成*入侵*或*预处理程序事件*（有时统称为入侵事件）。受管设备将其事件传输到防御中心，在其中可以查看聚合数据并更好地了解针对网络资产的攻击。在内联部署中，受管设备还可以丢弃或替换已知有害的数据包。

数据库中的每个入侵事件均包括事件报头并包含有关事件名称和分类的信息；源和目标 IP 地址；端口；生成事件的进程；事件的日期和时间，以及有关攻击源及其目标的情景信息。对于基于数据包的事件，系统还记录触发事件的数据包的已解码的数据包报头和负载的副本。

数据包解码器、预处理程序和入侵规则引擎都可能导致系统生成事件。例如：

- 如果数据包解码器（在网络分析策略中配置）接收少于 20 字节（没有任何选项或负载的 IP 数据报的大小）的 IP 数据包，解码器将此解释为异常流量。如果之后启用了用于检查数据包的入侵策略中的配套解码器规则，则系统会生成预处理程序事件。
- 如果 IP 分片重组预处理程序遇到一系列重叠的 IP 片段，则预处理程序会将此解释为可能的攻击，当启用了配套预处理程序规则时，系统会生成预处理程序事件。
- 在入侵规则引擎内，大多数标准文本规则和共享对象规则编写为在由数据包触发时会生成入侵事件。

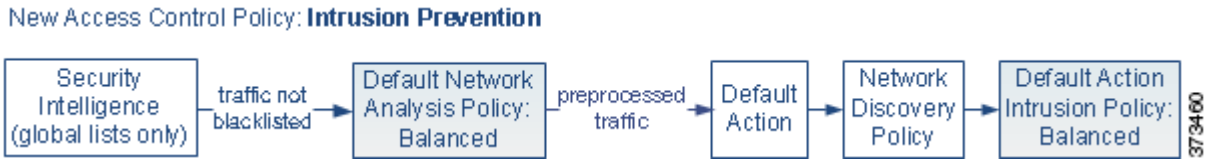
随着数据库累计入侵事件，您可以开始分析潜在攻击。系统还提供必要的工具，可以用来审查入侵事件并评估它们在网络环境和安全策略中是否重要。

比较系统提供的策略与自定义策略

许可证：保护

新建访问控制策略是使用 FireSIGHT 系统管理流量的初始步骤之一。默认情况下，新建的访问控制策略调用系统提供的网络分析和入侵策略来检查流量。

下图显示内联入侵防御部署中新建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。



请注意以下各种操作的方式：

- 默认网络分析策略监管访问控制策略处理的*所有*流量的预处理。最初，系统提供的 *Balanced Security and Connectivity 网络分析策略*是默认策略。
- 访问控制策略的默认操作允许所有非恶意流量（由系统提供的 *Balanced Security and Connectivity 入侵策略*确定）通过。由于默认操作允许流量通过，在入侵策略能够检查并可能阻止恶意流量之前，发现功能可以检查流量中的主机、应用和用户数据。
- 策略使用默认的安全情报选项（仅全局白名单和黑名单），不使用 SSL 解密已加密的流量，并且不使用访问控制规则对网络流量执行特殊处理和检查。

可以采取用于调整入侵防御部署的一个简单步骤是使用系统提供的一组不同的网络分析和入侵策略为作为默认值。思科通过 FireSIGHT 系统提供了多对网络分析和入侵策略。

或者，您可以通过创建和使用自定义策略来定制您的入侵防御部署。不过，您可能会发现这些策略中配置的预处理程序选项、入侵规则和其他高级设置无法满足网络的安全需求。通过调整网络分析和入侵策略，可以非常精细地配置系统如何处理网络流量并检查其是否存在入侵。

有关详情，请参阅：

- 第 23-7 页上的了解系统提供的策略
- 第 23-8 页上的自定义策略的优点
- 第 23-10 页上的自定义策略的局限性

了解系统提供的策略

许可证：保护

思科通过 FireSIGHT 系统提供了多对网络分析和入侵策略。使用系统提供的网络分析和入侵策略，您可以利用思科漏洞研究团队 (VRT) 的经验。对于这些策略，VRT 设置入侵和预处理程序规则状态，并提供预处理程序和其他高级设置的初始配置。您可以原样使用系统提供的策略，也可以使用其作为自定义策略的基础。

提示 即使您使用系统提供的网络分析和入侵策略，也应该配置系统的入侵变量，以准确反映网络环境。至少修改默认变量集中的关键默认变量；请参阅第 3-16 页上的优化预定义默认变量。

随着新漏洞变成已知，VRT 会发布入侵规则更新。这些规则更新可以修改系统提供的任何网络分析或入侵策略，并且可以提供新的和已更新的入侵规则及预处理程序规则、现有规则的已修改状态，以及已修改的默认策略设置。规则更新也可以从系统提供的策略中删除规则并提供新规则类别，还可以修改默认变量集。

如果规则更新影响您的部署，则网络界面将受影响的入侵和网络分析策略标记为已过期，并标记其父访问控制策略。只有重新应用已更新的策略才能使其更改生效。

为了您的方便，您可将规则更新配置为自动重新应用受影响的入侵策略，无论是单独还是与受影响的访问控制策略一起应用。这使，您就可轻松地让您的部署自动保持与时俱进，从而防范最新发现的漏洞和入侵。

为了确保最新预处理设置，**必须**重新应用访问控制策略，该策略也会重新应用与当前运行的策略不同的所有关联的 SSL、网络分析和文件策略，同时还可以更新高级预处理和性能选项的默认值。有关详细信息，请参阅 第 66-13 页上的导入规则更新和本地规则文件。

思科通过 FireSIGHT 系统提供以下网络分析和入侵策略：

Balanced Security and Connectivity 网络分析和入侵策略

这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数组织和部署类型的良好起点。系统在大多数情况下均使用 Balanced Security and Connectivity 策略和设置作为默认值。

Connectivity Over Security 网络分析和入侵策略

这些策略专为连接性 （能够获取所有资源）优先于网络基础设施安全性的组织而构建。此入侵策略启用的规则远远少于 Security over Connectivity 策略中启用的规则。只有妨碍流量的最重要的规则才被启用。

Security Over Connectivity 网络分析和入侵策略

这些策略专为网络基础设施安全性优先于用户便利性的组织而构建。此入侵策略启用可能就合法流量发出警报或放弃合法流量的许多网络异常入侵规则。

No Rules Active 入侵策略

在 No Rules Active 入侵策略中，所有入侵规则和高级设置均已禁用。如果您要创建自己的入侵策略而不是将其基于系统提供的其他策略之一中的已启用规则，则此策略提供一个起点。

注意事项　思科使用另一个策略 `Experimental Policy 1` 进行测试。请勿使用 Experimental Policy 1，除非思科代表指示这样做。

自定义策略的优点

许可证：保护

您可能会发现系统提供的网络分析和入侵策略中配置的预处理程序选项、入侵规则和其他高级设置不完全满足贵组织的安全需要。

构建自定义策略可以提高系统在环境中的性能，并且可以更密切监控在网络上发生的恶意流量和违反策略的情况。通过创建和调整自定义策略，可以非常精细地配置如何系统处理和检查网络流量是否存在入侵。

所有自定义策略都具有基本策略 （也称为基层），用于为策略中所有配置定义默认设置。层是一个构建块，可供您有效地管理多个网络分析或入侵策略；请参阅第 24-1 页上的在网络分析或入侵策略中使用层。

在大多数情况下，您将根据系统提供的策略构建自定义策略，但是，您也可以使用其他自定义策略。然而，所有自定义策略都有一个系统提供的策略作为策略链中最终基础。由于规则更新会修改系统提供的策略，因此导入规则更新可能会影响您，即使是使用自定义策略作为基础也如此。如果规则更新影响部署，则网络界面将受影响策略标记为过期。有关详细信息，请参阅第 24-4 页上的允许规则更新修改系统提供的基本策略。

除了您创建的自定义策略之外，系统还提供两种自定义入侵策略和两种自定义网络分析策略：初始内联策略和初始被动策略。这些策略使用相应的 Balanced Security and Connectivity 策略作为其基本策略。两种策略之间的唯一区别在于其 *丢弃行为*，该行为在内联策略中启用流量阻止和修改，在被动策略中禁用该功能。您可以编辑和使用系统提供的这些自定义策略。

有关详情，请参阅：

- 第 23-8 页上的自定义网络分析策略的优点
- 第 23-9 页上的自定义入侵策略的优点

自定义网络分析策略的优点

许可证：保护

默认情况下，一个网络分析策略预处理访问控制策略处理的所有未加密流量。这意味着根据设置相同设置对所有数据包进行解码和预处理，无论之后检查数据包的入侵策略 （和入侵规则集）如何。

最初，系统提供的 Balanced Security and Connectivity 网络分析策略是默认策略。调整预处理的一个简单方法是创建和使用自定义网络分析策略作为默认值；请参阅第 25-3 页上的为访问控制设置默认网络分析策略。

可用的调整选项因预处理程序而异，但是可以调整预处理程序和解码器的一些方法包括：

- 可以禁用不适用于正在监控的流量的预处理程序。例如， HTTP Inspect 预处理程序规范化 HTTP 流量。如果确信网络中没有任何使用 Microsoft 互联网信息服务 (IIS) 的 Web 服务器，则可以禁用查找特定于 IIS 的流量的预处理程序选项，从而减少系统处理开销。

注 如果禁用自定义网络分析策略中的预处理程序，但系统稍后需要使用该预处理程序利用已启用的入侵或预处理程序规则对数据包进行评估，系统会自动启用并使用预处理程序，不过它在网络分析策略网络界面中保持禁用。

- 在适当情况下指定端口，以某些预处理程序的活动为重点。例如，可以确定要对 DNS 服务器响应或加密 SSL 会话进行监控的其他端口，或者确定解码 telnet、 HTTP 和 RPC 流量所在的端口

对于采用复杂部署的高级用户，可以创建多个网络分析策略，每个策略量身定制以不同方式对流量进行预处理。然后，可以配置系统使用这些策略管理使用不同的安全区域、网络或 VLAN 的流量的预处理。（请注意， ASA FirePOWER 设备无法通过 VLAN 限制预处理。）

注 使用自定义网络分析策略定制预处理 （特别是使用多个网络分析策略）是一项高级任务。由于预处理和入侵检查密切相关，因此，您**必须**注意，要确保允许检查单个数据包的网络分析和入侵策略能够互补。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

自定义入侵策略的优点

许可证：保护

在新建的初始配置为执行入侵防御的访问控制策略中，默认操作允许所有流量，但是首先会使用系统提供的 Balanced Security and Connectivity 入侵策略对流量进行检查。除非添加访问控制规则或更改默认操作，否则所有流量都由该入侵策略进行检查；请参阅第 23-6 页上的比较系统提供的策略与自定义策略中的图。

要自定义入侵防御部署，可以创建多个入侵策略，每个策略定制为以不同方式检查流量。然后，使用指定哪个策略检查哪个流量的规则来配置访问控制策略。访问控制规则可能很简单，也可能很复杂，使用多个条件来匹配和检测流量，包括安全区域、网络或地理位置、 VLAN、端口、应用、请求的 URL 或用户。第 23-2 页上的了解策略如何检查流量是否存在入侵中的情景显示由两个入侵策略之一检查流量的部署。

入侵策略的主要功能是管理启用哪些入侵和预处理程序规则及其如何配置，如下所示：

- 在每个入侵策略内，您应确认适用于您的环境的所有规则均已启用，并通过禁用不适用于您的环境的规则来提高性能。在内联部署中，可指定哪些规则应该丢弃或修改恶意数据包。有关详细信息，请参阅第 32-18 页上的设置规则状态。
- 如果遵从 FireSIGHT 的建议，则可将您的网络中检测到的操作系统、服务器和客户端应用协议与为了保护这些资产而特别编写的规则相关联；请参阅第 33-1 页上的为您的网络资产定制入侵防御。
- 您可以根据需要修改现有规则和编写新 标准文本规则，以捕获新的漏洞或执行您的安全策略；请参阅第 36-1 页上的了解和编写入侵规则。

您可对入侵策略做出的其他自定义包括：

- 敏感数据预处理程序检测敏感信息，例如 ASCII 文本格式的信用卡号和社会保障号。请注意，检测具体威胁的其他预处理程序 （Back Orifice 攻击、多种端口扫描类型和试图通过大量流量淹没网络的基于速度的攻击）在网络分析策略中配置。有关详细信息，请参阅第 34-1 页上的检测特定威胁。
- 全局阈值导致系统根据与入侵规则匹配的流量在指定时间段内源自或流向特定地址或地址范围的次数来生成事件。这有助于防止系统无法应付大量涌现的事件。有关详细信息，请参阅第 35-1 页上的从全局限制入侵事件记录。

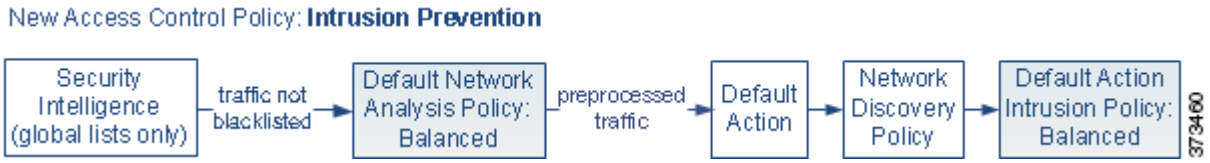
- 禁止入侵事件通知和设置个别规则或全体入侵策略的阈值也可以防止系统被大量事件淹没。有关详细信息，请参阅第 32-20 页上的按策略过滤入侵事件通知。
- 除了网络界面中的各种入侵事件视图之外，您还可以启用将日志记录到系统日志工具或者将事件数据发送到 SNMP 陷阱服务器。根据策略，您可以指定入侵事件通知限制，设置发送到外部日志记录工具的入侵事件通知，以及配置对入侵事件的外部响应。请注意，除了基于策略的这些警报配置，对于每个规则或规则组，您还可以在入侵事件上全局启用或禁用邮件警报。无论处理数据包的是哪个入侵策略，都会使用您的邮件警报设置。有关详细信息，请参阅第 44-1 页上的配置入侵规则的外部警报。

自定义策略的局限性

许可证：保护

由于预处理和入侵检测如此密切相关，因此，您**必须**小心确保自己的配置允许网络和入侵策略处理和检查单个数据包，以实现互补。

默认情况下，系统使用一个网络分析策略预处理由受管设备使用单个访问控制策略处理的所有流量。下图显示内联入侵防御部署中新建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。



请留意默认网络分析策略如何监管访问控制策略处理的*所有*流量的预处理。最初，系统提供的 Balanced Security and Connectivity 网络分析策略是默认策略。

调整预处理的一种简单方法是创建并使用自定义网络分析策略作为默认值，如第 23-8 页上的自定义网络分析策略的优点中概述。如果在自定义网络分析策略中禁用预处理程序，但系统需要使用已启用的入侵或预处理程序规则对预处理过的数据包进行评估，系统会自动启用并使用该预处理程序，不过它在网络分析策略网络界面中保持禁用。

注　为了获取禁用预处理程序的性能优势，您**必须**确保自己的入侵策略均未启用需要该预处理程序的规则。

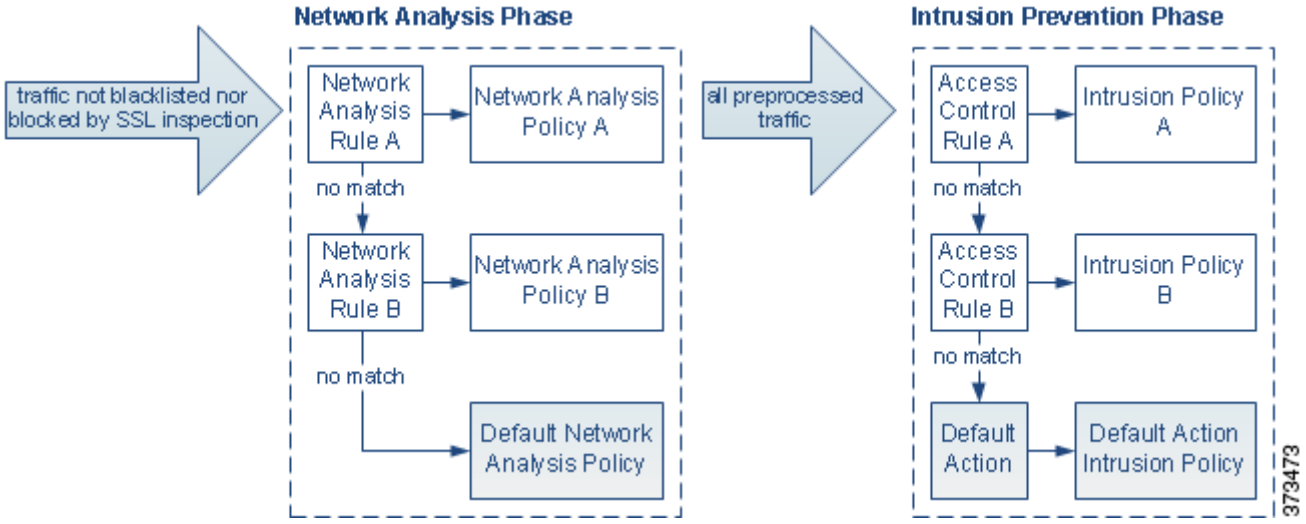
如果使用多个自定义网络分析策略，则会引起其他挑战。对于使用复杂部署的高级用户，可以分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 自定义预处理。（请注意， ASA FirePOWER 设备无法通过 VLAN 限制预处理。）为实现此目的，您可以将自定义*网络分析规则*添加到您的访问控制策略。每条规则均具有关联的网络分析策略，用于监管与该规则匹配的流量的预处理。

提示　可以将网络分析规则配置为访问控制策略中的高级设置。不同于 FireSIGHT 系统 中其他类型的规则，网络分析规则调用 （而不是被纳入）网络分析策略。

系统按规则号由上而下将数据包与任何已配置的网络分析规则相匹配。不与任何网络分析规则相匹配的流量由默认网络分析策略预处理。虽然这使您在预处理流量时具有极大灵活性，但请记住，所有数据包**无论**由哪个网络分析策略进行了预处理，后来都会与访问控制规则匹配，从而在

其各自的进程中可能由入侵策略检查。换句话说，使用特定网络分析策略预处理数据包**不**保证将通过任何特殊入侵策略检查该数据包。您**必须**仔细配置访问控制策略，以使其调用正确的网络分析和入侵策略来评估特殊数据包。

下图重点显示网络分析策略 （预处理）选择阶段如何先于且独立于入侵防御 （规则）阶段发生。为简单起见，此图省去了发现和文件/恶意软件检查阶段。它还突出显示默认网络分析和默认动作入侵策略。



在此情景中，访问控制策略配置为拥有两条网络分析规则和一个默认网络分析策略：

- Network Analysis Rule A 预处理与 Network Analysis Policy A 匹配的流量。之后，您希望此流量由 Intrusion Policy A 检查。
- Network Analysis Rule B 预处理与 Network Analysis Policy B 匹配的流量。之后，您希望此流量由 Intrusion Policy B 检查。
- 所有其他剩余流量由默认网络分析策略进行预处理。之后，您希望此流量由与访问控制策略的默认操作关联的入侵策略进行检查。

在系统预处理流量之后，系统可以检查流量是否存在入侵。下图显示了具有两条访问控制规则和一个默认操作的访问控制策略：

- Access Control Rule A 允许匹配流量通过。该流量然后由 Intrusion Policy A 进行检查。
- Access Control Rule B 允许匹配流量通过。该流量然后由 Intrusion Policy B 进行检查。
- 访问控制策略的默认操作允许匹配流量通过。该流量然后由默认操作的入侵策略进行检查。

每个数据包的处理均由网络分析策略和入侵策略对进行监管，但系统**不**为您协调该策略对。请考虑以下情景：访问控制策略配置错误，以致网络分析规则 A 和访问控制规则 A 不处理相同流量。例如，您可能希望配对的策略监管特殊安全区域上流量的处理，但是在两条规则的条件中错误地使用不同的区域。这可能导致流量被错误地预处理。因此，使用网络分析规则和自定义策略定制预处理是一**项高级**任务。

请注意，对于单条连接，尽管系统会选择先网络分析策略再选择访问控制规则，但在选择访问控制规则之后还是会进行一些预处理 （特别是应用层预处理）。这**不会**影响您如何在自定义网络分析策略中配置预处理。

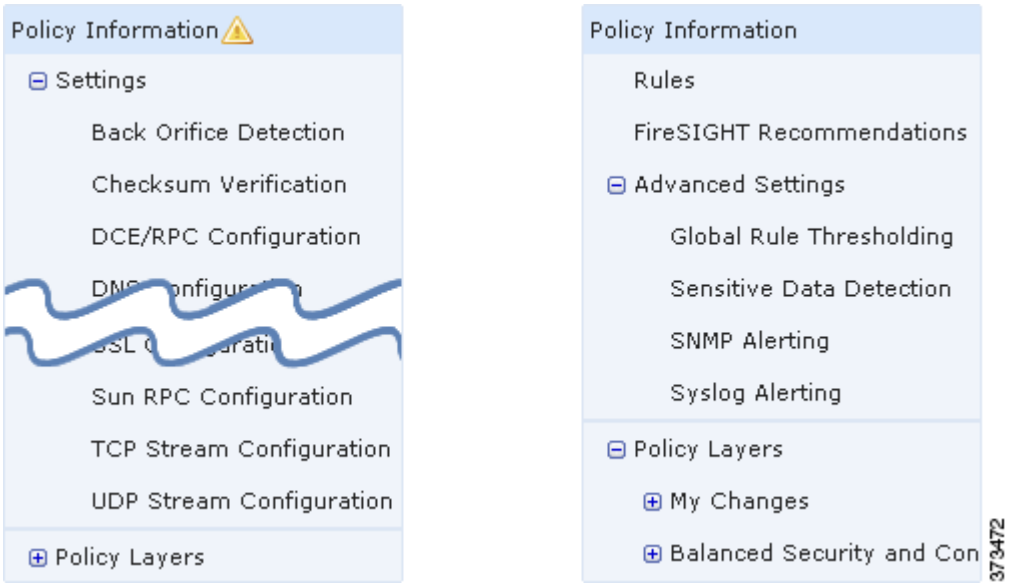
使用导航面板

许可证：保护

网络分析和入侵策略使用类似的网络界面编辑和保存对其配置做出的更改；请参阅：

- 第 26-3 页上的编辑网络分析策略
- 第 31-4 页上的编辑入侵策略

编辑任一类型的策略时，导航面板会出现在网络界面左侧。下图显示网络分析策略 （左侧）和入侵策略 （右侧）的导航面板。



导航面板被一条分界线分割成下方指向可以利用与策略层直接交互配置的策略设置的链接和上方指向可以不用与策略层直接交互配置的策略设置的链接。要浏览到任何设置页面，请在导航面板中点击其名称。导航面板中带有深色阴影的项目突出显示您当前的设置页面。例如，上面的插图中，导航面板右侧会显示 Policy Information 页面。

策略信息

Policy Information 页面提供常用设置的配置选项。如以上的网络分析策略面板图所示，当策略包含未保存的更改时，策略更改图标 (⚠) 显示在导航面板中 **Policy Information** 的旁边。当您保存更改时，该图标消失。

Rules （仅入侵策略）

入侵策略中的 Rules 页面可供您配置共享对象规则、标准文本规则和预处理程序规则的规则状态及其他设置。有关详细信息，请参阅第 32-1 页上的使用规则调整入侵策略。

FireSIGHT Recommendations （仅入侵策略）

入侵策略中的 FireSIGHT Recommendations 页面可供您将在您的网络中检测到的操作系统、服务器和客户端应用协议与为了保护这些资产而特别编写的入侵规则相关联。这样，您就可定制根据受监控网络的特定需求定制您的入侵策略。有关详细信息，请参阅第 33-1 页上的为您的网络资产定制入侵防御。

Settings （网络分析策略）和 Advanced Settings （入侵策略）

网络分析策略中的 Settings 页面可供您启用或禁用预处理程序以及访问预处理程序配置页面。展开 **Settings** 链接会显示指向策略中所有已启用预处理程序的个别配置页面的子链接。有关详细信息，请参阅第 26-5 页上的在网络分析策略中配置预处理器。

入侵策略中的 Advanced Settings 页面可供您启用或禁用高级设置以及访问这些高级设置的配置页面。展开 **Advanced Settings** 链接会显示指向策略中所有已启用高级设置的个别配置页面的子链接。有关详细信息，请参阅第 31-6 页上的在入侵策略中配置高级设置。

策略层

Policy Layers 页面显示构成网络分析或入侵策略的各层的摘要。展开 Policy Layers 链接会显示指向策略中的各层的摘要页面的子链接。展开各层子链接会显示指向层中已启用的所有规则、预处理程序或高级设置的配置页面的进一步子链接。有关详细信息，请参阅第 24-1 页上的在网络分析或入侵策略中使用层。

解决冲突和提交策略更改

许可证：保护

在编辑网络分析或入侵策略时，策略更改图标 (⚠) 显示在导航面板中 **Policy Information** 的旁边以指示策略包含未保存的更改。必须首先保存 （或*提交*）更改，然后系统才会认可这些更改。

注 在保存之后，必须应用网络分析或入侵策略，更改才会生效。如果应用策略而不保存，则系统将使用最近保存的配置。虽然您可以独立重新应用入侵策略，但网络分析策略将随其父访问控制策略一起应用。

解决编辑冲突

Network Analysis Policy 页面 (**Policies > Access Control**，然后点击 **Network Analysis Policy**) 和 Intrusion Policy 页面 (**Policies > Intrusion Policy > Intrusion Policy**) 显示每个策略是否有未保存的更改，还显示有关当前正在编辑策略的用户的信息。思科建议每次仅由一位人员编辑一个策略。如果执行同时编辑，则将产生以下后果：

- 如果在您编辑某条网络分析或入侵策略的同时另一用户也在编辑该策略，并且该用户保存对此策略的更改，则当您提交策略时系统将警告您会覆盖另一用户的更改。
- 如果以同一用户身份通过多个网络界面实例编辑同一网络分析或入侵策略，而且，您保存对一个实例的更改，则无法保存对其他实例的更改。

解决配置依赖关系

为了执行特殊分析，许多预处理程序和入侵规则均要求流量首先以某种方式得以解码或预处理，或者具有其他依存关系。当保存网络分析或入侵策略时，系统会自动启用必需的设置或警告您已禁用设置不会对流量产生影响，如下所述：

- 如果添加 SNMP 规则警报但未配置 SNMP 警报，则无法保存入侵策略。您必须配置 SNMP 警告或禁用规则警报，然后再次保存。
- 如果入侵策略包含已启用的敏感数据规则，但是您尚未启用敏感数据预处理程序，则无法保存该入侵策略。必须允许系统启用预处理程序并保存策略，或者禁用规则并再次保存。
- 如果在网络分析策略中禁用必需的预处理程序，则仍然可以保存该策略。但是，系统会通过已禁用预处理程序的当前设置使用该预处理程序，即使该预处理程序在网络界面中保持禁用亦如此。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

- 如果在网络分析策略中禁用内联模式，但是启用内联规范化预处理程序，则仍然可以保存该策略。然而，系统会警告您规范化设置将被忽略。禁用内联模式还会导致系统忽略允许预处理程序修改或阻止流量的其他设置，包括校验和验证和基于速率的攻击防御。有关详细信息，请参阅第 26-4 页上的允许预处理器影响内联部署中的流量和第 29-6 页上的规范化内联流量。

提交、放弃和缓存策略更改

在编辑网络分析或入侵策略时，如果您退出策略编辑器但不保存更改，则系统会缓存这些更改。即使注销系统或系统崩溃，更改依然会被缓存下来。系统缓存可以按照每个用户一个网络分析和一个入侵策略来存储未保存的更改；编辑同一类型的另一个策略之前，必须提交或放弃更改。编辑另一个策略而不保存对第一个策略的更改时，或者导入入侵规则更新时，系统会放弃缓存的更改。

可以在网络分析或入侵策略编辑器的 Policy Information 页面上提交或丢弃策略更改；请参阅第 26-3 页上的编辑网络分析策略和第 31-4 页上的编辑入侵策略。

下表总结如何保存或丢弃对网络分析或入侵策略做出的更改。

表 23-1　提交对网络分析或入侵策略做出的更改

要.....	在 Policy Information 页面上，您可以...
保存对策略的更改	点击 **Commit Changes**。 系统策略中设置监管是否提示（或要求）您在提交网络分析或入侵策略更改时对其添加注释。系统策略还监管是否将更改和注释记录到审核日志中。有关详细信息，请参阅第 63-18 页上的配置网络分析策略首选项和第 63-19 页上的配置入侵策略首选项。
放弃所有未保存的更改	点击 **Discard Changes**，然后点击 **OK** 放弃更改并转到 Intrusion Policy 页面。如果您不希望放弃更改，请点击 **Cancel** 返回到 Policy Information 页面。
退出策略，但是缓存更改	选择任意菜单或选择指向另一个页面的其他路径。请在系统提示的时候点击 **Leave page** 退出，或者点击 **Stay on page** 停留在高级编辑器中。

在网络分析或入侵策略中使用层

拥有众多受管设备的大型组织可能具有许多入侵策略和网络分析策略来支持不同部门、业务单位或（某些情况下）不同公司的独特需求。这两种策略类型中的配置均纳入称为*层*的构建块中，您可以使用层有效地管理多个策略。

层在入侵和网络分析策略中以基本相同的方式工作。您可创建和编辑任一策略类型，无需刻意使用层。可以修改策略配置，并且，如果尚未向策略中添加用户层，则系统会自动将您的更改纳入单个可配置层（初始命名为 *My Changes*）。或者，也可添加最多 200 个层，可在其中配置设置的任何组合。可以复制、合并、移动和删除用户层，并且最重要的是，可与同一类型的其他策略共享个别用户层。

有关详细信息，请参阅以下各节：

- 第 24-1 页上的了解层堆栈描述由一个基本策略构成的用户可配置和内置层。
- 第 24-6 页上的管理层说明如何在策略中使用层。

了解层堆栈

许可证：保护

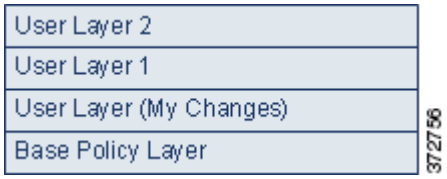
其中未添加层的网络分析或入侵策略包含内置、只读基本策略层和初始命名为 My Changes 的单个用户可配置层。可以复制、合并、移动或删除任何用户可配置的层，还可将其设置为由相同类型的其他策略共享。

每个策略层均包含网络分析策略中所有预处理程序或入侵策略中所有入侵规则和高级设置的完整配置。最低的基本策略层包括您在创建策略时所选择的基本策略中的所有设置。较高层的设置优先于较低层的相同设置。在某一层中未明确设置的功能从对其进行了明确设置的下一最高层*继承*其设置。

系统将层*扁平化*，也就是说，系统在处理网络流量时仅应用所有设置的累积效果。

提示 可以仅根据基本策略中的默认设置创建入侵或网络分析策略，或者，对于入侵策略，使用 FireSIGHT 规则状态建议。

下图显示了一个示例层堆栈，除了基本策略层和初始 My Changes 层，还包括两个附加用户可配置层，*User Layer 1* 和 *User Layer 2*。请注意，图中已添加的每个用户可配置层最初均位于堆栈中的最高层；因此，图中 User Layer 2 最后添加且位于堆栈的最高层。



在使用多层时，请注意以下问题：

- 当策略中的最高层为只读层或第 24-9 页上的在策略之间共享层中描述的共享层时，系统将在入侵策略中自动添加一个用户可配置层作为最高层，前提是执行以下两项操作之一：
  - 在入侵策略 Rules 页面上修改规则操作 （即规则状态、事件过滤、动态状态或警报）。有关详细信息，请参阅第 32-1 页上的使用规则调整入侵策略。
  - 启用、禁用或修改任何预处理程序、入侵规则或高级设置。

  系统添加层中的所有设置会被继承，但是，会导致生成新层的更改除外。
- 如果最高的一层是共享层，则当您执行下列操作之一时，系统将添加一层。
  - 与其他策略共享最高层
  - 向策略添加共享层
- 无论是否允许规则更新修改策略，规则更新中的更改都绝不会覆盖在层中所做出的更改。这是因为规则更新中的更改是在基本策略中做出，基本策略会确定基本策略层中的默认设置；您的更改始终在更高层中做出，因此其会覆盖规则更新对基本策略所做出的任何更改。有关详细信息，请参阅第 66-13 页上的导入规则更新和本地规则文件。

有关详细信息，请参阅以下各节：

- 第 24-2 页上的了解基本层
- 第 24-5 页上的了解 FireSIGHT 建议层

了解基本层

许可证：保护

入侵或网络分析策略的基本层 （也称为基本策略）定义该策略中所有配置的默认设置，也是该策略中的最低层。当新建策略并更改设置而不添加新层时，更改存储在 My Changes 层中并覆盖（但不更改）基本策略中的设置。

有关详细信息，请参阅以下各节：

- 第 24-3 页上的了解系统提供的基本策略
- 第 24-3 页上的了解自定义基本策略
- 第 24-3 页上的更改基本策略
- 第 24-4 页上的允许规则更新修改系统提供的基本策略

了解系统提供的基本策略

许可证：保护

思科通过 FireSIGHT 系统提供了多对网络分析和入侵策略。通过使用系统提供的网络分析和入侵策略，您可以借鉴思科漏洞研究团队 (VRT) 的经验。对于这些策略，VRT 会设置入侵和预处理程序规则状态，以及提供预处理程序和其他高级设置的初始配置。可以按现状使用系统提供的这些策略，也可以将其用作自定义策略的基础。

如果使用系统提供的策略作为基础，则导入规则更新可能修改基本策略中的设置。但是，可将自定义策略配置为不对系统提供的其基本策略做出这些更改。这使您能够根据独立于规则更新导入的计划手动更新系统提供的基本策略。在任一情况下，规则更新对基本策略所做出的更改不会更改或覆盖 My Changes 或任何其他层中的设置。有关详细信息，请参阅第 24-4 页上的允许规则更新修改系统提供的基本策略。

系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，“平衡式安全性和连接性”网络分析策略和“平衡式安全性和连接性”入侵策略共同作用而且都可以在入侵规则更新中更新。有关详细信息，请参阅第 23-7 页上的了解系统提供的策略。

了解自定义基本策略

许可证：保护

如果您不想使用系统提供的策略作为网络分析或入侵策略中的基本策略，则可以使用自定义策略作为基本策略。您可以调整自定义策略中的设置，以对您最重要的方式检查流量，从而能够提高受管设备的性能以及您有效响应其生成的事件的能力。

可以链接最多五个自定义策略，这五个策略中有四个使用其余四个之一以前创建的策略作为其基本策略；第五个策略必须使用系统提供的策略作为其基础。

对用作另一个策略之基础的自定义策略所做出的更改会自动用作使用该基础的策略的默认设置。此外，由于在策略链中所有策略都以系统提供的策略作为最终基础，因此，导入规则更新可能会影响您的策略，即使您使用自定义基本策略亦如此。如果策略链中的第一个自定义策略 （使用系统提供的策略作为其基本策略的自定义策略）允许规则更新修改其基本策略，则您的策略可能受到影响。有关更改此设置的信息，请参阅第 24-4 页上的允许规则更新修改系统提供的基本策略。

无论如何进行更改，对基本策略的更改 （由规则更新或在修改用作基本策略的自定义策略时所做出）都不会更改或覆盖 My Changes 或任何其他层中的设置。

更改基本策略

许可证：保护

可以为网络分析或入侵策略选择不同的基本策略，或者，允许规则更新修改系统提供的基本策略，而不影响在更高层的修改。

要更改基本策略，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　编辑策略时，请在导航面板中点击 **Policy Information**。

系统将显示 Policy Information 页面。

步骤 2　从 **Base Policy** 下拉列表中选择基本策略。

步骤 3　或者，如果选择系统提供的基本策略，请点击 **Manage Base Policy** 指定入侵规则更新是否可以自动修改您的基本策略。

有关详细信息，请参阅第 24-4 页上的允许规则更新修改系统提供的基本策略。

步骤 4　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

允许规则更新修改系统提供的基本策略

许可证：保护

您导入的规则更新会为系统提供的策略提供能够已修改的网络分析预处理程序设置、已修改的入侵策略高级设置、新的和已更新的入侵规则，以及已修改的现有规则状态。规则更新还可以删除规则并提供新规则类别和默认变量。有关详细信息，请参阅第 66-13 页上的导入规则更新和本地规则文件。

规则更新始终通过对预处理程序、高级设置和规则的任何更改来修改系统提供的策略。对默认变量和规则类别的更改在系统级别处理。有关详细信息，请参阅第 24-3 页上的了解系统提供的基本策略。

使用系统提供的策略作为基本策略时，可以允许规则更新修改基本策略 （在这种情况下，指系统提供的策略的副本）。如果允许规则更新更新基本策略，则新规则更新在基本策略中所做的更改与其对用作基本策略的系统提供的策略所做出的更改相同。如果尚未修改相应的设置，则基本策略中的设置会确定策略中的设置。但是，规则更新不会覆盖您在策略中所做出的更改。

如果不允许规则更新更新基本策略，可以在导入一个或多个规则更新后手动更新基本策略。

无论入侵策略中的规则状态如何或者是否允许规则更新更新基本入侵策略，规则更新始终会删除 VRT 删除的入侵规则。除非您对网络流量重新应用您做出的更改，否则当前应用的入侵策略中的规则采取以下操作：

- 禁用规则将保持禁用。
- 设置为 Generate Events 的规则在触发时将继续生成事件。
- 设置为 Drop and Generate Events 的规则在触发时将继续生成事件并放弃冲突的数据包。

除非同时符合下列两个条件，否则规则更新不修改自定义基本策略：

- 允许规则更新修改父策略 （即生成自定义基本策略的策略）的系统提供的基本策略。
- 在父策略中尚未进行覆盖父策略基本策略中相应设置的更改。

如果同时满足两个条件，保存父策略时，规则更新中的更改将传递给子策略 （即使用自定义基本策略的策略）。

例如，如果规则更新启用以前禁用的入侵规则，并且您尚未修改该规则在父入侵策略中的状态，则在保存父策略时，已修改的规则状态会传递到基本策略。

同样，如果规则更新修改默认预处理程序设置，并且您尚未修改父网络分析策略中的设置，则在保存父策略时，已修改的设置会传递到基本策略。

有关详细信息，请参阅第 24-3 页上的更改基本策略。

要允许规则更新修改系统提供的基本策略，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在编辑使用系统提供的策略作为其基本策略的策略时，请在导航面板中点击 **Policy Information**。

系统将显示 Policy Information 页面。

步骤 2　点击 **Manage Base Policy**。

系统将显示 Base Policy 摘要页面。

步骤 3　选择或清除 **Update when a new Rule Update is installed** 复选框。

在清除此复选框的情况下保存策略，然后导入规则更新时，在 Base Policy 摘要页面将出现 **Update Now** 按钮，并且在页面更新上会出现状态消息，通知该策略已过期。可以点击 **Update Now**，用最近导入的规则更新中的更改更新基本策略。

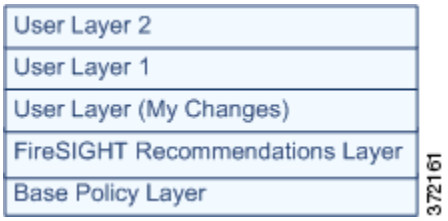
步骤 4　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

了解 FireSIGHT 建议层

许可证：保护

当在入侵策略中生成规则状态建议时，可以选择是否根据建议自动修改规则状态。有关详细信息，请参阅第 33-1 页上的为您的网络资产定制入侵防御。

如下图所示，使用建议的规则状态会在紧挨基本层之上添加一个内置只读 FireSIGHT 建议层。



请注意，此层对于入侵策略是唯一的。

如果您随后选择不使用建议的规则状态，则系统将移除 FireSIGHT 建议层。您无法手动删除该层，但是，您可以通过选择使用或不使用建议的规则状态来添加和移除该层。

如添加 FireSIGHT Recommendations 层，将在导航面板中 Policy Layers 下方添加一条 FireSIGHT Recommendations 链接。此链接引导您进入 FireSIGHT Recommendations 层页面的只读视图，在其中您可以只读模式访问 Rules 页面的建议过滤视图。有关如何在 Rules 页面处理规则的详细信息，请参阅第 32-1 页上的使用规则调整入侵策略。

使用建议的规则状态还会在导航面板中的 FireSIGHT Recommendations 链接之下添加 Rules 子链接。借助于 Rules 子链接，可访问 FireSIGHT Recommendations 层中 Rules 页面的只读显示。注意此视图中的以下内容：

- 如果状态栏中没有规则状态图标，则从基本策略继承状态。
- 如果这个或其他 Rules 页面视图的 FireSIGHTRecommendations 栏中没有规则状态图标，则没有适合此规则的建议。

提示　对于并非建议的规则状态，规则的开销评分高于生成建议时的 **Recommendation Threshold (By Rule Overhead)** 的设置 有关详细信息，请参阅第 33-3 页上的了解规则开销。

管理层

许可证：保护

Policy Layers 页面为网络分析或入侵策略提供完整层堆叠的单页摘要。在此页面上可以添加共享和非共享层，复制、合并、移动和删除层，访问每层的摘要页面，以及访问配置页面了解各层中已启用、禁用和覆盖的配置。

对于每层，您均可查看以下信息：

- 层是为内置、共享用户还是非共享用户层
- 哪些层包含最高 （即有效的）预处理程序或高级设置配置 （按功能名称）
- 在入侵策略中，在层中设置了其状态的入侵规则数，以及设置为各个规则状态的规则数。

各层摘要中的功能名称指明哪些配置在层中已启用、禁用、被覆盖或继承，如下所示：

当功能是...	功能名称是...
层中已启用	以纯文本写入
层中已禁用	删除
被高级层中的配置覆盖	以斜体文本写入
从下层中继承	不存在

此页面还提供所有已启用预处理程序 （网络分析）或高级设置 （入侵）的实际效果的摘要，以及入侵策略和入侵规则的摘要。

下表列出 Policy Layers 页面上可执行的操作。

表 24-1　网络分析和入侵策略层配置操作

要.....	您可以.....
显示 Policy Information 页面	点击 **Policy Summary**。 有关可在 Policy Information 页面上执行的操作的信息，请参阅第 32-1 页上的使用规则调整入侵策略、第 26-1 页上的网络分析策略使用入门和第 31-1 页上的入侵策略入门。
显示一个层的摘要页面	单击层所在行中的层名称，或者，点击用户层旁的编辑图标 ( )。也可以点击查看图标 ( ) 访问共享层的只读摘要页面。 有关可在层摘要页面上执行的操作的信息，请参阅第 24-9 页上的在策略之间共享层、第 24-14 页上的配置层中的预处理程序和高级设置和第 24-11 页上的在层中配置入侵规则。
访问层级别预处理程序或高级设置配置页	点击层所在行中的功能名称。请注意，基本策略和共享层中的配置页面均为只读。有关详细信息，请参阅第 24-14 页上的配置层中的预处理程序和高级设置。
访问按规则状态类型过滤的层级别规则配置页	在层的摘要中点击丢弃并生成事件图标 ( )、生成事件图标 ( ) 或禁用图标 ( )。如果层不包含设置为选定规则状态的规则，则不显示规则。
向策略添加层	请参阅第 24-7 页上的添加层。
从另一策略添加共享层	请参阅第 24-9 页上的在策略之间共享层。
更改层的名称或说明	请参阅第 24-7 页上的更改层的名称和说明。
复制、移动或删除层	请参阅第 24-8 页上的移动、复制和删除层。
合并一层至其下的层	请参阅第 24-9 页上的合并层。

要使用 Policy Layers 页面，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　编辑策略时，请在导航面板中点击 **Policy Layers**。

系统将显示 Policy Layers 摘要页面。

步骤 2　可以采取网络分析和入侵策略层配置操作表中的任何操作。

步骤 3　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

添加层

许可证：保护

您最多可以将 200 个层添加到网络分析或入侵策略。当您添加一个层时，它显示在策略的最高层。所有功能的初始状态均为 Inherit，在入侵策略中，未设置事件过滤、动态状态或警告规则操作。

在向网络分析或入侵策略添加层，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　编辑策略时，请在导航面板中点击 **Policy Layers**。

系统将显示 Policy Layers 页面。

步骤 2　点击 User Layers 旁的添加层图标 ( )。

系统将显示 Add Layer 弹出窗口。

步骤 3　键入一个唯一的层**名称**并点击 **OK**。

新层显示为用户层下方的最高层。

步骤 4　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

更改层的名称和说明

许可证：保护

可以更改网络分析或入侵策略中的用户可配置层的名称，或者，可添加或修改在编辑层时可见的说明。

要更改层的名称和添加或修改其说明，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　编辑策略时，请在导航面板中点击 **Policy Layers**。

系统将显示 Policy Layers 页面。

步骤 2　点击要编辑的用户层旁的编辑图标 ( )。

系统将显示该层的摘要页面。

步骤 3　可执行以下操作：

- 修改层**名称**。
- 添加或修改层**说明**。

步骤 4　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

移动、复制和删除层

许可证：保护

可以复制、移动或删除网络分析或入侵策略中的用户层，包括初始的 My Changes 层。请注意以下考虑事项：

- 在复制层时，副本显示为最高的一层。
- 复制一个共享层会创建非共享副本，或者，您可以随后与其他策略共享该副本。
- 不能删除一个共享层；启用了共享但尚未与其他策略共享的层不是共享层。

要复制、移动或删除层，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　编辑策略时，请在导航面板中点击 **Policy Layers**。

系统将显示 Policy Layers 页面。

步骤 2　可执行以下操作：

- 要复制层，请点击要复制的层旁的复制图标 ( )。

  页面刷新，该层的副本作为最高层出现。
- 要在 User Layers 页面区域内将层上移或下移，请点击层摘要中的任何开放区域并将其拖动，直至位置箭头 ( ) 指向层上方或下方要将该层移到的行。

  屏幕刷新，层出现在新位置。
- 要删除层，请点击要删除的层旁的删除图标 ( )，然后点击 **OK**

  页面刷新，该层删除成功。

步骤 3　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

合并层

许可证：保护

可以将网络分析或入侵策略中的用户可配置层与其下方的下一个用户层合并。合并层保留任一层特有的所有设置，并且如果两层均包含同一预处理程序、入侵规则或高级设置的设置，则会接受更高层中的设置。合并层保留下层的名称。

如在一个策略中创建的一个共享层已添加至其他策略，则可将紧接共享层并在其之上的非共享层与该共享层合并，但不能将该共享层与其下方的非共享层合并。

如在一个策略中添加了在其他策略中创建的共享层，则可将该共享层合并到紧接其下方的非共享层，合并生成的层将不再共享；不能将非共享层合并到其下方的共享层。

要将用户层与其下方的用户层合并，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　编辑策略时，请在导航面板中点击 **Policy Layers**。

系统将显示 Policy Layers 页面。

步骤 2　在两个层中的上层中点击合并图标 ( )，然后点击 **OK**。

页面刷新，随后该层与其下的层合并。

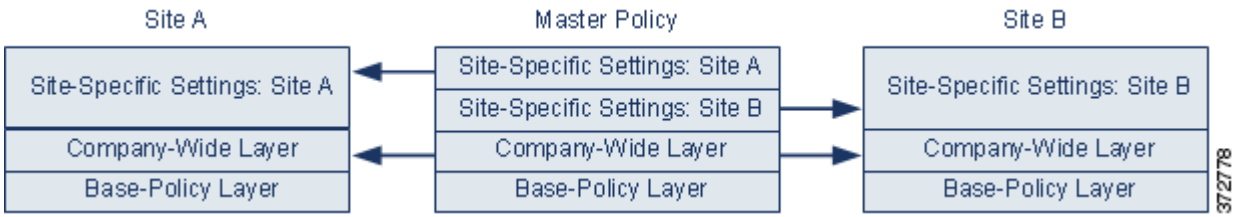
步骤 3　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

在策略之间共享层

许可证：保护

可以将用户可配置层与同一类型的其他策略 （入侵或网络分析）共享。在共享层中修改配置后提交更改时，系统会更新使用该共享层的所有策略，并为您提供所有受影响策略的列表。您只能在创建共享层所在策略中修改该共享层的功能配置。

下图显示的示例主策略作为站点特定策略的来源。



图中的主策略包括一个公司范围层，该层的设置同时适用于站点 A 和站点 B 的策略。它还包括每个策略的站点特定层。例如，如果使用网络分析策略，则 Site A 在受监控网络上可能没有 Web 服务器，并且不需要 HTTP Inspect 预处理程序的保护或处理开销，但两个站点均可能需要 TCP 数据流预处理。可在与两个站点共享的公司范围层启用 TCP 数据流处理，在与 Site A 共享的站点特定层禁用 HTTP Inspect 预处理程序，在与 Site B 共享的站点特定层启用 HTTP Inspect 预处理程序。如果编辑站点特定策略中更高层中的配置，还可进一步调整每个站点的策略，必要时可借助任何配置调整。

示例主策略中的扁平化网络设置不大可能对流量监控有用，但配置和更新站点特定策略所节省的时间使得它成为策略层的一种有用应用。

也可使用许多其他层配置。例如，您可以按公司、部门、网络甚至用户来界定策略层。对于入侵策略而言，还可以在一个层中纳入高级设置，而在另一个层中纳入规则设置。

提示 当基本策略是在其中已创建要共享的层的自定义策略时，不能向策略中添加共享层。如要尝试保存更改，将出现一条错误消息，指明策略包括循环依赖。有关详细信息，请参阅第 24-3 页上的了解自定义基本策略。

要与其他策略共享一个层，您必须执行以下操作：

- 在要共享的层的层摘要页面上启用共享。
- 在要共享共享层的策略的 Policy Layers 页面上添加该共享层。

不能禁用共享另一个策略正在使用的层，必须首先从该策略删除该层或删除该策略。

要启用或禁用与其他策略共享一个层，请执行以下操作：

访问：管理员/入侵管理员

步骤 1 编辑策略时，请在导航面板中点击 **Policy Layers**。

系统将显示 Policy Layers 页面。

步骤 2 点击要与其他策略共享的层旁的编辑图标 ( )。

系统将显示该层的摘要页面。

步骤 3 选择 （启用）或清除 （禁用） **Sharing** 复选框。

步骤 4 保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

要向策略添加共享层，请执行以下操作：

访问：管理员/入侵管理员

步骤 1 编辑策略时，请在导航面板中点击 **Policy Layers**。

系统将显示 Policy Layers 页面。

步骤 2 点击 User Layers 旁的添加共享层图标 ( )。

系统将显示 Add Shared Layer 弹出窗口。

步骤 3 从 Add Shared Layer 下拉列表中选择要添加的共享层，然后点击 **OK**。

系统将显示 Policy Layers 摘要页面，而且您选择的共享层显示为策略中的最高层。

如果任何其他策略中没有共享层，不会显示下拉列表；在弹出窗口中点击 **OK** 或 **Cancel** 返回 Policy Layers 摘要页面。

步骤 4 保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

在层中配置入侵规则

许可证：保护

在入侵策略中，可为任何用户可配置层中的规则设定规则状态、事件过滤、动态状态、警报和规则评论。访问要进行更改的层之后，可以按照在入侵策略 Rules 页面上所用的相同方法在该层的 Rules 页面上添加设置；请参阅第 32-1 页上的使用规则调整入侵策略。

可以在该层的 Rules 页面上查看个别层设置，也可以在 Rules 页面的策略视图中查看所有设置的实际效果。在 Rules 页面的策略视图中修改规则设置时，修改的是策略中最高用户可配置层。可使用任何 Rules 页面上的下拉列表切换到另一层。

下表介绍了在多个层中配置相同设置类型的效果。

表 24-2　　层规则设置

您可设定.....	此设置类型.....	以.....
一个	规则状态	覆盖为较低层规则设定的规则状态，并忽略在较低层为该规则配置的所有阈值、抑制、基于速率的规则状态和警报。有关详细信息，请参阅第 32-18 页上的设置规则状态。 如果想要规则从基本策略或较低层继承状态，请将规则状态设置为 Inherit。请注意，在入侵策略 Rules 页面操作时，不能将规则状态设置为 Inherit。 另请注意，当在特定层的 Rules 页面上查看规则状态设置时，规则状态设置会进行颜色编码：其有效状态设置在更低层中的规则以黄色突出显示；其有效状态设置在更高层中的规则以红色突出显示；其有效状态设置在当前层中的规则不突出显示。由于入侵策略 Rules 页面是所有规则设置的实际效果的综合视图，因此，在该页面上未对规则状态进行颜色编码。
一个	阈值 SNMP 警报	覆盖较低层中规则的相同类型设置。请注意，设置阈值时会覆盖层中规则的任何现有阈值。有关详细信息，请参阅第 32-20 页上的配置事件阈值和第 32-29 页上的添加 SNMP 告警。
一个或多个	抑制 基于速率的规则状态	会将每个所选规则的相同类型设置累积合并至为该规则设定规则状态所在的第一层。设定规则状态所在层下的设置均被忽略。有关详细信息，请参阅第 32-24 页上的按入侵策略配置抑制和第 32-26 页上的添加动态规则状态。
一个或多个	注释	向规则添加注释。注释因规则而异，而非因策略或层而异。可以向任何层中的规则添加一条或多条注释。有关详细信息，请参阅第 32-8 页上的为规则添加规则注释。

例如，如在一层中将规则状态设置为 Drop and Generate Events，但在上层设置为 Disabled，则入侵策略的 Rules 页面将显示规则已被禁用。

再比如，如在一层中为规则将基于源的抑制设置为 192.168.1.1，同时也为该规则将基于目标的抑制设置为 192.168.1.2，则 Rules 页面显示：累积效应将为源地址 192.168.1.1 和目标地址 192.168.1.2 抑制事件。请注意，抑制和基于速率的规则状态设置会将每个所选规则的相同类型设置累积合并至为该规则设定规则状态所在的第一层。设定规则状态所在层下的设置均被忽略。

要修改层中的规则，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　编辑入侵策略时，请在导航面板中展开 **Policy Layers**，然后展开要修改的策略层。

步骤 2　点击紧挨要修改的策略层下方的 **Rules**。

系统将显示该层的 Rules 页面。

可在层规则设置表中修改任何设置。有关配置入侵规则的详细信息，请参阅第 32-1 页上的使用规则调整入侵策略。

要从可编辑层删除单项设置，请双击该层 Ruels 页面的规则消息，以显示规则详细信息。在要删除的设置旁，单击 **Delete**，然后双击 **OK**。

步骤 3　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

移除多层规则设置

许可证：保护

您可以在入侵规则 Rules 页面上选择一条或多条规则，然后从入侵策略中的多个层同时移除特定类型的事件过滤器、动态状态或警报。

系统将往下移除每层的设置类型，直至移除所有设置或遇到为规则设定了规则状态的层。如果遇到规则状态已设定的层，系统将从该层移除设置，并停止移除此设置类型。

当系统在共享层或在基本策略中遇到此设置类型时，如果策略的最高层可以编辑，则系统会将该规则的剩余设置和规则状态复制至该可编辑层。或者，如果策略最高层是共享层，系统会在共享层上方新建一个可编辑层，并将该规则的剩余设置和规则状态复制至该可编辑层。

注　移除从共享层或基本策略派生的规则设置会导致忽略从更低层或基本策略中对该规则做出的任何更改。要停止忽略从更低层或基本策略做出的更改，请在最高层的摘要页面上将规则状态设置为 **Inherit**。有关详细信息，请参阅第 32-18 页上的设置规则状态。

要移除多层中的规则设置：

访问：管理员/入侵管理员

步骤 1　编辑入侵策略时，请在导航面板中紧挨 Policy 信息下方点击 **Policy Information**。

提示　也可为所有层在 Rules 页面的层下拉列表中选择 **Policy**，或在 Policy Information 页面选择 **Manage Rules**。

系统将显示入侵策略的 Rules 页面。

步骤 2　选择要为其移除多项设置的一条或多条规则。您有以下选项：

- 要选择一条特定规则，请选择该规则旁的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

有关如何查找规则的信息，请参阅第 32-9 页上的了解入侵策略中的规则过滤和第 32-16 页上的在入侵策略中设置规则过滤器。

步骤 3　您有以下选项：

- 要移除某条规则的所有阈值，请选择 **Event Filtering > Remove Thresholds**。
- 要移除某条规则的所有抑制，请选择 **Event Filtering > Remove Suppressions**。
- 要移除某条规则的所有基于速率的规则状态，请选择 **Dynamic State > Remove Rate-Based Rule States**。
- 要移除某条规则的所有 SNMP 警报设置，请选择 **Alerting > Remove SNMP Alerts**。

系统将显示一个确认弹出窗口。

注　移除从共享层或基本策略派生的规则设置会导致忽略从更低层或基本策略中对该规则做出的任何更改。要停止忽略从更低层或基本策略做出的更改，请在最高层的摘要页面上将规则状态设置为 **Inherit**。有关详细信息，请参阅第 32-18 页上的设置规则状态。

步骤 4　点击 **OK**。

系统移除规则中选定的设置并将剩余设置复制至策略中的最高可编辑层。参阅此操作步骤的说明，了解影响系统复制剩余设置的条件。

步骤 5　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

接受来自自定义基本策略的规则更改

许可证：保护

当尚未添加层的自定义网络分析或入侵策略使用另一个自定义策略作为其基本策略时，在以下情况下，必须将规则设置为继承其规则状态：

- 您删除为该基本策略中规则设置的事件过滤器、动态状态或 SNMP 警告
- 您希望规则接受在用作基本策略的另一个自定义策略中对其做出的后续更改

以下操作步骤说明如何完成此任务。关于在已经添加策略层的策略中接受对这些规则的设置，请参阅第 24-12 页上的移除多层规则设置。

要在未添加层的策略中接受规则更改，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　编辑入侵策略时，请在导航面板中展开 **Policy Layers** 链接，然后展开 **My Changes** 链接。

步骤 2　点击紧邻 My Changes 下方的 **Rules** 链接。

系统将显示 My Changes 层的 Rules 页面。

步骤 3　选择要接受其设置的规则。您有以下选项：

- 要选择一条特定规则，请选择该规则旁的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

有关如何查找规则的信息，请参阅第 32-9 页上的了解入侵策略中的规则过滤和第 32-16 页上的在入侵策略中设置规则过滤器。

步骤 4　从 **Rule State** 下拉列表选择 **Inherit**。

步骤 5　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

配置层中的预处理程序和高级设置

许可证：保护

您使用类似的机制在网络分析策略中配置预处理程序和在入侵策略中配置高级设置。您可以启用和禁用预处理程序（在网络分析 Settings 页面上）和入侵策略高级设置（在入侵策略 Advanced Settings 页面上）。这些页面还提供所有相关功能的有效状态的摘要。例如，如果网络分析 SSL 预处理程序在一层中已禁用但在更高层中已启用，则 Settings 页面将其显示为已启用。在这些页面上做出的更改显示在策略的顶层中。

您也可以在用户可配置层的摘要页面上启用或禁用预处理程序或高级设置并访问其配置页面。在此页面上可以修改层名称和说明，以及配置是否将层与相同类型的其他策略共享；有关详细信息，请参阅第 24-9 页上的在策略之间共享层。可以通过选择导航面板中 **Policy Layers** 下方的层名称来切换到另一层的摘要页面。

启用预处理程序或高级设置时，在导航面板中的层名称下方会显示指向该功能的配置页面的子链接，并且在层的摘要页面上的功能旁边会显示编辑图标 ( )；在层中禁用该功能或将其设置为 Inherit 时，这些图标会消失。

设置预处理程序或高级设置的状态（已启用或已禁用）会覆盖更低层中该功能的状态和配置设置。如果希望预处理程序或高级设置从基本策略或更低层继承其状态和配置，请将其设置为 **Inherit**。请注意，当在 Settings 或 Advanced Settings 页面上操作时，无法选择 Inherit。

每层摘要页面上的颜色编码按如下指明有效配置位于更高层、更低层还是当前层中：

- 红色 - 有效配置在较高层中
- 黄色 - 有效配置在较低层中
- 未突出显示 - 有效配置在当前层中

由于 Settings 和 Advanced Settings 页面是所有相关设置的综合视图，因此，这些页面不使用颜色编码指明有效配置的位置。

系统使用已启用该功能的最高层中的配置。除非特地修改该配置，系统将使用默认配置。例如，如果在一层中启用并修改网络分析 DCE/RPC 预处理程序，并且还在更高层中将其启用但不修改，则系统使用更高层中的默认配置。

下表描述用户可配置层的摘要页面上可执行的操作。

表 24-3　　Layer 摘要页面操作

要.....	**您可以.....**
修改层名称或说明	为 **Name** 或 **Description** 键入一个新值。
与其他入侵策略共享层	选择 **Allow this layer to be used by other policies**。 有关详细信息，请参阅第 24-9 页上的在策略之间共享层。
在当前层中启用或禁用预处理程序/高级设置	点击功能旁的 **Enabled** 或 **Disabled** 当您启用该功能时，导航面板中层名称下方将出现该功能配置页面的子链接，并且该功能旁的摘要页面上将出现 Edit 图标 ( )。 禁用该功能后，将会移除该子链接和编辑图标。
从当前层下方最高层中的设置继承预处理程序/高级设置状态和配置	点击 **Inherit**。 系统将刷新页面，如果该功能已启用，则不再显示导航面板中的功能子链接和编辑图标。
访问已启用的预处理程序/高级设置的配置页面	点击编辑图标 ( ) 或功能子链接以修改当前配置。 请注意， Back Orifice 预处理程序没有用户可配置选项。

要修改用户层中的预处理程序/高级设置，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　编辑策略时，请在导航面板中展开 **Policy Layers**，然后点击要修改的层的名称。

系统将显示该层的摘要页面。

步骤 2　可以采取 Layer 摘要页面操作表中的任何操作。

步骤 3　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

自定义流量预处理

访问控制策略中的多项高级设置可监管需要特定专门技术才能做出的入侵检测和防御配置。高级设置通常只需要很少的修改或者不需要修改，不通用于各个部署。

本章介绍如何设置以下首选项：

- 第 25-1 页上的设置用于访问控制的默认入侵策略说明如何更改访问控制策略的默认入侵策略，用于在系统准确确定如何检查流量之前初始检查流量。
- 第 25-2 页上的使用网络分析策略自定义预处理说明如何通过分配自定义网络分析策略预处理匹配流量，根据特定安全区域、网络和 VLAN 定制某些流量预处理选项。

其他章节介绍访问控制策略的策略范围预处理和性能选项。有关详细信息，请参阅：

- 第 29-1 页上的配置高级传输/网络设置
- 第 30-1 页上的调整被动部署中的预处理
- 第 18-7 页上的调整的入侵防御性能
- 第 18-17 页上的调整文件和恶意软件检查性能和存储

设置用于访问控制的默认入侵策略

许可证：任何环境

每个访问控制策略使用其*默认入侵策略*初始检测流量，然后系统才能准确确定如何检测该流量。之所以这样做，是因为有时系统必须处理连接中的前几个数据包，**允许其通过**，然后它才能确定哪条访问控制规则 （如有）将处理流量。因此，这些数据包不会未经检测就到达其目的地，然而，您可以使用称为默认入侵策略的入侵策略对其进行检测并生成入侵事件。

默认入侵策略在执行应用控制和 URL 过滤时尤为有用，因为系统无法在客户端与服务器之间完全建立连接之前识别应用或过滤 URL。例如，如果一个数据包与具有应用或 URL 条件的访问控制规则中的所有其他条件相匹配，则将允许该数据包及其后续数据包通过，直到建立连接且完成应用或 URL 识别，通常为 3 到 5 个数据包。

系统使用默认入侵策略检查这些允许的数据包，该策略可以生成事件，并且，如果内联，还可以阻止恶意流量。系统识别应处理连接的访问控制规则或默认操作后，相应地处理和检测连接中剩余的数据包。

在创建访问控制策略时，其默认入侵策略取决于您**首次**选择的默认操作。用于访问控制的初始默认入侵策略如下：

- Balanced Security and Connectivity （系统提供的策略）是在您首先选择 **Intrusion Prevention** 默认操作时访问控制策略的默认入侵策略。

- No Rules Active 是在您首先选择 **Block all traffic 或 Network Discovery** 默认操作时访问控制策略的默认入侵策略。尽管选择此选项会禁用对上述已允许数据包的入侵检测，但是，如果您对入侵数据不感兴趣，它可提高性能。

注　如未执行入侵检测 （例如，在没有保护许可的仅发现部署中），则保持 No Rules Active 策略作为为默认入侵策略。有关详细信息，请参阅第 12-17 页上的 IPS 或仅发现性能注意事项。

请注意，如果您在创建访问控制策略后更改默认操作，则默认入侵策略**不**会自动更改。要手动更改它，请使用访问控制策略的高级选项。

要更改访问控制策略的默认入侵策略，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在想要更改其默认入侵策略的访问控制策略中，选择 **Advanced** 选项卡，然后点击 Network Analysis and Intrusion Policies 分区旁的编辑图标 ( )。

系统将显示 Network Analysis Policies 对话框。

步骤 2　从 **Intrusion Policy used before Access Control rule is determined** 下拉列表中，选择一条默认入侵策略。可以选择系统或用户创建的策略。

请注意，如果选择用户创建的策略，则可点击编辑图标 ( ) 在新窗口中编辑该策略。您无法编辑系统提供的策略。

注意事项　请**勿**使用 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 3　点击 **OK**，保存更改。

必须应用访问控制策略，使更改生效。

使用网络分析策略自定义预处理

许可证：任何环境

受支持的设备：因功能而异

*网络分析策略*监管如何解码和预处理流量，以便进一步对其进行评估，特别适用于可能表明入侵尝试的异常流量。此流量预处理发生在安全情报黑名单和流量解密之后，但是，发生在入侵策略对数据包进行详细检查之前。默认情况下，系统提供的 Balanced Security and Connectivity 网络分析策略应用于由访问控制策略处理的*所有*流量。

提示　系统提供的 Balanced Security and Connectivity 网络分析策略和 Balanced Security and Connectivity 入侵策略共同发挥作用，均可在入侵规则更新中更新。但是，网络分析策略主要监管预处理选项，而入侵策略主要监管入侵规则。

调整预处理的一个简单方法是创建和使用自定义网络分析策略作为默认值；请参阅第 26-2 页上的创建自定义网络分析策略。可用调整选项因预处理程序而异。

对于采用复杂部署的高级用户，可以创建多个网络分析策略，每个策略经过定制以不同方式预处理流量。然后，可以将系统配置为使用这些策略通过不同的安全区域、网络或 VLAN 监管流量的预处理。（请注意， ASA FirePOWER 设备无法通过 VLAN 限制预处理。）

为此，请向访问控制策略中添加自定义*网络分析规则*。每条规则无有：

- 一组规则条件，用于识别想要预处理的特定流量
- 一条关联的网络分析策略，想要用来预处理符合所有规则条件的流量

在系统预处理流量时，其将数据包按照规则编号自上而下的顺序与网络分析规则相匹配。不与任何网络分析规则匹配的流量由默认网络分析策略预处理。

注　如果禁用预处理程序，但系统需要根据已启用的入侵或预处理程序规则评估预处理的数据包，系统将自动启用和使用预处理程序，尽管它在网络分析策略 Web 界面中保持禁用。定制预处理，特别是使用多个自定义网络分析策略，是一项**高级**任务。由于预处理和入侵检测如此密切相关，因此，请**务必**小心确保检查单个数据包的网络分析策略与入侵策略实现互补。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

有关详细信息，请参阅以下各节：

- 第 25-3 页上的为访问控制设置默认网络分析策略
- 第 25-4 页上的指定要使用网络分析规则进行预处理的流量
- 第 25-8 页上的管理网络分析规则

为访问控制设置默认网络分析策略

许可证：任何环境

默认情况下，系统提供的 Balanced Security and Connectivity 网络分析策略应用于由访问控制策略处理的所有流量。如果您添加网络分析规则来定制流量预处理选项，默认网络分析策略预处理这些规则未处理的所有流量。

访问控制策略的高级设置可供您更改此默认策略。

要更改访问控制策略的默认网络分析策略，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在想要更改默认网络分析策略的访问控制策略中，选择 **Advanced** 选项卡，然后点击 Network Analysis and Intrusion Policies 分区旁的编辑图标 ( )。

系统将显示 Network Analysis Policies 对话框。

步骤 2　从 **Default Network Analysis Policy** 下拉列表中，选择默认网络分析策略。可以选择系统或用户创建的策略。

请注意，如果选择用户创建的策略，则可点击编辑图标 ( ) 在新窗口中编辑该策略。您无法编辑系统提供的策略。

注意事项　请**勿**使用 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 3　点击 **OK** 保存更改。

必须应用访问控制策略，使更改生效。

指定要使用网络分析规则进行预处理的流量

许可证：任何环境

受支持的设备：因功能而异

在访问控制策略的高级设置中，可以使用网络分析规则定制网络流量的预处理配置。类似于访问控制规则，网络分析规则从 1 开始编号。

在系统预处理流量时，它将数据包按照升序规则编号自上而下的顺序与网络分析规则相匹配，然后根据所有条件都匹配的第一个规则预处理流量。下表描述可添加到规则的条件。

表 25-1　网络分析规则条件类型

此条件...	匹配流量...	详细信息
Zones	通过特定安全区域中的一个接口进入或离开设备	安全区域是根据您的部署和安全策略对一个或多个接口进行的逻辑组合。区域中的接口可能位于多台设备上。要构建区域条件，请参阅第 25-5 页上的按每个区域预处理流量。
Networks	按其源或目标 IP 地址、国家/地区或大陆	您可以明确指定 IP 地址。要构建网络条件，请参阅第 25-6 页上的按每个网络预处理流量。
VLAN Tags	按 VLAN 进行标记	系统使用最内部的 VLAN 标记来通过 VLAN 识别数据包。请注意，ASA FirePOWER 无法通过 VLAN 限制预处理。要构建 VLAN 条件，请参阅第 25-7 页上的按 VLAN 预处理流量。

如果不为规则配置特殊条件，则系统将不根据该条件匹配流量。例如，一条包含网络条件但不含区域条件的规则根据其源 IP 地址或目标 IP 地址评估流量，不管其进出接口如何。不与任何网络分析规则匹配的流量由默认网络分析策略预处理。

要添加自定义网络分析规则，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在想要创建自定义预处理配置的访问控制策略中，选择 **Advanced** 选项卡，然后点击 Intrusion and Network Analysis Policies 分区旁的编辑图标 ( )。

系统将显示 Network Analysis Policies 对话框。如果您尚未添加任何自定义网络分析规则，网络界面表明您具有 **No Custom Rules**，否则将显示您配置的规则数。

提示　点击 **Network Analysis Policy List** 以在新窗口中显示 Network Analysis Policy 页面。在此页中可查看和编辑您的自定义网络分析策略；请参阅第 26-3 页上的管理网络分析策略

步骤 2　在 **Network Analysis Rules** 旁，点击表明您拥有的自定义规则数目的语句。

对话框展开以显示自定义规则 （如有）。

步骤 3　点击 **Add Rule**。

系统将显示网络分析规则编辑器。

步骤 4　构建您规则的条件。可以使用以下条件限制 NAP 预处理：

- 第 25-5 页上的按每个区域预处理流量
- 第 25-6 页上的按每个网络预处理流量
- 第 25-7 页上的按 VLAN 预处理流量

步骤 5　点击 **Network Analysis** 选项卡，然后从 **Network Analysis Policy** 下拉列表中选择一条策略，以便将网络分析策略与规则相关联。

系统使用您选择的网络分析策略预处理符合规则的所有条件的流量。请注意，如果选择用户创建的策略，则可点击编辑图标 ( ) 在新窗口中编辑该策略。您无法编辑系统提供的策略。

注意事项　请勿使用 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 6　点击 **Add**。

该规则添加在任何其他规则之后。要更改规则的评估顺序，请参阅第 25-8 页上的管理网络分析规则。

按每个区域预处理流量

许可证：任何环境

网络分析规则中的区域条件可供您根据其源和目标安全区域预处理流量。安全区域是一个或多个接口的分组，这些接口可能以有利于部署和安全策略的方式跨多台设备分布。有关创建区域的详细信息，请参阅第 3-34 页上的使用安全区域。

在单一区域条件中最多可向每个 **Source Zones** 和 **Destination Zones** 添加 50 个区域：

- 要与从一个区域的接口*离开*设备的流量相匹配，请将该区域添加到 **Destination Zones**。请注意，由于被动部署的设备不传输流量，您无法在 **Destination Zones** 条件中使用包含被动接口的区域。
- 要与从一个区域的接口*进入*设备的流量想匹配，请将该区域添加到 **Source Zones**。

如果同时向一条规则添加源区域和目标区域条件，则匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

请注意，正如一个区域中的所有接口必须为相同类型 （全部为内联、全部为被动、全部已交换或全部已路由），网络分析规则的区域条件中使用的全部区域必须为同一类型。也就是说，您不能编写与源自或流出不同类型区域的流量相匹配的单条规则。

警告图标 ( ) 指明无效配置，如不包含接口的区域。如欲查看详细信息，请将鼠标指针悬停在该图标上。

要按区域预处理流量，请执行以下步骤：

访问：管理员/访问管理员/网络管理员

步骤 1　在想要按区域预处理流量的访问控制策略中，新建一条网络分析规则或编辑现有规则。

有关详细说明，请参阅第 25-4 页上的指定要使用网络分析规则进行预处理的流量。

步骤 2　在网络分析规则编辑器中，选择 **Zones** 选项卡。

系统将显示 Zones 选项卡。

步骤 3　查找并选择您要从 **Available Zones** 添加的用户和组。

要搜索需要添加的区域，请点击 **Available Zones** 列表上方的 **Search by name** 提示，然后键入区域名称。列表会在您键入内容时进行更新，以显示匹配区域。

点击选择区域。要选择多个区域，请使用 **Shift** 和 **Ctrl** 键，或点击右键并选择 **Select All**。

步骤 4　点击 **Add to Source** 或 **Add to Destination** 将选定区域添加到适当列表。

您也可以拖放选定的区域。

步骤 5　保存或继续编辑规则。

只有应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

按每个网络预处理流量

许可证：任何环境

网络分析规则中的网络条件可供您按流量的源 IP 地址和目标 IP 地址预处理流量。您可以手动为想要预处理的流量指定源 IP 地址和目标 IP 地址，也可以用网络对象配置网络条件，这些网络对象可重复使用并将名称与一个或多个 IP 地址和地址块相关联。

提示　创建网络对象后，您不仅可将其用于构建网络分析规则，还可以在系统的网络模块接口中的各个其他位置将其用于代表 IP 地址。您可以使用对象管理器创建这些对象；也可在配置网络分析规则时即时创建网络对象。有关详细信息，请参阅第 3-4 页上的使用网络对象。

在单一网络条件中最多可向每个 **Source Networks** 和 **Destination Networks** 添加 50 个项目：

- 要匹配源自某个 IP 地址的流量，请配置 **Destination Networks**。
- 要匹配流向某个 IP 地址的流量，请配置 **Destination Networks**。

如果要同时添加源和目标网络添加到规则，匹配流量必须来自指定 IP 地址并且目标为其中一个目标 IP 地址。

在构建网络条件时，警告图标 (⚠) 指明无效配置。如欲查看详细信息，请将鼠标指针悬停在该图标上。

要按每个网络预处理流量，请执行以下步骤：

访问：管理员/访问管理员/网络管理员

步骤 1　在想要按网络预处理流量的访问控制策略中，新建一条网络分析规则或编辑现有规则。

有关详细说明，请参阅第 25-4 页上的指定要使用网络分析规则进行预处理的流量。

步骤 2　在网络分析规则编辑器中，选择 **Networks** 选项卡。

系统将显示 Networks 选项卡。

步骤 3　查找并选择您要从 **Available Networks** 添加的网络，如下所述：

- 要动态添加网络对象，以便随后可将其添加到条件，请点击 **Available Networks** 列表上方的添加图标 (⊕)；请参阅第 3-4 页上的使用网络对象。
- 要搜索需要添加的网络，请点击 **Available Networks** 列表上方的 **Search by name or value** 提示，然后键入对象名称或其中一个对象组件的值。列表会在您键入内容时进行更新，以显示匹配对象。

要选择一个对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键，或右键单击并选择 **Select All**。

步骤 4　点击 **Add to Source** 或 **Add to Destination** 将选定对象添加到适当的列表。

您也可以拖放选定的对象。

步骤 5　添加要手动指定的所有源或目标 IP 地址或地址块。

点击 **Source Networks** 或 **Destination Networks** 列表下方的 **Enter an IP address** 提示；然后键入一个 IP 地址或地址块并点击 **Add**。

步骤 6　保存或继续编辑规则。

只有应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

按 VLAN 预处理流量

许可证：任何环境

受支持的设备：任何防御中心，除了ASA FirePOWER

网络分析规则中的 VLAN 条件可供您控制如何预处理具有 VLAN 标记的流量。系统使用最内部的 VLAN 标记来通过 VLAN 识别数据包。请注意，ASA FirePOWER 设备无法通过 VLAN 限制预处理。

在构建基于 VLAN 的网络分析条件时，可以手动指定 VLAN 标记。或者，您可以使用 VLAN 标记 objects 配置 VLAN 条件，这些对象可重复使用并将名称与一个或多个 VLAN 对象相关联。

提示　创建 VLAN 标记对象后，您不仅可将其用于构建网络分析规则，还可以在系统的网络接口中的各个其他位置将其用于代表 VLAN 标记。可以使用对象管理器创建 VLAN 标记对象或在配置网络分析规则时动态创建该对象。有关详细信息，请参阅第 3-12 页上的使用 VLAN 标记对象。

在单个 VLAN 标记条件中，最多可向 **Selected VLAN Tags** 添加 50 项。在构建 VLAN 标记条件时，警告图标 (⚠) 指明无效的配置。如欲查看详细信息，请将鼠标指针悬停在该图标上。

要按 VLAN 标记预处理流量，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在想要按 VLAN 标记预处理流量的访问控制策略中，新建一条网络分析规则或编辑现有规则。

有关详细说明，请参阅第 25-4 页上的指定要使用网络分析规则进行预处理的流量。

步骤 2　在网络分析规则编辑器中，选择 **VLAN Tags** 选项卡。

系统将显示 VLAN Tags 选项卡。

步骤 3　查找并选择您要从 **Available VLAN Tags** 添加的 VLAN，如下所述：

- 要动态添加 VLAN 标记，以便随后可将其添加到条件，请点击 Available VLAN Tags 列表上方的添加图标 (⊕)；请参阅第 3-12 页上的使用 VLAN 标记对象。
- 要搜索需要添加的 VLAN 标记对象和组，请点击 **Available VLAN Tags** 列表上方的 **Search by name or value** 提示，然后键入对象的名称或对象中的一个 VLAN 标记的值。列表会在您键入内容时进行更新，以显示匹配对象。
- 要选择一个对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键，或右键单击并选择 **Select All**。

步骤 4　点击 **Add to Rule** 或通过拖放将选定的对象添加到 **Selected VLAN Tags** 列表。

步骤 5　添加要手动指定的任何 VLAN 标记。

或者，点击 **Selected VLAN Tags** 列表下方的 **Enter a VLAN Tag** 提示，然后键入一个 VLAN 标记或范围，最后点击 **Add**。可以指定介于 1 和 4094 之间的任何 VLAN 标记；使用连字符指定 VLAN 标记的范围。

步骤 6　保存或继续编辑规则。

只有应用访问控制策略才能使更改生效；请参阅第 369 页的 Applying an Access Control Policy。

管理网络分析规则

许可证：任何环境

网络分析规则只是指定如何预处理与这些限制条件匹配的流量的一组配置和条件。可以在现有访问控制策略的高级选项中创建和编辑网络分析规则。每条规则只属于一个策略。

要编辑自定义网络分析规则，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　在想要更改自定义预处理配置的访问控制策略中，选择 **Advanced** 选项卡，然后点击 Intrusion and Network Analysis Policies 分区旁的编辑图标 ( )。

系统将显示 Network Analysis Policies 对话框。如果您尚未添加任何自定义网络分析规则，网络界面表明您具有 **No Custom Rules**，否则将显示您配置的规则数。

步骤 2　在 **Network Analysis Rules** 旁，点击表明您拥有的自定义规则数目的语句。

对话框展开以显示自定义规则 （如有）。

步骤 3　编辑自定义规则。您有以下选项：

- 要编辑某条规则的条件或更改该规则调用的网络分析策略，请点击该规则旁的编辑图标 ( )。
- 要更改某条规则的评估顺序，请点击该规则并将其拖至正确的位置。要选择多条规则，请使用 Shift 和 Ctrl 键。
- 要删除某条规则，请点击该规则旁的删除图标 ( )。

提示　右键单击规则可显示上下文菜单，该菜单可供您剪切、复制、粘贴、编辑和添加新的网络分析规则。

步骤 4　点击 **OK**，保存更改。

只有应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

第 26 章

网络分析策略使用入门

*网络分析策略*管理许多流量预处理选项，并供访问控制策略中的高级设置调用。网络分析相关预处理发生在安全情报黑名单和 SSL 解密之后进行，但在入侵或文件检查开始之前进行。

默认情况下，系统使用*平衡的安全性和*网络分析策略预处理由访问控制策略处理的所有流量。但是，您可以选择不同的默认网络分析策略执行此预处理。为方便您使用，系统提供多种无法修改的网络分析策略供选择，这些策略由思科漏洞研究团队 (VRT) 针对安全性和连接的特定平衡专门进行过调整。您也可以用具有自定义预处理设置的自定义网络分析策略替换此默认策略。

提示 系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，平衡安全性和连接网络分析策略和平衡安全性和连接入侵策略配合工作并可以在入侵规则更新中同时更新。但是，网络分析策略管理的主要是预处理选项，而入侵策略管理的主要是入侵规则。第 23-1 页上的了解网络分析和入侵策略概述了网络分析和入侵策略如何配合工作检查流量，以及使用导航面板、解决冲突和确认更改的基本信息。

您也可以通过以下方式根据特定安全区域、网络和 VLAN 定制流量预处理选项：创建多个自定义网络分析策略，然后分配它们预处理不同流量。（请注意， ASA FirePOWER 设备无法通过 VLAN 限制预处理。）

注 定制预处理 （特别是使用多个自定义网络分析策略）是一项**高级**任务。由于预处理和入侵检查密切相关，检查每个数据包的网络分析和入侵策略**必须**相互补充。系统**不会**为您协调策略。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

本章介绍如何创建简单的自定义网络分析策略。本章还包含有关管理网络分析策略的基本信息：编辑和比较等。有关详情，请参阅：

创建自定义网络分析策略

许可证：保护

当您创建新的网络分析策略时必须为其提供唯一的名称，指定基本策略并选择*内联模式*。

基本策略定义网络分析策略的默认设置。修改新策略中的设置会覆盖（但不会更改）基本策略中的该设置。您可以使用系统提供的策略或自定义策略作为您的基本策略。有关详细信息，请参阅第 24-2 页上的了解基本层。

网络分析策略的内联模式允许预处理器修改（标准化）和丢弃流量，从而使攻击者避开检测的可能性最小化。请注意，在被动部署中，系统无法影响流量传输，无论内联模式如何设置。有关详细信息，请参阅第 26-4 页上的允许预处理器影响内联部署中的流量。

要创建网络分析策略，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

如果您的 FireSIGHT 系统用户帐户的角色被限制为 Intrusion Policy 或 Modify Intrusion Policy，您可以创建和编辑网络分析策略及入侵策略。要访问 Network Analysis Policy 页面，请选择 **Policies > Intrusion**，然后点击 **Network Analysis Policy**。有关详细信息，请参阅第 61-48 页上的管理自定义用户角色。

步骤 2　点击 **Create Policy**。

如果您在另一策略中有未保存的更改，当系统提示您返回 Network Analysis Policy 页面时请点击 **Cancel**。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Create Network Analysis Policy 弹出窗口。

步骤 3　在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

步骤 4　指定初始**基本策略**。

您可以使用系统提供的策略或自定义策略作为您的基本策略。

注意事项　请**勿**使用 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 5　指定是否允许预处理器影响内联部署中的流量：

- 要允许预处理器影响流量，请启用 **Inline Mode**。
- 要阻止预处理器影响流量，请禁用 **Inline Mode**。

步骤 6　创建策略：

- 点击 **Create Policy** 创建新策略并返回到 Network Analysis Policy 页面。新策略的设置与其基本策略相同。
- 点击 **Create and Edit Policy** 创建策略并在高级网络分析策略编辑器中对其进行编辑；请参阅第 26-3 页上的编辑网络分析策略。

管理网络分析策略

许可证：保护

在 Network Analysis Policy 页面（**Policies > Access Control**，然后点击 **Network Analysis Policy**）上，可以查看当前自定义网络分析策略以及以下信息：

- 最近一次修改策略的时间和日期 （采用当地时间）以及执行此修改的用户。
- 是否已启用**内联模式**设置，该设置允许预处理器影响流量
- 哪些访问控制策略和设备使用网络分析策略来预处理流量
- 策略是否有未保存的更改，以及有关谁 （如果有任何人）当前正在编辑该策略的信息

除了您创建的自定义策略之外，系统还提供两种自定义策略：初始内联策略和初始被动策略。这两个网络分析策略使用 Balanced Security and Connectivity 网络分析策略作为其基本策略。两者之间的唯一区别在于其内联模式，在内联策略中允许预处理器影响流量，但在被动策略中禁用了该功能。您可以编辑和使用这些系统提供的自定义策略。

Network Analysis Policy 页面上的选项允许您采取下表中的措施。

表 26-1　　网络分析策略管理操作

要.....	您可以.....	请参阅.....
创建新的网络分析策略	点击 **Create Policy**。	第 26-2 页上的创建自定义网络分析策略.
编辑现有网络分析策略	点击编辑图标 ( )。	第 26-3 页上的编辑网络分析策略.
查看列出网络分析策略中当前配置设置的 PDF 报告	点击报告图标 ( )。	第 26-7 页上的生成当前网络分析设置的报告
比较两个网络分析策略或同一策略两个版本的设置	点击 **Compare Policies**。	第 26-8 页上的比较两个网络分析策略或版本.
删除网络分析策略	请点击删除图标 ( ) 并确认要删除策略。如果网络分析策略被访问控制策略引用，则无法删除该网络分析策略。	

请注意，如果您的 FireSIGHT 系统用户帐户的角色被限制为 Intrusion Policy 或 Modify Intrusion Policy，则您可以创建和编辑网络分析策略及入侵策略。要访问 Network Analysis Policy 页面，请选择 **Policies > Intrusion**，然后点击 **Network Analysis Policy**。有关详细信息，请参阅第 61-48 页上的管理自定义用户角色。

编辑网络分析策略

许可证：保护

当您创建新的网络分析策略时，它具有与其基本策略相同的设置。下表列出了根据您的需求自定义新策略时可执行的最常见的操作：

表 26-2　　网络分析策略编辑操作

要.....	您可以.....	请参阅.....
允许预处理器修改或丢弃流量	选择 Policy Information 页面上的 **Inline Mode** 复选框。	第 26-4 页上的允许预处理器影响内联部署中的流量

表 26-2　网络分析策略编辑操作 （续）

要.....	您可以.....	请参阅.....
更改基本策略	从 Policy Information 页面上的 **Base Policy** 下拉列表中选择基本策略。	第 24-3 页上的更改基本策略
查看基本策略中的设置	在 Policy Information 页面上点击 **Manage Base Policy**。	第 24-2 页上的了解基本层
启用、禁用或编辑预处理器设置	在导航面板中点击 **Settings**。	第 26-5 页上的在网络分析策略中配置预处理器
管理策略层	在导航面板中点击 **Policy Layers**。	第 24-1 页上的在网络分析或入侵策略中使用层

当您自定义网络分析策略时，特别是在禁用预处理器时，请记住一些预处理器和入侵规则要求首先以某种方式对流量进行解码或预处理。如果您禁用一个必需的预处理程序，虽然该预处理程序在网络分析策略网络界面中保持禁用，但系统仍自动通过其当前设置使用它。

注 由于预处理和入侵检查密切相关，检查每个数据包的网络分析和入侵策略**必须**相互补充。定制预处理 （特别是使用多个自定义网络分析策略）是一项**高级**任务。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

系统为每个用户缓存一条网络分析策略。在编辑网络分析策略时，如果您选择任何菜单或指向另一页的其他路径，您的更改将保留在系统缓存中，即使您离开此页。除了可执行上表中的操作，第 23-1 页上的了解网络分析和入侵策略还提供了有关使用导航面板、解决冲突和确认更改的信息

要编辑网络分析策略，请执行以下操作：

访问：管理员/入侵管理员

步骤 1 选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2 点击想要配置的网络分析策略旁的编辑图标 ( )。

系统将显示网络分析策略编辑器，焦点位于 Policy Information 页面上，并且左侧带导航面板。

步骤 3 编辑您的策略。采取上面总结的任何操作。

步骤 4 保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

允许预处理器影响内联部署中的流量

许可证：保护

在内联部署中，有些预处理器可以修改和阻止流量：例如：

- 内联规范化预处理器用于标准化数据包，以准备由其他预处理器和入侵规则引擎进行分析。您还可以使用预处理器的 **Allow These TCP Options** 和 **Block Unrecoverable TCP Header Anomalies** 选项阻止某些数据包。有关详细信息，请参阅第 29-6 页上的规范化内联流量。

- 系统可以丢弃具有无效校验和的数据包；请参阅第 29-5 页上的验证校验和。
- 系统可以丢弃匹配基于速率的攻击防护设置的数据包；请参阅第 34-8 页上的防御基于速率的攻击。

要使网络分析策略中配置的预处理器影响流量，还必须启用并正确配置预处理器，并正确部署受管设备内联，也就是说，与内联接口集内联。最后，您必须启用网络分析策略的 **Inline Mode** 设置。

如果要评估您的配置如何在内联部署中起作用，而不会实际修改流量，您可以禁用内联模式。在被动部署或分路模式的内联部署中，系统无法影响流量，无论内联模式如何。

请注意，禁用内联模式可能会影响入侵事件性能统计数据图表。当在内联部署中启用内联模式时，Intrusion Event Performance 页面 (**Overview > Summary > Intrusion Event Performance**) 显示表示已规范化和阻止的数据包的图表。如果禁用内联模式，或者在被动部署中，许多图表显示有关系统应当已规范化或丢弃的流量的数据。有关详细信息，请参阅第 41-4 页上的生成入侵事件性能统计信息图表。

提示 在内联部署中，思科建议您启动内联模式并配置启用了 **Normalize TCP Payload** 选项的内联规范化预处理器。在被动部署中，思科建议您配置自适应配置文件。

要允许预处理器影响内联部署中的流量，请执行以下操作：

访问：管理员/入侵管理员

步骤 1 选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

系统将显示 Policy Information 页面。

步骤 3 指定是否允许预处理器影响流量：

- 要允许预处理器影响流量，请启用 **Inline Mode**。
- 要阻止预处理器影响流量，请禁用 **Inline Mode**。

步骤 4 保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

在网络分析策略中配置预处理器

许可证：保护

*预处理器*准备流量以备进一步检查，规范化流量和标识协议异常。预处理器在数据包触发您配置的预处理器选项时可生成预处理器事件 （请参阅第 41-33 页上的解读预处理器事件）。网络分析策略的基本策略决定了默认情况下启用哪些预处理器及各自的默认配置。

当您在网络分析策略的导航面板中选择 **Settings** 时，策略将按类型列出其预处理器。在 Settings 页面中，您可以启用或禁用网络分析策略中的预处理器，以及访问预处理器配置页面。

必须启用预处理器，这样您才能对其进行配置。当您启用预处理器时，该预处理器配置页面的子链接出现在导航面板中 **Settings** 链接下，并且到配置页的 **Edit** 链接出现在 Settings 页面上的预处理器旁边。

提示 要将预处理器的配置恢复为基本策略中的设置，请点击预处理器配置页面上的 **Revert to Defaults**。出现提示时，请确认您要恢复。

当您禁用预处理器时，子链接和 **Edit** 将不再显示，但您的配置将被保留。请注意，为了执行其特定分析，许多预处理器和入侵规则要求首先以某种方式对流量进行解码或预处理。如果您禁用一个必要的预处理器，系统会自动使用其当前设置，但是，预处理器在网络分析策略网络界面中将保持禁用状态。

注 在大多数情况下，配置预处理器要求特定专业知识，并且通常很少需要修改或不需要任何修改。定制预处理（特别是使用多个自定义网络分析策略）是一项**高级**任务。由于预处理和入侵检查密切相关，检查每个数据包的网络分析和入侵策略**必须**相互补充。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

修改预处理器配置要求了解配置及其对您的网络的潜在影响。以下部分提供指向每个预处理器的具体配置详细信息的链接。

应用层预处理器

应用层协议解码器将特定类型的数据包数据标准化转换成规则引擎可以分析的格式。

表 26-3　应用层预处理器设置

想了解以下内容.....	请参阅.....
DCE/RPC 配置	第 27-2 页上的解码 DCE/RPC 流量
DNS 配置	第 27-13 页上的检测 DNS 域称服务器响应中的漏洞
FTP 和 Telnet 配置	第 27-16 页上的解码 FTP 和 Telnet 流量
HTTP 配置	第 27-26 页上的解码 HTTP 流量
Sun RPC 配置	第 27-39 页上的使用 Sun RPC 预处理器
SIP 配置	第 27-40 页上的解码会话发起协议
GTP 命令通道配置	第 27-44 页上的配置 GTP 命令通道
IMAP 配置	第 27-45 页上的解码 IMAP 流量
POP 配置	第 27-48 页上的解码 POP 流量
SMTP 配置	第 27-51 页上的解码 SMTP 流量
SSH 配置	第 27-57 页上的使用 SSH 预处理器检测攻击
SSL 配置	第 27-60 页上的使用 SSL 预处理器

SCADA 预处理器

Modbus 和 DNP3 预处理器检测流量异常并为入侵规则引擎提供数据，以供检查。

表 26-4　SCADA 预处理器设置

想了解以下内容.....	请参阅.....
Modbus 配置	第 28-1 页上的配置 Modbus 预处理器
DNP3 配置	第 28-3 页上的配置 DNP3 预处理器

传输层/网络层预处理器

网络层和传输层预处理器检测网络层和传输层的漏洞。数据包发送到预处理器之前，数据包解码器将数据包报头和负载转换为便于预处理器和入侵规则引擎使用的格式；它还检测数据包报头中的各种异常行为。

表 26-5　　传输层和网络层预处理器设置

想了解以下内容.....	请参阅.....
校验和验证	第 29-5 页上的验证校验和
内联规范化	第 29-6 页上的规范化内联流量
IP 分片重组	第 29-10 页上的对 IP 数据包进行分片重组
数据包解码	第 29-14 页上的了解数据包解码
TCP 数据流配置	第 29-18 页上的使用 TCP 数据流预处理
UDP 数据流配置	第 29-28 页上的使用 UDP 数据流预处理

请注意，一些高级传输和网络预处理器设置全局应用于您应用访问控制策略所在的所有网络、区域和 VLAN。您在一个访问控制策略而非网络分析策略中配置这些高级设置；请参阅第 29-1 页上的配置高级传输/网络设置。

具体威胁检测

Back Orifice 预处理器分析 Back Orifice 神奇 cookie 的 UDP 流量。可以配置端口扫描检测器来报告扫描活动。基于速率的攻击防御有助于保护您的网络免受 SYN 泛洪和旨在击溃网络的海量并发连接。

表 26-6　　具体威胁检测设置

想了解以下内容.....	请参阅.....
Back Orifice 检测	第 34-1 页上的检测 Back Orifice
端口扫描检测	第 34-2 页上的检测端口扫描
基于速率的攻击防御	第 34-8 页上的防御基于速率的攻击

请注意，您在入侵策略中配置敏感数据预处理器，该预处理器用于检测敏感信息（例如， ASCII 文本中的信用卡号和社会安全保障号）。有关详细信息，请参阅第 34-17 页上的检测敏感数据。

生成当前网络分析设置的报告

许可证：保护

网络分析策略报告是在特定时间点对策略配置的记录。该系统将基本策略中的设置与策略层的设置组合，不区分源自基本策略或策略层的设置。

您可以将包括以下信息的报告用于审计目的或检查当前配置。

表 26-7　网络分析策略报告项

项	说明
策略信息	提供策略的名称和说明、上次修改策略的用户的名称以及策略上次修改的日期和时间 并指明是否可以启用内联规范化，当前规则更新版本，以及基本策略是否锁定为当前规则更新。
设置	列出所有已启用预处理器设置及其配置。

还可以生成比较两个网络分析策略或同一策略的两个版本的比较报告。有关详细信息，请参阅第 26-8 页上的比较两个网络分析策略或版本。

要查看网络分析策略报告，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要生成报告的策略旁的报告图标 ()。请记住，应先确认所有更改，再生成网络分析策略报告；只有确认的报告才会显示在报告中。

系统将会生成报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

比较两个网络分析策略或版本

许可证：保护

如要审阅策略更改以便符合组织的标准或提高系统性能，可以检查两个网络分析策略之间的差异。可以比较任何两个网络分析策略或同一网络分析策略的两个版本。比较之后，可以生成 PDF 报告，记录两个策略或两个版本的策略之间的区别。

您可以使用两个工具来比较网络分析策略或策略版本：

- 比较视图只并排显示两个网络分析策略或两个版本之间的区别；每个策略的名称或策略版本则显示在比较视图的左右两侧。

  您可以使用该工具在网络界面上查看和导航两个策略修订版，其中突出显示其差异。

- 比较报告创建两个网络分析策略或网络分析策略版本之间的差异，其格式类似于网络分析策略报告的格式，但是采用 PDF 格式。

  可以将其用于保存、复制、打印和共享策略比较，以备进一步检查。

如需了解和使用策略比较工具的更多相关信息，请参阅：

- 第 26-9 页上的使用网络分析策略比较视图
- 第 26-9 页上的使用网络分析策略比较报告

使用网络分析策略比较视图

许可证：保护

比较视图以并列格式显示两个策略或策略版本，每个策略或策略版本在比较视图的左右两侧标题栏上通过名称来识别。上次修改时间和最近一次做出修改的用户会与策略名称一起显示。

两个策略之间的差异将会突出显示：

- 蓝色指示突出显示的设置在两个策略中不同，不同之处以红色文本标注。
- 绿色指示突出显示的设置在一个策略中存在，但在另一个策略中不存在。

您可以执行下表中的任何操作。

表 26-8　网络分析策略比较视图操作

要.....	您可以.....
逐一浏览更改	点击标题栏上方的 **Previous** 或 **Next**。 在左右两侧之间以双箭头图标 (◂▸) 为中心移动， **Difference** 数字调整为识别您正在查看哪个差异。
确定哪一层包含特定预处理器的配置	将鼠标光标悬停在想要查看的配置旁的高级配置图标 (*i*) 上方。 窗口随即显示包含预处理器配置的层的名称。
生成新的策略比较视图	点击 **New Comparison**。 系统将显示 **Select Comparison** 窗口。有关详情，请参见第 26-9 页上的使用网络分析策略比较报告。
生成策略比较报告	点击 **Comparison Report**。 策略比较报告将会创建仅列出两个策略或策略版本之间的差异的 PDF 文档。

使用网络分析策略比较报告

许可证：保护

网络分析策略比较报告是两个网络分析策略或同一网络分析策略的两个版本之间的所有差异的记录，通过网络分析策略比较视图识别，并采用 PDF 格式。可以使用此报告来进一步检查两个网络分析策略配置之间差异，以及保存和分发您的发现。

对于您能够访问的任何策略，都可以通过比较视图生成网络分析策略比较报告。在生成策略报告前，切记保存所有更改，只有已保存的更改会在报告中显示。

策略比较报告的格式与策略报告相同，有一处例外：策略报告包含策略中的所有配置，而策略比较报告仅列出策略之间的那些不同配置。网络分析策略比较报告包含第 26-8 页上的表 26-7 中描述的部分。

提示　您可以使用类似的操作步骤比较 SSL、访问控制、入侵、文件、系统或运行状况策略。

要比较两个网络分析策略或策略修订，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击 **Compare Policies**。

系统将显示 Select Comparison 窗口。

步骤 3　从 **Compare Against** 下拉列表中选择要进行比较的类型：

- 要比较两个不同的策略，请选择 **Other Policy**。

  页面将会刷新，并显示 Policy A 和 Policy B 下拉列表。

- 要比较同一策略的两个修订版，请选择 **Other Revision**。

  页面即会刷新并显示 Policy、 Revision A 和 Revision B 下拉列表。

步骤 4　根据您选择的比较类型，有以下选项可供选择：

- 如果您比较两个不同的策略，请从 Policy A 和 Policy B 下拉列表中选择要比较的策略。
- 如果您比较同一策略的两个版本，请选择策略，然后从 Revision A 和 Revision B 下拉列表中选择要比较的有时间戳的版本。

步骤 5　点击 **OK** 显示策略比较视图。

系统将显示比较视图。

步骤 6　或者点击 **Comparison Report** 生成网络分析策略比较报告。

系统将显示网络分析策略比较报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

使用应用层预处理器

您在网络分析策略中配置应用层预处理器，该预处理器准备流量，以便使用在入侵策略中启用的规则检查该流量。有关详情，请参见第 23-1 页上的了解网络分析和入侵策略。

应用层协议可以多种方式呈现相同的数据。思科提供应用层协议解码器，这些解码器可将特定类型的数据包数据规范化为入侵规则引擎可以分析的格式。规范化应用层协议编码使得规则引擎可以有效地将相同的内容相关规则应用于其数据以不同方式呈现的数据包，并获得有意义的结果。

当入侵规则或规则参数要求禁用的预处理器时，系统会自动使用其当前设置，即使其在网络分析策略网络界面中保持禁用状态。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

注意事项 有些具有自定义用户角色的用户无法通过标准菜单路径 (**Policies > Access Control > Network Analysis Policy**) 访问网络分析策略。这些用户可以通过入侵策略访问网络分析策略：**Policies > Intrusion > Intrusion Policy > Network Analysis Policy**。有关自定义用户角色的详细信息，请参阅第 61-48 页上的管理自定义用户角色。

请注意，大多数情况下，预处理器不会生成事件，除非已启用入侵策略中随附的预处理器规则。有关详情，请参见第 32-18 页上的设置规则状态。

有关详细信息，请参阅以下各节：

- 第 27-2 页上的解码 DCE/RPC 流量介绍 DCE/RPC 预处理器，并解释如何对其进行配置以防止检测躲避行为并检测 DCE/RPC 流量异常。
- 第 27-13 页上的检测 DNS 域称服务器响应中的漏洞介绍 DNS 预处理器，并解释如何对其进行配置以检测 DNS 域名服务器响应中三种特定漏洞的任何一种。
- 第 27-16 页上的解码 FTP 和 Telnet 流量介绍 FTP/Telnet 解码器，并解释如何对其进行配置以规范化和解码 FTP 与 Telnet 流量。
- 第 27-26 页上的解码 HTTP 流量介绍 HTTP 解码器，并解释如何对其进行配置以规范化 HTTP 流量。
- 第 27-39 页上的使用 Sun RPC 预处理器介绍 HTTP 解码器，并解释如何对其进行配置以规范化 RPC 流量。
- 第 27-40 页上的解码会话发起协议解释如何使用 SIP 预处理器来解码和检测 SIP 流量异常。
- 第 27-44 页上的配置 GTP 命令通道解释如何使用 GTP 预处理器向规则引擎提供数据包解码器提取的 GTP 命令通道消息。
- 第 27-45 页上的解码 IMAP 流量解释如何使用 IMAP 预处理器来解码和检测 IMAP 流量异常。
- 第 27-48 页上的解码 POP 流量解释如何使用 POP 预处理器来解码和检测 POP 流量异常。
- 第 27-51 页上的解码 SMTP 流量介绍 SMTP 解码器，并解释如何对其进行配置以解码和规范化 SMTP 流量。

- 第 27-57 页上的使用 SSH 预处理器检测攻击解释如何识别和处理 SSH 加密流量中的漏洞。
- 第 27-60 页上的使用 SSL 预处理器解释如何使用 SSL 预处理器识别加密流量，以及如何通过停止流量检查来消除误报。
- 第 28-1 页上的配置 SCADA 预处理解释如何使用 Modbus 和 DNP3 预处理器检测相应流量中的异常，以及如何向入侵规则引擎提供数据以检查某些协议字段。

解码 DCE/RPC 流量

许可证：保护

DCE/RPC 协议使不同网络主机上的进程可以像在同一主机上一样进行通信。这些进程间通信一般通过 TCP 和 UDP 在主机之间传输。在 TCP 传输中， DCE/RPC 也可以进一步封装在 Windows 服务器消息块 (SMB) 协议或 Samba 中；Samba 是一种在由 Windows 和类似 UNIX 或类似 Linux 操作系统组成的混合环境中用于进程间通信的开源 SMB 实现。此外，网络上的 Windows IIS网络服务器可能使用 IIS RPC over HTTP，后者通过防火墙向代理 TCP 传输 DCE/RPC 流量提供分布式通信。

请注意，对 DCE/RPC 预处理器选项和功能的说明包括 DCE/RPC 的 Microsoft 实现 （又称为 MSRPC）；对 SMB 选项和功能的说明涉及 SMB 和 Samba。

虽然大多数 DCE/RPC 漏洞出现在针对 DCE/RPC 服务器 （实际上可能是网络上任何主机）的 DCE/RPC 客户端请求中，但在服务器响应中也可能出现漏洞。 DCE/RPC 预处理器检测封装在 TCP、 UDP 和 SMB 传输 （包括使用版本 1 RPC over HTTP 的 TCP 传输 DCE/RPC）中的 DCE/RPC 请求和响应。此预处理器分析 DCE/RPC 数据流并检测 DCE/RPC 流量中的异常行为和逃避技术。它还分析 SMB 数据流并检测异常 SMB 行为和逃避技术。

除了 IP 分片重组预处理器提供的 IP 分片重组和 TCP 数据流预处理器提供的 TCP 数据流重组外，DCE/RPC 预处理器还可对 SMB 进行碎片整理以及对 DCE/RPC 进行分片重组。请参阅第 29-18 页上的使用 TCP 数据流预处理和第 29-10 页上的对 IP 数据包进行分片重组。

最后， DCE/RPC 预处理器会规范化 DCE/RPC 流量，以便规则引擎进行处理。有关使用特定 DCE/RPC 规则关键字检测 DCE/RPC 服务、操作和存根数据的详细信息，请参阅第 36-54 页上的 DCE/RPC 关键字。

要配置 DCE/RPC 预处理器，可以修改控制预处理器工作方式的全局选项，并指定一个或多个基于目标的服务器策略，从而通过 IP 地址和运行的 Windows 或 Samba 版本识别网络上的 DCE/RPC 服务器：

必须启用生成器 ID (GID) 为 132 或 133 的 DCE/RPC 预处理器规则才可生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

有关详细信息，请参阅以下各节：

- 第 27-3 页上的选择全局 DCE/RPC 选项
- 第 27-4 页上的了解基于目标的 DCE/RPC 服务器策略
- 第 27-4 页上的了解 DCE/RPC 传输
- 第 27-7 页上的选择 DCE/RPC 基于目标的策略选项
- 第 27-10 页上的配置 DCE/RPC 预处理器

选择全局 DCE/RPC 选项

许可证：保护

DCE/RPC 预处理器全局选项控制预处理器的工作方式。修改这些选项可能会对性能或检测能力造成负面影响，但 **Memory Cap Reached** 选项除外。除非您已充分理解此预处理器及其与已启用的 DCE/RPC 规则之间的交互，否则请勿修改这些选项。尤其是，必须确保 **Maximum Fragment Size** 选项和 **Reassembly Threshold** 选项大于或等于规则需要检测的深度。有关详细信息，请参阅第 36-16 页上的限制内容匹配和第 36-28 页上的使用 Byte_Jump 和 Byte_Test。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

Maximum Fragment Size

如果选择了 **Enable Defragmentation**，可指定介于 1514 到 65535 字节之间的最大 DCE/RPC 分片长度。预处理器会在分片重组前将较大分片截断成为指定的尺寸以便进行处理，但不会改变实际数据包。空白字段将禁用此选项。

Reassembly Threshold

如果选择了 **Enable Defragmentation**，0 将禁用该选项，而 1 到 65535 字节将指定在向规则引擎发送重组数据包前要排队的分片 DCE/RPC 最小字节数和（如适用）分段 SMB 最小字节数量。值越小，实现早期检测的可能性越高，但可能会对性能造成负面影响。如果启用此选项，应当测试性能所受影响。

Enable Defragmentation

指定是否对 DCE/RPC 流量进行分片整理。当此选项处于禁用状态时，预处理器仍会检测异常并向规则引擎发送 DCE/RPC 数据，但可能会检测不出分片 DCE/RPC 数据中的漏洞。

尽管通过此选项可灵活选择是否对 DCE/RPC 流量进行分片重组，但大多数 DCE/RPC 漏洞都会尝试利用分片隐藏自己。禁用此选项将会忽略大多数已知漏洞，从而造成大量漏报。

Memory Cap Reached

检测达到或超过分配给预处理器的最大内存限制的时间。当达到或超过最大内存上限时，预处理器会释放与造成内存上限事件的会话相关的所有待处理数据并忽略该会话的剩余部分。

可以启用规则 133:1 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Auto-Detect Policy on SMB Session

检测在 SMB `Session Setup And` 请求和响应中识别出的 Windows 或 Samba 版本。如果检测到的版本不同于为 **Policy** 配置选项配置的 Windows 或 Samba 版本，检测到的版本将会仅覆盖为该会话配置的版本。有关详情，请参见第 27-4 页上的了解基于目标的 DCE/RPC 服务器策略。

例如，如果将 **Policy** 设置为 Windows XP，而预处理器检测到 Windows Vista，预处理器将对该会话使用 Windows Vista 策略。其他设置仍然有效。

如果 DCE/RPC 传输不是 SMB（即，传输协议为 TCP 或 UDP），将无法检测到版本，且策略不能实现自动配置。

要启用此选项，请从下拉列表中选择以下其中一项：

- 选择 **Client**，检查该策略类型的服务器到客户端流量。
- 选择 **Server**，检查该策略类型的客户端到服务器流量。
- 选择 **Both**，检查该策略类型的服务器到客户端流量和客户端到服务器流量。

了解基于目标的 DCE/RPC 服务器策略

许可证：保护

可以创建一个或多个基于目标的服务器策略，并使用这些策略将 DCE/RPC 预处理器配置为像指定类型的服务器一样检查 DCE/RPC 流量。基于目标的策略配置包括识别在网络上识别出的主机上运行的 Windows 或 Samba 版本，启用传输协议并指定将 DCE/RPC 流量传输到这些主机的端口，以及设置其他特定于服务器的选项。

Windows 和 Samba DCE/RPC 的实现有很大不同。例如，在对 DCE/RPC 流量进行分片重组时，所有 Windows 版本都在第一个分片中使用 DCE/RPC 上下文 ID，而所有 Samba 版本都在最后一个分片中使用上下文 ID。再如， Windows Vista 在第一个分片中使用操作编号报头字段来识别特定函数调用，而 Samba 及其他所有 Windows 版本都在最后一个分片中使用操作编号字段。

Windows 和 Samba SMB 的实现也有很大不同。例如， Windows 在与命名管道配合使用时可识别 SMB OPEN 和 READ 命令，而 Samba 不能识别这些命令。

启用 DCE/RPC 预处理器会自动启用默认基于目标的策略。或者，可以添加针对运行不同 Windows 或 Samba 版本的其他主机的基于目标的策略，方法是从 **Policy** 下拉列表选择所需的版本。默认基于目标的策略适用于未包含在其他基于目标的策略的任何主机。

在每个基于目标的策略中，可以启用一个或多个传输并为每个传输指定*检测端口*。还可以启用和指定*自动检测端口*。有关详情，请参见第 27-4 页上的了解 DCE/RPC 传输。

还可以配置基于目标的策略的其他选项。可以设置预处理器，使它检测试图连接一个或多个识别出的共享 SMB 资源的情况。可以将预处理器配置为会检测 SMB 流量中的文件，以及会检查检测出的文件中的指定字节数。还可以修改原本只能由具备 SMB 协议专业知识的用户修改的高级选项；通过该选项，可以将预处理器设置为会检测链式 SMB AndX 命令数量超过指定最小数量的情况。

在每个基于目标的策略中，可以：

- 启用一个或多个传输并为每个传输指定*检测端口*。
- 启用和指定*自动检测端口*。有关详情，请参见第 27-4 页上的了解 DCE/RPC 传输。
- 设置预处理器，使它检测试图连接一个或多个识别出的共享 SMB 资源的情况。
- 将预处理器配置为会检测 SMB 流量中的文件，以及会检查检测出的文件中的指定字节数。
- 修改原本只能由具备 SMB 协议专业知识的用户修改的高级选项；通过该选项，可以将预处理器设置为会检测链式 SMB AndX 命令数量超过指定最小数量的情况。

请注意，可以启用 **Auto-Detect Policy on SMB Session** 全局选项，以便在 DCE/RPC 传输是 SMB 时自动覆盖为每个会话的目标策略配置的策略类型。请参阅第 27-3 页上的Auto-Detect Policy on SMB Session。

除了在 DCE/RPC 预处理器中启用 SMB 流量文件检测功能，还可以配置文件策略以便选择性地捕获和拦截这些文件，或者将这些文件提交到综合安全智能云以进行动态分析。在策略中，必须创建具有**操作**为 **Detect Files** 或 **Block Files** 且选定**应用协议**为 **Any** 或 **NetBIOS-ssn (SMB)** 的文件规则。有关详细信息，请参阅第 37-14 页上的创建文件策略和第 37-15 页上的使用文件规则。

了解 DCE/RPC 传输

许可证：保护

在每个基于目标的策略中，都可以启用一个或多个 TCP、 UDP、 SMB 和 RPC over HTTP 传输。启用传输时，还必须指定一个或多个*检测端口*（即，已知用于传输 DCE/RPC 流量的端口）。或者，也可以启用和指定*自动检测端口*；预处理器会首先对这些端口进行测试，以确定它们是否传输 DCE/RPC 流量，仅在检测到 DCE/RPC 流量的情况下，预处理器才会继续进行处理。

思科建议您使用默认检测端口（可以是已知端口，也可以是各协议的常用端口）。在非默认端口检测到 DCE/RPC 流量的情况下才可以添加端口。

启用自动检测端口时，请确保将端口范围设置为 1024 到 65535，以便覆盖整个临时端口范围。请注意，很少会为 RPC over HTTP Proxy Auto-Detect Ports 选项和 SMB Auto-Detect Ports 选项启用或指定自动检测端口，因为这两者出现流量的可能性很低甚至不可能出现，除非是在指定的默认检测端口上。另请注意，传输检测端口未识别出的端口才会出现自动检测。有关为每个传输启用或禁用自动检测端口的建议，请参阅第 27-7 页上的选择 DCE/RPC 基于目标的策略选项。

可以在 Windows 基于目标的策略中为一个或多个传输指定任意组合的端口，以便与网络流量匹配，但是，在 Samba 基于目标的策略中只能为 SMB 传输指定端口。

请注意，在默认基于目标的策略中必须至少启用一个 DCE/RPC 传输，除非已经添加至少已启用一个传输的 DCE/RPC 基于目标的策略。例如，您可能想为所有 DCE/RPC 实现指定主机，但没有适用于未指定主机的默认基于目标的策略，在这种情况下，您不会为默认基于目标的策略启用传输。

有关详细信息，请参阅以下各节：

- 第 27-5 页上的了解无连接和面向连接 DCE/RPC 流量
- 第 27-6 页上的了解 RPC over HTTP 传输

了解无连接和面向连接 DCE/RPC 流量

许可证：保护

DCE/RPC 消息符合两种不同的 DCE/RPC 协议数据单元（PDU）之一：

- 面向连接 DCE/RPC PDU 协议

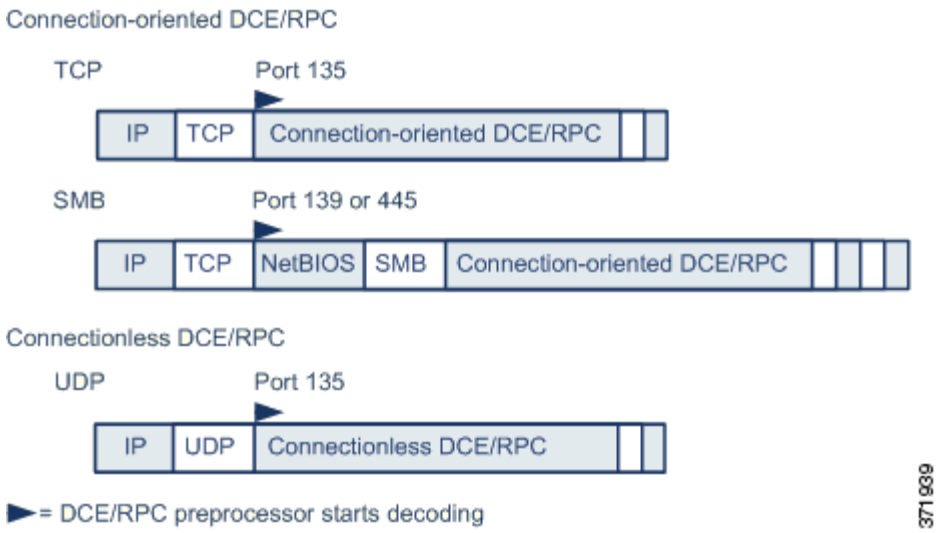
  DCE/RPC 预处理器在 TCP、 SMB 和 RPC over HTTP 传输中检测面向连接 DCE/RPC。

- 无连接 DCE/RPC PDU 协议

  DCE/RPC 预处理器在 UDP 传输中检测无连接 DCE/RPC。

这两种 DCE/RPC PDU 协议都有独特的报头和数据特性。例如，面向连接的 DCE/RPC 的报头长度通常为 24 字节，而无连接 DCE/RPC 的报头长度固定为 80 字节。此外，分片无连接 DCE/RPC 的正确分片顺序不能通过无连接传输处理，而必须通过无连接 DCE/RPC 报头值提供保证；相比之下，传输协议可确保面向连接 DCE/RPC 的分片顺序正确。 DCE/RPC 预处理器使用这些特性及其他特定协议特性监控这两种协议是否存在异常和其他躲避技术，对流量进行解码和分片重组，然后再将流量传送到规则引擎。

下图说明了 DCE/RPC 预处理器开始为不同传输处理 DCE/RPC 流量的点。



对于上图，请注意以下几点：

- 已知 TCP 或 UDP 端口 135 识别 TCP 和 UDP 传输中的 DCE/RPC 流量。
- 图中未包含 RPC over HTTP。

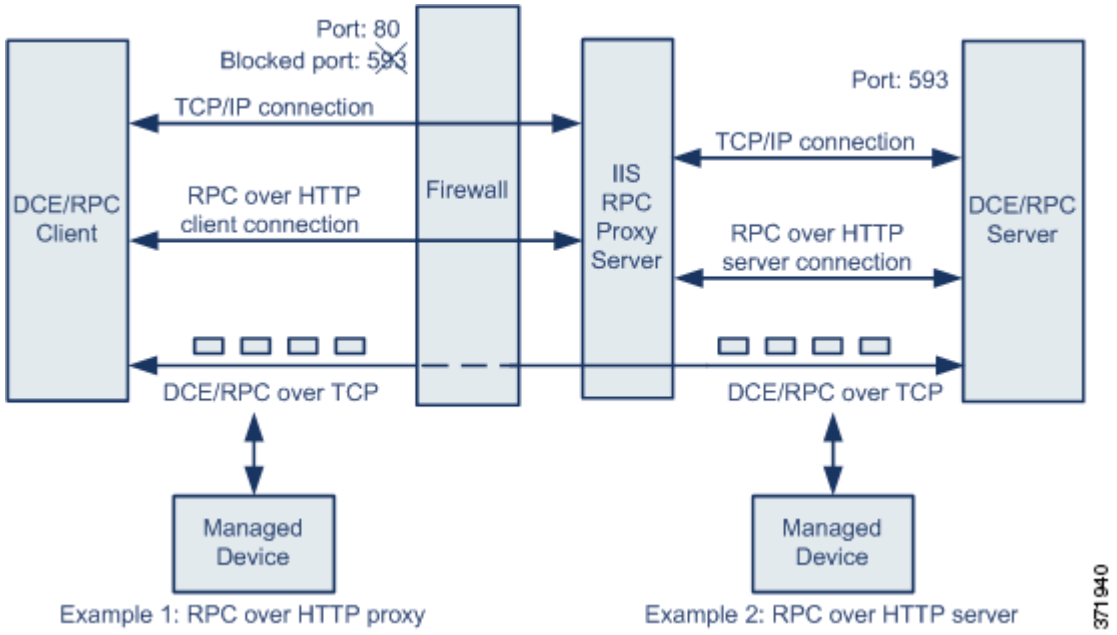
  对于 RPC over HTTP，面向连接 DCE/RPC 在完成 HTTP 初始设置序列后直接通过 TCP 传输（如图所示）。有关详情，请参见第 27-6 页上的了解 RPC over HTTP 传输。
- DCE/RPC 预处理器通常接收适用于 NetBIOS 会话服务的已知 TCP 端口 139 或以类似方式实现的已知 Windows 端口 445 上的 SMB 流量。

  由于 SMB 具有除传输 DCE/RPC 以外的许多功能，因此，预处理器会首先测试 SMB 流量是否正在传输 DCE/RPC 流量，如果不是，预处理器会停止处理，如果是，则继续进行处理。
- IP 封装所有 DCE/RPC 传输。
- TCP 传输所有面向连接 DCE/RPC。
- UDP 传输无连接 DCE/RPC。

了解 RPC over HTTP 传输

许可证：保护

借助 Microsoft RPC over HTTP，可以引导 DCE/RPC 流量穿过防火墙，如下图所示。DCE/RPC 预处理器检测版本 1 Microsoft RPC over HTTP。



Microsoft IIS 代理服务器和 DCE/RPC 服务器可以位于同一主机上，也可以位于不同的主机上。对于这两种情况，都提供独立的代理和服务器选项。对于上图，请注意以下几点：

- DCE/RPC 服务器监控端口 593 的 DCE/RPC 客户端流量，但防火墙阻止该端口。

  默认情况下，防火墙通常会阻止端口 593。
- RPC over HTTP 使用已知 HTTP 端口 80（防火墙通常允许此端口）通过 HTTP 传输 DCE/RPC。
- 在示例 1 中，将会选择 **RPC over HTTP proxy** 选项来监控 DCE/RPC 客户端与 MicroSoft IIS RPC 代理服务器之间流量。
- 在示例 2 中，如果 MicroSoft IIS RPC 代理服务器与 DCE/RPC 服务器位于不同的主机，且设备监控这两个服务器之间的流量，将会选择 **RPC over HTTP server** 选项。
- RPC over HTTP 完成 DCE/RPC 客户端和服务器代理设置后，流量仅包含通过 TCP 传输的面向连接 DCE/RPC。

选择 DCE/RPC 基于目标的策略选项

许可证：保护

每个基于目标的策略都允许指定以下各个选项。请注意，除 **Memory Cap Reached** 和 **Auto-Detect Policy on SMB Session** 这两个选项外，修改这些选项可能会对性能或检测能力造成负面影响。除非您已充分理解此预处理器及其与已启用的 DCE/RPC 规则之间的交互，否则请勿修改这些选项。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

网络

需要应用 DCE/RPC 基于目标的服务器策略的主机 IP 地址。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。总共最多可以指定 255 个配置文件 （包括默认策略）。有关在 FireSIGHT 系统中指定 IPv4 和 IPv6 地址块的详细信息，请参阅。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如， 0.0.0.0/0 或 ::/0）。

另请注意，为了让基于目标的策略处理流量，您标识的网络必须匹配您在其中配置该策略的网络分析策略处理的网络、区域和 VLAN 或是其子集。有关详情，请参见第 25-2 页上的使用网络分析策略自定义预处理。

策略

目标主机或受监控网段上主机使用的 Windows 或 Samba DCE/RPC 实现。有关这些策略的详细信息，请参阅第 27-4 页上的了解基于目标的 DCE/RPC 服务器策略。

请注意，可以启用 **Auto-Detect Policy on SMB Session** 全局选项，以便在 DCE/RPC 传输是 SMB 时自动覆盖每个会话的此选项的设置。请参阅第 27-3 页上的Auto-Detect Policy on SMB Session。

SMB Invalid Shares

用于识别一个或多个 SMB 共享资源的字母数字文本字符串，不区分大小写；预处理器将会检测是否有程序试图连接您指定的共享资源。您可以在逗号分隔列表中指定多个共享，或者可以将共享用引号引起来（旧版软件要求这样做，但现在不再有此要求），例如：

```
"C$", D$, "admin", private
```

当 SMB 端口和 SMB 流量检测功能都处于启用状态时，预处理器会检测 SMB 流量中的无效共享。

请注意，大多数情况下，对于被识别为无效共享的 Windows 命名的驱动器，应该在其后面附上一个美元符号。例如，将驱动器 C 标识为 C$ 或 "C$"。

可以启用规则 133:26 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

SMB Maximum AndX Chain

允许的的链式 SMB AndX 命令最大数量，介于 0 到 255 之间。通常，超过若干链式 AndX 命令即表示存在异常行为，可能代表有躲避行为。指定 1 表示不允许链式命令，指定 0 将会禁止检测链式命令数量。

请注意，预处理器会首先计算链式命令数量，如果随附的 SMB 预处理器规则已启用，并且链式命令数量等于或超过配置的值，预处理器将会生成事件。然后会继续进行处理。

注　只有 SMB 协议专业人员才可以修改此选项的默认设置。

可以启用规则 133:20 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

RPC proxy traffic only

当 **RPC over HTTP Proxy Ports** 处于启用状态时，此选项指明检测到的客户端 RPC over HTTP 流量是仅包含代理流量还是可能包含其他网络服务器流量。例如，端口 80 可能传输代理流量和其他网络服务器流量。

此选项处于禁用状态时，将会同时传输代理流量和其他网络服务器流量。例如，如果服务器是专用代理服务器，请启用此选项。启用此选项后，预处理器会测试流量以确定其是否传输 DCE/RPC，如果不是，预处理器将会忽略该流量，如果是，则继续进行处理。请注意，仅在已选择 **RPC over HTTP Proxy Ports** 复选框的情况下，此选项才有用。

RPC over HTTP Proxy Ports

如果受管设备位于 DCE/RPC 客户端与 MicroSoft IIS RPC 代理服务器之间，可以使用此选项对 RPC over HTTP 通过每个指定端口传输的 DCE/RPC 流量启用检测。请参阅第 27-6 页上的了解 RPC over HTTP 传输。

启用此选项后，可以添加任意发现 DCE/RPC 流量的端口，但是这项操作一般并不必要，因为网络服务器通常使用默认端口传输 DCE/RPC 和其他流量。启用此选项后，不可以启用 **RPC over HTTP Proxy Auto-Detect Ports**，但如果检测到的客户端 RPC over HTTP 流量仅包含代理流量而不包含其他网络服务器流量，可以启用 **RPC Proxy Traffic Only**。

RPC over HTTP Server Ports

如果 MicroSoft IIS RPC 代理服务器与 DCE/RPC 服务器位于不同的主机，且设备监控这两个服务器之间的流量，可以使用此选项对 RPC over HTTP 通过每个指定端口传输的 DCE/RPC 流量启用检测。请参阅第 27-6 页上的了解 RPC over HTTP 传输。

启用此选项后，通常还应启用 **RPC over HTTP Server Auto-Detect Ports** （端口范围介于 1025 到 65535 之间），即使不知道网络上是否存在任何代理网络服务器。请注意，RPC over HTTP 服务器端口有时会重新配置，在这种情况下，应该为此选项将重新配置的服务器端口添加到端口列表。

TCP Ports

对每个指定端口上 TCP 中的 DCE/RPC 流量启用检测。

合法 DCE/RPC 流量和漏洞可能使用多种端口，高于端口 1024 的其他端口很常用。启用此选项后，通常还应启用 **TCP Auto-Detect Ports** （端口范围介于 1025 到 65535 之间）。

UDP Ports

对每个指定端口上 UDP 中的 DCE/RPC 流量启用检测。

合法 DCE/RPC 流量和漏洞可能使用多种端口，高于端口 1024 的其他端口很常用。启用此选项后，通常还应启用 **UDP Auto-Detect Ports** （端口范围介于 1025 到 65535 之间）。

SMB Ports

对每个指定端口上 SMB 中的 DCE/RPC 流量启用检测。

可能会出现使用默认检测端口的 SMB 流量。其他端口很少见。通常使用默认设置。

RPC over HTTP Proxy Auto-Detect Ports

如果受管设备位于 DCE/RPC 客户端与 MicroSoft IIS RPC 代理服务器之间，可以使用此选项对 RPC over HTTP 通过指定端口传输的 DCE/RPC 流量启用自动检测。请参阅第 27-6 页上的了解 RPC over HTTP 传输。

启用此选项后，通常需要指定介于 1025 到 65535 之间的端口范围，以覆盖整个临时端口范围。

RPC over HTTP Server Auto-Detect Ports

如果 MicroSoft IIS RPC 代理服务器与 DCE/RPC 服务器位于不同的主机，且设备监控这两个服务器之间的流量，可以使用此选项对 RPC over HTTP 通过指定端口传输的 DCE/RPC 流量启用自动检测。请参阅第 27-6 页上的了解 RPC over HTTP 传输。

TCP Auto-Detect Ports

对指定端口上 TCP 中的 DCE/RPC 流量启用自动检测。

UDP Auto-Detect Ports

对指定端口上 UDP 中的 DCE/RPC 流量启用自动检测。

SMB Auto-Detect Ports

对 SMB 中的 DCE/RPC 流量启用自动检测。

SMB File Inspection

启用 SMB 流量检查以检测文件。您有以下选项：

- 选择 **Off** 禁用文件检查。
- 选择 **Only**，检查文件数据但不检查 SMB 中的 DCE/RPC 流量。选择此选项可以提高文件和 DCE/RPC 流量检查性能。
- 选择 **On**，检查 SMB 中的文件和 DCE/RPC 流量。选择此选项可能会影响性能。

以下各项不支持 SMB 流量检查：

- 在 SMB2.x 和 SMB3.x 中传输的文件
- 在启用此选项和应用政策之前在建立的 TCP 或 SMB 会话中传输的文件
- 单一 TCP 或 SMB 会话同时传输的文件
- 在多个 TCP 或 SMB 会话之间传输的文件
- 与非连续数据一起传输的文件 （例如，协商了消息签名时）
- 与具有相同偏移量的不同数据一起传输的文件 （与数据重叠）
- 在远程客户端打开用于编辑并由客户端保存到文件服务器的文件

SMB File Inspection Depth

如果 **SMB File Inspection** 设置为 **Only** 或 **On**，此选项表示在 SMB 流量中检测到文件时检查的字节数。指定以下各项之一：

- `1` 到 `2147483647` （约 2GB）之间的任意整数
- `0` 以检查整个文件
- `-1` 以禁用文件检查

在此字段中输入的值应等于或小于在访问控制策略中指定的值。如果为此选项设置的值大于为 **Limit the number of bytes inspected when doing file type detection** 定义的值，系统会将访问控制策略设置用作有效的最大值。有关详细信息，请参阅第 18-17 页上的调整文件和恶意软件检查性能和存储。

如果 **SMB File Inspection** 设置为 **Off**，此字段将被禁用。

配置 DCE/RPC 预处理器

许可证：保护

可以配置 DCE/RPC 预处理器全局选项以及一个或多个基于目标的服务器策略。

除非启用带有生成器 ID (GID) 133 的规则，否则预处理器不会生成事件。有关与特定检测选项相关的规则，请参阅第 27-3 页上的选择全局 DCE/RPC 选项和第 27-7 页上的选择 DCE/RPC 基于目标的策略选项；另请参阅第 32-18 页上的设置规则状态。

此外，大多数 DCE/RPC 预处理器规则都会针对 SMB、面向连接 DCE/RPC 或无连接 DCE/RPC 流量中检测到的异常和躲避技术生成事件。下表列出了可为各类流量启用的规则。

表 27-1　　流量相关 DCE/RPC 规则

流量	预处理器规则 GID:SID
中小企业 (SMB)	133:2 到 133:26，以及 133:48 到 133:57
面向连接 DCE/RPC	133:27 到 133:39
检测无连接 DCE/RPC	133:40 到 133:43

要配置 DCE/RPC 预处理器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **DCE/RPC Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 DCE/RPC Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　可以修改第 27-3 页上的选择全局 DCE/RPC 选项中所述的任何选项。

步骤 6　此时您有两种选择：

- 添加新的基于目标的策略。点击页面左侧 **Servers** 旁边的添加图标 ( )。系统将显示 Add Target 弹出窗口。在 **Server Address** 字段中指定一个或多个 IP 地址，然后点击 **OK**。

  可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。有关在 FireSIGHT 系统中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-16 页上的IP 地址约定。

  总共最多可以配置 255 个策略 （包括默认策略）。

  请注意，为了让基于目标的策略处理流量，您标识的网络必须匹配您在其中配置该策略的网络分析策略处理的网络、区域和 VLAN 或是其子集。有关详情，请参见第 25-2 页上的使用网络分析策略自定义预处理。

  新条目将出现在页面左侧的服务器列表中，突出显示以表明其已被选定；Configuration 部分会进行更新，以反映所添加的策略的当前配置。

- 修改现有基于目标的策略的设置。点击在页面左侧 **Servers** 中添加的策略的配置地址，或者点击 **default**。

  所选项目将会突出显示，并且 Configuration 部分会进行更新以显示所选策略的当前配置。要删除现有策略，请点击要删除的策略旁边的删除图标 ( )。

步骤 7　可以修改以下基于目标的策略选项：

- 要指定要对其应用 DCE/RPC 基于目标的服务器策略的主机，请在 **Networks** 字段中输入单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。

  总共最多可以指定 255 个配置文件 （包括默认策略）。请注意，不能修改默认策略中的 **Networks** 设置。默认策略适用于网络上未在其他策略中识别出的所有服务器。

- 要指定要应用于网段上指定主机的策略类型，请从 **Policy** 下拉列表选择 Windows 或 Samba 策略类型之一。

  请注意，可以启用 **Auto-Detect Policy on SMB Session** 全局选项，以便在 DCE/RPC 传输是 SMB 时自动覆盖每个会话的此选项的设置。请参阅第 27-3 页上的Auto-Detect Policy on SMB Session。

- 要将预处理器设置为会检测是否有企图连接到特定 SMB 共享资源的情况，请在 **SMB Invalid Shares** 字段中输入用以识别共享资源的单一字符串或字符串的逗号分隔列表 （字符串不区分大小写）。或者，用引号将单个字符串引起来 （旧版软件要求这样做，但现在不再有此要求）

  例如，要检测名为 C$、 D$、 admin 和 private 的共享资源，可以输入：

  ```
  "C$", D$, "admin", private
  ```

  请注意，要检测 SMB 无效共享，还必须启用 **SMB Ports** 或 **SMB Auto-Detect Ports** 和 **SMB Traffics** 全局选项。

  另请注意，大多数情况下，对于被识别为无效共享的 Windows 命名的驱动器，应该在其后面附上一个美元符号。例如，可输入 `C$` 或 `"C$"` 来标识驱动器 C。

- 要检查在 SMB 中的 DCE/RPC 流量中检测到的文件而不分析 DCE/RPC 流量，请从 **SMB File Inspection** 下拉列表选择 **Only**。要检查在 SMB 中的 DCE/RPC 流量中检测到的文件和 DCE/RPC 流量，请从 **SMB File Inspection** 下拉列表选择 **On**。在 **SMB File Inspection Depth** 字段输入要在检测到的文件中检查的字节数。输入 `0` 将会检查整个检测到的文件。

- 要指定允许的链式 SMB AndX 命令最大数量，请在 **SMB Maximum AndX Chains** 字段中输入 0 到 255 之间的值。指定 `1` 表示不允许任何链式命令。指定 `0` 或将此选项留空将会禁用此功能。

注　只有 SMB 协议专业人员可以修改 **SMB Maximum AndX Chains** 选项的设置。

- 要为 Windows 策略传输对已知用于传输 DCE/RPC 流量的端口上的 DCE/RPC 流量启用处理，请选择或清除检测传输旁边的复选框，或者添加或删除用于该传输的端口。

  为 Windows 策略选择 **RPC over HTTP Proxy Ports**、**RPC over HTTP Server Ports**、**TCP Ports** 或 **UDP Ports** 或者它们的任意组合。如果 **RPC over HTTP proxy** 已启用，且检测到的客户端 RPC over HTTP 流量仅包含代理流量 （也就是说，不包含其他网络服务器流量），可选择 **RPC Proxy Traffic Only**。

  为 Samba 策略选择 **SMB Ports**。

  大多数情况下使用默认设置。有关详细信息，请参阅第 27-4 页上的了解 DCE/RPC 传输、第 27-6 页上的了解 RPC over HTTP 传输和第 27-7 页上的选择 DCE/RPC 基于目标的策略选项。

  可以输入单一端口、用破折线 (-) 分隔的一系列端口编号或者用逗号分隔的端口编号和端口范围列表。

- 要测试指定端口是否传输 DCE/RPC 流量并在指定端口是传输 DCE/RPC 流量的情况下继续进行处理，请选择或清除自动检测传输旁边的复选框，或者添加或删除用于该传输的端口。

  为 Windows 策略选择 **RPC over HTTP Server Auto-Detect Ports**、**TCP Auto-Detect Ports** 或 **UDP Auto-Detect Ports** 或者它们的任意组合。

  请注意，极少情况下需要甚至无需选择 **RPC over HTTP Proxy Auto-Detect Ports** 或 **SMB Auto-Detect Ports**。

  通常应该为自动检测端口指定 1025 到 65535 之间的端口范围，以涵盖整个临时端口范围。有关详细信息，请参阅第 27-4 页上的了解 DCE/RPC 传输、第 27-6 页上的了解 RPC over HTTP 传输和第 27-7 页上的选择 DCE/RPC 基于目标的策略选项。

有关详情，请参见第 27-7 页上的选择 DCE/RPC 基于目标的策略选项。

步骤 8　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

检测 DNS 域称服务器响应中的漏洞

许可证：保护

DNS 预处理器会检查 DNS 域称服务器响应中是否存在以下具体漏洞：

- RData 文本字段中的溢出尝试
- 过时的 DNS 资源记录类型
- 试验性 DNS 资源记录类型

有关详细信息，请参阅以下各节：

了解 DNS 预处理器资源记录检查

许可证：保护

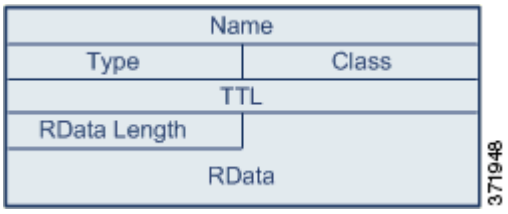
最常见的 DNS 域称服务器响应类型提供与促成响应的查询中域名对应的一个或多个 IP 地址。其他服务器响应类型提供邮件消息目的地或者可提供从最初查询的服务器无法获得的信息的域名服务器位置，等等。

DNS 响应包括一个消息头、一个包含一个或多个请求的 Question 部分以及响应 Question 部分中请求的三个部分 （Answer、 Authority 和 Additional Information）。这三个部分中的响应反映域名服务器内保留的*资源记录* (RR)。下表将介绍这三个部分。

表 27-2　　DNS 域称服务器 RR 响应

部分	包含的内容	示例
回答	（可选）为查询提供明确答复的一个或多个资源记录	对应于域名的 IP 地址
职权	（可选）指向授权域名服务器的一个或多个资源记录	用于响应的授权域名服务器的名称
更多信息	（可选）提供与 Answer 部分相关的其他信息的一个或多个资源记录	要查询的另一个服务器的 IP 地址

有许多类型的资源记录，全部遵循以下结构：



理论上，任何类型的资源记录均可用于域名服务器响应消息的 Answer、 Authority 或 Additional Information 部分。 DNS 预处理器会检查这三个响应部分中的资源记录是否存在其会检测的漏洞。

Type 和 RData 资源记录字段对于 DNS 预处理器特别重要。 Type 字段识别资源记录类型。 RData（资源数据）字段提供响应内容。 RData 字段的大小和内容因资源记录类型而异。

DNS 消息通常使用 UDP 传输协议，但如果消息类型需要可靠传输或者消息大小超过 UDP 能力，DNS 消息也会使用 TCP。 DNS 预处理器会检查 UDP 和 TCP 流量中的 DNS 服务器响应。

DNS 预处理器不会检查在中途恢复的 TCP 会话，如果会话因丢包而丧失状态， DNS 预处理器将会停止检查。

为 DNS 预处理器配置的典型端口为已知端口 53， DNS 域名服务器对在 UDP 和 TCP 中传输的 DNS 消息使用该端口。

检测 RData 文本字段中的溢出尝试

许可证：保护

当资源记录类型为 TXT （文本）时， RData 字段为长度可变的 ASCII 文本字段。

如果选择 DNS 预处理器的 **Detect Overflow attempts on RData Text fields** 选项，将会检测条目 CVE-2006-3441 在 MITRE 的通用漏洞字典数据库中识别出的具体漏洞。这是 Microsoft Windows 2000 Service Pack 4、Windows XP Service Pack 1、Windows XP Service Pack 2 和 Windows Server 2003 Service Pack 1 中的已知漏洞。攻击者可以利用该漏洞发送或者导致主机接收恶意域名服务器响应，导致 RData 文本字段长度计算错误，造成缓冲区溢出，最终全面控制主机。

如果网络上可能有主机运行尚未升级纠正该漏洞的操作系统，应该启用此功能。

可以启用规则 131:3 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

检测过时的 DNS 资源记录类型

许可证：保护

RFC 1035 将多种资源记录类型识别为过时类型。由于这些是过时记录类型，因此，某些系统未对其进行说明，可能容易产生漏洞。在正常 DNS 响应中不会遇到这些记录类型，除非故意将网络配置为包含这些记录类型。

可以将系统配置为会检测过时的资源记录类型。下表列出并说明这些记录类型。

表 27-3　过时的 DNS 资源记录类型

RR 类型	代码	说明
3	MD	邮件目的地
4	MF	邮件转发器

可以启用规则 131:1 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

检测试验性 DNS 资源记录类型

许可证：保护

RFC 1035 将多种资源记录类型识别为试验性类型。由于这些是试验性记录类型，因此，某些系统未对其进行说明，可能容易产生漏洞。在正常 DNS 响应中不会遇到这些记录类型，除非故意将网络配置为包含这些记录类型。

可以将系统配置为会检测试验性资源记录类型。下表列出并说明这些记录类型。

表 27-4　试验性 DNS 资源记录类型

RR 类型	代码	说明
7	MB	邮箱域名
8	MG	邮件组成员
9	MR	邮件重命名域名
10	NUL	空资源记录

可以启用规则 131:2 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

配置 DNS 预处理器

许可证：保护

可按照以下步骤配置 DNS 预处理器。有关配置本页中所述选项的详细信息，请参阅第 27-14 页上的检测 RData 文本字段中的溢出尝试、第 27-14 页上的检测过时的 DNS 资源记录类型和第 27-15 页上的检测试验性 DNS 资源记录类型。

要配置 DNS 预处理器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **DNS Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 DNS Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　或者，可以修改 Settings 区域中的以下任何内容：

- 在 **Ports** 字段中指定 DNS 预处理器应为 DNS 服务器响应监控的源端口。使用逗号分隔多个端口。
- 选择 **Detect Overflow Attempts on RData Text fields** 复选框将会检测 RData 文本字段缓冲区溢出尝试。
- 选择 **Detect Obsolete DNS RR Types** 复选框将会检测过时资源记录类型。
- 选择 **Detect Experimental DNS RR Types** 复选框将会检测试验性资源记录类型。

步骤 6　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

解码 FTP 和 Telnet 流量

许可证：保护

FTP/Telnet 解码器会分析 FTP 和 Telnet 数据流，对 FTP 和 Telnet 命令进行规范化，再由规则引擎处理这些命令。

必须启用生成器 ID (GID) 分别为 125 和 126 的 FTP 和 Telnet 预处理器规则才可生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

有关详细信息，请参阅以下主题：

了解 FTP 和 Telnet 全局选项

许可证：保护

可以设置全局选项以确定 FTP/Telnet 解码器是否对数据包执行状态检查或无状态检查，是否检测加密 FTP 或 Telnet 会话，以及是否在遇到加密数据后继续检查数据流。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

状态性检查

如果选择此选项， FTP/Telnet 解码器将会保存状态，提供各个数据包的会话上下文，并且仅检查重组的会话。如果清除此选项，将会在没有会话上下文的情况下分析每个数据包。

要检查 FTP 数据传输，必须选择此选项。

Detect Encrypted Traffic

检测加密 Telnet 和 FTP 会话。

可以启用规则 125:7 和 126:2 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Continue to Inspect Encrypted Data

指示预处理器在数据流加密后持续检查数据流，以寻找最终解密数据。

配置 FTP/Telnet 全局选项

许可证：保护

需要配置 FTP/Telnet 解码器的全局选项，以控制是否执行无状态检查或状态化检查，是否检测已加密流量，以及解码器是否继续在其确定为已加密的数据流中查找已解码数据。有关全局设置的详细信息，请参阅第 27-16 页上的了解 FTP 和 Telnet 全局选项。

要配置全局选项，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

系统将显示 Advanced Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **FTP and Telnet Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 FTP and Telnet Configuration 页面。

页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

提示　有关配置本页中所述其他选项的详细信息，请参阅第 27-18 页上的配置 Telnet 选项、第 27-22 页上的配置服务器级别 FTP 选项和第 27-25 页上的配置客户端级别 FTP 选项。

步骤 5　或者，您可以修改 Global Settings 页面区域中的以下任何项：

- 选择 **Stateful Inspection** 将会检查包含 FTP 数据包的重组 TCP 数据流。清除 **Stateful Inspection** 将只会检查非重组数据包。
- 选择 **Detect Encrypted Traffic** 将会检测加密流量。清除 **Detect Encrypted Traffic** 将会忽略加密流量。

- 如有需要，可选择 **Continue to Inspect Encrypted Data**，以便在数据流加密后继续检查数据流，以及如果数据流再次解码，可以对其进行处理。

步骤 6　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

了解 Telnet 选项

许可证：保护

可以通过 FTP/Telnet 解码器启用或禁用 Telnet 命令规范化，启用或禁用特定异常情况，以及设置允许的 Are You There (AYT) 攻击阈值。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

端口

指明要实现 Telnet 流量规范化的端口。可在此界面列出多个端口，端口之间用逗号分隔。

Normalize

对流向指定端口的 Telnet 流量进行规范化。

Detect Anomalies

检测没有对应 SE （下级协商终点）的 Telnet SB （下级协商起点）。

Telnet 支持以 SB （下级协商起点）开始并且必须以 SE 结束 （下级协商终点）的下级协商。但是， Telnet 服务器的某些实现将忽略无对应 SE 的 SB。这是异常行为，可能意味着存在躲避行为。由于 FTP 在控制接口使用 Telnet 协议，因此也容易受此行为影响。

如果在 Telnet 流量中检测到这种异常，可以启用规则 126:3 生成事件；如果在 FTP 命令通道中检测到这种异常，可以启用规则 125:9 生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Are You There Attack Threshold Number

检测超过指定阈值的连续 AYT 命令数量。思科建议您将 AYT 阈值设置为不超过 20 的数值。

可以启用规则 126:1 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

配置 Telnet 选项

许可证：保护

可以启用或禁用规范化，启用或禁用特定异常情况，以及控制允许的 Are You There (AYT) 攻击阈值。有关 Telnet 选项的更多信息，请参阅第 27-18 页上的了解 Telnet 选项。

要配置 Telnet 选项，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **FTP and Telnet Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 FTP and Telnet Configuration 页面。

页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

提示　有关配置本页中所述其他选项的详细信息，请参阅第 27-17 页上的配置 FTP/Telnet 全局选项、第 27-22 页上的配置服务器级别 FTP 选项和第 27-25 页上的配置客户端级别 FTP 选项。

步骤 5　或者，您可以修改 Telnet Settings 页面区域中的以下任何项：

- 在 **Ports** 字段中指定应解码 Telnet 流量的端口。Telnet 通常连接到 TCP 端口 23。使用逗号分隔多个端口。

注意事项　由于加密流量 (SSL) 无法解码，因此，添加端口 22 (SSH) 可能会产生意外结果。

- 选择或清除 **Normalize** Telnet Protocol Options 复选框，以启用或禁用 Telnet 规范化。
- 选择或清除 **Detect Anomalies** Telnet Protocol 复选框，以启用或禁用异常检测功能。
- 使用 **Are You There Attack Threshold Number** 指定允许的连续 AYT 命令阈值。

提示　思科建议将 AYT 阈值设置为不超过默认值的数值。

步骤 6　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

了解服务器级别 FTP 选项

许可证：保护

可以在多个 FTP 服务器上设置解码选项。创建的每个服务器配置文件都包含服务器 IP 地址以及应监控其流量的服务器端口。可以为特定服务器指定需要验证和可忽略的 FTP 命令，以及设置最大命令参数长度。还可以设置解码器应针对特定命令验证的具体命令语法，以及设置替代最大命令参数长度。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

网络

使用此选项可指定 FTP 服务器的一个或多个 IP 地址。

可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。最多可配置 1024 个字符，最多可指定 255 个配置文件 （包括默认配置文件）。有关在 FireSIGHT 系统中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-16 页上的IP 地址约定。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或地址块，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any` （例如， 0.0.0.0/0 或 ::/0）。

另请注意，为了让基于目标的策略处理流量，您标识的网络必须匹配您在其中配置该策略的网络分析策略处理的网络、区域和 VLAN 或是其子集。有关详情，请参见第 25-2 页上的使用网络分析策略自定义预处理。

端口

使用此选项可指定受管设备应监控其流量的 FTP 服务器上的端口。可在此界面列出多个端口，端口之间用逗号分隔。

File Get Commands

使用此选项可定义用于从服务器向客户端传输文件的 FTP 命令。请勿改变此选项的值，除非支持人员要求这样做。

File Put Commands

使用此选项可定义用于从客户端向服务器传输文件的 FTP 命令。请勿改变此选项的值，除非支持人员要求这样做。

Additional FTP Commands

使用此行可指定解码器应检测的其他命令。使用空格隔开其他命令。

Default Max Parameter Length

在未设置替代最大参数长度的情况下，使用此选项可检测命令的最大参数长度。

可以启用规则 125:3 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Alternate Max Parameter Length

使用此选项可指定要为其检测其他最大参数长度的命令，并指定这些命令的最大参数长度。点击 **Add** 可添加行，在添加的行中可指定其他最大参数长度，以便检测特定命令。

Check Commands for String Format Attacks

使用此选项可检查指定命令的字符串格式攻击。

可以启用规则 125:5 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Command Validity

使用此选项可为特定命令输入有效格式。有关创建 FTP 命令参数验证语句来验证作为 FTP 通信一部分接收的参数的语法的详细信息，请参阅第 27-21 页上的创建 FTP 命令参数验证语句。点击 **Add** 可添加命令验证行。

可以启用规则 125:2 和 125:4 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Ignore FTP Transfers

使用此选项可禁用除数据传输通道状态检查之外的所有检查，从而提高 FTP 数据传输的性能。

Detect Telnet Escape Codes within FTP Commands

使用此选项可检测何时在 FTP 命令通道上使用 Telnet 命令。

可以启用规则 125:1 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Ignore Erase Commands during Normalization

如果选择了 **Detect Telnet Escape Codes within FTP Commands**，使用此选项可在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令。此选项的设置应与 FTP 服务器处理 Telnet 擦除命令的方式相匹配。请注意，新 FTP 服务器通常会忽略 Telnet 擦除命令，而旧服务器通常会进行处理。

故障排除选项：记录 FTP 命令验证配置

在故障排除呼叫期间，支持代表可能要求您将系统配置为打印为服务器列出的每条 FTP 命令的配置信息。

注意事项 更改此故障排除选项的设置会影响性能，并只能在支持代表的指导下进行。

创建 FTP 命令参数验证语句

许可证：保护

为 FTP 命令创建验证语句时，可以通过使用空格隔开参数来指定一组替代参数。还可以在两个参数之间建立二进制 OR 关系，方法是使用竖线 (|) 隔开这两个参数。用方括号 ([]) 引起来的参数是可选参数。用花括号 ({}) 引起来的参数是必要参数。

可以创建 FTP 命令参数验证语句，以验证作为 FTP 通信一部分接收的参数的语法。有关详情，请参见第 27-19 页上的了解服务器级别 FTP 选项。

下表中列出的任何参数均可用于 FTP 命令参数验证语句中。

表 27-5　　FTP 命令参数

使用的参数	出现的验证
`int`	所代表的参数必须是整数。
`number`	所代表的参数必须是 1 到 255 之间的整数。
`char _chars`	所代表的参数必须是单个字符，并且必须是 *_chars* 参数中指定的字符之一。 例如，定义带有验证语句 `char` *SBC* 的 `MODE` 的命令有效性可检查如下内容：`MODE` 命令的参数是否包含字符 `S`（代表数据流模式）、字符 `B`（代表数据块模式），或字符 `C`（代表压缩模式）。
`date _datefmt`	如果 *_datefmt* 包含 `#`，所代表的参数必须是数字。 如果 *_datefmt* 包含 `C`，所代表的参数必须是字符。 如果 *_datefmt* 包含文字字符串，所代表的参数必须与文字字符串相匹配。
`字符串`	所代表的参数必须是字符串。
`host_port`	所代表的参数必须是有效的主机端口说明符 （如网络工作组发布的 RFC959 《文件传输协议规范》中所规定）。

可以根据需要结合使用上表中的语法来创建参数验证语句，以便在需要验证流量时能够正确验证每个 FTP 命令。

注　如果要在 TYPE 命令中包含复杂的表达式，应将表达式放在空格之间。此外，应将每个操作数放在空格之间。例如，键入字符 `char A | B` ，而非 `char A|B`。

配置服务器级别 FTP 选项

许可证：保护

可以配置多个服务器级别的选项。对于添加的每个 FTP 服务器，可以指定要监控的端口、要验证的命令、命令的默认最大参数长度、特定命令的替代参数长度，以及特定命令的验证语法。还可以选择是否在 FTP 通道上检查字符串格式攻击和 Telnet 命令，以及是否打印每个命令的配置信息。有关服务器级别 FTP 选项的更多信息，请参阅第 27-19 页上的了解服务器级别 FTP 选项。

要配置服务器级别 FTP 选项，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **FTP and Telnet Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 FTP and Telnet Configuration 页面。

页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

提示　有关配置本页中所述其他选项的详细信息，请参阅第 27-17 页上的配置 FTP/Telnet 全局选项、第 27-18 页上的配置 Telnet 选项和第 27-25 页上的配置客户端级别 FTP 选项。

步骤 5　此时您有两种选择：

- 添加新的服务器配置文件。点击页面左侧 **FTP Server** 旁边的添加图标 ( )。系统将显示 Add Target 弹出窗口。在 **Server Address** 字段中为客户端指定一个或多个 IP 地址，然后点击 **OK**。

  可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可指定 1024 个字符，最多可配置 255 个策略（包括默认策略）。有关在 FireSIGHT 系统中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-16 页上的IP 地址约定。

  请注意，为了让基于目标的策略处理流量，您标识的网络必须匹配您在其中配置该策略的网络分析策略处理的网络、区域和 VLAN 或是其子集。有关详情，请参见第 25-2 页上的使用网络分析策略自定义预处理。

新条目将出现在页面左侧的 FTP 服务器列表中，突出显示以表明其已被选定；Configuration 部分会进行更新，以反映所添加的策略的当前配置。

- 修改现有服务器配置文件的设置。点击在页面左侧 **FTP Server** 中添加的配置文件的配置地址，或者点击 **default**。

  所选项目将会突出显示，并且 Configuration 部分会进行更新以显示所选配置文件的当前配置。要删除现有配置文件，请点击要删除的配置文件旁边的删除图标 ( )。

步骤 6　或者，您可以修改 Configuration 页面区域中的以下任何项：

- 修改 **Networks** 字段中列出的地址，并点击页面的任何其他区域。

  突出显示的地址在页面左侧进行更新。

  请注意，不能修改默认配置文件中的 **Network** 设置。默认配置文件适用于网络上未在其他策略中识别出的所有服务器。

- 在 **Ports** 中指定任何应进行 FTP 流量监控的任何端口。端口 21 是已知的 FTP 流量端口。
- 在 **File Get Commands** 字段中更新用于从服务器向客户端传输文件的 FTP 命令。
- 在 **File Put Commands** 字段中更新用于从客户端向服务器传输文件的 FTP 命令。

注　请勿修改 **File Get Commands** 和 **File Put Commands** 字段中的值，除非支持人员要求这样做。

- 要检测除 FTP/Telnet 预处理器在默认情况下检查的命令以外的其他 FTP 命令，请在 **Additional FTP Commands** 中键入命令，命令之间用空格隔开。

  可以根据需要添加尽可能多的其他 FTP 命令。

注　可能需要添加的其他命令包括 `XPWD`、`XCWD`、`XCUP`、`XMKD` 和 `XRMD`。有关这些命令的详细信息，请参阅网络工作组发布的 RFC775 《面向目录的 FTP 命令规范》。

- 在 **Default Max Parameter Length** 字段中指定命令参数的默认最大字节数。
- 要为特定命令检测其他最大参数长度，请点击 **Alternate Max Parameter Length** 旁边的 **Add**。在出现的行的第一个文本框中，指定最大参数长度。在第二个文本框中指定命令，命令之间用空格隔开，在这种情况下，应适用替代最大参数长度。

  可以根据需要添加尽可能多的替代最大参数长度。

- 要检查特定命令的字符串格式攻击，请在 **Check Commands for String Format Attacks** 文本框中指定命令，命令之间用空格隔开。
- 要指定命令的有效格式，请点击 **Command Validity** 旁边的 **Add**。指定要验证的命令，然后键入命令参数的验证语句。有关验证语句语法的详细信息，请参阅第 27-19 页上的了解服务器级别 FTP 选项。
- 要禁用除数据传输通道状态检查之外的所有检查，从而提高 FTP 数据传输的性能，请启用 **Ignore FTP Transfers**。

注　要检查数据传输，必须选择 FTP/Telnet **Stateful Inspection** 全局选项。有关设置全局选项的详细信息，请参阅第 27-16 页上的了解 FTP 和 Telnet 全局选项。

- 要检测何时在 FTP 命令通道上使用 Telnet 命令，请选择 **Detect Telnet Escape Codes within FTP Commands**。
- 在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令，请启用 **Ignore Erase Commands during Normalization**。

步骤 7　或者，修改相关的故障排除选项 （但应仅在支持人员要求的情况下才这样做）；点击 **Troubleshooting Options** 旁边的 **+** 号可展开故障排除选项部分。

步骤 8　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

了解客户端级别 FTP 选项

许可证：保护

可以为 FTP 客户端创建配置文件。在每个配置文件中，可以指定来自客户端的 FTP 响应的最大响应长度。还可以配置解码器是否检测反弹攻击，以及为特定客户端在 FTP 命令通道上使用 Telnet 命令。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

网络

使用此选项可指定 FTP 客户端的一个或多个 IP 地址。

可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。最多可指定 1024 个字符，最多可指定 255 个配置文件 （包括默认配置文件）。有关在 FireSIGHT 系统中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-16 页上的IP 地址约定。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或地址块，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any` （例如， 0.0.0.0/0 或 ::/0）。

另请注意，为了让基于目标的策略处理流量，您标识的网络必须匹配您在其中配置该策略的网络分析策略处理的网络、区域和 VLAN 或是其子集。有关详情，请参见第 25-2 页上的使用网络分析策略自定义预处理。

Max Response Length

使用此选项可指定来自 FTP 客户端的响应字符串的最大长度。

可以启用规则 125:6 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Detect FTP Bounce Attempts

使用此选项可检测 FTP 反弹攻击。

可以启用规则 125:8 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Allow FTP Bounce to

使用此选项可配置包含附加主机以及这些主机上端口的列表，在这些主机上， FTP PORT 命令不应被视为 FTP 反弹攻击。

Detect Telnet Escape Codes within FTP Commands

使用此选项可检测何时在 FTP 命令通道上使用 Telnet 命令。

可以启用规则 125:1 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Ignore Erase Commands During Normalization

如果选择了 **Detect Telnet Escape Codes within FTP Commands**，使用此选项可在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令。此选项的设置应与 FTP 客户端处理 Telnet 擦除命令的方式相匹配。请注意，新 FTP 客户端通常会忽略 Telnet 擦除命令，而旧客户端通常会进行处理。

配置客户端级别 FTP 选项

许可证：保护

可以为 FTP 客户端配置客户端配置文件，以监控来自客户端的 FTP 流量。有关可设置用于监控客户端的选项的更多信息，请参阅第 27-24 页上的了解客户端级别 FTP 选项。有关 Telnet 选项的详细信息，请参阅第 27-18 页上的了解 Telnet 选项。有关其他 FTP 选项的详细信息，请参阅第 27-19 页上的了解服务器级别 FTP 选项和第 27-16 页上的了解 FTP 和 Telnet 全局选项。

要配置客户端级别 FTP 选项，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **FTP and Telnet Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 FTP and Telnet Configuration 页面。

步骤 5　此时您有两种选择：

- 添加新的客户端配置文件。点击页面左侧 **FTP Client** 旁边的添加图标( )。系统将显示 Add Target 弹出窗口。在 **Client Address** 字段中为客户端指定一个或多个 IP 地址，然后点击 **OK**。

  可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可指定 1024 个字符，最多可配置 255 个策略（包括默认策略）。有关在 FireSIGHT 系统中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-16 页上的IP 地址约定。

  请注意，为了让基于目标的策略处理流量，您标识的网络必须匹配您在其中配置该策略的网络分析策略处理的网络、区域和 VLAN 或是其子集。有关详情，请参见第 25-2 页上的使用网络分析策略自定义预处理。

  新条目将出现在页面左侧的 FTP 客户端列表中，突出显示以表明其已被选定；Configuration 部分会进行更新，以反映所添加的策略的当前配置。

- 修改现有客户端配置文件的设置。点击在页面左侧 **FTP Client** 中添加的配置文件的配置地址，或者点击 **default**。

  所选项目将会突出显示，并且 Configuration 部分会进行更新以显示所选配置文件的当前配置。要删除现有配置文件，请点击要删除的配置文件旁边的删除图标 ( )。

步骤 6　或者，您可以修改 Configuration 页面区域中的以下任何项：

- 或者，修改 **Networks** 字段中列出的地址，并点击页面的任何其他区域。

  突出显示的地址在页面左侧进行更新。

请注意，不能修改默认配置文件中的 **Network** 设置。默认配置文件适用于网络上未在其他策略中识别出的所有客户端主机。

- 在 **Max Response Length** 字段中指定来自 FTP 客户端的响应的最大长度 （以字节为单位）。
- 要检测 FTP 反弹攻击，请选择 **Detect FTP Bounce attempts**。

  FTP/Telnet 解码器检测何时发出 FTP PORT 命令以及指定主机与客户端的指定主机不匹配这种情况。
- 要配置包含附加主机和端口的列表 （FTP PORT 命令在这些主机和端口上不应被视为 FTP 反弹攻击），请在 **Allow FTP Bounce to** 字段中指定每个主机（或 CIDR 格式的网络），后跟一个冒号 (:) 和端口或端口范围。要为主机输入端口范围，请使用破折号 (-) 隔开范围内的开始端口和最终端口。可以通过用逗号隔开主机条目来输入多个主机。

  例如，要允许指向端口 21 处的主机 192.168.1.1 的 FTP PORT 命令，以及指向 22 到 1024 之间任一端口处的主机 192.168.1.2 的命令，请键入：

  ```
  192.168.1.1:21, 192.168.1.2:22-1024
  ```

  有关在 FireSIGHT 系统中使用 CIDR 表示法和前缀长度的信息，请参阅第 1-16 页上的 IP 地址约定。

注　要为主机指定多个单独端口，必须为每个端口定义重复主机 IP 地址。例如，要指定 192.168.1.1 上的端口 22 和 25，请键入 `192.168.1.1:22, 192.168.1.1:25`。

- 要检测何时在 FTP 命令通道上使用 Telnet 命令，请选择 **Detect Telnet Escape Codes within FTP Commands**。
- 在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令，请选择 **Ignore Erase Commands During Normalization**。

步骤 7　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

解码 HTTP 流量

许可证：保护

HTTP 检查预处理器负责以下工作：

- 解码和规范化发送到网络上网络服务器的 HTTP 请求以及来自该服务器的 HTTP 响应
- 将发送到网络服务器的消息分成 URI、非 cookie 报头、 cookie 报头、方法和消息正文等组成部分，以提高与 HTTP 相关的入侵规则的性能
- 将从网络服务器接收到的消息分成状态代码、状态消息、非 set-cookie 报头、cookie 报头和响应正文等组成部分，以提高与 HTTP 相关的入侵规则的性能
- 检测可能的 URI 编码攻击
- 使规范化数据可用于附加规则处理

HTTP 流量可以各种格式进行编码，因此规则很难适当地进行检查。 HTTP 检查可解码 14 种编码，从而确保 HTTP 流量获得可能的最佳检查。

可以在一个服务器上或者对服务器列表全局配置 HTTP 检查选项。

使用 HTTP 检查预处理器时，请注意以下几点：

- 预处理器引擎*无状态地*执行 HTTP 规范化。也就是说，它会逐个数据包进行 HTTP 字符串规范化，并且只能处理已由 TCP 数据流预处理器重组的 HTTP 字符串。
- 必须启用生成器 ID (GID) 为 119 的 HTTP 预处理器规则才可生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

有关详细信息，请参阅以下各节：

选择全局 HTTP 规范化选项

许可证：保护

为 HTTP 检查预处理器的全局 HTTP 选项用于控制预处理器的工作方式。如果由未指定为网络服务器的端口接收 HTTP 流量，可使用这些选项启用或禁用 HTTP 规范化。

请注意：

- 如果启用 **Unlimited Decompression**，提交修改时， **Maximum Compressed Data Depth** 和 **Maximum Decompressed Data Depth** 选项将会自动设置为 65535。有关详情，请参见第 27-28 页上的选择服务器级别 HTTP 规范化选项。
- 如果在与访问控制策略的默认操作相关的入侵策略以及与访问控制规则相关的入侵策略中， **Maximum Compressed Data Depth** 和 **Maximum Decompressed Data Depth** 选项的值不同，将会使用最大值。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

Detect Anomalous HTTP Servers

检测发送到未指定为网络服务器的端口或由其接收的 HTTP 流量。

注　如果启用该选项，请确保在 HTTP Configuration 页面上的服务器配置文件中列出接收 HTTP 流量的所有端口。如果不这样做，并且已启用此选项以及随附的预处理器规则，则发送至该服务器和来自该服务器的正常流量均会生成事件。默认的服务器配置文件包含所有通常用于 HTTP 流量的端口，但如果修改了该配置文件，可能需要将这些端口添加到另一个配置文件中，以防止生成事件。

可以启用规则 120:1 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Detect HTTP Proxy Servers

检测使用未由 **Allow HTTP Proxy Use** 选项定义的代理服务器的 HTTP 流量。

可以启用规则 119:17 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Maximum Compressed Data Depth

当启用 **Inspect Compressed Data** （或者 **Decompress SWF File (LZMA)**、 **Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）时，可设置要解压的压缩数据的最大大小。可指定 1 到 65535 字节。

Maximum Decompressed Data Depth

当启用 **Inspect Compressed Data** （或者 **Decompress SWF File (LZMA)**、 **Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）时，可设置规范化的解压数据的最大大小。可指定 1 到 65535 字节。

配置全局 HTTP 配置选项

许可证：保护

可以配置对流向非标准端口的 HTTP 流量以及使用代理服务器的 HTTP 流量的检测。有关全局 HTTP 配置选项的详细信息，请参阅第 27-27 页上的选择全局 HTTP 规范化选项。

要配置全局 HTTP 配置选项，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **HTTP Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 HTTP Configuration 页面。

步骤 5　可以修改第 27-27 页上的选择全局 HTTP 规范化选项中所述的任何全局选项。

步骤 6　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

选择服务器级别 HTTP 规范化选项

许可证：保护

可以为监控的每个服务器、全局地为所有服务器或者为服务器列表设置服务器级别选项。此外，可以根据环境需求，使用预定义的服务器配置文件来设置这些选项，或者单独设置这些选项。可以使用这些选项或设置这些选项的其中一个默认配置文件来指定要规范化其流量的 HTTP 服务器端口、要规范化的服务器响应负载以及要规范化的编码的类型。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

网络

使用此选项可指定一个或多个服务器的 IP 地址。可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。

配置文件总数（包括默认配置文件）上限为 255 个，此外，最多可在 HTTP 服务器列表中包含 496 个字符（约 26 个条目），为所有服务器配置文件总共最多可指定 256 个地址条目。有关在 FireSIGHT 系统中使用 IPv4 CIDR 记法和 IPv6 前缀长度的详细信息，请参阅第 1-16 页上的 IP 地址约定。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如， 0.0.0.0/0 或 ::/0）。

另请注意，为了让基于目标的策略处理流量，您标识的网络必须匹配您在其中配置该策略的网络分析策略处理的网络、区域和 VLAN 或是其子集。有关详情，请参见第 25-2 页上的使用网络分析策略自定义预处理。

端口

预处理器引擎会对其 HTTP 流量进行规范化的端口。使用逗号分隔多个端口号。

Oversize Dir Length

检测长度超过指定值的 URL 目录。

可以启用规则 119:15 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Client Flow Depth

为要在 **Ports** 中定义的客户端 HTTP 流量中的原始 HTTP 数据包（包括报头和负载数据）中检查的规则指定字节数。如果规则中的 HTTP 内容规则选项检查请求消息的特定部分，客户端流量深度不适用。有关详情，请参见第 36-21 页上的 HTTP 内容选项。

可指定 -1 到 1460 之间的值。思科建议将客户端流量深度设置为最大值。可指定以下任意值：

- 1 到 1460，检查第一个数据包中的指定字节数。如果第一个数据包包含的字节数小于指定值，将会检查整个数据包。请注意，指定值适用于分段和重组的数据包。

  另请注意，值 300 通常表示许多客户端请求报头末尾出现的大尺寸 HTTP Cookie 无需检查。
- 0 将会检查所有客户端流量，包括会话中的多个数据包，在必要时可超出 1460 字节这个限制。请注意，此值可能会影响性能。
- -1 将会忽略所有客户端流量。

Server Flow Depth

为要在 **Ports** 中指定的服务器端 HTTP 流量中的原始 HTTP 数据包中检查的规则指定字节数。**Inspect HTTP Responses** 处于禁用状态时，会检查原始报头和负载；**Inspect HTTP Response** 处于启用状态时，仅检查原始响应正文。

Server Flow Depth 为要在 **Ports** 中定义的服务器端 HTTP 流量中检查的规则指定会话中原始服务器响应数据的字节数。可以使用此选项来平衡 HTTP 服务器响应数据的性能和检查水平。如果规则中的 HTTP 内容规则选项检查响应消息的特定部分，服务器流量深度不适用。有关详情，请参见第 36-21 页上的 HTTP 内容选项。

不同于客户端流量深度，服务器流量深度为要检查的规则指定每个 HTTP 响应而非每个 HTTP 请求数据包的字节数。

可指定 -1 到 65535 之间的值。思科建议将服务器流量深度设置为最大值。可以指定以下任何内容：

- 1 到 65535：

  当 **Inspect HTTP Responses** 处于**启用**状态时，仅检查原始 HTTP 响应正文，不会检查非原始 HTTP 报头；当 **Inspect Compressed Data** 处于启用状态时，还会同时检查解压缩数据。

  当 **Inspect HTTP Responses** 处于**禁用**状态时，会检查原始数据包报头和负载。

如果会话包含的响应字节小于指定值，规则将会根据需要在多个数据包中彻底检查给定会话中的所有响应数据包。如果会话包含的响应字节大于指定值，规则将会根据需要在多个数据包中仅检查该会话中的指定字节数。

请注意，流量深度值小可能会导致针对 **Ports** 中定义的服务器端流量的规则出现漏报。大多数这些规则针对的是，可能处于非报头数据的大约前 100 字节中的 HTTP 报头或内容。报头长度通常少于 300 字节，但报头大小可以不同。

另请注意，指定值适用于分段和重组的数据包。

– 0 将会为 **Ports** 中定义的所有 HTTP 服务器端流量检查整个数据包 （包括超过 65535 字节的会话中的响应数据）。

请注意，此值可能会影响性能。

– -1：

当 **Inspect HTTP Responses** 处于**启用**状态时，仅检查原始 HTTP 响应正文，不会检查原始 HTTP 响应正文。

当 **Inspect HTTP Responses** 处于**禁用**状态时，会忽略在 **Ports** 中定义的所有服务器端流量。

Maximum Header Length

检测 HTTP 请求中长度超过指定最大字节数的报头字段；如果启用了 **Inspect HTTP Responses**，还会对 HTTP 响应执行此项检查。值 0 将会禁用此选项。指定 1 到 65535 之间的任何值将会启用此选项。

可以启用规则 119:19 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Maximum Number of Headers

检测 HTTP 请求中的报头数量超过此设置的情况。指定 1 到 1024 之间的任何值将会启用此选项。

可以启用规则 119:20 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Maximum Number of Spaces

当 HTTP 请求中折线中的空格数量等于或超过此设置时，进行检测。值 0 将会禁用此选项。指定 1 到 65535 之间的任何值将会启用此选项。

可以启用规则 119:26 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

HTTP Client Body Extraction Depth

指定从 HTTP 客户端请求的消息正文提取的字节数。通过选择 `content` 或 `protected_content` 关键字 **HTTP Client Body** 选项，可以使用入侵规则检查提取的数据。有关详情，请参见第 36-21 页上的 HTTP 内容选项。

可指定 -1 到 65495 之间的值。指定 -1 将会忽略客户端正文。指定 0 将会提取整个客户端正文。请注意，指定特定字节数进行提取可提高系统性能。另请注意，要使 **HTTP Client Body** 选项在入侵规则中起作用，必须为此选项指定一个 0 到 65495 之间的值。

Small Chunk Size

指定被认为是小数据块的数据块可包含的最大字节数。可指定 1 到 255 之间的值。值 0 将会禁用对异常连续小片段的检测。有关详细信息，请参阅 **Consecutive Small Chunks** 选项。

Consecutive Small Chunks

指定在使用分块传输编码的客户端流量或服务器流量中，代表异常大数量的连续小数据块的数量。 **Small Chunk Size** 选项指定小数据块的最大大小。

例如，将 **Small Chunk Size** 设置为 10 并将 **Consecutive Small Chunks** 设置为 5，可检测包含 10 个或更少字节的 5 个连续数据块。

对于客户端流量和服务器流量，可分别启用预处理器规则 119:27 和 120:7 针对过多小数据块这种情况触发事件。如果 **Small Chunk Size** 已启用且此选项设置为 0 或 1，启用这些规则将会对每个指定大小或更小的数据块触发事件。有关详情，请参见第 32-18 页上的设置规则状态。

HTTP Methods

指定除系统预期会在流量中遇到的 GET 和 POST 以外的 HTTP 请求方法。使用逗号隔开多个值。

入侵规则结合使用 `content` 或 `protected_content` 关键字及其 **HTTP Method** 参数来搜索 HTTP 方法中的内容。请参阅第 36-21 页上的 HTTP 内容选项。如果在流量中遇到 GET、POST 或为此选项配置的方法以外的方法，可以启用规则 119:31 生成事件。

No Alerts

当随附的预处理器规则处于启用状态时禁用入侵事件。

注　此选项**不**会禁用 HTTP 标准文本规则和共享对象规则。

Normalize HTTP Headers

当 **Inspect HTTP Responses** 处于启用状态时，启用请求和响应报头中非 cookie 数据的规范化。如果**未**启用 **Inspect HTTP Responses**，启用请求和响应报头中 HTTP 报头（包括 cookie）的规范化。

Inspect HTTP Cookies

允许从 HTTP 请求提取 cookie。如果 **Inspect HTTP Responses** 已启用，还允许从响应报头提取 set-cookie 数据。当不需要提取 cookie 时，禁用此选项可提高性能。

请注意，`Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

Normalize Cookies in HTTP headers

启用 HTTP 请求报头中 cookie 的规范化。当 **Inspect HTTP Responses** 处于启用状态时，还会启用响应报头中 set-cookie 数据的规范化。选择了 **Inspect HTTP Cookies** 之后才能选择此选项。

Allow HTTP Proxy Use

允许将受监控的网络服务器用作 HTTP 代理。此选项仅用于检查 HTTP 请求。

Inspect URI Only

仅检查规范化 HTTP 请求数据包的 URI 部分。

Inspect HTTP Responses

启用对 HTTP 响应的延展检查，从而使预处理器不仅会对 HTTP 请求消息进行解码和规范化，还会提取响应字段以供规则引擎进行检查。启用此选项后，系统会提取响应报头、正文、状态代码等；如果还启用了 **Inspect HTTP Cookies**，系统还会提取 set-cookie 数据。有关详细信息，请参阅第 36-21 页上的 HTTP 内容选项、第 36-87 页上的生成关于 HTTP 编码类型和位置的事件和第 36-90 页上的指向特定负载类型。

可以启用规则 120:2 和 120:3 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Normalize UTF Encodings to UTF-8

如果启用了 **Inspect HTTP Responses**，此选项检测 HTTP 响应中的 UTF-16LE、 UTF-16BE、 UTF-32LE 和 UTF32-BE 编码，并将其规范化为 UTF-8。

可以启用规则 120:4 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Inspect Compressed Data

当 **Inspect HTTP Responses** 已启用时，此选项启用 HTTP 响应正文中的 gzip 和兼容 deflate 的压缩数据的解压，以及对规范化解压缩数据的检查。系统将检查分块和非分块 HTTP 响应数据。系统会根据需要逐一检查多个数据包中的解压缩数据；也就是说，系统不会将来自不同数据包的解压缩数据合并来进行检查。当达到 **Maximum Compressed Data Depth** 或 **Maximum Decompressed Data Depth** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到 **Server Flow Depth** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了 **Unlimited Decompression**。可以使用 `file_data` 规则关键字检查解压缩数据；有关详细信息，请参阅第 36-90 页上的指向特定负载类型。

Unlimited Decompression

当启用 **Inspect Compressed Data**（或者 **Decompress SWF File (LZMA)**、**Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）时，会覆盖跨多个数据包的 **Maximum Decompressed Data Depth**；即，此选项会启用跨多个数据包的无限解压缩。请注意，启用此选项不会影响单个数据包中的 **Maximum Compressed Data Depth** 或 **Maximum Decompressed Data Depth**。另请注意，如果启用此选项，提交修改时 **Maximum Compressed Data Depth** 和 **Maximum Decompressed Data Depth** 将会设置为 65535。请参阅第 27-27 页上的选择全局 HTTP 规范化选项。

Normalize Javascript

当 **Inspect HTTP Responses** 已启用时，此选项启用对 HTTP 响应正文中 Javascript 的检测和规范化。预处理器会对模糊 JavaScript 数据 （例如， unescape 函数、 decodeURI 函数和 String.fromCharCode 方法）进行规范化。预处理器会对 unescape、 decodeURI 和 decodeURIComponent 函数中的以下编码进行规范化：

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

预处理器检测连续空格，并将其规范化为一个空格。此选项处于启用状态时，配置字段允许您指定模糊 Javascript 数据中允许的最大连续空格数量。可输入 1 到 65535 之间的值。值 0 将会禁止生成事件，不管与该字段相关的预处理器规则 (120:10) 是否启用。

预处理器还会对 Javascript 加号 (+) 运算符进行规范化，并使用该运算符连接字符串。

可以使用 `file_data` 关键字使入侵规则指向规范化的 Javascript 数据。有关详情，请参见第 36-90 页上的指向特定负载类型。

可以启用规则 120:9、 120:10 和 120:11 为此选项生成事件，如下所示：

表 27-6　　规范化 Javascript 选项规则

规则	会触发事件的情况
120:9	预处理器内的模糊级别大于或等于 2。

表 27-6　规范化 Javascript 选项规则 （续）

规则	会触发事件的情况
120:10	Javascript 模糊数据中的连续空格数量大于或等于为允许的最大连续空格数量配置的值。
120:11	经转义或编码的数据包含多于一种类型的编码。

有关详情，请参见第 32-18 页上的设置规则状态。

解压缩 SWF 文件 (LZMA) 和解压缩 SWF 文件 (Deflate)

当启用 **HTTP Inspect Responses** 时，这些选项会解压缩位于 HTTP 请求的 HTTP 响应正文内的文件的压缩部分。

注　您**只能**解压缩在 HTTP GET 响应中找到的文件的压缩部分。

- **Decompress SWF File (LZMA)** 可解压缩 Adobe ShockWave Flash (`.swf`) 文件的 LZMA 兼容压缩部分
- **Decompress SWF File (Deflate)** 可解压缩 Adobe ShockWave Flash (`.swf`) 文件的 Deflate 兼容压缩部分

当达到 **Maximum Compressed Data Depth** 或 **Maximum Decompressed Data Depth** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到 **Server Flow Depth** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了 **Unlimited Decompression**。可以使用 `file_data` 规则关键字检查解压缩数据；有关详细信息，请参阅第 36-90 页上的指向特定负载类型。

可以启用规则 120:12 和 120:13 为此选项生成事件，如下所述：

表 27-7　解压缩 SWF 文件选项规则

规则	会触发事件的情况
120:12	deflate 文件解压缩失败。
120:13	LZMA 文件解压缩失败。

解压缩 PDF 文件 (Deflate)

当启用 **HTTP Inspect Responses** 时，**Decompress PDF File (Deflate)** 会解压缩位于 HTTP 请求的 HTTP 响应正文内的可移植文件格式 (`.pdf`) 文件的 deflate 兼容压缩部分。系统只能使用 `/FlateDecode` 流过滤器解压缩 PDF 文件。其他流过滤器 （包括 `/FlateDecode /FlateDecode` ）不受支持。

注　您**只能**解压缩在 HTTP GET 响应中找到的文件的压缩部分。

当达到 **Maximum Compressed Data Depth** 或 **Maximum Decompressed Data Depth** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到 **Server Flow Depth** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了 **Unlimited Decompression**。可以使用 `file_data` 规则关键字检查解压缩数据；有关详细信息，请参阅第 36-90 页上的指向特定负载类型。

您可以启用规则 120:14、 120:15、 120:16 和 120:17 来生成此选项的事件，如下所述：

表 27-8　　解压缩 PDF 文件 (Deflate) 选项规则

规则	会触发事件的情况
120:14	文件解压缩失败。
120:15	由于一种不支持的压缩类型，导致文件解压缩失败。
120:16	由于一种不支持的 PDF 流过滤器，导致文件解压缩失败。
120:17	文件解析失败。

Extract Original Client IP Address

允许从 X-Forwarded-For (XFF)、True-Client-IP 或自定义 HTTP 报头提取原始客户端 IP 地址。可以在入侵事件表视图中显示提取的原始客户端 IP 地址。有关详情，请参见第 41-8 页上的了解入侵事件。

可以启用规则 119:23、 119:29 和 119:30 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

XFF 报头优先级

当启用 **Extract Original Client IP Address** 时，指定系统处理原始客户端 IP HTTP 报头的顺序。如果您预期在受监控网络上遇到 X-Forwarded-For (XFF) 或 True-Client-IP 之外的原始客户端 IP 报头，则可以点击 **Add** 将其他报头名称添加到优先级列表。然后，可以使用每个报头类型旁的向上和向下箭头图标调整其优先级。请注意，如果在 HTTP 请求中出现多个 XFF 报头，则系统仅处理优先级最高的报头。

Log URI

允许从 HTTP 请求数据包提取原始 URI （如果有），并将该 URI 与为会话生成的所有入侵事件相关联。

启用此选项后，可以在入侵事件表视图的 HTTP URI 列中显示提取的 URI 的前 50 个字符。可以在数据包视图中显示完整的 URI （最多 2048 字节）。有关详细信息，请参阅第 41-8 页上的了解入侵事件和第 41-20 页上的查看事件信息。

Log Hostname

允许从 HTTP 请求主机报头中提取主机名 （如果有），并将该主机名与为会话生成的所有入侵事件相关联。如果存在多个主机报头，将会从第一个报头提取主机名。

启用此选项后，可以在入侵事件表视图的 HTTP Hostname 列中显示提取的主机名的前 50 个字符。可以在数据包视图中显示完整的主机名 （最多 256 字节）。有关详细信息，请参阅第 41-8 页上的了解入侵事件和第 41-20 页上的查看事件信息。

可以启用规则 119:25 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

请注意，在启用了预处理器和规则 119:24 的情况下，如果在 HTTP 请求中检测到多个主机报头，预处理器将会生成入侵事件，不管此选项的设置如何。有关详情，请参见第 27-38 页上的启用其他 HTTP 检查预处理器规则。

简档

指定为 HTTP 流量规范化的编码的类型。系统提供了一个适用于大多数服务器的默认配置文件、适用于 Apache 服务器和 IIS 服务器的若干默认配置文件以及自定义默认设置，您可以对这些设置进行自定义，以满足受监控流量的需求。有关详情，请参见第 27-35 页上的选择服务器级别的 HTTP 规范化编码选项。

选择服务器级别的 HTTP 规范化编码选项

许可证：保护

可以选择服务器级别的 HTTP 规范化选项来指定为 HTTP 流量进行规范化的编码类型，并使系统针对包含指定类型编码的流量生成事件。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

ASCII Encoding

对编码的 ASCII 字符进行解码，并指定规则引擎是否生成关于 ASCII 编码 URI 的事件。

可以启用规则 119:1 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

UTF-8 Encoding

对 URI 中的标准 UTF-8 Unicode 序列进行解码。

可以启用规则 119:6 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Microsoft %U Encoding

对 IIS %u 编码方案进行解码（该编码方案使用 %u，%u 后紧跟着 4 个字符；其中的 4 个字符为十六进制编码的值，并与 IIS Unicode 代码点相关）。

提示 合法的客户端很少使用 %u 编码，因此，思科建议对使用 %u 编码的 HTTP 流量进行解码。

可以启用规则 119:3 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Bare Byte UTF-8 Encoding

对裸字节编码进行解码 （这种解码方法使用非 ASCII 字符作为解码 UTF-8 值时的有效值）。

提示 裸字节编码允许用户模拟 IIS 服务器和正确解释非编码标准。思科建议启用此选项，因为合法的客户端不以这种方式编码 UTF-8。

可以启用规则 119:4 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Microsoft IIS Encoding

使用 Unicode 代码点映射进行解码。

提示 思科建议启用此选项，因为它主要出现在攻击和躲避尝试中。

可以启用规则 119:7 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Double Encoding

通过在每个进行解码的请求 URI 中形成两条通道，解码 IIS 双编码流量。思科建议启用此选项，因为它通常只存在于攻击情况中。

可以启用规则 119:2 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Multi-Slash Obfuscation

将连续的多个斜杠规范化为一个斜杠。

可以启用规则 119:8 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

IIS Backslash Obfuscation

将反斜杠规范化为正斜杠。

可以启用规则 119:9 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Directory Traversal

对目录遍历和自引用目录进行规范化。如果启用随附的预处理器规则来生成关于此类型流量的事件，可能会产生误报，因为有些网站使用目录遍历来引用文件。

可以启用规则 119:10 和 119:11 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Tab Obfuscation

规范化有关对空格分隔符使用制表符的非 RFC 标准。Apache 及其他非 IIS网络服务器在 URL 中使用制表符 (0x09) 作为分隔符。

注 无论此选项的配置如何，如果制表符前有空格字符 (0x20)， HTTP 检查预处理器都将制表符看作空格。

可以启用规则 119:12 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Invalid RFC Delimiter

规范化 URI 数据中的换行符 (\n)。

可以启用规则 119:13 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Webroot Directory Traversal

检测穿过 URL 中初始目录的目录遍历。

可以启用规则 119:18 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Tab URI Delimiter

将制表符 (0x09) 用作 URI 的分隔符。 Apache、新版本的 IIS 以及其他一些网络服务器使用制表符作为 URL 的分隔符。

注 无论此选项的配置如何，如果制表符前有空格字符 (0x20)， HTTP 检查预处理器都将制表符看作空格。

Non-RFC characters

检测在相应字段中添加的并出现在传入或传出 URI 数据中的非 RFC 字符列表。修改该字段时，请使用表示字节字符的十六进制格式。如果要配置此选项，请谨慎设置它的值。使用极常见的字符可能会生成大量事件。

可以启用规则 119:14 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Max Chunk Encoding Size

检测 URI 数据中异常大的数据块的大小。

可以启用规则 119:16 和 119:22 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Disable Pipeline Decoding

禁止对管道化请求进行 HTTP 解码。禁用此选项可提高性能，因为不会对管道中等待的 HTTP 请求进行解码和分析，且只会使用通用模式匹配对这些请求进行检查。

Non-Strict URI Parsing

允许非严格的 URI 解析。应仅在接受 "GET /index.html abc xo qr \n" 格式的非标准 URI 的服务器上使用此选项。此选项处于启用状态时，解码器会假设 URI 在第一和第二空格之间，即使第二个空格后没有有效的 HTTP 标识符。

Extended ASCII Encoding

允许对 HTTP 请求 URI 中的扩展 ASCII 字符进行解析。请注意，此选项仅适用于自定义的服务器配置文件，不适用于为 Apache、 IIS 或所有服务器提供的默认配置文件。

配置 HTTP 服务器选项

许可证：保护

可按照以下步骤配置 HTTP 服务器选项。有关 HTTP 服务器选项的详细信息，请参阅第 27-28 页上的选择服务器级别 HTTP 规范化选项和第 27-35 页上的选择服务器级别的 HTTP 规范化编码选项。

要配置服务器级别的 HTTP 配置选项，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **HTTP Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 HTTP Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　此时您有两种选择：

- 添加新的服务器配置文件。点击页面左侧 **Servers** 旁边的添加图标 ( )。系统将显示 Add Target 弹出窗口。在 **Server Address** 字段中为客户端指定一个或多个 IP 地址，然后点击 **OK**。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可在列表中包含 496 个字符，为所有服务器配置文件总共最多可指定 256 个地址条目，总共最多可创建 255 个配置文件 （包括默认配置文件）。有关在 FireSIGHT 系统中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-16 页上的IP 地址约定。

请注意，为了让基于目标的策略处理流量，您标识的网络必须匹配您在其中配置该策略的网络分析策略处理的网络、区域和 VLAN 或是其子集。有关详情，请参见第 25-2 页上的使用网络分析策略自定义预处理。

新条目将出现在页面左侧的服务器列表中，突出显示以表明其已被选定；Configuration 部分会进行更新，以反映所添加的策略的当前配置。

- 修改现有配置文件的设置。点击在页面左侧 **Servers** 中添加的配置文件的配置地址，或者点击 **default**。

  所选项目将会突出显示，并且 Configuration 部分会进行更新以显示所选配置文件的当前配置。要删除现有配置文件，请点击要删除的配置文件旁边的删除图标 ( )。

步骤 6　或者，修改 **Networks** 字段中列出的地址，并点击页面的任何其他区域。

突出显示的地址在页面左侧进行更新。

请注意，不能修改默认配置文件中的 **Network** 设置。默认配置文件适用于网络上未在其他策略中识别出的所有服务器。

步骤 7　在 **Ports** 字段中，列出要使用 HTTP 检查对其进行流量检查的端口。使用逗号分隔多个端口。

步骤 8　可以修改第 27-28 页上的选择服务器级别 HTTP 规范化选项中所述的任何其他选项。

步骤 9　如下所述选择服务器配置文件：

- 选择 **Custom** 将会创建自己的服务器配置文件 （有关详细信息，请参阅第 27-35 页上的选择服务器级别的 HTTP 规范化编码选项）。
- 选择 **All** 将会使用适用于所有服务器的标准默认配置文件。
- 选择 **IIS** 将会使用默认的 IIS 配置文件。
- 选择 **Apache** 将会使用默认的 Apache 配置文件。

步骤 10　如果选择 **Custom**，将出现自定义选项。

步骤 11　在配置文件中对要使用的 HTTP 解码选项进行配置。

有关可用规范化选项的详细消息，请参阅第 27-28 页上的选择服务器级别 HTTP 规范化选项。

步骤 12　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

启用其他 HTTP 检查预处理器规则

许可证：保护

可以启用下表的 **Preprocessor Rule GID:SID** 列中的规则，为与特定配置选项无关的 HTTP 检查预处理器规则生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

表 27-9　其他 HTTP 检查预处理器规则

预处理器规则 GID:SID	说明
120:5	如果在 HTTP 响应流量中遇到 UTF-7 编码，将会生成事件；UTF-7 应仅在需要 7 位奇偶校验的情况下出现，例如， SMTP 流量。
119:21	如果 HTTP 请求报头包含多于一个 `content-length` 字段，将会生成事件。
119:24	如果 HTTP 请求包含多于一个主机报头，将会生成事件。
119:28 120:8	如果启用，这些规则不生成事件。
119:32	如果在流量中遇到 HTTP 0.9，将会生成事件。请注意，还必须启用 TCP Stream Configuration。请参阅第 29-18 页上的使用 TCP 数据流预处理。
119:33	如果 HTTP URI 包含非转义空格，将会生成事件。
119:34	如果 TCP 连接包含 24 个或更多管道化 HTTP 请求，将会生成事件。

使用 Sun RPC 预处理器

许可证：保护

RPC （远程过程调用）规范化采用分片 RPC 记录，并将这些记录规范化为单个记录，以便规则引擎可以检查完整的记录。例如，攻击者可能会试图发现 RPC `admind` 运行所在的端口。某些 UNIX 主机使用 RPC `admind` 执行远程分布式系统任务。如果主机执行弱身份验证，恶意用户可能会控制远程管理。 Snort ID (SID) 为 575 的标准文本规则 （生成器 ID：1）会搜索特定位置中的内容，并识别不适当的 `portmap GETPORT` 请求，以此来检测这种攻击。

端口

指定要规范化其流量的端口。可在此界面列出多个端口，端口之间用逗号分隔。典型的 RPC 端口为 111 和 32771。如果网络将 RPC 流量发送到其他端口，可考虑添加这些端口。

Detect fragmented RPC records

检测 RPC 分片记录。

可以启用规则 106:1 和 106:5 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Detect multiple records in one packet

在每个数据包 （或重组数据包）中检测多于一个 RPC 请求。

可以启用规则 106:2 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Detect fragmented record sums which exceed one fragment

检测超过当前数据包长度的重组分片记录长度。

可以启用规则 106:3 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Detect single fragment records which exceed the size of one packet

检测部分记录。

可以启用规则 106:4 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

配置 Sun RPC 预处理器

许可证：保护

可以按照以下步骤配置 Sun RPC 预处理器。有关 Sun RPC 预处理器的配置选项的详细消息，请参阅第 27-39 页上的使用 Sun RPC 预处理器。

要配置 Sun RPC 预处理器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **Sun RPC Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Sun RPC Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　在 **Ports** 字段中，键入要解码其 RPC 流量的端口号。使用逗号分隔多个端口。

步骤 6　可以在 Sun RPC 配置页面上选择或清除以下任何检测选项：

- **Detect fragmented RPC records**
- **Detect multiple records in one packet**
- **Detect fragmented record sums which exceed one packet**
- **Detect single fragment records which exceed the size of one packet**

步骤 7　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

解码会话发起协议

许可证：保护

会话初始协议 (SIP) 为客户端应用 （例如网络电话、多媒体会议、即时消息、网络游戏和文件传输）的一个或多个用户提供一个或多个会话的呼叫建立、修改和取消。每个 SIP 请求中的 *method* 字段识别请求的目的，请求 URI 则指定发送请求的目的地。每个 SIP 响应中的状态代码指明请求操作的结果。

使用 SIP 建立呼叫后，实时传输协议 (RTP) 负责随后的音频和视频通信；会话的此部分有时又称为呼叫通道、数据通道或音频/视频数据通道。对于数据通道参数协商、会话公告和会话邀请，RTP 在 SIP 消息正文中使用会话描述协议 (SDP)。

SIP 预处理器负责：

- 解码和分析 SIP 2.0 流量
- 提取包括 SDP 数据 （如果有）在内的 SIP 报头和消息正文，并将提取的数据传递给规则引擎，以进行进一步检查
- 在检测到以下条件并且相应的预处理器规则已启用的情况下，将会生成事件：SIP 数据包中存在异常和已知漏洞；调用序列乱序和无效。
- 或者，忽略呼叫通道

预处理器会根据在 SDP 消息中识别出的端口来识别 RTP 通道 （该消息嵌入在 SIP 消息正文中），但预处理器不提供 RTP 协议检查。

使用 SIP 预处理器时，请注意以下几点：

- UDP 通常传输 SIP 支持的媒体会话。 UDP 数据流预处理为 SIP 预处理器提供 SIP 会话跟踪。
- SIP 规则关键字允许您指向 SIP 数据包报头或消息正文，并限制为对特定 SIP 方法或状态代码进行数据包检测。有关详细信息，请参阅第 36-56 页上的SIP 关键字。
- 如果启用了预处理器，在向规则引擎发送提取的数据之前，预处理器不会生成事件，除非还启用了随附的带有生成器 ID (GID) 140 的规则。有关详情，请参见第 32-18 页上的设置规则状态。

有关详细信息，请参阅以下各节：

- 第 27-41 页上的选择 SIP 预处理器选项
- 第 27-43 页上的配置 SIP 预处理器
- 第 27-43 页上的启用其他 SIP 预处理器规则

选择 SIP 预处理器选项

许可证：保护

以下列表说明可修改的 SIP 预处理器选项。

对于 **Maximum Request URI Length**、**Maximum Call ID Length**、**Maximum Request Name Length**、**Maximum From Length**、 **Maximum To Length**、 **Maximum Via Length**、 **Maximum Contact Length** 和 **Maximum Content Length** 选项，可指定 1 到 65535 字节，或者指定 0 以禁止生成事件，不管相关规则是否已启用。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

端口

指定用于检查 SIP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Methods to Check

指定 SIP 检测方法。可以指定以下当前定义的任何 SIP 方法：

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

方法不区分大小写。方法名称可以包含字母字符、数字和下划线字符。不得使用其他特殊字符。使用逗号隔开多种方法。

由于将来可能会定义新的 SIP 方法，因此，配置可以包含当前未定义的字母串。系统最多支持 32 种方法，包括 21 种当前定义的方法和 11 种其他方法。系统将忽略您可能配置的任何未定义的方法。

请注意，除了为此选项指定的方法外，总共 32 种方法中包括入侵规则中使用 `sip_method` 关键字的指定方法。有关详情，请参见第 36-57 页上的 sip_method。

Maximum Dialogs within a Session

指定数据流会话中允许的最大对话数量。如果创建了多于此数量的对话，将会丢弃最早的对话，直至对话数量不超过指定的最大数量；如果启用了规则 140:27，还将触发事件。

可指定 1 到 4194303 之间的整数。

Maximum Request URI Length

指定 Request-URI 报头字段中允许的最大字节数。如果启用了规则 140:3，长度大于此设置的 URI 将会触发事件。请求 URI 字段指明请求的目标路径或目标页面。

Maximum Call ID Length

指定请求或响应 Call-ID 报头字段中允许的最大字节数。如果启用了规则 140:5，长度大于此设置的 Call-ID 字段将会触发事件。 Call-ID 字段唯一地识别请求和响应中的 SIP 会话。

Maximum Request Name Length

指定请求名称中允许的最大字节数 （该名称是 CSeq 事务标识符中指定的方法的名称）。如果启用了规则 140:7，长度大于此设置的请求名称将会触发事件。

Maximum From Length

指定请求或响应 From 报头字段中允许的最大字节数。如果启用了规则 140:9，长度大于此设置的 From 字段将会触发事件。 From 字段识别消息发起方。

Maximum To Length

指定请求或响应 To 报头字段中允许的最大字节数。如果启用了规则 140:11，长度大于此设置的 To 字段将会触发事件。 To 字段识别消息收件人。

Maximum Via Length

指定请求或响应 Via 报头字段中允许的最大字节数。如果启用了规则 140:13，长度大于此设置的 Via 字段将会触发事件。 Via 字段提供请求的路径，并在响应中提供回执信息。

Maximum Contact Length

指定请求或响应 Contact 报头字段中允许的最大字节数。如果启用了规则 140:15，长度大于此设置的 Contact 字段将会触发事件。 Contact 字段提供用以指定与后续消息进行联系的位置的 URI。

Maximum Content Length

指定在请求或响应消息正文的内容中允许的最大字节数。如果启用了规则 140:16，长度大于此设置的内容将会触发事件。

Ignore Audio/Video Data Channel

启用和禁用数据通道流量检查。请注意，如果启用了此选项，预处理器会继续检查其他非数据通道 SIP 流量。

配置 SIP 预处理器

许可证：保护

可按照以下步骤配置 SIP 预处理器。

要配置 SIP 预处理器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **SIP Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 SIP Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　可以修改第 27-41 页上的选择 SIP 预处理器选项中所述的任何选项。

步骤 6　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

启用其他 SIP 预处理器规则

许可证：保护

下表中的 SIP 预处理器规则与特定配置选项无关。与其他 SIP 预处理器规则一样，如果要使这些规则生成事件，必须启用它们。有关启用规则的详细信息，请参阅第 32-18 页上的设置规则状态。

表 27-10　其他 SIP 预处理器规则

预处理器规则 GID:SID	说明
140:1	如果预处理器正在监控系统允许的最大 SIP 会话数量，将会生成事件。
140:2	如果必填的 Request_URI 字段在 SIP 请求中为空，将会生成事件。
140:4	如果 Call-ID 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:6	如果 SIP 请求或响应 CSeq 字段中的序列号值不是小于 231 的 32 位无符号整数，将会生成事件。
140:8	如果 From 报头字段在 SIP 请求或响应中为空，将会生成事件。

表 27-10　其他 SIP 预处理器规则（续）

预处理器规则 GID:SID	说明
140:10	如果 To 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:12	如果 Via 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:14	如果必填的 Contact 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:17	如果 UDP 流量中的单个 SIP 请求或响应数据包包含多条消息，将会生成事件。请注意，旧版本 SIP 支持多条消息，但 SIP 2.0 仅在每个数据包中支持一条消息。
140:18	如果 UDP 流量中的 SIP 请求或响应中消息正文的实际长度与 SIP 请求或响应中的 Content-Length 报头字段中指定的值不匹配时，将会生成事件。
140:19	如果预处理器无法识别 SIP 响应的 CSeq 字段中的方法名称，将会生成事件。
140:20	如果 SIP 服务器不质询经过身份验证的邀请消息，将会生成事件。请注意，当有 InviteReplay 计费攻击时，会出现这种情况。
140:21	如果会话信息在建立呼叫前发生变化，将会生成事件。请注意，当有 FakeBusy 计费攻击时，会出现这种情况。
140:22	如果响应状态代码不是一个三位数字，将会生成事件。
140:23	如果 Content-Type 报头字段未指定内容类型且消息正文包含数据，将会生成事件。
140:24	如果 SIP 版本不是 1、 1.1 或 2.0，将会生成事件。
140:25	如果 CSeq 报头字段中指定的方法与 SIP 请求中的 method 字段不匹配，将会生成事件。
140:26	如果预处理器无法识别在 SIP 请求方法字段中命名的方法，将会生成事件。

配置 GTP 命令通道

许可证：保护

通用分组无线业务 (GPRS) 隧道协议 (GTP) 实现通过 GTP 核心网络进行通信。GTP 预处理器检测 GTP 流量中的异常，并将命令通道信令消息转发给规则引擎进行检查。可以使用 `gtp_version`、`gtp_type` 和 `gtp_info` 规则关键字检查 GTP 命令通道流量中是否存在漏洞。

单一配置选项允许为预处理器进行 GTP 命令通道消息检查的端口修改默认设置。

如果要下表中所列的 GTP 预处理器规则生成事件，必须启用它们。有关启用规则的详细信息，请参阅第 32-18 页上的设置规则状态。

表 27-11　GTP 预处理器规则

预处理器规则 GID:SID	说明
143:1	如果预处理器检测到无效的消息长度，将会生成事件。
143:2	如果预处理器检测到无效的信息元素长度，将会生成事件。
143:3	如果预处理器检测到无序的信息元素，将会生成事件。

可以按照以下步骤修改 GTP 预处理器为其监控 GTP 命令消息的端口。

要配置 GTP 命令通道，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **GTP Command Channel Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 GTP Command Channel Configuration 页面。

步骤 5　或者，修改预处理器进行 GTP 命令消息检查的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口。

步骤 6　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

解码 IMAP 流量

许可证：保护

互联网邮件应用协议 (IMAP) 用于从远程 IMAP 服务器检索邮件。IMAP 预处理器检查服务器到客户端的 IMAP4 流量，如果相关的预处理器规则已启用，还会生成关于异常流量的事件。此预处理器还可以提取和解码客户端到服务器 IMAP4 流量中的邮件附件，并将附件数据发送到规则引擎。可以在入侵规则中使用 `file_data` 关键字以指向附件数据。有关详情，请参见第 36-90 页上的指向特定负载类型。

提取和解码涵盖多个附件 （如果有）以及同时存在于多个数据包中的大型附件。

如果要 IMAP 预处理器规则生成事件，必须启用这些规则。 IMAP 预处理器规则有生成器 ID (GID) 141。有关详细信息，请参阅第 32-18 页上的设置规则状态。

有关详细信息，请参阅以下各节：

选择 IMAP 预处理器选项

许可证：保护

以下列表说明可修改的 IMAP 预处理器选项。

请注意，解码 （或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件 （如果有）以及同时存在于多个数据包中的大型附件。

另请注意，当 **Base64 Decoding Depth**、 **7-Bit/8-Bit/Binary Decoding Depth**、 **Quoted-Printable Decoding Depth** 或 **Unix-to-Unix Decoding Depth** 选项的值在以下策略中不相同时，将使用最高的值：

- 默认网络分析策略
- 同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

有关详细信息，请参阅第 25-3 页上的为访问控制设置默认网络分析策略和第 25-4 页上的指定要使用网络分析规则进行预处理的流量。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

端口

指定用于检查 IMAP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Base64 Decoding Depth

指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、 65534、 65535 除外，因为它们将向下舍入为 65532。

如果启用了 Base64 解码，可以启用规则 141:4，以在解码失败时生成事件；导致解码失败的原因包括，编码不正确或数据损坏，等等。

7-Bit/8-Bit/Binary Decoding Depth

指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、 8 位、二进制以及各种多部分内容类型 （例如，纯文本、 jpeg 图像、 mp3 文件等）。可指定 1 到 65535 字节，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。

Quoted-Printable Decoding Depth

指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。

如果启用了 Quoted-Printable 解码，可以启用规则 141:6，以在解码失败时生成事件；导致解码失败的原因包括，编码不正确或数据损坏，等等。

Unix-to-Unix Decoding Depth

指定要从每个 Unix-to-Unix 编码 （UuEncode 编码）的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。

如果启用了 Unix-to-Unix 解码，可以启用规则 141:7，以在解码失败时生成事件；导致解码失败的原因包括，编码不正确或数据损坏，等等。

配置 IMAP 预处理器

许可证：保护

可按照以下步骤配置 IMAP 预处理器。有关 IMAP 预处理器配置选项的更多信息，请参阅第 27-46 页上的选择 IMAP 预处理器选项。

要配置 IMAP 预处理器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **IMAP Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 IMAP Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　在 **Ports** 中指定应解码其 IMAP 流量的端口。使用逗号分隔多个端口号。

步骤 6　指定要从以下邮件附件类型的任意组合中提取和解码数据的最大字节数：

- **Base64 Decoding Depth**
- **7-Bit/8-Bit/Binary Decoding Depth**（包括各种多部分内容类型，例如纯文本格式、jpeg 图像、mp3 文件等）
- **Quoted-Printable Decoding Depth**
- **Unix-to-Unix Decoding Depth**

对于每种类型，可指定 1 到 65535 字节；或者指定 0 以提取和 （如有必要）解码数据包中的所有数据。指定 -1 将会忽略附件类型的数据。

可以在入侵规则中使用 `file_data` 规则关键字来检查附件数据。有关详情，请参见第 36-90 页上的指向特定负载类型。

步骤 7　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

启用其他 IMAP 预处理器规则

许可证：保护

下表中的 IMAP 预处理器规则与特定配置选项无关。与其他 IMAP 预处理器规则一样，如果要使这些规则生成事件，必须启用它们。有关启用规则的详细信息，请参阅第 32-18 页上的设置规则状态。

表 27-12　其他 IMAP 预处理器规则

预处理器规则 GID:SID	说明
141:1	如果预处理器检测到未在 RFC 3501 中定义的客户端命令，将会生成事件。
141:2	如果预处理器检测到未在 RFC 3501 中定义的服务器响应，将会生成事件。
141:3	如果预处理器正在使用系统允许的最大内存量，将会生成事件。在这种情况下，预处理将会停止解码，直至内存可用。

解码 POP 流量

许可证：保护

邮局协议 (POP) 用于从远程 POP 邮件服务器检索邮件。 POP 预处理器检查服务器到客户端的 POP3 流量，如果相关的预处理器规则已启用，还会生成关于异常流量的事件。此预处理器还可以提取和解码客户端到服务器 POP3 流量中的邮件附件，并将附件数据发送到规则引擎。可以在入侵规则中使用 `file_data` 关键字以指向附件数据。有关详情，请参见第 36-90 页上的指向特定负载类型。

提取和解码涵盖多个附件 （如果有）以及同时存在于多个数据包中的大型附件。

如果要 POP 预处理器规则生成事件，必须启用这些规则。 POP 预处理器规则的生成器 ID (GID) 为 142。有关详情，请参见第 32-18 页上的设置规则状态。

有关详细信息，请参阅以下各节：

- 第 27-48 页上的选择 POP 预处理器选项
- 第 27-49 页上的配置 POP 预处理器
- 第 27-50 页上的启用其他 POP 预处理器规则

选择 POP 预处理器选项

许可证：保护

以下列表说明可修改的 POP 预处理器选项。

请注意，解码 （或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件 （如果有）以及同时存在于多个数据包中的大型附件。

另请注意，如果在与访问控制策略的默认操作相关的入侵策略以及与访问控制规则相关的入侵策略中， **Base64 Decoding Depth**、 **7-Bit/8-Bit/Binary Decoding Depth**、 **Quoted-Printable Decoding Depth** 或 **Unix-to-Unix Decoding Depth** 选项的值不同，将会使用最大值。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

端口

指定用于检查 POP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Base64 Decoding Depth

指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、 65534、 65535 除外，因为它们将向下舍入为 65532。

如果启用了 Base64 解码，可以启用规则 142:4，以在解码失败时生成事件；导致解码失败的原因包括，编码不正确或数据损坏，等等。有关详情，请参见第 32-18 页上的设置规则状态。

7-Bit/8-Bit/Binary Decoding Depth

指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、 8 位、二进制以及各种多部分内容类型 （例如，纯文本、 jpeg 图像、 mp3 文件等）。可指定 1 到 65535 字节，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。

Quoted-Printable Decoding Depth

指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。

当启用可打印字符引用编码时，您可以启用规则 142：6，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。有关详情，请参见第 32-18 页上的设置规则状态。

Unix-to-Unix Decoding Depth

指定要从每个 Unix-to-Unix 编码 （UuEncode 编码）的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。

当启用 Unix-to-Unix 解码时，您可以启用规则 142：7，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。有关详情，请参见第 32-18 页上的设置规则状态。

配置 POP 预处理器

许可证：保护

可按照以下步骤配置 POP 预处理器。有关 POP 预处理器配置选项的更多信息，请参阅第 27-48 页上的选择 POP 预处理器选项。

要配置 POP 预处理器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **POP Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 POP Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　在 **Ports** 中指定应解码其 IMAP 流量的端口。使用逗号分隔多个端口号。

步骤 6　指定要从以下邮件附件类型的任意组合中提取和解码数据的最大字节数：

- **Base64 Decoding Depth**
- **7-Bit/8-Bit/Binary Decoding Depth**（包括各种多部分内容类型，例如纯文本格式、jpeg 图像、mp3 文件等）
- **Quoted-Printable Decoding Depth**
- **Unix-to-Unix Decoding Depth**

对于每种类型，可指定 1 到 65535 字节；或者指定 0 以提取和 （如有必要）解码数据包中的所有数据。指定 -1 将会忽略附件类型的数据。

可以在入侵规则中使用 `file_data` 规则关键字来检查附件数据。有关详情，请参见第 36-90 页上的指向特定负载类型。

步骤 7　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

启用其他 POP 预处理器规则

许可证：保护

下表中的 POP 预处理器规则与特定配置选项无关。与其他 POP 预处理器规则一样，如果要使这些规则生成事件，必须启用它们。有关启用规则的详细信息，请参阅第 32-18 页上的设置规则状态。

表 27-13　其他 POP 预处理器规则

预处理器规则 GID:SID	说明
142:1	如果预处理器检测到未在 RFC 1939 中定义的客户端命令，将会生成事件。
142:2	如果预处理器检测到未在 RFC 1939 中定义的服务器响应，将会生成事件。
142:3	如果预处理器正在使用系统允许的最大内存量，将会生成事件。在这种情况下，预处理将会停止解码，直至内存可用。

解码 SMTP 流量

许可证：保护

SMTP 预处理器指示规则引擎对 SMTP 命令进行规范化。预处理器还可以提取和解码客户端到服务器流量中的邮件附件，并根据不同的软件版本，提取邮件的文件名、地址和报头数据，以在显示 SMTP 流量触发的入侵事件时提供上下文。

使用 SMTP 预处理器时，请注意以下几点：

- 必须启用生成器 ID (GID) 为 124 的 SMTP 预处理器规则才可生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

有关详细信息，请参阅以下各节：

- 第 27-51 页上的了解 SMTP 解码
- 第 27-54 页上的配置 SMTP 解码
- 第 27-57 页上的启用 SMTP 最大解码内存警报

了解 SMTP 解码

许可证：保护

可以启用或禁用规范化，还可以对选项进行配置以控制 SMTP 解码器检测的异常流量类型。

请注意，解码 （或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件 （如果有）以及同时存在于多个数据包中的大型附件。

另请注意，如果在与访问控制策略的默认操作相关的入侵策略以及与访问控制规则相关的入侵策略中，**Base64 Decoding Depth**、**7-Bit/8-Bit/Binary Decoding Depth**、**Quoted-Printable Decoding Depth** 或 **Unix-to-Unix Decoding Depth** 选项的值不同，将会使用最大值。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

端口

指定要实现 SMTP 流量规范化的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口。

状态性检查

如果选择此选项， SMTP 解码器将会保存状态，提供各个数据包的会话上下文，并且仅检查重组的会话。如果清除此选项，将会在没有会话上下文的情况下分析每个数据包。

Normalize

如果设置为 All，将会规范化所有命令。会检查命令后是否有多个空格字符。

如果设置为 None，不会对命令进行规范化。

如果设置为 Cmds，将会规范化 **Custom Commands** 中列出的命令。

Custom Commands

如果 **Normalize** 设置为 Cmds，此选项会规范化列出的命令。

可在文本框中指定应进行规范化的命令。会检查命令后是否有多个空格字符。

空格 (ASCII 0x20) 和制表符 (ASCII 0x09) 字符被视为是用于规范化目的的空格字符。

Ignore Data

不处理邮件数据；仅处理 MIME 邮件报头数据。

Ignore TLS Data

不处理根据传输层安全协议加密的数据。

No Alerts

当随附的预处理器规则处于启用状态时禁用入侵事件。

Detect Unknown Commands

检测 SMTP 流量中的未知命令。

可以启用规则 124:5 和 124:6 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Max Command Line Len

检测 SMTP 命令行的长度何时大于此值。指定 0 将不会检测命令行长度。

RFC2821 （网络工作组制定的关于简单邮件传输协议的规范）建议将最大命令行长度设置为 512。

可以启用规则 124:1 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Max Header Line Len

检测 SMTP 数据报头行的长度何时大于此值。指定 0 将不会检测数据报头行长度。

可以启用规则 124:2 和 124:7 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Max Response Line Len

检测 SMTP 响应行的长度何时大于此值。指定 0 将不会检测响应行长度。

RFC 2821 建议将最大响应行长度设置为 512。

可以启用规则 124:3 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Alt Max Command Line Len

检测任何指定命令的 SMTP 命令行的长度何时大于此值。指定 0 将不会检测指定命令的命令行长度。为众多命令设置了不同的默认行长度。

此设置将覆盖指定命令的 Max Command Line Len 设置。

可以启用规则 124:3 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Invalid Commands

检测命令是否是从客户端发出的。

可以启用规则 124:5 和 124:6 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Valid Commands

允许此列表中的命令。

即使此列表为空，预处理器仍允许下列有效命令：ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR

注 RCPT TO 和 MAIL FROM 是 SMTP 命令。对这两个命令，预处理器配置分别使用命令名 RCPT 和 MAIL。在代码中，预处理器会将 RCPT 和 MAIL 映射到正确的命令名。

可以启用规则 124:4 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Data Commands

列出以与 SMTP DATA 命令按照 RFC5321 的要求发送数据相同的方法发起数据发送的命令。使用空格分隔多个命令。

Binary Data Commands

列出以与 BDAT 命令按照 RFC 3030 的要求发送数据类似的方法发起数据发送的命令。使用空格分隔多个命令。

Authentication Commands

列出发起客户端和服务器之间的身份认证交换的命令。使用空格分隔多个命令。

Detect xlink2state

检测作为 X-Link2State Microsoft Exchange 缓冲区数据溢出攻击的一部分的数据包。在内联部署中，系统还可以丢弃这些数据包。

可以启用规则 124:8 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Base64 Decoding Depth

在 **Ignore Data** 已禁用的情况下，指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。如果选择了 **Ignore Data**，预处理器将不会对数据进行解码。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、65534、65535 除外，因为它们将向下舍入为 65532。

如果启用了 Base64 解码，可以启用规则 124:10，以在解码失败时生成事件；导致解码失败的原因包括，编码不正确或数据损坏，等等。有关详情，请参见第 32-18 页上的设置规则状态。

请注意，此选项取代已被弃用的 **Enable MIME Decoding** 和 **Maximum MIME Decoding Depth** 选项，后两个选项由于具有向后兼容性，因此在现有入侵策略中仍受到支持。

7-Bit/8-Bit/Binary Decoding Depth

在 **Ignore Data** 已禁用的情况下，指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、 8 位、二进制以及各种多部分内容类型 （例如，纯文本、jpeg 图像、mp3 文件等）。可指定 1 到 65535 字节，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。如果选择了 **Ignore Data**，预处理器将不会提取数据。

Quoted-Printable Decoding Depth

在 **Ignore Data** 已禁用的情况下，指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。

可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。如果选择了 **Ignore Data**，预处理器将不会对数据进行解码。

当启用可打印字符引用编码时，您可以启用规则 124：11，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。有关详情，请参见第 32-18 页上的设置规则状态。

Unix-to-Unix Decoding Depth

在 **Ignore Data** 已禁用的情况下，指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。如果选择了 **Ignore Data**，预处理器将不会对数据进行解码。

当启用 Unix-to-Unix 解码时，您可以启用规则 124：13，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。有关详情，请参见第 32-18 页上的设置规则状态。

Log MIME Attachment Names

允许从 MIME Content-Disposition 报头提取 MIME 附件文件名，并将提取的文件名与为会话生成的所有入侵事件相关联。支持多个文件名。

启用此选项后，可以在入侵事件表视图的 Email Attachment 列中查看与事件相关的文件名。有关详情，请参见第 41-8 页上的了解入侵事件。

Log To Addresses

允许从 SMTP RCPT TO 命令提取收件人邮件地址，并将提取的收件人地址与为会话生成的所有入侵事件相关联。支持多个收件人。

启用此选项后，可以在入侵事件表视图的 Email Recipient 列中查看与事件相关的收件人。有关详情，请参见第 41-8 页上的了解入侵事件。

Log From Addresses

允许从 SMTP MAIL FROM 命令提取发件人邮件地址，并将提取的发件人地址与为会话生成的所有入侵事件相关联。支持多个发件人地址。

启用此选项后，可以在入侵事件表视图的 Email Sender 列中查看与事件相关的收件人。有关详情，请参见第 41-8 页上的了解入侵事件。

Log Headers

允许提取邮件报头。要提取的字节数取决于 **Header Log Depth** 中指定的值。

可以使用 `content` 或 `protected_content` 关键字来编写将邮件报头数据用作模式的入侵规则。还可以在入侵事件数据包视图中查看提取的邮件报头。有关详细信息，请参阅第 36-16 页上的限制内容匹配和第 41-19 页上的使用数据包视图。

Header Log Depth

指定在 **Log Headers** 已启用的情况下要提取的邮件报头的字节数。可指定 0 到 20480 字节。值 0 将会禁用 **Log Headers**。

配置 SMTP 解码

许可证：保护

可以使用入侵策略的 SMTP Configuration 页面来配置 SMTP 规范化。有关 SMTP 预处理器配置选项的详细信息，请参阅第 27-51 页上的了解 SMTP 解码。

要配置 SMTP 解码选项，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **SMTP Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 SMTP Configuration 页面。下图显示了防御中心数据包视图。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　在 **Ports** 中指定应解码其 SMTP 流量的端口，端口之间用逗号分隔。

步骤 6　选择 **Stateful Inspection** 将会检查包含 SMTP 数据包的重组 TCP 数据流。清除 **Stateful Inspection** 将只会检查非重组数据包

步骤 7　配置规范化选项：

- 要对所有命令进行规范化，请选择 **All**。
- 要只对 **Custom Commands** 中指定的命令进行规范化，请选择 **Cmds** 并指定要规范化的命令。使用空格分隔各个命令。
- 如果不想对任何命令进行规范化，请选择 **None**。
- 要忽略除 MIME 邮件报头数据以外的邮件数据，请选择 **Ignore Data**。
- 要忽略根据传输层安全协议加密的数据，请选择 **Ignore TLS Data**。
- 要禁止在随附的预处理器规则已启用的情况下生成事件，请选择 **No Alerts**。
- 要检测 SMTP 数据中的未知命令，请选择 **Detect Unknown Commands**。

步骤 8　在 **Max Command Line Len** 字段中指定最大命令行长度。

步骤 9　在 **Max Header Line Len** 字段中指定最大数据报头行长度。

步骤 10　在 **Max Response Line Len** 字段中指定最大响应行长度。

注　RCPT TO 和 MAIL FROM 是 SMTP 命令。对这两个命令，预处理器配置分别使用命令名 RCPT 和 MAIL。在代码中，预处理器会将 RCPT 和 MAIL 映射到正确的命令名。

步骤 11　如有需要，点击 **Alt Max Command Line Len** 旁边的 **Add**，添加要为其指定替代最大命令行长度的命令，然后指定行长度以及要对其应用该指定长度的命令 （命令之间用空格隔开）。

步骤 12　在 **Invalid Commands** 字段中指定要将其看作无效命令并进行检测的任何命令。使用空格分隔各个命令。

步骤 13　在 **Valid Commands** 字段中指定要将其看作有效命令的任何命令。使用空格分隔各个命令。

注　即使 **Valid Commands** 列表为空，预处理器仍会将下列命令看作有效命令：ATRN、AUTH、BDAT、DATA、DEBUG、EHLO、EMAL、ESAM、ESND、ESOM、ETRN、EVFY、EXPN、HELO、HELP、IDENT、MAIL、NOOP、QUIT、RCPT、RSET、SAML、SOML、SEND、ONEX、QUEU、STARTTLS、TICK、TIME、TURN、TURNME、VERB、VRFY、X-EXPS、X-LINK2STATE、XADR、XAUTH、XCIR、XEXCH50、XGEN、XLICENSE、XQUE、XSTA、XTRN 或 XUSR。

步骤 14　在 **Data Commands** 字段中指定您希望以与 SMTP DATA 命令按照 RFC5321 的要求发送数据相同的方法发起数据发送的任何命令。使用空格分隔各个命令。

步骤 15　在 **Binary Data Commands** 字段中指定您希望以与 BDAT 命令按照 RFC 3030 的要求发送数据类似的方法发起数据发送的任何命令。使用空格分隔各个命令。

步骤 16　在 **Authentication Commands** 字段中指定发起客户端和服务器之间的身份验证交换的任何命令。使用空格分隔各个命令。

步骤 17　检测作为 X-Link2State Microsoft Exchange 缓冲区数据溢出攻击的一部分的数据包，请选择 **Detect xlink2state**。

步骤 18　要为不同类型的邮件附件指定要提取和解码的数据的最大字节数，请为以下任何类型的附件指定一个值：

- **Base64 Decoding Depth**
- **7-Bit/8-Bit/Binary Decoding Depth**（包括各种多部分内容类型，例如纯文本格式、jpeg 图像、mp3 文件等）
- **Quoted-Printable Decoding Depth**
- **Unix-to-Unix Decoding Depth**

可指定 1 到 65535 字节，或者指定 0 以提取和（必要时）解码该类型数据包中的所有数据。指定 -1 将会忽略附件类型的数据。

可以在入侵规则中使用 `file_data` 规则关键字来检查提取的数据。有关详情，请参见第 36-90 页上的指向特定负载类型。

要提取和解码跨数据包数据或跨越多个 TCP 分段的数据，还必须选择 SMTP **Stateful Inspection** 选项。

步骤 19　配置用于将上下文信息与 SMTP 流量触发的入侵事件相关联的选项：

- 要允许提取 MIME 附件文件名以便与入侵事件相关联，请选择 **Log MIME Attachment Names**。
- 要允许提取收件人邮件地址，请选择 **Log To Addresses**。
- 要允许提取发件人邮件地址以便与入侵事件相关联，请选择 **Log From Addresses**。
- 要提取邮件报头以便与入侵事件相关联并编写用于检查邮件报头的规则，请选择 **Log Headers**。

  请注意，报头信息显示在入侵事件数据包视图中。另请注意，还可以编写将使用 `content` 或 `protected_content` 关键字以及邮件报头数据作为模式的入侵规则。有关详细信息，请参阅第 41-20 页上的查看事件信息和第 36-14 页上的搜索内容匹配。

  或者，可以在 **Header Log Depth** 中指定 0 到 20480 字节之间的邮件标头，便于进行提取。值 0 将会禁用 **Log Headers**。

步骤 20　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

启用 SMTP 最大解码内存警报

许可证：保护

可以启用 SMTP 预处理器规则 124:9，以便当启用的预处理器使用系统允许用于解码以下类型编码数据的最大内存量时生成事件：

- Base64
- 7 位/8 位/二进制
- Quoted-printable
- Unix-to-Unix

如果超过最大解码内存，预处理器将停止解码这些类型的编码数据，直至内存可用。这个预处理器规则与单个特定配置选项不相关。有关启用规则的详细信息，请参阅第 32-18 页上的设置规则状态。

使用 SSH 预处理器检测攻击

许可证：保护

SSH 预处理器可检测质询-响应缓冲区溢出攻击、CRC-32 攻击、SecureCRT SSH 客户端缓冲区溢出攻击、协议不匹配攻击以及错误的 SSH 消息传输方向。预处理器还可以检测任何版本字符串（版本 1 和 2 除外）。

密钥交换后，会发生质询-响应缓冲区溢出攻击和 CRC-32 攻击，进而被加密。这两种攻击在身份验证质询之后立即向服务器发送超过 20 KB 的反常态大量负载。CRC-32 攻击仅适用于 SSH 版本 1；质询-响应缓冲区溢出攻击仅适用于 SSH 版本 2。会话开始时可读取版本字符串。除了版本字符串中存在差异外，这两种攻击都可以同样的方式加以处理。

在密钥交换之前尝试进行连接时，会发生 SecureCRT SSH 攻击和协议不匹配攻击。SecureCRT 漏洞会向客户端发送超长协议标识符字符串，从而导致缓冲区溢出。如果非 SSH 客户端应用试图连接到安全 SSH 服务器或者服务器和客户端的版本号不匹配，会出现协议不匹配攻击。

可以将预处理器配置为会检查指定端口或端口列表的流量，或者会自动检测 SSH 流量。预处理器将会继续检查 SSH 流量，直至传递了未超过指定字节数的指定数量的加密数据包，或者直至超过指定数量的数据包中指定的最大字节数。如果超过最大字节数，系统将会假设出现了 CRC-32（SSH 版本 1）攻击或质询-响应缓冲区溢出 （SSH 版本 2）攻击。此外，还可以检测 SecureCRT 攻击、协议不匹配攻击及错误的消息传输方向。请注意，预处理器检测时无需配置任何版本字符串值 （版本 1 和 2 除外）。

使用 SSH 预处理器时，请注意以下几点：

- 必须启用生成器 ID (GID) 为 128 的 SSH 预处理器规则才可生成事件。有关详情，请参见第 32-18 页上的设置规则状态。
- SSH 预处理器不处理蛮力攻击。有关蛮力攻击的详细信息，请参阅第 32-26 页上的添加动态规则状态。

有关详细信息，请参阅以下各节：

- 第 27-58 页上的选择 SSH 预处理器选项
- 第 27-60 页上的配置 SSH 预处理器

选择 SSH 预处理器选项

许可证：保护

本节介绍了可用于配置 SSH 预处理器的选项。

如果发生以下任何一种情况，预处理器将停止检查会话流量：

- 对于某个数量的加密数据包，服务器与客户端之间发生有效交换；连接继续保持。
- 在达到在 **Number of Bytes Sent Without Server Response** 中设置的值之前，达到要检查的加密数据包数量；假设发生了攻击。

在 **Number of Encrypted Packets to Inspect** 中设置的数量内的每个有效服务器响应会重置 **Number of Bytes Sent Without Server Response**，且数据包计数继续进行。

可考虑以下 SSH 预处理器配置示例：

- **Server Ports**：22
- **Autodetect Ports**：off
- **Maximum Length of Protocol Version String**：80
- **Number of Encrypted Packets to Inspect**：25
- **Number of Bytes Sent Without Server Response**：19,600
- 所有检测选项均启用。

在本示例中，预处理器仅检查端口 22 的流量。也就是说，自动检测被禁用，因此只检查指定的端口。

此外，如果发生以下任何一种情况，本示例中的预处理器会停止检查流量：

- 客户端发送 25 个加密数据包，这些数据包总共不超过 19,600 字节。假设没有发生攻击。
- 客户端发送 25 个加密数据包，这些数据包总共不超过 19,600 字节。在这种情况下，预处理器可将发生的攻击视为质询-响应缓冲区溢出攻击，因为本示例中的会话为 SSH 版本 2 会话。

本示例中的预处理器还将检测处理流量过程中发生的以下任何情况：

- 服务器溢出，由大于 80 字节的版本字符串触发，表明为 SecureCRT 攻击
- 协议不匹配
- 数据包的传输方向错误

最后，预处理器将自动检测任何版本字符串 （版本 1 和 2 除外）。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

服务器端口

指定 SSH 预处理器应检查其流量的端口。

可以配置单个端口或端口的逗号分隔列表。

Autodetect Ports

将预处理器设置为会自动检测 SSH 流量。

如果选择此选项，预处理器会检查某个 SSH 版本号的所有流量。如果客户端和服务器数据包均没有包含版本号，预处理器将会停止处理。如果禁用此选项，预处理器只检查在 **Server Ports** 选项中确定的流量。

Number of Encrypted Packets to Inspect

指定每个会话待检查的加密数据包的数量。

将此选项设置为 0 将允许所有流量通过。

减少待检查的加密数据包的数量可能会导致一些攻击避开检测。增加待检查的加密数据包的数量可能会对性能造成负面影响。

Number of Bytes Sent Without Server Response

指定在假设存在质询-响应缓冲区溢出或 CRC-32 攻击之前， SSH 客户端在未获得响应的情况下可以向服务器发送的最大字节数。

如果预处理器对于质询-响应缓冲区溢出或 CRC-32 攻击生成误报，请增加此选项的值。

Maximum Length of Protocol Version String

指定在假设存在 SecureCRT 攻击之前，服务器版本字符串中允许的最大字节数。

Detect Challenge-Response Buffer Overflow Attack

启用或禁用质询-响应缓冲区溢出攻击检测。

可以启用规则 128:1 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Detect SSH1 CRC-32 Attack

启用或禁用 CRC-32 攻击检测。

可以启用规则 128:2 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Detect Server Overflow

启用或禁用 SecureCRT SSH 客户端缓冲区溢出攻击检测。

可以启用规则 128:3 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Detect Protocol Mismatch

启用或禁用协议不匹配检测。

可以启用规则 128:4 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Detect Bad Message Direction

允许或禁止检测流量传输方向错误这种情况 （即，如果假定的服务器生成客户端流量，或者客户端生成服务器流量）。

可以启用规则 128:5 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Detect Payload Size Incorrect for the Given Payload

允许或禁止检测负载大小不正确的数据包，例如， SSH 数据包中指定的长度与 IP 报头中指定的总长度不一致，或者消息被截断 （即，无足够的数据用于整个 SSH 报头）。

可以启用规则 128:6 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

Detect Bad Version String

请注意，启用预处理器后，它在检测时无需配置任何版本字符串 （版本 1 和 2 除外）。

可以启用规则 128:7 为此选项生成事件。有关详情，请参见第 32-18 页上的设置规则状态。

配置 SSH 预处理器

许可证：保护

本节说明如何配置 SSH 预处理器。

要配置 SSH 预处理器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **SSH Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 SSH Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　可以修改 SSH Configuration 预处理器页面上的任何选项。有关详情，请参见第 27-58 页上的选择 SSH 预处理器选项。

步骤 6　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

使用 SSL 预处理器

许可证：功能相关

SSL 预处理器可供您配置 SSL 检查，从而可以阻止、解密或使用访问控制检查已加密的流量。无论您是否配置 SSL 检查，SSL 预处理器还会分析在流量中检测到的 SSL 握手消息，并确定会话何时被加密。系统通过识别已加密流量可以停止对已加密负载执行入侵和文件检查，这有助于减少误报并提高性能。有关详细信息，请参阅第 19-1 页上的了解流量解密和第 14-2 页上的创建和编辑访问控制规则。

SSL 预处理器还可以检查已加密流量以检测 Heartbleed 漏洞攻击尝试，并在检测到此类漏洞攻击时生成事件。

使用 SSL 预处理器解密已加密流量无需许可证。所有其他 SSL 预处理器功能 （包括暂停检查已加密负载是否存在恶意软件和入侵，并检测 Heartbleed 漏洞攻击）均需要保护许可证。

注　默认情况下，系统提供的网络分析策略启用 SSL 预处理器。如果预期有已加密流量通过您的网络，思科建议不要在自定义部署中禁用 SSL 预处理器。

有关详细信息，请参阅以下各节：

了解 SSL 预处理

许可证：保护

如果配置了 SSL 检查，则 SSL 预处理器停止对已加密数据进行入侵和文件检查，然后使用 SSL 策略对已加密流量进行检查。这有助于清除误报。SSL 预处理器在检查 SSL 握手时会维护状态信息，跟踪该会话的状态和 SSL 版本。如果预处理器检测到会话状态已被加密，系统会将该会话的流量标记为“加密”。可将系统配置为在确定会话已加密时停止处理已加密会话中的所有数据包，并在检测到 Heartbleed 漏洞攻击尝试时生成事件。

对于每个数据包， SSL 预处理器都会验证流量是否包含 IP 报头、 TCP 报头和 TCP 负载，以及流量发生在指定适用于 SSL 预处理的端口上。对于符合条件的流量，可根据以下情况确定流量是否已加密：

- 系统检测会话中的所有数据包，未启用 **Server side data is trusted**，会话中包含来服务器和客户端的 Finished 消息和至少一个来自服务器和客户端的数据包 （包含应用记录但不包含警报记录）
- 系统漏检了一些流量，未启用 **Server side data is trusted**，而且会话中至少包含来自服务器和客户端的一个数据包 （包含应用记录但不包含警报记录）
- 系统检测会话中的所有数据包，未启用 **Server side data is trusted**，会话中包含来客户端的 Finished 消息和至少一个来自客户端的数据包 （包含应用记录但不包含警报记录）
- 系统漏检了一些流量，未启用 **Server side data is trusted**，而且会话中至少包含来自客户端的一个数据包 （包含应用记录但不包含警报记录）

如果选择停止处理加密流量，系统会在将该会话标记为“加密”后忽略其中的后续数据包。

此外，在 SSL 握手期间，预处理器监控心跳请求和响应。检测到以下对象时，预处理器生成事件。

- 包含的负载长度值大于负载本身的心跳请求
- 大于 Max Heartbeat Length 字段中存储的值的心跳响应

注　可向某规则添加 `ssl_state` 和 `ssl_version` 关键字，以便在该规则中使用 SSL 状态或版本信息。有关详细信息，请参阅第 36-50 页上的从会话提取 SSL 信息。

启用 SSL 预处理器规则

许可证：保护

启用 SSL 预处理器后，它会检查 SSL 会话开始时交换的握手和密钥交换消息的内容。会话加密之后，可以暂停检查流量是否存在入侵和恶意软件。如果配置 SSL 检查，则 SSL 预处理器还将确定您可以阻止、解密或使用访问控制进行检查的已加密流量。

请注意，如果您希望 SSL 预处理器规则生成事件，则必须启用这些规则，其生成器 ID (GID) 为 137。有关详情，请参见第 32-18 页上的设置规则状态。

下表说明了可启用的 SSL 预处理器规则。

表 27-14　SSL 预处理器规则

预处理器规则 GID:SID	说明
137:1	在服务器问候消息之后检测到客户端问候消息，后者是无效的，被视为异常行为。
137:2	在 **Server side data is trusted** 禁用的情况下检测到服务器问候消息（但没有检测到客户端问候消息），该问候消息是无效状态，被视为异常行为。有关详情，请参见第 27-62 页上的配置 SSL 预处理器。
137:3	当 **Max Heartbeat Length** 包含非零值时，检测到负载长度超过负载本身的心跳请求，这指示 Heartbleed 漏洞攻击尝试。
137:4	检测到大于在 **Max Heartbeat Length** 中指定的非零值的心跳响应，这指示 Heartbleed 漏洞攻击尝试。

配置 SSL 预处理器

许可证：保护

如果未配置 SSL 检查，则系统尝试检查已加密流量是否存在恶意软件和入侵，而不对其进行解密。如果启用了 SSL 预处理器，它会检测会话加密的时间。启用 SSL 预处理器后，规则引擎可以调用预处理器来获得 SSL 状态和版本信息。如果在某个入侵策略中启用使用 `ssl_state` 和 `ssl_version` 关键字的规则，则还应在该策略中启用 SSL 预处理器。

此外，可以启用 **Stop inspecting encrypted traffic** 选项来禁止检查和重组加密的会话。SSL 预处理器会维护会话状态，因此，它可以禁止对会话中所有流量的检查。如果启用了 SSL 预处理**并**选择了 **Stop inspecting encrypted traffic** 选项，则系统只停止检查加密会话中的流量。请注意，如果清除 **Stop inspecting encrypted traffic** 选项，将无法修改 **Server side data is trusted** 选项。

要仅以服务器流量为依据标别加密流量，可以启用 **Server side data is trusted** 选项；也就是说，可信赖服务器端数据来指明流量是否已加密。 SSL 预处理器通常会检查客户端流量以及服务器对该流量的响应，从而确定会话是否已加密。但是，如果系统无法检测会话的两端，就可能不会将会话标记为“加密”，因此，可依赖于 SSL 服务器来确定会话是否已加密。请注意，如果启用 **Server side data is trusted** 选项，还必须启用 **Stop inspecting encrypted traffic** 选项，这样系统就不会继续检查加密会话中的流量。

可可预处理器 **Max Heartbeat Length** 选项配置为通过检查 SSL 握手内部的心跳请求和响应而检测 Heartbleed 漏洞攻击尝试。如果预处理器检测到负载长度超过实际负载长度或心跳响应大小超过 **Max Heartbeat Length** 值的心跳请求，则预处理器会生成事件。

可以指定预处理器监控加密会话流量的端口。

注　如果 SSL 预处理器检测到指定用于 SSL 监控的端口上有非 SSL 流量，它会尝试将该流量作为 SSL 流量进行解码，然后将其标记为“损坏”。

要配置 SSL 预处理器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **SSL Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 SSL Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　输入 SSL 预处理器应监控加密会话流量的端口 （用逗号隔开）。只会检查包含在 **Ports** 字段中的端口的加密流量。

步骤 6　点击 **Stop inspecting encrypted traffic** 复选框，以允许或禁止在会话被标记为“加密”后检查会话中的流量。

步骤 7　点击 **Server side data is trusted** 复选框，以允许或禁止仅以客户端流量为依据标别加密流量。

步骤 8　在 **Max Heartbeat Length** 字段中输入字节数以启用检查 SSL 握手内部的心跳请求和响应是否存在 Heartbleed 漏洞攻击尝试。您可以指定介于 1 和 65535 之间的整数，或指定 0 禁用该选项。

步骤 9　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

配置 SCADA 预处理

您在网络分析策略中配置监控与数据采集 （SCADA）预处理器，该预处理器准备流量以备使用在入侵策略中启用的规则进行检查。有关详情，请参见第 23-1 页上的了解网络分析和入侵策略。

SCADA 协议可监视和控制工业、基础设施以及工厂流程 （例如制造、生产、水处理、配电、机场和运输系统等）并从中获取数据。 FireSIGHT 系统为您可在网络分析策略中配置的 Modbus 和 DNP3 SCADA 协议提供预处理器。

注意事项 某些具有自定义用户角色的用户无法通过标准菜单路径 (**Policies > Access Control > Network Analysis Policy**) 访问网络分析策略。这些用户可以通过入侵策略访问网络分析策略：**Policies > Intrusion > Intrusion Policy > Network Analysis Policy**。有关自定义用户角色的详细信息，请参阅第 61-48 页上的管理自定义用户角色。

如果在相应的入侵策略中启用了包含 Modbus 或 DNP3 关键字的规则，系统将自动分别使用带有当前设置的 Modbus 或 DNP3 预处理器，尽管该预处理器在网络分析策略网络界面中保持禁用状态。有关详细信息，请参阅第 36-68 页上的 Modbus 关键字和第 36-70 页上的 DNP3 关键字。

有关详细信息，请参阅以下各节：

配置 Modbus 预处理器

许可证：保护

Modbus 协议由 Modicon 于 1979 年首次发布，是一种广泛使用的 SCADA 协议。 Modbus 预处理器可检测 Modbus 流量中的异常，解码 Modbus 协议以供规则引擎进行处理 （规则引擎使用 Modbus 关键字来访问某些协议字段）。有关详情，请参见第 36-68 页上的 Modbus 关键字。

单一配置选项允许为预处理器进行 Modbus 流量检查的端口修改默认设置。

如果要下表中所列的 Modbus 预处理器规则生成事件，必须启用这些规则。有关启用规则的详细信息，请参阅第 32-18 页上的设置规则状态。

表 28-1　Modbus 预处理器规则

预处理器规则 GID:SID	说明
144:1	如果 Modbus 报头中的长度与 Modbus 函数代码所要求的长度不匹配，将会生成事件。 每个 Modbus 函数都有预期的请求和响应格式。如果消息长度与预期格式不匹配，将会生成此事件。
144:2	如果 Modbus 协议 ID 未非零值，将会生成事件。协议 ID 字段用于将其他协议与 Modbus 协议复用。由于预处理器并不处理此类其他协议，因此会生成此事件。
144:3	如果预处理器检测到保留的 Modbus 函数代码，将会生成事件。

请注意，关于 Modbus 预处理器的使用，如果您的网络不包含任何启用了 Modbus 的设备，您不应该在应用于流量的网络分析策略中启用此预处理器。

可以按照以下步骤修改 Modbus 预处理器监控的端口。

要配置 Modbus 预处理器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **SCADA Preprocessors** 下的 **Modbus Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Modbus Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　或者，在 **Ports** 中修改预处理器要检查其 Modbus 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口。

步骤 6　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

配置 DNP3 预处理器

许可证：保护

分布式网络协议 (DNP3) 是一种 SCADA 协议，最初开发用于为电站之间提供一致的通信。DNP3 还广泛应用于供水、废物处置、运输及其他行业。

DNP3 预处理器可检测 DNP3 流量中的异常，解码 DNP3 协议以供规则引擎进行处理 （规则引擎使用 DNP3 关键字来访问某些协议字段）。有关详情，请参见第 36-70 页上的 DNP3 关键字。

如果要下表中所列的 DNP3 预处理器规则生成事件，必须启用这些规则。有关启用规则的详细信息，请参阅第 32-18 页上的设置规则状态。

表 28-2　　DNP3 预处理器规则

预处理器规则 GID:SID	说明
145:1	在 **Log bad CRC** 已启用的情况下，如果预处理器检测到具有无效校验和的链路层帧，将会生成事件。
145:2	如果预处理器检测到具有无效长度的 DNP3 链路层帧，将会生成事件并阻止该数据包。
145:3	如果预处理器检测到具有无效序列号的传输层分段，将会生成事件并在重组期间阻止数据包。
145:4	如果需要清除 DNP3 重组缓冲区后才能重组完整的分片，将会生成事件。如果在其他分片已加入队列后出现带有 FIR 标志的分片，将会发生这种情况。
145:5	如果预处理器检测到使用保留地址的 DNP3 链路层帧，将会生成事件。
145:6	如果预处理器检测到使用保留函数代码的 DNP3 请求或响应，将会生成事件。

请注意，关于 DNP3 预处理器的使用，如果您的网络不包含任何启用了 DNP3 的设备，您不应该在应用于流量的网络分析策略中启用此预处理器。有关详情，请参见第 29-25 页上的配置 TCP 数据流预处理。

以下列表说明可配置的 DNP3 预处理器选项。

端口

启用对每个指定端口的 DNP3 流量检查。可以指定单个端口或端口的逗号分隔列表。可以为每个端口指定一个 0 到 65535 之间的值。

Log bad CRCs

如果启用此选项，将会验证包含在 DNP3 链路层帧中的校验和。具有无效校验和的帧将被忽略。

可以启用规则 145:1，以便在检测到无效校验和时生成事件。

要配置 DNP3 预处理器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **SCADA Preprocessors** 下的 **DNP3 Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 DNP3 Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　或者，在 **Ports** 中修改预处理器要检查其 DNP3 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口。

步骤 6　或者，选择或清除 **Log bad CRCs** 复选框，以便指定是否验证包含在 DNP3 链路层帧中的校验和并忽略具有无效校验和的帧。

步骤 7　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅网络分析策略编辑操作表。

配置传输和网络层预处理

您在网络分析策略中的网络层预处理器上配置大多数传输，从而使用在入侵策略中启用的规则准备用于检查的流量。有关详细信息，请参阅第 23-1 页上的了解网络分析和入侵策略。

传输和网络层预处理器检测对 IP 分片、校验和验证及 TCP 和 UDP 会话预处理加以利用的攻击。在将数据包发送到预处理器之前，数据包解码器将数据包报头和负载转换为便于预处理器和入侵规则引擎使用的格式，并检测数据包报头的各种异常行为。在数据包解码后到将数据包发送到其他预处理器之前这段期间，内联规范化预处理器会对流量进行规范化以便进行内联部署。

当入侵规则或规则参数要求禁用的预处理器时，尽管预处理器在网络分析策略网络界面中保持禁用状态，系统还会自动使用其当前设置。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

注意事项 某些具有自定义用户角色的用户无法通过标准菜单路径 (**Policies > Access Control > Network Analysis Policy**) 访问网络分析策略。这些用户可以通过入侵策略访问网络分析策略：**Policies > Intrusion > Intrusion Policy > Network Analysis Policy**。有关自定义用户角色的详细信息，请参阅第 61-48 页上的管理自定义用户角色。

可以定制通过 VLAN、区域或网络在网络分析策略中配置的传输层和网络层预处理器设置。请注意，某些传输层和网络层设置全局应用于所有流量，并且可以在访问控制策略中配置这些设置。

配置高级传输/网络设置

许可证：保护

高级传输和网络预处理器设置全局应用于所有应用访问控制策略的网络、区域和 VLAN。在一个访问控制策略而非网络分析策略中配置这些高级设置。

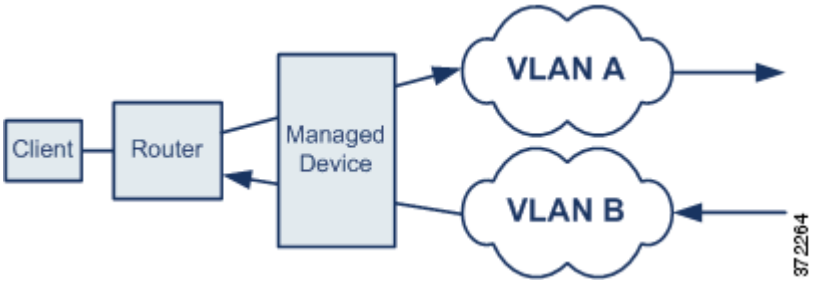
以下各节介绍这些设置：

忽略 VLAN 报头

许可证：保护

受支持的设备：任何防御中心，除了ASA FirePOWER

同一连接但行进方向不同的流量中的不同 VLAN 标记会影响流量重组和规则处理。例如，在下图中，同一连接的流量可以通过 VLAN A 进行传输，并通过 VLAN B 进行接收。



如果启用 **Ignore the VLAN header when tracking connections**，则系统忽略 VLAN 报头，因此可以针对部署正确处理数据包。

要忽略 VLAN 报头，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Transport/Network Layer Preprocessor Settings** 旁边的编辑图标 ( )。

系统将显示 Transport/Network Layer Preprocessor Settings 弹出窗口。

步骤 5　有以下选项可供选择：

- 对于可能会对在不同行进方向的流量中的同一连接检测到不同 VLAN 标记的已部署设备，请选择 **Ignore the VLAN header when tracking connections** 复选框，以在识别流量时忽略 VLAN 报头。
- 对于不会对在不同行进方向的同一连接流量检测到不同 VLAN 标记的已部署设备，请清除 **Ignore the VLAN header when tracking connections** 复选框，以在识别流量时包含 VLAN 报头。

步骤 6　点击 **OK**。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

使用入侵丢弃规则启动活动响应

许可证：保护

丢弃规则是指规则状态设置为 Drop and Generate Events 的入侵规则或预处理器规则。在内联部署中，系统通过丢弃触发数据包并阻止数据包起始的会话来对 TCP 或 UDP 丢弃规则作出响应。在被动部署中，系统无法丢弃数据包，并且除使用活动响应的情况以外，不会阻止会话。

提示　由于在*会话*方面通常未考虑 UDP 数据流，因此，请参阅第 29-28 页上的使用 UDP 数据流预处理，以进一步了解数据流预处理器如何使用封装 IP 数据报报头中的源和目标 IP 地址字段及 UDP 报头中的端口字段来确定流动方向并识别 UDP 会话。

您可以配置 **Maximum Active Responses** 选项来启动一个或多个*活动响应*，从而在有问题的数据包触发 TCP 或 UDP 丢弃规则时，更精确具体地关闭 TCP 连接或 UDP 会话。

在内联部署中启用活动响应后，系统通过丢弃触发数据包并在客户端和服务器流量中均插入 TCP 重置 (RST) 数据包来对 TCP 丢弃规则作出响应。系统在被动部署中无法丢弃数据包；在被动部署中启用活动响应时，系统通过向 TCP 连接的客户端和服务器端均发送 TCP 重置来对 TCP 丢弃规则作出响应。在内联部署或被动部署中启用活动响应后，系统通过向会话的两端发送 ICMP 不可达数据包来关闭 UDP 会话。活动响应在内联部署中最有效，因为重置更有可能及时到达以影响连接或会话。

根据 **Maximum Active Responses** 选项的配置，如果系统看到连接或会话的任一端有其他流量，也可以启动其他活动响应。自从先前响应以来经过指定的秒数后，系统最多会启动数量为指定最大值的每个其他活动响应。

有关有关设置最大活动响应数的信息，请参阅第 29-19 页上的选择 TCP 全局选项。

请注意，无论 **Maximum Active Responses** 的配置如何，已触发的 **resp** 或 **react** 规则也会启动活动响应；但是， **Maximum Active Responses** 控制系统是否以与其控制丢弃规则的最大活动响应数相同的方式来启动 **resp** 和 **react** 规则的其他活动响应。有关详细信息，请参阅第 36-77 页上的使用规则关键字发起活动响应。

您还可以使用 `config response` 命令配置要使用的活动响应接口以及要在被动部署中尝试的 TCP 重置次数。有关详细信息，请参阅第 36-80 页上的设置活动响应重置尝试次数和界面。

没有预处理器规则与以下选项关联。

Maximum Active Responses

指定每次 TCP 连接的最大活动响应数 （1 至 25）。如果已启动活动响应的连接上出现其他流量，并且在先前活动响应后流量出现超过**最小响应秒数**，系统会发送其他活动响应，除非已达到指定的最大数量。设置为 0 会禁用丢弃规则触发的活动响应，并禁用 **resp** 或 **react** 规则触发的其他活动响应。有关详细信息，请参阅第 29-3 页上的使用入侵丢弃规则启动活动响应和第 36-77 页上的使用规则关键字发起活动响应。

Minimum Response Seconds

指定等待 1 到 300 秒，直至出现**最大活动响应数**，然后在系统已启动活动响应的连接上的任何其他流量都会产生后续活动响应。

要使用丢弃规则启动活动响应，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Transport/Network Layer Preprocessor Settings** 旁边的编辑图标 ( )。

系统将显示 Transport/Network Layer Preprocessor Settings 弹出窗口。

步骤 5　您有以下选项：

- 为每个 TCP 连接指定介于 1 到 25 之间的 **Maximum Active Responses** 值。设置为 0 会禁用丢弃规则触发的活动响应，并禁用 **resp** 或 **react** 规则触发的其他活动响应。
- 为 **Minimum Response Seconds** 指定 1 到 300 之间的值，等待直至发生 **Maximum Active Responses** 为止，或者在系统已发起活动响应的连接上的任何其他流量产生后续活动响应为止。

步骤 6　点击 **OK**。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

故障排除：记录会话终止消息

许可证：保护

在故障排除呼叫期间，支持代表可能要求您配置系统在单个连接超过指定阈值时记录一条消息。更改此选项的设置会影响性能，并仅应在支持代表指导下进行。

要记录会话终止消息，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Transport/Network Layer Preprocessor Settings** 旁边的编辑图标 ( )。

系统将显示 Transport/Network Layer Preprocessor Settings 弹出窗口。

步骤 5　展开 **Troubleshooting Options**。

步骤 6　为 **Session Termination Logging Threshold** 指定字节数，从而当会话终止并且超出指定的数值时会记录消息。

1GB 的上限还受数据流处理分配的受管设备上的内存容量限制。

步骤 7　点击 **OK**。

您必须应用更改的访问控制策略以使更改生效；请参阅第 12-13 页上的应用访问控制策略。

验证校验和

许可证：保护

系统可验证所有协议级校验和，以确保接收完整的 IP、TCP、UDP 和 ICMP 传输，且基本级别的数据包在传输过程中未被篡改或意外修改。校验和使用算法来验证数据包中协议的完整性。如果系统计算所得的值与终端主机在数据包中写入的值相同，则数据包将被视为未更改。

禁用校验和验证可能使网络容易受到插入攻击。请注意，系统不生成校验和验证事件。在内联部署中，您可以将系统配置为会丢弃校验和无效的数据包。

要配置校验和，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Edit Policy 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Transport/Network Layer Preprocessors 中的 **Checksum Verification**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Checksum Verification 页面。页面底部的消息标识包含配置的策略层。有关详细信息，请参阅第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　在被动或内联部署中，可以将 Checksum Verification 部分中的任何选项设置为 **Enable** 或 **Disable**；在内联部署中，可以设置为 **Drop**：

- **ICMP Checksums**
- **IP Checksums**
- **TCP Checksums**
- **UDP Checksums**

请注意，要丢弃恶意数据包，除将选项设置为 **Drop** 以外，还必须在关联网络分析策略中启用 **Inline Mode**。有关详细信息，请参阅第 26-4 页上的允许预处理器影响内联部署中的流量。另请注意，在被动部署中或在分路模式下的内联部署中将这些选项设置为 **Drop** 与将其设置为 **Enabled** 的作用相同。

步骤 6　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

规范化内联流量

许可证：保护

内联规范化预处理器会将流量规范化，从而尽可能降低攻击者在内联部署中得以避开检测的可能性。如果在网络分析策略中启用内联规范化预处理器，系统测试以下两个条件以确保使用内联部署：

- 在策略中已启用 **Inline Mode**。请参阅第 26-4 页上的允许预处理器影响内联部署中的流量。
- 启用内联规范化的访问控制策略已应用到以内联方式部署或使用内联集的设备。

仅当两个条件均得到满足时，预处理器才会对指定流量进行规范化。

您可以指定 IPv4、IPv6、ICMPv4、ICMPv6 和 TCP 流量的任意组合的规范化。大多数规范化由内联规范化预处理器逐个数据包执行。但是，TCP 数据流预处理器处理大多数状态相关的数据包和数据流规范化，包括 TCP 负载规范化。

在数据包解码器进行解码后会立即执行内联规范化，直至其他预处理器进行处理。规范化从内数据包层继续执行到外数据包层。

内联规范化预处理器不会生成事件；它准备数据包以供内联部署中的其他预处理器和规则引擎使用。预处理器还有助于确保系统处理的数据包与网络中主机接收的数据包相同。

提示　在内联部署中，思科建议您配置已启用 **Normalize TCP Payload** 选项的内联规范化预处理器。在被动部署中，思科建议您配置自适应配置文件。有关详细信息，请参阅第 30-1 页上的调整被动部署中的预处理。

Minimum TTL

当 **Reset TTL** 大于或等于为此选项设置的值 （1 至 255）时，请指定以下设置：

- 启用 **Normalize IPv4** 后系统允许 IPv4 Time to Live (TTL) 字段使用的最小值；较小的值会导致将 TTL 的数据包值规范化为针对 **Reset TTL** 设置的值
- 启用 **Normalize IPv6** 后系统允许 IPv6 Hop Limit 字段使用的最小值；较小的值会导致将 TTL 的数据包值规范化为针对 **Reset TTL** 设置的值

此字段为空时，系统假设值为 1。

请注意，可以启用解码器规则类别中的以下规则来生成此选项的事件：

- 您可以启用规则 116:428，以在系统检测到 TTL 小于指定最小值的 IPv4 数据包时生成事件。
- 您可以启用规则 116:270，以在系统检测到跳数限制小于指定最小值的 IPv6 数据包时生成事件。

有关详细信息，请参阅第 29-17 页上的配置数据包解码中的 **Detect Protocol Header Anomalies** 选项。

Reset TTL

如果设置为大于或等于 **Minimum TTL** 的值 （1 到 255），请规范化以下字段：

- IPv4 TTL 字段 （如果启用了 **Normalize IPv4**）
- IPv6 Hop Limit 字段 （如果启用了 **Normalize IPv6**）

当数据包值小于 **Minimum TTL** 时，系统会通过将其 TTL 或 Hop Limit 值更改为针对此选项设置的值来规范化数据包。将此选项设置为值 0 或任何小于 **Minimum TTL** 的值会禁用此选项。此字段为空时，系统假设值为 0。

Normalize IPv4

启用 IPv4 流量规范化。此选项处于启用状态并且为 **Reset TTL** 设置的值会启用 TTL 规范化时，系统还会根据需要规范化 TTL 字段。启用此选项后，还可以启用 **Normalize Don't Fragment Bits** 和 **Normalize Reserved Bits**。

启用此选项时，系统执行以下基本 IPv4 规范化：

- 将具有多余负载的数据包截断至 IP 报头中指定的数据报长度
- 清除 Differentiated Services (DS) 字段 （以前称为 Type of Service (TOS) 字段）
- 将所有选项八位元设置为 1 (No Operation)

Normalize Don't Fragment Bit

清除 IPv4 Flags 报头字段的 1 位 Don't Fragment 子字段。通过启用此选项，下游路由器可在必要时对数据包进行分片而不是将其丢弃；启用此选项还可以根据要丢弃的构造数据包来防止躲避检测。必须启用 **Normalize IPv4** 后才可以选择此选项。

Normalize Reserved Bit

清除 IPv4 Flags 报头字段的 1 位 Reserved 子字段。通常会启用此选项。必须启用 **Normalize IPv4** 后才可以选择此选项。

Normalize TOS Bit

清除一个字节的 Differentiated Services 字段（以前称为 Type of Service）。必须启用 **Normalize IPv4** 后才可以选择此选项。

Normalize Excess Payload

将具有多余负载的数据包截断至 IP 报头中指定的数据报长度加上第 2 层 （例如以太网）报头，但是不截断为小于最小帧长度。必须启用 **Normalize IPv4** 后才可以选择此选项。

Normalize IPv6

将 Hop-by-Hop Options 和 Destination Options 扩展报头中的所有 Option Type 字段设置为 00（跳过并继续处理）。此选项处于启用状态并且为 **Reset TTL** 设置的值会启用跳数限制规范化时，系统还会根据需要规范化 Hop Limit 字段。

Normalize ICMPv4

清除 ICMPv4 流量中 Echo (Request) 和 Echo Reply 消息内的 8 位 Code 字段。

Normalize ICMPv6

清除 ICMPv6 流量中 Echo (Request) 和 Echo Reply 消息内的 8 位 Code 字段。

Normalize/Clear Reserved Bits

清除 TCP 报头中的保留位。

Normalize/Clear Option Padding Bytes

清除所有 TCP 选项填充字节

Clear Urgent Pointer if URG=0

如果未设置紧急 (URG) 控制位，则清除 16 位 TCP 报头 Urgent Pointer 字段

Clear Urgent Pointer/URG on Empty Payload

如果没有负载，则清除 TCP 报头的 Urgent Pointer 字段和 URG 控制位。

Clear URG if Urgent Pointer is Not Set

如果未设置紧急指针，则清除 TCP 报头 URG 控制位。

Normalize Urgent Pointer

如果指针大于负载长度，则将两个字节的 TCP 报头 Urgent Pointer 字段设置为负载长度。

Normalize TCP Payload

启用 TCP Data 字段的规范化以确保重传数据的一致性。无法正确重组的所有数据段都会被丢弃。

Remove Data on SYN

如果 TCP 操作系统策略**不是** Mac OS，则会移除同步 (SYN) 数据包中的数据。

此选项还会禁用规则 129:2 的事件生成。

Remove Data on RST

从 TCP 重置 (RST) 数据包中移除所有数据。

Trim Data to Window

将 TCP Data 字段调整为在 Window 字段中指定的大小。

Trim Data to MSS

如果负载长度大于 MSS，则将 TCP Data 字段调整为最大分段大小 (MSS)

Block Unrecoverable TCP Header Anomalies

启用此选项时，系统阻止异常 TCP 数据包，这些数据包在规范化的情况下会无效，并可能受到接收主机的阻止。例如，系统阻止已建立的会话后传输的任何 SYN 数据包。

系统还会丢弃符合下列任何 TCP 数据流预处理器规则的任何数据包 （无论是否启用了规则）：

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 到 129:19

Total Blocked Packets 性能图跟踪内联部署中阻止的数据包的数量，并且，在被动部署和轻触模式下的内联部署中，跟踪在内联部署中已阻止的数量。有关详细信息，请参阅第 41-4 页上的生成入侵事件性能统计信息图表。

Explicit Congestion Notification

对显式堵塞通知 (ECN) 标志启用逐个数据包或逐条数据流规范化，如下所示：

- 无论协商与否，都选择 **Packet** 以数据包为单位清除 ECN 标记
- 如果未协商 ECN 使用，则选择 **Stream** 以数据流为单位清除 ECN 标记

如果选择 **Stream**，您还必须确保启用 TCP 数据流预处理器的 **Require TCP 3-Way Handshake** 选项以进行此规范化；有关详细信息，请参阅第 29-20 页上的选择 TCP 策略选项。

Allow These TCP Options

禁用您在流量中允许的特定 TCP 选项的规范化。

系统不对您明确允许的选项进行规范化。系统会通过将您未明确允许的选项设置为 No Operation （TCP 选项 1）来规范化这些选项。

系统始终允许 Maximum Segment Size (MSS)、 Window Scale 和 Time Stamp TCP 选项，因为这些选项常用于实现最佳 TCP 性能。无论 **Allow These TCP Options** 的配置如何，系统都会规范化这些常用选项。系统不会自动允许其他不太常用的选项。

您可以通过配置选项关键字和/或选项编号的逗号分隔列表来允许特定选项，如下例所示：

```
sack, echo, 19
```

指定选项关键字等同于指定与该关键字相关的一个或多个 TCP 选项的编号。例如，指定 `sack` 等同于指定 TCP 选项 4 (Selective Acknowledgement Permitted) 和选项 5 (Selective Acknowledgement)。选项关键字不区分大小写。

您还可以指定 `any`，这样将会允许所有 TCP 选项并有效地禁用所有 TCP 选项的规范化。

下表总结了如何指定要允许的 TCP 选项。如果将字段留空，则系统仅允许 MSS、 Window Scale 和 Time Stamp 选项。

可指定的内容	以允许.....
sack	TCP 选项 4 (Selective Acknowledgement Permitted) 和选项 5 (Selective Acknowledgement)
echo	TCP 选项 6 (Echo Request) 和选项 7 (Echo Reply)
partial_order	TCP 选项 9 (Partial Order Connection Permitted) 和选项 10 (Partial Order Service Profile)
conn_count	TCP 连接计数选项 11 (CC)、选项 12 (CC.New) 和选项 13 (CC.Echo)
alt_checksum	TCP 选项 14 (Alternate Checksum Request) 和选项 15 (Alternate Checksum)
md5	TCP 选项 19 (MD5 Signature)
选项编号 （2 至 255）	特定选项，包括没有关键字的选项
any	所有 TCP 选项；此设置会有效地禁用 TCP 选项规范化

当没有为此选项指定`any`，规范化包括以下内容：

- 除 MSS、 Window Scale、 Time Stamp 及任何明确允许的选项以外，所有选项字节都设置为 No Operation （TCP 选项 1）
- 如果时间戳存在但无效，或者有效但未协商，则将时间戳八位元设置为 No Operation
- 如果时间戳已协商但不存在，则阻止数据包
- 如果未设置 Acknowledgement (ACK) 控制位，则清除 Time Stamp Echo Reply (TSecr) 选项字段
- 如果未设置 SYN 控制位，则将 MSS 和 Window Scale 选项设置为 No Operation （TCP 选项 1）

要配置内联规范化预处理器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Edit Policy 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　根据在 Transport/Network Layer Preprocessors 下是否已启用 **Inline Normalization**，有两个选项：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Inline Normalization 页面。页面底部消息会标识出包含配置的策略层。有关详细信息，请参阅第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　您可以设置第 29-6 页上的规范化内联流量中所述的任何选项。

步骤 6　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

对 IP 数据包进行分片重组

许可证：保护

由于 IP 数据报大于最大传输单位 (MTU) 而将其分为两个或多个更小的 IP 数据报，这个过程即为数据报*分片*。单个 IP 数据报片段可能未包含足够的信息来识别隐藏攻击。攻击者可能尝试通过将攻击数据传输到分片数据包中来躲避检测。规则引擎对分片的 IP 数据报执行规则之前， IP 分片重组预处理器会重组这些数据报，以便规则可以更适当地识别这些数据包中的攻击。如果分片的数据报无法重组，则不对其执行规则。

请注意，如果您希望 IP 分片重组预处理器规则生成事件，则必须启用这些规则，其生成器 ID (GID) 为 123。有关详细信息，请参阅第 32-18 页上的设置规则状态。

有关详细信息，请参阅以下各节：

了解 IP 分片漏洞

许可证：保护

启用 IP 分片重组可以帮助您检测针对网络上主机的攻击 （例如泪滴 [teardrop] 攻击）和针对系统本身的资源消耗攻击 （例如 Jolt2 攻击）。

泪滴攻击利用某些操作系统中在尝试重组重叠 IP 片段时会导致这些操作系统崩溃的漏洞。 IP 分片重组预处理器在被启用并配置为识别重叠片段之后，会执行此操作。 IP 分片重组预处理器会检测重叠片段攻击 （例如泪滴攻击）中的第一批数据包，但对于同一攻击不会检测后续数据包。

Jolt2 攻击会发送同一分片的 IP 数据包的大量副本，以尝试过度使用 IP 分片重组器并导致拒绝服务攻击。内存使用上限会中断此攻击以及 IP 分片重组预处理器中的类似攻击，并在全面检查基础上注重系统自我保护。这样，系统不会因攻击而崩溃，可保持运行，并继续检查网络流量。

不同的操作系统以不同方式重组分片数据包。可以确定主机运行的操作系统的攻击者还可以对恶意数据包进行分片，以便目标主机以特定方式对这些数据包进行重组。由于系统不知道受监控网络上的主机运行的操作系统，因此预处理器可能会不正确地重组和检查数据包，致使漏洞未经检测即通过。要缓解这种攻击，您可以配置分片重组预处理器，使其会针对网络中的每个主机使用适当方法对数据包进行分片重组。有关详细信息，请参阅第 29-11 页上的基于目标的分片重组策略。

请注意，您也可以使用自适应配置文件，通过数据包中目标主机的主机操作系统信息来为 IP 分片重组预处理器动态选择基于目标的策略。有关详细信息，请参阅第 30-1 页上的调整被动部署中的预处理。

基于目标的分片重组策略

许可证：保护

主机的操作系统使用三个条件来确定重组数据包时支持哪些数据包片段：操作系统接收片段的顺序；片段的偏移量 （片段的距离，以字节为单位，从数据包开头起算）；以及片段相对于重叠片段的开始和结束位置。虽然每个操作系统都使用这些条件，但是不同的操作系统在重组分片数据包时支持不同的片段。因此，网络中具有不同操作系统的两个主机可能会以完全不同的方式重组同一组重叠片段。

攻击者 （了解其中一个主机的操作系统）可能会尝试通过发送隐藏在重叠数据包片段中的恶意内容来逃避检测并利用该主机。该数据包经过重组和检查后看似无害，但是由目标主机进行重组后则会包含恶意的漏洞。但是，如果将 IP 分片重组预处理器配置为可感知受监控网络段上运行的操作系统，则它会以与目标主机相同的方式重组分片，从而识别攻击。

根据目标主机的操作系统，可以将 IP 分片重组预处理器配置为使用七个分片重组策略之一。下表列出了这七个策略以及使用每个策略的操作系统。First 和 Last 这两个策略名称反映这些策略是否支持原始或后续重叠数据包。

表 29-1　　基于目标的分片重组策略

策略	操作系统
BSD	AIX
	FreeBSD
	IRIX
	VAX/VMS
BSD-right	HP JetDirect

表 29-1　基于目标的分片重组策略 （续）

策略	操作系统
首页	Mac OS HP-UX
Linux	Linux OpenBSD
Last	Cisco IOS
Solaris	SunOS
Windows	Windows

选择分片重组选项

许可证：保护

您可以选择简单启用或禁用 IP 分片重组；但是，思科建议您以更精细的级别指定已启用的 IP 分片重组预处理器的行为。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

您可以配置全局 **Preallocated Fragments** 选项：

Preallocated Fragments

预处理器一次可以处理的最大单个片段数量。指定要预分配的片段节点的数量会启用静态内存分配。

注意事项

处理单个片段会使用大约 1550 字节的内存。如果预处理器需要比受管设备的预定允许内存限制更多的内存来处理单个片段，则设备的内存限制优先。

您可以为每个 IP 分片重组策略配置以下选项：

Networks

要对其应用分片重组策略的一个或多个主机的 IP 地址。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。您可以指定总共最多 255 个配置文件 （包括默认策略）。有关在 FireSIGHT 系统中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-16 页上的 IP 地址约定。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any` （例如， 0.0.0.0/0 或 ::/0）。

另请注意，为了让基于目标的策略处理流量，您标识的网络必须匹配您在其中配置该策略的网络分析策略处理的网络、区域和 VLAN 或是其子集。有关详细信息，请参阅第 25-2 页上的使用网络分析策略自定义预处理。

Policy

要为受监控网段上的主机组使用的分片重组策略。有七个策略可供选择：BSD、 BSD-Right、First、 Linux、 Last、 Solaris 和 Windows。有关这些策略的详细信息，请参阅第 29-11 页上的基于目标的分片重组策略。

Timeout

指定预处理器引擎在重组分片数据包时可用的最长时间 （以秒为单位）。如果在指定的时间段内无法重组数据包，则预处理器引擎会停止尝试重组数据包并丢弃接收到的片段。

Minimum TTL

指定数据包可具有的可接受最小 TTL 值。此选项检测基于 TTL 的插入攻击。

您可以启用规则 123:1 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

Detect Anomalies

确定分片问题，例如重叠片段。

您可以启用以下规则来生成此选项的事件：

- 123:1 至 123:4
- 123:5 （BSD 策略）
- 123:6 至 123:8

Overlap Limit

指定在检测到某会话中存在所配置数量 （介于 0 [无限制] 和 255 之间）的重叠片段时，针对该会话的分片重组将会停止。必须启用 **Detect Anomalies** 后才可以配置此选项。不指定值将会禁用此选项。

您可以启用规则 123:12 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

Minimum Fragment Size

指定在检测到小于配置数量 （介于 0 [无限制] 和 255 字节之间）的非最后一个片段时，数据包将被视为恶意数据包。必须启用 **Detect Anomalies** 后才可以配置此选项。不指定值将会禁用此选项。

您可以启用规则 123:13 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

配置 IP 分片重组

许可证：保护

您可以使用以下步骤配置 IP 分片重组预处理器。有关 IP 分片重组预处理器配置选项的详细信息，请参阅第 29-12 页上的选择分片重组选项。

要配置 IP 分片重组，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Edit Policy 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　根据是否已启用 Transport/Network Layer Preprocessors 下的 **IP Defragmentation**，有两个选项：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 IP Defragmentation 页面。页面底部消息会标识出包含配置的策略层。有关详细信息，请参阅第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　或者，可以修改 Global Settings 页面区域中的 **Preallocated Fragments** 设置。

步骤 6　此时您有两种选择：

- 添加新的基于目标的策略。点击页面左侧 **Servers** 旁边的添加图标 ( )。系统将显示 Add Target 弹出窗口。在 **Host Address** 字段中指定一个或多个 IP 地址，然后点击 **OK**。

  可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。您可以创建总共 255 个基于目标的策略（包括默认策略）。有关在 FireSIGHT 系统中使用 IP 地址块的信息，请参阅第 1-16 页上的 IP 地址约定。

  请注意，为使基于目标的策略可以处理流量，您识别的网络必须与由网络分析策略（其中已配置该基于目标的策略）处理的网络、区域和 VLAN 匹配或者是其子集。有关详细信息，请参阅第 25-2 页上的使用网络分析策略自定义预处理。

  新条目将出现在页面左侧的目标列表中，突出显示以表明其已被选定；Configuration 部分会进行更新，以反映所添加的策略的当前配置。

- 修改现有基于目标的策略的设置。点击您在页面左侧 **Hosts** 中添加的策略的配置地址，或者点击 **default**。

  所选项目将会突出显示，并且 Configuration 部分会进行更新以显示所选策略的当前配置。要删除现有的基于目标的策略，请点击要删除的策略旁边的删除图标 ( )。

步骤 7　或者，您可以修改 Configuration 页面区域中的任意选项。

步骤 8　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

了解数据包解码

许可证：保护

在将捕获的数据包发送到预处理器之前，系统首先会将数据包发送到数据包解码器。数据包解码器将数据包报头和负载转换为便于预处理器和规则引擎使用的格式。从数据链路层开始，每个堆栈层依次进行解码，并继续至网络层和传输层。

请注意，如果您希望数据包解码器规则生成事件，则必须启用这些规则，其生成器 ID (GID) 为 116。有关详细信息，请参阅第 32-18 页上的设置规则状态。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

解码 GTP 数据信道

解码封装的 GTP（通用分组无线业务 [GPRS] 隧道协议）数据通道。默认情况下，解码器会解码端口 3386 上的版本 0 数据和端口 2152 上的版本 1 数据。您可以使用 `GTP_PORTS` 默认变量修改用于识别封装的 GTP 流量的端口。有关详细信息，请参阅第 3-16 页上的优化预定义默认变量。

您可以启用规则 116:297 和 116:298 来生成此选项的事件。

检测非标准端口上的 Terado

检查除端口 3544 以外的其他 UDP 端口上识别的 IPv6 流量的 Teredo 隧道。

系统始终检查存在的 IPv6 流量。默认情况下，IPv6 检查包括 4in6、6in4、6to4 和 6in6 隧道方案，如果 UDP 报头指定端口 3544，还包括 Teredo 隧道。

在 IPv4 网络中，IPv4 主机可以使用 Teredo 协议通过 IPv4 网络地址转换 (NAT) 设备传输 IPv6 流量。 Teredo 将 IPv6 数据包封装在 IPv4 UDP 数据报中，以允许在 IPv4 NAT 设备后面进行 IPv6 连接。系统通常使用 UDP 端口 3544 识别 Teredo 流量。但是，攻击者可能会使用非标准端口来尝试避开检测。您可以启用 **Detect Teredo on Non-Standard Ports** 来促使系统检查 Teredo 隧道的所有 UDP 负载。

Teredo 解码仅发生在第一个 UDP 报头上，并且仅当 IPv4 用于外部网络层时才会发生。如果由于 IPv6 数据中封装的 UDP 数据而在 Teredo IPv6 层之后出现第二个 UDP 层，则规则引擎会使用 UDP 入侵规则对内部和外部 UDP 层均进行分析。

请注意，**policy-other** 规则类别中的入侵规则 12065、12066、12067 和 12068 会检测 Teredo 流量，但不对这些流量进行解码。您可以根据需要在内联部署中使用这些规则丢弃 Teredo 流量；但是，启用 **Detect Teredo on Non-Standard Ports** 时，应确保这些规则处于禁用状态或者设置为生成事件而不丢弃流量。有关详细信息，请参阅第 32-9 页上的过滤入侵策略中的规则和第 32-18 页上的设置规则状态。

检测过大长度值

在数据包报头指定的数据包长度大于实际数据包长度时进行检测。

您可以启用规则 116:6、 116:47、 116:97 和 116:275 来生成此选项的事件。

检测无效 IP 选项

检测无效 IP 报头选项以识别使用无效 IP 选项的漏洞。例如，存在针对防火墙的拒绝服务攻击，该攻击导致系统冻结。防火墙尝试解析无效的 Timestamp 和 Security IP 选项且未能检查到零长度，导致无法恢复的无限循环。规则引擎会识别零长度选项并提供可用于缓解对防火墙的攻击的信息。

您可以启用规则 116:4 和 116:5 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

检测试验性 TCP 选项

检测具有试验性 TCP 选项的 TCP 报头。下表介绍了这些选项。

TCP 选项	说明
9	允许的偏序连接
10	偏序服务配置文件
14	替代校验和请求
15	替代校验和数据
18	尾部校验和
20	空间通信协议标准 (SCPS)
21	选择性否定确认 (SCPS)
22	记录边界 (SCPS)

TCP 选项	说明
23	损坏 (SPCS)
24	SNAP
26	TCP 压缩过滤器

由于这些是试验性选项，因此，某些系统未对其进行说明，可能容易产生漏洞。

注　除上表中列出的试验性选项外，系统还将选项编号大于 26 的任何 TCP 选项视为试验性选项。

您可以启用规则 116:58 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

检测过时 TCP 选项

检测具有过时 TCP 选项的 TCP 报头。由于这些是过时选项，因此，某些系统未对其进行说明，可能容易产生漏洞。下表介绍了这些选项。

TCP 选项	说明
6	回显
7	回应应答
16	Skeeter
17	Bubba
19	MD5 签名
25	未分配

您可以启用规则 116:57 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

检测 T/TCP

检测带有 CC.ECHO 选项的 TCP 报头。CC.ECHO 选项确认使用的是事务 TCP (T/TCP)。由于 T/TCP 报头选项未广泛使用，因此，某些系统未对其进行说明，可能容易产生漏洞。

您可以启用规则 116:56 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

检测其他 TCP 选项

检测具有其他 TCP 解码事件选项未检测到的无效 TCP 选项的 TCP 报头。例如，此选项检测长度不正确或者选项数据长度超过 TCP 报头范围的 TCP 选项。

您可以启用规则 116:54、 116:55 和 116:59 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

检测协议报头异常

检测更具体的 IP 和 TCP 解码器选项未检测到的其他解码错误。例如，解码器可能会检测到格式错误的数据链路协议报头。

要生成此选项的事件，可以启用除了与其他数据包解码器选项专门相关的规则以外的任何数据包解码器规则。有关详细信息，请参阅第 32-18 页上的设置规则状态

请注意，以下规则生成异常 IPv6 流量触发的事件：116:270 至 116:274、116:275 至 116:283、116:291、116:292、116:295、116:296、116:406、116:458、116:460、116:461。

另请注意与内联规范化预处理器的 **Minimum TTL** 选项相关的以下规则：

- 您可以启用规则 116:428，以在系统检测到 TTL 小于指定最小值的 IPv4 数据包时生成事件。
- 您可以启用规则 116:270，以在系统检测到跳数限制小于指定最小值的 IPv6 数据包时生成事件。

有关详细信息，请参阅第 29-6 页上的规范化内联流量中的内联规范化 **Minimum TTL** 选项。

配置数据包解码

许可证：保护

您可以在 Packet Decoding 配置页面上配置数据包解码。有关数据包解码配置选项的详细信息，请参阅第 29-14 页上的了解数据包解码。

要配置数据包解码，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Edit Policy 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Transport/Network Layer Preprocessors 中的 **Checksum Verification**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Packet Decoding 页面。页面底部消息会标识出包含配置的策略层。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改

步骤 5　可以启用或禁用 Packet Decoding 页面上的任何检测选项。有关详细信息，请参阅第 29-14 页上的了解数据包解码。

步骤 6　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

使用 TCP 数据流预处理

许可证：保护

TCP 协议定义连接可以处于的各种状态。每个 TCP 连接通过源 IP 地址和目标 IP 地址以及源端口和目标端口进行识别。 TCP 一次仅允许存在一个具有相同连接参数值的连接。

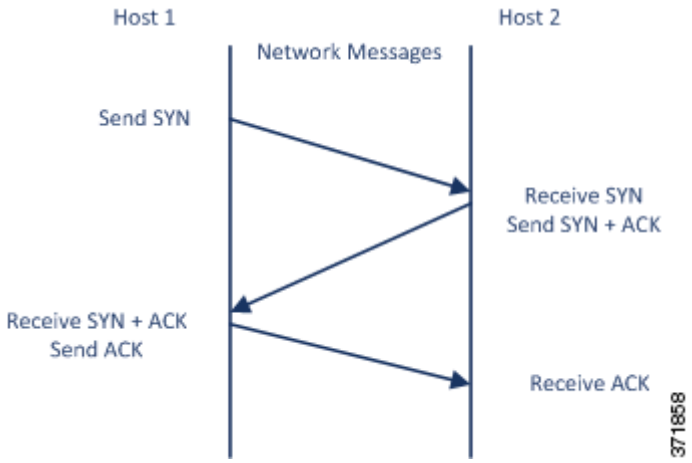
请注意，如果您希望 TCP 数据流预处理器规则生成事件，则必须启用这些规则，其生成器 ID (GID) 为 129。有关详细信息，请参阅第 32-18 页上的设置规则状态。

有关详细信息，请参阅以下各节：

了解与状态相关的 TCP 漏洞

许可证：保护

如果向入侵规则添加带有 `established` 参数的 `flow` 关键字，则入侵规则引擎会在状态模式下检查与规则和流指令匹配的数据包。状态模式仅评估通过客户端与服务器之间的合法三次握手建立的 TCP 会话所包含的流量。下图说明三次握手。



您可以配置系统，以便预处理器对无法识别为已建立的 TCP 会话的一部分的任何 TCP 流量进行检测；但是，对于典型使用不建议此操作，因为事件会使系统迅速过载且不会提供有意义的数据。

stick 和 snot 之类的攻击使用系统的广泛的规则集和数据包检测自身。这些工具根据基于 Snort 的入侵规则生成数据包，并通过网络发送这些数据包。如果您的规则不包括用于为状态检查配置规则的 `flow` 或 `flowbits` 关键字，则每个数据包将触发规则，进而导致系统过载。您可以通过状态检查来忽略这些数据包，因为它们不是已建立的 TCP 会话的一部分，而且不提供有意义的信息。执行状态检查时，规则引擎仅检测属于已建立的 TCP 会话的一部分的那些攻击，从而使分析人员关注这些攻击而不是由 stick 或 snot 攻击导致的事件量。

选择 TCP 全局选项

许可证：保护

TCP 数据流预处理器有一个控制 TCP 数据流预处理器如何发挥功能的全局选项。

没有预处理器规则与此选项关联。

Packet Type Performance Boost

支持忽略已启用规则中未指定的所有端口和应用协议的 TCP 流量，但在源端口和目标端口均设置为 `any` 的 TCP 规则具有 `flow` 或 `flowbits` 选项时除外。这种性能改进可能会导致未能检测出某些攻击。

了解基于目标的 TCP 策略

许可证：保护

不同操作系统以不同方法实施 TCP。例如， Windows 和其他一些操作系统需要 TCP 重置段以具有精确的 TCP 序列号来重置会话，而 Linux 和其他操作系统则允许使用一系列序列号。在本示例中，数据流预处理器必须明确了解目标主机会如何根据序列号对重置作出响应。仅当目标主机认为重置有效时，数据流预处理器才会停止跟踪会话，因此，攻击在预处理器停止检查数据流后无法通过发送数据包来躲避检测。在 TCP 实施中的其他变化包括操作系统是否采用 TCP 时间戳选项，并且在采用时如何处理时时间戳，以及操作系统接受还是忽略 SYN 数据包中的数据等等方面。

不同操作系统也以不同方式重组重叠的 TCP 数据段。重叠的 TCP 数据段可能会反映未确认的 TCP 流量的正常重传。它们也可能表示攻击者 （了解其中一个主机的操作系统）尝试通过发送隐藏在重叠数据段中的恶意内容来躲避检测并利用该主机。但是，您可以将数据流预处理器配置为可感知受监控网段上运行的操作系统，使其以与目标主机相同的方式重组数据段，从而识别攻击。

您可以创建一个或多个 TCP 策略，以根据受监控网段上的不同操作系统定制 TCP 数据流检查和重组。对于每个策略，可识别 13 个操作系统策略之一。您根据需要使用尽可能多的 TCP 策略将每个 TCP 策略绑定到特定 IP 地址或地址块，以识别使用其他操作系统的任意或所有主机。默认 TCP 策略适用于在任何其他 TCP 策略中未识别的受监控网络上的任何主机，因此无需为默认 TCP 策略指定 IP 地址、 CIDR 块或前缀长度。

请注意，您也可以使用自适应配置文件，通过数据包中目标主机的主机操作系统信息来为 TCP 数据流预处理器动态选择基于目标的策略。有关详细信息，请参阅第 30-1 页上的调整被动部署中的预处理。

下表列出了操作系统策略以及使用每个策略的主机操作系统。

表 29-2　　TCP 操作系统策略

策略	操作系统
首页	未知 OS
Last	Cisco IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 内核 Linux 2.6 内核
旧 Linux	Linux 2.2 及更低版本的内核

表 29-2　　TCP 操作系统策略 （续）

策略	操作系统
Windows	Windows 98
	Windows NT
	Windows 2000
	Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS
	SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 及更高版本
HPUX 10	HP-UX 10.2 及更低版本
Mac OS	Mac OS 10 (Mac OS X)

提示 当您不知道主机操作系统时， First 操作系统策略可以提供一些保护。但是，它可能会导致未能检测出某些攻击。如果您知道操作系统，则应该编辑策略以指定正确的操作系统。

选择 TCP 策略选项

许可证：保护

以下列表介绍可设置以识别和控制 TCP 数据流预处理器检查的 TCP 流量的选项。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

Network

指定要对其应用 TCP 数据流重组策略的主机 IP 地址。

可以指定单个 IP 地址或地址块。总共最多可以指定 255 个配置文件（包括默认策略）。有关在 FireSIGHT 系统中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-16 页上的 IP 地址约定。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如， 0.0.0.0/0 或 ::/0）。

另请注意，为了让基于目标的策略处理流量，您识别的网络必须匹配您在其中配置该策略的网络分析策略处理的网络、区域和 VLAN 或是其子集。有关详细信息，请参阅第 25-2 页上的使用网络分析策略自定义预处理。

策略

识别一个或多个目标主机的 TCP 策略操作系统。如果选择除 **Mac OS** 以外的其他策略，则系统会从同步 (SYN) 数据包中删除数据并禁用规则 129:2 的事件生成。

有关详细信息，请参阅第 29-19 页上的了解基于目标的 TCP 策略。

Timeout

规则引擎在状态表中保持数据流处于非活动状态的秒数 （介于 1 和 86400 之间）。如果数据流在指定时间内未重组，则入侵规则引擎会将其从状态表中删除。

注 如果受管设备部署在网络流量可能达到设备的带宽限制的网段上，则应该考虑将该值设置为较高的值 （例如 600 秒），以降低处理开销。

Maximum TCP Window

指定由接收主机指定的所允许的最大 TCP 窗口大小（1 至 1073725440 字节）。值设置为 0 会禁用检查 TCP 窗口大小。

注意事项 上限是 RFC 允许的最大窗口大小，旨在防止攻击者躲避检测；但是，设置明显过大的最大窗口大小可能导致自愿接受的拒绝服务。

您可以启用规则 129:6 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

Overlap Limit

指定在检测到某会话中存在所配置数量 （介于 0 [无限制] 和 255 之间）的重叠分段时，针对该会话的分段重组将会停止，并且，如果 **Stateful Inspection Anomalies** 以及随附的预处理器规则均处于启用状态，将会生成事件。

您可以启用规则 129:7 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

Flush Factor

在内联部署中，指定在经过所配置数量 （介于 1 和 2048 之间）的大小未减小的分段后检测到大小减小的分段时，系统会刷新为进行检测而累积的分段数据。将该值设置为 0 会禁用此分段模式的检测，这可能意味着请求或响应结束。请注意，为了使此选项有效，必须启用 Inline Normalization **Normalize TCP Payload** 选项。有关详细信息，请参阅第 29-6 页上的规范化内联流量。

Stateful Inspection Anomalies

检测 TCP 堆栈中的异常行为。启用随附的预处理器规则后，如果 TCP/IP 堆栈编写得不好，可能会生成许多事件。

您可以启用以下规则来生成此选项的事件：

- 129:1 至 129:5
- 129:6 （仅适用于 Mac OS）
- 129:8 至 129:11
- 129:13 至 129:19

有关详细信息，请参阅第 32-18 页上的设置规则状态。

TCP Session Hijacking

通过针对会话上接收到的后续数据包验证三次握手期间从 TCP 连接两端检测到的硬件 (MAC) 地址来检测 TCP 会话劫持。当一端或另一端的 MAC 地址不匹配时，如果启用了 **Stateful Inspection Anomalies** 以及两个对应的预处理器规则之一，系统会生成事件。

您可以启用规则 129:9 和 129:10 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

Consecutive Small Segments

启用 **Stateful Inspection Anomalies** 后，可指定允许的连续 TCP 小分段的最大数量（1 至 2048）。值设置为 0 会禁止连续小分段。

此选项必须与 **Small Segment Size** 选项一起进行设置；您可以同时禁用这两个选项或者将它们都设置为非零值。请注意，在无干预确认的情况下接收多达 2000 个连续分段，即使每个分段长度为 1 字节，分段数量也会远远超出您通常的预期。

您可以启用规则 129:12 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

Small Segment Size

启用 **Stateful Inspection Anomalies** 后，可指定被视为小分段的 TCP 分段大小（1 至 2048 字节）。值设置为 0 会禁止指定小分段的大小。

此选项必须与 **Consecutive Small Segments** 选项一起进行设置；您可以同时禁用这两个选项或者将它们都设置为非零值。请注意，一个 2048 字节的 TCP 分段大于普通的 1500 字节的以太网帧。

Ports Ignoring Small Segments

启用 **Stateful Inspection Anomalies**、**Consecutive Small Segments** 和 **Small Segment Size** 后，您或者可以指定一个或多个会忽略小 TCP 分段检测的端口的逗号分隔列表。将此选项留空表示未忽略任何端口。

您可以向列表中添加任何端口，但是列表仅影响 TCP 策略中的某个 **Perform Stream Reassembly on port** 列表中指定的端口。

Require TCP 3-Way Handshake

指定仅在 TCP 三次握手完成后，会话才被视为已建立的会话。禁用此选项可提高性能，防御 SYN 泛洪攻击，并允许在部分异步环境中操作。启用此选项可避免尝试通过发送不属于已建立的 TCP 会话的信息来生成误报的攻击。

您可以启用规则 129:20 来生成此选项的事件。有关详细信息，请参阅第 32-18 页上的设置规则状态。

3-Way Handshake Timeout

指定启用 **Require TCP 3-Way Handshake** 后必须允许用于完成握手的时间（0 [无限制] 至 86400 秒 [24 小时]）。必须启用 **Require TCP 3-Way Handshake** 后才能修改此选项的值。

Packet Size Performance Boost

将预处理器设置为在重组缓冲区中不对大数据包进行排队。这种性能改进可能会导致未能检测出某些攻击。禁用此选项可防止使用 1 到 20 字节的小数据包尝试躲避检测。当您肯定所有流量都由超大数据包组成并因此无此类攻击时，可启用此选项。

Legacy Reassembly

重组数据包时，将数据流预处理器设置为模拟废弃的数据流 4 预处理器，借此可以将该数据流预处理器重组的事件与基于数据流 4 预处理器重组的相同数据流的事件相比较。

Asynchronous Network

指定受监控网络是否为异步网络，即，系统只能看到一半流量的网络。启用此选项后，系统不重组 TCP 数据流来提高性能。

Perform Stream Reassembly on Client Ports, Server Ports, Both Ports

为客户端端口和/或服务器端口指定用于识别要重组的数据流预处理器流量的端口的逗号分隔列表。请参阅第 29-23 页上的选择数据流重组选项。

Perform Stream Reassembly on Client Services, Server Services, Both Services

为客户端服务和/或服务器服务指定用于识别要重组的数据流预处理器流量的服务。请参阅第 29-23 页上的选择数据流重组选项。

Troubleshooting Options: Maximum Queued Bytes

支持代表在故障排除呼叫期间可能要求您指定可以在 TCP 连接的一端排队的数据量。值 0 表示无限字节数。

注意事项 更改此故障排除选项的设置会影响性能，并仅应在支持代表指导下进行。

Troubleshooting Options: Maximum Queued Segments

支持代表在故障排除呼叫期间可能要求您指定可以在 TCP 连接的一端排队的数据分段的最大字节数。值 0 表示无限的数据段字节数。

注意事项 更改此故障排除选项的设置会影响性能，并仅应在支持代表指导下进行。

重组 TCP 数据流

许可证：保护

数据流预处理器收集和重组属于 TCP 会话的服务器到客户端通信数据流和/或客户端到服务器通信数据流的一部分的所有数据包。这允许规则引擎将数据流作为单个已重组实体进行检查，而不是仅检查属于指定数据流的一部分的个别数据包。

有关详细信息，请参阅以下各节：

- 第 29-23 页上的了解基于数据流的攻击
- 第 29-23 页上的选择数据流重组选项

了解基于数据流的攻击

许可证：保护

数据流重组允许规则引擎识别基于数据流的攻击，在检查个别数据包时它可能无法检测此类攻击。您可以根据网络需要指定规则引擎重组哪些通信数据流。例如，在监控网络服务器上的流量时，您可能只希望检查客户端流量，因为您不太可能从自己的网络服务器接收到恶意流量。

选择数据流重组选项

许可证：保护

在每个 TCP 策略中，您可以指定用于识别要重组的数据流预处理器流量的端口的逗号分隔列表。启用自适应配置文件后，您还可以列出用于识别要重组的流量的服务 （以替代端口或端口组合的形式）。有关启用和使用自适应配置文件的详细信息，请参阅第 30-1 页上的调整被动部署中的预处理。

您可以指定端口和/或服务。您可以为客户端端口和/或服务器端口的任意组合指定单独的端口列表。您还可以为客户端服务和/或服务器服务指定单独的服务列表。例如，假设您要重组以下内容：

- 来自客户端的 SMTP （端口 25）流量
- FTP 服务器响应 （端口 21）
- 两个方向的 telnet （端口 23）流量

您可以配置以下内容：

- 对于客户端端口，指定 `23 和 25`
- 对于服务器端口，指定 `21 和 23`

或者，您可以配置以下内容：

- 对于客户端端口，指定 `25`
- 对于服务器端口，指定 `21`
- 对于客户端端口和服务器端口，指定 `23`

此外，请参考以下示例，该示例将端口和服务进行组合，并在启用自适应配置文件后有效：

- 对于客户端端口，指定 `23`
- 对于客户端服务，指定 `smtp`
- 对于服务器端口，指定 `21`
- 对于服务器服务，指定 `telnet`

取消一个端口 （例如，`!80`）可通过阻止 TCP 数据流预处理器处理该端口的流量来提升性能。

虽然您也可以指定 `all` 作为参数来为所有端口提供重组，但是思科**不**建议将端口设置为 `all`，因为这样做可能会不必要地增加此预处理器检查的流量并降低性能。

TCP 重组自动透明地包括添加到其他预处理器的端口。但是，如果明确向已添加到其他预处理器配置的 TCP 重组列表中添加端口，这些端口将进行正常处理。这包括以下预处理器的端口列表：

- FTP/Telnet （服务器级别 FTP）
- DCE/RPC
- HTTP 检查
- SMTP
- 会话发起协议
- POP
- IMAP
- SSL

请注意，重组其他流量类型 （客户端和/或服务器）会增加资源需求。

如果在以下描述中未提到任何预处理器规则，该选项不与预处理规则相关。

Perform Stream Reassembly on Client Ports

根据连接的客户端的端口启用数据流重组。换句话说，它对目标为网络服务器、邮件服务器或通常由 $HOME_NET 中指定的 IP 地址定义的其他 IP 地址的数据流进行重组。如果您预计客户端会发出恶意流量，请使用此选项。

Perform Stream Reassembly on Client Services

根据连接的客户端的服务启用数据流重组。如果您预计客户端会发出恶意流量，请使用此选项。

必须为选择的每个客户端服务至少启用一个客户端检测器（请参阅第 46-24 页上的激活和停用检测器）。默认情况下，思科提供的所有检测器均已激活。如果没有为相关客户端应用启用检测器，则系统会自动为应用启用思科提供的所有检测器；如果不存在任何检测器，则系统会为应用启用最近修改的用户定义的检测器。

此功能需要保护和可控性许可证。

Perform Stream Reassembly on Server Ports

根据连接的服务器端的端口启用数据流重组。换句话说，它对从网络服务器、邮件服务器或通常由 $EXTERNAL_NET 中指定的 IP 地址定义的其他 IP 地址发出的数据流进行重组。当您要监控服务器端攻击时，请使用此选项。您可以通过不指定端口来禁用此选项。

Perform Stream Reassembly on Server Services

根据连接的服务器端的服务启用数据流重组。当您要监控服务器端攻击时，请使用此选项。您可以通过不指定服务来禁用此选项。

必须为选择的每个服务至少启用一个检测器（请参阅第 46-24 页上的激活和停用检测器）。默认情况下，思科提供的所有检测器均已激活。如果没有为服务启用检测器，则系统会自动为相关应用协议启用思科提供的所有检测器；如果不存在任何检测器，则系统会为该应用协议启用最近修改的用户定义的检测器。

此功能需要保护和可控性许可证。

Perform Stream Reassembly on Both Ports

根据连接的客户端和服务器端的端口启用数据流重组。如果您预计相同端口的恶意流量在客户端和服务器之间可能以任一方向传播，请使用此选项。您可以通过不指定端口来禁用此选项。

Perform Stream Reassembly on Both Services

根据连接的客户端和服务器端的服务启用数据流重组。如果您预计相同服务的恶意流量在客户端和服务器之间可能以任一方向传播，请使用此选项。可以通过不指定服务来禁用此选项。

必须为选择的每个服务至少启用一个检测器（请参阅第 46-24 页上的激活和停用检测器）。默认情况下，思科提供的所有检测器均已激活。如果没有为相关客户端应用或应用协议启用检测器，则系统会自动启用为应用或应用协议启用思科提供的所有检测器；如果不存在任何检测器，则系统会为应用或应用协议启用最近修改的用户定义的检测器。

此功能需要保护和可控性许可证。

配置 TCP 数据流预处理

许可证：保护

您可以配置 TCP 数据流预处理（包括 TCP 策略）。有关 TCP 数据流预处理器配置选项的详细信息，请参阅第 29-20 页上的选择 TCP 策略选项。

要配置数据流预处理器以跟踪 TCP 会话，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Edit Policy 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Transport/Network Layer Preprocessors 中的 **Checksum Verification**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 TCP Stream Configuration 页面。页面底部消息会标识出包含配置的策略层。有关详细信息，请参阅第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　或者，修改 Global Settings 下的 **Packet Type Performance Boost**。有关详细信息，请参阅第 29-19 页上的选择 TCP 全局选项。

步骤 6　此时您有两种选择：

- 添加新的基于目标的策略。点击页面左侧 **Hosts** 旁边的添加图标 ( )。系统将显示 Add Target 弹出窗口。在 **Host Address** 字段中指定一个或多个 IP 地址，然后点击 **OK**。

  可以指定单个 IP 地址或地址块。您可以创建总共 255 个基于目标的策略 （包括默认策略）。有关在 FireSIGHT 系统中使用 IP 地址块的信息，请参阅第 1-16 页上的 IP 地址约定。

  请注意，为了让基于目标的策略处理流量，您标识的网络必须匹配您在其中配置该策略的网络分析策略处理的网络、区域和 VLAN 或是其子集。有关详细信息，请参阅第 25-2 页上的使用网络分析策略自定义预处理。

  新条目将出现在页面左侧的目标列表中，突出显示以表明其已被选定；Configuration 部分会进行更新，以反映所添加的策略的当前配置。

- 修改现有基于目标的策略的设置。点击您在页面左侧 **Hosts** 中添加的策略的配置地址，或者点击 **default**。

  所选项目将会突出显示，并且 Configuration 部分会进行更新以显示所选策略的当前配置。要删除现有的基于目标的策略，请点击要删除的策略旁边的删除图标 ( )。

步骤 7　或者，修改 Configuration 中的任何 TCP 策略选项。

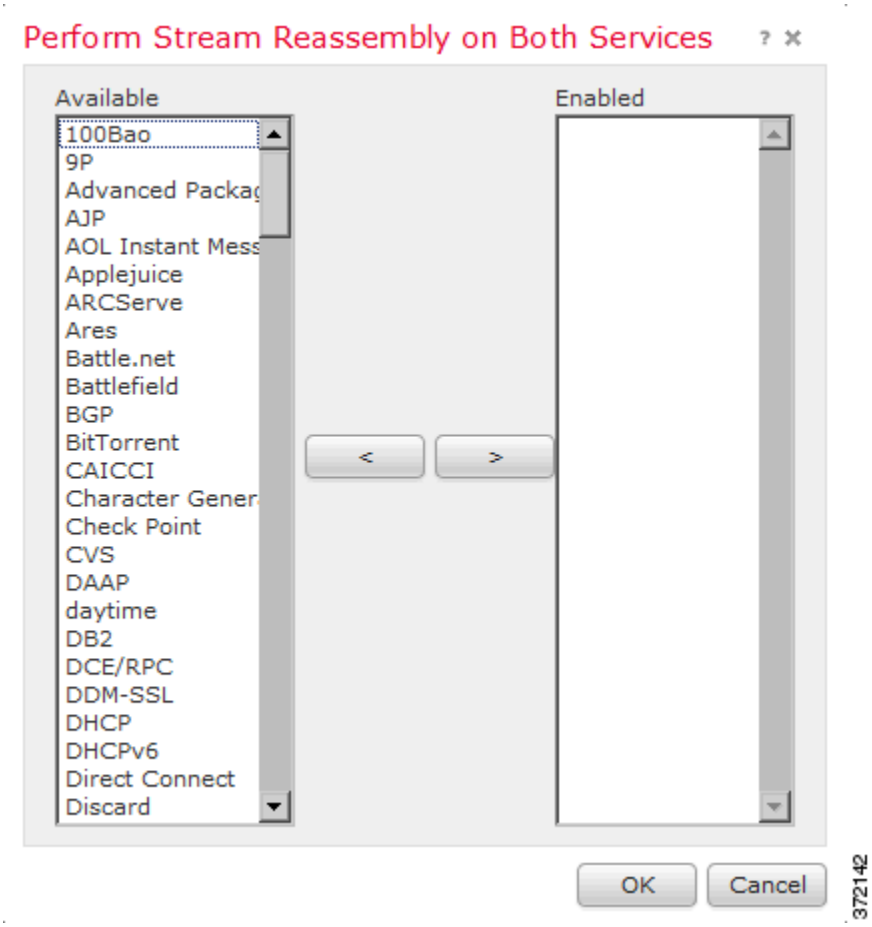
有关根据客户端服务和/或服务器服务修改数据流重组的设置的特定说明，请转至步骤 8；否则，转至步骤 11。

有关详细信息，请参阅第 29-20 页上的选择 TCP 策略选项和第 29-23 页上的选择数据流重组选项。

步骤 8　要根据客户端服务和/或服务器服务修改数据流重组的设置，请在要修改的字段内点击，或者点击要修改的该字段旁边的 **Edit**。

将会出现所选字段的弹出窗口。

例如，下图中显示 Perform Stream Reassembly on Both Services 弹出窗口。



请注意，您可以启用自适应配置文件，以根据在网络上发现的服务监控要重组的数据流预处理器的流量。有关详细信息，请参阅第 50-31 页上的使用服务器和第 30-1 页上的调整被动部署中的预处理。

步骤 9　您有两种选择：

- 要添加要监控的服务，请从左侧的 **Available** 列表中选择一个或多个服务，然后点击右箭头 (**>**) 按钮。
- 要删除服务，请从右侧的 **Enabled** 列表中选择要删除的服务，然后点击左箭头 (**<**) 按钮。

按住 Ctrl 或 Shift 键的同时点击可选择多个服务检测器。您也可以点击并拖动以选择多个相邻服务检测器。

步骤 10　点击 **OK** 以添加所选的项目。

系统将显示 TCP Stream Configuration 页面并更新服务。

步骤 11　或者，展开 **Troubleshooting Options** 并修改任一 TCP 数据流预处理策略设置 （仅当支持代表要求时才应执行此操作）。有关详细信息，请参阅第 29-20 页上的选择 TCP 策略选项。

步骤 12　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

使用 UDP 数据流预处理

许可证：保护

当规则引擎使用以下任何参数根据包含 `flow` 关键字 （请参阅第 36-47 页上的将规则应用于 TCP 或 UDP 客户端或服务器流量）的 UDP 规则处理数据包时，会发生 UDP 数据流预处理：

- `Established`
- `To Client`
- `From Client`
- `To Server`
- `From Server`

UDP 是一个无连接协议，并不提供在两个终端之间建立通信信道、交换数据和关闭该信道的方法。在*会话*方面通常未考虑 UDP 数据流。但是，数据流预处理器使用封装 IP 数据报报头中的源和目标 IP 地址字段及 UDP 报头中的端口字段来确定流动方向并识别会话。当出现下列情况时，会话将会结束：超过可配置的计时器时；或者，任一终端收到表明另一个终端不可达或所请求的服务不可用。

请注意，系统不生成与 UDP 数据流预处理相关的事件；但是，您可以启用相关数据包解码器规则来检测 UDP 协议报头异常。有关数据包解码器生成的事件的信息，请参阅第 29-14 页上的了解数据包解码。

配置 UDP 数据流预处理

许可证：保护

您可以配置 UDP 数据流预处理。

要配置数据流预处理器以跟踪 UDP 会话，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control** 显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Edit Policy 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 Transport/Network Layer Preprocessors 中的 **Checksum Verification**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 UDP Stream Configuration 页面。页面底部消息会标识出包含配置的策略层。有关详细信息，请参阅第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　或者，配置**超时**值以指定预处理器在状态表中保留非活动数据流的秒数 （1 至 86400）。如果在指定时间内看不到其他数据报，预处理器会从状态表中删除数据流。

步骤 6　或者，选择 **Packet Type Performance Boost** 以忽略已启用的规则中未指定的所有端口和应用协议的 UDP 流量，但在源端口和目标端口均设置为 `any` 的 UDP 规则具有 `flow` 或 `flowbits` 选项时除外。这种性能改进可能会导致未能检测出某些攻击。

步骤 7　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

调整被动部署中的预处理

通常，系统使用网络分析策略中的静态设置预处理和分析流量。然而，通过自适应配置文件功能，该系统可将主机信息与网络映射的流量关联从而适应网络流量，然后据此处理网络流量。

当主机接收流量时，主机上运行的操作系统重组 IP 片段。重组所用顺序取决于操作系统。与之类似，每个操作系统都可能以不同方式执行 TCP，因此 TCP 数据流重组方式也有不同。如果预处理器重组数据时所用格式与目标主机操作系统所用格式不同，该系统在接受主机端重组数据时有可能错过可能是恶意的内容。

提示 在被动部署中，思科建议您配置自适应配置文件。在内嵌式部署中，思科建议您配置启用了 **Normalize TCP Payload** 选项的内联规范化预处理程序。有关详细信息，请参阅第 29-6 页上的规范化内联流量。

有关使用自适应配置文件改善数据包片段和 TCP 数据流重组的详细信息，请参阅以下主题：

- 第 30-1 页上的了解自适应配置文件
- 第 30-3 页上的配置自适应配置文件

了解自适应配置文件

许可证：保护

借助于自适应配置文件，可启用最适合 IP 分片重组和 TCP 数据流预处理的操作系统配置文件。有关网络分析策略中受自适应配置文件这影响的各方面的详细信息，请参阅第 29-10 页上的对 IP 数据包进行分片重组和第 29-18 页上的使用 TCP 数据流预处理。

该系统可以使用由网络发现工具检出、通过 Nmap 扫描工具获得或通过主机输入功能添加的主机信息来适应处理行为。

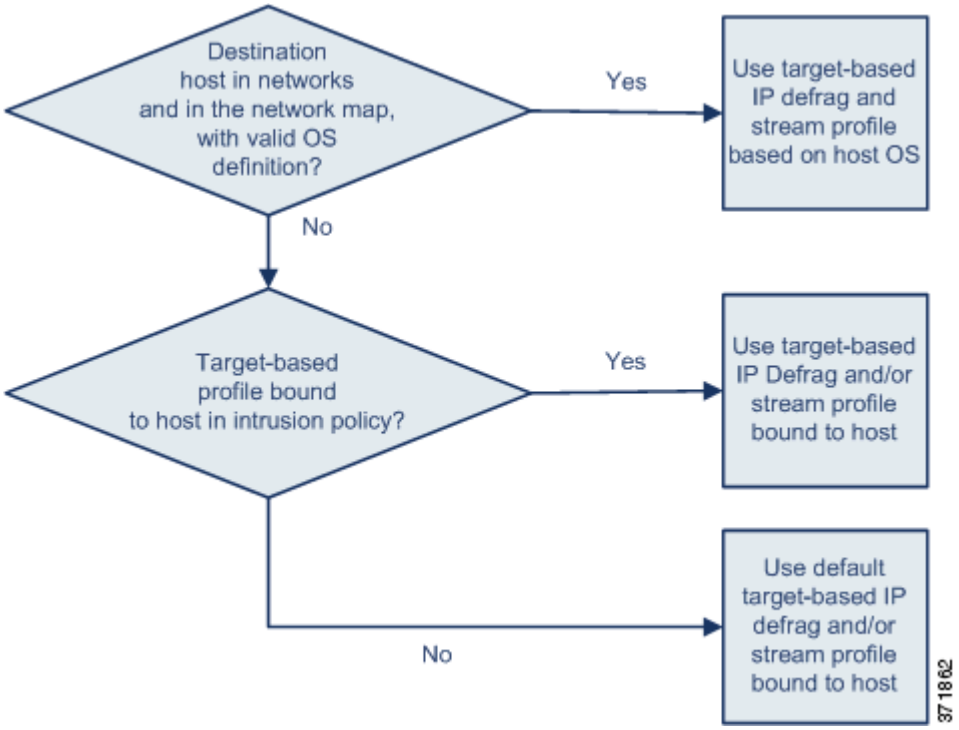
注 当您使用命令行导入实用程序或主机输入 API 通过第三方应用程序输入主机信息时，您必须首先映射该数据至产品定义，以便系统将其用于自适应配置文件。有关详细信息，请参阅第 46-27 页上的管理第三方产品映射。

通过预处理器使用自适应配置文件

许可证：保护

自适应配置文件 （就像可在网络分析策略中配置的基于目标的配置文件）有助于以与目标主机上操作系统相同的方式对 IP 数据包进行分片重组并重组数据流。然后入侵规则引擎使用与目标主机所用的相同格式分析数据。

手动配置的基于目标的配置文件只适用于您选择的操作系统默认配置文件或您绑定到特定主机的配置文件。然而，自适应配置文件会为了目标主机而切换至主机配置文件中基于操作系统的适当操作系统配置文件，如下图所示。



例如，您为 10.6.0.0/16 子网配置自适应配置文件并将基于目标的默认 IP 分片重组策略设置为 Linux。配置设置的防御中心中有一个包括 10.6.0.0/16 子网的网络映射。

当设备检测到来自主机 A （未连至 10.6.0.0/16 子网）的流量时，它使用基于 Linux 目标的策略重组 IP 片段。然而，当它检测到来自主机 B （未连至 10.6.0.0/16 子网）的流量时，它将从网络映射中获取主机 B 的操作系统数据，此处主机 B 被列为运行 Microsoft Windows XP 专业版。该系统使用基于 Windows 目标的配置文件对指定给主机 B 的流量进行 IP 分片重组。

有关 IP 分片重组预处理器的信息，请参阅第 29-10 页上的对 IP 数据包进行分片重组。有关流量预处理器的信息，请参阅第 29-18 页上的使用 TCP 数据流预处理。

自适应配置文件和 FireSIGHT 建议规则

许可证：保护

自适应配置文件功能是访问控制策略中的高级设置，全局应用于由该访问控制策略调用的所有入侵策略。 FireSIGHT 建议的规则功能适用于您配置它所处的个别入侵策略。

类似 FireSIGHT 建议规则，自适应配置文件将规则中元数据与主机信息进行比对，确定是否为规则申请特定主机。然而，虽然FireSIGHT建议规则为使用该信息的启用或禁用规则提供建议，但是自适应配置文件仍使用这些信息将特定规则应用于特定流量。

FireSIGHT建议规则需要您的互动才能对规则状态执行建议的更改。在另一方面，自适应配置文件不能修改入侵策略。在逐包基础上进行规则自适应处理。

此外， FireSIGHT建议规则可能会启用已禁用的规则。相反，自适应配置文件仅影响在入侵策略中已启用的规则的应用。自适应配置文件永不改变规则状态。

可以组合使用自适应配置文件和 FireSIGHT 建议的规则。当应用入侵策略来确定是否纳入某条规则作为应用备选项时，自适应配置文件使用该规则的规则状态，您是选择接受还是拒绝建议均反映在该规则状态中。您可以同时使用这两个功能以确保您已启用或禁用每个监测网络中最合适的规则，然后应用对特定流量最为有效的已启用规则。

有关详情，请参见第 33-1 页上的为您的网络资产定制入侵防御。

配置自适应配置文件

许可证：保护

要使用主机信息来确定哪些基于目标的配置文件可用于 IP 分片重组和 TCP 数据流预处理，您可配置自适应配置文件。

注 要使用自适应配置文件，您必须在网络发现策略中为要保护的网络启用主机发现，然后重新应用网络发现策略。有关详细信息，请参阅第 45-19 页上的创建网络发现策略。

在配置自适应配置文件时，您需要将自适应配置文件设置绑定到一个特定网络或多个网络。要成功使用自适应配置文件，该网络必须存在于网络映射中，并且必须处于您应用访问控制策略所在设备监测的区段中。

您可以指明在网络映射中的哪些主机上应使用自适应配置文件处理流量，只需用与访问控制策略的默认入侵策略相链接的变量集中配置的所需值指定 IP 地址、地址块或网络变量。有关详情，请参见第 25-1 页上的设置用于访问控制的默认入侵策略。

您可以单独或以任意组合方式使用此类寻址方法，作为 IP 地址、地址块或由逗号分隔的变量列表，如下列实例所示：

```
192.168.1.101, 192.168.4.0/24, $ HOME_NET
```

有关在 FireSIGHT 系统中指定地址块的信息，请参阅第 1-16 页上的 IP 地址约定。

提示 通过使用带有*任意值*的变量或指定 `0.0.0.0/0` 作为网络值，您可以将自适应配置文件应用至网络映射中的所有主机。

您还可以控制网络映射数据从防御中心同步到其受管设备的频率。系统使用该数据确定处理流量时应使用哪些配置文件。

要配置自适应配置文件，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1 选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Detection Enhancement Settings** 旁的编辑图标 ( )。

系统将显示 Detection Enhancement Settings 弹出窗口。

步骤 5　选择 **Adaptive Profiles - Enabled** 启用自适应配置文件。

步骤 6　或者，在 **Adaptive Profiles - Attribute Update Interval** 字段中，键入从防御中心到其受管设备同步网络映射数据持续的分钟数。

注　增加此选项的值可提升大型网络的性能。

步骤 7　在 **Adaptive Profiles - Networks** 字段中，键入特定 IP 地址、地址块、变量或者包括由逗号隔开的任何此类寻址方法的列表，以标识网络映射中您要使用自适应配置文件的任何主机。

有关配置变量的信息，请参阅第 3-15 页上的使用变量集。有关配置网络映射的信息，请参阅第 45-19 页上的创建网络发现策略。

步骤 8　点击 **OK** 保留设置。

第 31 章

入侵策略入门

*入侵策略*是定义的各组入侵检测和防御配置，这些配置检查流量是否存在安全性违规，并且在内联部署中还可以阻止或修改恶意流量。入侵策略由您的访问控制策略调用，是允许流量到达目标之前，系统的最后一道防线。

思科通过 FireSIGHT 系统提供多种入侵策略。通过系统提供的策略，您可以利用思科漏洞研究团队 (VRT) 的经验。对于这些策略，VRT 设置入侵和预处理程序规则状态（启用或禁用），并提供其他高级设置的初始配置。启用规则将使系统为与规则匹配的流量生成入侵事件（或者阻止该流量）。禁用规则将停止该规则的处理。

提示 系统提供的入侵和网络分析策略命名相似，但包含不同的配置。例如，“平衡式安全性和连接性”网络分析策略和“平衡式安全性和连接性”入侵策略共同作用而且都可以在入侵规则更新中更新。但是，网络分析策略主要监管预处理选项，而入侵策略主要监管入侵规则。第 23-1 页上的了解网络分析和入侵策略概述网络分析和入侵策略如何共同作用以检查您的流量以及关于使用导航面板、解决冲突和执行改变的一些基本知识。

如果创建了自定义入侵策略，则可以：

- 通过启用和禁用规则以及通过编写和添加您自己的规则，调整检测。
- 使用 FireSIGHT 建议将在您的网络中检测到的操作系统、服务器和客户端应用程序协议与专为保护这些资产而编写的规则相关联。
- 配置各种高级设置，例如外部警报、敏感数据预处理和全局规则阈值。
- 以层作为构建块，有效地管理多个入侵策略。

当定制您自己的入侵策略时，特别是在启用和添加规则时，请记住一些入侵规则要求首先以某种方式解码或预处理流量。在入侵策略检查数据包之前，系统将根据网络分析策略中的预处理数据包。如果您禁用一个必需的预处理程序，虽然该预处理程序在网络分析策略网络界面中保持禁用，但系统仍自动通过其当前设置使用它。

注 由于预处理和入侵检查如此密切关联，因此，检查单个数据包的网络分析和入侵策略**必须**相互补充。定制预处理，特别是使用多个自定义网络分析策略，是一个**高级**任务。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

在配置自定义入侵策略后，可通过将入侵策略与一个或多个访问控制规则或访问控制策略的默认操作关联起来，将其用作您的访问控制配置的一部分。这强制系统在某些允许的流量传递至其最终目标之前使用入侵策略对其进行检查。与入侵策略配对的变量集可供您准确地反映您的家庭和外部网络，以及根据情况反映您网络上的服务器。有关详细信息，请参阅第 18-1 页上的使用入侵和文件策略控制流量。

请注意，默认情况下，系统禁用加密负载的入侵检查。当加密连接与已配置入侵检查的访问控制规则匹配时，这有助于减少误报和提高性能。有关详细信息，请参阅第 19-1 页上的了解流量解密和第 27-60 页上的使用 SSL 预处理器。

本章介绍如何创建简单的自定义入侵策略。本章还包含有关编辑、比较等管理入侵策略的基本信息。有关详情，请参阅：

创建自定义入侵策略

许可证：保护

当新建入侵策略时，必须为其提供唯一的名称，指定基本策略并指定丢弃行为。

基本策略定义入侵策略的默认设置。修改新策略的一项设置会覆盖而不是变更基本策略中的设置。您可以使用系统提供的或自定义策略作为您的基本策略。有关详细信息，请参阅第 24-2 页上的了解基本层。

入侵策略的丢弃行为或 **Drop when Inline** 设置决定着系统如何处理丢弃规则（规则状态设置为 Drop and Generate Events 的入侵或预处理程序规则）和影响流量的其他入侵策略配置。当您要放弃或替换恶意数据包时，您应该在内嵌部署中启用丢弃行为。请注意，在被动部署中，无论丢弃行为如何，系统均无法影响流量。有关详细信息，请参阅第 31-5 页上的在内联部署中设置丢弃行为。

要创建入侵策略，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion Policy > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

提示　您也可以从另一个防御中心导入策略；请参阅第 A-1 页上的导入和导出配置。

步骤 2　点击 **Create Policy**。

如果您在另一策略中有未保存的更改，当系统提示您返回 Intrusion Policy 页面时请点击 **Cancel**。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Create Intrusion Policy 弹出窗口。

步骤 3　在 **Name** 和 **Description** 中为策略提供唯一名称和说明 （后者为可选项）。

步骤 4　指定初始**基本策略**。

您可以使用系统提供的或自定义策略作为您的基本策略。

注意事项　请**勿**使用 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 5　在内联部署中设置系统的丢弃行为：

- 要允许入侵策略影响流量并生成事件，请启用 **Drop when Inline**。
- 要防止入侵策略影响流量，同时生成事件，请禁用 **Drop when Inline**。

步骤 6　创建策略：

- 点击 **Create Policy** 以新建策略并返回到 Intrusion Policy 页面。新策略的设置与其基本策略相同。
- 点击 **Create and Edit Policy** 以创建策略并打开它以便在高级入侵策略编辑器中进行编辑；请参阅第 31-4 页上的编辑入侵策略。

管理入侵策略

许可证：保护

在 Intrusion Policy 页面 (**Policies > Intrusion > Intrusion Policy**)，您可以查看自己的当前自定义入侵策略，以及以下信息：

- 最近一次修改策略的时间和日期 （当地时间）以及执行此修改的用户
- 是否已启用 **Drop when Inline** 设置，从而使您在内联部署中丢弃和修改流量
- 哪些访问控制策略和设备在使用入侵策略检查流量
- 策略是否有未保存的更改，以及有关谁 （如有人）正在编辑策略的信息

除了您创建的自定义策略之外，系统还提供两种自定义策略：初始内联策略和初始被动策略。这两个入侵策略都使用“平衡式安全性和连接性”入侵策略作为其基本策略。两者之间的唯一区别在于其 **Drop When Inline** 设置，该设置在内联策略中启用丢弃行为，而在被动策略中禁用丢弃行为。您可以编辑并使用系统提供的这些自定义策略。

Intrusion Policy 页面上的选项可供您可以采取下表中的操作。

表 31-1　　入侵策略管理操作

要.....	您可以.....	请参阅.....
创建新的入侵策略	点击 **Create Policy**。	第 31-2 页上的创建自定义入侵策略
编辑现有入侵策略	点击编辑图标 ( )。	第 31-4 页上的编辑入侵策略
为您的受管设备重新应用一条入侵策略	点击应用图标 ( )。	第 31-7 页上的应用入侵策略
导出入侵策略以导入到另一个防御中心	点击导出图标 ( )。	第 A-1 页上的导出配置
查看列出入侵策略中当前配置设置的 PDF 报告	点击报告图标 ( )。	第 31-8 页上的生成当前入侵设置的报告
比较两个入侵策略或同一策略两个版本的设置	点击 **Compare Policies**。	第 31-9 页上的比较两个入侵策略或版本
删除入侵策略	点击删除图标 ( )，然后确认要删除策略。如果访问控制策略引用了某条入侵策略，则无法删除该入侵策略。	

编辑入侵策略

许可证：保护

当您新建入侵策略时，它的入侵规则和高级设置与其基本策略相同。下表说明了编辑入侵策略时最常见的操作：

表 31-2　　入侵策略编辑操作

要.....	您可以.....	请参阅.....
在内联部署中指定丢弃行为	选择或清除 Policy Information 页面上的 **Drop when Inline** 复选框。	第 31-5 页上的在内联部署中设置丢弃行为
更改基本策略	从 Policy Information 页面上的 **Base Policy** 下拉列表选择基本策略。	第 24-3 页上的更改基本策略
查看基本策略中的设置	在 Policy Information 页面上点击 **Manage Base Policy**。	第 24-2 页上的了解基本层
显示或配置入侵规则	在 Policy Information 页面上点击 **Manage Rules**。	第 32-2 页上的查看入侵策略中的规则
按当前规则状态显示入侵规则的已过滤视图并且可选地配置这些规则	在 Policy Information 页面上，点击 **Management Rules** 下方设置成 Generate Events 或 Drop and Generate Events 的规则数量旁边的 **View**。	第 32-9 页上的过滤入侵策略中的规则
配置 FireSIGHT 建议的规则	在导航面板中点击 **FireSIGHT Recommendations**。	第 33-3 页上的使用 FireSIGHT 建议
按当前建议的规则状态显示入侵规则的已过滤视图并且可选地配置这些规则	在 Policy Information 页面上，在生成建议后： • 点击建议数量旁的 **View**，以生成事件、丢弃和生成事件或禁用规则 • 点击 **View Recommended Changes** 以查看所有建议	第 33-3 页上的使用 FireSIGHT 建议
启用、禁用或者编辑高级设置	在导航面板中点击 **Advanced Settings**	第 31-6 页上的在入侵策略中配置高级设置
管理策略层	在导航面板中点击 **Policy Layers**	第 24-1 页上的在网络分析或入侵策略中使用层

定制入侵策略时，特别是在启用和添加规则时，请记住一些入侵规则要求首先以某种方式解码或预处理流量。在入侵策略检查数据包之前，系统将根据网络分析策略中的预处理数据包。如果您禁用一个必需的预处理程序，虽然该预处理程序在网络分析策略网络界面中保持禁用，但系统仍自动通过其当前设置使用它。

注　由于预处理和入侵检查如此密切关联，因此，检查单个数据包的网络分析和入侵策略**必须**相互补充。定制预处理，特别是使用多个自定义网络分析策略，是一个**高级**任务。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

系统为每个用户缓存一个入侵策略。在编辑入侵策略时，如果您选择任何菜单或指向另一页面的其他路径时，即使您离开此页，您的更改也会保留在系统缓存中。除了上表中您可以执行的操作，第 23-1 页上的了解网络分析和入侵策略还提供了关于使用导航面板、解决冲突和执行更改的信息

要编辑入侵策略，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要配置的入侵策略旁的编辑图标 ( )。

系统将显示入侵策略编辑器，其以 Policy Information 页面为中心，在左侧显示导航面板。

步骤 3　编辑您的策略。采取上面总结的任何操作。

步骤 4　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

在内联部署中设置丢弃行为

许可证：保护

在内联部署中，入侵策略会阻止和修改流量：

- *Drop rules* 可以丢弃匹配的数据包并生成入侵事件。要配置入侵或预处理程序丢弃规则，请将其状态设置为 Drop and Generate Events；请参阅第 32-18 页上的设置规则状态。
- 入侵规则可使用 `replace` 关键字替换恶意内容；请参阅第 36-27 页上的替换内联部署中的内容。

要使入侵规则影响流量，必须正确配置丢弃规则和内容替换规则，以及正确部署内联受管设备，也就是与内联接口集内联。最后，您必须启用入侵策略的*丢弃行为*或 **Drop when Inline** 设置。

注　要阻止通过 FTP 传输恶意软件文件，不仅必须正确配置基于网络的高级恶意软件防护 (AMP)，而且还要在访问控制策略的默认入侵策略中启用 **Drop when Inline**。要确定或更改默认入侵策略，请参阅第 25-1 页上的设置用于访问控制的默认入侵策略。

如果要评估您的配置在内联部署中如何运行，而不实际影响流量，您可以禁用丢弃行为。在这种情况下，系统会生成入侵事件，但不会丢弃触发丢弃规则的数据包。当您对结果满意时，您可以启用丢弃行为。

请注意，在分路模式下，在被动部署或内联部署中，无论丢弃行为如何，系统都无法影响流量。换句话说，在被动部署中，设置为 Drop and Generate Events 的规则的行为与设置为 Generate Events 的规则完全一致 - 系统生成入侵事件，但不会丢弃数据包。

当您查看入侵事件时，工作流可能包括 *inline result*，其指明流量是确实已丢弃，还只是本该已丢弃。当数据包与丢弃规则匹配时，内联结果如下：

- `Dropped`，适合已启用丢弃行为时正确配置的内联部署所丢弃的数据包
- `Would have dropped`，适合由于已被动部署设备或已禁用丢弃行为而未丢弃的数据包。请注意，系统在修剪时，无论如何部署，对于检测到的数据包，内联结果始终为 `Would have dropped`。

要在内联部署中设置入侵策略的丢弃行为，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

系统将显示 Policy Information 页面。

步骤 3　设置策略的丢弃行为：

- 要使入侵规则影响流量并生成活动，请启用 **Drop when Inline**。
- 要防止入侵规则影响流量，同时生成事件，请禁用 **Drop when Inline**。

步骤 4　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

在入侵策略中配置高级设置

许可证：保护

入侵策略的*高级设置*需要特定专业知识才能配置。入侵策略的基本策略决定了默认情况下启用哪些高级设置及各自的默认配置。

当您在入侵策略的导航面板中选择 **Advanced Settings** 时，策略将按类型列出其高级设置。在 Advanced Settings 页面中，您可以启用或禁用入侵策略中的高级设置，以及访问高级设置配置页面。

高级设置必须在启用后才能配置。当您启用高级设置后，导航面板中 **Advanced Settings** 链接下方将会显示指向高级设置配置页面的子链接， Advanced Settings 页面高级设置旁边将会出现指向配置页面的 **Edit** 链接。

提示　要将高级设置的配置恢复成基本策略中的设置，请在高级设置的配置页面上点击 **Revert to Defaults**。出现提示时，请确认您要恢复。

当您禁用高级设置时，系统不再显示子链接和 **Edit** 链接，但是会保留您的配置。注意某些入侵策略配置 （敏感数据规则、入侵规则的 SNMP 警报）需要启用和正确配置高级设置。您无法保存以这种方式错误配置的入侵策略；请参阅第 23-13 页上的解决冲突和提交策略更改。

修改高级设置的配置要求了解正在进行的修改及其对网络的潜在影响。以下部分提供指向每项高级设置具体配置详细信息的链接。

具体威胁检测

敏感数据预处理器检测敏感信息，例如 ASCII 文本格式的信用卡号和社会保障号。有关配置此预处理程序的信息，请参阅第 34-17 页上的检测敏感数据。

请注意，检测特定威胁 （Back Orifice 攻击、多个端口扫描类型和试图利用超大流量击败您网络的基于速率的攻击）的其他预处理程序在网络分析策略中进行配置。有关详细信息，请参阅第 34-1 页上的检测特定威胁。

入侵规则阈值

全局规则阈值允许使用阈值来限制系统记录和显示的入侵事件数量，从而可以防止您的系统由于无法应付大量事件而崩溃。有关详细信息，请参阅第 35-1 页上的从全局限制入侵事件记录。

外部响应

除了网络界面中的各种入侵事件视图之外，您还可以启用记录到系统日志 (syslog) 工具或者将事件数据发送到 SNMP 陷阱服务器。根据策略，您可以指定入侵事件通知限制，设置发送到外部日志记录工具的入侵事件通知，以及配置对入侵事件的外部响应。有关详情，请参阅：

- 第 44-3 页上的配置 SNMP 响应
- 第 44-5 页上的配置系统日志响应

请注意，除了基于策略的这些警报配置，对于每个规则或规则组，您还可以在入侵事件上全局启用或禁用邮件警报。无论哪个入侵规则处理数据包，都会使用您的邮件警报设置。有关详细信息，请参阅第 44-6 页上的了解邮件警报。

应用入侵策略

许可证：保护

向使用访问控制 （请参阅第 12-13 页上的应用访问控制策略）的受管设备应用入侵策略后，可以随时重新应用此入侵策略。这样就可以在监控下的网络上实施入侵策略更改，而无需重新应用访问控制策略。重新应用时，还可以查看比较报告，检查自从最后一次应用此入侵策略之后所做的更改。

重新应用入侵策略时,请注意以下事项：

- 可以安排定期重复执行入侵策略重新应用任务；请参阅第 62-6 页上的自动应用入侵策略。
- 在无效目标设备上无法重新应用入侵策略。例如，应用从设备上删除之前已应用入侵策略的访问控制策略，然后在解决访问控制策略应用任务之前尝试重新应用此入侵策略，就无法重新应用此入侵策略。
- 对于运行不同版本 FireSIGHT 系统的堆栈设备无法应用入侵策略 （例如，在其中一个设备上升级失败）。可以向设备堆栈重新应用入侵策略，但是，无法向堆栈内的各个设备单独应用入侵策略。
- 导入规则更新时，可以在导入完成后自动应用入侵策略。如果不启用此选项，就必须手动重新应用被规则更新更改的策略。有关详情，请参见第 66-13 页上的导入规则更新和本地规则文件。
- 如果防御中心上 Snort 的版本与受管设备上的不同，不应用访问控制策略就无法向此设备应用入侵策略。如果入侵策略应用因此失败，请改为重新应用整个访问控制策略。

要重新应用入侵策略，请执行以下操作：

访问：管理员/安全审批者

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的应用图标 ( )。

系统将显示 Reapply Intrusion Policy 窗口，其中列出了当前应用该策略的设备。

步骤 3　指定要重新应用该策略的设备。

提示　如果设备列为 **Out-of-date**，请点击比较图标 ( )，查看比较当前应用入侵策略和更新入侵策略的报告。

步骤 4　点击 **Reapply**。

策略重新应用成功。可以使用任务队列监控应用的状态 (**System > Monitoring > Task Status**)。有关详情，请参见第 C-1 页上的查看任务队列。

生成当前入侵设置的报告

许可证：保护

入侵策略报告是对特定时间点策略配置的记录。该系统将基本策略中的设置与策略层的设置组合，不区分源自基本策略或策略层的设置。

您可以将包含以下信息的报告用于审核或检查当前配置。

表 31-3　　入侵策略报告部分

项	说明
策略信息	提供入侵策略的名称和说明、最后一次修改策略的用户的名称以及策略最后一次修改的日期和时间。此外还指明在内联部署中丢弃数据包是启用还是禁用状态，当前规则更新版本以及基本策略是否锁定为当前规则更新。
FireSIGHT建议	根据主机和您的网络上的应用程序提供有关任何建议规则状态的信息。或者，在您配置 FireSIGHT 建议时，如果您已启用该设置，它将会包含建议之间的差异以及策略报告中的规则状态。
高级设置	列出所有已启用入侵策略高级设置及其配置。
规则	提供所有已启用规则及其操作的列表。

还可以生成比较两个入侵策略或同一入侵策略两个版本的比较报告。有关详细信息，请参阅第 31-9 页上的比较两个入侵策略或版本。

要查看入侵策略报告，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击您想要生成报告的入侵策略旁边的报告图标 ( )。请记住，应先确认任何潜在更改再生成入侵策略报告；只有确认的报告才会显示在报告中。

系统生成入侵策略报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

比较两个入侵策略或版本

许可证：保护

如要查看策略更改是否符合贵组织的标准或优化系统性能，可以检查这两个入侵策略之间的区别。对于可以访问的安全策略，可以比较任意两个入侵策略或同一个入侵策略的两个版本。比较之后，可以生成 PDF 报告，记录两个策略或两个版本的策略之间的区别。

有两个工具可以用来比较入侵策略或入侵策略版本：

- 比较视图只并排显示两个入侵策略或两个版本之间的区别；每个策略的名称或策略版本则显示在比较视图的左右两侧。

  您可以使用该工具在网络界面上查看和导航两个策略修订版，其中突出显示其差异。

- 比较报告只以类似于入侵策略报告的形式创建关于两个入侵策略或两个版本之间区别的记录，但采用的是 PDF 格式。

  可以将其用于保存、复制、打印和共享策略比较，以备进一步检查。

如需了解和使用入侵策略比较工具的更多信息，请参阅：

- 第 31-9 页上的使用入侵策略比较视图
- 第 31-10 页上的使用入侵策略比较报告

使用入侵策略比较视图

许可证：保护

此比较视图并排显示两个入侵策略或其两个版本，比较视图左右两侧标题栏中将按照名称标识每个策略或每个版本。最近一次修改的时间和执行最后一次修改的用户显示在策略名称右侧。请注意，Intrusion Policy 页面用本地时间显示最后一次修改策略的时间，但是入侵策略报告则用 UTC 时间列出此修改时间。两个入侵策略或两个版本之间的区别会突出显示出来：

- 蓝色表示两个策略或两个版本中此突出显示的设置不同。并且用红色文本注明其不同之处。
- 绿色表示此突出显示的设置在一个策略或一个版本中出现了，而在另一个策略或版本中却没有出现。

可以执行下表中的任何操作。

表 31-4　　入侵策略比较视图操作

要.....	您可以.....
逐一浏览更改	点击标题栏上方的 **Previous** 或 **Next**。 在左右两侧之间以双箭头图标 () 为中心移动，**Difference** 数字调整为识别您正在查看哪个差异。
确定哪一层包含特定高级设置的配置	将指针悬停在想要查看的配置旁边的高级配置图标 () 上方。 窗口随即显示包含高级配置的策略层的名称。
生成新的入侵策略比较视图	点击 **New Comparison**。 系统将显示 **Select Comparison** 窗口。有关详情，请参见使用入侵策略比较报告。
生成入侵策略比较报告	点击 **Comparison Report**。 策略比较报告将会创建仅列出两个策略或策略版本之间的差异的 PDF 文档。

使用入侵策略比较报告

许可证：保护

入侵策略比较报告是关于入侵策略比较视图标识的两个入侵策略或同一入侵策略两个版本之间全部区别的一个 PDF 格式记录。可以使用此报告进一步检查两个入侵策略配置之间的区别以及保存和分发其比较结果。

对于可以访问的任何入侵策略，都可以从此比较视图生成入侵策略比较报告。请记住，应先确认任何潜在更改再生成入侵策略报告；只有确认的报告才会显示在报告中。

入侵策略比较报告的格式与入侵策略报告相同，但有一个区别：入侵策略报告包含入侵策略中的所有设置，而入侵策略比较报告则只包含策略之间存在区别的那些设置。

根据配置，入侵策略报告可能包含表入侵策略报告部分所述的一个或多个分区。

提示　您可以使用类似的操作步骤比较 SSL、访问控制、网络分析、文件、系统或运行状况策略。

要比较两个入侵策略或同一策略的两个版本，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击 **Compare Policies**。

系统将显示 Select Comparison 窗口。

步骤 3　从 **Compare Against** 下拉列表中选择要进行比较的类型：

- 要比较两个不同的策略，请选择 **Other Policy**。
- 要比较同一策略的两个修订版，请选择 **Other Revision**。

请记住，应先确认所有更改，再生成入侵策略报告；只有确认的报告才会显示在报告中。

步骤 4　根据您选择的比较类型，有以下选项可供选择：

- 如果您比较两个不同的策略，请从 **Policy A** 和 **Policy B** 下拉列表中选择要比较的策略。
- 如果您比较同一策略的两个修订版，请从 **Policy** 下拉列表中选择该策略，然后从 **Revision A** 和 **Revision B** 下拉列表中选择要比较的修订版。

步骤 5　点击 **OK** 显示入侵策略比较视图。

系统将显示比较视图。

步骤 6　点击 **Comparison Report**，生成入侵策略比较报告。

步骤 7　系统将显示入侵策略报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

使用规则调整入侵策略

可以使用入侵策略中的 Rules 页面为共享对象规则、标准文本规则和预处理器规则配置规则状态和其他设置。

将规则的状态设置为 Generate Events 或 Drop and Generate Events 即可启用该规则。启用规则后，系统将对匹配该规则的流量生成事件。禁用规则将停止该规则的处理。或者，也可以设置入侵策略，使内联部署中设置为 Drop and Generate Events 的规则对匹配的流量生成事件并丢弃该流量。有关详情，请参见第 31-5 页上的在内联部署中设置丢弃行为。在被动部署中，设置为 Drop and Generate Events 的规则仅对匹配的流量生成事件。

您可以对规则进行过滤来显示规则的一个子集，这样就能选择要更改其规则状态或规则设置的一整组规则。

当入侵规则或规则参数要求禁用的预处理器时，系统会自动使用其当前设置，即使其在网络分析策略网络界面中保持禁用状态。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

有关详细信息，请参阅以下各节：

- 第 32-2 页上的了解入侵防御规则类型说明可在入侵策略中查看和配置的入侵规则和预处理器规则。
- 第 32-2 页上的查看入侵策略中的规则说明如何在 Rules 页面中更改规则的顺序，解释该页面中的图标，并着重介绍了规则的详细信息。
- 第 32-9 页上的过滤入侵策略中的规则说明如何使用规则过滤器来查找要对其应用规则设置的规则。
- 第 32-18 页上的设置规则状态说明如何从 Rules 页面启用和禁用规则。
- 第 32-20 页上的按策略过滤入侵事件通知介绍如何为具体规则设置事件过滤阈值以及如何对具体规则设置抑制。
- 第 32-26 页上的添加动态规则状态介绍在匹配的流量中检测到速率异常时如何设置动态触发的规则状态。
- 第 32-29 页上的添加 SNMP 告警说明如何将 SNMP 告警与具体规则相关联。
- 第 32-30 页上的添加规则注释说明如何向入侵策略中的规则添加注释。

了解入侵防御规则类型

许可证：保护

入侵策略包含两种类型的规则：入侵规则和预处理器规则。

入侵规则是一组指定的关键字和参数，用于检测企图利用网络漏洞的行为；入侵规则通过分析网络流量来检查其是否符合规则中的条件。系统将数据包与每条规则中指定的条件进行比较，如果数据包数据符合规则中指定的所有条件，则触发此规则。系统包含两种由思科漏洞研究团队 (VRT) 创建的入侵规则：其一为共享对象规则，已编写好且不能修改（源端口、目标端口和 IP 地址等规则头信息除外）；其二为标准文本规则，可以修改并另存为新的自定义规则实例。

系统中还包含预处理器规则，即与预处理器和数据包解码器检测选项相关联的规则。预处理器规则不能复制或编辑。大多数预处理器规则默认禁用，如果需要系统为预处理器规则生成事件并在内联部署中丢弃违规的数据包，必须启用这些规则（即设置为 Generate Events 或 Drop and Generate Events）。

VRT 为系统随附的每个默认入侵策略确定思科共享对象规则、标准文本规则和预处理器规则的默认规则状态。

下表介绍 FireSIGHT 系统配套的每种规则类型。

表 32-1　规则类型

类型	说明
共享对象规则	思科漏洞研究团队 (VRT) 创建的入侵规则，以 C 源代码编译的二进制模块方式提供。您可以使用共享对象规则，以标准文本规则无法采取的方式来检测攻击。不能修改共享对象规则中的规则关键字和参数；限制修改规则中使用的变量，限制修改源端口、目标端口和 IP 地址等方面的信息，也限制将新的规则实例另存为自定义共享对象规则。共享对象规则的 GID（生成器 ID）为 3。有关详情，请参见第 36-95 页上的修改现有规则。
标准文本规则	由 VRT 创建、复制并另存为新的自定义规则的入侵规则、使用规则编辑器创建的入侵规则或导入为本地规则（在本地设备上创建和导入）的入侵规则。不能修改 VRT 创建的标准规则中的规则关键字和参数；限制修改规则中使用的变量，限制修改源端口、目标端口和 IP 地址等方面的信息，也限制将新的规则实例另存为自定义标准文本规则。有关详细信息，请参阅第 36-95 页上的修改现有规则、第 36-1 页上的了解和编写入侵规则和第 66-17 页上的导入本地规则文件。VRT 创建的标准文本规则的 GID（生成器 ID）为 1。使用规则编辑器创建的或导入为本地规则的自定义标准文本规则，其 SID（签名 ID）为 1000000 或更大值。
预处理器规则	与数据包解码器的检测选项相关联或与 FireSIGHT 系统配套的预处理器之一相关联的规则。如果需要预处理器规则生成事件，必须启用这些规则。这些规则的 GID（生成器 ID）为解码器或预处理器专用的 GID。有关详细信息，请参阅生成器 ID 表。

查看入侵策略中的规则

许可证：保护

可以调整规则如何在入侵策略中显示，并且可以按多个条件对规则排序。也可以显示特定规则的详细信息，以便查看规则设置、规则文档和其他规则详情。

Rules 页面有四个主要的功能区域：

- 过滤功能 - 有关详细信息，请参阅第 32-9 页上的过滤入侵策略中的规则
- 规则属性菜单 - 有关详细信息，请参阅第 32-18 页上的设置规则状态、第 32-20 页上的按策略过滤入侵事件通知、第 32-26 页上的添加动态规则状态、第 32-29 页上的添加 SNMP 告警和第 32-30 页上的添加规则注释

- 规则列表 - 有关详细信息，请参阅 Rules 页面的列表。
- 规则详细信息 - 有关详细信息，请参阅第 32-4 页上的查看规则详细信息

此外，还可以按不同的条件对规则排序；有关详细信息，请参阅第 32-4 页上的对规则的显示排序。

请注意，用作列标题的图标与用于访问这些配置项的菜单栏中的菜单相对应。例如， Rule State 菜单使用与 Rule State 列相同的图标 ( ) 标记。

下表介绍 Rules 页面中的各列。

表 32-2　　Rules 页面的列

标题	说明	有关详细信息，请参阅.....
GID	该整数表示规则的生成器 ID (GID)。	第 41-34 页上的解读预处理器生成器 ID
SID	该整数表示充当规则唯一标识符的 Snort ID (SID)。	第 41-34 页上的解读预处理器生成器 ID
Message	此规则生成的事件中包含的消息，亦充当该规则的名称。	第 36-10 页上的定义事件消息
	该规则的规则状态，可为以下三种状态之一： • drop and generate events ( ) • generate events ( ) • disable ( ) 请注意，点击某条规则的规则状态图标即可访问该规则的 Set rule state 对话框。	第 32-18 页上的设置规则状态
	FireSIGHT 为规则建议的规则状态。	第 33-1 页上的为您的网络资产定制入侵防御
	事件过滤器，包括应用于该规则的事件阈值和事件抑制。	第 32-20 页上的按策略过滤入侵事件通知
	该规则的动态规则状态，如果发生指定的速率异常则会生效。	第 32-26 页上的添加动态规则状态
	为规则配置的告警 （当前仅包括 SNMP 告警）。	第 32-29 页上的添加 SNMP 告警
	向规则添加的注释。	第 32-30 页上的添加规则注释

也可以使用层下拉列表切换到策略中其他层的 Rules 页面。请注意，除非将层添加到策略中，否则下拉列表中列出的唯一可编辑视图为策略的 Rules 页面和最初命名为 `My Changes` 的策略层的 Rules 页面；另请注意，在这些视图中进行更改与在其他视图中进行更改相同。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。该下拉列表中还会列出只读基本策略的 Rules 页面。有关基本策略的详细信息，请参阅第 24-2 页上的了解基本层。

要查看入侵策略中的规则，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 Policy Information 页面中的 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

请注意，选择导航面板中的分割线以上的 **Rules** 会转到相同的规则列表。在此视图中可查看和设置策略中的所有规则属性。

对规则的显示排序

许可证：保护

点击标题或图标可按 Rules 页面中的任意列对规则排序。

请注意，标题或图标上的向上 (▲) 或向下 (▼) 箭头表示目前是按该列的这个方向排序。

要对入侵策略中的规则排序，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　点击要按其排序的列顶部的标题或图标。

此时将按列标题上显示的箭头所指示的方向依据该列对规则排序。要按相反方向排序，请再次点击标题。排序顺序和箭头都将颠倒过来。

查看规则详细信息

许可证：保护

在 Rule Detail 视图中，可以查看规则文档、 FireSIGHT 建议和规则开销。还可以查看和添加规则专用的功能。

请注意，本地规则没有任何开销，除非被映射到漏洞。

表 32-3　规则详细信息

项目	说明	有关详细信息，请参阅.....
Summary	规则摘要。对基于规则的事件，此行将在规则文档包含摘要信息时显示。	第 41-20 页上的查看事件信息
Rule State	规则的当前规则状态。也表示设置规则状态所在的层。	第 32-18 页上的设置规则状态；第 24-1 页上的在网络分析或入侵策略中使用层
FireSIGHT Recommendation	如果已生成 FireSIGHT 建议，则为建议的规则状态。	第 33-1 页上的为您的网络资产定制入侵防御
Rule Overhead	规则对系统性能的潜在影响以及规则产生误报的可能性。	第 33-3 页上的了解规则开销
Thresholds	当前为此规则设置的阈值，以及用于为该规则添加阈值的工具。	第 32-6 页上的为规则设置阈值
Suppressions	当前为此规则设置的抑制设置，以及用于为该规则添加抑制的工具。	第 32-6 页上的为规则设置抑制
Dynamic State	当前为此规则设置的基于速率的规则状态，以及用于为该规则添加动态规则状态的工具。	第 32-7 页上的为规则设置动态规则状态
Alerts	当前为此规则设置的告警，以及用于为该规则添加告警的工具。目前，只有 SNMP 告警受支持。	第 32-8 页上的为规则设置 SNMP 告警
Comments	向此规则添加的注释，以及用于为该规则添加注释的工具。	第 32-8 页上的为规则添加规则注释
Documentation	当前规则的规则文档，由思科漏洞研究团队 (VRT) 提供。	第 41-23 页上的使用数据包视图操作

要查看规则详细信息，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　突出显示要查看其规则详细信息的规则。

步骤 5　点击 **Show details**。

系统将显示 Rule Detail 视图。要重新隐藏详细信息，请点击 **Hide details**。

提示　双击 Rules 视图中的规则也可打开 Rule Detail。

为规则设置阈值

许可证：保护

您可以在 Rule Detail 页面中为规则设置一个阈值。添加阈值将覆盖该规则的任何现有阈值。有关阈值的详细信息，请参阅第 32-20 页上的配置事件阈值。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清空该字段的值。

要在规则详细信息中设置阈值，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　点击 **Thresholds** 旁边的 **Add**。

系统将显示 Set Threshold 对话框。

步骤 2　从 **Type** 下拉列表中选择要设置的阈值的类型：

- 选择 **Limit** 则在每个时间段内只为指定数量的事件实例提供通知。
- 选择 **Threshold** 则在每个时间段内每次事件实例数达到指定数量时提供通知。
- 选择 **Both** 则在每个时间段内事件实例数达到指定数量后提供一次通知。

步骤 3　从 **Track By** 下拉列表中选择 **Source** 或 **Destination** 以指示要按源还是目标 IP 地址跟踪事件实例。

步骤 4　在 **Count** 字段中，键入要用作阈值的事件实例数。

步骤 5　在 **Seconds** 字段中键入一个介于 0 和 2147483647 之间的数字来指定跟踪事件实例的时间段（以秒为单位）。

步骤 6　点击 **OK**。

系统将添加阈值并在 Event Filtering 列中该规则旁显示事件过滤器图标 ( )。如果将多个事件过滤器添加到规则，系统将在图标上注明事件过滤器的数量。

为规则设置抑制

许可证：保护

您可以在 Rule Detail 页面中为规则设置一个或多个抑制。有关抑制的详细信息，请参阅第 32-24 页上的按入侵策略配置抑制。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清空该字段的值。

要在规则详细信息中设置抑制，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　点击 **Suppressions** 旁边的 **Add**。

系统将显示 Add Suppression 对话框。

步骤 2　从 **Suppression Type** 下拉列表中选择以下选项之一：

- 选择 **Rule** 将完全抑制所选规则的事件。
- 选择 **Source** 将抑制由指定源 IP 地址发出的数据包生成的事件。
- 选择 **Destination** 将抑制由发往指定目标 IP 地址的数据包生成的事件。

步骤 3　如果为抑制类型选择 **Source** 或 **Destination**，系统将显示 Network 字段。在 **Network** 字段中，输入 IP 地址、地址块或由这些内容的任意组合组成的逗号分隔列表。当入侵策略与一个访问控制策略的默认操作相关联时，还可以在默认操作变量集中指定或列出网络变量。

有关在 FireSIGHT 系统中使用 IPv4 CIDR 和 IPv6 前缀长度地址块的详细信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 4　点击 **OK**。

系统将添加抑制条件并在 Event Filtering 列中被抑制的该规则旁显示事件过滤器图标 ( )。如果将多个事件过滤器添加到规则，图标上的数字表示过滤器的数量。

为规则设置动态规则状态

许可证：保护

您可以在 Rule Detail 页面中为规则设置一个或多个动态规则状态。列出的第一个动态规则状态的优先级最高。请注意，当两个动态规则状态相冲突时，将执行第一个状态的操作。有关动态规则状态的详细信息，请参阅第 32-26 页上的了解动态规则状态。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清空该字段的值。

要在规则详细信息中设置动态规则状态，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　点击 **Dynamic State** 旁边的 **Add**。

系统将显示 Add Rate-Based Rule State 对话框。

步骤 2　从 **Track By** 下拉列表中选择一个选项，以指示如何跟踪规则匹配项：

- 选择 **Source** 将跟踪由特定的一个或一组源地址发出的该规则匹配项的数量。
- 选择 **Destination** 将跟踪发往特定的一个或一组目标地址的该规则匹配项的数量。
- 选择 **Rule** 将跟踪该规则的所有匹配项。

步骤 3　或者，在将 **Track By** 设置为 **Source** 或 **Destination** 时，在 **Network** 字段中输入要跟踪的每台主机的 IP 地址。

有关在 FireSIGHT 系统中使用 IPv4 CIDR 和 IPv6 前缀长度表示法的详细信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 4　下一个是 **Rate**，指示每个时间段的规则匹配项数量，用于设置攻击速率：

- 在 **Count** 字段中，使用 0 到 2147483647 之间的整数指定要用作阈值的规则匹配项数量。
- 在 **Seconds** 字段中，使用 0 到 2147483647 之间的整数指定构成时间段的秒数，系统将跟踪该时间段内的攻击。

步骤 5　从 **New State** 下拉列表中选择满足条件时应执行的新操作。

- 选择 **Generate Events** 将生成事件。
- 选择 **Drop and Generate Events** 将在内联部署中生成事件并丢弃触发该事件的数据包，或在被动部署中生成事件。
- 选择 **Disabled** 将不执行任何操作。

步骤 6　在 **Timeout** 字段中，使用 1 到 2147483647（约为 68 年）之间的整数，键入希望新操作保持有效的秒数。在超时后，规则将恢复到原始状态。指定 0 可防止新操作超时。

步骤 7　点击 **OK**。

系统将添加动态规则状态并在 Dynamic State 列中该规则旁显示动态状态图标 ( )。如果将多个动态规则状态过滤器添加到规则，图标上的数字表示过滤器的数量。

如果将任何必填字段留空，您将收到错误消息，指出哪些字段必须填写。

为规则设置 SNMP 告警

许可证：保护

您可以在 Rule Detail 页面中为规则设置 SNMP 告警。有关 SNMP 告警的详细信息，请参阅第 32-29 页上的添加 SNMP 告警。

要在规则详细信息中添加 SNMP 告警，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　点击 **Alerts** 旁边的 **Add SNMP Alert**。

系统将添加告警并在 Alerting 列中该规则旁显示告警图标 ( )。如果将多个告警添加到规则，系统将在图标上注明告警的数量。

为规则添加规则注释

许可证：保护

您可以在 Rule Detail 页面中为规则添加规则注释。有关规则注释的详细信息，请参阅第 32-30 页上的添加规则注释。

要在规则详细信息中添加注释，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　点击 **Comments** 旁边的 **Add**。

系统将显示 Add Comment 对话框。

步骤 2　在 **Comment** 字段中，键入规则注释。

步骤 3　点击 **OK**。

系统将添加注释并在 Comments 列中该规则旁显示注释图标 ( )。如果将多个注释添加到规则，图标上的数字表示注释的数量。

提示　要删除规则注释，请点击规则注释部分的 **Delete**。请注意，只能删除尚未提交的入侵策略更改所缓存的注释。一旦入侵策略更改提交之后，规则注释就是永久性的。

过滤入侵策略中的规则

许可证：保护

可以按单一条件或按一个或多个条件的组合来过滤 Rules 页面中显示的规则。

您所构造的过滤器显示于 Filter 文本框中。点击过滤器面板中的关键字和关键字参数可以构造过滤器。当选择多个关键字时，系统会使用 AND 逻辑将其合并，创建合成的搜索过滤器。例如，如果选择 **Category** 下的 **preprocessor**，然后选择 **Rule Content > GID** 并输入 `116`，会得到过滤器 `Category: "preprocessor" GID:"116"`，检索属于预处理器规则**而且** GID 为 116 的所有规则。

Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific、Preprocessor 和 Priority 过滤器组可以为一个关键字提交多个参数，以逗号分隔。例如，按住 Shift，然后从 **Category** 中选择 **os-linux** 和 **os-windows** 得到过滤器 `Category:"os-windows,os-linux"`，检索 `os-linux` 类别中或 `os-windows` 类别中的任意规则。

要显示过滤器面板，请点击显示图标 ( )。

要隐藏过滤器面板，请点击隐藏图标 ( )。

有关详细信息，请参阅以下主题：

- 第 32-9 页上的了解入侵策略中的规则过滤
- 第 32-16 页上的在入侵策略中设置规则过滤器

了解入侵策略中的规则过滤

许可证：保护

规则过滤器关键字可帮助您找到要对其应用规则状态或事件过滤器等规则设置的规则。您可以按关键字进行过滤，同时从 Rules 页面的过滤器面板选择所需参数作为关键字的参数。

有关详细信息，请参阅以下各节：

- 第 32-9 页上的构造入侵策略规则过滤器的指导原则
- 第 32-11 页上的了解规则配置过滤器
- 第 32-14 页上的了解规则内容过滤器
- 第 32-15 页上的了解规则类别
- 第 32-15 页上的直接编辑规则过滤器

构造入侵策略规则过滤器的指导原则

许可证：保护

在大多数情况下，构建过滤器时可以在入侵策略中使用 Rules 页面左侧的过滤器面板来选择要使用的关键字/参数。

规则过滤器在过滤器面板中分为不同的规则过滤器组。许多规则过滤器组包含子条件，因此可以更轻松地找到所需的特定规则。某些规则过滤器有多个级别，可以展开后向下找到各个规则。

过滤器面板中的项目有时代表过滤器类型组，有时代表关键字，还有时代表关键字的参数。以下经验法则可以帮助您构建过滤器：

- 当选择不是关键字的过滤器类型组标题 （Rule Configuration、 Rule Content、 Platform Specific 和 Priority）时，该标题会展开并列出可用的关键字。

  点击条件列表中的节点选择关键字时将显示一个弹出窗口，供您提供要作为过滤条件的参数。

如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

例如，如果点击过滤器面板中 **Rule Configuration > Recommendation** 下的 **Drop and Generate Events**，`Recommendation:"Drop and Generate Events"` 会被添加到过滤器文本框中。如果随后点击 **Rule Configuration > Recommendation** 下的 **Generate Events**，过滤器将更改为 `Recommendation:"Generate Events"`。

- 当选择属于关键字的过滤器类型组标题 （Category、 Classifications、 Microsoft Vulnerabilities、 Microsoft Worms、 Priority 和 Rule Update）时，该标题会列出可用参数。

  从这种类型的组中选择项目时，该参数及其应用到的关键字将立即添加到过滤器中。如果该关键字已经在过滤器中，它将替换与该组对应的关键字的现有参数。

  例如，如果点击过滤器面板上 **Category** 下的 **os-linux**，`Category:"os-linux"` 会被添加到过滤器文本框中。如果随后点击 **Category** 下的 **os-windows**，过滤器将更改为 `Category:"os-windows"`。

- Rule Content 下的 Reference 是关键字，其下方列出的具体引用 ID 类型同样如此。选择任何引用关键字时，系统都会显示一个弹出窗口，供您运用参数并向现有过滤器添加关键字。如果过滤器中已在使用该关键字，则提供的新参数将替换现有参数。

  例如，如果点击过滤器面板中的 **Rule Content > Reference > CVE ID**，系统将显示弹出窗口，提示您提供 CVE ID。如果输入 `2007`，则 `CVE:"2007"` 会被添加到过滤器文本框中。又如，如果点击过滤器面板中的 **Rule Content > Reference**，系统将显示弹出窗口，提示您提供该引用。如果输入 `2007`，则 `Reference:"2007"` 会被添加到过滤器文本框中。

- 当从不同的组中选择规则过滤器关键字时，会将每个过滤器关键字都添加到过滤器中并保留所有现有关键字 （除非被同一关键字的新值覆盖）。

  例如，如果点击过滤器面板中 **Category** 下的 **os-linux**，`Category:"os-linux"` 会被添加到过滤器文本框中。如果随后点击 **Microsoft Vulnerabilities** 下的 **MS00-006**，过滤器将更改为 `Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`。

- 当选择多个关键字时，系统会使用 AND 逻辑将其合并，创建合成的搜索过滤器。例如，如果选择 **Category** 下的 **preprocessor**，然后选择 **Rule Content > GID** 并输入 `116`，会得到过滤器 `Category: "preprocessor" GID:"116"`，检索属于预处理器规则**而且** GID 为 116 的所有规则。

- Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific 和 Priority 过滤器组可以为一个关键字提交多个参数，以逗号分隔。例如，按住 Shift，然后从 **Category** 中选择 **os-linux** 和 **os-windows** 得到过滤器 `Category:"os-windows,os-linux"`，检索 `os-linux` 类别中或 `os-windows` 类别中的任意规则。

同一规则可以按多个过滤器关键字/参数对进行检索。例如，如果按 **dos** 类别过滤规则，系统将显示 DOS Cisco 尝试规则 (SID 1545)，按 **High** 优先级进行过滤亦如此。

注　思科 VRT 可能会使用规则更新机制来添加和删除规则过滤器。

请注意， Rules 页面中的规则可以是共享对象规则 （生成器 ID 为 3），也可以是标准文本规则（生成器 ID 为 1）。下表介绍不同的规则过滤器。

表 32-4　规则过滤器组

过滤器组	说明	是否支持多个参数？	标题为……	列表中的项目为……
Rule Configuration	根据规则的配置查找规则。请参阅第 32-11 页上的了解规则配置过滤器。	否	组	关键词
Rule Content	根据规则的内容查找规则。请参阅第 32-14 页上的了解规则内容过滤器。	否	组	关键词

表 32-4　规则过滤器组 （续）

过滤器组	说明	是否支持多个参数？	标题为……	列表中的项目为……
Category	根据规则编辑器使用的规则类别来查找规则。请注意，本地规则显示于本地子组中。请参阅第 32-15 页上的了解规则类别。	是	关键字	参数
Classifications	根据规则生成的事件的数据包显示中所显示的攻击分类来查找规则。请参阅第 41-36 页上的搜索入侵事件和第 36-11 页上的定义入侵事件分类。	否	关键字	参数
Microsoft Vulnerabilities	根据 Microsoft 公告号查找规则。	是	关键字	参数
Microsoft Worms	根据影响 Microsoft Windows 主机的特定蠕虫查找规则。	是	关键字	参数
Platform Specific	根据规则与特定操作系统版本的相关性来查找规则。 请注意，规则可能会影响多个操作系统或某个操作系统的多个版本。例如，启用 SID 2260 会影响多个版本的 Mac OS X、 IBM AIX 以及其他操作系统。	是	关键字	参数 请注意，如果从子列表中选择一个项目，则会将一个修饰符添加到参数。
Preprocessors	查找各个预处理器的规则。 请注意，在启用预处理器时，必须启用与预处理器选项相关联的预处理器规则才能生成该选项的事件，请参阅第 32-18 页上的设置规则状态。	是	组	子组
Priority	根据高、中和低优先级查找规则。 分配给规则的分类将确定该规则的优先级。这些组进一步分为不同的规则类别。请注意，本地规则（即您创建的规则）不会显示于优先级组中。	是	关键字	参数 请注意，如果从子列表中选择一个项目，则会将一个修饰符添加到参数。
Rule Update	查找通过特定规则更新添加或修改的规则。对于每个规则更新，可以查看该更新中的所有规则、仅查看更新中导入的新规则或仅查看更新所更改的现有规则。	否	关键字	参数

了解规则配置过滤器

许可证：保护

您可以按多个规则配置设置来过滤 Rules 页面中列出的规则。例如，如果要查看规则状态与建议的规则状态不匹配的一组规则，可以选择 **Does not match recommendation** 来根据规则状态进行过滤。

点击条件列表中的节点选择关键字时将显示一个弹出窗口，供您提供要作为过滤条件的参数。

如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

例如，如果点击过滤器面板中 **Rule Configuration > Recommendation** 下的 **Drop and Generate Events**，`Recommendation:"Drop and Generate Events"` 会被添加到过滤器文本框中。如果随后点击 **Rule Configuration > Recommendation** 下的 **Generate Events**，过滤器将更改为 `Recommendation:"Generate Events"`。

有关可用于过滤的规则配置设置的详细信息，请参阅以下操作步骤。

要使用 Rule State 过滤器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 **Rule Configuration** 下，点击 **Rule State**。

步骤 2　从 **Rule State** 下拉列表中选择要作为过滤条件的规则状态：

- 要查找只生成事件的规则，请选择 **Generate Events**，然后点击 **OK**。
- 要查找设置为生成事件并丢弃匹配的数据包的规则，请选择 **Drop and Generate Events**，然后点击 **OK**。
- 要查找已禁用的规则，请选择 **Disabled**，然后点击 **OK**。
- 要查找规则状态与建议的状态不匹配的规则，请选择 **Does not match recommendation**，然后点击 **OK**。

Rules 页面将更新，根据当前的规则状态显示规则。

要使用 Recommendation 过滤器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 **Rule Configuration** 下，点击 **Recommendation**。

步骤 2　从 **Recommendation** 下拉列表中选择要作为过滤条件的 FireSIGHT 规则状态建议，然后点击 **OK**。

Rules 页面将更新，根据建议的规则状态显示规则。

要使用 Threshold 过滤器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 **Rule Configuration** 下，点击 **Threshold**。

步骤 2　从 **Threshold** 下拉列表中选择要作为过滤条件的阈值设置：

- 要查找阈值类型为 `limit` 的规则，请选择 **Limit**，然后点击 **OK**。
- 要查找阈值类型为 `threshold` 的规则，请选择 **Threshold**，然后点击 **OK**。
- 要查找阈值类型为 `both` 的规则，请选择 **Both**，然后点击 **OK**。
- 要查找按 `source` 跟踪阈值的规则，请选择 **Source**，然后点击 **OK**。
- 要查找按 `destination` 跟踪阈值的规则，请选择 **Destination**，然后点击 **OK**。
- 要查找设置了阈值的所有规则，请选择 **All**，然后点击 **OK**。

Rules 页面将更新，显示已经应用了过滤器中所示类型的阈值的规则。

要使用 Suppression 过滤器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 **Rule Configuration** 下，点击 **Suppression**。

步骤 2　从 **Suppression** 下拉列表中选择要作为过滤条件的抑制设置：

- 要查找面向该规则所检查的数据包抑制事件的规则，请选择 **By Rule**，然后点击 **OK**。
- 要查找根据流量的源地址抑制事件的规则，请选择 **By Source**，然后点击 **OK**。
- 要查找根据流量的目标地址抑制事件的规则，请选择 **By Destination**，然后点击 **OK**。
- 要查找设置了抑制的所有规则，请选择 **All**，然后点击 **OK**。

Rules 页面将更新，显示已经应用了过滤器中所示类型的抑制的规则。

要使用 Dynamic State 过滤器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在**Rule Configuration** 下，点击 **Dynamic State**。

步骤 2　从 **Dynamic State** 下拉列表中选择要作为过滤条件的抑制设置：

- 要查找为该规则所检查的数据包配置动态状态的规则，请选择 **By Rule**，然后点击 **OK**。
- 要查找根据流量的源地址为数据包配置动态状态的规则，请选择 **By Source**，然后点击 **OK**。
- 要查找根据流量的目标地址配置动态状态的规则，请选择 **By Destination**，然后点击 **OK**。
- 要查找已配置 `Generate Events` 动态状态的规则，请选择 **Generate Events**，然后点击 **OK**。
- 要查找已配置 `Drop and Generate Events` 动态状态的规则，请选择 **Drop and Generate Events**，然后点击 **OK**。
- 要查找已配置 `Disabled` 动态状态的规则，请选择 **Disabled**，然后点击 **OK**。
- 要查找设置了抑制的所有规则，请选择 **All**，然后点击 **OK**。

Rules 页面将更新，显示已经应用了过滤器中所示动态规则状态的规则。

要使用告警过滤器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 **Rule Configuration** 下，点击 **Alert**。

步骤 2　从 **Alert** 下拉列表中选择要作为过滤条件的告警设置：**SNMP**。

步骤 3　点击 **OK**。

Rules 页面更新显示您已应用告警过滤器的规则。

要使用 Comment 过滤器，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 **Rule Configuration** 下，点击 **Comment**。

步骤 2　在 **Comment** 字段中，键入要作为过滤依据的注释文本字符串，然后点击 **OK**。

Rules 规则页面将更新，显示对规则应用的注释中包含过滤器中所示字符串的规则。

了解规则内容过滤器

许可证：保护

您可以按多个规则内容项来过滤 Rules 页面中列出的规则。例如，通过搜索规则的 SID 可以快速检索到该规则。也可以查找用于检查发往特定目标端口的流量的所有规则。

点击条件列表中的节点选择关键字时将显示一个弹出窗口，供您提供要作为过滤条件的参数。

如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

例如，如果点击过滤器面板中 **Rule Content** 下的 **SID**，系统将显示弹出窗口，提示您提供 SID。如果键入 `1045`，则 `SID:"1045"` 会被添加到过滤器文本框中。如果随即再次点击 **SID** 并将 SID 过滤器更改为 `1044`，过滤器将更改为 `SID:"1044"`。

有关可用于过滤的规则内容的详细信息，请参阅下表。

表 32-5　Rule Content 过滤器

要使用此过滤器，请点击……	然后……	结果
通信	键入要作为过滤条件的消息字符串并点击 **OK**。	查找消息字段中包含所提供字符串的规则。
SID	键入要作为过滤条件的 SID 编号并点击 **OK**。	查找 SID 为指定值的规则。
GID	键入要作为过滤条件的 GID 编号并点击 **OK**。	查找 GID 为指定值的规则。
参考编号	键入要作为过滤条件的引用字符串并点击 **OK**。 要为作为过滤条件的特定引用类型输入字符串，请选择 **CVE ID**、**URL**、**Bugtraq ID**、**Nessus ID**、**Arachnids ID** 或 **Mcafee ID**，然后键入字符串并点击 **OK**。	查找引用字段中包含所提供字符串的规则。
操作	选择要作为过滤条件的操作： • 要查找告警规则，请选择 **Alert**，然后点击 **OK**。 • 要查找通过规则，请选择 **Pass**，然后点击 **OK**。	查找以 `alert` 或 `pass` 开头的规则。
协议	选择要作为过滤条件的协议：**ICMP**、**IP**、**TCP** 或 **UDP**；然后点击 **OK**。	查找包含所选协议的规则。
方向	选择要作为过滤条件的方向设置： • 要查找用于检查按特定方向传输的流量的规则，请选择 **Directional**，然后点击 **OK**。 • 要查找用于检查在源地址与目标地址之间按任意方向传输的流量的规则，请选择 **Bidirectional**，然后点击 **OK**。	根据规则是否包含指示的方向设置来查找规则。

表 32-5　Rule Content 过滤器（续）

要使用此过滤器，请点击……	然后……	结果
源 IP：	键入要作为过滤条件的源 IP 地址，然后点击 **OK**。 请注意，您可以根据有效 IP 地址、 CIDR 块/前缀长度或者使用 `$HOME_NET` 或 `$EXTERNAL_NET` 等变量进行过滤。	查找使用指定的地址或变量作为规则中的源 IP 地址标识的规则。
目标 IP：	键入要作为过滤条件的目标 IP 地址，然后点击 **OK**。 请注意，您可以根据有效 IP 地址、 CIDR 块/前缀长度或者使用 `$HOME_NET` 或 `$EXTERNAL_NET` 等变量进行过滤。	查找使用指定的地址或变量作为规则中的源 IP 地址标识的规则。
Source port	键入要作为过滤条件的源端口，然后点击 **OK**。 端口值必须为 1 到 65535 之间的整数或端口变量。	查找包含指定源端口的规则。
目标端口	键入要作为过滤条件的目标端口，然后点击 **OK**。 端口值必须为 1 到 65535 之间的整数或端口变量。	查找包含指定目标端口的规则。
Rule Overhead	选择要作为过滤条件的规则开销数量：**Low**、**Medium**、 **High** 或 **Very High**；然后点击 **OK**。	查找具有规则开销为所选值的规则。
元数据	键入要作为过滤条件的元数据键值对，以空格分隔；然后点击 **OK**。 例如，键入 `metadata:"service http"` 可查找元数据与 HTTP 应用协议相关的规则。	查找元数据包含匹配的键值对的规则。

了解规则类别

许可证：保护

FireSIGHT 系统根据规则检测的流量类型对规则分类。在 Rules 页面中，可以按规则类别过滤，以便为某个类别的所有规则设置规则属性。例如，如果网络中没有 Linux 主机，可以按 **os-linux** 类别过滤，然后禁用显示的所有规则，从而禁用整个 **os-linux** 类别。

将鼠标指针悬停在类别名称的上方可以显示该类别中的规则数量。

注　思科 VRT 可能会使用规则更新机制来添加和删除规则类别。

直接编辑规则过滤器

许可证：保护

通过编辑过滤器可以修改您在过滤器面板中点击过滤器时所提供的特定关键字及其参数。 Rules 页面中的自定义过滤器的功能与规则编辑器中使用的过滤器类似，但除此之外，您还可以使用在 Rules 页面过滤器中提供的任何关键字，使用在过滤器面板中选择过滤器时显示的语法。要确定供今后使用的关键字，请点击右侧过滤器面板中的相应参数。过滤器关键字和参数语法显示于过滤器文本框中。

要查看仅支持特定值的关键字参数列表，请参阅第 32-11 页上的了解规则配置过滤器、第 32-14 页上的了解规则内容过滤器和第 32-15 页上的了解规则类别。请记住，只有 Category 和 Priority 过滤器类型支持关键字有多个以逗号分隔的参数。

您可以使用关键字和参数、字符串及带引号的原义字符串，以空格分隔多个过滤条件。过滤器不能包含正则表达式、通配符或任何特殊运算符，例如取反字符 (!)、大于号 (>) 和小于号 (<) 等。当键入的搜索条件没有关键字、关键字的首字母没有大写或者没有用引号将参数引起来时，该搜索将被视为字符串搜索，并搜索类别、消息和 SID 字段中有无指定条件。

所有关键字、关键字参数和字符串都不区分大小写。除关键字 `gid` 和 `sid` 之外，所有参数和字符串都被视为部分字符串。`gid` 和 `sid` 的参数只会返回完全匹配项。

每个规则过滤器都可以包含一个或多个关键字，其格式如下：

`Keyword:"argument"`

其中，*`keyword`* 是规则类型表中所述过滤器组中的关键字之一，而 *`argument`* 则是要在与该关键字相关的一个或多个指定字段中搜索的一个字母数字字符串，需用双引号引起来且不区分大小写。请注意，键入的关键字应该首字母大写。

除 `gid` 和 `sid` 之外的所有关键字的参数都会被视为部分字符串。例如，参数 `123` 将返回 `"12345"`、`"41235"`、`"45123"` 等结果。`gid` 和 `sid` 的参数只会返回完全匹配项；例如，`sid:3080` 只会返回结果 `SID 3080`。

每个规则过滤器还可以包含一个或多个字母数字字符串。字符串将搜索规则的 Message 字段、Signature ID 和 Generator ID。例如，字符串 `123` 会返回规则消息中的 `"Lotus123"`、`"123mania"` 等字符串，也会返回 `SID 6123`、`SID 12375` 等。有关规则的 Message 字段的详细信息，请参阅第 36-10 页上的定义事件消息。有关规则的 SID 和 GID 的详细信息，请参阅第 41-34 页上的解读预处理器生成器 ID。使用一个或多个字符串来进行过滤可以搜索部分 SID。

所有字符串都不区分大小写并被视为部分字符串。例如，`ADMIN`、`admin` 或 `Admin` 等字符串中任意一个字符串都会返回 `"admin"`、`"CFADMIN"`、`"Administrator"` 等结果。

用引号将字符串引起来可以返回完全匹配项。例如，用引号引起来的原义字符串 `"overflow attempt"` 只会返回完全匹配的该字符串，而由 `overflow` 和 `attempt` 这两个字符串组成的未加引号的过滤器则会返回 `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` 等结果。

输入关键字、文字字符串或这二者的任意组合并以空格分隔可以缩小过滤结果的范围。结果包括符合所有过滤条件的任意规则。

可以按照任意顺序输入多个过滤条件。例如，以下每个过滤器返回的规则相同：

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

在入侵策略中设置规则过滤器

许可证：保护

您可以对 Rules 页面中的规则进行过滤来显示其中一组规则。然后，您可以使用该页面的任何功能，包括选择上下文菜单中可用的任何功能。例如，当您需要为某个特定类别的所有规则设置阈值时，此功能会非常有用。您可以对已过滤或未过滤列表中的规则使用相同的功能。例如，您可以将新的规则状态应用到已过滤或未过滤列表中的规则。

可以从入侵策略中 Rules 页面左侧的过滤器面板中选择预定义的过滤器关键字。选择过滤器时，该页面会显示所有匹配的规则，或者指出没有匹配的规则。

有关可以使用的所有关键字和参数以及如何在过滤器面板中构造过滤器的详细信息，请参阅第 32-9 页上的了解入侵策略中的规则过滤。

您可以对过滤器添加关键字来进一步对其进行限制。输入的任何过滤器都会搜索整个规则数据库并返回所有匹配的规则。当您在页面仍显示上一过滤器的结果时输入过滤条件，页面将清空，转而返回新过滤器的结果。

您也可以使用在选择过滤器时提供的相同关键字和参数语法来键入过滤条件，或者在选择过滤器后修改其中的参数值。当键入的搜索条件没有关键字、关键字的首字母没有大写或者没有用引号将参数引起来时，该搜索将被视为字符串搜索，并搜索类别、消息和 SID 字段中有无指定条件。

要过滤入侵策略中的特定规则，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　点击左侧过滤器面板中的关键字或参数构造过滤器。请注意，如果点击过滤器中已存在的关键字的参数，则该参数将替换现有的参数。有关详情，请参阅：

- 第 32-9 页上的构造入侵策略规则过滤器的指导原则
- 第 32-11 页上的了解规则配置过滤器
- 第 32-14 页上的了解规则内容过滤器
- 第 32-15 页上的了解规则类别
- 第 32-15 页上的直接编辑规则过滤器

页面将刷新，显示所有匹配的规则，而与该过滤器匹配的规则数量将显示于过滤器文本框的上方。

步骤 5　选择要在其中应用新设置的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　或者，对规则作出通常会在该页面上作出的任何更改。有关详细信息，请参阅以下各节：

- 有关在 Rules 页面中启用和禁用规则的详细信息，请参阅第 32-18 页上的设置规则状态。
- 有关向规则添加阈值和抑制的详细信息，请参阅第 32-20 页上的按策略过滤入侵事件通知。
- 有关如何设置在匹配的流量中发生速率异常时触发的动态规则状态的详细信息，请参阅第 32-26 页上的添加动态规则状态。
- 有关向具体规则添加 SNMP 告警的详细信息，请参阅第 32-29 页上的添加 SNMP 告警。
- 有关向规则添加规则注释的信息，请参阅第 32-30 页上的添加规则注释。

步骤 7　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。

有关详细信息，请参阅第 31-3 页上的管理入侵策略和第 31-4 页上的编辑入侵策略。

设置规则状态

许可证：保护

思科漏洞研究团队 (VRT) 为每个默认策略中的每条入侵规则和预处理器规则设置了默认状态。例如，一条规则可能会在 Security over Connectivity 默认策略中启用而在 Connectivity over Security 默认策略中禁用。您创建的入侵策略规则将继承用于创建该策略的默认策略中相应规则的默认状态。

您可以将规则逐一设置为 Generate Events、Drop and Generate Events 或 Disable，也可以按各种因素过滤规则以选择要修改其状态的规则。在内联部署中，可以在内联入侵部署中使用 Drop and Generate Events 规则状态来丢弃恶意数据包。请注意，在被动部署中，包括当 3D9900 或 3 系列设备的内联接口设置处于分路模式时，规则状态为 Drop and Generate Events 的规则会生成事件但不会丢弃数据包，将规则设置为 Generate Events 或 Drop and Generate Events 可启用该规则；将规则设置为 Disable 将禁用该规则。

我们以两种情况为例。在第一种情况下，特定规则的规则状态被设置为 Generate Events。当恶意数据包通过网络并触发该规则时，数据包被发送到其目标，系统生成入侵事件。在第二种情况下，假设同一规则的规则状态在内联部署中被设置为 Drop and Generate Events。在此情况下，当恶意数据包通过网络时，系统会丢弃恶意数据包并生成入侵事件。该数据包永远不会到达其目标。

在入侵策略中，可将规则的状态设置为以下设置之一：

- 如果需要系统检测特定的入侵企图并在发现匹配的流量时生成入侵事件，可将规则状态设置为 **Generate Events**。
- 如果需要系统检测特定的入侵企图，然后在内联部署中发现匹配的流量时丢弃包含攻击的数据包并生成入侵事件，或者在被动部署 （包括当 3D9900 或 3 系列设备的内联接口设置处于分路模式时）中发现匹配的流量时生成入侵事件，可将规则状态设置为 **Drop and Generate Events**。

  请注意，要让系统丢弃数据包，在内联部署中必须将入侵策略设置为丢弃规则；有关详细信息，请参阅第 31-5 页上的在内联部署中设置丢弃行为。
- 如果不需要系统评估匹配的流量，可将规则状态设置为 **Disable**。

要使用丢弃规则，必须：

- 在入侵策略中启用 **Drop when Inline** 选项。
- 对于所有应该丢弃与其匹配的数据包的规则，将规则状态设置为 **Drop and Generate Events**。
- 找到包含与入侵策略相关联的访问控制规则的访问控制策略，将其应用到使用内联设置的受管设备。

在 Rules 页面中过滤规则可帮助您找到要设置为丢弃规则的规则。有关详细信息，请参阅第 32-9 页上的过滤入侵策略中的规则。

有关规则剖析、规则关键字及其选项和规则编写语法的详细信息，请参阅第 36-1 页上的了解和编写入侵规则。

VRT 有时会使用规则更新来更改默认策略中一条或多条规则的默认状态。如果允许规则更新对基本策略进行更新，则意味着当用于创建策略的默认策略中的默认状态发生更改时，也允许规则更新更改策略中的规则默认状态。但请注意，如果您已经更改了规则状态，规则更新不会覆盖您的更改。

要更改一条或多条规则的规则状态，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

请注意，此页面指出了已启用规则的总数、设置为 Generate Events 的已启用规则总数以及设置为 Drop and Generate Events 的总数。还应注意，在被动部署中，设置为 Drop and Generate Events 的规则仅生成事件。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　查找要在其中设置规则状态的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅以下主题：第 32-9 页上的了解入侵策略中的规则过滤和第 32-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择要在其中设置规则状态的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　您有以下选项：

- 要在流量与所选规则匹配时生成事件，请选择 **Rule State > Generate Events**。
- 要在流量与所选规则匹配时在内联部署中生成事件并丢弃流量，请选择 **Rule State > Drop and Generate Events**。
- 如果要不检查与所选规则匹配的流量，请选择 **Rule State > Disable**。

注　思科**强烈**建议**不要**启用入侵策略中的所有入侵规则。如果启用所有规则，受管设备的性能可能会下降。相反，应调整规则集，使之与网络环境尽可能相符。

步骤 7　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详细信息，请参阅第 31-3 页上的管理入侵策略和第 31-4 页上的编辑入侵策略。

按策略过滤入侵事件通知

许可证：保护

入侵事件的重要性可根据发生的频率或者源或目标 IP 地址而定。在某些情况下，您可能并不在意发生不到一定次数的事件。例如，如果有人企图登录服务器，在其失败达到一定次数之前，您可能不会关心。但在其他情况下，也许只需要发生几次，就能让您知道存在普遍性问题。例如，如果有人对网络服务器发动 DoS 攻击，可能只需要发生区区数次入侵事件，您就会明白需要解决这种情况。发生数百次相同事件只会让系统不堪重负。

有关详细信息，请参阅以下各节：

- 第 32-20 页上的配置事件阈值说明如何根据发生次数设置指定显示事件频率的阈值。您可以按事件和按策略配置阈值。
- 第 32-24 页上的按入侵策略配置抑制说明如何按源或目标 IP 地址、按策略抑制指定事件的通知。

配置事件阈值

许可证：保护

您可以按入侵策略为每条规则设置阈值，以根据在指定时间段内生成事件的次数来限制系统记录和显示入侵事件的次数。这可以防止因相同事件数量过多而使系统不堪重负。您可以按每条共享对象规则、标准文本规则或预处理器规则设置阈值。

有关详细信息，请参阅以下各节：

- 第 32-20 页上的了解事件阈值
- 第 32-21 页上的添加和修改入侵事件阈值
- 第 32-23 页上的查看和删除入侵事件阈值
- 第 32-6 页上的为规则设置阈值

了解事件阈值

许可证：保护

首先，必须指定阈值类型。可以选择的选项如下表所述。

表 32-6　阈值选项

选项	说明
Limit	为指定时间段内触发规则的指定数量的数据包 （由 Count 参数指定）记录并显示事件。例如，如果将类型设置为 **Limit**，将 **Count** 设置为 10，并将 **Seconds** 设置为 60，而同一分钟内有 14 个数据包触发规则，则系统在显示发生的前 10 个违反该规则的事件后将停止记录违反该规则的事件。
Threshold	在指定时间段内，当指定数量的数据包 （由 Count 参数指定）触发规则时，记录并显示一个事件。请注意，达到事件阈值计数且系统记录该事件之后，时间计数器将重新开始计数。例如，将类型设置为 **Threshold**，将 **Count** 设置为 10，并将 **Seconds** 设置为 60 时，如果到 33 秒时规则触发 10 次，则系统将生成一个事件，然后将 Seconds 和 Count 计数器重置为 0。其后，该规则在接下来 25 秒内又触发 10 次。由于计数器在第 33 秒时已重置为 0，因此系统此时会再记录一个事件。

表 32-6　阈值选项 （续）

选项	说明
Both	每个指定时间段在指定数量 （计数）的数据包触发规则后记录并显示一次事件。例如，如果将类型设置为 **Both**，将 **Count** 设置为 2，并将 **Seconds** 设置为 10，则事件计数结果如下： • 如果 10 秒内触发规则一次，系统不会生成任何事件 （未达到阈值） • 如果 10 秒内触发规则两次，系统将生成一个事件 （第二次触发规则时达到阈值） • 如果 10 秒内触发规则四次，系统将生成一个事件 （第二次触发规则时达到阈值，忽略其后的事件）

接下来，必须指定跟踪，确定事件阈值是按源 IP 地址计算还是按目标 IP 地址计算。从下表中选择一个选项来指定系统如何跟踪事件实例。

表 32-7　阈值 IP 选项

选项	说明
Source	按源 IP 地址计算事件实例计数。
Destination	按目标 IP 地址计算事件实例计数。

最后，必须指定用于定义阈值的实例数和时间段。

表 32-8　阈值实例/时间选项

选项	说明
Count	每个跟踪 IP 地址在每个指定时间段内达到阈值所需的事件实例数量。
Seconds	计数重置之前经过的秒数。如果将阈值类型设置为 **limit**，将跟踪设置为 **Source IP**，将 **count** 设置为 10，并将 **seconds** 设置为 10，则系统将记录并显示 10 秒钟内发生的来自指定源端口的前 10 个事件。如果前 10 秒内只发生了 7 个事件，系统将记录并显示这些事件，而如果前 10 秒内发生了 40 个事件，系统将记录并显示 10 个事件，然后在 10 秒过后重新开始计数。

请注意，入侵事件阈值可单独使用，也可与基于速率的攻击防御、`detection_filter` 关键字和入侵事件抑制的任意组合配合使用。有关详细信息，请参阅第 32-26 页上的添加动态规则状态、第 36-80 页上的过滤事件和第 32-24 页上的按入侵策略配置抑制。

有关详细信息，请参阅以下各节：

- 第 32-21 页上的添加和修改入侵事件阈值
- 第 32-6 页上的为规则设置阈值
- 第 32-23 页上的查看和删除入侵事件阈值

提示　也可以在入侵事件的数据包视图中添加阈值。有关详情，请参见第 41-20 页上的查看事件信息。

添加和修改入侵事件阈值

许可证：保护

您可以为一条或多条特定规则设置阈值。也可以单独或同时修改现有阈值设置。可以为每条规则设置一个阈值。添加阈值将覆盖该规则的任何现有阈值。

有关查看和删除阈值配置的详细信息，请参阅第 32-23 页上的查看和删除入侵事件阈值。

您还可以修改默认应用到所有规则和预处理器生成的事件的全局阈值。有关详细信息，请参阅第 35-1 页上的从全局限制入侵事件记录。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清空该字段的值。

提示　在有多个 CPU 的受管设备上，全局阈值或单独的阈值可能会导致事件数量高于预期。

要添加或修改事件阈值，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　查找要在其中设置阈值的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅以下主题：第 32-9 页上的了解入侵策略中的规则过滤和第 32-16 页上的在入侵策略中设置规则过滤器。

页面将刷新，显示所有匹配的规则。

步骤 5　选择要在其中设置阈值的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　选择 **Event Filtering > Threshold**。

系统将显示阈值弹出窗口。

步骤 7　从 **Type** 下拉列表，选择要查看的阈值的类型。

- 选择 **Limit** 则在每个时间段内只为指定数量的事件实例提供通知。
- 选择 **Threshold** 则在每个时间段内每次事件实例数达到指定数量时提供通知。
- 选择 **Both** 则在每个时间段内事件实例数达到指定数量后提供一次通知。

步骤 8　从 **Track By** 下拉列表中选择要按 **Source** 或 **Destination** IP 地址跟踪事件实例。

步骤 9　在 **Count** 字段中，指定要用作阈值的事件实例数。

步骤 10　在 **Seconds** 字段中指定时间段的秒数，系统将跟踪该时间段内的事件实例。

步骤 11　点击 **OK**。

系统将添加阈值并在 Event Filtering 列中该规则旁显示事件过滤器图标 ( )。如果将多个事件过滤器添加到规则，图标上的数字表示事件过滤器的数量。

步骤 12　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。

有关详细信息，请参阅第 31-3 页上的管理入侵策略和第 31-4 页上的编辑入侵策略。

查看和删除入侵事件阈值

许可证：保护

您可能需要查看或删除现有阈值设置。可以使用 Rules Details 视图显示为阈值配置的设置，看其是否适合系统。如果不适合，可以添加新的阈值来覆盖现有值。

请注意，您也可以修改默认应用到所有规则和预处理器生成的事件的全局阈值。有关详情，请参见第 35-1 页上的从全局限制入侵事件记录。

要查看或删除阈值，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　查找配置了要查看或删除的阈值的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅：第 32-9 页上的了解入侵策略中的规则过滤和第 32-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择配置了要查看或删除的阈值的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　要删除每条所选规则的阈值，请选择 **Event Filtering > Remove Thresholds** 。在随即显示的确认弹出窗口中点击 **OK**。

提示　要删除特定阈值，还可以突出显示该规则，然后点击 **Show details**。展开阈值设置，然后点击要删除的阈值设置旁边的 **Delete**。点击 **OK** 确认要删除该配置。

页面将刷新，该阈值被删除。

步骤 7　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详细信息，请参阅第 31-3 页上的管理入侵策略和第 31-4 页上的编辑入侵策略。

按入侵策略配置抑制

许可证：保护

您可以在特定 IP 地址或 IP 地址范围触发特定规则或预处理器时抑制入侵事件通知。这对杜绝误报十分有用。例如，如果邮件服务器传输的数据包看起来像某种特定的漏洞，可以在邮件服务器触发该事件时抑制对其发出的事件通知。所有数据包都会触发该规则，但您只会看到真正的攻击事件。

请注意，入侵事件抑制可单独使用，也可与基于速率的攻击防御、`detection_filter` 关键字和入侵事件阈值的任意组合配合使用。有关详细信息，请参阅第 32-26 页上的添加动态规则状态、第 36-80 页上的过滤事件和第 32-20 页上的配置事件阈值。

有关详细信息，请参阅以下各节：

- 第 32-24 页上的抑制入侵事件
- 第 32-25 页上的查看和删除抑制条件

提示　也可以在入侵事件的数据包视图中添加抑制。有关详情，请参见第 41-20 页上的查看事件信息。在 Rule Editor 页面和任何入侵事件页面（如果该事件由入侵规则触发）上，也可以使用右键单击上下文菜单访问抑制设置。

抑制入侵事件

许可证：保护

您可以抑制一条或多条规则的入侵事件通知。当某条规则的通知被抑制时，规则会触发，但不会生成事件。您可以为规则设置一个或多个抑制。列出的第一个抑制的优先级最高。请注意，当两个抑制相冲突时，将执行第一个抑制的操作。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清空该字段的值。

要抑制事件显示，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　查找要在其中设置抑制的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅：第 32-9 页上的了解入侵策略中的规则过滤和第 32-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择要为其配置抑制条件的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　选择 **Event Filtering > Suppression**。

系统将显示抑制弹出窗口。

步骤 7　选择下列 **Suppression Type** 选项之一：

- 选择 **Rule** 将完全抑制所选规则的事件。
- 选择 **Source** 将抑制由指定源 IP 地址发出的数据包生成的事件。
- 选择 **Destination** 将抑制由发往指定目标 IP 地址的数据包生成的事件。

步骤 8　如果为抑制类型选择 **Source** 或 **Destination**，则在 **Network** 字段中输入要指定为源或目标 IP 地址的 IP 地址、地址块或变量，或者输入由这些值的任意组合组成并以逗号分隔的列表。

有关在 FireSIGHT 系统中使用 IPv4 CIDR 和 IPv6 前缀长度地址块的详细信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 9　点击 **OK**。

系统将添加抑制条件并在 Event Filtering 列中被抑制的该规则旁显示事件过滤器图标 ( )。如果将多个事件过滤器添加到规则，图标上的数字表示事件过滤器的数量。

步骤 10　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。

有关详细信息，请参阅第 31-3 页上的管理入侵策略和第 31-4 页上的编辑入侵策略。

查看和删除抑制条件

许可证：保护

您可能需要查看或删除现有抑制条件。例如，由于某个邮件服务器通常会传输看起来像漏洞的数据包，因此可以抑制由该邮件服务器 IP 地址发出的数据包的事件通知。如果以后停用该邮件服务器并将此 IP 地址重新分配给其他主机，应删除对该源 IP 地址的抑制条件。

要查看或删除定义的抑制条件，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　查找要在其中查看或删除抑制的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅：第 32-9 页上的了解入侵策略中的规则过滤和第 32-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择要查看或删除其抑制设置的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　此时您有两种选择：

- 要删除某条规则的所有抑制，请选择 **Event Filtering > Remove Suppressions** 。在随即显示的确认弹出窗口中点击 **OK**。
- 要删除特定的抑制设置，请突出显示该规则，然后点击 **Show details**。展开抑制设置，然后点击要删除的抑制设置旁边的 **Delete**。点击 **OK** 确认要删除所选设置。

页面将刷新，该抑制设置被删除。

步骤 7　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详细信息，请参阅第 31-3 页上的管理入侵策略和第 31-4 页上的编辑入侵策略。

添加动态规则状态

许可证：保护

基于速率的攻击通过向网络或主机发送过大的流量，企图让网络或主机不堪重负，导致其速度下降或拒绝合法请求。为了应对特定规则出现过多规则匹配项的情况，可以使用基于速率的防御来更改规则的操作。

有关详细信息，请参阅以下各节：

- 第 32-26 页上的了解动态规则状态
- 第 32-27 页上的设置动态规则状态

了解动态规则状态

许可证：保护

您可以配置入侵策略，使其包含基于速率的过滤器，在指定时间段内出现某条规则的太多匹配项时进行检测。此功能可以用于内联部署的受管设备上，先在指定时间内拦截基于速率的攻击，然后恢复为规则匹配项仅生成事件而不丢弃流量的规则状态。

基于速率的攻击防御可确定异常流量模式，并可将这些流量对合法请求的影响降至最低。您可以识别出发往一个或多个特定目标 IP 地址或者由一个或多个特定源 IP 地址发出的流量中存在的过多规则匹配项。也可以对检测的所有流量中符合特定规则的过多匹配项作出反应。

在入侵策略中，可以为任何入侵规则或预处理器规则配置基于速率的过滤器。基于速率的过滤器包含三个组成部分：

- 规则的匹配速率，配置为特定秒数内的规则匹配项数量
- 超过速率时要执行的新操作，可用的操作有三项：Generate Events、Drop and Generate Events 和 Disable
- 操作的持续时间，配置为超时值

请注意，新操作自开始之后，在到达超时时间之前会一直执行，即使速率在这段时间内降到配置的速率以下亦不会停止。当超时周期结束后，如果速率低于阈值，则规则的操作会恢复到最初为该规则配置的操作。

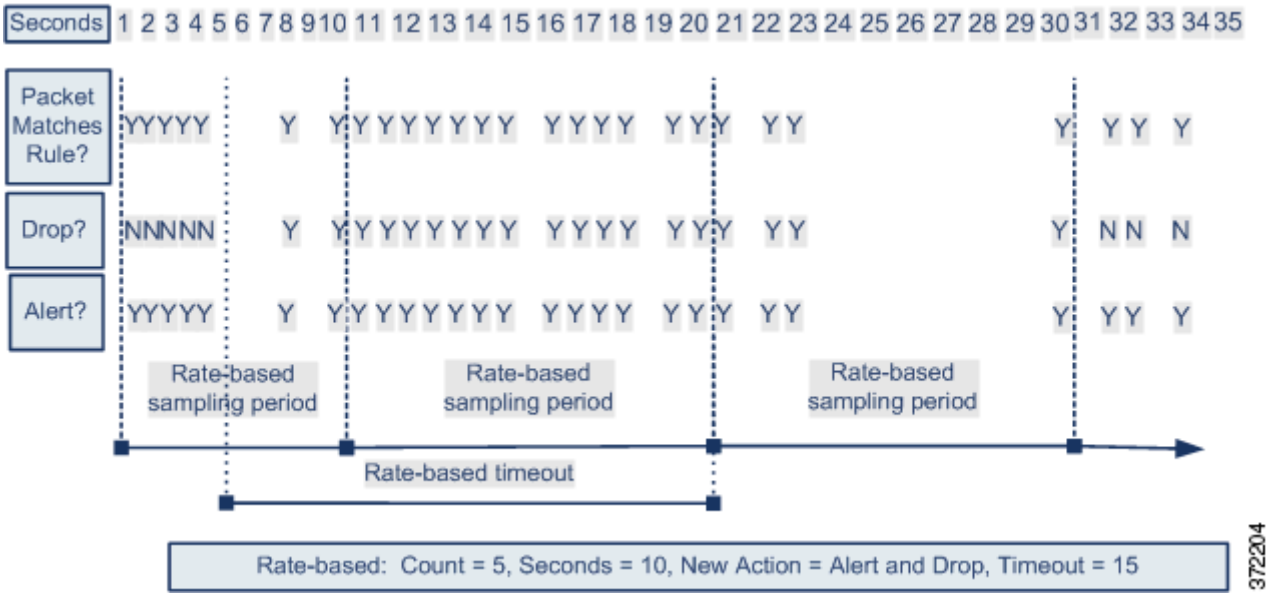
在内联部署中，可以将基于速率的攻击防御临时或永久配置为拦截攻击。如果没有基于速率的配置，设置为 Generate Events 的规则确实会生成事件，但系统不会丢弃这些规则的数据包。但是，如果攻击流量所匹配的规则配置了基于速率的条件，则基于速率的操作可能会导致系统在该操作处于活动状态的时间内丢弃数据包，即便这些规则最初并未设置为 Drop and Generate Events。

注　基于速率的操作无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。

可以对同一规则定义多个基于速率的过滤器。入侵策略中列出的第一个过滤器优先级最高。请注意，当两个基于速率的过滤器的操作相冲突时，将执行第一个基于速率的过滤器的操作。

下图显示的例子中，攻击者正在尝试访问主机。反复尝试查找密码触发了配置有基于速率的攻击防御的规则。当在 10 秒的时间跨度内发生五次规则匹配之后，基于速率的设置会将规则属性更改为 Drop and Generate Events。新的规则属性在 15 秒之后超时。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样速率高于当前或前一个采样周期的阈值，新操作将继续。只有在采样周期完毕而采样速率低于阈值速率之后，新操作才会恢复为 Generate Events。



设置动态规则状态

许可证：保护

在某些情况下，您可能不希望将某规则设置为 Drop and Generate Events 状态，因为您不想丢弃与该规则匹配的每个数据包，但同时您又确实希望在指定事件内出现特定频率的匹配项时丢弃与该规则匹配的数据包。动态规则状态可用于配置应该触发规则操作更改的速率、达到该速率时应该改而执行的操作以及新操作应该持续的时间。

您可以通过指定计数来设置该规则匹配项的数量，并设置应该在多少秒数内达到该匹配项数量才触发操作更改。此外，您还可以设置超时，让该操作在超时时间到期后恢复为该规则以前的状态。

可以为同一规则定义多个动态规则状态过滤器。入侵策略的规则详细信息中列出的第一个过滤器优先级最高。请注意，当两个基于速率的过滤器的操作相冲突时，将执行第一个基于速率的过滤器的操作。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清空该字段的值。

注　动态规则状态无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。

要添加动态规则状态，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。

步骤 4　查找要在其中添加动态规则状态的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅：第 32-9 页上的了解入侵策略中的规则过滤和第 32-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择要在其中添加动态规则状态的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　选择 **Dynamic State > Add Rate-Based Rule State**。

系统将显示 Add Rate-Based Rule State 对话框。

步骤 7　从 **Track By** 下拉列表中选择您希望如何跟踪规则匹配项：

- 选择 **Source** 将跟踪由特定的一个或一组源地址发出的该规则匹配项的数量。
- 选择 **Destination** 将跟踪发往特定的一个或一组目标地址的该规则匹配项的数量。
- 选择 **Rule** 将跟踪该规则的所有匹配项。

步骤 8　将 **Track By** 设置为 **Source** 或 **Destination** 时，在 **Network** 字段中输入要跟踪的每台主机的地址。

可以指定单个 IP 地址、地址块、变量或由这些值的任意组合组成并以逗号分隔的列表。有关在 FireSIGHT 系统中使用 IPv4 CIDR 和 IPv6 前缀长度地址块的详细信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 9　下一个是 **Rate**，指示每个时间段的规则匹配项数量，用于设置攻击速率：

- 在 **Count** 字段中，使用 1 到 2147483647 之间的整数指定要用作阈值的规则匹配项数量。
- 在 **Count** 字段中，使用 1 到 2147483647 之间的整数指定时间段的秒数，系统将跟踪该时间段内的攻击。

步骤 10　从 **New State** 下拉列表中指定满足条件时应执行的新操作。

- 选择 **Generate Events** 将生成事件。

- 选择 **Drop and Generate Events** 将在内联部署中生成事件并丢弃触发该事件的数据包，或在被动部署中生成事件。
- 选择 **Disabled** 将不执行任何操作。

步骤 11　在 **Timeout** 字段中，键入希望新操作保持有效的秒数。在超时后，规则将恢复到原始状态。指定 0 或将 **Timeout** 字段留空可防止新操作超时。

步骤 12　点击 **OK**。

系统将添加动态规则状态并在 Dynamic State 列中该规则旁显示动态状态图标 ( )。如果将多个动态规则状态过滤器添加到规则，图标上的数字表示过滤器的数量。

如果将任何必填字段留空，您将收到错误消息，指出哪些字段必须填写。

提示　要删除一组规则的所有动态规则设置，请在 Rules 页面中选择这些规则，然后选择 **Dynamic State > Remove Rate-Based States**。也可以从规则的规则详细信息中删除单独的基于速率的规则状态过滤器，方法是选择该规则后点击 **Show details**，然后点击要删除的基于速率的过滤器旁边的 **Delete**。

步骤 13　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。

有关详细信息，请参阅第 31-3 页上的管理入侵策略和第 31-4 页上的编辑入侵策略。

添加 SNMP 告警

许可证：保护

如果为 FireSIGHT 系统配置 SNMP 告警，可以配置特定规则以在该规则生成事件时提供 SNMP 告警。有关详细信息，请参阅第 44-1 页上的使用 SNMP 响应。

要设置 SNMP 告警，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。

步骤 4　查找要在其中设置 SNMP 告警的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅以下主题：第 32-9 页上的了解入侵策略中的规则过滤和第 32-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择要在其中设置 SNMP 告警的一条或多条规则：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　选择 **Alerting > Add SNMP Alert**。

系统将添加告警并在 Alerting 列中该规则旁显示告警图标 ( )。如果将多个告警类型添加到规则，图标上的数字表示告警类型的数量。

提示　要从规则中移除 SNMP 告警，请点击规则旁边的复选框并选择 **Alerting > Remove SNMP Alerts**，然后点击 **OK** 确认删除。

步骤 7　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详细信息，请参阅第 31-3 页上的管理入侵策略和第 31-4 页上的编辑入侵策略。

添加规则注释

许可证：保护

您可以向规则添加注释。添加的任何注释都将显示于 Rules 页面的 Rule Details 视图中。

提交包含注释的入侵策略更改后，点击该规则 Edit 页面中的 **Rule Comment** 也可查看该注释。有关编辑规则的详细信息，请参阅第 36-95 页上的修改现有规则。

要将注释添加到规则，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。

步骤 4　查找要在其中向规则添加注释的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅以下主题：第 32-9 页上的了解入侵策略中的规则过滤和第 32-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择要在其中添加注释的一条或多条规则：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　选择 **Comments > Add Rule Comment**。

系统将显示 Add Comment 对话框。

步骤 7　在 **Comment** 字段中，键入规则注释。

步骤 8　点击 **OK**。

系统将添加注释并在 Comments 列中该规则旁显示注释图标 ( )。如果将多个注释添加到规则，图标上的数字表示注释的数量。

提示　要删除规则注释，请突出显示该规则并点击 **Show Details**，然后点击 **Comments** 部分的 **Delete**。请注意，只能删除尚未提交的入侵策略更改所缓存的注释。一旦入侵策略更改提交之后，规则注释就是永久性的。

步骤 9　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。

有关详细信息，请参阅第 31-3 页上的管理入侵策略和第 31-4 页上的编辑入侵策略。

为您的网络资产定制入侵防御

您可以使用 FireSIGHT 建议规则功能将网络中检测到的操作系统、服务器和客户端应用协议（请参阅第 45-1 页上的网络发现简介）按照入侵策略与为保护这些资产而专门编写的规则相关联。这样，您就可根据自己的受监控网络的特定需求定制您的入侵策略。 FireSIGHT 建议规则功能要求使用 FireSIGHT 和保护许可证。

在配置 FireSIGHT 建议规则功能时，系统会搜索基本策略，查找防范网络资产相关漏洞的规则，并确定基本策略中的规则的当前状态。然后，系统会建议规则状态，并使用下表中的条件将规则设置为建议的状态 （此项可选）。

表 33-1 基于漏洞的 FireSIGHT 规则状态建议

基本策略规则状态	规则是否保护发现的资产？	建议的规则状态
Generate Events 或关闭	是	Generate Events
Drop and Generate Events	是	Drop and Generate Events
any	no	关闭

思科漏洞研究团队 (VRT) 为思科提供的默认策略中的每条规则确定了适当的状态。因此，当基本策略是思科提供的默认策略时，允许系统将规则设置为 FireSIGHT 建议的规则状态的有效作用就在于，入侵策略中的规则与思科对网络资产建议的设置相符。有关详情，请参见第 23-7 页上的了解系统提供的策略。

生成规则状态建议非常简单，只需在生成建议时或在其之后选择是否使用建议的规则状态即可。高级建议选项可供您进一步定制配置。请注意，选择使用建议的规则状态会在入侵策略中添加只读的 FireSIGHT Recommendations 层，在此后选择不使用建议的规则状态可删除该层。有关使用策略层更有效地管理多个入侵策略的详细信息，请参阅第 24-1 页上的在网络分析或入侵策略中使用层。

请注意，虽然系统通常建议更改的是标准文本规则和共享对象规则的规则状态，但也可能会建议更改预处理器规则和解码器规则的状态。

您可以安排任务来根据入侵策略中最近保存的配置设置自动生成建议。有关安排任务来生成建议的规则状态的详细信息，请参阅第 62-9 页上的自动 FireSIGHT 生成建议。

有关详细信息，请参阅以下各节：

- 了解基本规则状态建议
- 了解高级规则状态建议
- 使用 FireSIGHT 建议

了解基本规则状态建议

许可证：保护 + FireSIGHT

您可以不使用建议的规则状态而在策略中生成建议。然后，可以使用 Rules 页面中三个已过滤视图中的任意一个，显示系统建议设置为 Generate Events、Drop and Generate Events 或 Disable 的规则。这样就可以在选择使用建议的规则状态之前，预先了解哪些规则会被修改。您也可以选择生成建议并立即使用。

在显示对建议过滤后的 Rules 页面时，或者从导航面板或 Policy Information 页面直接访问 Rules 页面后，可以手动设置规则状态、对规则排序并执行 Rules 页面中的任何其他可用操作，例如抑制规则、设置规则阈值等。有关手动更改所选规则的状态的详细信息，请参阅第 32-18 页上的设置规则状态。有关 Rules 页面中可用于定制入侵策略中规则的其他操作的详细信息，请参阅第 32-1 页上的使用规则调整入侵策略。

系统不会更改手动设置的规则状态。当您在生成建议时选择使用建议的规则状态时：

- 先手动设置指定规则的状态再生成建议可以防止系统今后修改这些规则的状态
- 生成建议后再手动设置指定规则的状态可以覆盖这些规则的建议状态

提示 您可以在入侵策略报告中包含一份列表，列出规则状态与建议状态不同的规则。有关详情，请参见第 31-8 页上的生成当前入侵设置的报告。

另请注意，为 FireSIGHT 建议的规则生成建议而不更改高级设置时，系统会建议更改发现的整个网络中所有主机的规则状态。还应注意，默认情况下，系统仅为低开销或中等开销的规则生成建议，并生成禁用规则的建议。有关详情，请参见第 33-2 页上的了解高级规则状态建议。

了解高级规则状态建议

许可证：保护或保护 + FireSIGHT

通过高级设置，可以重新定义系统要监控网络中的哪些主机以防漏洞，影响系统根据规则开销对哪些规则给出建议，并指定是否生成禁用规则的建议。

如果要根据主机信息动态调整规则对特定数据包的当前处理方式，也可以启用自适应配置文件。有关详细信息，请参阅第 30-2 页上的自适应配置文件和 FireSIGHT 建议规则。

有关详细信息，请参阅以下各节：

- 第 33-2 页上的了解要检查的网络
- 第 33-3 页上的了解规则开销

了解要检查的网络

许可证：保护 + FireSIGHT

通过在网络映射中确定要检查的网络，可以配置 FireSIGHT 建议规则功能。然后，系统将建议可激活以保护网络的规则。有关网络映射的详细信息，请参阅第 48-1 页上的使用网络映射。

使用为给出建议而要检查的主机来配置 **Networks** 字段。可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。

指定主机中的地址列表与一个逻辑或运算关联，但逻辑非除外，逻辑非在所有逻辑或运算计算完之后与一个逻辑与运算关联。

了解规则开销

许可证：保护

思科根据规则对系统性能的潜在影响以及规则产生误报的可能性，将每条入侵规则的开销评为无、低、中、或高。在 Rules 页面的规则详细信息视图中，可以查看规则的开销级别。有关详情，请参见第 32-4 页上的查看规则详细信息。

您可以将系统设置为根据最高包括指定开销级别 （极高级别除外）。例如，为开销为中的规则生成建议时，系统会根据开销级别为无、低或中的所有规则来给出建议，而不会为开销为高的规则给出任何建议。

请注意，系统在给出是生成事件还是丢弃并生成事件的建议时，会将规则开销作为一项考虑因素。但是系统在给出禁用规则的建议时，不会将规则开销作为一项考虑因素。另请注意，本地规则没有开销，除非被映射到第三方漏洞。有关详细信息，请参阅第 66-17 页上的导入本地规则文件和第 46-27 页上的管理第三方产品映射。

为开销级别为特定设置的规则生成建议并不会妨碍您使用不同的开销生成建议后再重新为原来的开销设置生成建议。每次为同一规则集生成建议时，无论生成多少次建议或者生成多少不同的开销设置，为每个开销设置获得的规则状态建议都相同。例如，您可以将开销依次设置为中、高，并最终设置为中来生成建议，如果网络中的主机和应用尚未更改，对于该规则集给出的开销设置为中的两组建议均相同。

使用 FireSIGHT 建议

许可证：FireSIGHT + 保护

无论是否使用建议的规则状态或是否修改用于生成建议的高级设置，都可以生成建议。有关详细信息，请参阅第 33-2 页上的了解基本规则状态建议和第 33-2 页上的了解高级规则状态建议。

生成建议之后，可以使用建议的规则状态；还可以查看建议的状态和使用 Rules 页面中可用的任何功能。

要使用 FireSIGHT 规则状态建议，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　此时您有两种选择：

- 如果尚未生成建议，请选择 **No recommendations have been generated.Click here to set up FireSIGHT recommendations**。
- 如果已生成建议，请选择 **Click to change recommendations**。

系统将显示 FireSIGHT Recommended Rules Configuration 页面。

步骤 4　有以下选项可供选择：

- 要让相应的入侵策略报告为实际状态与建议状态不同的所有规则列出规则消息、建议状态和实际状态，请选择 **Include all differences between recommendations and rule states in policy reports**。有关详情，请参见第 31-8 页上的生成当前入侵设置的报告。
- 要使用默认设置生成建议，请转到第 9 步。
- 要修改高级建议选项，请转到第 5 步。

步骤 5　点击加号图标 (⊕) 展开 **Advanced Settings** 部分。

系统将显示高级 FireSIGHT 建议选项。

步骤 6　在 **Networks to Examine** 下方的 **Networks** 字段，指定要为建议检查的网络。

有关在 FireSIGHT 系统中使用 IP 地址表示法的详细信息，请参阅第 1-16 页上的 IP 地址约定。

请注意，地址列表与一个逻辑或运算关联，但逻辑非除外，逻辑非在所有逻辑或运算计算完之后与一个逻辑与运算关联。有关详情，请参见第 33-2 页上的了解要检查的网络。

步骤 7　或者，在 **FireSIGHT Recommended Rules Configuration** 下方，拖动 **Recommended Rules Configuration** 滑动条，指定规则必须达到多大开销才能纳入生成的建议中。

向右拖动滑动条时，包含的规则开销更高，得到的建议可能也更多，但是对系统性能的影响也越来越大。有关详情，请参见第 33-3 页上的了解规则开销。

步骤 8　您有以下选项：

- 要生成禁用规则的建议，请选择 **Accept Recommendations to Disable Rules** 复选框。

  请注意，接受禁用规则的建议会限制规则的覆盖范围。
- 要防止生成禁用规则的建议，请清除 **Accept Recommendations to Disable Rules** 复选框。

  请注意，忽略禁用规则的建议会扩大规则的覆盖范围。

步骤 9　此时有多个选择：

- 如果尚未生成建议而且希望系统在生成建议的同时将规则状态自动更改为建议的状态，请点击 **Generate and Use Recommendations**。

  系统将生成建议的规则状态更改并自动将规则设置为建议的状态。
- 如果希望系统生成建议但不将规则状态自动更改为建议的状态，请点击 **Generate Recommendations**。

  系统将生成建议的规则状态更改。
- 如果以前曾经生成过建议，请点击 **Update Recommendations** 以更新现有建议。

  系统将生成建议的规则状态更改，如果建议正在使用，还会将规则自动设置为建议的状态。建议数、建议的规则状态发生更改的主机数以及对生成事件规则、丢弃并生成事件规则或禁用规则给出的建议数均会更新其状态。
- 如果以前曾经生成过建议，请点击 **Use Recommendations** 以使用已经生成但尚未使用的建议。

  系统会将规则自动设置为建议的状态。
- 如已生成且在使用建议，请点击 **Do Not Use Recommendations** 以停止使用当前正在使用的建议。

  系统会将规则自动重置为默认规则状态，除非在使用建议前将特定的规则状态应用到该规则；在此情况下，规则将恢复为该特定规则状态。

请注意，系统不会为基于使用 Impact Qualification 功能禁用的漏洞的入侵规则建议规则状态。有关详细信息，请参阅第 49-25 页上的设置漏洞影响限定。

另请注意，将策略更新为使用或不使用建议可能需要几分钟时间，具体取决于网络规模和规则集。

注　系统始终建议启用与映射到主机的第三方漏洞相关联的本地规则。对于未映射的本地规则，系统不会给出状态建议。有关详细信息，请参阅第 46-27 页上的管理第三方产品映射。

步骤 10　或者，点击建议类型旁边的 **View**，显示 Rules 页面对建议进行过滤后得到的所选建议类型视图。

步骤 11　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

检测特定威胁

您可以在网络分析策略中使用多个预处理程序来检测对受监控网络的特定威胁，例如 Back Orifice 攻击、几种类型的端口扫描和试图利用超大流量颠覆网络的基于速率的攻击。请注意，当入侵规则或规则参数要求禁用的预处理器时，尽管预处理器在网络分析策略网络界面中保持禁用状态，系统还会自动使用其当前设置。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

注意事项 某些具备自定义用户角色的用户无法通过标准菜单路径 (**Policies > Access Control > Network Analysis Policy**) 访问网络分析策略。这些用户可以通过入侵策略访问网络分析策略：**Policies > Intrusion > Intrusion Policy > Network Analysis Policy**。有关自定义用户角色的详细信息，请参阅第 61-48 页上的管理自定义用户角色。

您还可以使用在入侵规则中配置的敏感数据检测来检测以非安全方式传输的敏感数字数据。

有关检测具体威胁的详细信息，请参阅以下各节。

- 第 34-1 页上的检测 Back Orifice说明了 Back Orifice 攻击检测。
- 第 34-2 页上的检测端口扫描介绍不同类型的端口扫描并说明如何在威胁发展成攻击之前使用端口扫描检测来识别网络威胁。
- 第 34-8 页上的防御基于速率的攻击说明如何限制拒绝服务 (DoS) 和 SYN 泛洪攻击。
- 第 34-17 页上的检测敏感数据说明如何在 ASCII 文本中检测和生成关于敏感数据 （例如，信用卡号和社会保障号码）的事件。

检测 Back Orifice

许可证：保护

FireSIGHT 系统提供了一种检测是否存在 Back Orifice 程序的预处理器。此程序可用于获取对 Windows 主机的管理员访问权限。 Back Orifice 预处理器为 Back Orifice 神奇 cookie "*!*QWTY?"（位于数据包的前八个字节且使用 XOR 加密）分析 UDP 流量。

Back Orifice 预处理器具有配置页面，但没有配置选项。如果启用此预处理器，还必须为其启用下表中的预处理器规则，以生成相应的事件。有关详情，请参见第 32-18 页上的设置规则状态。

表 34-1 Back Orifice GID:SIDs

预处理器规则 GID:SID	说明
105:1	检测到 Back Orifice 流量
105:2	检测到 Back Orifice 客户端流量

表 34-1　Back Orifice GID:SIDs （续）

预处理器规则 GID:SID	说明
105:3	检测到 Back Orifice 服务器流量
105:4	检测到 Back Orifice snort 缓冲区攻击

要查看 Back Orifice Detection 页面，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Access Control > Access Control Policy** 以显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　在左侧的导航面板中，点击 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Back Orifice Detection**：

- 如果已启用预处理器，请点击 **Edit**。
- 如果已禁用预处理器，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Back Orifice Detection 页面。页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

检测端口扫描

许可证：保护

端口扫描是一种通常被攻击者用作攻击前奏的网络侦察形式。在端口扫描中，攻击者将特制的数据包发送到目标主机。通过检查主机响应时所用的数据包，攻击者通常可以直接或通过推理确定主机上的哪些端口是开放的，以及哪种应用协议正在这些端口上运行。

请注意，当启用端口扫描检测时，必须在入侵策略 Rules 页面上为启用的端口扫描类型启用生成器 ID (GID) 为 122 的规则，以便端口扫描检测器可以生成端口扫描事件。有关详细信息，请参阅第 32-18 页上的设置规则状态和第 34-6 页上的表 34-5。

端口扫描本身不算是攻击。事实上，攻击者使用的一些端口扫描技术也可能会被网络上的合法用户使用。思科的端口扫描检测器旨在通过检测活动模式来帮助确定哪些端口扫描可能是恶意的。

攻击者可能会使用多种方法来探测网络。他们通常使用不同的协议从目标主机获取不同的响应，以期即使某一种协议被阻止，也可以使用另一种。下表介绍了可在端口扫描检测器中激活的协议。

表 34-2　　协议类型

协议	说明
TCP	检测 TCP 探针，例如 SYN 扫描、 ACK 扫描、 TCP connect() 扫描和带异常标志组合（如 Xmas tree、 FIN 和 NULL）的扫描
UDP	检测 UDP 探针，如零字节 UDP 数据包
ICMP	检测 ICMP 回应请求 (ping)
IP	检测 IP 协议扫描。这些扫描与 TCP 和 UDP 扫描不同，因为攻击者不是查找开放端口，而是尝试去发现目标主机支持哪些 IP 协议。

注 对于端口扫描连接检测器生成的事件，协议号设置为 255。由于默认情况下端口扫描没有特定协议与之关联，因此，互联网编号分配机构 (IANA) 未将协议号分配给它。IANA 指定 255 作为保留号码，因此，该号码用于端口扫描事件中以指明事件没有关联的协议。

根据目标主机的数量、扫描主机的数量和扫描的端口数量，端口扫描通常分为四种类型。下表介绍了可检测的端口扫描活动的类型。

表 34-3　　端口扫描类型

类型	说明
端口扫描检测	一对一端口扫描，在这种扫描中，攻击者使用一个或几个主机扫描单个目标主机上的多个端口。 一对一端口扫描具有如下特征： • 扫描主机的数量少 • 扫描单个主机 • 扫描的端口数量多 此选项检测 TCP、 UDP 和 IP 端口扫描。
端口清扫	一对多端口清扫，在这种扫描中，攻击者使用一个或几个主机扫描多个目标主机上的单个端口。 端口清扫具有如下特征： • 扫描主机的数量少 • 扫描的主机数量多 • 扫描的唯一端口数量少 此选项检测 TCP、 UDP、 ICMP 和 IP 端口清扫。
诱骗端口扫描	一对一端口扫描，在这种攻击中，攻击者将伪造的源 IP 地址与真实的扫描 IP 地址混合在一起。 诱骗端口扫描具有如下特征： • 扫描主机的数量多 • 一次扫描的端口数量少 • 扫描的主机为一个 （或数量少） 诱骗端口扫描选项检测 TCP、 UDP 和 IP 协议端口扫描。

表 34-3　端口扫描类型 （续）

类型	说明
分布式端口扫描	多对一端口扫描，在这种攻击中，多个主机查询单个主机是否有开放端口。 分布式端口扫描具有如下特征： • 扫描主机的数量多 • 一次扫描的端口数量多 • 扫描的主机为一个 （或数量少） 分布式端口扫描选项检测 TCP、 UDP 和 IP 协议端口扫描。

端口扫描检测器所了解的关于探针的信息主要是基于查看探测主机的否定响应。例如，当网络客户端尝试连接到网络服务器时，客户端会使用端口 80/tcp 且可以依靠服务器将该端口打开。但是，当攻击者探测服务器时，攻击者事先并不知道该服务器是否提供网络 服务。当端口扫描检测器看到否定响应 （即，无法到达 ICMP 或 TCP RST 数据包）时，它会将响应记录为潜在的端口扫描。当目标主机位于设备 （例如，过滤否定响应的防火墙或路由器）的另一端，这个过程更难以执行。在这种情况下，端口扫描检测器可以根据选择的灵敏度级别生成*已过滤*端口扫描事件。

下表介绍了可选择的三种不同的灵敏度级别。

表 34-4　灵敏度级别

功率水平	说明
低	只检测目标主机的否定响应。选择此级别的灵敏度可抑制误报，但请记住，这样可能会遗漏某些类型的端口扫描 （慢速扫描、过滤扫描）。 此级别使用最短的时间周期进行端口扫描检测。
中	根据主机的连接数量检测端口扫描，这意味着，可以检测过滤的端口扫描。但是，非常活跃的主机 （例如网络地址转换器和代理）可能会生成误报。 请注意，可以将这些活跃主机的 IP 地址添加到 **Ignore Scanned** 字段以减少此类误报。 此级别使用较长的时间周期进行端口扫描检测。
高	根据时间周期侦测端口扫描，这意味着，可以检测基于时间的端口扫描。但是，如果使用此选项，应在 **Ignore Scanned** 和 **Ignore Scanner** 字段中指定 IP 地址，随时间小心地调整检测器。 此级别使用更长的时间周期进行端口扫描检测。

有关详细信息，请参阅以下各节：

- 第 34-4 页上的配置端口扫描检测
- 第 34-6 页上的了解端口扫描事件

配置端口扫描检测

许可证：保护

端口扫描检测配置选项可用于精细调整端口扫描检测器如何报告扫描活动。

请注意，当启用端口扫描检测时，必须在 Rules 页面上为启用的端口扫描类型启用生成器 ID (GID) 为 122 的规则，以便端口扫描检测器生成端口扫描事件。有关详细信息，请参阅第 32-18 页上的设置规则状态和端口扫描检测 SID (GID:122)表。

要配置端口扫描检测，请执行以下操作：

管理员/入侵管理员

步骤 1　选择 **Policies > Access Control > Access Control Policy** 以显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存在另一策略中未保存的信息，请参见[曾是“确认入侵策略更改”；更新 xref]。

系统将显示 Policy Information 页面。

步骤 3　在左侧的导航面板中，点击 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Portscan Detection**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

  系统将显示 Portscan Detection 页面。页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　在 **Protocol** 字段中，指定要启用以下哪些协议：

- TCP
- UDP
- ICMP
- IP

按住 Ctrl 或 Shift 键的同时点击可选择多个协议或清除单个协议。有关详细信息，请参阅协议类型表。

请注意，必须确保已启用 TCP 流处理以在 TCP 上检测扫描，并确保已启用 UDP 流处理以在 UDP 上检测扫描。

步骤 6　在 **Scan Type** 字段中，指定要检测以下哪些端口扫描：

- 端口扫描检测
- 端口清扫
- 诱骗端口扫描
- 分布式端口扫描

按住 Ctrl 或 Shift 键的同时点击可选择或取消选择多个协议。有关详细信息，请参阅端口扫描类型表。

步骤 7　在 **Sensitivity Level** 列表中，选择要使用的级别：低、中或高。

有关详细信息，请参阅灵敏度级别表。

步骤 8　或者，在 **Watch IP** 字段中，指定要监视哪个主机的端口扫描活动标志，或者将字段留空以监视所有网络流量。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。有关在 FireSIGHT 系统中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 9　或者，在 **Ignore Scanners** 字段中，指定要作为扫描器而忽略的主机。可使用此字段指示在网络上特别活跃的主机。可能需要随时间修改此主机列表。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。有关在 FireSIGHT 系统中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 10 或者，在 **Ignore Scanned** 字段中，指定要作为扫描目标而忽略的主机。可使用此字段指示在网络上特别活跃的主机。可能需要随时间修改此主机列表。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。有关在 FireSIGHT 系统中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 11 或者，清除 **Detect Ack Scans** 复选框以停止监视在中途恢复的会话。

注 检测中途会话有助于识别 ACK 扫描，但可能会导致错误事件，特别是在含大流量和丢弃数据包的网络中。

步骤 12 保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

了解端口扫描事件

许可证：保护

当启用端口扫描检测时，必须启用生成器 ID (GID) 为 122 且 Snort® ID (SID) 为 1 至 27 的规则，从而为每种启用的端口扫描类型生成事件。有关详情，请参见第 32-18 页上的设置规则状态。下表中的 **Preprocessor Rule SID** 列列出了必须为每种端口扫描类型启用的预处理器规则的 SID。

表 34-5　端口扫描检测 SID (GID:122)

端口扫描类型	协议:	灵敏度级别	预处理器规则 SID
端口扫描检测	TCP	低	1
		中或高	5
	UDP	低	17
		中或高	21
	ICMP	低	不生成事件。
		中或高	不生成事件。
	IP	低	9
		中或高	13
端口清扫	TCP	低	3, 27
		中或高	7
	UDP	低	19
		中或高	23
	ICMP	低	25
		中或高	26
	IP	低	11
		中或高	15

表 34-5　端口扫描检测 SID (GID:122)（续）

端口扫描类型	协议:	灵敏度级别	预处理器规则 SID
诱骗端口扫描	TCP	低	2
		中或高	6
	UDP	低	18
		中或高	22
	ICMP	低	不生成事件。
		中或高	不生成事件。
	IP	低	10
		中或高	14
分布式端口扫描	TCP	低	4
		中或高	8
	UDP	低	20
		中或高	24
	ICMP	低	不生成事件。
		中或高	不生成事件。
	IP	低	12
		中或高	16

启用随附的预处理器规则后，端口扫描检测器会生成入侵事件，可以像任何其他事件一样进行查看。但是，数据包视图上显示的信息不同于其他类型的入侵事件。本节介绍了端口扫描事件的数据包视图上显示的字段，以及如何使用这些信息来了解网络中发生的探测的类型。

首先使用入侵事件视图展开端口扫描事件的数据包视图。可以遵循第 41-1 页上的处理入侵事件中所述的操作步骤。

请注意，不能下载端口扫描数据包，因为单个端口扫描事件是基于多个数据包；但是，端口扫描数据包视图提供了所有可用的数据包信息。

注　对于端口扫描连接检测器生成的事件，协议号设置为 255。由于默认情况下端口扫描没有特定协议与之关联，因此，互联网编号分配机构 (IANA) 未将协议号分配给它。IANA 指定 255 作为保留号码，因此，该号码用于端口扫描事件中以指明事件没有关联的协议。

下表介绍了端口扫描事件的数据包视图中提供的信息。对于所有 IP 地址，可点击地址查看上下文菜单并选择 **whois** 以在 IP 地址上执行查找，或者选择 **View Host Profile** 以查看该主机的主机配置文件。

表 34-6　端口扫描数据包视图

信息	说明
设备	检测事件的设备。
时间	事件发生的时间。
通信	预处理器生成的事件消息。
源 IP:	扫描主机的 IP 地址。
目标 IP:	被扫描主机的 IP 地址。
Priority Count	被扫描主机发出的否定响应（例如， TCP RST 和 ICMP unreachable）的数量。否定响应的数量越多，优先级计数就越高。
Connection Count	主机上的活动连接数量。此值对于基于连接的扫描（例如 TCP 和 IP）而言更准确。

表 34-6　端口扫描数据包视图（续）

信息	说明
IP Count	与被扫描主机联系的 IP 地址变化的次数。例如，如果第一个 IP 地址是 10.1.1.1，第二个 IP 是 10.1.1.2，第三 IP 是 10.1.1.1，那么 IP 计数为 3。 此数字对于活跃的主机（例如代理和 DNS 服务器）而言不太准确。
Scanner/Scanned IP Range	被扫描主机或扫描主机的 IP 地址范围，具体取决于扫描类型。对于端口清扫，此字段显示被扫描主机的 IP 范围。对于端口扫描，此字段显示扫描主机的 IP 范围。
Port/Proto Count	对于 TCP 和 UDP 端口扫描，是指正被扫描的端口变化的次数。例如，如果扫描的第一个端口是 80，扫描的第二个端口是 8080，扫描的第三个端口又是 80，那么端口计数为 3。 对于 IP 协议端口扫描，是指正用于连接至被扫描主机的协议变化的次数。
Port/Proto Range	对于 TCP 和 UDP 端口扫描，是指被扫描端口的范围。 对于 IP 协议端口扫描，是指已用于尝试连接至扫描的主机的 IP 协议号的范围。
Open Ports	在被扫描主机上打开的 TCP 端口。此字段仅在端口扫描检测到一个或多个开放端口时显示。

防御基于速率的攻击

许可证：保护

基于速率的攻击是取决于连接频率或攻击实施重复次数的攻击。可以使用基于速率的检测标准检测发生的基于速率的攻击，采取应对措施，在攻击停止后返回到常规检测设置。有关配置基于速率的检测的详细信息，请参阅以下主题：

- 第 34-8 页上的了解基于速率的攻击防御
- 第 34-11 页上的基于速率的攻击防御及其他过滤器
- 第 34-15 页上的配置基于速率的攻击防御
- 第 32-26 页上的了解动态规则状态
- 第 32-27 页上的设置动态规则状态

了解基于速率的攻击防御

许可证：保护

可以将网络分析策略配置为包括基于速率的过滤器，这种过滤器可检测针对网络中主机的过多活动。可以在内联模式下部署的受管设备上使用此功能，以在指定时间内阻止基于速率的攻击，然后恢复为仅生成事件而不丢弃流量。

基于速率的攻击防御可确定异常流量模式，并可将这些流量对合法请求的影响降至最低。基于速率的攻击通常具有以下其中一种特征：

- 任何包含与网络主机之间过多不完整连接的流量，表示 SYN 泛洪攻击

  要配置 SYN 攻击检测，请参阅第 34-10 页上的防御 SYN 攻击。
- 任何包含与网络主机之间过多完整连接的流量，表示 TCP/IP 泛洪攻击

  要配置同步连接检测，请参阅第 34-10 页上的控制同步连接。

- 在流向特定目标 IP 地址或来自特定源 IP 地址的流量中规则匹配过多。

  要配置基于源或目标的动态规则状态，请参阅第 32-27 页上的设置动态规则状态。

- 所有流量中某个特定规则的匹配过多。

  要配置基于规则的动态规则状态，请参阅第 32-27 页上的设置动态规则状态。

在网络分析策略中，您可以为整个策略配置 SYN 泛洪或 TCP/IP 连接泛洪检测；在入侵策略中，您可以设置各个入侵或预处理器规则的基于速率的过滤器。请注意，手动向规则 135:1 和 135:2 添加基于速率的过滤器是无效的。 GID:135 的规则使用客户端作为源值，使用服务器作为目标值。有关详细信息，请参阅第 34-10 页上的防御 SYN 攻击和第 34-10 页上的控制同步连接。

每个基于速率的过滤器都包含下列几个组成部分：

- 网络地址名称 （适用于整个策略或基于规则的源或目标设置）
- 规则的匹配速率，配置为特定秒数内的规则匹配项数量
- 超过该速率时要执行的新操作

  为整个策略设定基于速率的设置时，系统会在其检测到基于速率的攻击时生成事件，或者也可以在内联部署中丢弃流量。为具体规则设置基于速率的操作时，有三个可用的操作：Generate Events、 Drop and Generate Event 和 Disable。

- 操作的持续时间，配置为超时值

请注意，新操作自开始之后，在到达超时时间之前会一直执行，即使速率在这段时间内降到配置的速率以下亦不会停止。当超时周期结束后，如果速率低于阈值，则规则的操作会恢复到最初为该规则配置的操作。对于策略范围的设置，操作会恢复到流量匹配的每个规则的操作；如果不匹配任何规则，操作会停止。

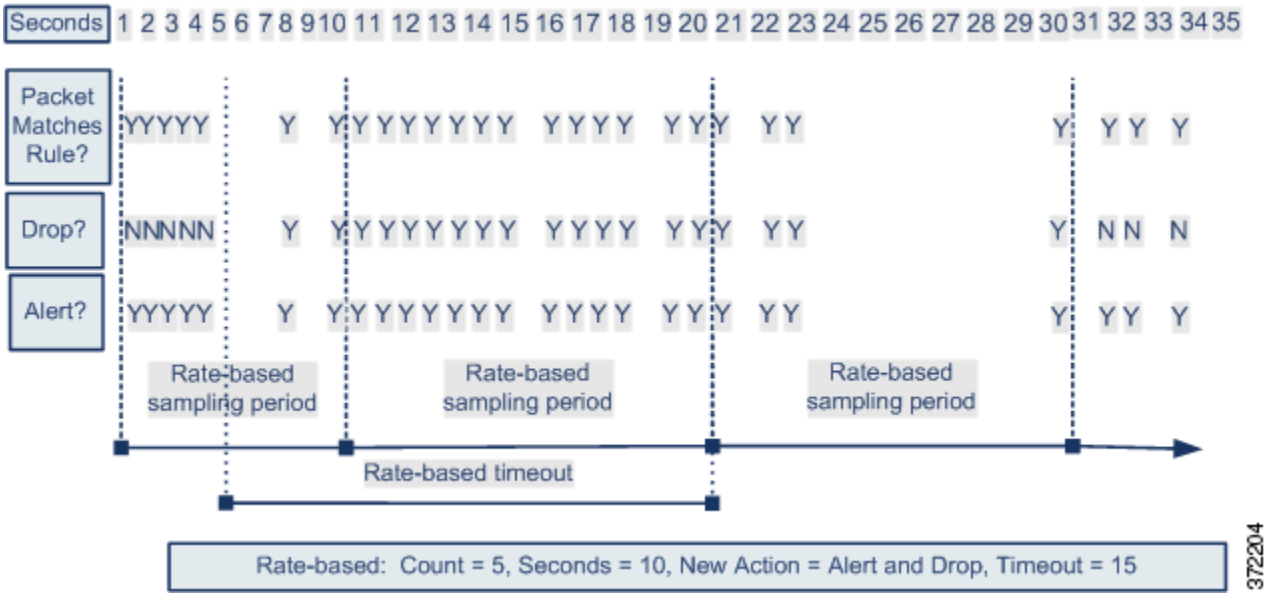
在内联部署中，可以将基于速率的攻击防御临时或永久配置为拦截攻击。在没有基于速率的配置的情况下，设置为 Generate Events 的规则会创建事件，但系统不会丢弃这些规则的数据包。但是，如果攻击流量所匹配的规则配置了基于速率的条件，则基于速率的操作可能会导致系统在该操作处于活动状态的时间内丢弃数据包，即便这些规则最初并未设置为 Drop and Generate Events。

注 基于速率的操作无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。但是，如果在策略级别设置基于速率的过滤器，则可以在指定时段内生成事件或生成事件并丢弃包含过多 SYN 数据包或 SYN/ACK 交互的流量。

可以对同一规则定义多个基于速率的过滤器。入侵策略中列出的第一个过滤器优先级最高。请注意，当两个基于速率的过滤器操作相冲突时，系统会实施第一个基于速率的过滤器的操作。同样，如果对整个策略设置的基于速率的过滤器与对具体规则设置的基于速率的过滤器相冲突，前者优先。

下图显示的例子中，攻击者正在尝试访问主机。反复尝试查找密码触发了配置有基于速率的攻击防御的规则。当在 10 秒的时间跨度内发生五次规则匹配之后，基于速率的设置会将规则属性更改为 Drop and Generate Events。新的规则属性在 15 秒之后超时。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样速率高于当前或前一个采样周期的阈值，新操作将继续。只有在采样周期完毕而采样速率低于阈值速率之后，新操作才会恢复为生成事件。



防御 SYN 攻击

许可证：保护

SYN 攻击防御选项有助于保护网络主机免受 SYN 泛洪攻击。可以根据在一段时间内看到的数据包数量保护单个主机或整个网络。如果设备采用被动部署，可以生成事件。如果设备采用内联部署，还可以丢弃恶意数据包。超时周期结束后，如果速率条件已停止，将会停止事件生成和数据包丢弃。

例如，可以配置一项设置以允许任一 IP 地址发出最多 10 个 SYN 数据包，并连续 60 秒阻止来自该 IP 地址的进一步连接。

启用此选项还会激活规则 135:1。手动激活此规则是无效的。规则状态始终显示为 Disabled，不会改变。如果此选项已启用且超过定义的速率条件，规则会生成事件。

控制同步连接

许可证：保护

可以限制与网路上主机之间的 TCP/IP 连接，以防止拒绝服务 (DoS) 攻击或用户进行过多活动。当系统检测到与指定 IP 地址成功连接的配置数量或地址范围时，它会对额外连接生成事件。基于速率的事件生成继续进行，直到超时周期结束且未发生速率条件。在内联部署中，可以选择丢弃数据包，直到速率条件超时。

例如，可以配置一项设置以允许任一 IP 地址发出最多 10 个成功的同步连接，并连续 60 秒阻止来自该 IP 地址的进一步连接。

启用此选项还会激活规则 135:2。手动激活此规则是无效的。规则状态始终显示为 Disabled，不会改变。如果此选项已启用且超过定义的速率条件，规则会生成事件。

基于速率的攻击防御及其他过滤器

许可证：保护

关键字 `detection_filter`、阈值和抑制功能提供了其他方式来过滤流量或系统生成的事件。可以单独使用基于速率的攻击防御，也可以将其与阈值、抑制功能或 `detection_filter` 关键字随意组合使用。

有关详细信息，请参阅以下示例：

- 第 34-11 页上的基于速率的攻击防御和检测过滤
- 第 34-12 页上的动态规则状态和阈值或抑制
- 第 34-13 页上的策略范围基于速率的检测和阈值或抑制
- 第 34-14 页上的使用多种过滤方法进行基于速率的检测

基于速率的攻击防御和检测过滤

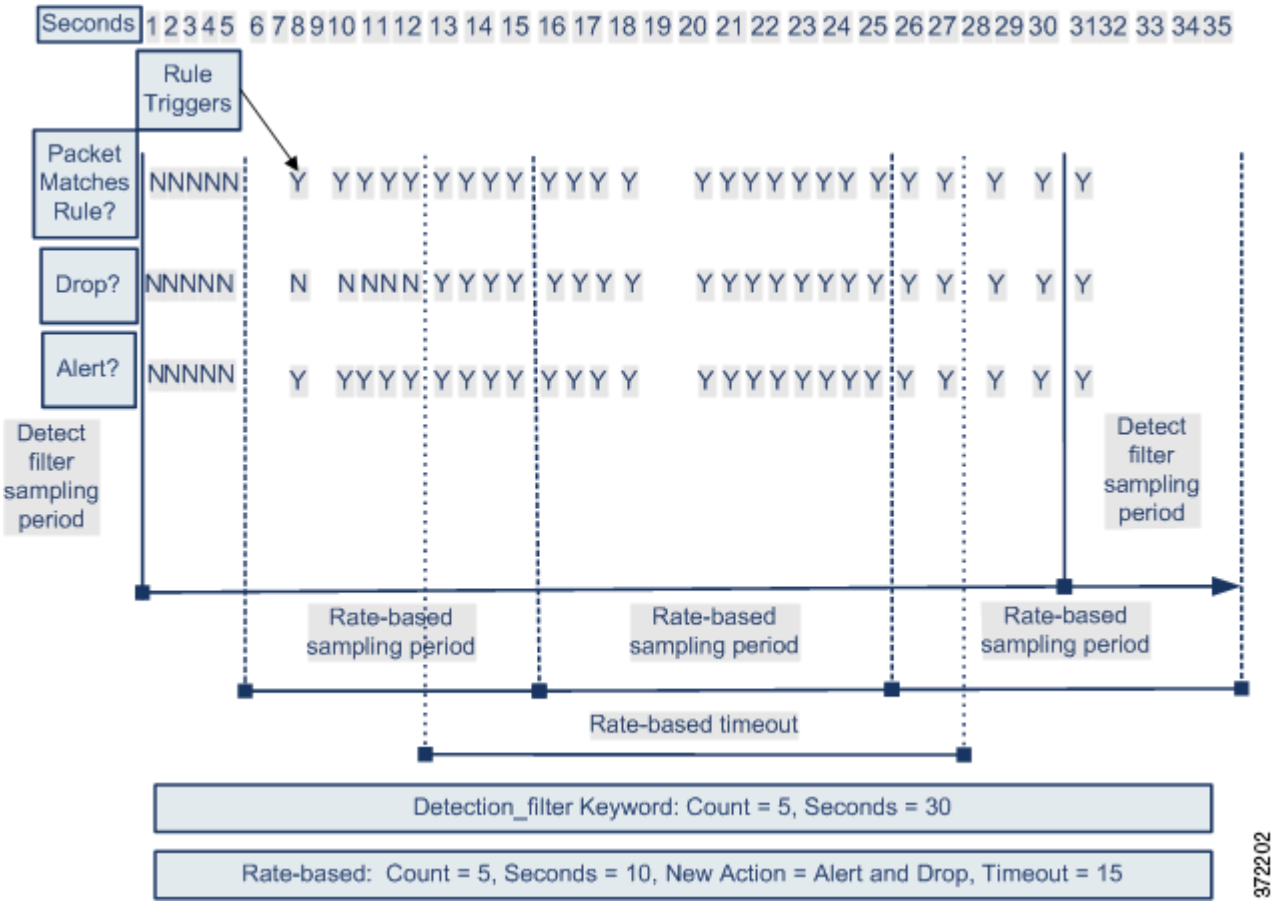
许可证：保护

关键字 `detection_filter` 可防止触发规则，直到指定时间内出现规则匹配的阈值次数。当规则包含 `detection_filter` 关键字时，系统会在每个超时周期跟踪传入数据包与规则中的模式相匹配的次数。系统可以从特定的源或目标 IP 地址计算该规则的匹配次数。速率超过规则中的速率后，会开始针对该规则的事件通知。

以下示例显示了尝试强行登录的攻击者。重复尝试查找密码会触发还包含 `detection_filter` 关键字且计数设置为 5 的规则。此规则已配置基于速率的攻击防御。如果在 10 秒内出现五次规则匹配，基于速率的设置会将规则属性更改为 Drop and Generate Events 并保持 20 秒。

如图所示，与规则匹配的前五个数据包不会生成事件，因为在速率超过 `detection_filter` 关键字所指示的速率之前规则不会触发。规则触发后，事件通知开始，但基于速率的标准在再通过五个数据包之前不会触发新操作 Drop and Generate Events。

如果符合基于速率的标准，将会生成事件并会丢弃数据包，直到基于速率的超时周期结束且速率低于阈值。20 秒之后，基于速率的操作超时。请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。由于采样的速率高于之前采样周期的阈值速率，因此发生超时时，基于速率的操作会继续。



请注意，虽然示例未进行描述，但可以将 Drop and Generate Events 规则状态与 `detection_filter` 关键字结合使用，以在规则的匹配速率达到指定速率时开始丢弃流量。确定是否为规则配置基于速率的设置时，请考虑将规则设置为 Drop and Generate Events 和包含 `detection_filter` 关键字是否会获得相同的结果，或者是否要在入侵策略中管理速率和超时设置。有关详细信息，请参阅第 32-18 页上的设置规则状态。

动态规则状态和阈值或抑制

许可证：保护

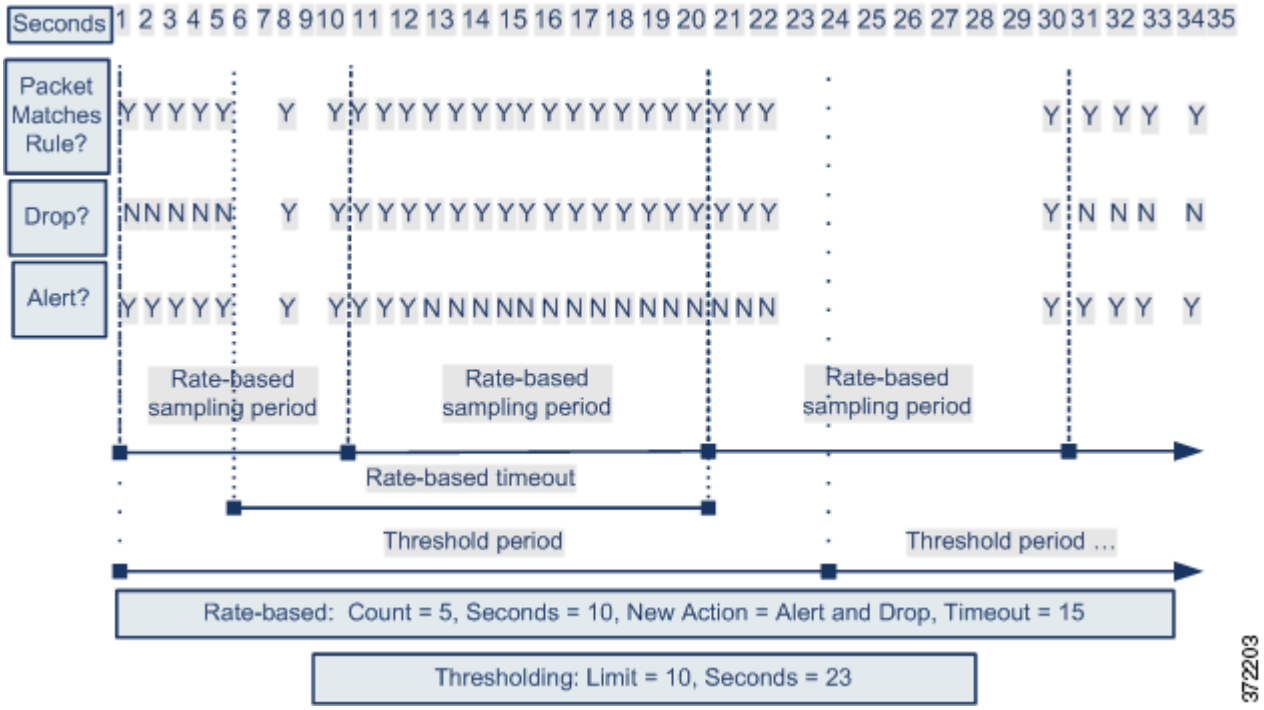
可以使用阈值和抑制功能来减少过多的事件，具体做法是，限制某一规则的事件通知数量或抑制该规则的所有通知。有关阈值和抑制功能的可用选项的详细信息，请参阅第 32-20 页上的配置事件阈值和第 32-24 页上的按入侵策略配置抑制。

如果将抑制功能应用于某一规则，系统会为所有适用的 IP 地址抑制该规则的事件通知，即使基于速率的操作发生变化。但是，阈值与基于速率的标准之间的交互更加复杂。

以下示例显示了尝试强行登录的攻击者。重复尝试查找密码会触发已配置基于速率的攻击防御的规则。如果在 10 秒内出现五次规则攻击，基于速率的设置会将规则属性更改为 Drop and Generate Events 并保持 15 秒。此外，极限阈值会在 23 秒内将规则可生成的事件数量限制为 10。

如图所示，规则为前五个匹配数据包生成事件。五个数据包之后，基于速率的标准会触发新操作 Drop and Generate Events，对于接下来的五个数据包，规则会生成事件且系统会丢弃数据包。第十个数据包之后，已达到极限阈值，因此，对于剩余的数据包，系统不会生成事件，但会丢弃数据包。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样的速率高于当前或之前采样周期的阈值速率，新操作将会继续。新操作只会在采样周期结束后恢复生成事件，在此情况下采样的速率低于阈值速率。



请注意，虽然本例中未显示，但如果在达到阈值*后*因基于速率的标准而触发新操作，系统会生成一个事件以指示操作变化。因此，例如，对于第 14 个数据包，如果达到极限阈值 10，系统停止生成事件且操作从 Generate Events 更改为 Drop and Generate Events，系统会生成第十一个事件以指示操作变化。

策略范围基于速率的检测和阈值或抑制

许可证：保护

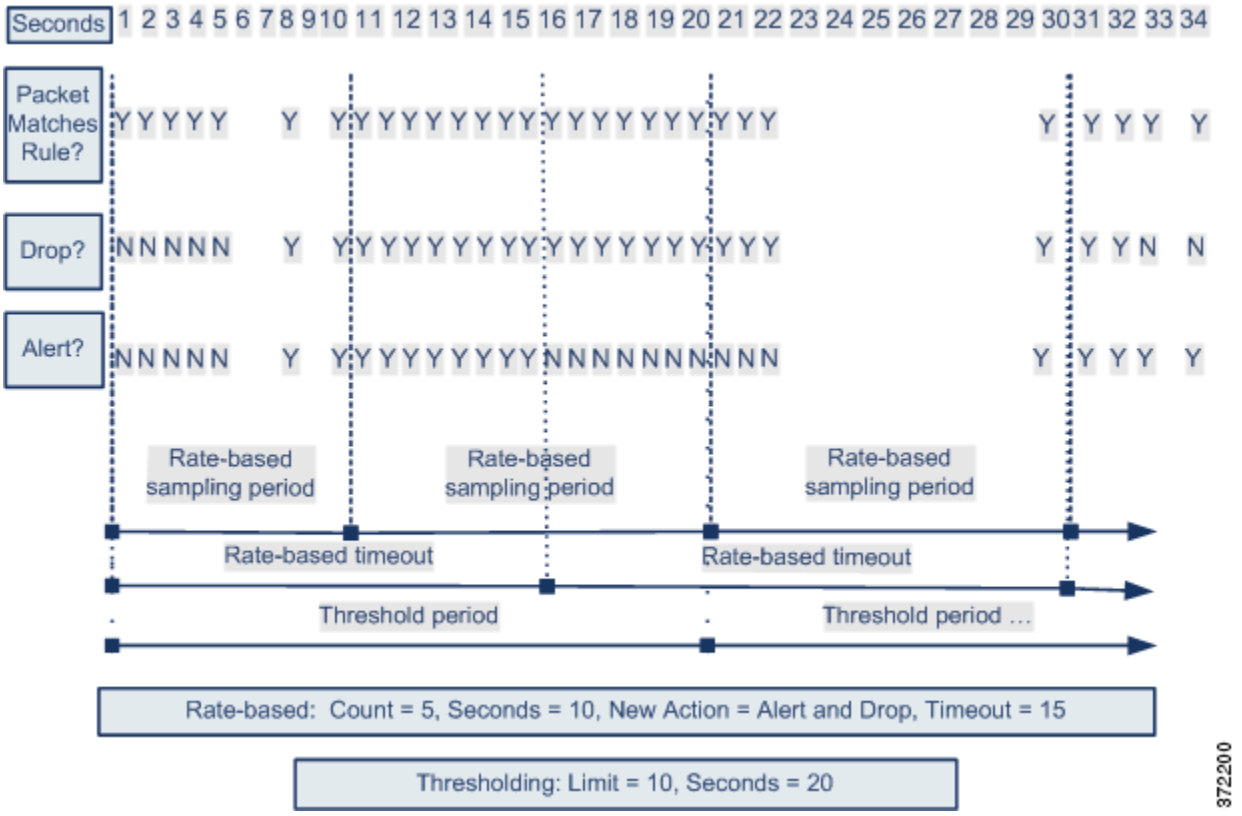
通过，可以使用阈值和抑制功能来减少过多的事件，具体做法是，限制源或目标的事件通知数量或者抑制该规则的所有通知。有关阈值和抑制功能的可用选项的详细信息，请参阅第 35-3 页上的配置全局阈值、第 32-20 页上的配置事件阈值和第 32-24 页上的按入侵策略配置抑制。

如果抑制功能应用于某一规则，系统会为所有适用的 IP 地址抑制该规则的事件通知，即使因策略范围或规则特定基于速率的设置而发生速率操作变化。但是，阈值与基于速率的标准之间的交互更加复杂。

以下示例显示了尝试对网络中的主机进行拒绝服务 (DoS) 攻击的攻击者。许多来自相同源的同步主机连接会触发策略范围的 Control Simultaneous Connections 设置。如果在 10 秒内一个源有五个连接，设置会生成事件并丢弃恶意流量。此外，全局极限阈值会在 20 秒内将所有规则或设置可生成的事件数量限制为 10。

如图所示，策略范围的设置会为前十个匹配数据包生成事件并丢弃流量。第十个数据包之后，已达到极限阈值，因此，对于剩余的数据包，不会生成事件，但会丢弃数据包。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样的速率高于当前或之前采样周期的阈值速率，生成事件和丢弃流量这两种基于速率的操作将会继续。基于速率的操作只在采样周期结束后停止，在此情况下采样的速率低于阈值速率。



请注意，虽然本例中未显示，但如果在达到阈值*后*因基于速率的标准而触发新操作，系统会生成一个事件以指示操作变化。因此，例如，对于第 14 个数据包，如果达到极限阈值 10，系统停止生成事件且操作更改为 Drop and Generate Events，系统会生成第十一个事件以指示操作变化。

使用多种过滤方法进行基于速率的检测

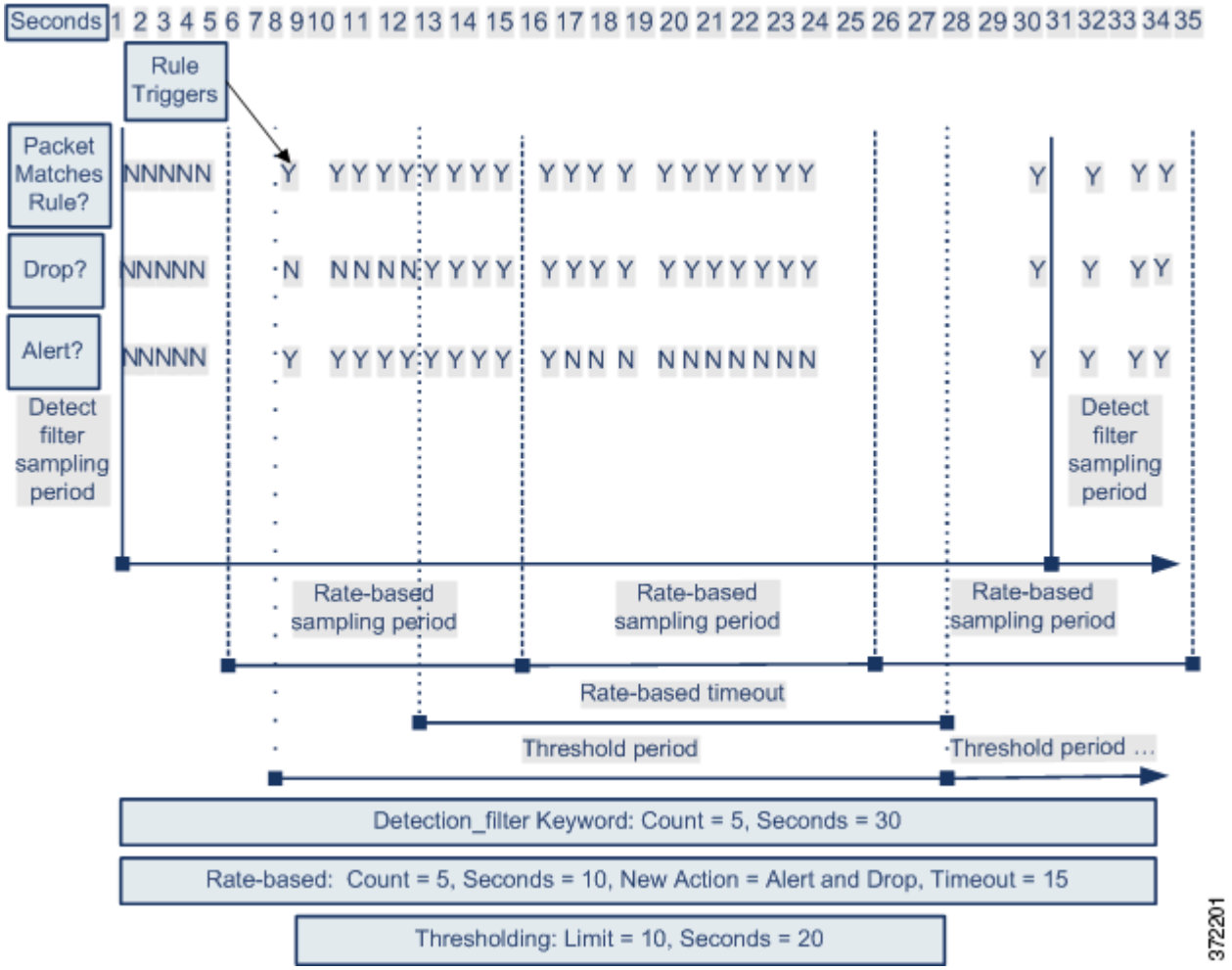
许可证：保护

可能会出现 `detection_filter` 关键字、阈值或抑制功能和基于速率的标准都适用于同一流量这种情况。为规则启用抑制功能后，系统会为指定 IP 地址抑制事件，即使发生基于速率的变化。

以下示例显示了尝试强行登录的攻击者，并描述了 `detection_filter` 关键字、基于速率的过滤和阈值功能交互的情况。重复尝试查找密码会触发包括 `detection_filter` 关键字且计数设置为 5 的规则。此规则还具有基于速率的攻击防御设置，如果在 15 秒内出现五次规则匹配，该设置会将规则属性更改为 Drop and Generate Events 并保持 30 秒。此外，极限阈值会在 30 秒内将规则限为 10 个事件。

如图所示，与规则匹配的前五个数据包不会产生事件通知，因为在速率超过 `detection_filter` 关键字所指示的速率之前规则不会触发。规则触发后，事件通知开始，但基于速率的标准在再通过五个数据包之前不会触发新操作 Drop and Generate Events。如果符合基于速率的标准，系统会为数据包 11 至 15 生成事件并丢弃数据包。第十五个数据包之后，已达到极限阈值，因此，对于剩余的数据包，系统不会生成事件，但会丢弃数据包。

请注意，基于速率的超时后，数据包仍会在随后的基于速率的采样周期内丢弃。因为采样的速率高于之前采样周期的阈值速率，新操作将会继续。



配置基于速率的攻击防御

许可证：保护

可以在策略级别配置基于速率的攻击防御以阻止 SYN 泛洪攻击，也可以阻止来自特定源或到达特定目标的过多连接。

要配置基于速率的攻击防御，请执行以下操作：

管理员/入侵管理员

步骤 1　选择 **Policies > Access Control > Access Control Policy** 以显示 Access Control Policy 页面，然后点击 **Network Analysis Policy**。

系统将显示 Network Analysis Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　在左侧的导航面板中，点击 **Settings**。

系统将显示 Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Rate-Based Attack Prevention**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Rate-Based Attack Prevention 页面。页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　此时您有两种选择：

- 要防止旨在对主机发起泛洪攻击的不完整连接，请点击 **SYN Attack Prevention** 下的 **Add**。

  系统将显示 SYN Attack Prevention 对话框。
- 要防止过多连接，请点击 **Control Simultaneous Connections** 下的 **Add**。

  系统将显示 Control Simultaneous Connections 对话框。

步骤 6　选择要跟踪流量的方式：

- 要跟踪来自特定源或一系列源的所有流量，请从 **Track By** 下拉列表选择 **Source**，然后在 **Network** 字段中输入单个 IP 地址或地址块。
- 要跟踪到达特定目标或一系列目标的所有流量，请从 **Track By** 下拉列表选择 **Destination**，然后在 **Network** 字段中输入单个 IP 地址或地址块。

请注意，系统会单独跟踪 Network 字段中包含的每个 IP 地址的流量。来自超过所配置速率的 IP 地址的流量会带来仅为该 IP 地址生成的事件。例如，进行网络设置时，可将源 CIDR 块设置为 `10.1.0.0/16` 并将系统配置为在有十个同步连接打开时生成事件。如果 10.1.4.21 有八个连接打开，10.1.5.10 有六个连接打开，则系统不会生成事件，因为这两个源地址的打开连接均未达到触发数量。但是，如果 10.1.4.21 有十一个同步连接打开，系统只会为来自 10.1.4.21 的连接生成事件。

有关在 FireSIGHT 系统中使用 CIDR 表示法和前缀长度的信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 7　指示速率跟踪设置的触发速率：

- 对于 SYN 攻击配置，在 **Rate** 字段中指明每个秒数的 SYN 数据包数量。
- 对于同步连接配置，在 **Count** 字段中指示连接数量。

步骤 8　要丢弃与基于速率的攻击防御设置匹配的数据包，请选择 **Drop**。

步骤 9　在 **Timeout** 字段中指定时间段，在该时间段结束后将会停止生成事件和丢弃流量 （如适用，针对具有 SYN 的匹配模式或同步连接的流量）。

注意事项　超时值可以是 1 至 1,000,000 之间的任意整数。但是，设置较高的超时值可能会完全阻止连接至内联部署中的某个主机。

步骤 10　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

检测敏感数据

许可证：保护

敏感数据（如社会保障号码、信用卡号码、驾驶证号码等）可能会被有意或无意地在互联网上泄露。系统提供的敏感数据预处理程序能够检测 ASCII 文本中的敏感数据并为之生成事件，此功能对于检测意外数据泄露特别有用。

系统不会检测经过加密的或模糊的敏感数据，也不会检测压缩或编码格式（例如 Base64 编码邮件附件）的敏感数据。例如，系统会检测电话号码 (555)123-4567，但不会检测该号码经过模糊处理的版本（即，每个数字用空格分开，例如 (5 5 5) 1 2 3 - 4 5 6 7，或者通过 HTML 代码介入，例如 (555)-123-4567）。但是，系统会检测采用 HTML 代码的号码 (555)-123-4567，在该号码中，没有介入代码中断编号模式。

提示 敏感数据预处理器可以检测使用 FTP 或 HTTP 上传和下载的未加密 Microsoft Word 文件中的敏感数据；之所以可以这样，大概是因为 Word 文件单独分组 ASCII 文本和格式命令的方式。

系统通过将各个数据类型与流量进行比对来检测每个 TCP 会话中的敏感数据。可以为每种数据类型和适用于入侵策略中所有数据类型的全局选项修改默认设置。思科提供了常用的预定义数据类型。您也可以创建自定义数据类型。

敏感数据预处理程序规则与每种数据类型相关联。可通过为数据类型启用相应的预处理器，为每种数据类型启用敏感数据检测和事件生成。配置页面上的链接会将您指向 Rules 页面上的敏感数据规则的过滤视图，可以在其中启用和禁用规则以及配置其他规则属性。

保存对入侵策略所做的更改时，如果与数据类型关联的规则已启用且敏感数据检测已禁用，可以选择自动启用敏感数据预处理器。

有关详细信息，请参阅以下各节：

- 第 34-17 页上的部署敏感数据检测
- 第 34-18 页上的选择全局敏感数据检测选项
- 第 34-18 页上的选择具体数据类型选项
- 第 34-19 页上的使用预定义数据类型
- 第 34-20 页上的配置敏感数据检测
- 第 34-22 页上的选择要监控的应用协议
- 第 34-23 页上的特殊情况：检测 FTP 流量中的敏感数据
- 第 34-23 页上的使用自定义数据类型

部署敏感数据检测

许可证：保护

由于敏感数据检测可以对FireSIGHT 系统性能产生很大影响，思科建议您遵循以下指导原则：

- 选择 No Rules Active 默认策略作为基本入侵策略；有关详细信息，请参阅第 24-3 页上的了解系统提供的基本策略。
- 确保在相应的网络分析策略中已启用以下设置：
  - **Application Layer Preprocessors** 下的 **FTP and Telnet Configuration**
  - **Transport/Network Layer Preprocessors** 下的 **IP Defragmentation** 和 **TCP Stream Configuration**

- 将包括含敏感数据配置的入侵策略的访问控制策略应用于为敏感数据检测保留的单独设备；有关详细信息，请参阅第 12-13 页上的应用访问控制策略。

选择全局敏感数据检测选项

许可证：保护

全局敏感数据检测选项用于控制预处理器的工作方式。可以修改指定以下内容的全局选项：

- 预处理器是否在触发数据包中替换信用卡号或社会保障号的最后四位数
- 网络上的哪些目标主机监控敏感数据
- 单个会话中所有数据类型总共出现多少次会产生事件

请注意，全局敏感数据选项是特定于策略的并适用于所有数据类型。

您可以配置以下全局敏感数据检测选项。

掩码

在触发数据包中用 X 替换信用卡号或社会保障号的最后四位数。掩码数字显示在网络界面中的入侵事件数据包视图中和下载的数据包中。有关详情，请参见第 41-19 页上的使用数据包视图。

网络

指定监控敏感数据的目标主机。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。系统会将空白字段解读为 `any`，意指任何目标 IP 地址。有关在 FireSIGHT 系统中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-16 页上的 IP 地址约定。

Global Threshold

指定在生成全局阈值事件之前预处理器必须在任何组合中检测的单个会话中所有数据类型出现的总次数。可以指定 1 至 65535 之间的任意数字。

思科建议将此选项的值设置为大于在策略中启用的任何单个数据类型的最高阈值。有关详情，请参见第 34-18 页上的选择具体数据类型选项。

关于全局阈值，请注意：

- 必须启用预处理器规则 139:1 才能检测和生成关于数据类型出现次数的事件。有关在入侵策略中启用规则的详细信息，请参阅第 32-18 页上的设置规则状态。
- 在每个会话中，预处理器最多生成一个全局阈值事件。
- 全局阈值事件与具体数据类型事件无关；也就是说，预处理器会在达到全局阈值时生成事件，而不管任何具体数据类型的事件阈值是否达到，反之亦然。

选择具体数据类型选项

许可证：保护

具体数据类型确定了在指定目标网络流量中可以针对其进行检测并生成事件的敏感数据。可以为指定以下内容的数据类型选项修改默认设置：

- 某种检测到的数据类型必须达到才能生成单个会话事件的阈值
- 每种数据类型要监控的目标端口
- 每种数据类型要监控的应用协议

每种数据类型至少必须指定一个事件阈值和至少一个要监控的端口或应用协议。

由思科提供的每种预定义数据类型使用一种其他方法无法访问的 `sd_pattern` 关键字来定义用于在流量中进行检测的内置数据模式。有关预定义数据类型的列表，请参阅第 34-20 页上的表 34-8。您还可以创建自定义数据类型，然后可以使用简单的正则表达式为这些数据类型指定自己的数据模式。有关详情，请参见第 34-23 页上的使用自定义数据类型。

请注意，数据类型名称和模式适用于整个系统；所有其他数据类型选项适用于策略。

下表介绍了可配置的数据类型选项。

表 34-7　　具体数据类型选项

选项	说明
数据类型	显示数据类型的唯一名称。
阈值	指定系统生成事件时数据类型出现的次数。如果没有为启用的数据类型设置阈值，在保存策略时会收到一条错误消息。可以指定 1 至 255 之间的数字。 请注意，在每个会话中，预处理器为检测到的数据类型生成一个事件。另请注意，全局阈值事件与具体数据类型事件无关；也就是说，预处理器会在达到数据类型事件阈值时生成事件，而不管全局事件阈值是否达到，反之亦然。
目标端口	为数据类型指定要监控的目标端口。可以指定单个端口、端口的逗号分隔列表或 `any`（表示任何目标端口）。如果在没有为某种数据类型设置至少一个端口或应用协议的情况下为该数据类型启用了规则，在保存策略时会收到一条错误消息。
应用协议 请注意，此功能需要可控性许可证。	最多可以为数据类型指定八个要监控的应用协议。如果在没有为某种数据类型设置至少一个端口或应用协议的情况下为该数据类型启用了规则，在保存策略时会收到一条错误消息。 必须为选择的每个应用协议至少启用一个检测器（参阅第 46-24 页上的激活和停用检测器）。默认情况下，思科提供的所有检测器均已激活。如果没有为应用协议启用检测器，系统会自动为应用启用思科提供的所有检测器；如果不存在，系统会为应用启用最近修改的用户定义的检测器。 有关为数据类型选择应用协议的详细说明，请参阅第 34-22 页上的选择要监控的应用协议。
Pattern	对于自定义数据类型，这是指定的检测模式（思科提供的数据类型的数据模式已预先定义）。有关详情，请参见第 34-23 页上的使用自定义数据类型。网络界面不显示预定义数据类型的内置模式。 请注意，自定义和预定义的数据模式是针对整个系统的。

使用预定义数据类型

许可证：保护

每个入侵策略都包括用于检测常用数据模式的预定义数据类型，例如信用卡号、邮件地址、美国电话号码以及 带和不带连字符的美国社会安全保障号。每种预定义数据类型都与一个生成器 ID (GID) 为 138 的敏感数据预处理器规则相关。必须启用入侵策略中的关联敏感数据规则才能为要用于策略中的每种数据类型启用检测和事件生成。有关在入侵策略中启用规则的详细信息，请参阅第 32-18 页上的设置规则状态。

为了帮助启用敏感数据规则，配置页面上的链接会将您指向 Rules 页面的过滤视图，其中显示所有预定义和自定义的敏感数据规则。您还可以在 Rules 页面上选择敏感数据规则过滤类别，从而只显示预定义的敏感数据规则。有关详情，请参见第 32-9 页上的过滤入侵策略中的规则。预定义的敏感数据规则还列于 Rule Editor 页面 (**Policies > Intrusion > Rule Editor**)，可在其中的敏感数据规则类别下查看这些规则，但不能进行编辑。

下表介绍了每种数据类型，并列出了必须启用才能为数据类型启用检测和事件生成的对应预处理器规则。

表 34-8　　敏感数据类型

数据类型	说明	预处理器规则 GID:SID
信用卡号	匹配 15 位和 16 位数字的 Visa®、 MasterCard®、 Discover® 和 American Express® 信用卡号 （无论是否带正常分隔破折号或空格）； 也可以使用 Luhn 算法来验证信用卡校验位。	138:2
邮件地址	匹配邮件地址。	138:5
美国 电话号码	与 遵循 `(\d{3}) ?\d{3}-\d{4}` 模式的美国电话号码匹配。	138:6
美国 带有连字符的社会安全保障号	与 包含有效的 3 位数区域号码、有效的 2 位数群组号码且不带连字符的 9 位数美国社会保障号匹配。	138:4
美国 带有连字符的社会安全保障号	与 包含有效的 3 位数区域号码、有效的 2 位数群组号码且带连字符的 9 位数美国社会保障号匹配。	138:3
自定义	匹配指定流量中的用户定义数据模式。有关详情，请参见第 34-23 页上的使用自定义数据类型。	138:>999999

为了减少对社会保障号以外的 9 位数号码的误报，预处理器使用一种算法来验证 3 位数区域号码和 2 位数群组号码；在每个社会保障号中，这两组号码位于 4 位数序列号的前面。预处理器可验证 2009 年 11 月之前的社会保障号中的群组号码。

配置敏感数据检测

许可证：保护

可以修改默认全局设置和具体数据类型的设置。还必须为要检测的每种数据类型启用预处理器规则。

如果在策略中启用敏感数据预处理器规则而未启用敏感数据检测，在保存策略更改时，系统会提示启用敏感数据检测。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

下表介绍了可在 Sensitive Data Detection 页面采取的操作。

表 34-9　　敏感数据配置操作

要.....	您可以.....
修改全局设置	有关可修改的全局设置的信息，请参阅第 34-7 页上的表 34-6。
修改数据类型选项	点击 Targets 页面区域中的数据类型名称。 Configuration 页面区域会进行更新以显示数据类型的当前设置。有关可修改的选项的详细信息，请参阅具体数据类型选项表。

表 34-9　　敏感数据配置操作 （续）

要.....	您可以.....
为数据类型添加或删除要监控的应用协议 请注意，此功能需要可控性许可证。	在 **Application Protocols** 字段中点击，或点击字段旁边的 **Edit**。系统将显示 Application Protocols 弹出窗口： • 要添加要监控的应用协议 （最多八个），请从左侧的 **Available** 列表中选择一个或多个应用协议，然后点击右箭头 (**>**) 按钮。 • 要删除应用协议，请从右侧的 **Enabled** 列表中选择，然后点击左箭头 (**<**) 按钮。 点击的同时使用 Ctrl 或 Shift 选择多个应用协议。您也可以点击并拖动鼠标，以选择多个相邻的应用协议。 必须为选择的每个应用协议至少启用一个检测器 （参阅第 46-24 页上的激活和停用检测器）。默认情况下，思科提供的所有检测器均已激活。如果没有为应用协议启用检测器，系统会自动为应用启用思科提供的所有检测器；如果不存在，系统会为应用启用最近修改的用户定义的检测器。 **注**　要检测 FTP 流量中的敏感数据，必须添加 `Ftp 数据`应用协议。有关详情，请参见第 34-23 页上的特殊情况：检测 FTP 流量中的敏感数据。
创建自定义数据类型	在页面左侧点击 **Data Types** 旁边的 **+** 符号。系统将显示 Add Data Type 弹出窗口。 指定唯一的数据类型名称和要使用该数据类型检测的模式，然后点击 **OK**，或者点击 **Cancel** 放弃编辑。有关详情，请参见第 34-23 页上的使用自定义数据类型。
显示敏感数据预处理器规则	点击 Global Settings 页面区域上方的 **Configure Rules for Sensitive Data Detection** 链接。所有敏感数据预处理器规则的列表显示在 Rules 页面的过滤视图中。 或者，可以启用或禁用任何列出的规则。请注意，必须为要用于入侵策略中的每种数据类型启用敏感数据预处理器规则。有关详情，请参见第 32-18 页上的设置规则状态。 还可以为 Rules 页面上可用的任何其他操作 （例如规则抑制、基于速率的攻击防御，等等）配置敏感数据规则；有关详细信息，请参阅第 32-1 页上的使用规则调整入侵策略。 点击 **Back** 返回到 Sensitive Data Detection 页面。

要配置敏感数据检测，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Sensitive Data Detection**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Sensitive Data Detection 页面。页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　可以采取敏感数据配置操作表中所述的任何操作。

步骤 6　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

选择要监控的应用协议

许可证：可控性

最多可以为每种数据类型指定八个应用协议进行监控。有关系统可在网络上检测的应用协议的详细信息，请参阅第 50-31 页上的使用服务器。

必须为选择的每个应用协议至少启用一个检测器（参阅第 46-24 页上的激活和停用检测器）。默认情况下，思科提供的所有检测器均已激活。如果没有为应用协议启用检测器，系统会自动为应用启用思科提供的所有检测器；如果不存在，系统会为应用启用最近修改的用户定义的检测器。

必须为每种数据类型至少指定一个要监控的应用协议或端口。但是，除了要检测 FTP 流量中的敏感数据的情况之外，思科建议在指定应用协议时指定相应的端口，以便实现最全面覆盖。例如，如果指定 HTTP，还可以配置通用的 HTTP 端口 80。如果网络上的新主机执行 HTTP，系统会在它发现新 HTTP 应用协议的时间间隔内监控端口 80。

在想要检测 FTP 流量中的敏感数据的情况下，您必须指定 FTP 数据应用协议；指定端口号没有好处。有关详情，请参见第 34-23 页上的特殊情况：检测 FTP 流量中的敏感数据。

要修改检测敏感数据的应用协议，请执行以下操作：

管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Sensitive Data Detection**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Sensitive Data Detection 页面。

页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　点击 **Data Types** 下的数据类型名称并选择要修改的数据类型。

Configuration 页面会进行更新以显示选定数据类型的当前设置。

步骤 6　在 **Application Protocols** 字段中点击，或点击字段旁边的 **Edit**。

系统将显示 Application Protocols 弹出窗口。

步骤 7　您有两种选择：

- 要添加要监控的应用协议 （最多八个），请从左侧的 **Available** 列表中选择一个或多个应用协议，然后点击右箭头 (**>**) 按钮。
- 要删除应用协议，请从右侧的 **Enabled** 列表中选择，然后点击左箭头 (**<**) 按钮。

点击的同时使用 Ctrl 或 Shift 选择多个应用协议。您也可以点击并拖动鼠标，以选择多个相邻的应用协议。

注　要检测 FTP 中的敏感数据，必须添加 `FTP data` 应用程序协议。有关详情，请参见第 34-23 页上的特殊情况：检测 FTP 流量中的敏感数据。

步骤 8　点击 **OK** 以添加应用协议。

系统将显示 Sensitive Data Detection 页面且应用协议会进行更新。

特殊情况：检测 FTP 流量中的敏感数据

许可证：可控性

通常，可通过指定要监控的端口或在部署中指定应用协议来确定要监控敏感数据的流量。但是，对于检测 FTP 流量中的敏感数据来说，指定端口或应用协议并不足够。在 FTP 应用协议的流量中找到 FTP 流量中的敏感数据，这种情况间歇出现并使用临时端口号，因此难以检测。要检测 FTP 流量中的敏感数据，**必须**在配置中包括以下几项：

- 指定 `FTP data` 应用协议。

  指定 `FTP data` 应用协议可检测 FTP 流量中的敏感数据。有关详情，请参见第 34-22 页上的选择要监控的应用协议。

  对于检测 FTP 流量中的敏感数据这种特殊情况，指定 `FTP data` 应用协议不会调用检测功能；而是会调用 FTP/Telnet 预处理器的快速处理功能来检测 FTP 流量中的敏感数据。有关详情，请参见第 27-16 页上的解码 FTP 和 Telnet 流量。
- 确保 FTP Data 检测器已启用 （默认情况下已启用）。

  请参阅第 46-24 页上的激活和停用检测器。
- 确保配置包括至少一个要监控敏感数据的端口。

  请注意，不需要指定 FTP 端口 （只要检测 FTP 流量中的敏感数据这种罕见情况除外）。大多数敏感数据配置将包括其他端口 （例如 HTTP 或邮件端口）。如果只要指定一个 FTP 端口进行监控，思科建议指定 FTP 命令端口 `23`。有关详细信息，请参阅第 34-20 页上的配置敏感数据检测。

使用自定义数据类型

许可证：保护

可以创建和修改自定义数据类型以检测指定的数据模式。例如，医院可以创建一种数据类型来保护患者编号；再如，大学可以创建一种数据类型来检测具有唯一编号模式的学号。

创建的每种自定义数据类型还会创建一个敏感数据预处理器规则，该规则的生成器 ID (GID) 为 138， Snort ID 为大于或等于 1000000 （也就是本地规则的 SID）。必须启用关联的敏感数据规则才能为要用于策略中的每种自定义数据类型启用检测和事件生成。有关在入侵策略中启用规则的详细信息，请参阅第 32-18 页上的设置规则状态。

为了帮助启用敏感数据规则，配置页面上的链接会将您指向 Rules 页面的过滤视图，其中显示所有预定义和自定义的敏感数据规则。您还可以在 Rules 页面上选择本地规则过滤类别，从而只显示自定义敏感数据规则。有关详情，请参见第 32-9 页上的过滤入侵策略中的规则。请注意，自定义敏感数据规则不会列于 Rule Editor 页面。

创建的自定义数据类型已添加到所有入侵策略。必须在要使用的任何策略中启用关联敏感数据规则，才能检测和生成特定自定义数据类型的事件。

请注意，必须使用 Sensitive Data Detection 配置页面才能创建数据类型及其关联的规则。不能使用规则编辑器创建敏感数据规则。

有关详细信息，请参阅以下各节：

- 第 34-24 页上的定义自定义数据类型的数据模式
- 第 34-26 页上的配置自定义数据类型
- 第 34-27 页上的编辑自定义数据类型名称和检测模式

定义自定义数据类型的数据模式

许可证：保护

可使用一组由以下部分组成的正则表达式来定义自定义数据类型的数据模式：

- 三个元字符
- 允许将元字符用作原义字符的转义字符
- 六个字符类

元字符是在正则表达式中具有特殊含义的原义字符。下表介绍了可在定义自定义数据模式时使用的元字符。

表 34-10　　敏感数据模式元字符

元字符	说明	示例
?	匹配前面的字符或转义序列零次或一次；也就是说，前面的字符或转义序列是可选的。	colou?r 匹配 color 或 colour
{*n*}	匹配前面的字符或转义序列 *n* 次。	例如， \d{2} 匹配 55、 12 等； \l{3} 匹配 AbC、 www 等； \w{3} 匹配 a1B、 25C 等； x{5} 匹配 xxxxx
\	元字符可用作实际字符，还可用于指定预定义的字符类。有关可在敏感数据模式下使用的字符类的说明，请参阅第 34-25 页上的表 34-12。	\?匹配问号； \\ 匹配反斜杠； \d 匹配数字字符；等等

必须将反斜杠用于转义下表中的字符，这样敏感数据预处理器才能将它们正确解释为原义字符。

表 34-11　　转义敏感数据模式字符

使用的转义字符	代表的原义字符
\?	?
\{	{

表 34-11　转义敏感数据模式字符（续）

使用的转义字符	代表的原义字符
\}	}
\\	\

下表介绍了可在定义自定义数据模式时使用的字符类。

表 34-12　敏感数据模式字符类

字符类	说明	字符类定义
\d	匹配任何 ASCII 数字字符 0-9	0-9
\D	匹配任何不是 ASCII 数字字符的字节	不是 0-9
\l（小写“ell”）	匹配任何 ASCII 字母	a-zA-Z
\L	匹配任何不是 ASCII 字母的字节	不是 a-zA-Z
\w	匹配任何 ASCII 字母数字字符 请注意，与 PCRE 正则表达式不同，这不包括下划线 (_)。	a-zA-Z0-9
\W	匹配任何不是 ASCII 字母数字字符的字节	不是 a-zA-Z0-9

预处理器将直接输入（而不是作为正则表达式的一部分输入）的字符视为原义字符。例如，数据模式 1234 匹配 `1234`。

以下数据模式示例（用于预定义的敏感数据规则 138:4）使用转义的数字字符类、乘数和选项说明符元字符、文字破折号 (-) 和左右括号 () 字符来检测美国 电话号码：

```
(\d{3}) ?\d{3}-\d{4}
```

创建自定义数据模式时务必谨慎。考虑将下列备用数据模式用于检测电话号码，尽管使用的是有效语法，但可能会导致许多误报：

```
(?\d{3})??\d{3}-?\d{4}
```

由于第二个示例结合了可选括号、可选空格和可选破折号，它会在下列所需模式中检测电话号码及其他方面：

- `(555)123-4567`
- `555123-4567`
- `5551234567`

但是，第二个示例模式也会检测以下可能无效的模式及其他方面，从而造成误报：

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

最后举一个极端的例子（仅作说明用途）：创建一种数据模式，用以在小型企业网络上的所有目标流量中使用一个低事件阈值来检测小写字母 `a`。这种数据模式能够在短短几分钟内生成数百万的事件，从而可能令系统不胜负荷。

配置自定义数据类型

许可证：保护

实质上，是为针对预定义的数据类型所配置的自定义数据类型配置相同的数据类型选项。有关设置所有数据类型通用的选项，请参阅第 34-18 页上的选择具体数据类型选项。此外，还必须为自定义数据类型指定名称和数据模式。

请注意，创建自定义数据类型还会创建关联的自定义敏感数据预处理规则，必须在要使用该数据类型的每个策略中启用该规则。有关在入侵策略中启用规则的详细信息，请参阅第 32-18 页上的设置规则状态。

要创建或修改自定义数据类型，请执行以下操作：

管理员/入侵管理员

步骤 1　选择 **Policies> Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Sensitive Data Detection**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Sensitive Data Detection 页面。

页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　您有以下选项：

- 要创建自定义数据类型，请在页面左侧点击 **Data Types** 旁边的 **+** 符号。系统将显示 Add Data Type 弹出窗口。

  指定唯一的数据类型名称和要使用该数据类型检测的模式，然后点击 **OK**，或者点击 **Cancel** 放弃编辑。有关详情，请参见第 34-27 页上的编辑自定义数据类型名称和检测模式。

  系统将显示 Sensitive Data Detection 页面。如果点击 **OK**，页面会进行更新以显示更改。

- 要修改任何预定义和自定义数据类型通用的选项，请点击 **Targets** 页面区域中的数据类型名称。

  Configuration 页面区域会进行更新以显示数据类型的当前设置。有关详情，请参见第 34-20 页上的配置敏感数据检测。

- 要为自定义数据类型编辑系统范围的名称和数据模式，请参阅第 34-27 页上的编辑自定义数据类型名称和检测模式。

- 要删除自定义数据类型，请点击要删除的数据类型旁边的删除图标 ( )，然后点击 **OK**，或者点击 **Cancel** 放弃删除数据类型。

  请注意，如果任何入侵策略中启用了某个数据类型的敏感数据类型规则，不能删除该数据类型。删除某个自定义数据类型会导致从所有入侵策略中删除该数据类型。

编辑自定义数据类型名称和检测模式

许可证：保护

可以为自定义敏感数据规则修改系统范围的名称和检测模式。请注意，更改这些设置会导致系统上所有其他策略中的设置也随之更改。另请注意，如果必须已应用的访问控制策略包含使用修改的自定义数据类型的入侵策略，必须重新应用这些策略。

除自定义数据类型名称和数据模式之外，所有数据类型选项都是特定于策略的，适用于自定义和预定义的数据类型。有关修改自定义数据类型名称和数据模式以外选项的详细信息，请参阅第 34-18 页上的选择具体数据类型选项。

要编辑自定义数据类型名称和数据模式，请执行以下操作：

管理员/入侵管理员

步骤 1　选择 **Policies> Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Sensitive Data Detection**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Sensitive Data Detection 页面。

页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　在 **Targets** 页面区域，点击要修改的自定义数据类型的名称。

页面会进行更新以显示数据类型的当前设置，并且 **Edit Data Type Name and Pattern** 链接显示在 Configuration 页面区域的右上方。

步骤 6　点击 **Edit Data Type Name and Pattern** 链接。

系统将显示 Edit Data Type 弹出窗口。

步骤 7　修改数据类型名称和/或模式，然后点击 **OK**，或者点击 **Cancel** 放弃所做的编辑。有关指定数据模式的详细信息，请参阅第 34-24 页上的定义自定义数据类型的数据模式。

系统将显示 Sensitive Data Detection 页面。如果点击 **OK**，页面将会显示更改。

从全局限制入侵事件记录

阈值可用于限制系统记录和显示入侵事件的次数。您配置作为入侵策略一部分的阈值会导致系统根据与规则匹配的流量在特定时间内从特定地址或地址范围传出或以其作为传入目标的次数，生成事件。这可以防止事件数量过多。此功能需要保护许可证。

设置事件通知阈值有两种方式：

- 可以跨所有流量设置全局阈值，用于限制每个指定时间段记录和显示来自特定源地址或目标地址的事件的频率。有关详细信息，请参阅第 35-1 页上的了解阈值和第 35-3 页上的配置全局阈值。
- 可以按照入侵策略配置中的每条共享对象规则、标准文本规则或预处理器规则设置阈值，如第 32-20 页上的配置事件阈值中所述。

了解阈值

许可证：保护

默认情况下，每个入侵策略都包含全局规则阈值。默认阈值将每条规则的事件生成频率限制为对发往同一个目标地址的流量每 60 秒生成一个事件。此全局阈值默认应用于所有入侵规则和预处理器规则。请注意，可以在入侵策略的 Advanced Settings 页面中禁用此阈值。

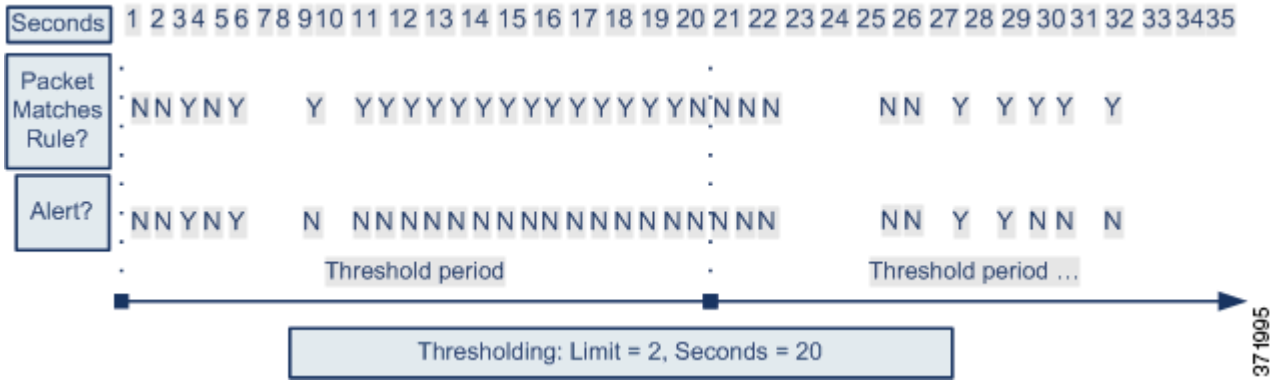
也可以对特定的规则设置单独的阈值，从而覆盖此阈值。例如，可将全局限值阈值设置为每 60 秒生成五个事件，然后为 SID 1315 设置每 60 秒生成十个事件的特定阈值。所有其他规则每 60 秒生成的事件不超过五个，但是系统每 60 秒可为 SID 1315 生成最多十个事件。

有关设置基于规则的阈值的详细信息，请参阅第 32-20 页上的配置事件阈值。

提示 在有多个 CPU 的受管设备上，全局阈值或单独的阈值可能会导致事件数量高于预期。

下图显示的例子中，系统正在受到违反特定规则的攻击。全局限值阈值将每条规则的事件生成频率限制为每 20 秒生成两个事件。

请注意，该时间段在 1 秒时开始，在 21 秒时结束。该时间段结束后，请注意时间周期重新开始，接下来两次规则匹配生成了事件，随后系统在这一时间段内不再生成事件。



了解阈值选项

许可证：保护

可以通过阈值来限制入侵事件的生成，只在某个时间段内生成特定数量的事件，或者只为一组事件生成一个事件。配置全局阈值时，首先必须指定阈值类型，如下表所述。

表 35-1　　阈值选项

选项	说明
限制	为指定时间段内触发规则的指定数量的数据包 （由计数参数指定）记录并显示事件。例如，如果将类型设置为 **Limit**，将 **Count** 设置为 10，并将 **Seconds** 设置为 60，而同一分钟内有 14 个数据包触发规则，则系统在显示发生的前 10 个违反该规则的事件后将停止记录违反该规则的事件。
阈值	在指定时间段内，当指定数量的数据包 （由计数参数指定）触发规则时，记录并显示一个事件。请注意，达到事件阈值计数且系统记录该事件之后，时间计数器将重新开始计数。例如，将类型设置为 **Threshold**，将 **Count** 设置为 10，并将 **Seconds** 设置为 60 时，如果到 33 秒时规则触发 10 次，系统将生成一个事件，然后将 Seconds 和 Count 计数器重置为 0。其后，该规则在接下来 25 秒内又触发 10 次。由于计数器在第 33 秒时已重置为 0，因此系统会再记录一个事件。
共通活动	每个指定时间段在指定数量 （计数）的数据包触发规则后记录并显示一次事件。例如，将类型设置为 **Both**，将 **Count** 设置为 2，并将 **Seconds** 设置为 10 时，事件计数结果如下： • 如果 10 秒内触发规则一次，系统不会生成任何事件 （未达到阈值） • 如果 10 秒内触发规则两次，系统将生成一个事件 （第二次触发规则时达到阈值） • 如果 10 秒内触发规则四次，系统将生成一个事件 （第二次触发规则时达到阈值，忽略其后的事件）

接下来指定跟踪，确定事件实例计数是按源 IP 地址计算还是按目标 IP 地址计算。最后，指定用于定义阈值的实例数和时间段。

表 35-2　　阈值实例/时间选项

选项	说明
计数	每个跟踪 IP 地址或地址范围在每个指定时间段内达到阈值所需的事件实例数。
数秒	计数重置之前经过的秒数。如果将阈值类型设置为 **Limit**，将跟踪设置为 **Source**，将 **Count** 设置为 10，并将 **Seconds** 设置为 10，则系统将记录并显示 10 秒钟内发生的来自指定源端口的前 10 个事件。如果前 10 秒内只发生了七个事件，系统将记录并显示这些事件，而如果前 10 秒内发生了 40 个事件，系统将记录并显示 10 个事件，然后在为期 10 秒的时间段过后重新开始计数。

配置全局阈值

许可证：保护

可以设置全局阈值来管理每个规则在一段时间内生成的事件数。设置全局阈值后，该阈值将应用于没有特定阈值可覆盖该阈值的每条规则。有关配置阈值的详细信息，请参阅第 35-1 页上的了解阈值。

默认情况下，在系统上配置全局阈值。默认值如下所示：

- **Type** - Limit
- **Track By** - Destination
- **Count** - 1
- **Seconds** - 60

要配置全局阈值，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　此时有两种选择，取决于 **Intrusion Rule Thresholds** 下的 **Global Rule Thresholding** 是否启用：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Global Rule Thresholding 页面。页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　从 **Type** 单选按钮，选择在由 seconds 参数指定的时间内要应用的阈值类型。有关详细信息，请参阅阈值选项表。

- 选择 **Limit** 则记录并显示触发规则的每个数据包的事件，直到超过计数参数指定的限值为止。
- 选择 **Threshold** 则为触发该规则并且代表与计数参数设置的阈值相匹配的实例或者是阈值倍数的每个数据包记录并显示一个事件。
- 选择 **Both** 则在触发规则的数据包达到计数参数指定的数量之后记录并显示一个事件。

步骤 6　从 **Track By** 单选按钮选择跟踪方法：

- 选择 **Source** 则在来自一个或多个特定源 IP 地址的流量中查找规则匹配项。
- 选择 **Destination** 则在发往特定目标 IP 地址的流量中查找规则匹配项。

步骤 7　在 **Count** 字段：

- 若为 **Limit** 阈值，在 Count 字段中指定每个跟踪 IP 地址在每个指定时间段内达到阈值所需的事件实例数。
- 若为 **Threshold** 阈值，在 Count 字段中指定要用作阈值的规则匹配项数量。

步骤 8　在 **Seconds** 字段：

- 若为 **Limit** 阈值，在 Seconds 字段指定跟踪攻击时构成该时间段的秒数。
- 若为 **Threshold** 阈值，在 Seconds 字段中指定计数重置之前经过的秒数。请注意，如果在指示的秒数过完之前规则匹配项数量即达到 **Count** 字段指示的数量，计数将重置。

步骤 9　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

禁用全局阈值

许可证：保护

默认情况下，全局限值阈值将发往目标地址的流量的事件数限制为每 60 秒一个事件。如果要为特定规则的事件设置阈值但不将阈值默认应用于每条规则，可以在最高策略层禁用全局阈值。

要禁用全局阈值，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　在 **Intrusion Rule Thresholds** 下，禁用 **Global Rule Thresholding**。

步骤 5　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

第 36 章

了解和编写入侵规则

*入侵规则*是一组指定的关键字和参数，通过分析网络流量来检查其是否符合规则中的条件，从而检测试图利用网络漏洞的行为。系统将数据包与每条规则中指定的条件进行比较，如果数据包数据符合规则中指定的所有条件，则触发此规则。如果规则是*警报规则*，将生成入侵事件。如果是*通过规则*，将忽略流量。可以通过防御中心或网络界面查看和评估入侵事件。

注意事项 将编写的入侵规则用于生产环境之前，请务必使用受控网络环境测试这些规则。编写错误的入侵规则可能会严重影响系统性能。

请注意：

- 对于内联部署中的*丢弃*规则，系统将丢弃数据包并生成事件。有关丢弃规则的详细信息，请参阅第 32-18 页上的设置规则状态。
- 思科提供两种类型的入侵规则：共享对象规则和标准文本规则。思科漏洞研究工作组 (VRT) 可以使用共享对象规则来检测传统标准文本规则无法检测的漏洞攻击。不能创建共享对象规则。在自行编写入侵规则时，可以创建标准文本规则。

可以编写自定义标准文本规则，以调整可能出现的事件类型。请注意，虽然本文档有时讨论以检测特定漏洞为目标的规则，但最成功的规则是以检测可能试图利用已知漏洞的流量为目标，而不是以检测特定已知漏洞为目标。通过编写规则和指定规则的事件消息，可以更轻松地识别可能存在攻击和策略逃避行为的流量。有关评估事件的详细信息，请参阅第 41-1 页上的处理入侵事件。

当您启用自定义入侵策略中的自定义标准文本规则时，请记住，某些控制关键字和参数需要首先以某种方式解码或预处理该流量。本章说明在用于管理预处理的网络分析策略中必须配置的选项。请注意，如果禁用所需的预处理器，系统会自动采用其当前设置使用该预处理器，尽管该预处理器在网络分析策略网络界面中保持禁用状态。

注 由于预处理和入侵检测如此密切相关，检查每个数据包的网络分析和入侵策略**必须**互相补充。定制预处理，特别是使用多个自定义网络分析策略，是一项**高级**任务。有关详细信息，请参阅第 23-10 页上的自定义策略的局限性。

有关详细信息，请参阅以下各节：

- 第 36-2 页上的了解规则结构介绍构成有效标准文本规则的组成部分，包括规则报头和规则选项。
- 第 36-3 页上的了解规则报头详细介绍规则报头的各个部分。
- 第 36-9 页上的了解规则中的关键字和参数解释 FireSIGHT 系统中可用的入侵规则关键字的使用和语法。
- 第 36-93 页上的构建规则解释如何使用规则编辑器构建新规则。

- 第 36-98 页上的搜索规则解释如何搜索现有规则。
- 第 36-99 页上的过滤 Rule Editor 页面上的规则解释如何显示规则子集以帮助查找特定规则。

了解规则结构

许可证：保护

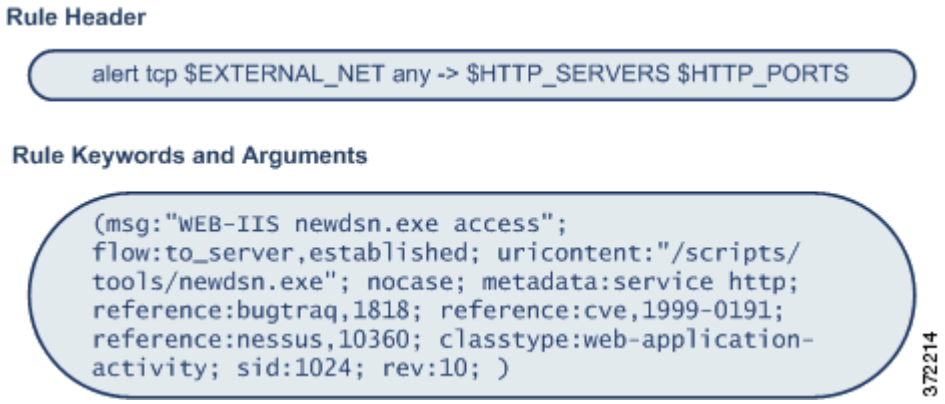
所有标准文本规则均包含两个逻辑部分：规则报头和规则选项。规则报头包含：

- 规则的操作或类型
- 协议
- 源 IP 地址、目标 IP 地址和子网掩码
- 方向指示符 （显示从源到目标的流量流动方向）
- 源端口和目标端口

规则选项部分包含：

- 事件消息
- 关键字及其参数
- 模式 （数据包负载必须与之匹配才能触发规则）
- 规范 （规定规则引擎应检查数据包的哪些部分）

下图说明规则的组成部分：

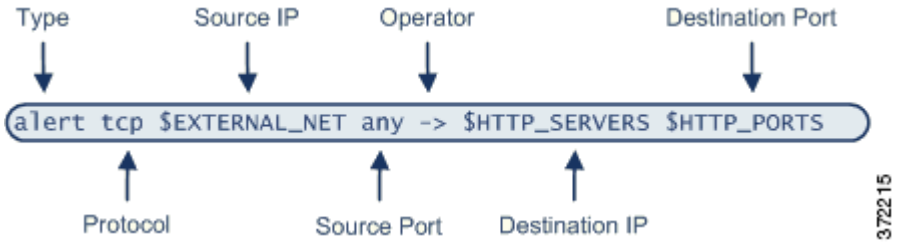


请注意，括号里的是规则选项部分。规则编辑器提供了一个易于使用的界面来帮助构建标准文本规则。

了解规则报头

许可证：保护

每个标准文本规则和共享对象规则都有一个包含参数的规则报头。下面说明规则报头的组成部分：



下表介绍了规则报头的上述各个部分。

表 36-1　　规则报头值

规则报头组成部分	示例值	示例值的作用
操作	警报	如果触发，将会生成事件。
协议	tcp	仅测试 TCP 流量。
源 IP 地址	$EXTERNAL_NET	测试来自不在内部网络上的任何主机的流量。
源端口	any	测试来自发起主机上任何端口的流量。
运算符	->	测试外部流量 （流向网络上的网络服务器）。
目标 IP 地址:	$HTTP_SERVERS	测试将要传送到内部网络上被指定为网络服务器的任何主机的流量
目标端口	$HTTP_PORTS	测试传送到内部网络上 HTTP 端口的流量。

注　与大多数入侵规则一样，以上示例使用默认变量。有关变量、变量的含义以及如何配置变量的详细信息，请参阅第 3-15 页上的使用变量集。

有关规则报头参数的详细信息，请参阅以下各节：

- 第 36-4 页上的指定规则操作介绍规则类型，并解释如何指定触发规则时发生的操作。
- 第 36-4 页上的指定协议解释如何为规则应测试的流量定义流量协议。
- 第 36-5 页上的在入侵规则中指定 IP 地址解释如何在规则报头中定义单个 IP 地址和 IP 地址块。
- 第 36-8 页上的在入侵规则中定义端口解释如何在规则报头中定义单个端口和端口范围。
- 第 36-9 页上的指定方向介绍可用的运算符，并解释应如何指定流量的流动方向才能使规则对流量进行测试。

指定规则操作

许可证：保护

每个规则报头都包含一个用于指定数据包触发规则时系统应采取的操作的参数。操作设置为 *alert* 的规则将会针对触发规则的数据包生成入侵事件并记录该数据包的详细信息。操作设置为 *pass* 的规则不会针对触发规则的数据包生成入侵事件，也不会记录该数据包的详细信息。

注 在内联部署中，规则状态设置为 *Drop and Generate Events* 的规则会针对触发规则的数据包生成入侵事件。此外，如果在被动部署中应用丢弃规则，该规则将会充当警报规则。有关丢弃规则的详细信息，请参阅第 32-18 页上的设置规则状态。

默认情况下，通过规则会覆盖警报规则。可以创建通过规则来防止符合通过规则中定义的条件的数据包在特定情况下触发警报规则，而无需禁用预警报则。例如，您可能希望使检测尝试作为“匿名”用户登录 FTP 服务器这种情况的规则保持活动状态。但是，如果网络有一个或多个合法的匿名 FTP 服务器，您可以编写并激活一个通过规则，在其中指明匿名用户不会对那些特定服务器触发原始规则。

在规则编辑器中，可以从 **Action** 列表中选择规则类型。有关使用规则编辑器构建规则报头的步骤的详细信息，请参阅第 36-93 页上的构建规则。

指定协议

许可证：保护

在每个规则报头中，必须指定规则检查的流量的协议。可以指定以下网络协议用于分析：

- ICMP （互联网控制消息协议）
- IP （互联网协议）

注 如果协议设置为 `ip`，系统将忽略入侵规则报头中的端口定义。有关详细信息，请参阅第 36-8 页上的在入侵规则中定义端口。

- TCP （传输控制协议）
- UDP （用户数据报协议）

如果使用 **IP** 作为协议类型，将会检查 IANA 分配的所有协议 （包括 TCP、UDP、ICMP、IGMP 等等）。有关 IANA 分配的协议的完整列表，请访问 http://www.iana.org/assignments/protocol-numbers。

注 目前不能编写与 IP 负载中下一个报头 （例如 TCP 报头）模式匹配的规则。相反，内容匹配从上一个解码的协议开始。要解决这个问题，可以使用规则选项来匹配 TCP 报头中的模式。

在规则编辑器中，可以从 **Protocol** 列表中选择协议类型。有关使用规则编辑器构建规则报头的步骤的详细信息，请参阅第 36-93 页上的构建规则。

在入侵规则中指定 IP 地址

许可证：保护

通过将数据包检查限制为仅针对来自或发往特定 IP 地址的数据包，可以减少系统必须执行的数据包检查工作量。这样做还可以令规则更加具体，并消除规则针对源和目标 IP 地址未指示可疑行为的数据包进行触发的可能性，从而减少误报。

提示　系统只能识别 IP 地址，不接受源或目标 IP 地址的主机名。

在规则编辑器中，可以在 **Source IPs** 和 **Destination IPs** 字段中指定源 IP 地址和目标 IP 地址。有关使用规则编辑器构建规则报头的步骤的详细信息，请参阅第 36-93 页上的构建规则。

编写标准文本规则时，可以根据自身需求以多种方法指定 IPv4 和 IPv6 地址。可以指定单个 IP 地址、`any`、IP 地址列表、CIDR 记法、前缀长度、网络变量、网络对象或网络对象组。此外，还可以指明要排除的特定 IP 地址或 IP 地址集。指定 IPv6 地址时，可使用 RFC 4291 中定义的任意寻址约定。

下表总结了可用于指定源 IP 地址和目标 IP 地址的各种方法。

表 36-2　源/目标 IP 地址语法

要指定.....	使用.....	示例
任何 IP 地址	`any`	`any`
特定 IP 地址	IP 地址 请注意，不能在同一规则中混合使用 IPv4 和 IPv6 源地址和目标地址。	`192.168.1.1` `2001:db8::abcd`
IP 地址列表	使用方括号 (`[]`) 将地址括起来，并使用逗号分隔各个 IP 地址	`[192.168.1.1,192.168.1.15]` `[2001:db8::b3ff, 2001:db8::0202]`
IP 地址块	IPv4 CIDR 块或 IPv6 地址前缀记法	`192.168.1.0/24` `2001:db8::/32`
除特定 IP 地址或地址集以外的任何项	在要否定的端口、端口列表或端口范围前面加上 `!`字符	`!192.168.1.15` `!2001:db8::0202:b3ff:fe1e`
IP 地址块中除一个或多个特定 IP 地址以外的任何 IP 地址	在地址块后加上被否定地址或地址块的列表	`[10.0.0/8, !10.2.3.4, !10.1.0.0/16]` `[2001:db8::/32, !2001:db8::8329, !2001:db8::0202]`
网络变量定义的 IP 地址	前面带有 `$` 的大写字母形式的变量名称 请注意，无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。有关详情，请参见第 3-15 页上的使用变量集。	`$HOME_NET`
除 IP 地址变量定义的地址以外的所有 IP 地址	前面带有 `!$` 的大写字母形式的变量名称 有关详情，请参见第 36-7 页上的在入侵规则中排除 IP 地址。	`!$HOME_NET`
网络对象或网络对象组定义的 IP 地址	采用 `!{object_name}` 这种格式的对象或对象组名称。 有关详情，请参见第 3-4 页上的使用网络对象。	`${192.168sub16}`

表 36-2　源/目标 IP 地址语法 （续）

要指定.....	使用.....	示例
除网络对象或网络对象组定义的地址以外的所有 IP 地址	对象或对象组名称用花括号 ({}) 括起来，前面带有 `!$`。 有关详情，请参见第 3-4 页上的使用网络对象。	`!${192.168sub16}`

有关可用于指定源和目标 IP 地址的语法的更多详细信息，以及有关使用变量指定 IP 地址的信息，请参阅以下各节：

- 第 1-16 页上的 IP 地址约定.
- 第 3-15 页上的使用变量集
- 第 36-6 页上的指定 IP 地址
- 第 36-6 页上的指定多个 IP 地址
- 第 36-7 页上的指定网络对象
- 第 36-7 页上的在入侵规则中排除 IP 地址

指定 IP 地址

许可证：保护

可以指定 `any` 这个词作为规则的源或目标 IP 地址，以指示 IPv4 或 IPv6 地址。

例如，以下规则在 **Source IPs** 和 **Destination IPs** 字段中使用参数 **`any`** 来评估具有 IPv4 或 IPv6 源地址或目标地址的数据包：

```
alert tcp any any -> any any
```

还可以指定 `::` 以指示 IPv6 地址。

指定多个 IP 地址

许可证：保护

可以列出多个 IP 地址，地址之间用逗号分隔，如有需要，还可以用方括号将非否定地址列表括起来，如以下示例所示：

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

可以单独或以任意组合列出 IPv4 和 IPv6 地址，如以下示例所示：

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

请注意，现在不再要求用方括号将 IP 地址列表括起来 （旧版软件要求这样做）。另请注意，输入列表时，可以在每个逗号前后添加一个空格。

注　必须用方括号将否定列表括起来。有关详情，请参见第 36-7 页上的在入侵规则中排除 IP 地址。

也可以使用 IPv4 无类别域际路由选择 (CIDR) 记法或 IPv6 前缀长度来指定地址块。例如：

- 192.168.1.0/24 指定子网掩码为 255.255.255.0 的 192.168.1.0 网络中的 IPv4 地址，即，192.168.1.0 至 192.168.1.255。有关详细信息，请参阅第 1-16 页上的 IP 地址约定。
- 2001:db8::/32 指定前缀长度为 32 位的 2001:db8:: 网络中的 IPv6 地址，即， 2001:db8:: 至 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff。

提示 如果需要指定 IP 地址块，但仅以 CIDR 或前缀长度记法无法表示出该地址块，可以在 IP 地址列表中使用 CIDR 块和前缀长度。

指定网络对象

许可证：保护

可以使用以下语法指定网络对象或网络对象组：

```
${object_name | group_name}
```

其中：

- *object_name* 是网络对象的名称
- *group_name* 是网络对象组的名称

有关创建网络对象和网络对象组的信息，请参阅第 3-4 页上的使用网络对象。

假设已创建一个名为 `192.168sub16` 的网络对象和一个名为 `all_subnets` 的网络对象组，那么，可以指定以下语法以识别使用该网络对象的 IP 地址：

```
${192.168sub16}
```

并且可以指定以下语法以使用该网络对象组：

```
${all_subnets}
```

还可以对网络对象和网络对象组进行否定。例如：

```
!${192.168sub16}
```

有关详情，请参见第 36-7 页上的在入侵规则中排除 IP 地址。

在入侵规则中排除 IP 地址

许可证：保护

可以使用感叹号 (`!`) 否定指定 IP 地址。也就是说，可以匹配除指定 IP 地址以外的所有 IP 地址。例如，`!192.168.1.1` 指定除 192.168.1.1 以外的任何 IP 地址，`!2001:db8:ca2e::fa4c` 指定除 2001:db8:ca2e::fa4c 以外的任何 IP 地址。

要否定某个 IP 地址列表，请用方括号将该 IP 地址列表括起来，并在其前面加上 `!`。例如，`![192.168.1.1,192.168.1.5]` 将定义除 192.168.1.1 和 192.168.1.5 以外的任何 IP 地址。

注 要否定 IP 地址列表，必须使用方括号。

对 IP 地址列表使用否定字符时务必要小心。例如，如果使用 `[!192.168.1.1,!192.168.1.5]` 匹配不是 192.168.1.1 和 192.168.1.5 的任何地址，系统会将此语法解释为“非 192.168.1.1 的任何地址，**或**非 192.168.1.5 的任何地址”。

由于 192.168.1.5 不是 192.168.1.1，且 192.168.1.1 不是 192.168.1.5，因此，这两个 IP 地址都与 `[!192.168.1.1,!192.168.1.5]` 的 IP 地址值匹配；此语法实质上与使用“`any`”相同。

应该使用 `![192.168.1.1,192.168.1.5]`。系统会将此语法为“**非** 192.168.1.1 **且非** 192.168.1.5”，这意味着，与方括号中所列地址以外的任何 IP 地址匹配。

请注意，从逻辑上讲，不能对 `any` 进行否定 （如果它被否定，将表示无地址）。

在入侵规则中定义端口

许可证：保护

在规则编辑器中，可以在 **Source Port** 和 **Destination Port** 字段中指定源端口和目标端口。有关使用规则编辑器构建规则报头的步骤的详细信息，请参阅第 36-93 页上的构建规则。

FireSIGHT 系统使用特定类型的语法来定义规则报头中使用的端口号。

注　如果协议设置为 `ip`，系统将忽略入侵规则报头中的端口定义。有关详细信息，请参阅第 36-4 页上的指定协议。

可以列出多个端口，端口之间用逗号分隔，如以下示例所示：

```
80, 8080, 8138, 8600-9000, !8650-8675
```

如有需要，可以用方括号将端口列表括起来（旧版软件要求这样做，但现在不再有此要求），如以下示例所示：

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

请注意，**必须**用方括号将否定端口列表括起来，如以下示例所示：

```
![20, 22, 23]
```

另请注意，入侵规则的源或目标端口列表最多可包含 64 个字符。

下表总结了可使用的语法：

表 36-3　　源/目标端口语法

要指定.....	使用	示例
任意端口	`any`	`any`
特定端口	端口号	`80`
端口范围	范围内第一个和最后一个端口号之间使用破折号	`80-443`
所有小于或等于指定端口号的端口	在端口号前面加上破折号	`-21`
所有大于或等于指定端口号的端口	在端口号后面加上破折号	`80-`
除特定端口或端口范围以外的所有端口	在要否定的端口、端口列表或端口范围前面加上 `!` 字符 请注意，从逻辑上讲，可以否定除 *any*（如果它被否定，将表示*无端口*）以外的所有端口名称。	`!20`
端口变量定义的所有端口	前面带有 `$` 的大写字母形式的变量名称 有关详情，请参见第 3-26 页上的使用端口变量。	`$HTTP_PORTS`
除端口变量定义的端口以外的所有端口	前面带有 `!$` 的大写字母形式的变量名称	`!$HTTP_PORTS`

指定方向

许可证：保护

在规则报头中，可以指定数据包接受规则检查必须流经的方向。下表介绍了这些选项。

表 36-4　　规则报头中的方向选项

使用.....	以测试.....
Directional	仅测试从指定源 IP 地址流向指定目标 IP 地址的流量
双向	测试指定的源 IP 地址和目标 IP 地址之间的所有流量

有关使用规则编辑器构建规则报头的步骤的详细信息，请参阅第 36-93 页上的构建规则。

了解规则中的关键字和参数

许可证：保护

借助规则语言，可以通过组合关键字来指定规则行为。关键字及其相关值（亦称为*参数*）规定系统如何评估规则引擎测试的数据包和数据包相关值。 FireSIGHT 系统目前支持允许执行检查功能的关键字，例如内容匹配、协议特定模式匹配和状态特定匹配。在每个关键字中最多可以定义 100 个参数，还可以组合任意数量的兼容关键字来创建非常具体的规则。这有助于降低出现误报和漏报的可能性，使您可以重点关注接收到的入侵信息。

请注意，也可以使用自适应配置文件，以根据规则元数据和主机信息动态调整规则对特定数据包的当前处理方式。有关详细信息，请参阅第 30-1 页上的调整被动部署中的预处理。

有关详细信息，请参阅以下各节：

- 第 36-10 页上的定义入侵事件详细信息介绍可用于定义事件消息、优先级信息以及关于规则检测的漏洞的外部信息参考的关键字的语法及使用。
- 第 36-14 页上的搜索内容匹配介绍如何使用 `content` 或 `protected_content` 关键字测试数据包负载的内容。
- 第 36-16 页上的限制内容匹配介绍如何对 `content` 或 `protected_content` 关键字使用修饰关键字。
- 第 36-27 页上的替换内联部署中的内容介绍如何在内联部署中使用 `replace` 关键字替换同等长度的指定内容。
- 第 36-28 页上的使用 Byte_Jump 和 Byte_Test介绍如何使用 `byte_jump` 和 `byte_test` 关键字计算规则引擎应在数据包中的哪个位置开始测试内容匹配以及应评估哪些字节。
- 第 36-32 页上的使用 PCRE 搜索内容介绍如何使用 `pcre` 关键字在规则中使用兼容 Perl 的正则表达式。
- 第 36-38 页上的向规则添加元数据介绍如何使用 `metadata` 关键字向规则添加信息。
- 第 36-41 页上的检查 IP 报头值介绍用于测试数据包 IP 报头中值的关键字的语法及使用。
- 第 36-44 页上的检查 ICMP 报头值介绍用于测试数据包 ICMP 报头中值的关键字的语法及使用。
- 第 36-45 页上的检查 TCP 报头值和数据流大小介绍用于测试数据包 TCP 报头中值的关键字的语法及使用。
- 第 36-49 页上的启用和禁用 TCP 数据流重组介绍在连接上检测到的流量与规则条件匹配的情况下，如何启用和禁用数据流重组。

- 第 36-50 页上的从会话提取 SSL 信息介绍用于从加密流量中提取版本和状态信息的关键字的使用及语法。
- 第 36-75 页上的将数据包数据读取到关键字参数中介绍如何将数据包中的值读入到某个变量，以便日后在同一规则中使用该变量来指定某些其他关键字中参数的值。
- 第 36-51 页上的检查应用层协议值介绍用于测试应用层协议属性的关键字的使用及语法。
- 第 36-73 页上的检查数据包特征介绍 `dsize`、`sameIP`、`isdataat`、`fragoffset` 和 `cvs` 关键字的使用及语法。
- 第 36-77 页上的使用规则关键字发起活动响应解释如何使用 `resp` 关键字主动关闭 TCP 连接或 UDP 会话，如何使用 `react` 关键字发送 HTML 页面并主动关闭 TCP 连接，以及如何使用 `config response` 命令指定活动响应接口和被动部署中的 TCP 重置尝试次数。
- 第 36-80 页上的过滤事件介绍如何防止规则触发事件 （除非指定数量的数据包在规定时间内满足规则检测条件）。
- 第 36-81 页上的评估攻击后流量介绍如何记录主机或会话的额外流量。
- 第 36-82 页上的检测跨越多个数据包的攻击介绍如何向来自在一个会话中涉及多个数据包的攻击的数据包分配状态名称，然后根据其状态对数据包进行分析和发出警报。
- 第 36-87 页上的生成关于 HTTP 编码类型和位置的事件介绍如何在规范化之前生成有关 HTTP 请求或响应 URI、报头或 cookie （包括 set-cookie）中编码类型的事件。
- 第 36-88 页上的检测文件类型和版本介绍如何使用 `file_type` 或 `file_group` 关键字指向特定文件类型或文件版本。
- 第 36-90 页上的指向特定负载类型介绍如何指向 HTTP 响应实体正文、SMTP 负载或编码邮件附件的开头。
- 第 36-91 页上的指向数据包负载的开头介绍如何指向数据包负载的开头。
- 第 36-92 页上的解码和检查 Base64 数据介绍如何使用 `base64_decode` 和 `base64_data` 关键字解码和检查 Base64 数据 （尤其是在 HTTP 请求中）。

定义入侵事件详细信息

许可证：保护

构建标准文本规则，可以在其中纳入描述规则检测到且容易被利用的漏洞的上下文信息。也可以在其中纳入对漏洞数据库的外部参考，以及定义入侵事件在贵公司中具有的优先级。这样，如果分析师发现入侵事件，他们可随时获取有关优先级、漏洞和已知缓解措施的信息。

有关事件相关关键字的详细信息，请参阅以下各节：

- 第 36-10 页上的定义事件消息
- 第 36-11 页上的定义事件优先级
- 第 36-11 页上的定义入侵事件分类
- 第 36-13 页上的定义事件参考

定义事件消息

许可证：保护

可以指定规则触发时以消息形式显示的有意义的文本。这类消息使您可以即时了解规则检测的漏洞的性质。可以使用除花括号 (`{}`) 以外的所有可打印标准 ASCII 字符。系统将移除将消息完全引起来的引号。

提示　必须指定规则消息。此外，消息不能只包含空白字符、一个或多个引号、一个或多个撇号或者仅由空白字符、引号或撇号组成的任意组合。

要在规则编辑器中定义事件消息，请在 **Message** 字段中输入事件消息。有关使用规则编辑器构建规则的详细信息，请参阅第 36-93 页上的构建规则。

定义事件优先级

许可证：保护

默认情况下，规则的优先级来源于其事件分类。但是，可以通过向规则添加 `priority` 关键字覆盖分类优先级。

要使用规则编辑器指定优先级，请从 **Detection Options** 列表中选择 **priority**，然后选择 **high**、 **medium** 或 **low**。例如，要为检测网络应用攻击的规则分配 **high** 优先级，请向该规则添加 `priority` 关键字，并选择 **high** 作为优先级。有关使用规则编辑器构建规则的详细信息，请参阅第 36-93 页上的构建规则。

定义入侵事件分类

许可证：保护

对于每个规则，可以指定事件数据包显示中出现的攻击分类。下表列出了每种分类的名称和编号。

表 36-5　　规则分类

编号	分类名称	说明
1	not-suspicious	非可疑流量
2	unknown	未知流量
3	bad-unknown	潜在不良流量
4	attempted-recon	尝试信息泄露
5	successful-recon-limited	信息泄露
6	successful-recon-largescale	大规模信息泄露
7	attempted-dos	尝试拒绝服务
8	successful-dos	拒绝服务攻击
9	attempted-user	尝试获取用户权限
10	unsuccessful-user	未成功获取用户权限
11	successful-user	成功获取用户权限
12	attempted-admin	尝试获取管理员权限
13	successful-admin	成功获取管理员权限
14	rpc-portmap-decode	解码 RPC 查询
15	shellcode-detect	检测到可执行代码
16	string-detect	检测到可疑字符串
17	suspicious-filename-detect	检测到可疑文件名
18	suspicious-login	检测到尝试使用可疑用户名的登录

表 36-5　　规则分类 （续）

编号	分类名称	说明
19	system-call-detect	检测到系统调用
20	tcp-connection	检测到 TCP 连接
21	trojan-activity	检测到网络木马
22	unusual-client-port-connection	客户端使用异常端口
23	network-scan	检测网络扫描
24	denial-of-service	检测拒绝服务攻击
25	non-standard-protocol	检测非标准协议或事件
26	protocol-command-decode	通用协议命令解码
27	web-application-activity	访问可能易受攻击的网络应用
28	web-application-attack	网络应用攻击
29	misc-activity	其他活动
30	misc-attack	其他攻击
31	icmp-event	一般 ICMP 事件
32	inappropriate-content	检测到不当内容
33	policy-violation	可能违反公司隐私策略
34	default-login-attempt	尝试使用默认用户名和密码登录
35	sdf	敏感数据
36	malware-cnc	已知恶意软件命令和控制流量
37	client-side-exploit	已知客户端攻击尝试
38	file-format	已知的恶意文件或基于文件的攻击

要在规则编辑器中指定分类，请从 **Classification** 列表中选择分类。有关规则编辑器的详细信息，请参阅第 36-93 页上的编写新规则。

添加自定义分类

许可证：保护

如果想将更多自定义内容用于对所定义的规则生成的事件的数据包显示描述中，可创建自定义分类。

要向 Classification 列表添加分类，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Rule Editor**。

系统将显示 Rule Editor 页面。

步骤 2　点击 **Create Rule**。

系统将显示 Create Rule 页面。

步骤 3　在 **Classification** 下拉列表中点击 **Edit Classifications**。

系统将显示一个弹出窗口。

步骤 4　在 **Classification Name** 字段中键入分类的名称。

最多可以使用 255 个字母数字字符，但如果使用的字符超过 40 个，页面将难以阅读。不支持以下字符：`<>()\'"&$;` 以及空格字符。

步骤 5　在 **Classification Description** 字段中键入对分类的描述。

最多可以使用 255 个字母数字字符和空格。不支持以下字符：`<>()\'"&$;`

步骤 6　从 **Priority** 列表中选择优先级。

可以选择 **high**、 **medium** 或 **low**。

步骤 7　点击**添加**。

新类别将被添加到列表并可在规则编辑器中使用。

步骤 8　点击**完成 (Done)**。

定义事件参考

许可证：保护

可以使用 `reference` 关键字添加对外部网站以及对关于事件的其他信息的参考。添加参考使分析师可以随时获得所需的资源，从而帮助他们确定数据包触发规则的原因。下表列出了一些可提供关于已知漏洞和攻击的数据的外部系统。

表 36-6　　外部攻击识别系统

系统 ID	说明	示例 ID
`bugtraq`	Bugtraq 页面	`8550`
`cve`	通用漏洞与风险页面	`CAN-2003-0702`
`mcafee`	McAfee 页面	`98574`
`url`	网站参考	`www.example.com?exploit=14`
`msb`	Microsoft 安全公告	`MS11-082`
`nessus`	Nessus 页面	`10039`
`secure-url`	安全网站参考 (https://...)	`intranet/exploits/exploit=14` 请注意，可以对任何安全网站使用 `secure-url`。

要使用规则编辑器指定参考，请从 **Detection Options** 列表中选择 **reference**，并在相应字段中输入一个值，如下所示：

`id_system``,`*`id`*

其中，*`id_system`* 是用作前缀的系统，*`id`* 是 Bugtraq ID、CVE 编号、Arachnids ID 或 URL（不包含 `http://`）。

例如，要指定 Microsoft Commerce Server 2002 服务器存在的、Bugtraq ID 为 17134 的身份验证绕过漏洞，请在 **reference** 字段中输入以下内容：

```
bugtraq,17134
```

向规则添加参考时应注意以下几点：

- 逗号后不能有空格。
- 系统 ID 不能是大写字母。

有关使用规则编辑器构建规则的详细信息，请参阅第 36-93 页上的构建规则。

搜索内容匹配

许可证：保护

使用 content 关键字或 protected_content 关键字可以指定要在数据包中检测的内容。有关详细信息，请参阅以下各节：

使用 content 关键字

当使用 content 关键字时，规则引擎在数据包负载或数据流中搜索该字符串。例如，如果您输入 /bin/sh 作为其中一个 content 关键字的值，规则引擎将在数据包负载中搜索字符串 /bin/sh。

可以使用 ASCII 字符串、十六进制内容 （二进制字节代码）或这两者的组合来匹配内容。可以在关键字值中将十六进制内容放在两条竖线 (|) 之间。例如，可以混合使用十六进制内容和 ASCII 内容，例如， |90C8 C0FF FFFF|/bin/sh。

可以在一个规则中指定多项内容匹配。要这样做，请使用 content 关键字的其他实例。对于各项内容匹配，可以指明必须在数据包负载或数据流中发现内容匹配才可触发规则。

使用 protected_content 关键字

protected_content 关键字使您可以在配置规则参数前对搜索内容字符串进行编码。原始规则作者在配置关键字前使用哈希函数 （SHA-512、 SHA-256 或 MD5）对字符串进行编码。

如果使用 protected_content 关键字而不使用 content 关键字，规则引擎在数据包负载或数据流中搜索字符串的方式并不会改变，且大多数关键字选项将起到预期作用。下表总结了 protected_content 关键字选项与 content 关键字选项存在差异的例外情况。

表 36-7　　protected_content 选项例外

选项	说明
Hash Type	protected_content 规则关键字的新增选项。有关详细信息，请参阅第 36-17 页上的 Hash Type。
Case Insensitive	不支持
Within	不支持
深度	不支持
长度	protected_content 规则关键字的新增选项。有关详细信息，请参阅第 36-19 页上的 Length。
Use Fast Pattern Matcher	不支持
Fast Pattern Matcher Only	不支持
Fast Pattern Matcher Offset and Length	不支持

思科建议在包含 protected_content 关键字的规则中至少包含一个 content 关键字，以确保规则引擎使用快速模式匹配程序，从而加快处理速度和提高性能。在规则中， content 关键字应置于 protected_content 关键字之前。请注意，如果规则包含至少一个 content 关键字，无论您是否启用 content 关键字的 Use Fast Pattern Matcher 参数，规则引擎都会使用快速模式匹配程序。

配置内容匹配

大多数情况下，应始终在 content 或 protected_content 关键字后面加上修饰符，指示对内容进行搜索的位置、搜索是否区分大小写及其他选项。有关 content 和 protected_content 关键字的修饰符的详细信息，请参阅限制内容匹配。

请注意，要使规则触发事件，所有内容匹配必须为真，也就是说，每项内容匹配与其他匹配之间都存在 AND 关系。

另请注意，在内联部署中，可以将规则设置为匹配恶意内容并将其更换为您自定义的等长文本字符串。有关详情，请参见第 36-27 页上的替换内联部署中的内容。

要输入待匹配的内容，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 content 字段中输入要查找的内容 （例如，|90C8 C0FF FFFF|/bin/sh）。

如果要搜索**不是**指定内容的任何内容，请选择 **Not** 复选框。

注意事项　如果创建的规则只包含一个 content 关键字，但没有为该关键字选择 **Not** 选项，可能会使入侵策略无效。有关详细信息，请参阅第 36-18 页上的非。

步骤 2　如有需要，可以添加用于修饰 content 关键字的其他关键字，或者为该关键字添加限制条件。有关其他关键字的详细信息，请参阅第 36-9 页上的了解规则中的关键字和参数。

有关限制 content 关键字的详细信息，请参阅第 36-16 页上的限制内容匹配。

步骤 3　继续创建或编辑规则。

有关详细信息，请参阅第 36-93 页上的编写新规则或第 36-95 页上的修改现有规则。

要输入待匹配的受保护内容，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　可使用 SHA-512、SHA-256 或 MD5 哈希生成器对要查找的内容进行编码（例如，通过 SHA-512 哈希生成器运行字符串 Sample1）。

生成器将为该字符串生成哈希。

步骤 2　在 protected_content 字段中，键入在第 1 步中生成的哈希 （例如，B20AABAF59605118593404BD42FE69BD8D6506EE7F1A71CE6BB470B1DF848C814BC5DBEC2081999F15691A71FAECA5FBA4A3F8B8AB56B7F04585DA6D73E5DD15）。

如果要搜索**不是**指定内容的任何内容，请选择 **Not** 复选框。

注意事项　如果创建的规则只包含一个 protected_content 关键字，但没有为该关键字选择 **Not** 选项，可能会使入侵策略无效。有关详细信息，请参阅第 36-18 页上的非。

步骤 3　从 **Hash Type** 下拉列表中选择在第 1 步中使用的哈希函数（例如 **SHA-512**）。请注意，在第 2 步中输入的哈希的位数**必须**与散列类型匹配，否则系统不会保存规则。有关详细信息，请参阅第 36-17 页上的 Hash Type。

提示　如果选择思科设置的**默认值**，系统将假设 SHA-512 为哈希函数。

步骤 4　在必填的 **Length** 字段中键入一个值。该值**必须**与要查找的原始非哈希字符串的长度（例如，步骤 2 中的字符串 `Sample1` 的长度为 `7`）一致。

有关详细信息，请参阅第 36-19 页上的 Length。

步骤 5　在 **Offset** 或 **Distance** 字段中键入一个值。不能在单个关键字配置中同时使用 **Offset** 和 **Distance** 选项。

有关详细信息，请参阅第 36-21 页上的在 protected_content 关键字中使用搜索位置选项。

步骤 6　如有需要，可添加其他限制选项来修饰 `protected_content` 关键字。

有关详细信息，请参阅第 36-16 页上的限制内容匹配。

步骤 7　如有需要，可添加其他关键字来修饰 `protected_content` 关键字。

有关详细信息，请参阅第 36-9 页上的了解规则中的关键字和参数。

步骤 8　继续创建或编辑规则。

有关详细信息，请参阅第 36-93 页上的编写新规则或第 36-95 页上的修改现有规则。

限制内容匹配

许可证：保护

可以通过修饰 `content` 或 `protected_content` 关键字的参数来限制内容搜索的位置以及搜索是否区分大小写。配置用于修饰 `content` 或 `protected_content` 关键字的选项可以指定要搜索的内容。

有关详细信息，请参阅以下各节：

Case Insensitive

许可证：保护

注　配置 `protected_content` 关键字时**不**支持此选项。有关详细信息，请参阅第 36-14 页上的使用 protected_content 关键字。

可以指示规则引擎在搜索 ASCII 字符串内容匹配时忽略大小写。要使搜索不区分大小写，请在指定内容搜索时选择 **Case Insensitive**。

要在进行内容搜索时指定不区分大小写，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　为添加的 `content` 关键字选择 **Case Insensitive**。

步骤 2　继续创建或编辑规则。

有关详细信息，请参阅限制内容匹配、第 36-14 页上的搜索内容匹配、第 36-93 页上的编写新规则或第 36-95 页上的修改现有规则。

Hash Type

许可证：保护

注　此选项**仅**对于 `protected_content` 关键字可配置。有关详细信息，请参阅第 36-14 页上的使用 protected_content 关键字。

使用 **Hash Type** 下拉列表确定用于编码搜索字符串的哈希函数。系统支持对 `protected_content` 搜索字符串进行 SHA-512、 SHA-256 和 MD5 哈希处理。如果哈希内容的长度与所选的哈希类型不匹配，系统将**不**会保存规则。

系统将自动选择思科设置的默认值。如果选择了 **Default**，将不会向规则写入特定哈希函数，且系统将假设 SHA-512 为哈希函数。

要在搜索受保护内容时指定哈希函数，请执行以下操作：

步骤 1　从 **Hash Type** 下拉列表中，选择 **Default**、**SHA-512**、**SHA-256** 或 **MD5** 作为添加的 `protected_content` 关键字的哈希。

提示　如果选择思科设置的**默认值**，系统将假设 SHA-512 为哈希函数。有关详细信息，请参阅第 36-17 页上的 Hash Type。

步骤 2　继续创建或编辑规则。有关详细信息，请参阅限制内容匹配、第 36-14 页上的搜索内容匹配、第 36-93 页上的编写新规则或第 36-95 页上的修改现有规则。

Raw Data

许可证：保护

Raw Data 选项指示规则引擎应在分析规范化负载数据 （由 网络分析策略解码）之前分析原始数据包负载，此选项不使用参数值。进行规范化之前，可以在分析 telnet 流量时使用此关键字在负载中检查 telnet 协商选项。

不能在同一个 `content` 或 `protected_content` 关键字中同时使用 **Raw Data** 选项和任何 HTTP 内容选项。有关详情，请参见第 36-21 页上的 HTTP 内容选项。

提示　可以配置 HTTP 检查预处理器 **Client Flow Depth** 和 **Server Flow Depth** 选项，以确定是否在 HTTP 流量中检查原始数据以及检查的原始数据量。有关详细信息，请参阅第 27-28 页上的选择服务器级别 HTTP 规范化选项。

要分析原始数据，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　为添加的 `content` 或 `protected_content` 关键字选择 **Raw Data** 复选框。

步骤 2　继续创建或编辑规则。有关详细信息，请参阅限制内容匹配、第 36-14 页上的搜索内容匹配、第 36-93 页上的编写新规则或第 36-95 页上的修改现有规则。

非

许可证：保护

选择 **Not** 选项可搜索与指定内容不匹配的内容。如果创建包含已选择 **Not** 选项的 `content` 或 `protected_content` 关键字的规则，还必须在该规则中至少包含另一个未选择 **Not** 选项的 `content` 或 `protected_content` 关键字。

注意事项　请勿创建仅包含一个选择了 Not 选项的 `content` 或 **protected_content** 关键字的规则。否则，可能会使入侵策略无效。

例如， SMTP 规则 1:2541:9 包含三个 `content` 关键字，其中一个选择了 **Not** 选项。如果移除除选择了 **Not** 选项的关键字以外的其他 `content` 关键字，基于该规则的自定义规则将无效。将该规则添加到入侵策略将导致策略失效。

要搜索与指定内容不匹配的内容，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　为添加的 `content` 或 `protected_content` 关键字选择 **Not** 复选框。

提示　不能对同一个 `content` 关键字同时选择 **Not** 复选框和 **Use Fast Pattern Matcher** 复选框。

步骤 2　在规则中至少包含另一个未选择 **Not** 选项的 `content` 或 `protected_content` 关键字。

步骤 3　继续创建或编辑规则。有关详细信息，请参阅限制内容匹配、第 36-14 页上的搜索内容匹配、第 36-93 页上的编写新规则或第 36-95 页上的修改现有规则。

搜索位置选项

许可证：保护

可以使用搜索位置选项指定开始搜索指定内容的位置以及继续搜索的深度。有关每个这些选项的详细信息，请参阅：

- 第 36-19 页上的 Depth
- 第 36-19 页上的 Distance
- 第 36-19 页上的 Length
- 第 36-20 页上的 Offset
- 第 36-20 页上的 Within

关于如何在 `content` 或 `protected_content` 关键字中使用搜索位置选项的信息，请参阅：

- 第 36-20 页上的在 content 关键字中使用搜索位置选项
- 第 36-21 页上的在 protected_content 关键字中使用搜索位置选项

Depth

注 此选项**仅**在配置 `content` 关键字时可用。有关详细信息，请参阅第 36-14 页上的使用 content 关键字。

指定最大内容搜索深度 （以字节为单位），从偏移量值起点开始计算，如果没有配置偏移量，则从数据包负载起点开始计算。

例如，如果规则的内容值为 `cgi-bin/phf`，`offset` 值为 `3`，`depth` 值为 `22`，规则将从字节 3 开始搜索 `cgi-bin/phf` 字符串内容匹配，并在处理完符合规则报头指定参数的数据包中的 22 个字节 （字节 25）后停止。

必须指定一个大于或等于指定内容长度的数值，最多 65535 字节。不能指定值 0。

默认深度是搜索至数据包终点。

Distance

指示规则引擎识别在上一次成功内容匹配后出现指定数量字节的后续内容匹配。

由于偏移量计数器从字节 0 开始计算，因此，应指定比所需字节数小 1 的值，以便从上一次成功内容匹配开始继续搜索。例如，如果指定 4，搜索将从第五个字节开始。

可指定 -65535 到 65535 字节之间的值。如果在 `Distance` 中指定负值，开始搜索的字节可能位于数据包开头以外。所有计算都会将数据包以外的字节考虑在内，尽管搜索实际上从数据包的第一个字节开始。例如，如果数据包当前位置是第五个字节，下一个内容规则选项指定 `Distance` 值为 -10，`Within` 值为 20，搜索将从负载起点开始，且 `Within` 选项将调整为 15。

默认距离是 0，表示继上一次内容匹配之后数据包中的当前位置。

Length

注 此选项**仅**在配置 `protected_content` 关键字时可用。有关详细信息，请参阅第 36-14 页上的使用 protected_content 关键字。

Length `protected_content` 关键字选项表示非哈希搜索字符串的长度 （以字节为单位）。

例如，如果使用了内容 `Sample1` 生成安全哈希，请将 **Length** 值设置为 `7`。**必须**在该字段中输入一个值。

Offset

指定数据包负载中开始内容搜索的位置与数据包负载起点之间的距离 （以字节为单位）。可指定 -65535 到 65535 字节之间的值。

由于偏移量计数器从字节 0 开始计算，因此，应指定比所需字节数小 1 的值，以便从数据包负载起点开始继续搜索。例如，如果指定 7，搜索将从第八个字节开始。

默认偏移量是 0，表示数据包起点。

Within

注 此选项**仅**在配置 `content` 关键字时可用。有关详细信息，请参阅第 36-14 页上的使用 content 关键字。

Within 选项指明，要触发规则，下一次内容匹配必须发生在上一次成功内容匹配结束之后指定数量的字节内。例如，如果将 **Within** 值指定为 `8`，下一次内容匹配必须出现在数据包负载中接下来的八个字节之内，否则将无法满足触发规则的条件。

可以指定一个大于或等于指定内容长度的数值，最多 65535 字节。

Within 的默认设置是搜索至数据包终点。

在 content 关键字中使用搜索位置选项

可以使用两个 `content` 位置对指定开始搜索指定内容的位置以及继续搜索的深度，如下所述：

- 同时使用 **Offset** 和 **Depth** 选项可相对于数据包负载起点进行搜索。
- 同时使用 **Distance** 和 **Within** 可相对于当前搜索位置进行搜索。

如果仅指定选项对中的其中一个选项，系统将会假设另一个选项使用默认值。

不能将 **Offset** 和 **Depth** 选项与 **Distance** 和 **Within** 选项混合使用。例如，不能将 **Offset** 和 **Within** 这两个选项配对。可以在规则中使用任意数量的位置选项。

如果未指定位置，系统将假设 **Offset** 和 **Depth** 选项为默认值；也就是说，将从数据包负载起点开始进行内容搜索，直至数据包终点。

还可以使用现有 `byte_extract` 变量指定位置选项的值。有关详情，请参见第 36-75 页上的将数据包数据读取到关键字参数中。

要通过网络界面在 content 关键字中指定搜索位置值，请执行以下操作：

访问：管理员/入侵管理员

步骤 1 在字段中为添加的 `content` 关键字键入一个值。有以下选项可供选择：

- **Offset**
- **Depth**
- **Distance**
- **Within**

可以在规则中使用任意数量的位置选项。

步骤 2 继续创建或编辑规则。有关详细信息，请参阅第 36-16 页上的限制内容匹配、第 36-14 页上的搜索内容匹配、第 36-93 页上的编写新规则或第 36-95 页上的修改现有规则。

在 protected_content 关键字中使用搜索位置选项

将必填的 **Length** protected_content 选项与 **Offset** 或 **Distance** 位置选项结合使用，可指定开始搜索指定内容的位置以及继续搜索的深度，如下所示：

- 同时使用 **Length** 和 **Offset** 选项可相对于数据包负载起点搜索受保护字符串。
- 同时使用 **Length** 和 **Distance** 选项可相对于当前搜索位置搜索受保护字符串。

提示 不能在单个关键字配置中同时使用 **Offset** 和 **Distance** 选项，但可以在规则内使用任意数量的位置选项。

如果未指定位置，系统将假设使用默认值；也就是说，将从数据包负载起点开始进行内容搜索，直至数据包终点。

还可以使用现有 byte_extract 变量指定位置选项的值。有关详细信息，请参阅第 36-75 页上的将数据包数据读取到关键字参数中。

要通过网络界面在 protected_content 关键字中指定搜索位置值，请执行以下操作：

访问：管理员/入侵管理员

步骤 1 在字段中为添加的 protected_content 关键字键入一个值。有以下选项可供选择：

- **Length** （必填）
- **Offset**
- **Distance**

不能在单个 protected_content 关键字配置中同时使用 **Offset** 和 **Distance** 选项，但可以在规则内使用任意数量的位置选项。

步骤 2 继续创建或编辑规则。有关详细信息，请参阅第 36-16 页上的限制内容匹配、第 36-14 页上的搜索内容匹配、第 36-93 页上的编写新规则或第 36-95 页上的修改现有规则。

HTTP 内容选项

许可证：保护

通过 HTTP content 或 protected_content 关键字选项，可以在 HTTP 检查预处理器解码的 HTTP 消息中指定搜索内容匹配的位置。

以下两个选项搜索 HTTP 响应中的状态字段：

- **HTTP Status Code**
- **HTTP Status Message**

请注意，尽管规则引擎搜索未规范化的原始状态字段，但这里分别列出这些选项，以方便在下文解释将其他原始 HTTP 字段与规范化 HTTP 字段结合使用时应考虑的限制。

以下五个选项搜索 HTTP 请求和/或 HTTP 响应 （视情况而定）中的规范化字段 （有关详细信息，请参阅第 36-21 页上的 HTTP 内容选项）：

- **HTTP URI**
- **HTTP Method**
- **HTTP Header**
- **HTTP Cookie**
- **HTTP Client Body**

以下三个选项搜索 HTTP 请求和/或 HTTP 响应 （视情况而定）中的 （未规范化）原始非状态字段 （有关详细信息，请参阅第 36-21 页上的 HTTP 内容选项）：

- **HTTP Raw URI**
- **HTTP Raw Header**
- **HTTP Raw Cookie**

选择 HTTP `content` 选项时，请遵循以下准则：

- HTTP `content` 选项仅适用于 TCP 流量。
- 为避免对性能造成负面影响，应只选择消息中那些可能出现指定内容的部分。

  例如，如果流量可能包含大型 cookie （例如，购物车消息中的 cookie），可以在 HTTP 报头中搜索指定内容，而不是在 HTTP cookie 中搜索。
- 为了利用 HTTP 检查预处理器规范化以及提高性能，应在创建的任何 HTTP 相关规则中至少包含一个选择了 **HTTP URI**、 **HTTP Method**、 **HTTP Header** 或 HTTP Client Body 选项的 `content` 或 **protected_content** 关键字。
- 不能将 `replace` 关键字与 HTTP `content` 或 `protected_content` 关键字选项配合使用。

可以指定单个规范化 HTTP 选项或状态字段，或者使用规范化 HTTP 选项与状态字段的任意组合，以指向要匹配的内容区域。但在使用 HTTP 字段选项时，请注意以下限制：

- 不能在同一个 `content` 或 `protected_content` 关键字中同时使用 **Raw Data** 选项和任何 HTTP 选项。
- 不能在同一个 `content` 或 `protected_content` 关键字中同时使用原始 HTTP 字段选项 （**HTTP Raw URI**、 **HTTP Raw Header** 或 **HTTP Raw Cookie**）和对应的规范化选项 （分别是 **HTTP URI**、 **HTTP Header** 或 **HTTP Cookie**）。
- 不同同时选择 **Use Fast Pattern Matcher** 和以下一个或多个 HTTP 字段选项：

  HTTP Raw URI、**HTTP Raw Header**、**HTTP Raw Cookie**、**HTTP Cookie**、**HTTP Method**、**HTTP Status Message** 或 **HTTP Status Code**

  但是，可以在使用快速模式匹配程序搜索以下其中一个规范化字段的 `content` 或 `protected_content` 关键字中包含上述选项：

  HTTP URI、 **HTTP Header** 或 **HTTP Client Body**

  例如，如果选择 **HTTP Cookie**、 **HTTP Header** 和 **Use Fast Pattern Matcher**，规则引擎将会在 HTTP cookie 和 HTTP 报头中搜索内容，但快速模式匹配程序仅适用于 HTTP 报头，而不适用于 HTTP cookie。
- 如果将受限选项和不受限选项结合使用，快速模式匹配程序将仅搜索您指定的不受限字段，以测试是否要将规则传递到规则编辑器以完成评估 （包括受限字段的评估）。有关详情，请参见第 36-24 页上的 Use Fast Pattern Matcher。

上述限制反映在下一列表内每个选项的说明中，此列表介绍 HTTP `content` 和 `protected_content` 关键字选项。

HTTP URI

选择此选项将会在规范化的请求 URI 字段中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP URI (U) 选项结合使用来搜索相同的内容。有关详细信息，请参阅特定于 Snort 的后正则表达式修饰符表。

注 管道化 HTTP 请求数据包包含多个 URI。如果选择了 **HTTP URI**，且规则引擎检测到管道化 HTTP 请求数据包，规则引擎将会搜索数据包中的所有 URI 以进行内容匹配。

HTTP Raw URI

选择此选项将会在规范化的请求 URI 字段中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP URI (U) 选项结合使用来搜索相同的内容。有关详细信息，请参阅特定于 Snort 的后正则表达式修饰符表。

注 管道化 HTTP 请求数据包包含多个 URI。如果选择了 **HTTP URI**，且规则引擎检测到管道化 HTTP 请求数据包，规则引擎将会搜索数据包中的所有 URI 以进行内容匹配。

HTTP Method

选择此选项将会在请求方法字段中搜索内容匹配，该字段确定要对 URI 中识别出的资源执行的操作 （例如 GET 和 POST）。

HTTP Header

选择此选项将会在 HTTP 请求内的规范化报头字段 （cookie 除外）中搜索内容匹配；如果 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项已启用，还会在响应中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP 报头 (H) 选项结合使用来搜索相同的内容。有关详细信息，请参阅特定于 Snort 的后正则表达式修饰符表。

HTTP Raw Header

选择此选项将会在 HTTP 请求内的原始报头字段 （cookie 除外）中搜索内容匹配；如果 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项已启用，还会在响应中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP 原始报头 (D) 选项结合使用来搜索相同的内容。有关详细信息，请参阅特定于 Snort 的后正则表达式修饰符表。

HTTP Cookie

选择此选项将会在规范化 HTTP 客户端请求报头内识别出的任何 cookie 中搜索内容匹配；如果 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项已启用，还会在响应 set-cookie 数据中搜索内容匹配。请注意，系统将消息正文中包含的 cookie 看作正文内容。

若要仅对 cookie 进行内容匹配搜索，必须启用 HTTP 检查预处理器的 **Inspect HTTP Cookies** 选项；否则，规则引擎将搜索包括 cookie 在内的整个报头。有关详情，请参见第 27-28 页上的选择服务器级别 HTTP 规范化选项。

请注意：

- 不能将此选项与 `pcre` 关键字 HTTP cookie (C) 选项结合使用来搜索相同的内容。有关详细信息，请参阅特定于 Snort 的后正则表达式修饰符表。
- `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

HTTP Raw Cookie

选择此选项将会在原始 HTTP 客户端请求报头内识别出的任何 cookie 中搜索内容匹配；如果 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项已启用，还会在响应 set-cookie 数据中搜索内容匹配；请注意，系统将消息正文中包含的 cookie 看作正文内容。

若要仅对 cookie 进行内容匹配搜索，必须启用 HTTP 检查预处理器的 **Inspect HTTP Cookies** 选项；否则，规则引擎将搜索包括 cookie 在内的整个报头。有关详情，请参见第 27-28 页上的选择服务器级别 HTTP 规范化选项。

请注意：

- 不能将此选项与 pcre 关键字 HTTP 原始 cookie (K) 选项结合使用来搜索相同的内容。有关详细信息，请参阅特定于 Snort 的后正则表达式修饰符表。
- Cookie: 和 Set-Cookie: 报头名称、标题行中的前导空格以及终止标题行的 CRLF 将作为报头的一部分而非 cookie 的一部分进行检查。

HTTP Client Body

选择此选项将会在 HTTP 客户端请求消息正文中搜索内容匹配。

请注意，要使此选项起作用，必须为 HTTP 检查预处理器的 **HTTP Client Body Extraction Depth** 选项指定一个 0 到 65535 之间的值。有关详情，请参见第 27-28 页上的选择服务器级别 HTTP 规范化选项。

HTTP Status Code

选择此选项将会在 HTTP 响应的三位数状态代码中搜索内容匹配。

要使此选项能够返回匹配，必须启用 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项。有关详情，请参见第 27-28 页上的选择服务器级别 HTTP 规范化选项。

HTTP Status Message

选择此选项将会在 HTTP 响应中状态代码随附的文字描述中搜索内容匹配。

要使此选项能够返回匹配，必须启用 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项。有关详情，请参见第 27-28 页上的选择服务器级别 HTTP 规范化选项。

要在进行 TCP 流量内容搜索时指定 HTTP 选项，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　或者，要利用 HTTP 检查预处理器规范化以及提高性能，请选择：

- 为添加的 content 或 protected_content 关键字至少选择 **HTTP URI**、 **HTTP Raw URI**、 **HTTP Method**、 **HTTP Header**、 **HTTP Raw Header** 或 **HTTP Client Body** 选项之一
- **HTTP Cookie** 或 **HTTP 原始 Cookie** 选项

步骤 2　继续创建或编辑规则。有关详细信息，请参阅第 36-16 页上的限制内容匹配、第 36-14 页上的搜索内容匹配、第 36-93 页上的编写新规则或第 36-95 页上的修改现有规则。

Use Fast Pattern Matcher

许可证：保护

注　配置 protected_content 关键字时，这些选项**不**可用。有关详细信息，请参阅第 36-14 页上的使用 protected_content 关键字。

快速模式匹配程序快速确定在将数据包传递到规则引擎之前要对哪些规则进行评估。这项初步工作可大大减少用于数据包评估的规则数量，从而提高性能。

默认情况下，快速模式匹配程序会在数据包内搜索规则中指定的最长内容；这样可最大程度地消除不必要的规则评估。以如下规则片段为例：

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

几乎所有 HTTP 客户端请求都包含内容 `GET`，但很少会包含 `/exploit.cgi`。使用 `GET` 作为快速模式内容将会导致规则引擎在大多数情况下评估此规则，但极少会产生匹配。但是，对于大多数客户端 `GET` 请求，将不会使用 `/exploit.cgi` 对其进行评估，从而提高性能。

规则引擎仅在快速模式匹配程序检测到指定内容时根据规则评估数据包。例如，如果某个规则中的三个 `content` 关键字分别指定内容 `short`、`longer` 和 `longest`，快速模式匹配程序将使用内容 `longest`，并且仅在规则引擎在负载中找到 `longest` 的情况下对该规则进行评估。

可以使用 **Use Fast Pattern Matcher** 选项为快速模式匹配程序指定较短的搜索模式。理想情况下，指定的模式在数据包中被找到的可能性低于最长模式，因此，因此能够更具体地识别所针对的漏洞。

在同一个 `content` 关键字中选择 **Use Fast Pattern Matcher** 和其他选项时，请注意以下限制：

- 只能为每个规则指定一次 **Use Fast Pattern Matcher**。
- 如果同时选择 **Use Fast Pattern Matcher** 和 **Not**，将不能使用 **Distance**、 **Within**、 **Offset** 和 **Depth**。
- 不同同时选择 Use Fast Pattern Matcher 和以下任何 HTTP 字段选项：

  HTTP Raw URI、**HTTP Raw Header**、**HTTP Raw Cookie**、**HTTP Cookie**、**HTTP Method**、**HTTP Status Message** 或 **HTTP Status Code**

  但是，可以在也使用快速模式匹配程序搜索以下其中一个规范化字段的 `content` 关键字中包含上述选项：

  HTTP URI、 **HTTP Header** 或 **HTTP Client Body**

  例如，如果选择 **HTTP Cookie**、 **HTTP Header** 和 **Use Fast Pattern Matcher**，规则引擎将会在 HTTP cookie 和 HTTP 报头中搜索内容，但快速模式匹配程序仅适用于 HTTP 报头，而不适用于 HTTP cookie。

  请注意，不能在同一个 `content` 关键字中同时使用原始 HTTP 字段选项（**HTTP Raw URI**、 **HTTP Raw Header** 或 **HTTP Raw Cookie**）和对应的规范化选项 （分别是 **HTTP URI**、 **HTTP Header** 或 **HTTP Cookie**）。有关详情，请参见第 36-21 页上的 HTTP 内容选项。

  如果将受限选项和不受限选项结合使用，快速模式匹配程序将仅搜索您指定的不受限字段，以测试是否要将数据包传递到规则引擎以完成评估 （包括受限字段的评估）。

- 或者，如果选择 **Use Fast Pattern Matcher**，还可以选择 **Fast Pattern Matcher Only** 或 **Fast Pattern Matcher Offset and Length** 选项，但不能同时选择这两个选项。
- 检查 Base64 数据时，不能使用快速模式匹配程序；有关详细信息，请参阅第 36-92 页上的解码和检查 Base64 数据。

仅使用快速模式匹配程序

通过 **Fast Pattern Matcher Only**，可以仅将 `content` 关键字作为快速模式匹配程序选项，而不作为规则选项。如果无需规则引擎评估指定的内容，可以使用此选项来节省资源。例如，假设规则仅要求内容 `12345` 位于负载中的任何位置。如果快速模式匹配程序检测到该模式，可根据规则中的其他关键字对数据包进行评估。规则引擎无需重新评估数据包来确定其是否包含模式 `12345`。

如果规则包含其他与指定内容相关的状况，无需使用此选项。例如，如果另一个规则条件尝试确定 `abcd` 是否出现在 `1234` 之前，将无需使用此项选项搜索内容 `1234`。在这种情况下，规则引擎无法确定相对位置，因为选择 **Fast Pattern Matcher Only** 将会指示规则引擎不搜索指定内容。

使用此选项时请注意：

- 指定的内容与位置无关，也就是说，该内容可出现在负载中的任何位置；因此，不能使用位置选项 （**Distance**、 **Within**、 **Offset**、 **Depth** 或 **Fast Pattern Matcher Offset and Length**）。

- 不能将此选项与 **Not** 结合使用。
- 不能将此选项与 **Fast Pattern Matcher Offset and Length** 结合使用。
- 指定的内容将被视为不区分大小写，因为所有模式均以不区分大小写的方式插入到快速模式匹配程序中；系统会自动处理这种情况，因此您无需在选择此选项时选择 **Case Insensitive**。
- 不可在使用 **Fast Pattern Matcher Only** 选项的 `content` 关键字后紧接着使用以下关键字 （这些关键字设置相对于当前搜索位置的搜索位置）：
- `isdataat`
- `pcre`
- `content` （在选择了 **Distance** 或 **Within** 的情况下）
- `content` （在选择了 **HTTP URI** 的情况下）
- `asn1`
- `byte_jump`
- `byte_test`
- `byte_extract`
- `base64_decode`

指定快速模式匹配程序偏移量和长度

使用 **Fast Pattern Matcher Offset and Length** 选项可指定要搜索的部分内容。如果模式很长，且只需模式的一部分即足以识别出可能是匹配的规则，使用此选项可减少内存消耗。如果快速模式匹配程序选择了某个规则，将会根据该规则评估整个模式。

可以确定快速模式匹配程序要使用的部分，方法是，使用以下语法以字节为单位指定搜索的开始位置 （偏移量）以及搜索内容的深入度 （长度）：

```
offset,length
```

例如，对于以下内容：

```
1234567
```

如果如下指定偏移量和长度字节数：

```
1.5
```

快速模式匹配器将仅搜索内容 `23456`。

请注意，不能将此选项与 **Fast Pattern Matcher Only** 结合使用。

要指定快速模式匹配程序要搜索的内容，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　为添加的 `content` 关键字选择 **Use Fast Pattern Matcher**。

步骤 2　或者，选择 **Fast Pattern Matcher Only**，以确定在无规则引擎评估的情况下数据包中是否存在指定模式。

仅在快速模式匹配程序检测到指定内容的情况下，评估才会继续进行。

步骤 3　或者，使用以下语法在 **Fast Pattern Matcher Offset and Length** 选项中指定要在其中搜索内容的部分模式：

```
offset,length
```

其中，*`offset`* 指定从内容开头到搜索开始位置之间的字节数，*`length`* 指定继续搜索的字节数。

步骤 4　继续创建或编辑规则。有关详细信息，请参阅第 36-16 页上的限制内容匹配、第 36-32 页上的使用 PCRE 搜索内容、第 36-93 页上的编写新规则或第 36-95 页上的修改现有规则。

替换内联部署中的内容

许可证：保护

可以在内嵌部署中使用 replace 关键字替换指定内容。

注 **不能**使用 replace 关键字替换思科 SSL 设备检测到的 SSL 流量中的内容。将会传输原始加密数据而非替代数据。有关详细信息，请参阅 《*思科 SSL 设备管理和部署指南*》。

要使用 replace 关键字，请构建一个使用 content 关键字来查找特定字符串的自定义标准文本规则。然后使用 replace 关键字指定一个字符串，以替换该内容。替代值和内容值必须是相同长度的字符串。

注 **不能**使用 replace 关键字替换 protected_content 关键字中的哈希内容。有关详细信息，请参阅第 36-14 页上的使用 protected_content 关键字。

或者，可以用引号将替代字符串引起来，以便向后兼容旧版的 FireSIGHT 系统软件。如果不加引号，替代字符串将被自动添加到规则，以使规则在语法上正确。要将前引号或后引号纳入为替代文本的一部分，必须使用反斜杠对引号进行转义，如以下示例所示：

```
"replacement text plus \"quotation\" marks""
```

每个规则可包含多个 replace 关键字，但只能包含一个 content 关键字。只会替换规则找到的内容中的第一个实例。

下面介绍 replace 关键字的使用示例：

- 如果系统检测到传入数据包包含漏洞，您可以使用一个无害字符串来替换该恶意字符串。有时，这种方法比单纯地丢弃违规数据包更有效。在某些攻击场景中，攻击者只需重新发送被丢弃的数据包，直至该数据包绕过网络防御或对网络造成泛洪攻击。通过将一个字符串替换为另一个字符串 （而非丢弃数据包），可以令攻击者相信其攻击的目标并非易受攻击。
- 如果您担心侦察攻击，这类攻击试图了解是您否正在运行易受攻击版本的设备 （例如，网络服务器），则您可以检测传出数据包，并将横幅替换为自己的文本。

注 请确保在要其中使用替换规则的内联入侵规则中将规则状态设置为 Generate Events；如果将规则设置为 Drop and Generate events，将会导致数据包被丢弃，进而造成无法替换内容。

在字符串替换过程中，该系统会自动更新数据包校验和，以使目标主机可以毫无差错地接收数据包。

请注意，不能将 replace 关键字与 HTTP 请求消息的 content 关键字选项结合使用。有关详细信息，请参阅第 36-14 页上的搜索内容匹配和第 36-21 页上的 HTTP 内容选项。

要在内联部署中替换内容，请执行以下操作：

访问：管理员/入侵管理员

步骤 1 在 Create Rule 页面上，从下拉列表中选择 **content** 并点击 **Add Option**。

系统将显示 content 关键字。

步骤 2 在 **content** 字段中指定要检测的内容，如有需要，还可以选择任何适用参数。请注意，不能将 HTTP 请求消息的 content 关键字选项与 replace 关键字结合使用。

步骤 3　从下拉列表中选择 **replace** 并点击 **Add Option**。

`replace` 关键字将显示在 `content` 关键字下方。

步骤 4　在 **replace:** 字段中为指定内容指定替代字符串。

使用 Byte_Jump 和 Byte_Test

许可证：保护

可以使用 `byte_jump` 和 `byte_test` 来计算规则引擎应在数据包中的哪个位置开始测试数据匹配以及应评估哪些字节。

还可以使用 `byte_jump` 和 `byte_test` **DCE/RPC** 参数来定制 DCE/RPC 预处理器处理的流量的关键字。如果使用 **DCE/RPC** 参数时，还可以将 `byte_jump` 和 `byte_test` 与其他特定 DCE/RPC 关键字一起使用。有关详细信息，请参阅第 27-2 页上的解码 DCE/RPC 流量和第 36-54 页上的 DCE/RPC 关键字。

有关详细信息，请参阅以下各节：

byte_jump

许可证：保护

`byte_jump` 关键字首先计算指定字节段中定义的字节数，然后在数据包中跳过该数量的字节 - 可以从指定字节段的末尾向前跳，也可以从数据包负载起点向前跳，具体取决于指定的选项。这对于具有如下特点的数据包很有用：数据包中的特定字节段描述数据包所包含的变量数据。

下表介绍了 `byte_jump` 关键字所需的参数。

表 36-8　所需的 byte_jump 参数

参数	说明
字节	从数据包进行计算的字节数。
Offset	从负载开头到开始进行处理之间的字节数。偏移量计数器从字节 0 开始计数，因此，应该如下计算 `offset` 值：用从数据包负载起点或上一次成功内容匹配起向前跳所需的字节数减去 1。 还可以使用现有 `byte_extract` 变量指定此参数的值。有关详情，请参见第 36-75 页上的将数据包数据读取到关键字参数中。

下表介绍了可用于定义系统如何解释您为必需参数指定的值的选项。

表 36-9　其他可选 byte_jump 参数

参数	说明
Relative	使偏移量相对于上一次成功内容匹配中找到的上一个模式。
调整	将转换的字节数四舍五入为下一个 32 位边界。

表 36-9　其他可选 byte_jump 参数 （续）

参数	说明
倍数	指示规则引擎应将其与从数据包得到的 byte_jump 值相乘的值，以获得最终的 byte_jump 值。 也就是说，规则引擎跳过一个与您通过 Multiplier 参数指定的整数相乘的字节数，而不是跳过指定字节段中定义的字节数。
Post Jump Offset	应用其他 byte_jump 参数后要向前跳或向后跳的字节数 （-63535 到 63535）。选择正值将会向前跳，选择负值将会向后跳。将此字段留空或输入 0 将会禁用此字段。 有关选择 **DCE/RPC** 参数后不适用的 byte_jump 参数，请参阅字节顺序参数表中的 **DCE/RPC** 参数。
From Beginning	指明规则引擎应从数据包负载起点跳过负载中指定的字节数，而不是从指定要跳过的字节数的字节段末尾跳过。

只能指定 **DCE/RPC**、 **Endian** 或 **Number Type**。

如果要定义 byte_jump 关键字如何计算字节，可以从下表所述的参数中进行选择 （如果没有指定参数，将使用网络字节顺序）。

表 36-10　字节顺序参数

参数	说明
Big Endian	按大端字节顺序处理数据 （大端字节顺序是默认的网络字节顺序）。
Little Endian	按小端字节顺序处理数据
DCE/RPC	指定 DCE/RPC 预处理器处理的流量的 byte_jump 关键字。有关详情，请参见第 27-2 页上的解码 DCE/RPC 流量。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序， **Number Type**、**Endian** 和 **From Beginning** 参数不适用。 如果启用此参数，还可以将 byte_jump 与其他特定 DCE/RPC 关键字结合使用。有关详情，请参见第 36-54 页上的 DCE/RPC 关键字。

可以使用下表所列的其中一个参数来定义系统如何在数据包中查看字符串。

表 36-11　数字类型参数

参数	说明
Hexadecimal String	使用十六进制格式表示转换的字符串数据。
Decimal String	使用十进制格式表示转换的字符串数据。
Octal String	使用八进制格式表示转换的字符串数据。

例如，如果如下设置 byte_jump 的值：

- Bytes = 4
- Offset = 12
- Relative 已启用
- Align 已启用

规则引擎将会计算自上一次成功内容匹配后显示的 13 个字节当中 4 个字节中描述的数量，并向前跳过数据包中该数量的字节。例如，如果特定数据包中计算出的 4 个字节是 `00 00 00 1F`，规则引擎会将它转换为 31。由于指定了 `align`（指示引擎移到下一个 32 位边界），因此，规则引擎将在数据包中向前跳过 32 个字节。

或者，如果如下设置 `byte_jump` 的值：

- Bytes = 4
- Offset = 12
- From Beginning 已启用
- Multiplier = 2

规则引擎将会计算在数据包起点后显示的 13 个字节当中 4 个字节中描述的数值。然后，引擎会将该数值乘以 2，以获得将要跳过的字节总数。例如，如果特定数据包中计算出的 4 个字节是 `00 00 00 1F`，规则引擎会将它转换为 31，然后再乘以 2 以得到 62。由于启用了 From Beginning，因此，规则引擎会跳过数据包中的前 63 个字节。

要使用 byte_jump，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　从下拉列表中选择 `byte_jump` 并点击 **Add Option**。

byte_jump 部分将显示在上次选择的关键字下方。

byte_test

许可证：保护

`byte_test` 关键字会计算指定字节段中的字节数，并将计算出的字节数与您指定的运算符和值作比较。

下表介绍了 `byte_test` 关键字所需的参数。

表 36-12　所需的 byte_test 参数

参数	说明
字节	从数据包进行计算的字节数。可指定 1 到 10 字节。
Operator and Value	将指定值与 <、 >、 =,、 !、 &、 ^、 !>、 !<、 !=、 !& 或 !^ 作比较。 例如，如果指定 `!1024`，`byte_test` 将会转换该指定数字，且如果该数字不等于 1024，则会生成事件 （如果其他所有关键字参数都匹配）。 请注意，! 和 != 是等效的。 还可以使用现有 `byte_extract` 变量指定此参数的值。有关详情，请参见第 36-75 页上的将数据包数据读取到关键字参数中。
Offset	从负载开头到开始进行处理之间的字节数。偏移量计数器从字节 0 开始计数，因此，应该如下计算 `offset` 值：用从数据包负载起点或上一次成功内容匹配起向前计算所需的字节数减去 1。 还可以使用现有 `byte_extract` 变量指定此参数的值。有关详情，请参见第 36-75 页上的将数据包数据读取到关键字参数中。

可以用下表中所述的参数进一步定义系统如何使用 byte_test 参数。

表 36-13　其他可选 byte_test 参数

参数	说明
Relative	使偏移量相对于上一次成功模式匹配。
调整	将转换的字节数四舍五入为下一个 32 位边界。

只能指定 **DCE/RPC**、 **Endian** 或 **Number Type**。

要定义 byte_test 关键字如何计算其测试的字节，请从下表中选择参数。如果未指定参数，将使用网络字节顺序。

表 36-14　字节顺序 byte_test 参数

参数	说明
Big Endian	按大端字节顺序处理数据 （大端字节顺序是默认的网络字节顺序）。
Little Endian	按小端字节顺序处理数据
DCE/RPC	指定 DCE/RPC 预处理器处理的流量的 byte_test 关键字。有关详情，请参见第 27-2 页上的解码 DCE/RPC 流量。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序， **Number Type** 和 **Endian** 参数不适用。 如果启用此参数，还可以将 byte_test 与其他特定 DCE/RPC 关键字结合使用。有关详情，请参见第 36-54 页上的 DCE/RPC 关键字。

可以使用下表所列的其中一个参数来定义系统如何在数据包中查看字符串。

表 36-15　数字类型 byte-test 参数

参数	说明
Hexadecimal String	使用十六进制格式表示转换的字符串数据。
Decimal String	使用十进制格式表示转换的字符串数据。
Octal String	使用八进制格式表示转换的字符串数据。

例如，如果如下指定 byte_test 的值：

- Bytes = 4
- Operator and Value > 128
- Offset = 8
- Relative 已启用

规则引擎会计算自 （相对于）上一次成功内容匹配后显示的 9 个字节当中 4 个字节中描述的数值，如果计算出的数值大于 128 字节，将触发规则。

要使用 byte_test，请执行以下操作：

访问：管理员/入侵管理员

步骤 1 在 Create Rule 页面上，从下拉列表中选择 `byte_test` 并点击 **Add Option**。

`byte_test` 部分将显示在上次选择的关键字下方。

使用 PCRE 搜索内容

许可证：保护

`pcre` 关键字使您可以使用兼容 Perl 的正则表达式 (PCRE) 为指定的内容检查数据包负载。使用 PCRE 可避免编写以匹配相同内容的细微变化为目的的多个规则。

搜索可以多种方式显示的内容时，正则表达式很有用。内容可能有不同的属性；在尝试从数据包负载中查找内容时，您会需要考虑其属性。

请注意，入侵规则使用的正则表达式语法是完整正则表达式库的一个子集，并该库中所用命令的语法在某些方面存在不同之处。使用规则编辑器添加 `pcre` 关键字时，请按以下格式键入完整的值：

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

其中：

- !是可选的否定式 （如果想匹配不匹配的正则表达式的模式，请使用此否定式）。
- */pcre/*是一个兼容 Perl 的正则表达式。
- `ismxAEGRBUIPHDMCKSY` 是修饰符选项的任意组合。

另请注意，在 PCRE 中使用下表所列字符在数据包负载中搜索特定内容时，必须对这些字符进行转义，以使规则引擎能正确地解释这些字符。

表 36-16　　转义 PCRE 字符

必须转义的字符	使用反斜杠.....	或使用十六进制代码.....
# （哈希标记）	\#	\x23
; （分号）	\;	\x3B
| （竖线）	\\|	\x7C
: （冒号）	\:	\x3A

提示 或者，可以用引号将兼容 Perl 的正则表达式引起来，例如，*pcre_expression* 或 *"pcre_expression"*。这一做法适合习惯使用旧版本的有经验的用户 （旧版本要求必须用引号将正则表达式引起来）。规则在保存后再显示时，规则编辑器不会显示引号。

还可以使用 `m?regex?`，其中，`?`是除 / 以外的分隔符。如果需要在正则表达式中匹配一个正斜杠，但不想用一个反斜杠来进行转义，可能需要使用此分隔符。例如，可以使用 `m?`*regex*`?ismxAEGRBUIPHDMCKSY`，其中 *regex* 是兼容 Perl 的正则表达式，`ismxAEGRBUIPHDMCKSY` 是修饰符选项的任意组合。有关正则表达式语法的详细信息，请参阅第 36-33 页上的有关兼容 Perl 的正则表达式的基础知识。

以下各节提供了有关为 pcre 关键字构建有效值的详细信息：

- 第 36-33 页上的有关兼容 Perl 的正则表达式的基础知识介绍用于兼容 Perl 的正则表达式中的常见语法。
- 第 36-34 页上的 PCRE 修饰符选项介绍可用于修改正则表达式的选项。
- 第 36-36 页上的 PCRE 关键字值示例提供了 pcre 关键字在规则中的使用示例。

有关兼容 Perl 的正则表达式的基础知识

许可证：保护

pcre 关键字接受兼容 Perl 的正则表达式 (PCRE) 标准语法。以下各节介绍这种语法。

提示 本节介绍了可用于 PCRE 的基本语法，如果您需要更高级的信息，可参阅专门关于 Perl 和 PCRE 的网上参考资料或书籍。

元字符

许可证：保护

元字符是在正则表达式中具有特殊含义的原义字符。在正则表达式中使用元字符时，必须通过在元字符前添加一个反斜杠来对其进行“转义”。

下表举例说明可用于 PCRE 的元字符。

表 36-17　PCRE 元字符

元字符	说明	示例
.	匹配除换行符以外的任何字符。如果将 s 用作修饰选项，还将匹配换行符。	abc.匹配 abcd、 abc1、 abc# 等等。
*	匹配字符或表达式的零次或多次出现次数。	abc* 匹配 abc、 abcc、 abccc、 abccccc 等等。
?	匹配字符或表达式的零次或一次出现次数。	abc?匹配 abc。
+	匹配字符或表达式的一次或多次出现次数。	abc+ 匹配 abc、 abcc、 abccc、 abccccc 等等。
()	组表达。	(abc)+ 匹配 abc、 abcabc、 abcabcabc 等等。
{}	为字符或表达式指定匹配项数限制。如果要设置下限和上限，请用逗号将下限和上限隔开。	a{4,6} 匹配 aaaa、 aaaaa 或 aaaaaa。 (ab){2} 匹配 abab。
[]	允许定义字符类，并匹配字符集中包含的任意字符或字符组合。	[abc123] 匹配 a、 b 或 c 等等。
^	匹配字符串开头的内容。如果在字符类中使用，也可用于否定。	^in 匹配 info 中的“in”，但不匹配 bin 中的“in”。 [^a] 匹配不包含 a 的任何内容。
美元	匹配字符串结尾的内容。	ce$ 匹配 announce 中的“ce”，但不匹配 cent 中的“ce”。
|	指示 OR 表达式。	(MAILTO|HELP) 匹配 MAILTO 或 HELP。
\	元字符可用作实际字符，还可用于指定预定义的字符类。	\.匹配句号， * 匹配星号， \\ 匹配反斜线，依此类推。 \d 匹配数字字符， \w 匹配字母数字字符，依此类推。有关 PCRE 中使用的字符类的详细信息，请参阅第 36-34 页上的字符类。

字符类

许可证：保护

字符类包括字母字符、数字字符、字母数字字符和空白字符。可以用方括号 （参阅第 36-33 页上的元字符）创建自己的字符类，也可以使用预定义类作为不同字符类型的快捷方式。如果不与其他限定符配合使用，一个字符类通常匹配一个数字或字符。

下表举例说明 PCRE 接受的预定义字符类。

表 36-18　PCRE 字符类

字符类	说明	字符类定义
\d	匹配数字字符 （“数字”）。	[0-9]
\D	对应不是数字字符的任何字符。	[^0-9]
\w	匹配字母数字字符 （“单词”）。	[a-zA-Z0-9_]
\W	匹配不是字母数字字符的任何字符。	[^a-zA-Z0-9_]
\s	匹配空白字符，包括空格、回车符、制表符、换行符和换页符。	[\r\t\n\f]
\S	匹配不是空白字符的任何字符。	[^ \r\t\n\f]

PCRE 修饰符选项

许可证：保护

指定 `pcre` 关键字值中的正则表达式语法后，可以使用修饰选项。这些修饰符执行特定于 Perl、PCRE 和Snort 的处理功能。修饰符始终按以下格式显示在 PCRE 值的末尾：

`/pcre/ismxAEGRBUIPHDMCKSY`

其中， `ismxAEGRBUPHMC` 可以包括下表中的任何修饰选项。

提示　或者，可以用引号将正则表达式和任何修饰选项引起来，例如， `"/pcre/ismxAEGRBUIPHDMCKSY"`。这一做法适合习惯使用旧版本的有经验的用户 （旧版本要求必须用引号将正则表达式引起来）。规则在保存后再显示时，规则编辑器不会显示引号。

下表介绍了可用于执行 Perl 处理功能的选项。

表 36-19　Perl 相关的后正则表达式选项

选项	说明
i	使正则表达式不区分大小写。
s	点字符 (.) 匹配除换行符和 `\n` 字符以外的所有字符。可使用 `"s"` 选项覆盖此选项，这样，点字符将匹配所有字符 （包括换行符）。
m	默认情况下，一个字符串被视为单行字符，`^` 和 `$` 分别匹配特定字符串的开头和结尾。如果使用 `"m"` 代替选项， `^` 和 `$` 将匹配紧接在缓冲区内所有换行符之前或之后的内容，以及位于缓冲区开头或结尾的内容。
x	忽略可能在这一模式中出现的空白数据字符，除非其为转义字符 （前面加有反斜杠）或包含在字符类中。

下表介绍了可用于正则表达式后的 PCRE 修饰符。

表 36-20　PCRE 相关的后正则表达式选项

选项	说明
A	模式必须在字符串开头进行匹配 （与在正则表达式中使用 ^ 具有相同的效果）。
E	将 $ 设置为只在目标字符串结尾进行匹配。（如果最后一个字符是换行符，即使没有E， $ 也会匹配紧接在该字符之前的内容，但不会匹配任何其他换行符之前的内容）。
G	默认情况下， * + 和 ?是“贪婪”的，这意味着，如果找到两个或更多匹配项，将会选择最长的匹配项。使用 G 字符可使这些字符在后面无问号字符 (?)的情况下总是选择第一个匹配项。例如，在使用 G 修饰符的构造中，*?+?和 ?? 将是贪婪字符，*、+ 或 ? 在不附带问号的情况下将是非贪婪字符。

下表介绍了可用于正则表达式后的 Snort 特定修饰符。

表 36-21　特定于 Snort 的后正则表达式修饰符

选项	说明
R	相对于规则引擎上一次找到的匹配项的结尾搜索匹配的内容。
B	在未被预处理器解码的数据中搜索内容 （此选项类似于将 Raw Data 参数与 content 或 protected_content 关键字配合使用）。
你	在已由 HTTP 检查预处理器解码的规范化 HTTP 请求消息的 URI 中搜索内容。请注意，不能将此选项与 content 或 protected_content 关键字 **HTTP URI** 选项结合使用来搜索相同的内容。有关详情，请参见第 36-21 页上的 HTTP 内容选项。 **注**　管道化 HTTP 请求数据包包含多个 URI。包含 U 选项的 PCRE 表达式使规则引擎仅在管道化 HTTP 请求数据包的第一个 URI 中搜索内容匹配。要搜索数据包中的所有 URI，请将 content 或 protected_content 关键字与选定的 **HTTP URI** 配合使用 （可配合或不配合随附的使用 U 选项的 PCRE 表达式）。
I	在已由 HTTP 检查预处理器解码的原始 HTTP 请求消息的 URI 中搜索内容。请注意，不能将此选项与 content 或 protected_content 关键字 **HTTP Raw URI** 选项结合使用来搜索相同的内容。有关详情，请参见第 36-21 页上的 HTTP 内容选项。
P	在已由 HTTP 检查预处理器解码的规范化 HTTP 请求消息的正文中搜索内容。有关详细信息，请参阅第 36-21 页上的 HTTP 内容选项中的 content 和 protected_content 关键字 **HTTP Client Body** 选项。
H	在已由 HTTP 检查预处理器解码的 HTTP 请求或响应消息的报头 （不包括 cookie）中搜索内容。请注意，不能将此选项与 content 或 protected_content 关键字 **HTTP Header** 选项结合使用来搜索相同的内容。有关详情，请参见第 36-21 页上的 HTTP 内容选项。
D	在已由 HTTP 检查预处理器解码的原始 HTTP 请求或响应消息的报头 （不包括 cookie）中搜索内容。请注意，不能将此选项与 content 或 protected_content 关键字 **HTTP Raw Header** 选项结合使用来搜索相同的内容。有关详情，请参见第 36-21 页上的 HTTP 内容选项。
M	在已由 HTTP 检查预处理器解码的规范化 HTTP 请求消息的方法字段中搜索内容；该方法字段确定要对 URI 中识别出的资源执行的操作 （例如， GET、 PUT、 CONNECT 等）。有关详细信息，请参阅第 36-21 页上的 HTTP 内容选项中的 content 和 protected_content 关键字 **HTTP Method** 选项。

表 36-21　特定于 Snort 的后正则表达式修饰符 （续）

选项	说明
C	如果 HTTP 检查预处理器的 **Inspect HTTP Cookies** 选项已启用，将会在 HTTP 请求报头的任何 cookie 中搜索规范化内容；如果该预处理器的 **Inspect HTTP Responses** 选项已启用，还会在 HTTP 响应报头的任何 set-cookie 中搜索规范化内容。如果未启用 **Inspect HTTP Cookies** 选项，将会搜索包括 cookie 或 set-cookie 数据在内的整个报头。 请注意： • 消息正文中包含的 cookie 将被视为正文内容。 • 不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP Cookie** 选项结合使用来搜索相同的内容。有关详情，请参见第 36-21 页上的 HTTP 内容选项。 • `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。
K	如果 HTTP 检查预处理器的 **Inspect HTTP Cookies** 选项已启用，将会在 HTTP 请求报头的任何 cookie 中搜索原始内容；如果该预处理器的 **Inspect HTTP Responses** 选项已启用，还会在 HTTP 响应报头的任何 set-cookie 中搜索原始内容。如果未启用 **Inspect HTTP Cookies** 选项，将会搜索包括 cookie 或 set-cookie 数据在内的整个报头。 请注意： • 消息正文中包含的 cookie 将被视为正文内容。 • 不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP Raw Cookie** 选项结合使用来搜索相同的内容。有关详情，请参见第 36-21 页上的 HTTP 内容选项。 • `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。
S	搜索 HTTP 响应中的三位数状态代码。有关详细信息，请参阅第 36-21 页上的 HTTP 内容选项中的 `content` 和 `protected_content` 关键字 **HTTP Status Code** 选项。
有	搜索 HTTP 响应中状态代码随附的文字描述。有关详细信息，请参阅第 36-21 页上的 HTTP 内容选项中的 `content` 和 `protected_content` 关键字 **HTTP Status Message** 选项。

注　请勿将 U 选项与 R 选项结合使用，否则可能会导致性能问题。此外，请勿将 U 选项与任何其他 HTTP 内容选项 （I、 P、 H、 D、 M、 C、 K、 S 或 Y）结合使用。

PCRE 关键字值示例

许可证：保护

以下示例显示可为 `pcre` 输入的值，并说明每个示例将会匹配的内容。

- **`/feedback[(\d{0,1})]?\.cgi/U`**

  此示例搜索 `feedback` 的数据包负载， feedback 后面紧跟着零个或一个数字字符，再紧跟着 `.cgi`，且仅在 URI 数据中进行搜索。

  此示例将匹配：

- `feedback.cgi`
- `feedback1.cgi`
- `feedback2.cgi`
- `feedback3.cgi`

此示例不匹配：

- `feedbacka.cgi`
- `feedback11.cgi`
- `feedback21.cgi`
- `feedbackzb.cgi`
- **`/^ez(\w{3,5})\.cgi/iU`**

  此示例在字符串开头搜索 `ez` 的数据包负载，ez 后面跟有一个包含 3 到 5 个字母的单词，该单词后面跟着 `.cgi`。此搜索不区分大小写，且仅搜索 URI 数据。

  此示例将匹配：

- `EZBoard.cgi`
- `ezman.cgi`
- `ezadmin.cgi`
- `EZAdmin.cgi`

  此示例不匹配：

- `ezez.cgi`
- `fez.cgi`
- `abcezboard.cgi`
- `ezboardman.cgi`
- **`/mail(file|seek)\.cgi/U`**

  此示例在 URI 数据中搜索后面跟有 `file` 或 `seek` 的 `mail` 的数据包负载。

  此示例将匹配：

- `mailfile.cgi`
- `mailseek.cgi`

  此示例不匹配：

- `MailFile.cgi`
- `mailfilefile.cgi`
- **`m?http\\x3a\x2f\x2f.*(\n|\t)+?U`**

  此示例跟在任意数量字符后面的 HTTP 请求中为制表符或换行符搜索 URI 内容的数据包负载。此示例使用 `m?`*`regex`*`?`来避免在表达式中使用 `http\:\/\/`。请注意，冒号前面有一个反斜杠。

  此示例将匹配：

- `http://www.example.com?scriptvar=x&othervar=\n\..\..`
- `http://www.example.com?scriptvar=\t`

  此示例不匹配：

- `ftp://ftp.example.com?scriptvar=&othervar=\n\..\..`
- `http://www.example.com?scriptvar=|/bin/sh -i|`
- **`m?http\\x3a\x2f\x2f.*=\|.*\|+?sU`**

  此示例为带有任意数量字符 （包括换行符）的 URL 搜索数据包负载，后面跟有一个等号以及包含任意数量字符或空白字符的竖线。此示例使用 `m?`*`regex`*`?`来避免在表达式中使用 `http\:\/\/`。

  此示例将匹配：

- `http://www.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?input=|cat /etc/passwd|`

此示例不匹配：

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- **`/[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}/i`**

  此示例为任何 MAC 地址搜索数据包负载。请注意，此示例使用反斜杠对冒号进行转义。

向规则添加元数据

许可证：保护

可以使用 `metadata` 关键字向规则添加描述性信息。可以根据自身需求使用添加的信息来整理或识别规则以及搜索规则。

系统按以下格式验证元数据：

`key value`

其中，*`key`* 和 *`value`* 提供以空格分隔的组合描述。这是思科 VRT 用于向思科提供的规则添加元数据的格式。

也可以使用其他格式：

`key=value`

例如，借助 *`key value`* 格式，可以使用一个类别和子类别按作者和日期识别规则，如下所示：

```
author SnortGuru_20050406
```

可以在一个规则中使用多个 `metadata` 关键字。还可以使用逗号在一个 `metadata` 关键字中隔开多个 *`key value`* 语句，如以下示例所示：

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003, revised_by
SnortUser1_20070123
```

并非只能使用 *`key value`* 或 *`key=value`* 格式；但是，应了解根据这两种格式进行验证引起的局限性。

避免受限字符

许可证：保护

请注意以下字符限制：

- 请勿在 `metadata` 关键字中使用分号 (;) 和冒号 (:)。
- 请注意，如果使用逗号，系统会将逗号视为多个 *`key value`* 或 *`key=value`* 语句的分隔符。例如：

  ```
  key value, key value, key value
  ```

- 请注意，如果使用等号 (=) 字符或空格字符，系会将这些字符视为 *`key`* 和 *`value`* 之间的分隔符。例如：

  ```
  key value
  key=value
  ```

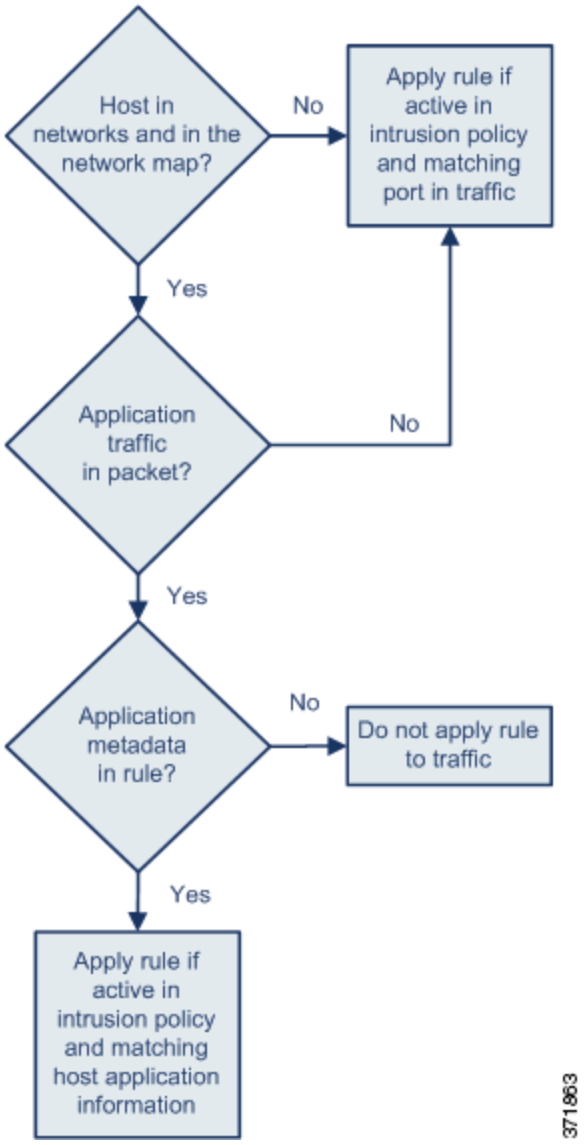
允许使用所有其他字。

添加 service 元数据

许可证：保护

规则引擎应用具有与数据包中用于主机的应用协议信息匹配的 `service` 元数据的活动规则来分析和处理流量。如果不匹配，系统不会将规则应用于流量 如果主机没有应用协议信息，或者规则没有 `service` 元数据，系统会对照规则中的端口检查流量中的端口，以确定是否将规则应用于流量。

下图说明根据应用信息来匹配规则和流量：



要将规则与确定的应用协议进行匹配，必须定义 `metadata` 关键字和 *`key value`* 语句，在其中，`service` 应作为 *`key`*，并指定 *`value`* 的应用。例如，`metadata` 关键字中的以下 *`key value`* 语句将规则与 HTTP 流量关联：

```
service http
```

下表介绍了最常用的应用值。

注　如需有关定义表中未列出的应用方面的帮助，请联系支持部门。

表 36-22　服务值

价值	说明
dcerpc	分布式计算环境/远程过程调用系统
dns	域名系统
finger	Finger 用户信息协议
ftp	文件传输协议
ftp-data	文件传输协议 （数据通道）
http	超文本传输协议
imap	互联网消息访问协议
isakmp	互联网安全关联和密钥管理协议
netbios-dgm	NetBIOS 数据报服务
NetBIOS-ns	NetBIOS 名称服务
NetBIOS-ssn	NetBios 会话服务
nntp	网络新闻传输协议
oracle	Oracle 网络服务
pop2	邮局协议第 2 版
POP3	邮局协议第 3 版
smtp	简单邮件传输协议
ssh	安全外壳网络协议
telnet	Telnet 网络协议
tftp	简单文件传输协议
x11	X Window 系统

避免使用保留的元数据

许可证：保护

应避免在 `metadata` 关键字使用以下词语，无论是作为单个参数还是作为 *`key value`* 语句中的关键字；这些词语被保留供 VRT 使用：

```
应用
引擎
impact_flag
操作系统
策略
rule-type
rule-flushing
soid
```

注　如需有关将受限元数据添加到可能不具有预期作用的本地规则方面的帮助，请联系支持部门。有关详情，请参见第 66-17 页上的导入本地规则文件。

搜索带有元数据的规则

许可证：保护

要搜索使用 metadata 关键字的规则，请在规则搜索页面上选择 metadata 关键字，或者键入元数据的任何部分。例如，可以键入：

- author，以显示在其中对 *key* 使用了 author 的所有规则。
- author snortguru，以显示在其中对 *key* 使用了 author 并对 *value* 使用了 SnortGuru 的所有规则。
- author s，以显示在其中为 *key* 使用了 author关键字并对 *value* 使用了任何词条 （例如 SnortGuru、 SnortUser1 或 SnortUser2）的所有规则。

提示 如果同时搜索 *key* 和 *value*，应在搜索中使用与规则的 *key value* 声明中使用的相同连接符（等号 [=] 或空格字符）；搜索将返回不同的结果，具体取决于 *key* 后面跟的是等号 (=) 还是空格字符。

请注意，无论使用何种格式添加元数据，系统都会将元数据搜索词解释为 *key value* 或 *key=value* 语句的全部或一部分。例如，以下是没有遵循 *key value* 或 *key=value* 格式的有效元数据：

```
ab cd ef gh
```

但是，系统会将此示例中的每个空格解释为关键字和值之间的分隔符。因此，对于并列和单个术语，可以使用以下任何搜索成功查找到包含示例元数据的规则：

```
cd ef
ef gh
ef
```

但是，使用以下搜索不能找到该规则 （在该搜索中，系统将会作为单个 *key value* 语句进行解释）：

```
ab ef
```

有关详细信息，请参阅第 36-98 页上的搜索规则。

设置影响级别 1

许可证：保护

可以在 metadata 关键字中使用以下保留的 *key value* 声明：

```
impact_flag red
```

此 *key value* 声明会将您导入的本地规则或您使用规则编辑器创建的自定义规则的影响标志设置为红色 （级别 1）。

请注意，当 VRT 在思科提供的某个规则中包含 impact_flag red 语句时，VRT 已经确定触发该规则的数据包指示源主机或目标主机可能已被病毒、特洛伊木马或其他恶意软件感染。有关详细信息，请参阅第 41-32 页上的使用影响级别评估事件。

检查 IP 报头值

许可证：保护

可以使用关键字来识别数据包 IP 报头中可能存在的攻击或安全策略违规。有关详细信息，请参阅以下各节：

- 第 36-42 页上的检查分片和保留位
- 第 36-42 页上的检查 IP 报头标别值
- 第 36-42 页上的识别指定的 IP 选项
- 第 36-43 页上的识别指定的 IP 协议号
- 第 36-43 页上的检查数据包的服务类型
- 第 36-43 页上的检查数据包的生存时间值

检查分片和保留位

许可证：保护

`fragbits` 关键字检查 IP 报头中的分片和保留位。可以检查每个数据包的 Reserved 位、 More Fragments位和 Don't Fragment 位的任意组合。

表 36-23　Fragbits 参数值

参数	说明
R	Reserved 位
M	More Fragments 位
D	Don’t Fragment 位

为进一步改进使用 `fragbits` 关键字的规则，可以在规则的参数值后指定下表中所述的任何运算符。

表 36-24　Fragbit 运算符

运算符	说明
加号 (`+`)	数据包必须匹配所有指定的位。
星号 (`*`)	数据包可以匹配任何指定的位。
感叹号 (`!`)	如果未设置任何指定的位，数据包将符合条件。

例如，要生成有关设置了 Reserved 位 （还可能设置了任何其他位）的数据包的事件，请使用 `R+` 作为 `fragbits` 值。

检查 IP 报头标别值

许可证：保护

`id` 关键字根据您在此关键字的参数中指定的值测试 IP 报头分片标别字段。某些拒绝服务工具和扫描仪将此字段设置为容易检测的特定数字。例如，在 SID630（检测 Synscan 端口扫描）中，`id` 设置为 `39426`，这是在扫描仪传输的数据包中用作 ID 号的静态值。

注　`id` 参数值必须为数字。

识别指定的 IP 选项

许可证：保护

使用 `IPopts` 关键字可在数据包中搜索指定的 IP 报头选项。下表列出了可用的参数值。

表 36-25　IPoption 参数

参数	说明
rr	记录路由
eol	列表结束
nop	无操作

表 36-25　IPoption 参数 （续）

参数	说明
ts	时间戳
秒	IP 安全选项
lsrr	松散源路由
ssrr	严格源路由
satid	数据流标识符

分析师最经常监视严格和松散源路由，因为这两个选项可能指出欺骗性源 IP 地址。

识别指定的 IP 协议号

许可证：保护

使用 `ip_proto` 关键字可识别使用指定为关键字值的 IP 协议的数据包。可以为 IP 协议指定 0 到 255 之间的数字。有关完整的协议号列表，请访问 http://www.iana.org/assignments/protocol-numbers。可以将这些协议号与以下运算符结合使用：`<`、`>` 或 `!`。例如，要检查使用非 ICMP 的任何协议的流量，请使用 `!1` 作为 `ip_proto` 关键字的值。也可以在一个规则中多次使用 `ip_proto` 关键字；但请注意，规则引擎会将此关键字的多个实例解释为具有布尔 AND 关系。例如，如果创建一个包含 `ip_proto:!3; ip_proto:!6` 的规则，该规则将忽略使用 GGP 协议和 TCP 协议的流量。

检查数据包的服务类型

许可证：保护

有些网络使用服务类型 (ToS) 值设置在网络上传输的数据包的优先级。使用 `tos` 关键字可根据指定为该关键字的参数的值测试数据包的 IP 报头 ToS 值。对于其 ToS 已设置为指定值且符合规则中规定的其他条件的数据包，使用 `tos` 关键字的规则将会触发。

注　`tos` 参数值必须为数字。

ToS 字段已在 IP 报头协议中弃用，取而代之的是 Differentiated Services Code Point (DSCP) 字段。

检查数据包的生存时间值

许可证：保护

数据包的生存时间 (ttl) 值指明数据包在被丢弃之前可以跳多少次。可以使用 `ttl` 关键字根据指定为关键字参数的值或值范围测试数据包的 IP 报头 ttl 值。将 `ttl` 关键字参数设置为较小的值 （例如 0 或 1）可能会有帮助，因为小的生存时间值有时表示跟踪路由或入侵逃避行为。（但请注意，此关键字的适当值取决于受管设备的位置和网络拓扑。）如下使用语法：

- 将 TTL 值设置为 0 到 255 之间的整数。也可以该值前面加上一个等号 (=) （例如，可以指定 `5` 或 `=5`）。
- 使用连字符 (-) 指定 TTL 值的范围 （例如，`0-2` 指定 0 到 2 之间的所有值，`-5` 指定 0 到 5 之间的所有值，`5-` 指定 5 到 255 之间的所有值）。
- 使用大于号 (>)指定 TTL 值大于一个特定值 （例如，`>3` 指定大于 3 的所有值）。

- 使用大于或等于号 (>=) 指定 TTL 值大于或等于一个特定值（例如，`>=3` 指定大于或等于 3 的所有值）。
- 使用小于号 (<)指定 TTL 值小于一个特定值 （例如，`<3` 指定小于 3 的所有值）。
- 使用小于或等于号 (<=) 指定 TTL 值小于或等于一个特定值（例如，`<=3` 指定小于或等于 3 的所有值）。

检查 ICMP 报头值

许可证：保护

FireSIGHT 系统支持可用于识别 ICMP 数据包报头中的攻击和安全策略违规的关键字。但请注意，存在的预定义规则检测大多数 ICMP 类型和代码。可考虑启用现有规则或者根据现有规则创建本地规则；如果您从头开始构建 ICMP 规则，可能会更快找到符合您需求的规则。

有关 ICMP 特定关键字的详细信息，请参阅以下各节：

- 第 36-44 页上的识别静态 ICMP ID 和序列值
- 第 36-44 页上的检查 ICMP 消息类型
- 第 36-45 页上的检查 ICMP 消息代码

识别静态 ICMP ID 和序列值

许可证：保护

ICMP 标别号和序列号有助于将 ICMP 响应与 ICMP 请求关联起来。在正常流量中，这些值动态地分配给数据包。有些隐蔽通道和分布式拒绝服务 (DDoS) 程序使用静态 ICMP ID 和序列值。使用以下关键字可识别具有静态值的 ICMP 数据包。

icmp_id

`icmp_id` 关键字检查 ICMP 回应请求或应答数据包的 ICMP ID 号。应使用对应于 ICMP ID 号的数值作为 `icmp_id` 关键字的参数。

icmp_seq

`icmp_seq` 关键字检查 ICMP 回应请求或应答数据包的 ICMP 序列。应使用对应于 ICMP 序列号的数值作为 `icmp_seq` 关键字的参数。

检查 ICMP 消息类型

许可证：保护

使用 `itype` 关键字可查找具有特定 ICMP 消息类型值的数据包。可以指定有效的 ICMP 类型值（有关 ICMP 类型编号的完整列表，请访问 http://www.iana.org/assignments/icmp-parameters 或 http://www.faqs.org/rfcs/rfc792.html）或无效的 ICMP 类型值来测试不同类型的流量。例如，攻击者可以将 ICMP 类型值设置为超出范围，从而导致拒绝服务和泛洪攻击。

可以使用小于号 (<) 和大于号 (>) 指定 `itype` 参数值的范围。

例如：

- <35
- >36
- 3<>55

提示 有关 ICMP 类型编号的完整列表，请访问 http://www.iana.org/assignments/icmp-parameters 或 http://www.faqs.org/rfcs/rfc792.html。

检查 ICMP 消息代码

许可证：保护

ICMP 消息有时包含代码值，用于在目标不可达的情况下提供有关详细信息。（有关与消息类型[可对其使用消息代码]相关的 ICMP 消息代码的完整列表，请参阅 http://www.iana.org/assignments/icmp-parameters 中的第二节。）

使用 `icode` 关键字可识别具有特定 ICMP 代码值的数据包。可以指定有效的 ICMP 代码值或无效的 ICMP 代码值来测试不同类型的流量。

可以使用小于号 (<) 和大于号 (>) 指定 `icode` 参数值的范围。

例如：

- 要查找小于 35 的值，请指定 `<35`。
- 要查找大于 36 的值，请指定 `>36`。
- 要查找 3 到 55 之间的值，请指定 `3<>55`。

提示 可以同时使用 `icode` 和 `itype` 关键字来识别与这两者都匹配的流量。例如，要识别包含 ICMP Destination Unreachable 代码类型和 ICMP Port Unreachable 代码类型的 ICMP 流量，请指定 3 作为 `itype` 关键字的值（用于 Destination Unreachable 类型），并指定 3 作为 `icode` 关键字的值（用于 Port Unreachable 类型）。

检查 TCP 报头值和数据流大小

许可证：保护

FireSIGHT 系统支持使用数据包 TCP 报头和 TCP 数据流大小识别尝试攻击的关键字。有关 TCP 特定关键字的详细信息，请参阅以下各节：

- 第 36-45 页上的检查 TCP 确认值
- 第 36-46 页上的检查 TCP 标志组合
- 第 36-47 页上的将规则应用于 TCP 或 UDP 客户端或服务器流量
- 第 36-48 页上的识别静态 TCP 序列号
- 第 36-48 页上的识别给定大小的 TCP 窗口
- 第 36-48 页上的识别给定大小的 TCP 数据流

检查 TCP 确认值

许可证：保护

使用 `ack` 关键字可将某个值与数据包的 TCP 确认号进行比较。如果数据包的 TCP 确认号与为 `ack` 关键字指定的值相匹配，规则将会触发。

`ack` 参数值必须为数字。

检查 TCP 标志组合

许可证：保护

可以使用 `flags` 关键字指定 TCP 标志的任意组合，如果在已检查的数据包中设置此关键字，将导致规则触发。

注 在使用 `A+` 作为 `flags` 的值的一般情况下，应转为使用具有 `established` 值的 `flow` 关键字。通常，如果使用标志以确保标志的所有组合均已检测到，应使用具有 `stateless` 值的 `flow` 关键字。关于 `flow` 关键字的详细信息，请参阅第 36-47 页上的将规则应用于 TCP 或 UDP 客户端或服务器流量。

可以检查或忽略下表中所述的 `flag` 关键字的值。

表 36-26　flag 参数

参数	TCP 标志
Ack	确认数据。
Psh	数据应该在此数据包中发送。
Syn	新的连接。
Urg	包含紧急数据的数据包。
Fin	关闭的连接。
Rst	中止的连接。
CWR	ECN 堵塞窗口已减少。这以前是 R1 参数，仍支持向后兼容。
ECE	ECN 响应。这以前是 R2 参数，仍支持向后兼容。

提示 有关显式拥塞通知 (ECN) 的详细信息，请参阅以下网址提供的信息：http://www.faqs.org/rfcs/rfc3168.html。

使用 `flags` 关键字时，可以使用运算符来指示系统如何匹配多个标志。下表介绍了这些运算符。

表 36-27　与 flags 配合使用的运算符

运算符	说明	示例
全部	数据包必须包含所有指定的标志。	选择 `Urg` 和 `all` 可规定数据包必须包含紧急标志，且可以包含任何其他标志。
any	数据包可包含任何指定的标志。	选择 `Ack`、`Psh` 和 `any` 可规定必须设置 `Ack` 和/或 `Psh` 标志才能触发规则，且也可以对数据包设置其他标志。
不会	数据包**不得**包含指定的标志集。	选择 `Urg` 和 `not` 可规定**不**对会触发此规则的数据包进行设置紧急标志。

将规则应用于 TCP 或 UDP 客户端或服务器流量

许可证：保护

可以使用 `flow` 关键字选择由规则根据会话特征进行的检查的数据包。`flow` 关键字允许您指定规则应用的流量的方向，从而将规则应用于客户端流量或服务器流量。要指定 `flow` 关键字如何检查数据包，可以设置要分析的流量的方向、已检查的数据包的状态以及这些数据包是否是重建数据流的一部分。

数据包状态检测发生在规则处理之后。如果要使某个 TCP 规则忽略无状态流量（尚未建立会话上下文的流量），必须将 `flow` 关键字添加到该规则，并为该关键字选择 **Established** 参数。如果要使某个 UDP 规则忽略无状态流量，必须将 `flow` 关键字添加到该规则，并选择 **Established** 参数和/或方向参数。这样， TCP 或 UDP 规则就会执行数据包状态检查。

如果添加方向参数，规则引擎将只检查具有已建立状态且流向与指定方向匹配的数据包。例如，如果将具有 `established` 参数和 `From Client` 参数的 `flow` 关键字添加到某个规则，且该规则会在检测到 TCP 或 UDP 连接的情况下触发，那么规则引擎将只检查从特定客户端发送的数据包。

提示 为了获得最佳性能，应始终在 TCP 规则或 UDP 会话规则中包含 `flow` 关键字。

要指定流量，请从 Create Rule 页面上的 **Detection Options** 列表中选择 `flow` 关键字，并点击 **Add Option**。然后，为每个字段从列表中选择参数。

下表介绍了可为 `flow` 关键字指定的数据流相关参数：

表 36-28　状态相关 flow 参数

参数	说明
成熟市场	在已建立连接的情况下触发。
无状态	无论数据流处理器的状态如何，都会触发。

下表介绍了可为 `flow` 关键字指定的方向选项：

表 36-29　flow 方向参数

参数	说明
To Client	服务器响应时触发。
To Server	客户端响应时触发。
From Client	客户端响应时触发。
From Server	服务器响应时触发。

请注意，`From Server` 和 `To Client` 执行相同的功能，`To Server` 和 `From Client` 执行相同的功能。这些选项是为了是规则具有上下文和可读性。例如，如果要创建用于检测从服务器向客户端发起的木马攻击的规则，应使用 `From Server`。但是，如果要创建用于检测从客户端向服务器发出的木马攻击的规则，应使用 `From Client`。

下表介绍了可为 flow 关键字指定的数据流相关参数：

表 36-30　数据流相关的 flow 参数

参数	说明
Ignore Stream Traffic	重建流数据包时不触发。
Only Stream Traffic	仅在重建流数据包时触发。

例如，可以使用 To Server, Established, Only Stream Traffic 作为 flow 关键字的值，这样将会检测在建立的会话中从客户端流向服务器并且由数据流预处理器重组的流量。

识别静态 TCP 序列号

许可证：保护

使用 seq 关键字可指定静态序列号值。序列号与指定参数相匹配的数据包将会触发包含此关键字的规则。虽然此关键字很少使用，但它有助于识别使用生成的具有静态序列号的数据包的攻击和网络扫描。

识别给定大小的 TCP 窗口

许可证：保护

可以使用 window 关键字指定想要的 TCP 窗口大小。包含此关键字的规则每当遇到具有指定大小 TCP 窗口的数据包时，都会触发。虽然此关键字很少使用，但它有助于识别使用生成的具有静态 TCP 窗口大小的数据包的攻击和网络扫描。

识别给定大小的 TCP 数据流

许可证：保护

可以将 stream_size 关键字与数据流预处理器配合使用，以确定 TCP 数据流的大小（以字节为单位），具体格式如下：

direction,*operator*,*bytes*

其中，*bytes* 是字节数。必须用逗号 (,) 分隔参数中的每个选项。

下表介绍了可为 stream_size 关键字指定的不区分大小写的方向选项：

表 36-31　stream_size 关键字定向参数

参数	说明
客户端	当来自客户端的数据流与指定数据流大小相匹配时触发。
服务器	当来自服务器的数据流与指定数据流大小相匹配时触发。
both	当来自客户端和服务器的流量都与指定数据流大小相匹配时触发。 例如，如果来自客户端的流量大于 200 字节，且来自服务器的流量也大于 200 字节，参数 both, >, 200 将会触发。
either	当来自客户端或服务器流量与指定数据流大小相匹配时触发（无论哪一种情况先发生）。 例如，如果来自客户端的流量大于 200 字节，或来自服务器的流量大于 200 字节，参数 either, >, 200 将会触发。

下表介绍了可与 stream_size 关键字配合使用的运算符：

表 36-32　stream_size 关键字参数运算符

运算符	说明
=	等于
!=	不等于
>	大于
<	小于
>=	大于或等于
<=	小于或等于

例如，可以使用 client, >=, 5001216 作为 stream_size 关键字的参数，以检测从客户端发往服务器的且大于或等于 5001216 字节的 TCP 数据流。

启用和禁用 TCP 数据流重组

许可证：保护

如果对连接检查的流量与规则条件相匹配，可以使用 stream_reassemble 关键字为单一连接启用或禁用 TCP 数据流重组。或者，可以在规则中多次使用此关键字。

可使用以下语法启用或禁用数据流重组：

```
enable|disable, server|client|both, option, option
```

下表介绍了可与 stream_reassemble 关键字配合使用的可选参数。

表 36-33　stream_reassemble 可选参数

参数	说明
noalert	无论规则中是否指定任何其他检测选项，都不生成事件。
fastpath	当有匹配时，忽略连接流量的其余部分。

例如，以下示例禁用 TCP 客户端数据流重组，而且不针对在 HTTP 响应中检测到 200 OK 状态代码的连接生成事件：

```
alert tcp any 80 -> any any (flow:to_client, established; content: "200 OK";
stream_reassemble:disable, client, noalert
```

要使用 stream_reassemble，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 stream_reassemble 并点击 **Add Option**。

系统将显示 stream_reassemble 部分。

从会话提取 SSL 信息

许可证：保护

可以使用 SSL 规则关键字调用安全套接字层 (SSL) 预处理器，并从加密会话中的数据包提取有关 SSL 版本和会话状态的信息。

客户机和服务器进行通信以使用 SSL 或安全传输层 (TLS) 建立加密会话时，它们之间会交换握手消息。虽然在会话中传输的数据是加密的，但握手消息没有加密。

SSL 预处理器从特定握手字段提取状态和版本信息。握手中的两个字段分别指明用于加密会话的 SSL 或 TLS 版本以及握手的阶段。

有关详细信息，请参阅以下各节：

- 第 36-50 页上的 ssl_state
- 第 36-51 页上的 ssl_version

ssl_state

许可证：保护

`ssl_state` 关键字可用于匹配加密会话的状态信息。要同时检查所用的两个或更多 SSL 版本，请在规则中使用多个 `ssl_version` 关键字。

如果规则使用 `ssl_state` 关键字，规则引擎将调用 SSL 预处理器来检查流量的 SSL 状态信息。

例如，要检测是否有攻击者试图通过发送具有超长长度和过量数据的 `ClientHello` 消息来造成服务器缓冲区溢出，可以使用带有 `client_hello` 参数的 `ssl_state` 关键字，然后检查异常大的数据包。

可使用逗号分隔列表为 SSL 状态指定多个参数。如果列出多个参数，系统将使用 OR 运算符对这些参数进行评估。例如，如果指定 `client_hello` 和 `server_hello` 作为参数，系统将会根据带有 `client_hello` 或 `server_hello` 的流量对规则进行评估。

还可以否定任何参数；例如：

```
!client_hello, !unknown
```

为确保连接已达到状态集中的每种状态，应使用具有 ssl_state 规则选项的多个规则。`ssl_state` 关键字将以下标识符作为参数：

表 36-34　ssl_state 参数

参数	目的
`client_hello`	当客户端请求加密会话时，匹配消息类型为 `ClientHello` 的握手消息。
`server_hello`	当服务器响应客户端的加密会话请求时，匹配消息类型为 `ServerHello` 的握手消息。
`client_keyx`	当客户端向服务器发出密钥以确认收到来自服务器的密钥时，匹配消息类型为 `ClientKeyExchange` 的握手消息。
`server_keyx`	当客户端向服务器发出密钥以确认收到来自服务器的密钥时，匹配消息类型为 `ServerKeyExchange` 的握手消息。
`unknown`	匹配任何握手消息类型。

ssl_version

许可证：保护

ssl_version 关键字可用于匹配加密会话的版本信息。如果规则使用 ssl_version 关键字，规则引擎将调用 SSL 预处理器来检查流量的 SSL 版本信息。

例如，如果知道 SSL 2 版本中存在缓冲区溢出漏洞，可以使用带有 sslv2 参数的 ssl_version 关键字来识别使用该 SSL 版本的流量。

可使用逗号分隔列表为 SSL 版本指定多个参数。如果列出多个参数，系统将使用 OR 运算符对这些参数进行评估。例如，如果要识别任何未使用 SSLv2 的加密流量，可以向规则添加 ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2。这样，规则将会评估任何使用 SSL 3 版本、TLS 1.0 版本、 TLS 1.1 版本或 TLS 1.2 版本的流量。

ssl_version 关键字将以下 SSL/TLS 版本标识符作为参数：

表 36-35　ssl_version 参数

参数	目的
sslv2	匹配使用安全套接字层 (SSL) 2 版本编码的流量。
sslv3	匹配使用安全套接字层 (SSL) 3 版本编码的流量。
tls1.0	匹配使用传输层安全 (TLS) 1.0 版本编码的流量。
tls1.1	匹配使用传输层安全 (TLS) 1.1 版本编码的流量。
tls1.2	匹配使用传输层安全 (TLS) 1.2 版本编码的流量。

检查应用层协议值

许可证：保护

虽然预处理器执行对于应用层协议值的大部分检查和规范化工作，但您仍可以使用以下各节中所述的关键字对应用层值进行检查。

- 第 36-51 页上的 RPC
- 第 36-52 页上的 ASN.1
- 第 36-53 页上的 urilen
- 第 36-54 页上的 DCE/RPC 关键字
- 第 36-56 页上的 SIP 关键字
- 第 36-58 页上的 GTP 关键字
- 第 36-68 页上的 Modbus 关键字
- 第 36-70 页上的 DNP3 关键字

RPC

许可证：保护

rpc 关键字在 TCP 或 UDP 数据包中识别开放网络计算远程过程调用 (ONC RPC) 服务。这使您可以检测尝试识别主机上 RPC 程序的行为。入侵者可以使用 RPC 端口映射程序来确定网络上是否运行着可以利用的任何 RPC 服务。他们还可能尝试访问不使用端口映射程序运行 RPC 的其他端口。下表列出了 rpc 关键字接受的参数。

表 36-36　rpc 关键字参数

参数	说明
application	RPC 应用编号
procedure	调用的 RPC 程序
version	RPC 版本

要为 rpc 关键字指定参数，请使用以下语法：

application,*procedure*,*version*

其中，*application* 是 RPC 应用编号，*procedure* 是 RPC 程序编号，*version* 是 RPC 版本号。必须为 rpc 关键字指定所有参数 - 如果不能够指定某一参数，应以星号 (*) 代替。

例如，要搜索具有任意程序或版本的 RPC 端口映射程序 （以数字 100000 表示的 RPC 应用），可使用 100000,*,* 作为参数。

ASN.1

许可证：保护

asn1 关键字使您可以解码整个或部分数据包，以查找各种恶意编码。

下表介绍了 asn1 关键字的参数。

表 36-37　asn.1 关键字参数

参数	说明
Bitstring Overflow	检测可远程攻击的无效位串编码。
Double Overflow	检测大于标准缓冲区的双 ASCII 编码。这是 Microsoft Windows 中的一个已知漏洞，但目前不知道哪些服务可能会被利用。
Oversize Length	检测长度大于提供的参数的 ASN.1 类型。例如，如果将 Oversize Length 设置为 500，任何大于 500 的 ASN.1 类型都会触发规则。
Absolute Offset	设置从数据包负载起点算起的绝对偏移量。（请记住，偏移量计数器从字节 0 开始计算。）例如，如果要解码 SNMP 数据包，请将 Absolute Offset 设置为 0，但不设置 Relative Offset。 Absolute Offset 可以是正数或负数。
Relative Offset	从上一次成功内容匹配、pcre 或 byte_jump 算起的相对偏移量。要解码紧接在内容“foo”后的 ASN.1 序列，请将 Relative Offset 设置为 0，但不设置 Absolute Offset。 Relative Offset 可以是正数或负数。（请记住，偏移量计数器从字节 0 开始计算。）

例如，Microsoft ASN.1 库中存在一个会造成缓冲区溢出的已知漏洞，使得攻击者能够利用包含特制的身份验证数据包的条件。当系统解码 ASN.1 数据时，数据包中的攻击代码可以在具有系统级别权限的主机上执行，或可能导致 DoS 条件。以下规则使用 asn1 关键字检测试图利用此漏洞的行为：

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|"; nocase;
offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length
100,relative_offset 54;)
```

当有 TCP 流量从 $EXTERNAL_NET 变量中定义的使用任何端口的任何 IP 地址流向 $HOME_NET 变量中定义的使用端口 445 的任何 IP 地址，上述规则将会生成事件。此外，它仅对与服务器之间建立的连接执行规则。然后，该规则在特定位置对特定内容进行测试。最后，该规则使用 `asn1` 关键字检测位串编码和双 ASCII 编码，以及确定自上一次成功内容匹配结束以来从 55 字节开始算起超过 100 字节的 asn.1 类型长度。（请记住，偏移量计数器从字节 0 开始计算。）

urilen

许可证：保护

可以将 `urilen` 关键字和 HTTP 检查预处理器结合使用，以检查 HTTP 流量中特定长度、小于最大长度、大于最小长度或在指定范围内的 URI。

在 HTTP 检查预处理器对数据包进行规范化和检查后，规则引擎将根据规则评估数据包，并确定 URI 是否与 `urilen` 关键字指定的长度条件相匹配。可以使用此关键字来检测试图利用 URI 长度漏洞的攻击，例如，创建缓冲区溢出，以使攻击者可以在具有系统级别权限的主机上形成 DoS 条件或执行代码。

在规则中使用 `urilen` 关键字时，请注意：

- 实际上，`urilen` 关键字总是与 `flow:established` 关键字以及一个或多个其他关键字结合使用。
- 规则协议始终是 TCP。有关详情，请参见第 36-4 页上的指定协议。
- 目标端口始终是 HTTP 端口。有关详细信息，请参阅第 36-8 页上的在入侵规则中定义端口和第 3-16 页上的优化预定义默认变量。

可以使用十进制字节数、小于号 (<) 和大于号 (>) 指定 URI 长度。

例如：

- 指定 `5` 将会检测长度为 5 字节的 URI。
- 指定 `< 5`（用一个空格字符隔开）将会检测长度小于 5 字节的 URI。
- 指定 `> 5`（用一个空格字符隔开）将会检测长度大于 5 字节的 URI。
- 指定 `3 <> 5`（`<>` 前后各有一个空格字符）将会检测长度为 3 到 5 字节的 URI。

例如， Novell 服务器的监控和诊断实用程序 iMonitor 2.4 版中存在一个已知漏洞，该漏洞来自 eDirectory 8.8 版。包含过长 URI 的一个数据包造成缓冲区溢出，使得攻击者者能够利用包含特制数据包的条件，该数据包可以在具有系统级别权限的主机上执行或可能导致 DoS 条件。以下规则使用 `urilen` 关键字检测试图利用此漏洞的行为：

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt";flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

当有 TCP 流量从 $EXTERNAL_NET 变量中定义的使用任何端口的任何 IP 地址流向 $HOME_NET 变量中定义的使用 $HTTP_PORTS 变量中定义的端口的任何 IP 地址，上述规则将会生成事件。此外，仅针对与服务器之间建立的 TCP 连接根据该规则评估数据包。该规则使用 `urilen` 关键字检测长度超过 8192 字节的任何 URI。最后，该规则在 URI 中搜索不区分大小写的特定内容 `/nds/`。

DCE/RPC 关键字

许可证：保护

下表中所述的三个 DCE/RPC 关键字可用于监控 DCE/RPC 会话流量的漏洞。当系统处理带有这些关键字的规则时，会调用 DCE/RPC 预处理器。有关详情，请参见第 27-2 页上的解码 DCE/RPC 流量。

表 36-38　　DCE/RPC 关键字

使用.....	使用方式	要检测的内容
dce_iface	独立	识别特定 DCE/RPC 服务的数据包
dce_opnum	在前面加上 dce_iface	识别特定 DCE/RPC 服务操作的数据包
dce_stub_data	在前面加上 dce_iface 和 dce_opnum	定义特定操作请求或响应的存根数据

请注意，在上表中，应始终在 dce_iface 前面加上 dce_iface，在 dce_stub_data 前面加上 dce_iface 和 dce_opnum。

也可以将这些 DCE/RPC 关键字与其他规则关键字结合连用。请注意，对于 DCE/RPC 规则，应使用选择了 **DCE/RPC** 参数的 byte_jump、byte_test 和 byte_extract 关键字。有关详细信息，请参阅第 36-28 页上的使用 Byte_Jump 和 Byte_Test和第 36-75 页上的将数据包数据读取到关键字参数中。

思科建议在包含 DCE/RPC 关键字的规则中至少包含一个 content 关键字，以确保规则引擎使用快速模式匹配程序，从而加快处理速度和提高性能。请注意，如果规则包含至少一个 content 关键字，无论您是否启用 content 关键字的 **Use Fast Pattern Matcher** 参数，规则引擎都会使用快速模式匹配程序。有关详细信息，请参阅第 36-14 页上的搜索内容匹配和第 36-24 页上的 Use Fast Pattern Matcher。

在以下情况下，可以将 DCE/RPC 版本及相邻报头信息用作匹配的内容：

- 规则不包括其他 content 关键字
- 规则包含另一个 content 关键字，但 DCE/RPC 版本及相邻信息代表比其他内容更独特的模式

  例如， DCE/RPC 版本及相邻信息更有可能比内容的单个字节更加独特。

应使用以下其中一个版本及相邻信息内容匹配来终止限定规则：

- 对于面向连接的 DCE/RPC 规则，使用内容 |05 00 00|（用于 05 主要版本、00 次要版本和请求 PDU [协议数据单元]类型 00）。
- 对于无连接的 DCE/RPC 规则，使用内容 |04 00|（用于 04 版本和请求 PDU 类型 00）。

在这两种情况下，都应将版本及相邻信息的 content 关键字放在规则末尾，以调用快速模式匹配程序而不重复 DCE/RPC 预处理器已完成的处理。请注意：将 content 关键字放在规则末尾这种做法适用于被用作调用快速模式匹配程序的手段的版本内容，对于规则中的其他内容匹配无需这样做。

有关详细信息，请参阅以下各节：

- 第 36-55 页上的 dce_iface
- 第 36-56 页上的 dce_opnum
- 第 36-56 页上的 dce_stub_data

dce_iface

许可证：保护

可以使用 dce_iface 关键字识别特定 DCE/RPC 服务。

此外，还可以将 dce_iface 与 dce_opnum 和 dce_stub_data 关键字结合使用，以进一步限制要检查的 DCE/RPC 流量。有关详细信息，请参阅第 36-56 页上的 dce_opnum和第 36-56 页上的 dce_stub_data。

固定的 16 字节通用唯一标识符 (UUID) 用于识别分配给每个 DCE/RPC 服务的应用接口。例如，UUID 4b324fc8-670-01d3-1278-5a47bf6ee188 识别 DCE/RPC lanmanserver 服务（又称为 srvsvc 服务），该服务提供大量用于共享对等网络打印机、文件和 SMB 命名管道的管理功能。 DCE/RPC 预处理器使用 UUID 及相关报头值来跟踪 DCE/RPC 会话。

接口 UUID 是由 5 个十六进制字符串 （字符串之间用连字符分隔）组成：

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

可以通过输入整个 UUID （包括连字符）来指定接口，如以下用于 netlogon 接口的 UUID 中所示：

```
12345678-1234-abcd-ef00-01234567cffb
```

请注意，必须以大端字节顺序指定 UUID 中的前三个字符串。尽管发布的接口列表和协议分析工具通常以正确的字节顺序显示 UUID，但您可能需要在输入前重新排列 UUID 字节顺序。考虑以下所示的信使服务 UUID，在原始 ASCII 文本中，该 UUID 的前三个字符串有时可能会以小端字节顺序显示：

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

可以为 dce_iface 关键字指定这个 UUID，方法是，插入连字符，并以大端字节顺序放置前三个字符串，如下所示：

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

尽管一个 DCE/RPC 会话可能包含发向多个接口的请求，但在一个规则中只能包含一个 dce_iface 关键字。可创建其他规则来检测其他接口。

DCE/RPC 应用接口也有接口版本号。或者，可以指定带有运算符的接口版本，用该操作符指明版本是等于、不等于、小于还是大于指定值。

除了 TCP 分段或 IP 分片外，还可以对面向连接和无连接的 DCE/RPC 进行分片。通常，将任何 DCE/RPC 分片 （第一个除外）与指定接口相关联没有任何作用，而且这样做可能导致大量误报。但是，为了提高灵活性，可以根据指定接口对所有分片进行评估。

下表总结了 dce_iface 关键字参数。

表 36-39　　dce_iface 参数

参数	说明
Interface UUID	UUID （包括连字符），用于识别要在 DCE/RPC 流量中检测的特定服务的应用接口。与指定接口相关的任何请求将匹配接口 UUID。
版本	或者，可以选择应用接口版本号 0 到 65535 和一个操作符，以指明是否检测大于 (>)、小于 (<)、等于 (=) 或不等于 (!) 指定值的版本。
All Fragments	或者，可以选择匹配与 DCE/RPC 分片相关的所有接口和 （如有指定）接口版本。默认情况下，此参数被禁用，表示关键字仅在第一个分片或整个未分片数据包与指定接口相关时才进行匹配。请注意，启用此参数可能会导致误报。

dce_opnum

许可证：保护

可以将 dce_opnum 关键字和 DCE/RPC 预处理器结合使用，以检测识别 DCE/RPC 服务提供的一个或多个特定操作的数据包。

客户端功能调用请求特定服务函数（这些函数在 DCE/RPC 规范中称为*操作*）。操作编号 (opnum) 用于识别 DCE/RPC 报头中的特定操作。漏洞可能会针对特定操作。

例如， UUID 12345678-1234-ABCD-ef00-01234567cffb 识别用于 netlogon 服务的接口；该服务提供几十个不同的操作，其中之一是操作 6， NetrServerPasswordSet 操作。

应该在 dce_opnum 关键字前面加上 dce_iface 关键字，以识别操作的服务。有关详情，请参见第 36-55 页上的 dce_iface。

可以为特定操作指定一个 0 到 65535 之间的十进制值，可以指定一系列由连字符分隔的操作，或者指定逗号分隔的操作和范围列表，其中的操作和范围可按任何顺序排列。

以下任何示例都将指定有效的 netlogon 操作编号：

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

dce_stub_data

许可证：保护

可以将 dce_stub_data 关键字和 DCE/RPC 预处理器结合使用，以指定无论任何其他规则选项如何，规则引擎都应从存根数据的开头开始检查。紧跟在 dce_stub_data 关键字后面的数据包负载规则选项相对于存根数据缓冲区适用。

DCE/RPC 存根数据提供客户端程序调用和 DCE/RPC 运行时系统之间的接口，这种机制可提供对于 DCE/RPC 至关重要的例程和服务。 DCE/RPC 漏洞在 DCE/RPC 数据包的存根数据部分中识别出。由于存根数据与特定的操作或函数调用相关，因此，应始终在 dce_stub_data 前面加上 dce_iface 和 dce_opnum，以识别相关的服务和操作。

dce_stub_data 关键字没有参数。有关详细信息，请参阅第 36-55 页上的 dce_iface和第 36-56 页上的 dce_opnum。

SIP 关键字

许可证：保护

有四个 SIP 关键字可用于监控 SIP 会话流量的漏洞。

请注意， SIP 协议容易受到拒绝服务 (DoS) 攻击。基于速率的攻击防御可能对解决这类攻击的规则有利。有关详细信息，请参阅第 32-26 页上的添加动态规则状态和第 34-8 页上的防御基于速率的攻击。

有关详细信息，请参阅以下各节：

- 第 36-57 页上的 sip_header
- 第 36-57 页上的 sip_body
- 第 36-57 页上的 sip_method
- 第 36-58 页上的 sip_stat_code

sip_header

许可证：保护

可以使用 `sip_header` 关键字从提取的 SIP 请求或响应报头开头开始检查，并将检查限制为仅针对报头字段。

`sip_header` 关键字没有参数。有关详细信息，请参阅第 36-57 页上的 sip_method和第 36-58 页上的 sip_stat_code。

以下示例规则分片指向 SIP 报头并匹配 Cseq 报头字段：

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

sip_body

许可证：保护

可以使用 `sip_body` 关键字在提取的 SIP 请求或响应消息正文开头开始检查，并将检查限制为仅针对消息正文。

`sip_body` 关键字没有参数。

以下示例规则分片指向 SIP 消息正文，并匹配所提取 SDP 数据的 c（连接信息）字段中的特定 IP 地址：

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

请注意，规则不仅限于搜索 SDP 内容。 SIP 预处理器将提取整个消息正文并使其可供规则引擎使用。

sip_method

许可证：保护

每个 SIP 请求中的 *method* 字段用于识别请求的目的。可以使用 `sip_method` 关键字测试特定方法的 SIP 请求。使用逗号隔开多种方法。

可以指定以下当前定义的任何 SIP 方法：

```
Ack、benotify、bye、cancel、do、info、invite、join、message、notify、options、prack、
publish、quath、refer、register、service、sprack、subscribe、unsubscribe、update
```

方法不区分大小写。可以使用逗号分隔多种方法。

由于可能在将来定义新的 SIP 方法，因此也可以指定自定义方法 （即，当前未定义的方法）。RFC 2616 中定义了接受的字段值，该规范允许除控制字符和分隔符 （例如 `=`、`(` 和 `}`）以外的所有字符。有关被排除分隔符的完整列表，请参阅 RFC 2616。如果系统在流量中遇到指定的自定义方法，它将检查数据包报头，但不检查消息。

系统最多支持 32 种方法，包括 21 种当前定义的方法和 11 种其他方法。系统将忽略您可能配置的任何未定义的方法。请注意，总共有 32 种方法，包括使用 **Methods to Check** SIP 预处理器选项指定的方法。有关详情，请参见第 27-41 页上的选择 SIP 预处理器选项。

如果使用否定形式，只能指定一种方法。例如：

```
!invite
```

但请注意，一个规则中的多个 `sip_method` 关键字与 **AND** 运算相关联。例如，要测试除 `invite` 和 `cancel` 以外的所有提取的方法，可以使用两个否定形式的 `sip_method` 关键字：

```
sip_method: !invite
sip_method: !cancel
```

思科建议在包含 `sip_method` 关键字的规则中至少包含一个 `content` 关键字，以确保规则引擎使用快速模式匹配程序，从而加快处理速度和提高性能。请注意，如果规则包含至少一个 `content` 关键字，无论您是否启用 `content` 关键字的 **Use Fast Pattern Matcher** 参数，规则引擎都会使用快速模式匹配程序。有关详细信息，请参阅第 36-14 页上的搜索内容匹配和第 36-24 页上的 Use Fast Pattern Matcher。

sip_stat_code

许可证：保护

每个 SIP 响应中的三位数状态代码指明请求操作的结果。可以使用 sip_stat_code 关键字测试 SIP 响应的特定状态代码。

可以指定一个一位响应型数字 （1 到 9）、一个特定的三位数 （100 到 999）或者包含这两项的任意组合的逗号分隔列表。如果列表中的任何一个数字与 SIP 响应中的代码相匹配，则列表匹配。

下表介绍了可指定的 SIP 状态代码值。

表 36-40　sip_stat_code 值

要检测的内容	可指定的内容	示例	会检测的内容
特定状态代码	三位数状态代码	189	189
任何以指定一位数开始的三位数代码	一位数	1	1xx；即， 100、101、 102 等
值列表	以逗号分隔的特定代码与一位数的组合	222, 3	222 以及 300、301、 302 等

另请注意，规则引擎不使用快速模式匹配程序搜索用 sip_stat_code 关键字指定的值，无论规则是否包含 content 关键字。

GTP 关键字

许可证：保护

有三个 GSRP 隧道协议 (GTP) 关键字可用于检查 GTP 命令通道的 GTP 版本、消息类型和信息元素。 GTP 关键字不可与其他入侵规则关键字 （例如 content 或 byte_jump 关键字）结合使用。如果规则使用了 gtp_info 或 gtp_type 关键字，还必须使用 gtp_version 关键字。

有关详细信息，请参阅以下各节：

- 第 36-58 页上的 gtp_version
- 第 36-59 页上的 gtp_type
- 第 36-63 页上的 gtp_info

gtp_version

可以使用 gtp_version 关键字检查 GTP 控制信息以确定 GTP 版本为 0、 1 还是 2。

由于不同的 GTP 版本定义不同的信息类型和信息元素，因此，使用 gtp_type 或 gtp_info 关键字时必须同时使用此关键字。可以将值指定为 0、 1 或 2。

要指定 GTP 版本，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **gtp_version** 并点击 **Add Option**。

系统将显示 gtp_version 关键字。

步骤 2　将值指定为 0、 1 或 2 以识别 GTP 版本。

gtp_type

每条 GTP 消息由一种消息类型标识，消息类型由一个数值和一个字符串组成。可以将 `gtp_type` 与 `gtp_version` 关键字结合使用，以检查流量中的特定 GTP 消息类型。

可以为消息类型指定定义的十进制值，可以指定定义的字符串，或者指定包含这两项的任意组合的逗号分隔列表，如以下示例所示：

```
10, 11, echo_request
```

系统使用 OR 操作来匹配列出的每个值或字符串。值和字符串的列出顺序并不重要。列表中的任何一个值或字符串均与此关键字匹配。如果尝试保存包含无法识别的字符串或超出范围的值的规则，将会出现错误消息。

请注意，下表中不同的 GTP 版本有时会对同一种消息类型使用不同的值。例如，`sgsn_context_request` 这一消息类型在 GTPv0 和 GTPv1 中值是 50，但在 GTPv2 中值是 130。

`gtp_type` 关键字匹配不同的值，具体取决于数据包中的版本号。在上述示例中，在 GTPv0 或 GTPv1 数据包中，此关键字匹配消息类型值 50，在 GTPv2 数据包中，则匹配值 130。如果数据包中的消息类型值不是在数据包中指定的版本的已知值，此关键字不会匹配数据包。

如果为消息类型指定一个整数，则当关键字中的消息类型与 GTP 数据包中的该值匹配时，关键字将会匹配，无论数据包中指定的版本如何。

下表列出了系统识别出的为每种 GTP 消息类型定义的值和字符串。

表 36-41　　GTP 消息类型

价值	0 版本	版本 1	版本 2
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	不适用
5	node_alive_response	node_alive_response	不适用
6	redirection_request	redirection_request	不适用
7	redirection_response	redirection_response	不适用
16	create_pdp_context_request	create_pdp_context_request	不适用
17	create_pdp_context_response	create_pdp_context_response	不适用
18	update_pdp_context_request	update_pdp_context_request	不适用
19	update_pdp_context_response	update_pdp_context_response	不适用
20	delete_pdp_context_request	delete_pdp_context_request	不适用
21	delete_pdp_context_response	delete_pdp_context_response	不适用
22	create_aa_pdp_context_request	init_pdp_context_activation_request	不适用
23	create_aa_pdp_context_response	init_pdp_context_activation_response	不适用
24	delete_aa_pdp_context_request	不适用	不适用
25	delete_aa_pdp_context_response	不适用	不适用
26	error_indication	error_indication	不适用
27	pdu_notification_request	pdu_notification_request	不适用
28	pdu_notification_response	pdu_notification_response	不适用
29	pdu_notification_reject_request	pdu_notification_reject_request	不适用

表 36-41　GTP 消息类型（续）

价值	0 版本	版本 1	版本 2
30	pdu_notification_reject_response	pdu_notification_reject_response	不适用
31	不适用	supported_ext_header_notification	不适用
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	不适用	不适用	change_notification_request
全球 39	不适用	不适用	change_notification_response
48	identification_request	identification_request	不适用
49	identification_response	identification_response	不适用
50	sgsn_context_request	sgsn_context_request	不适用
51	sgsn_context_response	sgsn_context_response	不适用
52	sgsn_context_ack	sgsn_context_ack	不适用
53	不适用	forward_relocation_request	不适用
54	不适用	forward_relocation_response	不适用
55	不适用	forward_relocation_complete	不适用
56	不适用	relocation_cancel_request	不适用
57	不适用	relocation_cancel_response	不适用
58	不适用	forward_srns_contex	不适用
59	不适用	forward_relocation_complete_ack	不适用
60	不适用	forward_srns_contex_ack	不适用
64	不适用	不适用	modify_bearer_command
65	不适用	不适用	modify_bearer_failure_indication
66	不适用	不适用	delete_bearer_command
67	不适用	不适用	delete_bearer_failure_indication
68	不适用	不适用	bearer_resource_command
69	不适用	不适用	bearer_resource_failure_indication
70	不适用	ran_info_relay	downlink_failure_indication
71	不适用	不适用	trace_session_activation
72	不适用	不适用	trace_session_deactivation
73	不适用	不适用	stop_paging_indication
95	不适用	不适用	create_bearer_request
96	不适用	mbms_notification_request	create_bearer_response

表 36-41　　GTP 消息类型 （续）

价值	0 版本	版本 1	版本 2
97	不适用	mbms_notification_response	update_bearer_request
98	不适用	mbms_notification_reject_request	update_bearer_response
99	不适用	mbms_notification_reject_response	delete_bearer_request
100	不适用	create_mbms_context_request	delete_bearer_response
101	不适用	create_mbms_context_response	delete_pdn_request
102	不适用	update_mbms_context_request	delete_pdn_response
103	不适用	update_mbms_context_response	不适用
104	不适用	delete_mbms_context_request	不适用
105	不适用	delete_mbms_context_response	不适用
112	不适用	mbms_register_request	不适用
113	不适用	mbms_register_response	不适用
114	不适用	mbms_deregister_request	不适用
115	不适用	mbms_deregister_response	不适用
116	不适用	mbms_session_start_request	不适用
117	不适用	mbms_session_start_response	不适用
118	不适用	mbms_session_stop_request	不适用
119	不适用	mbms_session_stop_response	不适用
120	不适用	mbms_session_update_request	不适用
121	不适用	mbms_session_update_response	不适用
128	不适用	ms_info_change_request	identification_request
129	不适用	ms_info_change_response	identification_response
130	不适用	不适用	sgsn_context_request
131	不适用	不适用	sgsn_context_response
132	不适用	不适用	sgsn_context_ack
133	不适用	不适用	forward_relocation_request
134	不适用	不适用	forward_relocation_response
135	不适用	不适用	forward_relocation_complete
136	不适用	不适用	forward_relocation_complete_ack
137	不适用	不适用	forward_access
138	不适用	不适用	forward_access_ack
139	不适用	不适用	relocation_cancel_request
140	不适用	不适用	relocation_cancel_response
141	不适用	不适用	configuration_transfer_tunnel
149	不适用	不适用	detach
150	不适用	不适用	detach_ack
151	不适用	不适用	cs_paging

表 36-41　GTP 消息类型（续）

价值	0 版本	版本 1	版本 2
152	不适用	不适用	ran_info_relay
153	不适用	不适用	alert_mme
154	不适用	不适用	alert_mme_ack
155	不适用	不适用	ue_activity
156	不适用	不适用	ue_activity_ack
160	不适用	不适用	create_forward_tunnel_request
161	不适用	不适用	create_forward_tunnel_response
162	不适用	不适用	suspend
163	不适用	不适用	suspend_ack
164	不适用	不适用	在如图所示的
165	不适用	不适用	resume_ack
166	不适用	不适用	create_indirect_forward_tunnel_request
167	不适用	不适用	create_indirect_forward_tunnel_response
168	不适用	不适用	delete_indirect_forward_tunnel_request
169	不适用	不适用	delete_indirect_forward_tunnel_response
170	不适用	不适用	release_access_bearer_request
171	不适用	不适用	release_access_bearer_response
176	不适用	不适用	downlink_data
177	不适用	不适用	downlink_data_ack
179	不适用	不适用	pgw_restart
180	不适用	不适用	pgw_restart_ack
200	不适用	不适用	update_pdn_request
201	不适用	不适用	update_pdn_response
211	不适用	不适用	modify_access_bearer_request
212	不适用	不适用	modify_access_bearer_response
231	不适用	不适用	mbms_session_start_request
232	不适用	不适用	mbms_session_start_response
233	不适用	不适用	mbms_session_update_request
234	不适用	不适用	mbms_session_update_response
235	不适用	不适用	mbms_session_stop_request
236	不适用	不适用	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	不适用
241	data_record_transfer_response	data_record_transfer_response	不适用
254	不适用	end_marker	不适用
255	pdu	pdu	不适用

要指定 GTP 消息类型，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **gtp_type** 并点击 **Add Option**。

系统将显示 `gtp_type` 关键字。

步骤 2　为消息类型指定一个定义的十进制值 （0 到 255）、定义的字符串或包含这两项的任意组合的逗号分隔列表。有关系统识别出的值和字符串，请参阅 GTP 消息类型表。

gtp_info

一条 GTP 消息可以包含多个信息元素，其中的每一个元素均由已定义的一个数值和一个字符串来识别。可以将 `gtp_info` 与 `gtp_version` 关键字结合使用，以在特定信息元素开头开始检查，并将检查限制为仅针对该信息元素。

可以为信息元素指定已定义的十进制值或字符串。可以指定一个值或字符串，也可以在一个规则中使用多个 `gtp_info` 关键字来检查多个信息元素。

如果一条消息包含相同类型的多个信息元素，将会全部检查这些元素来进行匹配。如果信息元素按无效顺序出现，将仅检查最后一个实例。

请注意，不同的 GTP 版本有时对同一个信息元素使用不同的值。例如， `cause` 这个信息元素在 GTPv0 和 GTPv1 中值是 1，但在 GTPv2 中值是 2。

`gtp_info` 关键字匹配不同的值，具体取决于数据包中的版本号。在上述示例中，在 GTPv0 或 GTPv1 数据包中，此关键字匹配信息元素值 1，在 GTPv2 数据包中，则匹配值 2。如果数据包中的信息元素值不是在数据包中指定的版本的已知值，此关键字不会匹配数据包。

如果为信息元素指定一个整数，则当关键字中的消息类型与 GTP 数据包中的该值匹配时，关键字将会匹配，无论数据包中指定的版本如何。

下表列出了系统识别出的每个 GTP 信息元素的值和字符串。

表 36-42　GTP 信息元素

价值	0 版本	版本 1	版本 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	恢复
4	tlli	tlli	不适用
5	p_tmsi	p_tmsi	不适用
6	qos	不适用	不适用
8	recording_required	recording_required	不适用
9	身份验证	身份验证	不适用
11	map_cause	map_cause	不适用
12	p_tmsi_sig	p_tmsi_sig	不适用
13	ms_validated	ms_validated	不适用
14	恢复	恢复	不适用
15	selection_mode	selection_mode	不适用

表 36-42　　GTP 信息元素 （续）

价值	0 版本	版本 1	版本 2
16	flow_label_data_1	teid_1	不适用
17	flow_label_signalling	teid_control	不适用
18	flow_label_data_2	teid_2	不适用
19	ms_unreachable	teardown_ind	不适用
20	不适用	nsapi	不适用
21	不适用	ranap	不适用
22	不适用	rab_context	不适用
23	不适用	radio_priority_sms	不适用
24	不适用	radio_priority	不适用
25	不适用	packet_flow_id	不适用
26	不适用	charging_char	不适用
27	不适用	trace_ref	不适用
28	不适用	trace_type	不适用
29	不适用	ms_unreachable	不适用
71	不适用	不适用	apn
72	不适用	不适用	ambr
73	不适用	不适用	ebi
74	不适用	不适用	ip_addr
75	不适用	不适用	mei
76	不适用	不适用	msisdn
77	不适用	不适用	indication
78	不适用	不适用	pco
79	不适用	不适用	paa
80	不适用	不适用	bearer_qos
80	不适用	不适用	flow_qos
82	不适用	不适用	rat_type
83	不适用	不适用	serving_network
84	不适用	不适用	bearer_tft
85	不适用	不适用	tad
86	不适用	不适用	uli
87	不适用	不适用	f_teid
88	不适用	不适用	tmsi
89	不适用	不适用	cn_id
90	不适用	不适用	s103pdf
91	不适用	不适用	s1udf
92	不适用	不适用	delay_value

表 36-42　　GTP 信息元素 （续）

价值	0 版本	版本 1	版本 2
93	不适用	不适用	bearer_context
94	不适用	不适用	charging_id
95	不适用	不适用	charging_char
96	不适用	不适用	trace_info
97	不适用	不适用	bearer_flag
99	不适用	不适用	pdn_type
100	不适用	不适用	pti
101	不适用	不适用	drx_parameter
103	不适用	不适用	gsm_key_tri
104	不适用	不适用	umts_key_cipher_quin
105	不适用	不适用	gsm_key_cipher_quin
106	不适用	不适用	umts_key_quin
107	不适用	不适用	eps_quad
108	不适用	不适用	umts_key_quad_quin
109	不适用	不适用	pdn_connection
110	不适用	不适用	pdn_number
111	不适用	不适用	p_tmsi
112	不适用	不适用	p_tmsi_sig
113	不适用	不适用	hop_counter
114	不适用	不适用	ue_time_zone
115	不适用	不适用	trace_ref
116	不适用	不适用	complete_request_msg
117	不适用	不适用	guti
118	不适用	不适用	f_container
119	不适用	不适用	f_cause
120	不适用	不适用	plmn_id
121	不适用	不适用	target_id
123	不适用	不适用	packet_flow_id
124	不适用	不适用	rab_contex
125	不适用	不适用	src_rnc_pdcp
126	不适用	不适用	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	不适用
131	apn	apn	change_report_action

表 36-42　GTP 信息元素 （续）

价值	0 版本	版本 1	版本 2
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	不适用	qos	node_type
136	不适用	authentication_qu	fqdn
137	不适用	tft	ti
138	不适用	target_id	mbms_session_duration
139	不适用	utran_trans	mbms_service_area
140	不适用	rab_setup	mbms_session_id
141	不适用	ext_header	mbms_flow_id
142	不适用	trigger_id	mbms_ip_multicast
143	不适用	omc_id	mbms_distribution_ack
144	不适用	ran_trans	rfsp_index
145	不适用	pdp_context_pri	uci
146	不适用	addi_rab_setup	csg_info
147	不适用	sgsn_number	csg_id
148	不适用	common_flag	cmi
149	不适用	apn_restriction	service_indicator
150	不适用	radio_priority_lcs	detach_type
151	不适用	rat_type	ldn
152	不适用	user_loc_info	node_feature
153	不适用	ms_time_zone	mbms_time_to_transfer
154	不适用	imei_sv	throttling
155	不适用	camel	ARP
156	不适用	mbms_ue_context	epc_timer
157	不适用	tmp_mobile_group_id	signalling_priority_indication
158	不适用	rim_routing_addr	tmgi
159	不适用	mbms_config	mm_srvcc
160	不适用	mbms_service_area	flags_srvcc
161	不适用	src_rnc_pdcp	nmbr
162	不适用	addi_trace_info	不适用
163	不适用	hop_counter	不适用
164	不适用	plmn_id	不适用
165	不适用	mbms_session_id	不适用
166	不适用	mbms_2g3g_indicator	不适用
167	不适用	enhanced_nsapi	不适用

表 36-42　　GTP 信息元素 （续）

价值	0 版本	版本 1	版本 2
168	不适用	mbms_session_duration	不适用
169	不适用	addi_mbms_trace_info	不适用
170	不适用	mbms_session_repetition_num	不适用
171	不适用	mbms_time_to_data	不适用
173	不适用	bss	不适用
174	不适用	cell_id	不适用
175	不适用	pdu_num	不适用
177	不适用	mbms_bearer_capab	不适用
178	不适用	rim_routing_disc	不适用
179	不适用	list_pfc	不适用
180	不适用	ps_xid	不适用
181	不适用	ms_info_change_report	不适用
182	不适用	direct_tunnel_flags	不适用
183	不适用	correlation_id	不适用
184	不适用	bearer_control_mode	不适用
185	不适用	mbms_flow_id	不适用
186	不适用	mbms_ip_multicast	不适用
187	不适用	mbms_distribution_ack	不适用
188	不适用	reliable_inter_rat_handover	不适用
189	不适用	rfsp_index	不适用
190	不适用	fqdn	不适用
191	不适用	evolved_allocation1	不适用
192	不适用	evolved_allocation2	不适用
193	不适用	extended_flags	不适用
194	不适用	uci	不适用
195	不适用	csg_info	不适用
196	不适用	csg_id	不适用
197	不适用	cmi	不适用
198	不适用	apn_ambr	不适用
199	不适用	ue_network	不适用
200	不适用	ue_ambr	不适用
201	不适用	apn_ambr_nsapi	不适用
202	不适用	ggsn_backoff_timer	不适用
203	不适用	signalling_priority_indication	不适用
204	不适用	signalling_priority_indication_nsapi	不适用
205	不适用	high_bitrate	不适用

表 36-42　GTP 信息元素 （续）

价值	0 版本	版本 1	版本 2
206	不适用	max_mbr	不适用
251	charging_gateway_addr	charging_gateway_addr	不适用
255	private_extension	private_extension	private_extension

可以按照以下步骤指定 GTP 信息元素。

要指定 GTP 信息元素，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **gtp_info** 并点击 **Add Option**。

系统将显示 `gtp_info` 关键字。

步骤 2　为信息元素指定一个已定义的十进制值 （0 到 255）或者一个已定义的字符串。有关系统识别出的值和字符串，请参阅 GTP 信息元素表。

Modbus 关键字

许可证：保护

可以使用 Modbus 关键字指向 Modbus 请求或响应中 Data 字段的开头，以匹配 Modbus 函数代码和 Modbus 单元 ID。可以单独使用 Modbus 关键字，也可以将它与其他关键字（例如 `content` 和 `byte_jump` 关键字）结合使用。

有关详细信息，请参阅以下各节：

- 第 36-68 页上的 modbus_data
- 第 36-69 页上的 modbus_func
- 第 36-70 页上的 modbus_unit

modbus_data

可以使用 `modbus_data` 关键字指向 Modbus 请求或响应中 Data 字段的开头。

要指向 Modbus Data 字段的开头，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **modbus_data** 并点击 **Add Option**。

系统将显示 `modbus_data` 关键字。

`modbus_data` 关键字没有参数。

modbus_func

可以使用 `modbus_func` 关键字来匹配 Modbus 应用层请求或响应报头中的 Function Code 字段。可以为 Modbus 函数代码指定一个已定义的十进制值或一个已定义的字符串。

下表列出了系统识别出的为 Modbus 函数代码定义的值和字符串。

表 36-43　　Modbus 函数代码

价值	字符串
1	read_coils
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
6	write_single_register
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

要指定 Modbus 函数代码，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **modbus_func** 并点击 **Add Option**。

系统将显示 `modbus_func` 关键字。

步骤 2　为函数代码指定一个已定义的十进制值 （0 到 255）或者一个已定义的字符串。有关系统识别出的值和字符串，请参阅 Modbus 函数代码表。

modbus_unit

可以使用 modbus_unit 关键字来匹配 Modbus 请求或响应报头中的 Unit ID 字段。

要指定 Modbus 单元 ID，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **modbus_unit** 并点击 **Add Option**。

系统将显示 modbus_unit 关键字。

步骤 2　指定一个 0 到 255 之间的十进制值。

DNP3 关键字

许可证：保护

DNP3 关键字可用于以下目的：指向应用层分片的开头；匹配 DNP3 响应和请求中的 DNP3 函数代码和函数对象；以及匹配 DNP3 响应中的内部指示标志。可以单独使用 DNP3 关键字，也可以将它与其他关键字（例如 content 和 byte_jump 关键字）结合使用。

有关详细信息，请参阅以下各节：

- 第 36-70 页上的 dnp3_data
- 第 36-70 页上的 dnp3_func
- 第 36-72 页上的 dnp3_ind
- 第 36-73 页上的 dnp3_obj

dnp3_data

可以使用 dnp3_data 关键字指向重组 DNP3 应用层分片的开头。

DNP3 预处理器将链路层帧重组到应用层分片中。dnp3_data 关键字指向每个应用层分片的开头；其他规则选项可匹配分片中的重组数据，而无需每 16 个字节分隔数据并添加校验和。

要指向重组 DNP3 分片的开头，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **modbus_data** 并点击 **Add Option**。

系统将显示 dnp3_data 关键字。

dnp3_data 关键字没有参数。

dnp3_func

可以使用 dnp3_func 关键字来匹配 DNP3 应用层请求或响应报头中的 Function Code 字段。可以为 DNP3 函数代码指定一个已定义的十进制值或一个已定义的字符串。

下表列出了系统识别出的为 DNP3 函数代码定义的值和字符串。

表 36-44　DNP3 函数代码

价值	字符串
0	confirm
1	read
2	write
3	选择
4	operate
5	direct_operate
6	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
14	warm_restart
15	initialize_data
16	initialize_appl
17	start_appl
18	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time
25	open_file
26	close_file
27	delete_file
28	get_file_info
29	authenticate_file
30	abort_file
31	activate_config
32	authenticate_req
33	authenticate_err
129	效率低下

表 36-44　DNP3 函数代码 （续）

价值	字符串
130	unsolicited_response
131	authenticate_resp

要指定 DNP3 函数代码，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **dnp3_func** 并点击 **Add Option**。

系统将显示 dnp3_func 关键字。

步骤 2　为函数代码指定一个已定义的十进制值 （0 到 255）或者一个已定义的字符串。有关系统识别出的值和字符串，请参阅 DNP3 函数代码表。

dnp3_ind

可以使用 dnp3_ind 关键字来匹配 DNP3 应用层响应报头中 Internal Indications 字段中的标志。

可以为一个已知标志指定一个字符串，也可以指定以逗号分隔的标志列表，如以下示例所示：

```
class_1_events, class_2_events
```

如果指定多个标志，此关键字将会匹配列表中的任何标志。要检测标志组合，可在一个规则中多次使用 dnp3_ind 关键字。

以下列表提供了系统识别出的用于已定义的 DNP3 内部指示标志的字符串语法。

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
reserved_2
reserved_1
```

要指定 DNP3 内部指示标志，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **dnp3_ind** 并点击 **Add Option**。

系统将显示 dnp3_ind 关键字。

步骤 2　可以为一个已知标志指定一个字符串，也可以指定以逗号分隔的标志列表。

dnp3_obj

可以使用 dnp3_obj 关键字来匹配请求或响应中的 DNP3 对象报头。

DNP3 数据由一系列不同类型的 DNP3 对象组成，例如模拟输入、二进制输入，等等。每种类型均以*组*进行识别，例如模拟输入组、二进制输入组等，每个组均可由一个十进制值进行识别。每个组中的对象均以*对象变体*进一步识别，例如 16 位整数、 32 位整数、短浮点等，每个这些变体均指定对象的数据格式。每种类型的对象变体也可以十进制值进行识别。

可以通过为对象报头组和类型和对象变体类型分别指定一个十进制数值来识别对象报头。这两种类型的组合可定义特定类型的 DNP3 对象。

要指定 DNP3 对象的指定，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **dnp3_obj** 并点击 **Add Option**。

系统将显示 dnp3_obj 关键字。

步骤 2　指定一个 0 到 255 之间的十进制值来识别已知对象组，并指定另一个 0 到 255 之间的十进制值来识别已知对象变体类型。

检查数据包特征

许可证：保护

可以编写只针对具有特定特征的数据包生成事件的规则。 FireSIGHT 系统提供以下关键字来评估数据包特征：

- 第 36-73 页上的 dsize
- 第 36-74 页上的 isdataat
- 第 36-74 页上的 sameip
- 第 36-74 页上的 fragoffset
- 第 36-75 页上的 cvs

dsize

许可证：保护

dsize 关键字测试数据包负载的大小。使用此关键字时，可以用大于号和小于号 （< 和 >）指定值的范围。可以使用以下语法来指定范围：

>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes

例如，要表示大于 400 字节的数据包大小，请使用 >400 作为 dtype 值。要表示小于 500 字节的数据包大小，请使用 <500。要规定规则应对介于 400 到 500 字节（包含 400 和 500 字节）的任何数据包触发，请使用 400<>500。

注意事项　dsize 关键字测试未经任何预处理器解码的数据包。

isdataat

许可证：保护

isdataat 关键字指示规则引擎验证数据是否驻留在负载中的特定位置。

下表列出了可与 isdataat 关键字配合使用的参数。

表 36-45　isdataat 参数

参数	类型	说明
Offset	必填	负载中的特定位置。例如，要测试显示在数据包中字节 50 处的数据，需要指定 50 作为偏移量值。A ! 修饰符否定 isdataat 测试的结果；如果负载中不存在一定数量的数据，此修饰符将会发出警报。 还可以使用现有 byte_extract 变量指定此参数的值。有关详情，请参见第 36-75 页上的将数据包数据读取到关键字参数中。
Relative	可选	使位置相对于上一次成功内容匹配。指定相对位置时请注意，计数器从字节 0 开始计算，因此，应该如下计算相对位置：用从上一次成功内容匹配起向前计算所需的字节数减去 1。例如，要指定数据必须显示在上一次成功内容匹配后的第九个字节处，需要将相对偏移量指定为 8。
Raw Data	可选	指定数据在由任何 FireSIGHT 系统预处理器进行解码或规范化之前位于原始数据包负载中。如果上一次内容匹配出现在原始数据包数据中，可以将此参数与 **Relative** 结合使用。

例如，在查找内容 foo 的规则搜索中，如果如下指定 isdataat 的值：

- Offset = !10
- Relative 已启用

那么，如果规则引擎在负载结束前未能在 foo 之后检测到 10 字节，系统将会发出警报。

要使用 isdataat，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 isdataat 并点击 **Add Option**。

系统将显示 isdataat 部分。

sameip

许可证：保护

sameip 关键字测试数据包的源 IP 地址和目标 IP 地址是否相同。此关键字没有参数。

fragoffset

许可证：保护

fragoffset 关键字测试分片数据包的偏移量。由于某些漏洞 （例如， WinNuke 拒绝服务攻击）使用手动生成的具有特定偏移量的数据包分片，因此，此关键字很有用。

例如，要测试分片数据包的偏移量是否为 31337 字节，应指定 31337 作为 fragoffset 的值。

为 fragoffset 关键字指定参数时，可以使用以下运算符。

表 36-46　fragoffset 关键字参数运算符

运算符	说明
!	不会
>	大于
<	小于

请注意，不能将 not (!) 运算符与 < 或 > 结合使用。

CVS

许可证：保护

cvs 关键字测试并发版本系统 (CVS) 流量中是否存在格式不正确的 CVS 条目。攻击者可以使用格式不正确的条目来强制堆溢出，并且在 CVS 服务器上执行恶意代码。此关键字可用于识别针对两种已知 CVS 漏洞的攻击：CVE-2004-0396 （CVS1.11.x 至 1.11.15，以及 CVS1.12.x 至 1.12.7）和 CVS-2004-0414（CVS1.12.x 至 1.12.8，以及 CVS1.11.x 至 1.11.16）。cvs 关键字检查格式正确的记录，如果检测到格式不正确的条目，将会发出警报。

规则应包含 CVS 运行所在的端口。此外，应将任何可能出现流量的端口添加到 TCP 策略的数据流重组端口列表，以便为 CVS 会话维护状态。 TCP 端口 2401 (pserver) 和 514 (rsh) 包含在出现数据流重组的客户端端口列表中。但请注意，如果服务器作为 xinetd 服务器 （即， pserver）运行，它可以在任何 TCP 端口上运行。应将任何非标准端口添加到数据流重组 **Client Ports** 列表中。有关详细信息，请参阅第 29-23 页上的选择数据流重组选项。

要检测格式不正确的 CVS 条目，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　将 cvs 选项作为关键字参数添加到规则和类型 invalid-entry。

将数据包数据读取到关键字参数中

许可证：保护

可以使用 byte_extract 将数据包中指定数量的字节读取到某个变量中。然后，可以在同一规则中使用该变量作为某些其他检测关键字中特定参数的值。

此参数很有用，例如，可用于从其中的特定字节段描述数据包数据所包含的字节数的数据包提取数据大小。例如，特定字节段可能指出后续数据是由 4 个字节组成；您可以提取 4 个字节的数据大小来作为变量值。

可以使用 byte_extract 在规则中最多同时创建两个独立的变量。可以任意多次地重新定义 byte_extract 变量；如果输入变量名称相同但变量定义不同的新的 byte_extract 关键字，将会覆盖该变量的上一个定义。

下表介绍了 byte_extract 关键字所需的参数。

表 36-47　所需的 byte_extract 参数

参数	说明
Bytes to Extract	要从数据包提取的字节数。可以指定 1、 2、 3 或 4 字节。
Offset	从负载开头到开始提取数据之间的字节数。可指定 -65534 到 65535 字节。偏移量计数器从字节 0 开始计数，因此，计算偏移量值时，应该用向前计算所需的字节数减去 1。例如，指定 7 将会从 8 字节开始向前计算。规则引擎会从数据包负载起点开始向前计算；如果还指定了 **Relative**，规则引擎会从上一次成功内容匹配起向前计算。请注意，如果还指定了 **Relative**，只能指定负数；有关详细信息，请参阅其他可选的 byte_extract 参数表。
Variable Name	用于其他检测关键字的参数中的变量名称。可以指定以字母开头的字母数字字符串。

要进一步定义系统如何查找要提取的数据，可以使用下表中所述的参数。

表 36-48　其他可选的 byte_extract 参数

参数	说明
倍数	从数据包提取的值的乘数。可指定 0 到 65535 之间的任意数字。如果未指定乘数，将会默认设置为 1。
调整	将提取的数值四舍五入为最接近的 2 字节或 4 字节边界。如果选择了 **Multiplier**，系统会在进行舍入之前应用该乘数。
Relative	使**偏移量**相对于上一次成功内容匹配的结尾而不是负载起点。有关详细信息，请参阅所需的 byte_extract 参数表。

只能指定 **DCE/RPC**、 **Endian** 或 **Number Type**。

要定义 byte_extract 关键字如何计算其测试的字节，可以从下表中选择参数。如果未选择任何参数，规则引擎将采用大端字节顺序。

表 36-49　字节顺序 byte_extract 参数

参数	说明
Big Endian	按大端字节顺序处理数据 （大端字节顺序是默认的网络字节顺序）。
Little Endian	按小端字节顺序处理数据
DCE/RPC	指定 DCE/RPC 预处理器处理的流量的 byte_extract 关键字。有关详情，请参见第 27-2 页上的解码 DCE/RPC 流量。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序， **Number Type** 和 **Endian** 参数不适用。 如果启用此参数，还可以将 byte_extract 与其他特定 DCE/RPC 关键字结合使用。有关详情，请参见第 36-54 页上的 DCE/RPC 关键字。

可以指定数字类型来将数据读取为 ASCII 字符串。要定义系统如何在数据包中查看字符串，可选择下表中所述的其中一个参数。

表 36-50　数字类型 byte_extract 参数

参数	说明
Hexadecimal String	以十六进制格式读取提取的字符串数据。
Decimal String	以十进制格式读取提取的字符串数据。
Octal String	以八进制格式读取提取的字符串数据。

例如，如果如下指定 `byte_extract` 的值：

- Bytes to Extract = 4
- Variable Name = var
- Offset = 8
- Relative 已启用

那么，规则引擎将会距离 （相对于）上一次成功内容匹配 9 字节的四个字节中描述的数字读取到名为 `var` 的变量中 （然后，您可以将该数字指定为某些关键字参数的值）。

下表列出了可以在其中指定 `byte_extract` 关键字中定义的变量的关键字参数。

表 36-51　接受 byte_extract 变量的参数

关键字	参数	有关详细信息，请参阅.....
content	Depth、 Offset、 Distance、 Within	第 36-16 页上的限制内容匹配
byte_jump	Offset	第 36-28 页上的 byte_jump
byte_test	Offset、 Value	第 36-30 页上的 byte_test
isdataat	Offset	第 36-74 页上的 isdataat

要使用 byte_extract，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 `byte_extract` 并点击 **Add Option**。

`byte_extract` 部分将显示在上次选择的关键字下方。

使用规则关键字发起活动响应

许可证：保护

系统可以发起活动响应，以在响应触发的 TCP 规则时关闭 TCP连接，或者在响应触发的 UDP 规则时关闭 UDP 会话。有两个关键字提供了两种不同的活动响应发起方法。如果数据包触发包含这两个关键字当中的任何一个，系统将发起单一活动响应。您还可以使用 `config response` 命令配置要使用的活动响应接口以及要在被动部署中尝试的 TCP 重置次数。

活动响应在内联部署中最有效，因为重置更有可能及时到达以影响连接或会话。例如，在内联部署中对 `react` 关键字作出响应时，系统会为连接的两端将 TCP 重置 (RST) 数据包直接插入到流量中 （正常情况下，这样应该会关闭连接）。

出于一些原因，活动响应并不用于取代防火墙；这些原因包括：系统不能在被动部署中插入数据包；攻击者可能已选择忽略或绕过活动响应。

由于活动响应可以回送，因此，系统不允许 TCP 重置发起 TCP 重置；这样可防止活动响应出现无穷尽的顺序。此外，为了符合标准做法，系统也不允许 ICMP 不可达数据包发起 ICMP 不可达数据包。

可以配置 TCP 数据流预处理器，使它在入侵规则触发了活动响应后检测连接或会话的其他流量。如果预处理器检测到其他流量，它会将指定最大数量的其他活动响应发送到连接或会话的两端。有关详情，请参见第 29-3 页上的使用入侵丢弃规则启动活动响应。

有关可用于发起活动响应的关键字的信息，请参阅以下各节：

- 第 36-78 页上的按类型和方向发起主动响应
- 第 36-79 页上的在 TCP 重置之前发送 HTML 页面
- 第 36-80 页上的设置活动响应重置尝试次数和界面

按类型和方向发起主动响应

许可证：保护

可以使用 `resp` 关键字来主动响应 TCP 连接或 UDP 会话，具体取决于在规则报头中指定的是 TCP 还是 UDP 协议。有关详情，请参见第 36-4 页上的指定协议。

使用关键字参数可指定数据包方向，以及指定是使用 TCP 重置 (RST) 数据包还是 ICMP 不可达数据包作为活动响应。

可以使用任何 TCP 重置或 ICMP 不可达参数来关闭 TCP 连接。只能使用 ICMP 不可达参数来关闭 UDP 会话。

此外，不同的 TCP 重置参数使得可以将数据包源和/或目标作为活动响应的目标。所有 ICMP 不可达参数都将数据包源作为目标，并且允许指定是使用 ICMP 网络、主机还是端口的不可达数据包，还是同时使用这三者的不可达数据包。

下表列出了可与 `resp` 关键字配合使用以指定您希望 FireSIGHT 系统在规则触发时会采取的操作的参数。

表 36-52　　resp 参数

参数	说明
reset_source	将 TCP 重置数据包引至发送触发规则的数据包的终端。此外，可以指定 `rst_snd`（为了获得向后兼容性，仍支持使用此参数）。
reset_dest	将 TCP 重置数据包引至触发规则的数据包的预期目标终端。此外，可以指定 `rst_rcv`（为了获得向后兼容性，仍支持使用此参数）。
reset_both	将 TCP 重置数据包引至发送终端和接收终端。此外，可以指定 `rst_all`（为了获得向后兼容性，仍支持使用此参数）。
icmp_net	将 ICMP 网络不可达消息引至发送方。
icmp_host	将 ICMP 主机不可达消息引至发送方。
icmp_port	将 ICMP 端口不可达消息引至发送方。此参数用于终止 UDP 流量。
icmp_all	将以下 ICMP 消息引至发送方： • 网络不可达消息 • 主机不可达消息 • 端口不可达消息

例如，要将规则配置为会在规则触发时重置连接的两端，可使用 reset_both 作为 resp 关键字的值。

可以使用逗号分隔列表指定多个参数，如下所示：

argument,argument,argument

关于使用 config response 命令配置用以使用的主动响应界面和试图在被动部署中进行的 TCP 重新设定数的详细信息，请参阅第 36-80 页上的设置活动响应重置尝试次数和界面。

要指定活动响应，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **resp** 并点击 **Add Option**。

系统将显示 resp 关键字。

步骤 2　在 **resp** 字段中指定 resp 参数表中所述的任意参数；使用逗号分隔列表可指定多个参数。

在 TCP 重置之前发送 HTML 页面

许可证：保护

如果数据包触发规则，您可以使用 react 关键字将默认 HTML 页面发送到 TCP 连接客户端；发送 HTML 页面后，系统将使用 TCP 重置数据包来发起对连接两端的活动响应 react 关键字不会对 UDP 流量触发活动响应。

或者，可以指定以下参数：

msg

如果数据包触发使用 msg 参数的 react 规则， HTML 页面将包含规则事件消息。关于事件消息字段的说明，请参阅第 36-2 页上的了解规则结构。

如果未指定 msg 参数， HTML 页面将包含以下消息：

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

注　由于活动响应可以回送，因此，请确保 HTML 响应页面不会触发 react 规则；否则，可能会导致活动响应出现无穷尽的顺序。思科建议您将 react 规则用于生产环境之前，先广泛测试这些规则。

关于使用 config response 命令配置用以使用的主动响应界面和试图在被动部署中进行的 TCP 重新设定数的详细信息，请参阅第 36-80 页上的设置活动响应重置尝试次数和界面。

要在发起活动响应之前发送 HTML 页面，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **react** 并点击 **Add Option**。

系统将显示 react 关键字。

步骤 2　您有两种选择：

- 要在关闭连接之前将包含为规则配置的事件消息的 HTML 页面发送到客户端，请在 **react** 字段中键入 msg。
- 要在关闭连接之前将包含以下默认消息的 HTML 页面发送到客户端，请将 **react** 字段留空：

```
You are attempting to access a forbidden site.
Consult your system administrator for details
```

设置活动响应重置尝试次数和界面

许可证：保护

可以使用 **config response** 命令进一步配置由 `resp` 和 `react` 规则发起的 TCP 重置的行为。此命令还会影响丢弃规则发起的活动响应的行为；有关详细信息，请参阅第 29-3 页上的使用入侵丢弃规则启动活动响应。

要使用 **config response** 命令，可以在 USER_CONF 高级变量中的单独一行插入此命令。有关使用 USER_CONF 变量的详细信息，请参阅第 3-28 页上的了解高级变量。

注意事项 请勿使用高级变量 `USER_CONF` 来配置入侵策略功能，除非功能描述或支持人员指示您这样做。存在冲突或重复的配置会导致系统停止。

要指定活动响应重置尝试次数和/或活动响应界面，请执行以下操作：

访问：管理员/入侵管理员

步骤 1 在 USER_CONF 高级变量中的单独一行插入 `config response` 命令的一种形式，具体取决于您是要仅指定活动响应重置尝试次数、仅指定活动响应界面还是要同时指定这两者。有以下选项可供选择：

- 要仅指定活动响应重置尝试次数，请插入以下命令：
  `config response: attempts att`

  例如：`config response: attempts 10`
- 要仅指定活动响应界面，请插入以下命令：
  `config response: device dev`

  例如：`config response: device eth0`
- 要指定活动响应重置尝试次数和活动响应界面，请插入以下命令：
  `config response: attempts att, device dev`

  例如：`config response: attempts 10, device eth0`

  其中：

  att 是尝试次数 （1 到 20），每个 TCP 重置数据包在达到指定的尝试次数后，就会停留在当前连接窗口，以使接收主机接受该数据包。这种*扫射式*序列仅对被动部署有用；在内联部署中，系统会将重置数据包直接插入到数据流中，而不是触发数据包。系统只发送 1 个 ICMP 可达活动响应。

  dev 备用接口，您希望系统在被动部署中使用该接口发送活动响应，或者在内联部署中在该接口处插入活动响应。

过滤事件

许可证：保护

可以使用 `detection_filter` 关键字来防止某个规则生成事件，除非在指定时间内有指定数量的数据包触发该规则。这样可防止规则过早生成事件。例如，在几秒钟内登录失败两三次可能是预期行为，但在同一时间内出现大量登录尝试可能表示存在蛮力攻击。

`detection_filter` 关键字需要使用参数来定义系统是否跟踪源或目标 IP 地址、满足检测条件多少次后才会触发事件以及持续计数多长时间。

可使用以下语法延迟事件触发：

```
track by_src/by_dst, count count, seconds number_of_seconds
```

track 参数指定在计算符合规则检测条件的数据包数量时，是否使用数据包的源或目标 IP 地址。可选择下表中所述的参数值来指定系统如何跟踪事件实例。

表 36-53　detection_filter 跟踪参数

参数	说明
by_src	按源 IP 地址计算检测条件。
by_dst	按目标 IP 地址计算检测条件。

count 参数指定要使某个规则生成事件，在指定时间内必须有多少数据包为指定 IP 地址触发该规则。

seconds 参数指定要使某个规则生成事件，必须在多少秒内有指定数量的数据包触发该规则。

假设某个规则在数据包中搜索内容 foo，并将以下参数与 detection_filter 关键字配合使用：

```
track by_src, count 10, seconds 20
```

在此示例中，规则在 20 秒内从来自给定 IP 地址的 10 个数据包中检测到 foo 后才会生成事件。如果系统在头 20 秒内仅检测到有 7 个数据包包含 foo，将不会生成事件。但是，如果在头 20 秒内 foo 出现 40 次，规则将会生成 30 个事件，并在 20 秒后再次进行计数。

比较 threshold 和 detection_filter 关键字

detection_filter 关键字取代已被弃用的 threshold 关键字。但是，为了获得向后兼容性，仍支持使用 threshold 关键字，其作用与您在入侵策略中设置的阈值相同。

detection_filter 关键字是一种检测功能，适合在数据包触发规则前使用。在达到指定的数据包数量之前，规则不会针对触发检测到的数据包生成事件；在内联部署中，如果规则设置为丢弃数据包，在达到指定的数据包数量之前，规则不会丢弃数据包。相反，规则会针对会触发规则且在达到指定数据包数量后出现的数据包生成事件；在内联部署中，如果规则设置为丢弃数据包，规则将会丢弃数据包。

阈值是一种事件通知功能，不会造成检测操作。此功能适合在数据包触发事件后使用。在内联部署中，被设置为丢弃数据包的规则将会丢弃触发其本身的所有数据包，无论规则阈值如何。

请注意，可以在入侵策略中使用使用 detection_filter 关键字与入侵事件阈值、入侵事件抑制和基于速率的攻击防御等功能的任意组合。另请注意，如果启用某个导入的本地规则，而该规则将弃用的 threshold 关键字与某个入侵策略中的入侵事件阈值功能结合起来使用，策略验证将会失败。有关详细信息，请参阅第 32-20 页上的配置事件阈值、第 32-24 页上的按入侵策略配置抑制、第 32-27 页上的设置动态规则状态和第 66-17 页上的导入本地规则文件。

评估攻击后流量

许可证：保护

使用 tag 关键字可指示系统记录主机或会话的其他流量。使用 tag 关键字指定要捕获的流量的类型和数量时，可使用以下语法：

```
tagging_type, count, metric, optional_direction
```

以下三个表介绍了其他可用参数。

有两种标记类型可供选择。下表介绍了这两种标记类型。请注意，如果您在入侵规则中仅配置规则报头选项，会话标记参数类型会使系统像记录来自不同会话的数据包一样来记录来自同一个会话的数据包。要对自同一个会话的数据包进行分组，请在同一入侵规则中配置一个或多个规则选项（例如，flag 关键字或 content 关键字）。

表 36-54　标记参数

参数	说明
会话	记录触发规则的会话中的数据包。
主机	记录来自发送触发规则的数据包的主机的数据包。可以添加方向修饰符，以仅记录来自主机 (src) 或发送到主机 (dst) 的流量。

要指明想要记录的流量数量，请使用以下参数：

表 36-55　计数参数

参数	说明
count	您想在规则触发后记录的数据包数量或秒数。 此度量单位用指标参数指定 （该参数跟在计数参数后面）。

选择下表中所述的其中一个指标，以指明是要按时间还是流量数量进行记录。

注意事项　高带宽网络可以每秒查看成千上万个数据包，而且对大量数据包进行标记可能会严重影响性能，因此，请务必根据网络环境调整设置。

表 36-56　记录指标参数

参数	说明
数据包	在规则触发后记录计数指定的数量的数据包。
秒	在规则触发后在计数指定的秒数内记录流量。

例如，如果带有以下 tag 关键字值的规则触发：

```
host, 30, seconds, dst
```

将会记录在接下来的 30 秒内从客户端传输到主机的所有数据包。

检测跨越多个数据包的攻击

许可证：保护

可以使用 flowbits 关键字为会话分配状态名称。通过根据之前命名的状态分析会话中的后续数据包，系统可以检测在一个会话中跨越多个数据包的攻击，并发出有关警报。

flowbits 状态名称是用户定义的标签，将被分配给会话特定部分中的数据包。可以根据数据包内容给数据包分配状态名称标签，以帮助将恶意数据包和那些您不想对其发出警报的数据包区分开。最多可以为每个受管设备定义 1024 个状态名称。例如，如果要对您知道仅在成功登录后才会出现的恶意数据包发出警报，可以使用 flowbits 关键字过滤掉构成初始登录尝试的数据包，这样就能够重点关注恶意数据包。要这样做，首先要创建一个会给具有状态为 logged_in 的已建立登录的会话中的所有数据包分配标签的规则，然后创建另一个包含 flowbits 的规则，用以检查具有您在第一个规则中设置的状态的数据包，并且只对这些数据包采取操作。有关使用 flowbits 来确定用户是否已登录的示例，请参阅第 36-84 页上的使用 state_name 的 flowbits 示例。

可选的*组名称*用于向状态组添加状态名称。一个状态名称可以属于若干个组。未与组关联的状态并不相互排斥，因此，触发和设置未与组关联的状态的规则不会影响其他同时设置的状态。有关在组中包含状态名称可如何防止误报的示例 （通过取消设置同一个组中的另一个状态），请参阅第 36-85 页上的导致误报的 flowbits 示例。

下表介绍了可用于 `flowbits` 关键字的运算符、状态和组的各种组合。请注意，状态名称可以包含字母数字字符、句号 (.)、下划线 (_) 和破折号 (-)。

表 36-57　　flowbits 选项

运算符	状态选项	组	说明
set	state_name	可选	为数据包设置某个指定状态。如果定义了某个组，则在该指定的组中设置该状态。
	state_name&state_name	可选	为数据包设置多个指定状态。如果定义了某个组，则在该指定的组中设置这些状态。
setx	state_name	必需	为数据包在指定组中设置某个指定状态，并取消设置该组中的所有其他状态。
	state_name&state_name	必需	为数据包在指定组中设置多个指定状态，并取消设置该组中的所有其他状态。
unset	state_name	没有组	为数据包取消设置某个指定状态。
	state_name&state_name	没有组	为数据包取消设置多个指定状态。
	全部	必需	取消设置指定组中的所有状态。
toggle	state_name	没有组	取消设置某个指定状态 （如果已设置），以及设置某个指定状态 （如果未设置）。
	state_name&state_name	没有组	取消设置多个指定状态 （如果已设置），以及设置多个指定状态 （如果未设置）。
	全部	必需	取消设置指定组中已设置的所有状态，以及设置指定组中未设置的所有状态。
isset	state_name	没有组	确定是否已在数据包中设置了某个指定状态。
	state_name&state_name	没有组	确定是否已在数据包中设置了多个指定状态。
	state_name|state_name	没有组	确定是否已在数据包中设置了任何指定状态。
	any	必需	确定是否已在指定组中设置了任何状态。
	全部	必需	确定是否已在指定组中设置了所有状态。
isnotset	state_name	没有组	确定是否未在数据包中设置某个指定状态。
	state_name&state_name	没有组	确定是否未在数据包中设置多个指定状态。
	state_name|state_name	没有组	确定是否未在数据包中设置任何指定状态。
	any	必需	确定是否未在数据包中设置任何状态。
	全部	必需	确定是否未在数据包中设置所有状态。
重置	（无状态）	可选	为所有数据包取消设置所有状态。取消设置某个组中的所有状态 （如果已指定该组）。
noalert	（无状态）	没有组	可将此运算符与任何其他运算符结合使用，以抑制事件生成。

使用 flowbits 关键字时，请注意：

- 使用 setx 运算符时，指定的状态只能属于指定的组，而不能属于任何其他组。
- 可以多次定义 setx 操作符，每次用一个实例指定不同的状态和同一个组。
- 如果使用 setx 运算符并指定了某个组，则不能对该指定的组使用 set、toggle 或 unset 运算符。
- isset 和 isnotset 运算符会对指定状态进行评定，无论该状态是否在组中。
- 保存入侵策略、重新应用入侵策略以及应用访问控制策略时 （不管访问控制策略是引用一个入侵策略还是多个入侵策略），如果您启用包含**未**指定组的 isset 或 isnotset 运算符的一个规则，而且您不会为对应的状态名称和协议启用至少一个会影响 flowbits 分配的规则 （set、setx、set、toggle），那么，将会启用会影响对应状态名称的 flowbits 分配的所有规则。
- 保存入侵策略、重新应用入侵策略以及应用访问控制策略时 （不管访问控制策略是引用一个入侵策略还是多个入侵策略），如果您启用包含**已**指定组的 isset 或 isnotset 运算符的一个规则，系统还将会启用会影响 flowbits 分配 （set、setx、unset、toggle）且定义对应组名称的所有规则。

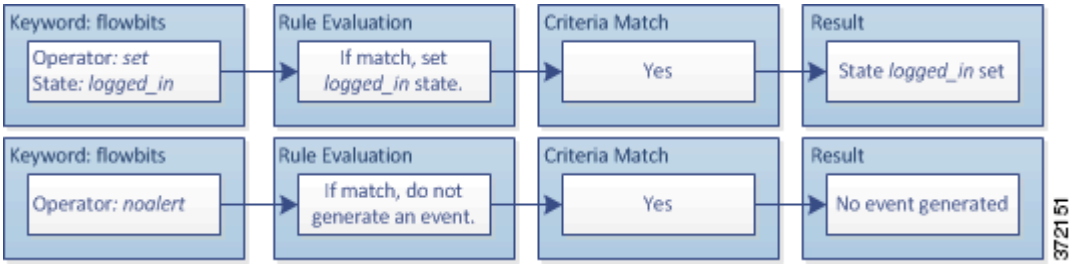
使用 state_name 的 flowbits 示例

以 Bugtraq ID #1110 中所述的 IMAP 漏洞为例。该漏洞存在于 IMAP 的实现中，尤其是在 LIST、LSUB、RENAME、FIND 和 COPY 命令中。但是，要想利用该漏洞，攻击者必须登录到 IMAP 服务器。由于来自 IMAP 服务器的登录确认及紧随着而来的漏洞必定存在于不同的数据包中，因此，难以构建非基于流量的规则来捕获该漏洞。使用 flowbits 关键字可以构建一系列规则来追踪用户是否登录到 IMAP 服务器；如果是，将会在检测到其中一项攻击时生成事件。如果用户未登录，则攻击不能利用该漏洞，且不会生成事件。

以下两个规则分片说明了此示例。第一个规则分片查找来自 IMAP 服务器的 IMAP 登录确认：

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK
LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

下图说明了上述规则分片中 flowbits 关键字的影响：

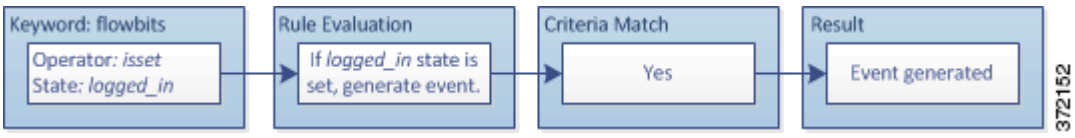


请注意， flowbits:set 设置 logged_in 状态， flowbits:noalert 则抑制警报，因为 IMAP 服务器上可能会出现许多无恶意的登录会话。

以下规则分片查找 LIST 字符串，但不生成事件，除非由于会话中某个之前的数据包而设置了 logged_in 状态：

```
alert tcp any any -> any 143 (msg:"IMAP LIST";
content:"LIST"; flowbits:isset,logged_in;)
```

下图说明了上述规则分片中 flowbits 关键字的影响：



在这种情况下，如果之前的数据包已促使包含第一个分片的规则触发，则包含第二个分片的规则将会触发并生成事件。

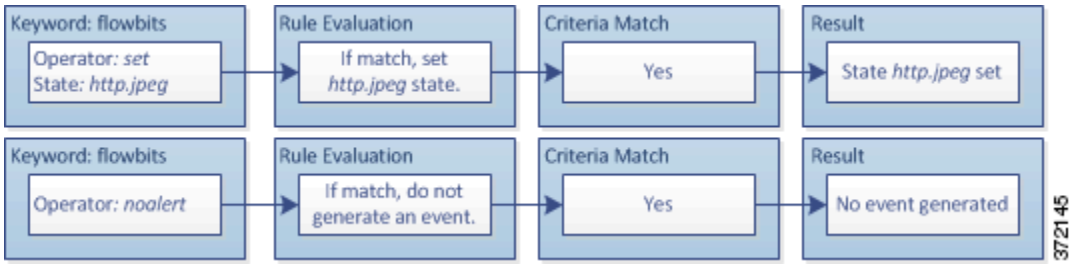
导致误报的 flowbits 示例

在一个组中包含在不同规则中设置的不同状态名称可防止误报事件；如果后续数据包中的内容与状态不再有效的规则相匹配，就会出现误报事件。以下示例说明不在一个组中包含多个状态名称如何会导致误报。

假设以下三个规则分片在一个会话中按所示的顺序触发：

```
(msg:"JPEG transfer"; content:"image/";pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
flowbits:set,http.jpeg; flowbits:noalert;)
```

下图说明了上述规则分片中 `flowbits` 关键字的影响：

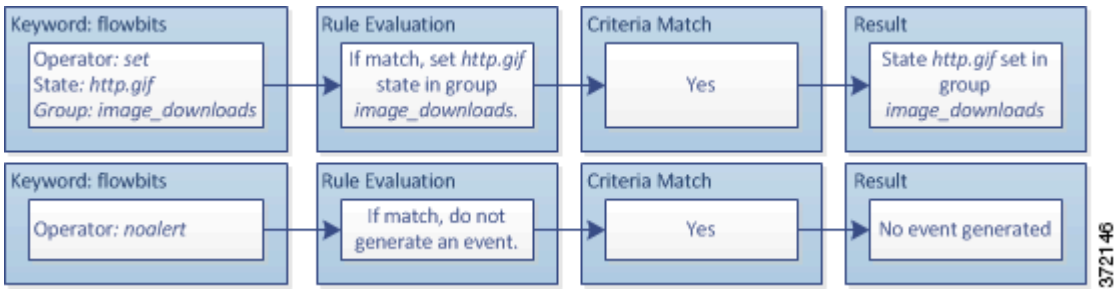


第一个规则分片中的 `content` 和 `pcre` 关键字与 JPEG 文件下载相匹配，`flowbits:set,http.jpeg` 设置 `http.jpeg flowbits` 状态，`flowbits:noalert` 使规则停止生成事件。将不会生成事件，因为该规则的目的是检测文件下载并设置 `flowbits` 状态；为此，一个或多个伴随规则可以测试状态名称和恶意内容，如果检测到恶意内容，将会生成事件。

以下规则分片检测在上述 JPEG 文件下载之后发生的 GIF 文件下载：

```
(msg:"GIF transfer"; content:"image/"; pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
flowbits:set,http.tif,image_downloads; flowbits:noalert;)
```

下图说明了上述规则分片中 `flowbits` 关键字的影响：

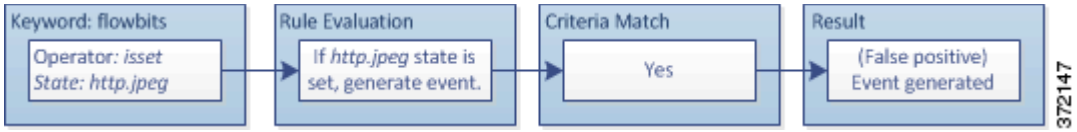


第二个规则中的 `content` 和 `pcre` 关键字与 GIF 文件下载相匹配，`flowbits:set,http.gif` 设置 `http.gif` 流位状态，`flowbits:noalert` 停止规则生成事件。请注意，仍会设置由第一个规则分片设置的 `http.jpeg` 状态，即使不再需要使用它；这是因为如果检测到后续 GIF 下载，JPEG 下载必须终止。

第三个规则分片伴随第一个规则分片出现：

```
(msg:"JPEG exploit";
flowbits:isset,http.jpeg;content:"|FF|"; pcre:"
/\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

下图说明了上述规则分片中 flowbits 关键字的影响：



在第三个规则分片中，flowbits:isset,http.jpeg 确定是否已设置现在不相关的 http.jpeg 状态，content 和 pcre 则匹配在 JPEG 文件中是恶意的但在 GIF 文件中并非恶意的内容。第三个规则分片会针对 JPEG 文件中不存在漏洞生成误报事件。

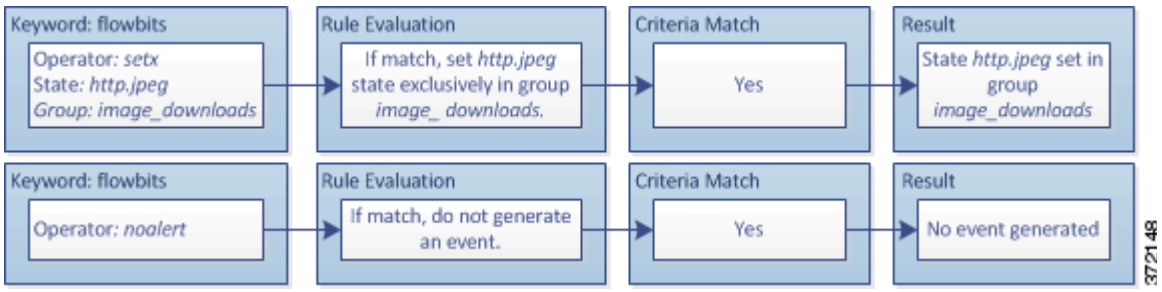
防止误报的 flowbits 示例

以下示例说明在一个组中包含多个状态名称并使用 setx 运算符如何能防止误报。

以下规则分片与上一个规则分片示例大致相同，不同之处是，以下示例的前两个规则将两个不同的状态名称包含在同一个状态组中。

```
(msg:"JPEG transfer"; content:"image/";pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

下图说明了上述规则分片中 flowbits 关键字的影响：

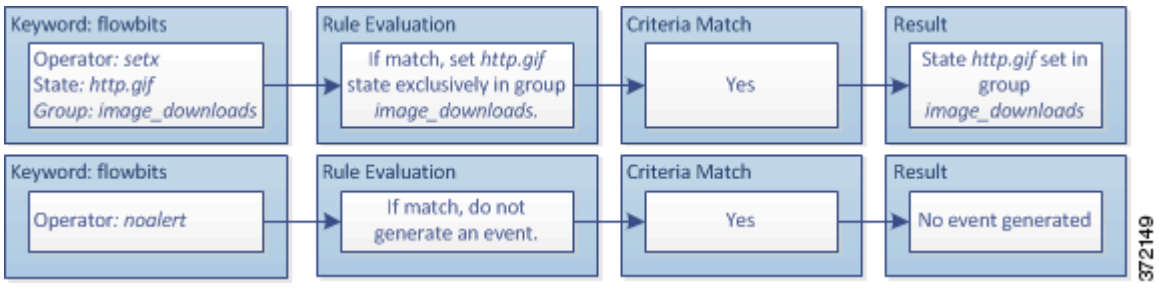


如果第一个规则分片检测到 JPEG 文件下载， flowbits:setx,http.jpeg,image_downloads 关键字会将 flowbits 状态设置为 http.jpeg，并将该状态包含在 image_downloads 组中。

然后，下一个规则会后续 GIF 文件下载：

```
(msg:"GIF transfer"; content:"image/"; pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
flowbits:setx,http.tif,image_downloads; flowbits:noalert;)
```

下图说明了上述规则分片中 flowbits 关键字的影响：

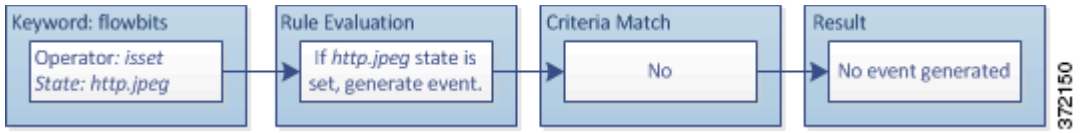


当第二个规则分片与 GIF 下载相匹配时， flowbits:setx,http.gif,image_downloads 关键字将会设置 http.gif flowbits 状态，并取消设置组中的另一个状态 http.jpeg。

第三个规则分片不会导致误报：

```
(msg:"JPEG exploit";
flowbits:isset,http.jpeg;content:"|FF|"; pcre:"/
\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

下图说明了上述规则分片中 `flowbits` 关键字的影响：



由于 `flowbits:isset,http.jpeg` 为假，因此，规则引擎会停止处理规则，且不会生成事件，从而避免误报 （即使 GIF 文件中的内容与 JPEG 文件的漏洞内容相匹配）。

生成关于 HTTP 编码类型和位置的事件

许可证：保护

可以使用 `http_encode` 关键字在未经规范化的 HTTP 请求或响应中生成关于编码类型的事件 - 可以是在 HTTP URI 中，在 HTTP 报头的非 cookie 数据中，在 HTTP 请求报头的 cookie 中，或者在 HTTP 响应的 set-cookie 数据。

必须配置 HTTP 检查预处理器以检查 HTTP 响应和 HTTP cookie，从而使用 `http_encode` 关键字返回规则的匹配项。有关详细信息，请参阅第 27-26 页上的解码 HTTP 流量和第 27-28 页上的选择服务器级别 HTTP 规范化选项。

此外，要使入侵规则中的 `http_encode` 关键字针对特定编码类型触发事件，必须在 HTTP 检查预处理器配置中为该编码类型启用解码和警报选项。有关详情，请参见第 27-35 页上的选择服务器级别的 HTTP 规范化编码选项。

请注意， base36 编码类型已被弃用。为了实现向后兼容性，允许在现有规则中使用 base36 参数，但它不会使规则引擎检查 base36 流量。

下表介绍了此选项可在 HTTP URI、报头、 cookie 和 set-cookie 中为其生成事件的编码类型。

表 36-58　HTTP_encode 编码类型

编码类型	说明
utf8	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测 UTF-8 编码。
double_encode	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测双编码。
non_ascii	如果检测到非 ASCII 字符但检测到的编码类型未启用，将会在指定位置检测非 ASCII 字符。
uencode	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测 Microsoft %u 编码。
bare_byte	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测裸字节编码。

要在入侵规则中识别 HTTP 编码类型和位置，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　向规则添加 `http_encode` 关键字。

步骤 2　从 **Encoding Location** 下拉列表中，选择是要在 HTTP URI、报头还是 cookie （包括 set-cookie）中搜索指定的编码类型。

步骤 3　使用以下其中一种格式指定一个或多个编码类型：

```
encode_type
encode_type|encode_type|encode_type...
!encode_type
```

其中， *encode_type* 是以下其中一项：

```
utf8, double_encode, non_ascii, uencode, bare_byte
```

请注意，不能同时使用否定 (!) 和 OR (|) 运算符。

步骤 4　或者，将多个 `http_encode` 关键字添加到同一个规则，并为每个关键字添加条件。例如，按照以下条件输入两个关键字：

第一个 `http_encode` 关键字：

- **Encoding Location：** `HTTP URI`
- **Encoding Type：** `utf8`

另一个 `http_encode` 关键字：

- **Encoding Location：** `HTTP URI`
- **Encoding Type：** `uencode`

此示例配置将在 HTTP URI 中搜索 UTF-8 和 Microsoft IIS %u 编码。

检测文件类型和版本

许可证：保护

`file_type` 和 `file_group` 关键字使您可以根据文件类型和版本检测通过 FTP、 HTTP、 SMTP、 IMAP、 POP3 和 NetBIOS-ssn (SMB) 发送的文件。**不能**在一个入侵规则中使用多个 `file_type` 或 `file_group` 关键字。

提示　更新漏洞数据库 (VDB) 可以使规则编辑器获得最新的文件类型、版本和组。有关详细信息，请参阅第 66-12 页上的更新漏洞数据库。

必须启用特定预处理器以生成流量与 `file_type` 或 `file_group` 关键字匹配的入侵事件。

表 36-59　file_type 和 file_group 入侵事件生成

传输协议	需要的预处理器或预处理器选项
FTP	FTP/Telnet 预处理器和**Normalize TCP Payload** 内嵌规范化预处理器选项；请参阅第 27-16 页上的解码 FTP 和 Telnet 流量和第 29-6 页上的规范化内联流量。
HTTP	HTTP 检查预处理器；请参阅第 27-26 页上的解码 HTTP 流量。

表 36-59　file_type 和 file_group 入侵事件生成

传输协议	需要的预处理器或预处理器选项
SMTP	SMTP 预处理器；请参阅第 27-51 页上的解码 SMTP 流量。
IMAP	IMAP 预处理器；请参阅第 27-45 页上的解码 IMAP 流量。
POP3	POP 预处理器；请参阅第 27-48 页上的解码 POP 流量。
NetBIOS-ssn (SMB)	**SMB File Inspection** DCE/RPC 预处理器选项；请参阅第 27-2 页上的解码 DCE/RPC 流量。

有关详细信息，请参阅以下各节：

- 第 36-89 页上的 file_type
- 第 36-89 页上的 file_group

file_type

使用 `file_type` 关键字可指定在流量中检测到的文件的类型和版本。文件类型参数（例如 **JPEG** 和 **PDF**）用于识别要在流量中查找的文件格式。

注　**不能**在同一个入侵规则中将 `file_type` 关键字与其他 `file_type` 或 `file_group` 关键字结合使用。

系统默认选择 **Any Version**，但某些文件类型允许选择版本选项（例如 PDF 版本 **1.7**）来确定要在流量中查找的特定文件类型版本。

要查看和配置最新的文件类型和版本，请更新 VDB。有关详细信息，请参阅第 66-12 页上的更新漏洞数据库。

要在入侵规则中选择文件类型和版本，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **file_type** 并点击 **Add Option**。

系统将显示 `file_type` 关键字。

步骤 2　从下拉列表中选择一个或多个文件类型。选择文件类型会自动将相应的参数添加到规则。

要从规则中移除文件类型参数，请点击要移除的文件类型旁边的删除 ( ) 图标。

步骤 3　或者，可以为每种文件类型自定义目标版本。系统默认选择 **Any Version**，但某些文件类型允许选择单个目标版本。

注　更新 VDB 可以使规则编辑器获得最新的文件类型和版本。如果选择 **Any Version**，系统将会配置规则，以包含在以后的 VDB 更新中添加的新版本。

file_group

使用 `file_group` 关键字可选择思科定义的、包含在流量中找到的类似文件类型（例如**多媒体**或**音频**）的组。文件组还包含思科为组中的每种文件类型定义的版本。

注　**不能**在同一个入侵规则中将 file_group 关键字与另一个 file_group 或 file_type 关键字结合使用。

要查看和配置最新的文件组，请更新 VDB。有关详细信息，请参阅第 66-12 页上的更新漏洞数据库。

要在入侵规则中选择文件组，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **file_group** 并点击 **Add Option**。

系统将显示 file_group 关键字。

步骤 2　或者，如果要查看某个组中文件类型的版本信息，请将指针悬停在该组上并点击 **(Show Version Info)**。

文件组信息将展开以显示版本。

步骤 3　选择要添加到规则的文件组。

指向特定负载类型

许可证：保护

file_data 关键字提供一个指针，该指针作为可用于其他关键字（例如 content、byte_jump、byte_test 和 pcre）的位置参数参考。检测到的流量确定 file_data 关键字指向的数据类型。您可以使用 file_data 关键字指向以下负载类型的开头：

- HTTP 响应正文

  要检查 HTTP 响应数据包，必须启用 HTTP 检查预处理器，还必须将该预处理器配置为会检查 HTTP 响应。有关详细信息，请参阅第 27-26 页上的解码 HTTP 流量和第 27-28 页上的选择服务器级别 HTTP 规范化选项中的 **Inspect HTTP Responses**。如果 HTTP 检查预处理器检测到 HTTP 响应正文数据， file_data 关键字将会进行匹配。

- 未压缩的 gzip 文件数据

  要检查 HTTP 响应正文中未压缩的 gzip 文件，必须启用 HTTP 检查预处理器，还必须将该预处理器配置为会检查 HTTP 响应以及会解压缩 HTTP 响应正文中的 gzip 压缩文件。有关详细信息，请参阅第 27-26 页上的解码 HTTP 流量以及第 27-28 页上的选择服务器级别 HTTP 规范化选项中的 **Inspect HTTP Responses** 和 **Inspect Compressed Data** 选项。如果 HTTP 检查预处理器在 HTTP 响应正文中检测到未压缩的 gzip 数据， file_data 关键字将会进行匹配。

- 规范化的 JavaScript

  要检查规范化的 JavaScript 数据，必须启用 HTTP 检查预处理器，还必须将该预处理器配置为检查 HTTP 响应。有关详细信息，请参阅第 27-26 页上的解码 HTTP 流量和第 27-28 页上的选择服务器级别 HTTP 规范化选项中的 **Inspect HTTP Responses**。如果 HTTP 检查预处理器在响应主体数据中检测到 JavaScript， file_data 关键字将会进行匹配。

- SMTP 负载

  要检查 SMTP 负载，必须启用 SMTP 预处理器。有关详情，请参见第 27-54 页上的配置 SMTP 解码。如果 SMTP 预处理器检测到 SMTP 数据， file_data 关键字将会进行匹配。

- SMTP、 POP 或 IMAP 流量中的编码邮件附件

  要检查 SMTP、 POP 或 IMAP 流量中的邮件附件，必须分别启用 SMTP、 POP 或 IMAP 预处理器或者启用它们的任意组合。然后，必须确保将已启用的每个预处理器配置为会对您想要解码的每种附件编码类型进行解码。可以为每个预处理器配置的附件解码选项是：**Base64 Decoding Depth**、 **7-Bit/8-Bit/Binary Decoding Depth**、 **Quoted-Printable Decoding Depth** 和 **Unix-to-Unix Decoding Depth**。有关详细信息，请参阅第 27-45 页上的解码 IMAP 流量、第 27-48 页上的解码 POP 流量和第 27-51 页上的解码 SMTP 流量。

  可以在一个规则中使用多个 `file_data` 关键字。

要指向特定负载类型的开头，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **file_data** 并点击 **Add Option**。

系统将显示 `file_data` 关键字。

`file_data` 关键字没有参数。

指向数据包负载的开头

许可证：保护

`pkt_data` 关键字提供一个指针，该指针作为可用于其他关键字 （例如 `content`、 `byte_jump`、 `byte_test` 和 `pcre`）的位置参数参考。

如果检测到规范化的 FTP、 telnet 或 SMTP 流量， `pkt_data` 关键字将指向规范化数据包负载的开头。如果检测到其他流量， `pkt_data` 关键字将指向原始 TCP 或 UDP 负载的开头。

必须启用以下规范化选项，系统才会对相应流量进行规范化以供入侵规则进行检测：

- 要规范化 FTP 流量以供检测，必须启用 FTP 和 Telnet 预处理器的 **Detect Telnet Escape codes within FTP commands** 选项；请参阅第 27-22 页上的配置服务器级别 FTP 选项。
- 要规范化 telnet 流量以供检测，必须启用 FTP 和 Telnet 预处理器的 **Normalize** telnet 选项；请参阅第 27-18 页上的了解 Telnet 选项。
- 要规范化 SMTP 流量以供检测，必须启用 SMTP 预处理器的 **Normalize** 选项；请参阅第 27-51 页上的了解 SMTP 解码。

可以在一个规则中使用多个 `pkt_data` 关键字。

要指向数据包负载的开头，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **pkt_data** 并点击 **Add Option**。

系统将显示 `pkt_data` 关键字。

`pkt_data` 关键字没有参数。

解码和检查 Base64 数据

许可证：保护

可以结合使用 `base64_decode` 和 `base64_data` 关键字，以指示规则引擎将指定数据作为 Base64 数据进行解码和检查。这可能很有用，例如，对于检查 Base64 编码 HTTP 身份验证请求报头，以及对于检查 HTTP PUT 和 POST 请求中的 Base64 编码数据。

这两个关键字对于编码和检查 HTTP 请求中的 Base64 数据尤其有用。但是，也可以将这两个关键字与像 HTTP 一样使用空格和制表符的任何协议（例如 SMTP）结合使用，以将长的报头行展开为跨越多行。如果协议中不存在这样的行展开（即为“折叠”），检查将在后面不跟有空格或制表符的任何回车符或换行符处结束。

有关详细信息，请参阅以下各节：

- 第 36-92 页上的 base64_decode
- 第 36-93 页上的 base64_data

base64_decode

许可证：保护

`base64_decode` 关键字指示规则引擎将数据包数据解码为 Base64 数据。使用可选参数可指定要解码的字节数量以及在数据中的哪个位置开始解码。

可以在一个规则中使用 `base64_decode` 关键字一次；此关键字必须位于至少一个 `base64_data` 关键字实例前面。有关详情，请参见第 36-93 页上的 base64_data。

解码 Base64 数据之前，规则引擎会将跨越多行的已折叠的长报头展开。当规则引擎遇到以下任何情况时，解码将会结束：

- 报头行结尾
- 要解码的指定字节数
- 数据包结尾

下表介绍了可与 `base64_decode` 关键字配合使用的参数。

表 36-60　可选的 base64_decode 参数

参数	说明
字节	指定要解码的字节数。如果未指定，解码将持续到报头行结尾或数据包负载结尾（以先到者为准）。可以指定非零的正值。
Offset	确定相对于数据包负载开头的偏移量，如果还指定了 **Relative**，则确定相对于当前检查位置的偏移量。可以指定非零的正值。
Relative	指定相对于当前检查位置的检查。

要解码 Base64 数据，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **base64_decode** 并点击 **Add Option**。

系统将显示 `base64_decode` 关键字。

步骤 2　或者，选择可选的 base64_decode 参数表中所述的任意参数。

base64_data

许可证：保护

base64_data 关键字提供用于检查使用 base64_decode 关键字进行解码的 Base64 数据的参考。base64_data 关键字将检查设置在解码的 Base64 数据开头开始。或者，可以随后使用可用于其他关键字的位置参数（例如 content 或 byte_test）进一步指定要检查的位置。

使用 base64_decode 关键字后，必须至少使用一次 base64_data 关键字至少一次；可以多次使用 base64_data 以返回到解码的 Base64 数据的开头。

检查 Base64 数据时，请注意：

- 不能使用快速模式匹配程序；有关详细信息，请参阅第 36-24 页上的 Use Fast Pattern Matcher。
- 如果在某个规则中以干预性 HTTP 内容参数中断 Base64 检查，必须在该规则中插入另一个 base64_data 关键字后再进一步检查 Base64 数据；有关详细信息，请参阅第 36-21 页上的 HTTP 内容选项。

要检查解码的 Base64数据，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **base64_data** 并点击 **Add Option**。

系统将显示 base64_data 关键字。

构建规则

许可证：保护

就像创建自定义标准文本规则一样，您也可以修改现有的由思科提供的标准文本规则和共享对象规则，并将所做的更改保存为新规则。请注意，对于思科提供的共享对象规则，您只能修改规则报头信息，例如，源端口、目标端口、源 IP 地址和目标 IP 地址。不能修改共享对象规则中的规则关键字和规则参数。

有关详细信息，请参阅以下各节：

- 第 36-93 页上的编写新规则
- 第 36-95 页上的修改现有规则
- 第 36-96 页上的向规则添加注释
- 第 36-97 页上的删除自定义规则

编写新规则

许可证：保护

您可以创建自己的标准文本规则。

在自定义标准文本规则中，可以设置规则报头设置、规则关键字和规则参数。或者，可以通过规则报头设置将规则设置为仅针对使用特定协议以及发往或来自特定 IP 地址或端口的流量。

创建新规则后，可以使用规则编号（其格式为 GID:SID:Rev）再次迅速找到该规则。所有标准文本规则的规则编号均以 1 开头。规则编号的第二部分（Snort ID (SID) 号）指明规则是本地规则还是由思科提供的规则。当您创建新规则时，系统会向新规则分配下一个可用于本地规则的 Snort ID 号，并将该规则保存在本地规则类别中。本地规则的 Snort ID 号从 1,000,000 开始（但在高可用性对中辅助防御中心上创建的入侵规则的 Snort ID 号从 1,000,000,000 开始），每个本地规则的 SID 号以 1 为增量。规则编号的最后一部分是修订号。对于新规则，修订号为 1。每修改一次自定义规则，修订号就增加 1。

注　系统会向您导入的入侵策略中的任何自定义规则分配一个新的 SID。有关详细信息，请参阅第 A-1 页上的导入和导出配置。

要使用规则编辑器编写自定义标准文本规则，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Rule Editor**。

系统将显示 Rule Editor 页面。

步骤 2　点击 **Create Rule**。

系统将显示 Create Rule 页面。

步骤 3　在 **Message** 字段中，输入要与事件一起显示的消息。

有关事件消息的详细信息，请参阅第 36-10 页上的定义事件消息。

提示　必须指定规则消息。此外，消息不能只包含空白字符、一个或多个引号、一个或多个撇号或者仅由空白字符、引号或撇号组成的任意组合。

步骤 4　从 **Classification** 列表中选择用以描述事件类型的分类。

有关有效分类的详细信息，请参阅第 36-11 页上的定义入侵事件分类。

步骤 5　从 **Action** 列表中选择要创建的规则的类型。可以使用以下其中一个选项：

- 选择 **alert**，将会创建在被流量触发时会生成事件的规则。
- 选择 **pass**，将会创建忽略触发自身的流量的规则。

步骤 6　从 **Protocol** 列表中选择您希望规则检查的数据包的流量协议（**tcp**、**udp**、**icmp** 或 **ip**）。

有关选择协议类型的详细信息，请参阅第 36-4 页上的指定协议。

步骤 7　在 **Source IPs** 字段中，为应触发规则的流量输入源 IP 地址或地址块。在 **Destination IPs** 字段中，为应触发规则的流量输入目标 IP 地址或地址块。

有关规则编辑器接受的 IP 地址语法的更多详细信息，请参阅第 36-5 页上的在入侵规则中指定 IP 地址。

步骤 8　在 **Source Port** 字段中，为应触发规则的流量输入发起端口号。在 **Destination Port** 字段中，为应触发规则的流量输入接收端口号。

注　如果协议设置为 ip，系统将忽略入侵规则报头中的端口定义。

有关规则编辑器接受的端口语法的更多详细信息，请参阅第 36-8 页上的在入侵规则中定义端口。

步骤 9　从 **Direction** 列表中，选择指示您希望触发规则的流量方向的运算符。可以使用以下其中一个选项：

- **Directional** 匹配从源 IP 地址流向目标 IP 地址的流量
- **Bidirectional** 从源 IP 地址流向目标 IP 地址或从目标 IP 地址流向源 IP 地址的流量

步骤 10　从 **Detection Options** 列表中选择要使用的关键字。

步骤 11　点击 **Add Option**。

步骤 12　输入要用于指定所添加的关键字的任何参数。有关规则关键字及其使用方式的详细信息，请参阅第 36-9 页上的了解规则中的关键字和参数。

添加关键字和参数时，还可以执行以下操作：

- 要对添加的关键字进行重新排序，请点击要移动的关键字旁边的向上或向下箭头。
- 要删除关键字，点击要删除的关键字旁边的 **X**。

对要添加的每个关键字选项重复第 12 至第 10 步。

步骤 13　点击 **Save As New** 保存规则。

系统会向新创建的规则分配规则编号序列中下一个可用于本地规则的 Snort ID (SID) 号，并将该规则保存在本地规则类别中。

系统不会根据新的或更改后的规则来评估流量，直至您在适当的入侵策略中启用这些规则，并将该入侵策略作为访问控制策略的一部分进行应用。有关详情，请参见第 12-13 页上的应用访问控制策略。

修改现有规则

许可证：保护

您可以修改自定义标准文本规则。您还可以修改思科提供的标准文本规则或共享对象规则，并通过保存规则来创建一个或多个规则实例。

创建规则或修改思科规则会将新规则或修订复制到本地规则类别中，并会向该规则分配下一个大于 100000 的可用 Snort ID (SID)。

对于共享对象规则，只能修改报头信息。不能修改共享对象规则或其参数中使用的规则关键字。修改共享对象规则的报头信息并保存更改将会为该规则创建生成器 ID (GID) 为 3 的新实例，并会为自定义规则创建下一个可用 SID。Rule Editor 将共享对象规则的新实例链接到保留的 `soid` 关键字，该关键字将创建的规则映射到 VRT 所创建的规则。您可以删除自行创建的共享对象规则实例，但是不能删除由思科提供的共享对象规则。有关详细信息，请参阅第 36-3 页上的了解规则报头和第 36-97 页上的删除自定义规则。

注　请勿修改共享对象规则的协议；否则，将会致使规则无效。

要修改规则，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Rule Editor**。

系统将显示 Rule Editor 页面。

步骤 2　找到要修改的规则。您有以下选项：

- 要通过浏览规则类别查找规则，请浏览文件夹以找到所需的规则，然后点击该规则旁边的编辑图标 ( )。
- 要通过搜索查找规则，请为要查找的规则输入搜索条件 （最简单的是 SID），然后点击 **Search**。如果适当，点击搜索返回的规则。有关详情，请参见第 36-98 页上的搜索规则。
- 要通过过滤页面上显示的规则来查找规则，请在规则列表左上方带有过滤器图标 ( ) 的文本框中输入一个规则过滤器。导航到所需的规则并点击该规则旁边的编辑图标 ( )。有关详情，请参见第 36-99 页上的过滤 Rule Editor 页面上的规则。

规则编辑器将会打开，其中显示所选的规则。

请注意，如果您选择共享对象规则，规则编辑器将仅显示规则报头信息。在 Rule Editor 页面上，可以通过以数字 3 (GID) 开头的列表来识别共享对象规则，例如 3:1000004。

步骤 3　修改规则 （有关规则选项的详细信息，请参阅第 36-93 页上的编写新规则），然后点击 **Save As New**。

规则将保存到本地规则类别中。

提示　如果您想使用规则的本地修而不使用系统规则，可按照第 32-18 页上的设置规则状态中所述的步骤禁用系统，并且激活本地规则。

步骤 4　如第 12-13 页上的应用访问控制策略中所述将入侵策略作为访问控制策略的一部分进行应用来激活入侵规则，以使所做的更改生效。

向规则添加注释

许可证：保护

可以向任何入侵规则添加注释。这样做可以提供有关规则以及其识别出的漏洞或策略违规的额外上下文和信息。

要将注释添加到规则，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Rule Editor**。

系统将显示 Rule Editor 页面。

步骤 2　找到要添加注释的规则。您有以下选项：

- 要通过浏览规则类别查找规则，请浏览文件夹以找到所需的规则，然后点击该规则旁边的编辑图标 ( )。
- 要通过搜索查找规则，请为要查找的规则输入搜索条件 （最简单的是 SID），然后点击 **Search**。如果适当，点击搜索返回的规则。有关详情，请参见第 36-98 页上的搜索规则。
- 要通过过滤页面上显示的规则来查找规则，请在规则列表左上方带有过滤器图标 ( ) 的文本框中输入一个规则过滤器。导航到所需的规则并点击该规则旁边的编辑图标 ( )。有关详情，请参见第 36-99 页上的过滤 Rule Editor 页面上的规则。

系统将显示规则编辑器。

步骤 3　点击 **Rule Comment**。

系统将显示 Rule Comment 页面。

步骤 4　在文本框中输入注释，然后点击 **Add Comment**。

输入的注释将保存在注释文本框中。

提示　也可以在入侵事件的数据包视图中添加和查看规则注释。有关详细信息，请参阅第 41-20 页上的查看事件信息。

删除自定义规则

许可证：保护

您可以删除当前未在入侵策略中启用的自定义规则。您不能删除思科提供的标准文本规则或共享对象规则规则。

系统将删除的规则存储在删除的类别中，您可以使用删除的规则作为新规则的依据。有关编辑规则的信息，请参阅第 36-95 页上的修改现有规则。

入侵策略中的 Rules 页面不显示删除的类别，因此您不能启用删除的自定义规则。

请注意，您还可以删除 Rule Updates 页面上的所有本地规则。有关示例，请参阅第 66-14 页上的使用一次性规则更新。

有关详细信息，请参阅以下各节：

- 有关创建自定义规则的信息，请参阅第 36-93 页上的编写新规则。
- 有关导入本地规则的信息，请参阅第 66-13 页上的导入规则更新和本地规则文件。
- 有关设置规则状态的信息，请参阅第 32-18 页上的设置规则状态。

要删除自定义规则，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Rule Editor**。

系统将显示 Rule Editor 页面。

步骤 2　您有两种选择：

- 点击 **Delete Local Rules**，然后点击 **OK**。

  入侵规则中当前未启用且对其的更改已保存的所有规则将从本地规则类别中删除，并移至删除的类别中。

- 浏览文件夹以找到本地规则类别；点击本地规则类别以展开它，然后点击要删除的规则旁边的删除图标 ( )。

  该规则从本地规则类别中删除，并移至删除的类别中。

  请注意，自定义标准文本规则的生成器 ID (GID) 为 1 （例如， 1:1000012），自定义共享对象规则的 GID 为 3 （例如， 3:1000005）。

提示 系统还会将您连同修改后的报头信息一起保存的共享对象规则存储在本地规则类别中，并以 3 作为 GID 将它们列出来。您可以删除您修改后的共享对象规则版本，但不能删除原始共享对象规则。

搜索规则

许可证：保护

FireSIGHT 系统提供成千上万个标准文本规则；而随着不断发现新的漏洞和攻击，思科漏洞研究团队会继续添加规则。您可以轻松搜索您想要激活、禁用或编辑的特定规则。

下表介绍了可用的搜索选项：

表 36-61　规则搜索条件

选项	说明
Signature ID	要根据 Snort ID （又称为 Signature ID）搜索一个规则，请输入一个 Snort ID 号。要搜索多个规则，请输入以逗号分隔的 Snort ID 号列表。此字段中最多可输入 80 个字符。
Generator ID	要搜索标准文本规则，请选择 **1**。要搜索共享对象规则，请选择 **3**。
通信	要搜索带有特殊消息的规则，请在 **Message** 字段中输入规则消息中的一个字。例如，要搜索 DNS 攻击，可输入 `DNS`；要搜索缓冲区溢出攻击，可输入 `overflow`。
协议	要搜索评估特定协议的流量的规则，请选择该协议。如果不选择协议，搜索结果将包含适用于所有协议的规则。
源端口	要搜索检查来自指定端口的数据包的规则，请输入源端口号或端口相关变量。
目的端口	要搜索检查发往特定端口的数据包的规则，请输入目标端口号或端口相关变量。
源 IP：	要搜索检查来自指定 IP 地址的数据包的规则，请输入源 IP 地址或 IP 地址相关变量。
目标 IP：	要搜索检查发往指定 IP 地址的数据包的规则，请输入目标 IP 地址或 IP 地址相关变量。
关键字	要搜索特定关键字，可以使用关键字搜索选项。可以选择要搜索的关键字和关键字值。也可以在关键字值前面加上感叹号 (!) 以匹配任何未指定的值。
类别	要搜索特定类别中的规则，请从 **Category** 列表中选择该类别。
分类	要搜索具有特定分类的规则，请从 **Classification** 列表中选择该分类名称。
Rule State	要在特定策略和特定规则状态中搜索规则，请从第一个 **Rule State** 列表中选择策略，并从第二个列表中选择状态，以搜索状态设置为 **Generate Events**、 **Drop and Generate Events** 或 **Disabled** 的规则。

要搜索特定规则，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Rule Editor**。

系统将显示 Rule Editor 页面。

步骤 2　点击工具栏上的 **Search**。

系统将显示 Search 页面。

步骤 3　使用规则搜索条件表中所述的任意字段添加搜索条件。

注　必须至少指定一个搜索条件才能搜索规则。

步骤 4　执行以下步骤以搜索包含特定关键字的规则：

- 从 **Keyword** 部分的下拉列表中选择要搜索的关键字。

  有关完整的可用关键字列表，请参阅第 36-9 页上的了解规则中的关键字和参数。
- 在 **Keyword** 字段中输入要搜索的参数。

步骤 5　点击 **Search**。

页面将重新加载，其中列出与搜索条件匹配的规则。

步骤 6　要查看或编辑规则 （或系统规则的副本），请点击超链接规则消息。有关编辑规则的详细信息，请参阅第 36-95 页上的修改现有规则。

过滤 Rule Editor 页面上的规则

许可证：保护

您可以对 Rule Editor 页面中的规则进行过滤来显示其中一组规则。例如，如果想要修改某个规则或更改其状态，但是难以在成千上万个可用规则中找到该规则，这个过滤功能可能很有用。

当您输入过滤器时，页面将显示至少包含一条匹配规则或消息 （如果没有匹配规则）的文件夹。过滤器可以包含特殊关键字及其参数、字符串和用引号引起来的文字字符串，多个过滤器条件之间用空格隔开。过滤器不能包含正则表达式、通配符或任何特殊运算符，例如取反字符 (!)、大于号 (>) 和小于号 (<) 等。

所有关键字、关键字参数和字符串都不区分大小写。除关键字 `gid` 和 `sid` 之外，所有参数和字符串都被视为部分字符串。`gid` 和 `sid` 的参数只会返回完全匹配项。

或者，可以在未经过滤的原始页面上展开某个文件夹，如果后续过滤器返回该文件夹中的匹配项，该文件夹将会保持展开。这对于在包含大量规则的文件夹中搜索规则可能有用。

不能使用后续过滤器限制任何过滤器。输入的任何过滤器都会搜索整个规则数据库并返回所有匹配的规则。当您在页面仍显示上一过滤器的结果时输入过滤条件，页面将清空，转而返回新过滤器的结果。

您可以对已过滤或未过滤列表中的规则使用相同的功能。例如，您可以编辑 Rule Editor 页面上经过过滤或未经过滤的列表中的规则。您也可以使用该页面上下文菜单中的任何选项。

有关详细信息，请参阅以下各节：

- 第 36-100 页上的在规则过滤器中使用关键字
- 第 36-101 页上的在规则过滤器中使用字符串

在规则过滤器中使用关键字

许可证：保护

每个规则过滤器都可以包含一个或多个关键字，其格式如下：

keyword:*argument*

其中，*keyword* 是规则过滤器关键字表中的其中一个关键字，*argument* 是要在与该关键字相关的一个或多个指定字段中搜索的一个字母数字字符串，不区分大小写。

除 `gid` 和 `sid` 之外的所有关键字的参数都会被视为部分字符串。例如，参数 `123` 将返回 `"12345"`、`"41235"`、`"45123"` 等结果。`gid` 和 `sid` 的参数只会返回完全匹配项；例如，`sid:3080` 只会返回结果 SID 3080。

提示 使用一个或多个字符串来进行过滤可以搜索部分 SID。有关详情，请参见第 36-101 页上的在规则过滤器中使用字符串。

下表介绍了可以用于过滤规则的特定过滤关键字和参数。

表 36-62　　规则过滤器关键字

关键字	说明	示例
`arachnids`	根据规则引用中的完整或部分 Arachnids ID 返回一个或多个规则。有关详情，请参见第 36-13 页上的定义事件参考。	`arachnids:181`
`bugtraq`	根据规则引用中的完整或部分 Bugtraq ID 返回一个或多个规则。有关详情，请参见第 36-13 页上的定义事件参考。	`bugtraq:2120`
`cve`	根据规则引用中的完整或部分 CVE 编号返回一个或多个规则。有关详情，请参见第 36-13 页上的定义事件参考。	`cve:2003-0109`
`gid`	参数 `1` 将返回标准文本规则。参数 `3` 将返回共享对象规则。有关详细信息，请参阅第 41-34 页上的解读预处理器生成器 ID和第 32-2 页上的表 32-1。	`gid:3`
`mcafee`	根据规则引用中的完整或部分 McAfee ID 返回一个或多个规则。有关详情，请参见第 36-13 页上的定义事件参考。	`mcafee:10566`
`msg`	根据规则的完整或部分 Message 字段（又称为事件消息）返回一个或多个规则。有关详情，请参见第 36-10 页上的定义事件消息。	`msg:chat`
`nessus`	根据规则引用中的完整或部分 Nessus ID 返回一个或多个规则。有关详情，请参见第 36-13 页上的定义事件参考。	`nessus:10737`
`ref`	根据规则引用或规则 Message 字段中一个完整的字母数字字符串或其一部分返回一个或多个规则。有关详细信息，请参阅第 36-13 页上的定义事件参考和第 36-10 页上的定义事件消息。	`ref:MS03-039`
`sid`	返回带有完全匹配的 Signature ID 的规则。有关详情，请参见第 41-34 页上的解读预处理器生成器 ID。	`sid:235`
`url`	根据规则引用中的完整或部分 URL 返回一个或多个规则。有关详情，请参见第 36-13 页上的定义事件参考。	`url:faqs.org`

在规则过滤器中使用字符串

许可证：保护

每个规则过滤器可以包含一个或多个字母数字字符串。字符串将搜索规则的 **Message** 字段、Signature ID 和 Generator ID。例如，字符串 `123` 会返回规则消息中的 `"Lotus123"`、`"123mania"` 等字符串，也会返回 SID 6123、 SID 12375 等。有关规则的 **Message** 字段的详细信息，请参阅第 36-10 页上的定义事件消息。有关规则的 SID 和 GID 的详细信息，请参阅第 41-34 页上的解读预处理器生成器 ID。

所有字符串都不区分大小写并被视为部分字符串。例如， `ADMIN`、 `admin` 或 `Admin` 等字符串中任意一个字符串都会返回 `"admin"`、 `"CFADMIN"`、 `"Administrator"` 等结果。

用引号将字符串引起来可以返回完全匹配项。例如，用引号引起来的原义字符串 `"overflow attempt"` 只会返回完全匹配的该字符串，而由 `overflow` 和 `attempt` 这两个字符串组成的未加引号的过滤器则会返回 `"overflow attempt"`、 `"overflow multipacket attempt"`、 `"overflow with evasion attempt"` 等结果。

在规则过滤器中结合使用关键字和字符串

许可证：保护

输入关键字、文字字符串或这二者的任意组合并以空格分隔可以缩小过滤结果的范围。结果包括符合所有过滤条件的任意规则。

可以按照任意顺序输入多个过滤条件。例如，以下每个过滤器返回的规则相同：

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

过滤规则

许可证：保护

可以对 Rule Editor 页面上的规则进行过滤以显示规则子集，以便更容易找到特定规则。然后，您可以使用该页面的任何功能，包括选择上下文菜单中可用的任何功能。

要过滤特定规则，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Rule Editor**。

系统将显示 Rule Editor 页面。

如果要查找要进行编辑的规则， Rule Editor 页面上的规则过滤功能可能特别有用。有关详情，请参见第 36-95 页上的修改现有规则。

步骤 2　或者，从 Group Rules By 列表中选择其他分组方法。

提示　如果所有子组中的总规则数量很大，过滤所需的时间可能大大增加，因为规则显示在多个类别中，即使唯一规则的总数少很多也是如此。

步骤 3　或者，点击要展开的任何组旁边的文件夹。

文件夹将会展开以显示该组中的规则。请注意，一些规则组包含也可以展开的子组。

另请注意，如果您预期规则可能在某个组中，在未经过滤的原始页面上展开该组可能有用。如果后续过滤器返回该文件夹中的匹配项，当您点击过滤器清除图标 (✖) 返回到未经过滤的原始页面时，该组将会保持展开。

步骤 4　要激活过滤器文本框，请点击规则列表左上方的文本框中的过滤器图标 ( )。

步骤 5　键入过滤器限制条件并按 Enter。

过滤器可以包含关键字、变量和字符串 （可以用引号引起来），多个条件之间用空格隔开。有关详情，请参见第 36-99 页上的过滤 Rule Editor 页面上的规则。

页面将会刷新以显示至少包含一个匹配规则的任何组。

步骤 6　或者，打开尚未打开的文件夹以显示匹配规则。您有以下过滤选择：

- 要输入新的过滤器，请将光标放在过滤器文本框中，并点击以激活它；键入过滤器并按 Enter。
- 要清除当前经过过滤的列表并返回到未经过滤的原始页面，请点击过滤器清除图标 (✖)。

步骤 7　或者，对规则作出通常会在该页面上作出的任何更改。请参阅第 36-95 页上的修改现有规则。

要使所做的更改生效，请按照第 12-13 页上的应用访问控制策略中所述将入侵策略作为访问控制策略的一部分进行应用。

第 37 章

阻止恶意软件和禁止的文件

*恶意软件*可以通过多种途径进入企业网络。为了帮助您识别和减轻恶意软件的影响， FireSIGHT 系统的文件控制、网络文件轨迹和高级恶意软件防护组件可以检测、跟踪、存储、分析并或者阻止恶意软件及其他类型的文件在网络流量中的传输。该系统还可以对档案文件 （例如，档案文件格式 `.zip` 或 `.rar`）中的嵌套文件进行分析和操作。

您可以配置系统执行恶意软件防护和文件控制，将其作为整体访问控制配置的一部分。您创建并与访问控制规则关联的*文件策略*会处理与规则匹配的网络流量。您可以下载在这些流量中检测到的文件，然后将其提交到思科的恶意软件感知网络 （称为*综合安全智能云*）来对文件的签名进行*动态分析*，从而确定其是否包含恶意软件。

Context Explorer 和控制面板提供在贵组织的网络流量中检测到的文件 （包括恶意软件文件）的不同类型的高级视图。要使分析更具针对性，可以使用恶意软件文件的*网络文件轨迹*页面跟踪个别威胁随时间推移跨主机进行的传播，从而在最有用的方面集中开展爆发控制和防御工作。

虽然您可以使用任何许可证创建文件策略，但是恶意软件防护和文件控制的某些方面要求在目标设备上启用特定获许可功能，如下表所述。

表 37-1 入侵和文件检查的许可证和设备要求

特性	说明	添加该许可证...	至其中一个防御中心...	并在其中一个设备上启用它...
入侵预防	检测和 （可选）阻止入侵和漏洞	保护	任何环境	任何环境
文件控制	检测和 （可选）阻止文件类型传输	保护	任何环境	任何环境
高级恶意软件防护 (AMP)	检测、存储、跟踪和 （可选）阻止恶意软件传输 将捕获的文件提交到思科云进行恶意软件分析	恶意软件	除 DC500 外的所有型号	除 2 系列或 X -系列外的所有型号

如果贵组织有订用 FireAMP，则防御中心还可以接收来自公共思科云的基于终端的恶意软件检测数据。防御中心呈现这些数据以及系统生成的基于网络的任何文件和恶意软件数据。除您的 FireAMP订阅外，导入FireAMP数据无需许可证。有关详细信息，请参阅第 37-21 页上的为 FireAMP 处理云连接。

对于基于文件和恶意软件云的功能，如果贵组织要求更高的安全性或希望限制外部连接，则可使用 FireAMP 私有云 （而不是标准云连接）。所有文件和恶意软件云查找，以及从FireAMP终端的事件数据收集和中继，均将通过私有云处理；当私有云与公共思科云联系时，它会通过不传输终端事件数据的匿名代理连接执行相关处理。

有关详细信息，请参阅：

- 第 37-2 页上的了解恶意软件防护和文件控制
- 第 37-8 页上的了解和创建文件策略
- 第 37-21 页上的为 FireAMP 处理云连接

有关评估与恶意软件防护和文件控制相关的事件数据的详细信息，请参阅第 40-1 页上的分析恶意软件和文件活动。

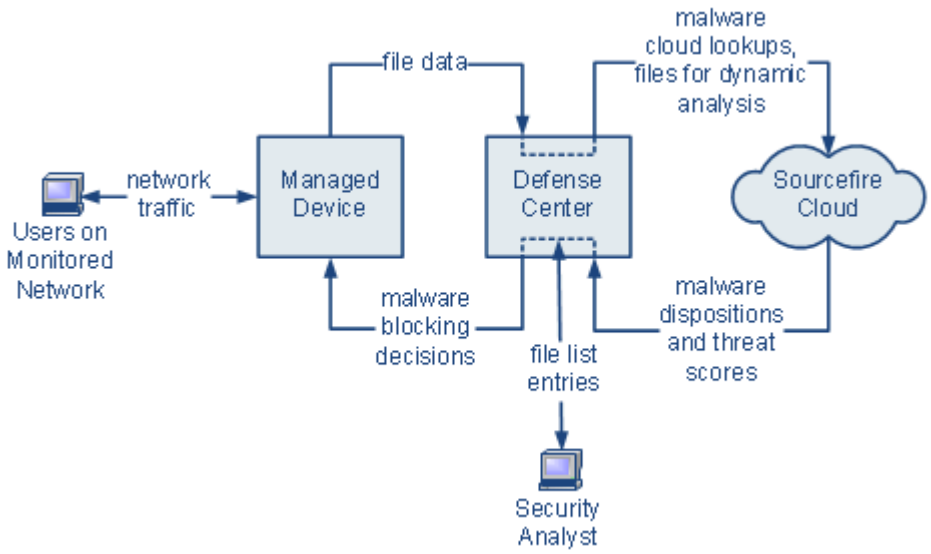
了解恶意软件防护和文件控制

许可证：保护、恶意软件或任何

受支持的设备：因功能而异

受支持的防御中心：因功能而异

使用*高级恶意软件防护*功能，您可以配置 FireSIGHT 系统来检测、存储、跟踪、分析并选择性地阻止网络上传输的恶意软件文件，如下图所示。



系统可以检测并或者阻止多种类型的文件（包括 PDF、Microsoft Office 文档及其他）中的恶意软件。受管设备监控这些文件类型传输的基于应用协议的特定网络流量。设备检测到合格文件时，它可以将该文件的 SHA-256 哈希值发送到 防御中心，后者然后使用这些信息执行*恶意软件云查找*。根据这些结果，思科云将文件性质返回到防御中心。

系统在网络流量中检测到文件时，*文件存储*功能允许设备将合格文件存储到硬盘或恶意软件存储包。对于性质为 Unknown 的可执行文件，无论设备是否存储文件，设备都可以提交该文件进行*动态分析*。云返回到防御中心：

- 威胁评分，指明文件包含恶意软件的可能性；以及
- 动态分析摘要报告，详述为云分配该威胁评分的原因。

如果文件是合格的可执行文件，则设备还可以对文件结构执行 Spero 分析，并将产生的 Spero 签名提交到云。云使用该签名对动态分析进行补充，从而确定文件是否是恶意软件。

如果文件在云中具有据您所知是不正确的处理，则可向文件列表中添加该文件的 SHA-256 值。

- 要好像云已为文件分配了安全性质一样对其进行处理，请将文件添加到*白名单*。
- 要好像云已为文件分配了恶意软件性质一样对其进行处理，请将文件添加到*自定义检测列表*。

如果系统在文件列表中检测到文件的 SHA-256 值，会采取适当措施而不执行恶意软件查找或检查文件性质。请注意，必须为文件策略中的某个规则配置 **Malware Cloud Lookup** 或 **Block Malware** 操作和匹配的文件类型，以计算文件的 SHA 值。可以按文件策略启用白名单或自定义检测列表。有关管理文件列表的详细信息，请参阅第 3-29 页上的使用文件列表。

系统可以检查并阻止存档文件内的嵌套文件 （例如， `.zip` 或 `.rar` 存档文件），与其分析和处理正常的未压缩文件一样。但是，请注意，如果系统阻止任何嵌套文件，它也会阻止包含该文件的整个存档文件。系统可以检查最外层存档文件 （级别为 0）以下的最多 3 级嵌套文件。您可以将文件策略配置为阻止超过指定嵌套级数的存档文件 （最多 3 级）。

您还可以将文件策略配置为阻止内容已加密或无法检查的存档文件。有关存档文件检查的详细信息，请参阅第 37-18 页上的配置存档文件检查选项。

要检查或阻止文件，必须在应用策略的受管设备上启用保护许可证。要存储文件，对其执行恶意软件云查找并选择性地阻止恶意软件文件，将文件提交到云进行动态分析，或者将文件添加到文件列表，还必须为这些设备启用恶意软件许可证。

了解文件性质

系统根据思科云返回的性质来确定文件性质。由于向文件列表中进行添加或由于威胁评分，文件可具有思科云返回的以下文件性质之一：

- `Malware` 表示云将文件归类为恶意软件，或文件威胁评分超过文件策略定义的恶意软件阈值。
- `Clean` 表示云将文件归类为安全，或用户将文件添加到安全列表。
- `Unknown` 表示在云分配性质之前发生恶意软件云查找。云尚未将文件分类。
- `Custom Detection` 表示用户将文件添加到自定义检测列表。
- `Unavailable` 表示防御中心无法执行恶意软件云查找。您可能看到有一小部分事件具有此性质，这是预期行为。

提示 如果在很短时间内连续遇到若干个 `Unavailable` 恶意活动，请检查您的云连接和端口配置。有关详细信息，请参阅第 E-1 页上的安全、互联网接入和通信端口。

存档文件所具有的性质是基于分配给存档内文件的性质。下面的按内容划分的存档文件性质列出了存档文件接收的、用于存档包含的文件的不同可能组合的性质。对于包含已确定的恶意软件文件的**所有**存档，将赋予其 `Malware` 性质。对于不含已确定恶意软件文件的存档，如果其包含任何未知文件，则其性质为 `Unknown`；如果其仅包含安全文件，则其性质为 `Clean`。有关存档文件检查的详细信息，请参阅第 37-18 页上的配置存档文件检查选项。存档文件与其他文件一样可以具有 `Custom Detection` 或 `Unavailable` 性质 （如果符合这些性质的条件）。

表 37-2　　按内容划分的存档文件性质

存档文件性质	未知文件数	安全文件数	恶意软件文件数
未知	1 个或多个	任何环境	0
清洁能源	0	1 个或多个	0
恶意软件	任何环境	任何环境	1 个或多个

根据文件性质，防御中心指示受管设备阻止文件或者允许上传或下载文件。请注意，如果档案文件中的任何嵌套文件被阻止，系统将阻止整个档案文件。为了提高性能，如果系统根据 SHA-256 已经知道文件的性质，防御中心会使用缓存的性质而不是查询思科云。

请注意，文件性质可以更改。例如，云可以确定先前被视为安全的文件现在被识别为恶意软件，或者正好相反，以前被识别为恶意软件的文件实际上是安全的。如果上一周对其执行了恶意软件查找的文件的性质发生变化，云会通知防御中心，因此系统在下次检测到该文件进行传输时可以采取适当措施。已更改的文件性质称为*追溯性*性质。

从恶意软件云查找返回的文件性质以及任何关联的威胁评分都具有生存时间 (TTL) 值。在 TTL 值中指定的持续时间内保持某种文件性质而无更新后，系统会清除缓存的信息。性质及关联的威胁评分具有以下 TTL 值：

- Clean - 4 小时
- Unknown - 1 小时
- Malware - 1 小时

如果缓存的恶意软件云查找识别出已超时的缓存性质，系统会执行新查找以确定文件性质。

了解文件控制

如果贵组织不仅要阻止恶意软件文件的传输，还要阻止所有特定类型的文件的传输 （无论文件是否包含恶意软件），则可通过*文件控制*功能来做到这一点。与恶意软件防护一样，受管设备也会监控特定文件类型传输的网络流量，然后阻止或允许文件。

系统可以检测恶意软件的所有文件类型以及许多其他文件类型都支持文件控制。这些文件类型分为三类：基本类别，包括多媒体 （swf 和 mp3）；可执行文件 （exe 和 torrent）；以及 PDF。请注意，与恶意软件防护不同，文件控制不需要思科云的查询。

使用捕获文件、文件事件和恶意软件事件进行分析

传输或阻止文件后，系统会生成恶意软件和文件事件。它还会收集有关受管设备捕获的所有文件的信息。可以使用防御中心的网络界面查看这些事件和信息。此外，Context Explorer 和控制面板提供贵组织检测到的文件 （包括恶意软件文件）的不同类型的高级视图。

要使分析更具针对性，可以通过*网络文件轨迹*功能跟踪个别文件的传输路径。文件的轨迹页面显示有关文件的摘要信息、文件的主机间传输 （包括受阻传输）的图形映射，以及与这些文件的检测或阻止相关联的恶意软件或文件事件的列表。

请注意：由于既不能对 DC500 使用恶意软件许可证，也不能在 2 系列设备或 用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此，您无法使用这些设备捕获或阻止个别文件，提交文件供动态分析，或者查看您为其执行恶意软件云查找的文件的文件轨迹。

有关详细信息，请参阅以下各节：

- 第 37-5 页上的配置恶意软件防护和文件控制
- 第 37-5 页上的根据恶意软件防护和文件控制记录事件
- 第 37-6 页上的集成 FireAMP 与 FireSIGHT 系统
- 第 37-7 页上的基于网络的 AMP 与基于终端的 FireAMP
- 第 40-30 页上的使用网络文件轨迹

配置恶意软件防护和文件控制

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

通过将文件策略与访问控制规则相关联，可以将恶意软件防护和文件控制配置为整体访问控制配置的一部分。这种关联保证系统在传递流量中与访问控制规则的条件匹配的文件之前，首先检查该文件。

文件策略 （例如父项访问控制策略）包含的规则用于确定系统如何处理与每个规则的条件相符的文件。可以配置单独的文件规则，以对不同的文件类型、应用协议或传输方向采取不同操作。

当文件与规则匹配时，规则可以：

- 根据简单文件类型匹配允许或阻止文件
- 根据恶意软件文件性质阻止文件
- 捕获文件并将其存储到设备
- 提交捕获文件以进行动态分析

此外，文件策略还可以：

- 根据白名单或自定义检测列表中的条目自动将文件视为安全文件或恶意软件
- 在文件的威胁评分超过可配置阈值时将文件视为恶意软件
- 检查存档文件 （例如， `.zip` 或 `.rar`）的内容
- 阻止内容已加密，嵌套超过指定的最大归档深度或因其他原因无法检查的档案文件

举一个简单的例子，您可以实施会阻止用户下载可执行文件的文件策略。再如，您可以检查恶意软件的已下载的 PDF 并阻止找到的任何实例。有关文件策略以及将其与访问控制规则相关联的详细信息，请参阅第 37-8 页上的了解和创建文件策略和第 18-7 页上的调整的入侵防御性能。

由于不能对 DC500 使用恶意软件许可证，因此，您无法使用该设备来应用可执行基于网络的恶意软件防护或检查存档文件的内容的文件策略。同样，由于不能在 2 系列设备或 用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此，您无法对这些设备应用可执行基于网络的恶意软件防护或检查存档文件的内容的文件策略。

根据恶意软件防护和文件控制记录事件

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

防御中心将系统文件检查和处理的记录作为捕获文件、文件事件和恶意软件事件进行记录：

- *捕获文件*表示系统捕获的文件。
- *文件事件*表示系统在网络流量中检测到并或者被阻止的文件。
- *恶意软件事件*表示系统在网络流量中检测到并或者被阻止的恶意软件文件。
- *追溯性恶意软件事件*表示恶意软件文件的性质已更改的文件。

当系统根据对网络流量中恶意软件的检测或阻止情况生成恶意软件事件时，它还会生成文件事件，因为要在文件中检测恶意软件，系统必须先检测该文件本身。请注意， FireAMP 连接器（请参阅第 37-6 页上的集成 FireAMP 与 FireSIGHT 系统）生成的基于终端的恶意软件事件不具备对应文件事件。同样，当系统在网络流量中捕获文件时，也会生成文件事件，因为系统将首先检测到该文件。

您可以使用防御中心查看、操作和分析捕获的文件、文件事件和恶意软件事件，然后与其他人交流您的分析结果。 Context Explorer、控制面板、事件查看器、网络文件轨迹映射和报告功能让您可以更深入地了解检测、捕获和阻止的文件及恶意软件。您也可以使用事件触发关联策略违规或者通过邮件、 SMTP 或系统日志向您发出警报。有关文件和恶意软件事件的详细信息，请参阅第 40-6 页上的使用文件事件和第 40-14 页上的使用恶意软件事件。

由于您无法在 DC500 上使用恶意软件许可证，也无法在2 系列 设备或 用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此，您无法使用这些设备生成或分析与恶意软件云查找或与存档文件的内容相关联的捕获文件、文件事件和恶意软件事件。

集成 FireAMP 与 FireSIGHT 系统

许可证：任何环境

FireAMP 是思科的企业级高级恶意软件分析和防护解决方案，用于发现、了解并阻止高级恶意软件爆发、高级持续威胁和针对性攻击。

如果贵组织有订用 FireAMP，则个人用户可以在*终端*（计算机和移动设备）上安装 *FireAMP 连接器*。 FireAMP 连接器是一种轻量级代理，具有多种功能，其中包括在执行上传、下载、执行、打开、复制、移动等操作时检查文件。这些连接器与思科云进行通信，以将确定检查的文件是否包含恶意软件。

文件被确定为恶意软件后，云会向防御中心发送威胁识别。云还可以向防御中心发送其他类型的信息，包括有关扫描、隔离、受阻执行和云召回的数据。防御中心将这些信息记录为恶意软件事件。

通过 FireAMP 部署，不仅可以配置防御中心根据恶意软件事件发起的补救和警报，还可以使用 FireAMP 门户 (http://amp.sourcefire.com/) 帮助降低恶意软件造成的影响。门户提供稳健灵活的网络界面，可以通过该界面控制 FireAMP 部署的所有方面并管理爆发的所有阶段。您能够：

- 为整个组织配置自定义恶意软件检测策略和配置文件，以及对所有用户的文件执行快速扫描和全面扫描
- 执行恶意软件分析，包括查看热图、详细文件信息、网络文件轨迹和威胁根本原因
- 配置爆发控制的多个方面，包括自动隔离、用于阻止运行非隔离可执行文件的应用阻止，以及排除列表
- 创建自定义保护，根据组策略阻止某些应用的执行，并创建自定义白名单

有关详细信息，请参阅以下各节：

- 第 37-7 页上的基于网络的 AMP 与基于终端的 FireAMP 比较了思科产品系列中提供的恶意软件防护策略。
- 第 37-21 页上的为 FireAMP 处理云连接说明如何在防御中心与思科云之间建立通信 （直接建立通信或通过 FireAMP 私有云连接建立通信）。

提示 有关 FireAMP 的详细信息，请参阅 FireAMP 门户的联机帮助。

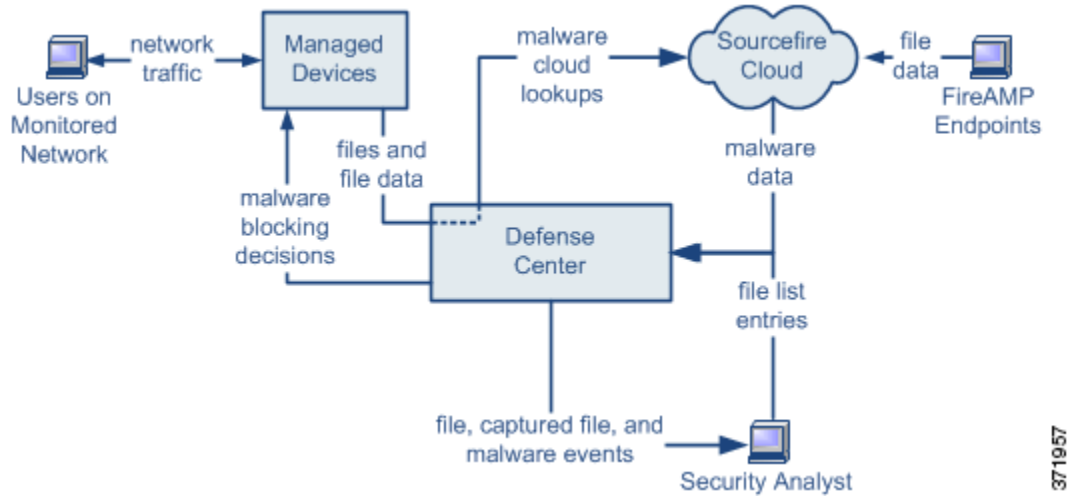
基于网络的 AMP 与基于终端的 FireAMP

许可证：恶意软件或任意

受支持的设备：因功能而异

受支持的防御中心：因功能而异

下图显示如何能够使用防御中心同时根据基于网络的高级恶意软件防护策略和基于终端的 FireAMP 策略处理数据。



请注意，由于 FireAMP 恶意软件检测是在下载或执行时于终端处执行，而受管设备在网络流量中检测恶意软件，因此两种类型的恶意软件事件中的信息不同。例如，基于终端的恶意软件事件包含有关文件路径、调用客户端应用等等的信息，而网络流量中的恶意软件检测则包含有关用于传输文件的连接的端口、应用协议和始发 IP 地址信息。

再例如，在基于网络的恶意软件事件中，用户信息向用户展示此用户最近登录的主机是恶意软件的攻击目标，并且恶意软件是由网络发现功能确定的。另一方面， FireAMP 报告的用户表示用户当前登录到本地连接器所确定的检测到恶意软件的终端。

注 在基于终端的恶意软件事件中报告的 IP 地址可能不在网络映射中，甚至可能不在受监控网络中。根据您的部署、网络架构、合规性级别及其他因素，连接器安装所在的终端与受管设备监控的主机可能不是相同的主机。

请注意，由于既不能对 DC500 使用恶意软件许可证，也不能在2 系列 设备或 用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此，您无法使用这些设备捕获或阻止个别文件，提交文件供动态分析，检查存档文件的内容，或者查看您为其执行恶意软件云查找的文件的轨迹。

下表总结了这两种策略之间的差异。

表 37-3　基于网络恶意软件防护策略与基于终端的恶意软件防护策略

特性	基于网络	基于终端 (FireAMP)
文件类型检测和阻止方法（文件控制）	在网络流量中，使用访问控制和文件策略	不支持
恶意软件检测和阻止方法	在网络流量中，使用访问控制和文件策略	在单个终端上，使用与思科云进行通信的已安装的连接器
检查的网络流量	流量传递通过受管设备	无；终端上安装的连接器直接检查文件
恶意软件检测稳健性	有限的文件类型	所有文件类型
恶意软件分析方案	基于防御中心的分析，以及在云中分析	基于防御中心的分析，以及 FireAMP 门户提供的其他方案
恶意软件缓解	网络流量中的恶意软件阻止，防御中心发起的纠错	基于FireAMP的隔离和爆发控制方案，防御中心发起的纠错
生成的事件	文件事件、捕获文件、恶意软件事件及追溯性恶意软件事件	恶意软件事件
恶意软件事件中的信息	基本的恶意软件事件信息，以及连接数据（IP 地址、端口和应用协议）	深入的恶意软件事件信息；无连接数据
网络文件轨迹	基于防御中心	基于防御中心的分析，以及 FireAMP 门户提供的其他方案
必需许可证或订用	保护许可证执行文件控制；恶意软件许可证执行恶意软件防护	FireAMP 订用 （不是基于许可证）

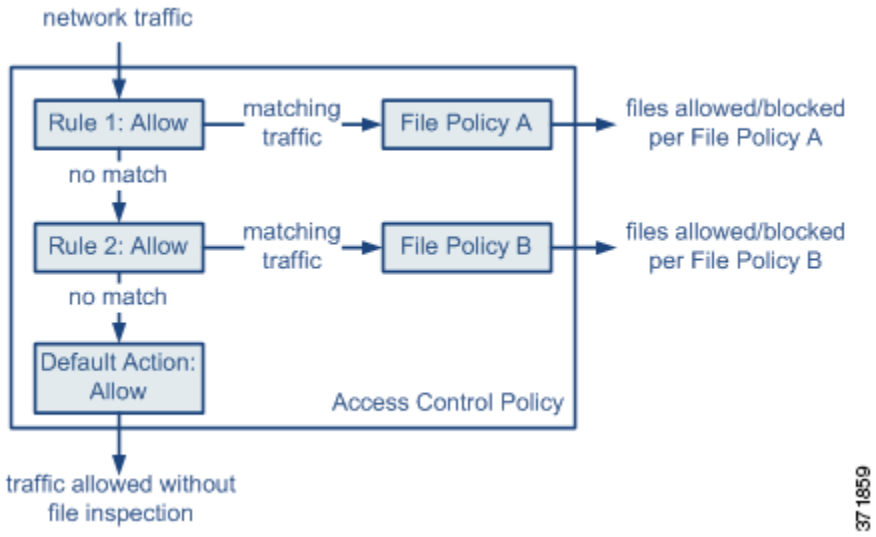
了解和创建文件策略

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

文件策略是作为整体访问控制配置的一部分供系统用于执行高级恶意软件防护和文件控制的一组配置。在内联部署中，可考虑下图所示的简单访问控制策略。



策略有两个访问控制规则，两者都使用 Allow 操作并与文件策略关联。策略的默认操作也是允许流量，但不执行文件策略检查。在本示例中，流量处理如下：

- 与 `Rule 1` 匹配的流量根据 `File Policy A` 进行检查。
- 与 `Rule 1` 不匹配的流量根据 `Rule 2` 进行评估。与 `Rule 2` 匹配的流量根据 `File Policy B` 进行检查。
- 允许与任一规则不匹配的流量；不能将文件策略与默认操作关联。

文件策略 （例如父项访问控制策略）包含的规则用于确定系统如何处理与每个规则的条件相符的文件。可以配置单独的文件规则，以对不同的文件类型、应用协议或传输方向采取不同操作。

文件与某个规则匹配后，规则可以：

- 根据简单文件类型匹配允许或阻止文件
- 根据恶意软件文件性质阻止文件
- 将捕获文件存储到设备
- 提交捕获文件以进行动态分析

此外，文件策略还可以：

- 根据白名单或自定义检测列表中的条目自动将文件视为安全文件或恶意软件
- 在文件的威胁评分超过可配置阈值时将文件视为恶意软件
- 检查存档文件 （例如， `.zip` 或 `.rar`）的内容
- 阻止内容已加密，嵌套超过指定的最大归档深度或因其他原因无法检查的档案文件

可以将单个文件策略与其操作为 **Allow**、**Interactive Block** 或 **Interactive Block with reset** 的访问控制规则关联。这样，系统将会使用该文件策略检查符合访问控制规则条件的网络流量。通过将不同文件策略与不同访问控制规则关联，可以精细控制如何识别并阻止网络上传输的文件。但请注意，您**不能**使用文件策略检查由访问控制默认操作处理的流量。有关详细信息，请参阅第 18-2 页上的检查允许的流量中是否存在入侵和恶意软件。

文件规则

可使用文件规则来填充文件策略。下表介绍文件规则的组成部分。

表 37-4　　文件规则组件

文件规则组件	说明
应用协议	系统可以检测和检查通过 FTP、 HTTP、 SMTP、 IMAP、 POP3 和 NetBIOS-ssn (SMB) 传输的文件。为了提高性能，可以逐个文件规则将文件检测仅限于其中一种应用协议。
传输方向	对于已下载的文件，可以检查通过 FTP、 HTTP、 IMAP、 POP3 和 NetBIOS-ssn (SMB) 传入的流量；对于已上传的文件，可以检查通过 FTP、 HTTP、 SMTP 和 NetBIOS-ssn (SMB) 传出的流量。
文件类别和类型	系统检测各种类型的文件。这些文件类型分为三类：基本类别，包括多媒体 （swf 和 mp3）；可执行文件 （exe 和 torrent）；以及 PDF。可以配置用于检测个别文件类型或整个类别的文件类型的规则。 例如，可以阻止所有多媒体文件，或者仅阻止 ShockWave Flash (swf) 文件。或者，可以将系统配置为会在用户下载 BitTorrent (torrent) 文件时向您发出警报。 ⚠ **注意事项** 频繁触发的文件规则可能会影响系统性能。例如，检测 HTTP 流量 （例如 YouTube，用于传输重要的 Flash 内容）中的多媒体文件可能会产生可能生成数量巨大的事件。
文件规则操作	文件规则操作用于确定系统如何处理与规则条件相符的流量。 **注** 文件规则是以规则操作顺序而非数字顺序进行评估。有关详细信息，请参阅下一节，文件规则操作和评估顺序。

文件规则操作和评估顺序

每个文件规则都有用于确定系统如何处理与规则条件匹配的流量的关联操作。可以在文件策略中设置单独的规则，以对不同的文件类型、应用协议或传输方向采取不同操作。规则操作如下 （按规则操作顺序列出）：

- *Block Files* 规则允许阻止特定文件类型。
- *Block Malware* 规则允许计算特定文件类型的 SHA-256 哈希值，然后使用云查找过程先确定通过网络传输的文件是否包含恶意软件，再阻止表示威胁的文件。
- *Malware Cloud Lookup* 规则允许根据云查找记录通过网络传输的恶意软件性质的文件，同时仍允许其传输。
- *Detect Files* 规则允许将特定文件类型的检测记录到数据库，同时仍允许其传输。

对于每个文件规则操作，可以配置选项以在阻止文件传输后重置连接，将捕获文件存储到受管设备，然后将捕获文件提交到云以进行动态分析和 Spero 分析。下表详细说明可用于每次文件操作的选项。

表 37-5　文件规则操作

操作	重置连接？	存储文件？	动态分析？	面向 MSEXE 的 Spero 分析？
Block Files	是 （推荐）	是，可以存储所有匹配的文件类型	否	否
Block Malware	是 （推荐）	是，可以存储与选择的文件性质匹配的文件类型	是，可以提交具有未知文件性质的可执行文件	是，可以提交可执行文件
Detect Files	否	是，可以存储所有匹配的文件类型	否	否
Malware Cloud Lookup	否	是，可以存储与选择的文件性质匹配的文件类型	是，可以提交具有未知文件性质的可执行文件	是，可以提交可执行文件

文件和恶意软件检测、捕获以及阻止附注与限制

请注意有关文件和恶意软件检测、捕获以及阻止行为的以下详细信息和限制：

- 无论使用何种传输协议，如果未检测到文件的文件结尾标记， **Block Malware** 规则或自定义检测列表不会阻止该文件。系统会等待接收整个文件后再阻止文件 （如文件结尾标记所指示），并在检测到该标记后阻止文件。
- 如果 FTP 文件传输的文件结尾标记单独从最后一个数据段进行传输，则会阻止该标记，并且 FTP 客户端会指示文件传输失败，但是文件实际上将完整传输到磁盘。
- FTP 通过不同信道传输命令和数据。在被动或内嵌分路器模式部署中， FTP 数据会话中的流量及其控制会话可能不会被负载均衡到同一个 Snort。
- 如果文件匹配包含应用协议条件的规则，在系统成功确定该文件的应用协议之后，会生成文件事件。无法识别的文件不生成文件事件。
- 对于使用适合于 FTP 的具有 **Block Malware** 规则的访问控制策略，如果将默认操作设置为已禁用 **Drop when Inline** 的入侵策略，则系统会为检测到的与规则匹配的文件或恶意软件生成事件，但不丢弃文件。要阻止 FTP 文件传输并使用入侵策略作为在其中选择文件策略的访问控制策略的默认操作，必须选择已启用 **Drop when Inline** 的入侵策略。
- 具有 **Block Files** 和 **Block Malware** 操作的文件规则会阻止通过 HTTP 自动恢复文件下载，方法是在进行初始文件传输尝试后检测到相同的文件、URL、服务器和客户端应用达到 24 小时的情况下阻止新会话。
- 在极少数情况下，如果来自 HTTP 上传会话的流量顺序错误，则系统无法正确重组流量，并因此不会阻止该会话或生成文件事件。
- 如果通过 NetBios-ssn 传输使用 **Block Files** 规则阻止的文件（例如 SMB 文件传输），则目标主机上可能会显示文件。但是，该文件不可用，原因是在下载启动后阻止了该文件，导致文件传输未完成。
- 如果创建文件规则以检测或阻止通过 NetBios-ssn 传输的文件 （例如 SMB 文件传输），则系统不检查在应用调用文件策略的访问控制策略前启动的已建立的 TCP 或 SMB 会话中传输的文件，因此不会检测或阻止这些文件。
- 配置为在被动部署中阻止文件的规则不会阻止匹配的文件。由于连接继续传输文件，因此如果配置规则以记录连接的开始，则您可能会看到为此连接记录的多个事件。
- 如果 POP3、POP、SMTP 或 IMAP 会话中文件的所有文件名的总字节数超过 1024，则会话中的文件事件可能无法反映文件名缓冲区填充后检测到的文件的正确文件名。

- 当通过 SMTP 发送基于文本的文件时，某些电子邮件客户端会将换行符转换为 CRLF 换行符标准。由于基于 MAC 的主机使用回车 (CR) 字符，并且基于 Unix/Linux 的主机使用换行 (LF) 字符，因此，邮件客户端进行的换行可能修改文件的大小。注意某些电子邮件客户端在处理无法识别的文件类型时默认进行换行符转换。
- 思科建议启用 **Reset Connection**（适用于 **Block Files** 和 **Block Malware** 操作）以防止受阻应用会话保持打开，直到 TCP 连接重置为止。如果不重置连接，则客户端会话会保持打开，直到 TCP 连接重置为止。
- 如果文件规则配置有 **Malware Cloud Lookup** 或 **Block Malware** 操作，并且防御中心无法与云建立连接，则系统无法执行任何已配置的规则操作选项，直到恢复云连接为止。
- 如果监控大量流量，请**勿**存储所有捕获文件，或者将所有捕获文件提交进行动态分析。否则可能对系统性能产生不利影响。

注　文件在会话中得以检测和阻止之前，来自该会话的数据包均可能接受入侵检查。

文件规则评估示例

与访问控制策略中不同 （规则按数字顺序进行评估），文件策略如第 37-10 页上的文件规则操作和评估顺序中所述处理文件。也就是说，简单阻止优先于恶意软件检测和阻止，后者优先于简单检测和日志记录。例如，可考虑使用在单个文件策略中处理 PDF 文件的四种规则。无论这些规则在网络界面中的显示顺序如何，它们都按以下顺序进行评估：

表 37-6　文件规则评估顺序示例

应用 协议	方向	操作	操作选项	结果
SMTP	上传	Block Files	重置连接	阻止用户通过邮件发送 PDF 文件并重置连接。
FTP	下载	Block Malware	存储具有 Unknown 性质的文件；重置连接	阻止通过文件传输下载恶意软件 PDF 文件，将具有 Unknown 文件性质的文件存储到设备，并重置连接。
POP3 IMAP	下载	Malware Cloud Lookup	存储具有 Unknown 性质的文件；动态分析	检查通过邮件收到的 PDF 文件是否含有恶意软件，并将具有 Unknown 文件性质的文件存储到设备。将文件提交到思科云以进行动态分析。
任何环境	任何环境	Detect Files	无	检测和记录，但是当用户在网络上（即，通过 HTTP）查看 PDF 文件时允许流量。

防御中心使用警告图标 (⚠) 来指出有冲突的文件规则。有关详细信息，请将指针悬停在警告图标上方。

请注意，不能对系统检测到的所有文件类型都执行恶意软件分析。从 **Application Protocol**、**Direction of Transfer** 和 **Action** 下拉列表中选择值之后，系统会对文件类型的列表进行约束。

请注意，由于 DC500 无法使用恶意软件许可证，因此无法创建使用 Block Malware 或 Malware Cloud Lookup 操作的文件规则，也无法使用该设备来应用包含具有这些操作的规则的文件策略。同样，由于不能在2 系列 设备或 用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此无法将包含具有这些操作的规则的文件策略应用于这些设备。

记录捕获文件、文件事件、恶意软件事件和警报

将文件策略与访问控制规则关联时，系统自动为匹配的流量启用文件和恶意软件事件日志记录。如果文件策略配置为捕获并存储文件，则捕获到文件时系统也会自动启用捕获文件日志记录。系统在检查文件时，可以生成以下类型的事件：

- *文件事件*，表示检测到的文件或受阻文件，以及检测到的恶意软件文件
- *恶意软件事件*，表示检测到的恶意软件文件
- *追溯性恶意软件事件*，在先前检测到的文件的 Malware 文件性质发生变化时生成

在文件策略生成文件事件或恶意软件事件或者捕获文件时，无论调用访问控制规则的日志记录配置如何，系统都会自动将关联的连接端记录到防御中心数据库。

注 检查 NetBIOS-ssn (SMB) 流量所生成的文件事件不会立即生成连接事件，因为客户端和服务器构建一个持久连接。系统在客户端或服务器结束会话之后生成连接事件。

对于每个这些连接事件：

- **File** 字段包含表示连接中检测到的文件（包括恶意软件文件）的数量的图标 ( )；点击该图标会显示这些文件的列表，并且对于恶意软件文件还会显示其文件性质。
- **Reason** 字段表示记录连接事件的原因，具体取决于文件规则操作：
- `File Monitor`（适用于 Detect Files 和 Malware Cloud Lookup 文件规则以及白名单中的文件）
- `File Block`（适用于 Block Files 或 Block Malware 文件规则）
- `File Custom Detection`（如果系统在自定义检测列表中遇到文件）
- `File Resume Allow`（如果 Block Files 或 Block Malware 文件规则最初阻止文件传输）。应用允许文件的新访问控制策略后，会自动恢复 HTTP 会话。
- `File Resume Block`（如果 Detect Files 或 Malware Cloud Lookup 文件规则最初允许文件传输）。应用阻止文件的新访问控制策略后，会自动停止 HTTP 会话。
- 对于已阻止文件或恶意软件的连接，**Action** 为 `Block`。

与 FireSIGHT 系统生成的任何类型的事件相同，您可以使用防御中心的网络界面查看、处理和分析文件事件及恶意软件事件。您还可以使用恶意软件事件来触发关联策略违例，或者通过邮件、SMTP 或系统日志向自己发出警报。

注 防御中心还可以使用贵组织的FireAMP 订用接收恶意软件事件。由于这些恶意软件事件是在下载或执行时于终端处生成，因此其信息与基于网络的恶意软件事件中的信息不同。

有关连接事件、文件事件和恶意软件事件以及这些事件的记录方式的详细信息，请参阅：

- 第 38-1 页上的记录网络流量中的连接
- 第 40-6 页上的使用文件事件
- 第 40-14 页上的使用恶意软件事件
- 第 39-2 页上的了解连接和安全情报数据

互联网访问和高可用性

系统使用端口 443 对基于网络的 AMP 执行恶意软件云查找。必须在防御中心上打开该端口（出站）。

高可用性对中的防御中心既不共享云连接，也不共享捕获文件、文件事件和恶意软件事件，但是共享文件策略和相关配置。为了确保业务连续性并确保在两个防御中心上对检测到文件的恶意软件的处置一致，主和辅助防御中心必须都有权访问云。

要将文件提交到云以进行动态分析，还必须在设备上打开端口 443 （出站）。

注　请注意， FireAMP 私有云需要相同的开放端口，并具有与公共思科云连接相同的高可用性限制。

管理文件策略

可以在 File Policies 页面 (**Policies > Files**) 上创建、编辑、修改和比较文件策略，该页面显示现有文件策略的列表及其上次修改日期。

点击文件策略的应用图标 ( ) 会显示一个对话框，该对话框指示哪些访问控制策略使用该文件策略，然后将您重定向到 Access Control Policy 页面。之所以出现此操作，是因为文件策略被视为其父访问控制策略的一部分，从而令您无法独立应用文件策略。要使用新文件策略，或者应用对现有文件策略进行的更改，必须应用或重新应用父访问控制策略。

请注意：

- 系统会检查云以获取适合于动态分析的文件类型列表的更新 （最多一天一次）。如果合格文件类型列表更改，这会构成文件策略发生更改；任何使用该文件策略的访问控制策略在应用于任何设备时都会标记为过期。必须重新应用父访问控制策略才能将更新后的文件策略应用于设备。
- 不能删除已保存或已应用的访问控制策略中使用的文件策略。

有关管理文件策略的详细信息，请参阅以下章节：

- 第 37-14 页上的创建文件策略
- 第 37-15 页上的使用文件规则
- 第 37-20 页上的比较两个文件策略

创建文件策略

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

创建文件策略并使用规则对其进行填充后，即可在访问控制策略中使用该文件策略。

请注意，由于 DC500 无法使用恶意软件许可证，因此无法创建使用 Block Malware 或 Malware Cloud Lookup 操作的文件规则，也无法使用该设备来应用包含具有这些操作的规则的文件策略。同样，由于不能在2 系列 设备或 用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此无法将包含具有这些操作的规则的文件策略应用于这些设备。

提示　要复制现有文件策略，请点击复制图标 ( )，然后在出现的对话框中为新策略键入唯一名称。然后就可以修改副本。

要创建文件策略，请执行以下操作：

访问：管理员/访问管理员

步骤 1　选择 **Policies > Files**。

系统将显示 File Policies 页面。

步骤 2　点击 **New File Policy**。

随即出现 File Policies 对话框。

对于新策略，网络界面会指出该策略未在使用。如果编辑的是使用中的文件策略，则网络界面会告知您使用该文件策略的访问控制策略的数量。在这两种情况下，都可以点击文本以跳至 Access Control Policies 页面；请参阅第 12-1 页上的访问控制策略入门。

步骤 3　在 **Name** 和 **Description**（可选）字段中为新策略输入名称和描述，然后点击 **Save**。

系统将显示 File Policy Rules 选项卡。

步骤 4　向文件策略添加一个或多个规则。

借助文件规则，可以精细控制要对其记录、阻止或扫描恶意软件的文件类型。有关添加文件规则的信息，请参阅第 37-15 页上的使用文件规则。

由于不能对 DC500 使用恶意软件许可证，因此无法创建使用 Block Malware 或 Malware Cloud Lookup 操作的文件规则，也无法使用该设备来应用包含具有这些操作的规则的文件策略。同样，由于不能在2 系列 设备或 用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此无法将包含具有这些操作的规则的文件策略应用于这些设备。

步骤 5　配置高级选项。有关详细信息，请参阅第 37-17 页上的配置高级文件策略常规选项和第 37-18 页上的配置存档文件检查选项。

步骤 6　点击 **Save**。

要使用新策略，必须向访问控制规则添加文件策略，然后应用该访问控制策略。如果编辑的是现有文件策略，必须重新应用任何使用该文件策略的访问控制策略。

使用文件规则

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

文件策略必须包含一个或多个规则才能生效。可以在 File Policy Rules 页面上创建、编辑和删除规则，该页面在您创建新文件策略或编辑现有策略时出现。该页面列出策略中的所有规则以及每个规则的基本特征。

该页面还提供有关使用此文件策略的访问控制策略数量的通知。可以点击通知以显示父策略的列表，并或者转至 Access Control Policies 页面。

要创建文件规则，请执行以下操作：

访问：管理员/访问管理员

步骤 1　选择 **Policies > Files**。

系统将显示 File Policies 页面。

步骤 2　您有以下选项：

- 要向新策略添加规则，请点击 **New File Policy** 创建新策略；请参阅第 37-14 页上的创建文件策略。
- 要向现有策略添加规则，请点击策略旁边的编辑图标 ( )。

步骤 3　在显示的 File Policy Rules 页面上，点击 **Add File Rule**。

系统将显示 Add File Rule 对话框。

步骤 4　选择 **Application Protocol**。

Any（默认值）检测 HTTP、 SMTP、 IMAP、 POP3、 FTP 和 NetBIOS-ssn (SMB) 流量中的文件。

步骤 5　选择 **Direction of Transfer**。

可以为下载的文件检查以下类型的传入流量：

- HTTP
- IMAP
- POP3
- FTP
- NetBIOS-ssn (SMB)

可以为上传的文件检查以下类型的传出流量：

- HTTP
- FTP
- SMTP
- NetBIOS-ssn (SMB)

无论用户是发送还是接收，使用 **Any** 都可通过多种应用协议检测文件。

步骤 6　选择文件规则 **Action**。有关详细信息，请参阅文件规则操作表。

选择 Block Files 或 Block Malware 时，默认会启用 **Reset Connection**。如果在发生文件传输受阻时不重置连接，请清除此选项。

注　思科建议保持启用 **Reset Connection**，以防止受阻应用会话保持打开，直到 TCP 连接重置为止。

有关文件规则操作的详细信息，请参阅第 37-10 页上的文件规则操作和评估顺序。

请注意，由于 DC500 无法使用恶意软件许可证，因此无法创建使用 Block Malware 或 Malware Cloud Lookup 操作的文件规则，也无法使用该设备来应用包含具有这些操作的规则的文件策略。同样，由于不能在2 系列 设备或 用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此无法将包含具有这些操作的规则的文件策略应用于这些设备。

步骤 7　选择一个或多个**文件类型**。使用 Shift 和 Ctrl 键以选择多个文件类型。可以通过以下方式过滤文件类型列表：

- 选择一个或多个**文件类型类别**。
- 按名称或描述搜索文件类型。例如，在 **Search name and description** 字段中键入 `Windows` 将会显示 Microsoft Windows 专用文件的列表。

提示　将指针悬停在文件类型上方可查看其描述。

可以在文件规则中使用的文件类型取决于您对 **Application Protocol**、**Direction of Transfer** 和 **Action** 所做的选择。

例如，为 **Direction of Transfer** 选择 **Download** 会删除 `GIF`、`PNG`、`JPEG`、`TIFF` 和 `ICO`（从 **Graphics** 类别中）以防止文件事件过量。

步骤 8　将所选文件类型添加到 **Selected Files Categories and Types** 列表：

- 点击 **Add** 以将所选文件类型添加到规则。
- 将一个或多个文件类型拖放到 **Selected Files Categories and Types** 列表中。
- 在选定类别的情况下，点击 **All types in selected Categories**，然后点击 **Add** 或将该选择拖放到 **Selected Files Categories and Types** 列表。

步骤 9　点击 **Save**。

文件规则即被添加到策略。如果编辑的是现有文件策略，必须重新应用任何使用该文件策略的访问控制策略，所做的更改才能生效。

配置高级文件策略常规选项

许可证：恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

在文件策略中，可以在 General 部分中设置以下高级选项。有关高级 Archive File Inspection 选项的信息，请参阅第 37-18 页上的配置存档文件检查选项。

表 37-7　高级文件策略常规选项

字段	说明	默认值
Enable Custom Detection List	选择此字段可在检测到自定义检测列表时阻止其中的文件。	启用
Enable Clean List	选择此字段可在检测到白名单时允许其中的文件。	启用
Mark files as malware based on dynamic analysis threat score	选择阈值可自动将具有该威胁评分或更高评分的文件视为如同恶意软件。选择 **Disabled** 可禁用此字段。 请注意，选择下限阈值时，可以增大作为恶意软件处理的文件的数量。根据文件策略中选择的操作，这可能导致受阻文件数增加。	极高（76 及以上）

请注意，由于不能对 DC500 使用恶意软件许可证，因此无法使用或修改这些设置。同样，由于不能在2 系列 设备或 用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此无法应用已启用这些设置的文件策略。

要配置高级文件策略常规选项，请执行以下操作：

访问：管理员/访问管理员

步骤 1　选择 **Policies > Files**。

系统将显示 File Policies 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

系统将显示 File Policy Rule 页面。

步骤 3　选择 **Advanced** 选项卡。

系统将显示 Advanced 选项卡。

步骤 4　在 **General** 部分中，修改选项，如高级文件策略常规选项表中所述。

步骤 5　点击 **Save**。

您必须重新应用任何使用已编辑的文件策略的访问控制策略。

配置存档文件检查选项

许可证：恶意软件

受支持的设备：除 2 系列或 X -系列外的所有型号

受支持的防御中心：除 DC500 外的所有型号

存档文件 （例如， `.zip` 或 `.rar`）经常出现在受监控流量中。其中一些可以方便地压缩和传输合法的信息；另一些可能试图隐藏恶意软件或其他不需要的文件。您可以将您的文件策略配置为检查存档文件的内容，这样就可以根据贵组织的需求分析和 （可选）阻止存档文件。所有适用于未压缩的文件的功能 （例如，动态分析和文件存储）也适用于存档文件中的嵌套文件。您可以从事件查看器或文件轨迹查看器使用上下文菜单查看存档文件的内容；有关详细信息，请参阅以下部分：第 37-19 页上的查看存档文件的内容。

注 如果包含存档文件的流量被安全情报列入黑名单或白名单，或者，如果顶级存档文件的 SHA -256 值在自定义检测列表中，则系统将不检查该存档文件的内容。如果嵌套文件被列入黑名单，则整个存档也将被阻止；但是，如果嵌套文件被列入白名单，则存档不会自动通过 （取决于任何其他嵌套文件和特性）。有关详细信息，请参阅第 3-6 页上的使用全局白名单和黑名单。

某些存档文件包含其他的存档文件 （以此类推）。文件嵌套的级别是其*存档文件深度*。请注意，深度计数中未计入顶级存档文件；深度从 1 （第一级嵌套文件）开始。虽然系统最多只能检查 3 级嵌套存档文件，但是可以将文件策略配置为阻止超过该深度 （或指定的较低最文件深度）的存档文件。如果要进一步限制嵌套文件，则可以选择配置较低的最大文件深度 （2 或 1）。如果您选择不阻止超过最大存档文件深度 3 的文件，当受监控流量中出现包含某些可提取内容和某些嵌套深度为 3 或更大值的内容的存档文件时，系统仅检查其能够检查的文件并报告相关数据。

将根据存档文件包含的文件性质赋予其性质。对于包含已确定的恶意软件文件的**所有**存档，将赋予其 `Malware` 性质。对于不含已确定恶意软件文件的存档，如果其包含任何未知文件，则其性质为 `Unknown`；如果其仅包含安全文件，则其性质为 `Clean`。有关文件性质的详细信息，请参阅第 37-3 页上的了解文件性质。

下表列出了可在您的文件策略中配置的存档文件检查选项。

表 37-8　　存档文件检查选项

字段	说明	默认值
Inspect Archives	选择此选项可检查存档文件的内容。如果取消选择此选项，下面的选项将变灰且不可用。	禁用
Block Encrypted Archives	选择此选项可阻止包含加密内容的存档文件。	禁用
Block Uninspectable Archives	选择此选项可阻止系统因加密以外的其他原因无法检查其内容的存档文件（这通常适用于以某种方式被毁损的文件，或超过指定的最大存档深度的存档文件）。	启用
Max Archive Depth	指定嵌套存档文件的最大深度。超过此深度的存档文件将被阻止。值必须是 `1`、`2` 或 `3`。此计数中未计入顶级存档文件；深度从 1 （第一级嵌套文件）开始。	`2`

要配置存档文件检查选项，请执行以下操作：

访问：管理员/访问管理员

步骤 1　选择 **Policies > Files**。

系统将显示 File Policies 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

系统将显示 File Policy Rule 页面。

步骤 3　选择 **Advanced** 选项卡。

系统将显示 Advanced 选项卡。

步骤 4　在 **Archive File Inspection** 部分中，修改选项，如存档文件检查选项表中所述。

步骤 5　点击 **Save**。

您必须重新应用任何使用已编辑的文件策略的访问控制策略。

查看存档文件的内容

许可证：恶意软件

受支持的设备：除 2 系列或 X -系列外的所有型号

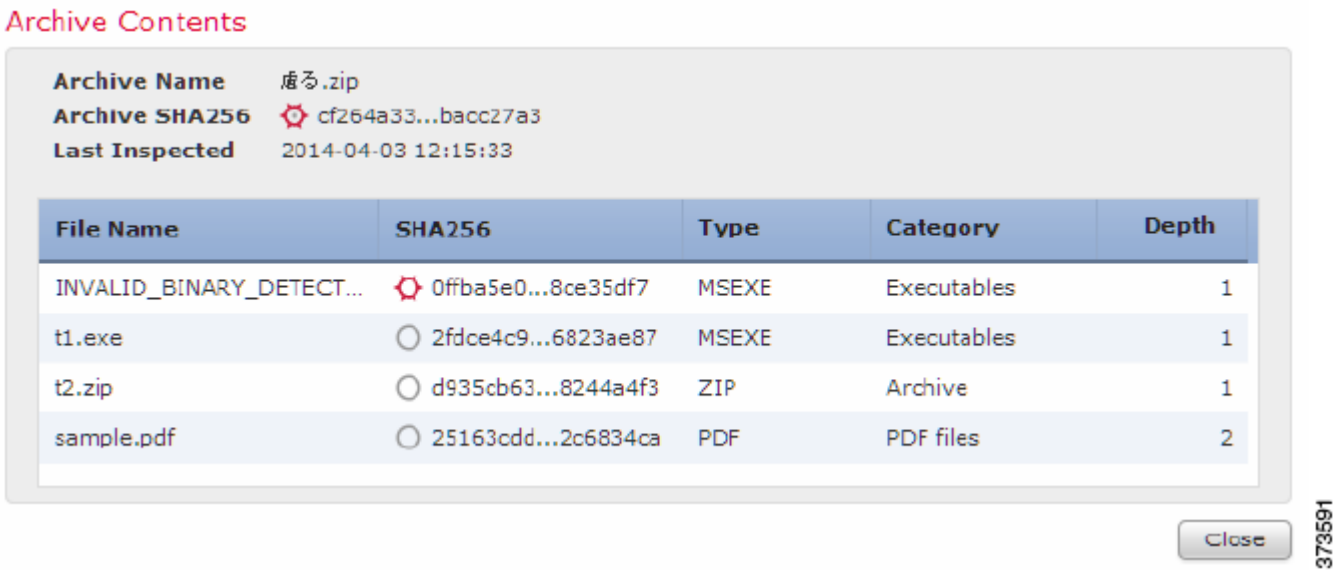
受支持的防御中心：除 DC500 外的所有型号

如将文件策略配置为检查存档文件内容，当存档文件出现在文件事件、恶意软件事件或捕获的文件中时，可以使用事件查看器上下文菜单和网络文件轨迹查看器查看有关存档内部文件的信息。

有关详细信息，请参阅：

- 第 2-4 页上的使用上下文菜单
- 第 40-7 页上的查看文件事件
- 第 40-16 页上的查看恶意软件事件
- 第 40-26 页上的查看捕获的文件
- 第 40-31 页上的审核网络文件轨迹

您可通过两种方式查看 Archive Contents 窗口：从事件查看器查看，只需右键单击合格的存档文件并从上下文菜单选择 **View Archive Contents**；或从存档文件的文件轨迹视图查看，只需点击 **Archive Contents** 下方的查看图标 ( )。在两种情况下，显示的窗口均相同。下图是 Archive Contents 窗口的示例。



存档的所有文件内容均以表形式列出，同时显示其相关信息的摘要：名称、 SHA-256 哈希值、类型、类别和存档深度。每个文件旁均显示一个网络文件轨迹图标，点击该图标即可通过网络轨迹功能查看有关该特定文件的详细信息。

要从事件查看器查看存档文件的内容，请执行以下操作：

访问：管理员/访问管理员

步骤 1　导航到您选择的事件查看器。您会看到三个选项：

- 对于恶意软件事件，请选择 **Analysis > Files > Malware Events**。
- 对于文件事件，请选择 **Analysis > Files > File Events**。
- 对于捕获的文件，请选择 **Analysis > Files > Captured Files**。

系统将显示默认事件工作流程首页。

步骤 2　右键单击显示了您要检查的存档文件的表行。

系统将显示上下文菜单。

步骤 3　从上下文菜单中，点击 **View Archive Contents**。

系统将显示 Archive Contents 窗口。

要从文件轨迹查看器查看存档文件的内容，请执行以下操作：

访问：管理员/访问管理员

步骤 1　选择 **Analysis > Files > Network File Trajectory**。

系统将显示 Network File Trajectory List 页面。

步骤 2　点击与您要检查的存档文件相对应的文件轨迹图标 ( )。

系统将显该文件的文件轨迹页面。

步骤 3　点击 **Archive Contents** 下方的查看图标 ( )。

系统将显示 Archive Contents 窗口。

比较两个文件策略

许可证：保护

要查看策略更改是否符合贵组织的标准或者要优化系统性能，您可以检查任意两个文件策略之间的差异或同一策略的两个修订版本。

文件策略*比较视图*并排显示两个文件策略或修订版本，其中上次修改时间和上次修改的用户显示在每个策略名称旁边。两个策略之间的差异将会突出显示：

- 蓝色指示突出显示的设置在两个策略中不同，不同之处以红色文本标注。
- 绿色指示突出显示的设置在一个策略中存在，但在另一个策略中不存在。

可以通过点击 **Previous** 和 **Next** 浏览差异。在左右两侧之间以双箭头图标 ( ) 为中心移动，**Difference** 数字调整为识别您正在查看哪个差异。或者，您可以生成文件策略*比较报告*，它是比较视图的 PDF 版本。

要比较两个文件策略，请执行以下操作：

访问：管理员/访问管理员

步骤 1　选择 **Policies > Files**。

系统将显示 File Policies 页面。

步骤 2　点击 **Compare Policies**。

系统将显示 Select Comparison 对话框。

步骤 3　从 **Compare Against** 下拉列表中选择要进行比较的类型：

- 要比较两个不同策略，请选择 **Running Configuration** 或 **Other Policy**。两个选项之间的实际区别是，如果选择 **Running Configuration**，则系统会将您的比较选项之一限制为当前应用的文件策略集。
- 要比较同一策略的修订版本，请选择 **Other Revision**。

对话框将会刷新，显示比较选项。

步骤 4　根据您选择的比较类型，有以下选项可供选择：

- 如果比较的是两个不同策略，请选择您要比较的策略：**Policy A** 或 **Target/Running Configuration A** 和 **Policy B**。
- 如果比较的是同一策略的修订版本，请选择要使用的 **Policy**，然后选择两个修订版本：**Revision A** 和 **Revision B**。修订版本按日期和用户名进行列出。

步骤 5　点击 **OK**。

系统将显示比较视图。

步骤 6　或者点击 **Comparison Report** 生成访问控制策略比较报告。

系统将显示比较报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

为 FireAMP 处理云连接

许可证：任何环境

FireAMP 是思科的企业级高级恶意软件分析和防护解决方案。如果贵组织有订用 FireAMP，则个人用户可以在其计算机和移动设备上安装 FireAMP 连接器。这些轻量级代理与思科云通信，后者又与防御中心通信。在配置防御中心并将其连接到云后，即可接收扫描、恶意软件检测和隔离的记录。记录作为恶意软件事件存储在防御中心数据库中。有关详细信息，请参阅第 37-2 页上的了解恶意软件防护和文件控制。

如果贵组织的安全策略不允许使用传统云服务器连接，则可获取并配置思科的私有内部云解决方案， FireAMP私有云是一种虚拟机，充当公共思科云的压缩本地版本。在此情况下，通常涉及云连接的数据和操作 （例如，来自 FireAMP 连接器的事件、文件性质查找、追溯性事件等）改为通过与私有云的本地连接来处理。当需要连接外部云时 （例如用于文件性质查找），私有云充当防御中心与公共思科云之间的匿名代理。借助于私有云，不通过外部连接共享终端事件数据。有关配置私有云的详细信息，请参阅第 37-24 页上的与 FireAMP 私有云协作的。

注　私有云不支持动态分析。

当在安装有 FireAMP 连接器的主机上检测到的基于终端的恶意软件检测活动表明该主机的安全性可能受到威胁时，该主机也生成生成危害表现 (IOC) 标记。要从防御中心查看某个主机的终端 IOC 信息，该主机必须显示在防御中心的网络映射上。思科不时会为基于终端的恶意软件事件开发新的 IOC 类型，系统可从思科云自动下载这些类型。有关威胁表现的详细信息，请参阅第 45-17 页上的了解危害表现和第 45-17 页上的基于终端的恶意软件事件 IOC 类型。

部署中的每个防御中心都可连接到思科云。默认情况下，云发送贵组织内所有组的恶意软件事件，但是在配置连接时可以按组进行限制。

互联网接入和高可用性

系统使用端口 443/HTTPS 连接到思科云 （公共或私有）以接收基于终端的恶意软件事件。必须在防御中心上打开该端口 （出站和入站）。此外，防御中心必须可以直接访问互联网。默认运行状况策略包括FireAMP状态监控，如果防御中心在初始成功连接后无法连接到云，或者如果使用FireAMP门户注销了连接，则会向您发出警告。

接收基于终端的恶意软件事件的云连接**未**在高可用性对的成员之间共享。要确保操作的连续性，请将主和辅助防御中心均连接到云。

管理云连接

使用防御中心的 AMP Management 页面 (**AMP > AMP Management**) 可以查看和创建与思科云或私有云的连接，以及禁用并删除这些连接。

旋转状态图标表示连接处于待定状态，例如，如果已在防御中心上配置连接，但现在必须使用 FireAMP 门户对连接进行授权。失败或拒绝图标 ( ) 表示云已拒绝连接，或者连接因其他原因而失败。

提示　点击任意云名称即可在新浏览器窗口中打开 FireAMP 门户。

有关详细信息，请参阅：

- 第 37-22 页上的创建思科云连接
- 第 37-23 页上的删除或禁用云连接
- 第 37-24 页上的与 FireAMP 私有云协作的

创建思科云连接

许可证：任何环境

在防御中心和思科云之间创建连接分两步执行。首先，配置防御中心以连接到云。然后，登录 FireAMP 门户以对连接进行授权。如果您没有订用 FireAMP，则无法完成注册过程。

要重新注册在注册到云时已恢复为出厂默认设置或还原的防御中心，必须连接到 FireAMP 并删除防御中心，然后进行重新注册。

要为 FireAMP 创建思科云连接，请执行以下操作：

访问：管理

步骤 1　选择 **AMP > AMP Management**。

系统将显示 AMP Management 页面。

步骤 2　点击 **Create FireAMP Connection**。

系统将显示 Create FireAMP Connection 对话框。

步骤 3　从 **Cloud Name** 下拉框中，选择要使用的云服务：

- 对于欧盟云，请选择 **EU Cloud**。
- 对于美国云，请选择 **US Cloud**。
- 对于私有云，请选择 **Private Cloud**，然后按照第 37-24 页上的与 FireAMP 私有云协作的中所述的其他步骤操作。

步骤 4　点击 **Register**。

步骤 5　确认是否要继续连接到 FireAMP 门户，然后登录门户。

系统将显示门户上 Applications 页面。使用此页面授权思科云将恶意软件事件发送到防御中心。

步骤 6　或者，选择贵组织内要为其接收恶意软件事件的特定组。

仅在要限制接收的事件的情况下才选择组。默认情况下，防御中心为所有组接收恶意软件事件。

提示　要管理组，请在 FireAMP 门户上选择 **Management > Groups**。有关详细信息，请参阅门户的联机帮助。

步骤 7　点击 **Allow**。

将返回到防御中心上的 FireAMP Management 页面。此时，连接已启用，并且防御中心开始从云接收恶意软件事件。

点击 **Deny** 也会返回到防御中心，但其中云连接标记为“已拒绝”。同样，如果导航离开 FireAMP 门户上的 Applications 页面，并且既未拒绝也未允许连接，则连接在防御中心的网络界面上标记为“待处理”。运行状况监控器在其中任一情况下都不发出警报。如果稍后要连接到云，则必须删除失败或待处理的连接，然后重新创建连接。

删除或禁用云连接

许可证：任何环境

如果您不想再从云接收恶意软件事件，请删除思科云连接或私有云连接。要暂时停止为特定连接发送恶意软件事件，可以禁用连接而不是将其删除。在这种情况下，云会存储事件，直到您重新启用连接为止；然后，云会发送存储的事件。

注意事项　在极少数情况下 （例如，事件率超高或连接长时间禁用），云在连接被禁用时可能无法存储生成的所有事件。

请注意，使用 FireAMP 门户 （而不是防御中心的网络界面）注销连接会停止发送事件，但不会从防御中心中删除连接。注销连接会在 FireAMP Management 页面上显示失败状态，必须将其删除。

要使用防御中心启用或禁用云连接，请执行以下操作：

访问：管理

步骤 1　在 AMP Management 页面上，点击要删除的连接旁边的滑块，然后确认要启用还是禁用该连接。

启用连接后，云开始将事件发送到防御中心，包括禁用连接时发生的任何事件。云不会为已禁用的连接发送事件。

要使用防御中心删除云连接，请执行以下操作：

访问：管理

步骤 1　在 AMP Management 页面上，点击要删除的连接旁边的删除图标 ( )，然后确认要删除该连接。

系统删除连接，并且云停止将事件发送到防御中心。

与 FireAMP 私有云协作的

许可证：任何环境

贵组织可能担心隐私或安全，以致在监控网络和外部云服务器之间难以或无法进行频繁连接。在这种情况下，可以获取并配置 FireAMP 私有云，它是思科专用虚拟机，充当您的网络与 思科 FireAMP 云之间的安全中介。与公共、外部思科云的所有必需连接 （而不仅是许多设备的可识别连接）均通过私有云进行筛选，私有云充当匿名代理，以确保受监控网络的安全和隐私。每个私有云可以支持多达 10,000 个独立的连接器。您可以在网络中配置多个私有云以满足贵组织的需求。

FireAMP 私有云处理文件性质查找、基于终端的 FireAMP 事件检索和追溯性恶意软件事件生成的基于云的操作。私有云 （代替公共云）从 FireAMP 连接器终端收集恶意软件事件并将其传输到防御中心。只有对公共思科云的查询 （用于确定文件性质和 SHA-256 值等）会通过匿名代理私有云连接离开网络。终端事件数据从不离开您的网络。

有关基于云的文件和恶意软件功能的详细信息，请参阅：

- 第 37-2 页上的了解恶意软件防护和文件控制
- 第 37-6 页上的集成 FireAMP 与 FireSIGHT 系统
- 第 40-4 页上的使用动态分析
- 第 40-14 页上的基于终端 (FireAMP) 的恶意软件事件
- 第 40-15 页上的追溯性恶意软件事件

在本文档及与私有云的受支持功能相关的其他文档中，提到的所有“云”或“思科云”也适用于通过私有云进行的连接，除非另有说明。私有云具有相同的开放端口，并具有与标准云连接相同的高可用性限制。

注　FireAMP 私有云仅支持与恶意软件和文件相关的基于云的功能，而不支持其他使用云连接的 FireSIGHT 系统功能，例如 URL 过滤或安全情报。私有云还不支持动态分析功能，不过，您可以使用私有云检索思科已动态分析的文件的威胁得分。

要在防御中心与 FireAMP 私有云之间创建连接，必须首先按照 《*FireAMP 私有云管理门户用户指南*》（可在支持网站上获取）中所述的操作步骤配置 FireAMP 私有云。在进行配置期间，请务必记下 FireAMP **Console** 字段中显示的私有云主机名；您必须具有此主机名才能将私有云连接到防御中心。请注意，成功配置私有云会自动禁用可能已配置的任何公共云连接。

要在防御中心和 FireAMP 私有云之间创建连接，请执行以下操作：

访问：管理

步骤 1　选择 **AMP > AMP Management**。

系统将显示 AMP Management 页面。

步骤 2　点击 **Create FireAMP Connection**。

系统将显示 Create FireAMP Connection 对话框。

步骤 3　从 **Cloud Name** 下拉列表中，选择 **Private Cloud**。

对话框中显示其他字段。

步骤 4　在 **Name** 字段中，键入私有云连接的名称。查看恶意软件事件时， FireAMP 云事件字段中会显示此名称。

步骤 5　在 **Host** 字段中，键入私有云的主机名 （即，配置 FireAMP 私有云虚拟机时显示在 FireAMP Console 字段中的名称）。

步骤 6　在 **Certificate Upload Path** 字段中，浏览至有关私有云的有效 TLS 或 SSL 加密证书信息的位置。有关详细信息，请参阅 《*FireAMP 私有云管理门户用户指南*》。

步骤 7　如果为监控网络配置了多个私有云并要确定哪个私有云处理基于网络的恶意软件查找，请选择或清除 **Use For NetworkAMP** 复选框。如果仅配置了一个私有云，则默认情况下会选择此复选框且无法清除。

步骤 8　如果您在防御中心上配置了代理连接并想要将该代理连接用于私有云，请选择 **Use Proxy for Connection** 复选框。如未选择此选项，则私有云不将您配置的代理用于其通信。

步骤 9　点击 **Register**。

系统将显示一个对话框，提醒您创建私有云配置会禁用可能已配置的所有公共云连接。

步骤 10　点击 **Yes**。

确认是否要继续连接到 FireAMP 门户，然后登录门户。

步骤 11　系统处理私有云信息并将您重定向到FireAMP站点以完成配置。有关进一步说明，请参阅 《*FireAMP 私有云管理门户用户指南*》。

记录网络流量中的连接

在受管设备监控网络主机生成的流量时，其可为其检测到的连接生成日志。访问控制和 SSL 策略中的各种设置可供您精细控制记录哪些连接、何时记录连接以及在何处存储数据。访问控制规则的特定日志记录配置还可以确定您是否记录与该连接相关联的文件和恶意软件事件。

在大多数情况下，您均可记录连接的开始和/或结束。当您记录连接时，系统将生成*连接事件*。无论何时基于声誉的安全情报功能阻止连接或将其列入黑名单，您均可记录一种特殊类型的连接事件，称为*安全情报事件*。

连接事件包含有关已检测会话的数据。任何个别连接事件的可用信息取决于多种因素，但是通常包括：

- 基本连接属性：时间戳、源和目标 IP 地址、入口和出口区域，处理连接的设备等
- 系统发现或推断的其他连接属性：应用、请求的 URL 或与连接关联的用户等
- 有关连接记录原因的元数据：哪个策略中的哪条访问控制规则 （或其他配置）处理了流量，连接是被允许还是被阻止，以及有关已加密和已解密连接的详细信息等

您应该根据组织的安全和合规性要求记录连接。除了那些在到达访问控制之前于设备级别使用快速路径的连接，您可以记录**任何**连接。

通过将连接事件保存到防御中心数据库，您可以利用 FireSIGHT 系统的许多报告、分析和数据关联功能；请参阅第 39-1 页上的使用连接与安全情报数据。或者，您可以将连接数据发送到外部系统日志 (syslog) 或 SNMP 陷阱服务器。

要补充受管设备采集到的连接数据，您可以使用由 NetFlow 启用设备生成的记录来生成连接事件。如果将 NetFlow 启用设备部署在FireSIGHT 系统受管设备无法监控的网络中，则此功能特别有用。

注 由于 NetFlow 数据收集与访问控制无关联，因此您无法对想要记录的 NetFlow 连接进行精细控制。 FireSIGHT 系统受管设备检测由 NetFlow 启用设备导出的记录，依据这些记录中的数据生成单向连接结束事件，并最终将这些事件发送至防御中心，以便在数据库中进行记录。 NetFlow 记录无法生成安全情报事件，也不会被记录到外部服务器中。有关详细信息，请参阅第 45-14 页上的了解 NetFlow。

有关记录连接数据的详细信息，请参阅：

决定要记录哪些连接

许可证：任何环境

利用访问控制和 SSL 策略中的各种设置，您可以记录您的设备监控的所有非快速路径连接。在大多数情况下，您均可记录连接的开始和/或结束。然而，因为受阻流量会被立即拒绝，无需进一步检查，在大多数情况下，您只能记录已阻止或列入黑名单的流量的连接开始事件；没有要记录的唯一连接结束。

当您记录连接事件后，您可以将它保存至防御中心数据库，以便使用 FireSIGHT 系统进行进一步分析。或者，您可以将连接数据发送到外部系统日志或 SNMP 陷阱服务器。

提示 要使用 FireSIGHT 系统对连接数据执行详细分析，思科建议您将关键连接的结束事件记录到防御中心数据库中。

有关详情，请参阅：

- 第 38-2 页上的记录关键连接
- 第 38-3 页上的记录连接的开始或结束事件
- 第 38-4 页上的将连接事件记录到防御中心或外部服务器中
- 第 38-5 页上的了解访问控制和 SSL 规则操作如何影响日志记录
- 第 38-8 页上的连接记录的许可证和型号要求

记录关键连接

许可证：任何环境

您应该根据组织的安全和合规性要求记录连接。如果您的目标是限制所生成事件的数量和提高性能，则只能启用对分析至关重要的连接的日志记录。然而，如果出于分析目的，您想要广泛了解网络流量，则可启用其他连接的日志记录。访问控制和 SSL 策略中的各种设置可供您精细控制记录哪些连接、何时记录连接以及在何处存储数据。

注意事项 在拒绝服务 (DoS) 攻击期间，记录受阻 TCP 连接可能会影响系统的性能，而且多个类似事件使数据库系统不堪重负。在对 Block 规则启用日志记录之前，请考虑该规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口上的流量。

除了您可以配置的日志记录，系统还会自动记录在其中检测到受禁文件、恶意软件或入侵尝试的大多数连接。除非您使用系统策略完全禁用连接事件存储，否则无论您的其他日志记录配置如何，系统均将这些连接结束事件保存至防御中心数据库，以供进一步分析。所有连接事件都会使用 Action 和 Reason 字段反映为何会被自动记录；请参阅第 39-4 页上的 Action和第 39-7 页上的 Reason。

安全情报黑名单决策 （可选）

每当基于声誉的安全情报功能阻止连接或将其接列入黑名单，您均可记录该连接。或者，如同被动部署中的建议，您可使用仅监控设置进行安全情报过滤。这使得系统可以进一步分析本应列入黑名单的连接，并仍将匹配项记录至黑名单。通过安全情报监控，您还可以使用安全情报信息创建流量配置文件。

当您启用安全情报日志记录时，黑名单匹配项会生成安全情报事件以及连接事件。安全情报事件是您可以单独查看和分析的一种特殊类型的事件，也可以单独存储和删除。有关详细信息，请参阅第 38-9 页上的记录安全情报 （黑名单）决策。

已加密连接 （可选）

您可以根据 SSL 策略中的设置，在系统阻止已加密会话时记录连接。您还可以强制系统记录其传递供访问控制规则进一步评估的连接，无论您是否解密具体流量，也无论系统之后如何处理或检查该流量。您可以按每条 SSL 规则配置此日志记录功能，以便仅记录关键连接。有关详细信息，请参阅第 38-11 页上的记录已加密连接。

访问控制处理 （可选）

您可以在访问控制规则或访问控制默认操作处理连接时记录该连接。您可以按每条访问控制规则配置此日志记录功能，以便仅记录关键连接。有关详细信息，请参阅第 38-13 页上的根据访问控制处理记录连接。

与入侵关联的连接 （自动）

访问控制规则调用的入侵策略 （请参阅第 14-1 页上的使用访问控制规则调整流量）检测到入侵并生成入侵事件时，系统会将发生入侵连接结束自动记录至防御中心数据库，而无论该规则的日志记录配置如何。

但是，当与访问控制默认操作 （请参阅第 12-6 页上的设置对网络流量的默认处理和检查）相关联的入侵策略生成入侵事件时，系统**不会**自动记录关联连接的结束事件。您必须显式启用默认操作连接记录。对于不想记录任何连接数据的仅入侵防御部署，这十分有用。

对于入侵受阻的连接，连接记录中的连接操作为 `Block`，原因为 `Intrusion Block`，即使执行入侵检查，也必须使用 Allow 规则。

提示　要在 3 系列或虚拟设备上禁用该连接记录，请使用 CLI；请参阅第 D-30 页上的 log-ips-connections。

与文件和恶意软件事件关联的连接

访问控制规则调用的文件策略检测到受禁文件 （包括恶意软件）并生成文件或恶意软件事件时，系统会将检测到文件的连接结束自动记录至 数据库，而无论该访问控制规则的日志记录配置如何。防御中心您**无法**禁用该记录。

注　检查 NetBIOS-ssn (SMB) 流量所生成的文件事件不会立即生成连接事件，因为客户端和服务器构建一个持久连接。系统在客户端或服务器结束会话之后生成连接事件。

对于文件受阻的连接，连接记录中的连接操作为 `Block`，即便要执行文件和恶意软件检查，也必须使用 Allow 规则。连接原因是 `File Monitor` （文件类型或恶意软件被检测）或者是 `Malware Block` 或 `File Block` （文件被阻止）。

记录连接的开始或结束事件

许可证：任何环境

当系统检测到连接时，在大多数情况下您可以在其开始或其结束时记录该连接。

然而，因为受阻流量会被立即拒绝，无需进一步检查，在大多数情况下，您只能记录已阻止或列入黑名单的流量的连接开始事件；没有要记录的唯一连接结束。阻止已加密流量时例外。当在 SSL 策略中启用连接记录时，系统将记录连接结束而不是连接开始事件。这是因为，系统无法确定连接是否使用会话中第一个数据包加密，因此无法立即阻止已加密会话。

注　对于单一未受阻连接，连接结束事件限制包含连接开始事件中的所有信息，以及在会话期间收集到的信息。

要优化性能，请记录任何连接的开始或结束事件，而不是同时记录两者。您可以根据连接开始或连接结束事件触发关联规则。请注意，出于任何原因监控连接均会强制执行连接结束日志记录；请参阅第 38-5 页上的了解受监控连接的记录。

下表详细说明连接开始和结束事件之间的区别，包括两种记录各自的优势。

表 38-1　　连接开始和连接结束事件比较

	连接开始事件	连接结束事件
生成事件的条件	当系统检测到连接开始（或者在头几个数据包之后，如果事件生成取决于应用或 URL 识别）	当系统存在以下情况时： • 检测到连接关闭 • 一段时间以后未检测到连接结束 • 由于内存限制无法跟踪会话
记录对象...	安全情报或访问控制规则评估的所有连接，尽管您可能无法在所有位置配置连接结束日志记录	所有连接，不过您可能无法在所有位置配置连接结束记录
包含...	仅在第一个数据包中可以确定的信息（如果事件的生成取决于应用或 URL 标识，则包含在前几个数据包中确定的信息）	连接开始事件中的所有信息，加上通过检查会话期间的流量而确定的信息，例如，所传输的数据总量或连接中最后一个数据包的时间戳。
有用于...	如果您要记录： • 受阻止的连接，包括安全情报黑名单决策 • 仅记录连接开始事件，因为连接结束信息对您来说不重要	如果您要： • 记录由 SSL 策略处理的已加密连接 • 使用在会话持续期间收集的信息执行任何类型的详细分析或者触发关联规则 • 在自定义工作流程中查看连接汇总（汇聚连接数据），查看图形格式的连接数据或创建和使用流量配置文件

将连接事件记录到防御中心或外部服务器中

许可证：任何环境

您可以将连接记录到防御中心数据库，以及外部系统日志或 SNMP 陷阱服务器中。您必须为外部服务器配置一个叫做*警报响应*的连接，才能将连接数据记录到该外部服务器中；请参阅第 43-2 页上的使用警报响应。

通过将日志记录到防御中心数据库，您可以利用 FireSIGHT 系统的很多报告、分析和数据关联功能。例如：

- 控制面板和 Context Explorer 为您提供由系统记录的连接的图形化概览视图；请参阅第 55-1 页上的使用控制面板和第 56-1 页上的使用 Context Explorer。
- 事件视图显示有关系统记录的连接的详细信息，您可以用图形或表格格式显示这些信息，也可以汇总于报告中；请参阅第 39-1 页上的使用连接与安全情报数据。
- 流量分析使用连接数据创建正常网络流量的配置文件，然后您可以将其用作检测和跟踪异常行为的基准；请参阅第 53-1 页上的创建流量量变曲线。
- 通过关联策略，您可以对特定类型的连接或流量配置文件变更生成事件并触发响应（例如警报或外部补救）；请参阅第 51-2 页上的创建关联策略规则。

注　要使用这些功能，**必须**将连接记录到防御中心数据库（而且在大多数情况下，必须记录连接结束而非开始事件）。这就是为什么系统自动记录关键连接，即与记录的入侵、受禁文件和恶意软件关联的那些链接。

防御中心可以记录的连接和安全情报事件的数量取决于其型号。有关这些限制的列表和有关禁用连接事件存储的信息，请参阅第 63-14 页上的配置控制面板事件限制。

了解访问控制和 SSL 规则操作如何影响日志记录

许可证：因功能而异

每一条访问控制*和 SSL* 规则都有一个操作，该操作不仅可以确定系统如何检查和处理与该规则匹配的流量，而且可以确定您何时和如何记录关于匹配流量的详细信息。

注　记录访问控制和 SSL 策略默认操作允许的连接的处理略有不同；请参阅第 38-15 页上的记录访问控制默认操作处理的连接和第 38-12 页上的为已加密和不可解密连接设置默认日志记录。

有关详情，请参阅：

- 第 14-6 页上的使用规则操作确定流量处理和检查
- 第 21-7 页上的使用规则操作确定加密流量处理和检查
- 第 38-5 页上的了解受监控连接的记录
- 第 38-6 页上的了解受信任连接的记录
- 第 38-6 页上的了解受阻和交互式受阻连接的记录
- 第 38-7 页上的了解受允许连接的记录
- 第 38-7 页上的为允许的连接禁用文件和恶意软件事件日志记录

了解受监控连接的记录

许可证：因功能而异

系统始终会将后续连接的结束记录至 防御中心数据库，而无论稍后处理该连接的规则或默认操作的日志记录配置如何：

- 与设定为监控的安全情报黑名单匹配的连接
- 与 SSL Monitor 规则匹配的连接
- 与访问控制 Monitor 规则匹配的连接

换句话说，如果数据包匹配监控规则或安全情报监控的黑名单，即使该数据包不与其他规则匹配且您不对默认操作启用日志记录，系统也会始终记录该连接。每当系统由于安装情报过滤而记录连接事件时，它也会记录匹配的安全情报事件，这是一种您可以单独查看时和分析的特殊类型的连接事件；请参阅第 38-9 页上的记录安全情报（黑名单）决策。

由于受监控的流量始终会在之后由另一规则或默认操作进行处理，因此由于监控规则而记录的连接相关联的操作绝不会是 `Monitor`。相反，它反映规则的操作或之后处理该连接的默认操作；请参阅第 39-4 页上的 Action。

每当单一连接与与 SSL 或访问控制监控规则匹配时，系统均**不会**生成单独的事件。由于单一连接可能与多条监控规则相匹配，记录至 防御中心数据库的每个连接事件均可能包含和显示关于该连接匹配的前八条监控访问控制规则，以及第一条匹配的监控 SSL 规则的信息。

与此相似，如果您将连接事件发送至外部系统日志或 SNMP 陷阱服务器，则每当单一连接与监控规则相匹配时，系统均不会发送单独的警报。相反，系统在连接结束时发送的警报包含有关连接匹配的 Monitor 规则的信息。

提示　即使连接日志中的规则操作绝不会是 `Monitor`，但您仍然可以对匹配 Monitor 规则的连接触发关联策略违规。有关详细信息，请参阅第 51-4 页上的指定关联规则触发标准。

了解受信任连接的记录

许可证：因功能而异

受信任的连接由访问控制策略中的 Trust 访问控制规则或默认操作处理。您可以记录这些连接的开始和结束；然而，请记住，系统不会检查受信任连接是否存在发现数据、入侵或受禁文件和恶意软件，无论它们是否被加密。因此，受信任连接的事件只包含有限的信息。

请注意，系统以不同方式记录 Trust 访问控制规则处理的 TCP 连接，具体取决于检测到相关连接的设备：

- 对于 3 系列设备，Trust 规则在第一个数据包中检测到的 TCP 连接会根据是否存在之前启用的 Monitor 规则生成不同的事件。如果 Monitor 规则处于活动状态，则系统评估数据包并生成连接开始和结束事件。如果没有 Monitor 规则处于活动状态，则系统仅生成连接结束事件。
- 对于所有其他型号，Trust 规则在第一个数据包上检测到的 TCP 连接仅生成连接结束事件。系统会在最终会话数据包之后一小时生成事件。

了解受阻和交互式受阻连接的记录

许可证：因功能而异

当您记录受阻连接时，系统如何进行记录该连接取决于其受阻原因；当根据连接日志配置关联规则时，必须记住这一点：

- 对于阻止已加密流量的 SSL 规则和 SSL 策略默认操作，系统记录连接**结束**事件。这是因为系统无法确定连接是否使用会话中的第一个数据包加密。
- 对于阻止已解密或非加密流量的访问控制规则和访问控制策略默认操作 （包括交互式阻止规则），系统记录连接**开始**事件。匹配流量会被拒绝，无需进一步检查。

对于访问控制或 `SSL` 规则阻止的会话的连接事件，其操作为 `Block` 或 Block with reset。受阻加密连接的原因为 `SSL Block`。

当用户浏览受禁网站时，交互式阻止访问控制规则导致系统显示警告页面，该等规则可供您配置连接结束日志记录。这是因为，如果用户点击浏览警告页面，连接会被视为系统可以监控和记录的已允许的新连接；请参阅第 38-7 页上的了解受允许连接的记录。

因此，对于与交互式阻止或交互式阻止并重置规则相匹配的数据包，系统可以生成以下连接事件：

- 用户的请求最初被阻止且警告页面显示时的连接开始事件；该事件的关联操作为 `Interactive Block` 或 `Interactive Block with reset`
- 当用户点击警告页面并加载最初请求的页面时生成的多个连接开始或连接结束事件；这些事件的关联操作为 `Allow`，原因为 `User Bypass`

请注意，只有内联部署的设备才能阻止流量。因为受阻连接在被动部署中实际上未被阻止，所以，系统可能会报告每条受阻连接的多个连接开始事件。

注意事项 在拒绝服务 (DoS) 攻击期间，记录受阻 TCP 连接可能会影响系统的性能，而且多个类似事件使数据库系统不堪重负。在您启用阻止规则的日志记录之前，请考虑该规则是监控面向互联网的接口上的流量，还是易遭受 DoS 攻击的其他接口上的流量。

了解受允许连接的记录

许可证：因功能而异

加密 SSL 规则、不加密 SSL 规则以及 Allow 访问控制规则允许匹配流量传递至下一阶段的检查和流量处理。

无论您是否使用 SSL 规则解密已加密的流量，该流量均会继续接受访问控制规则的评估。如果您为该 SSL 规则启用日志记录，系统均会记录匹配连接的结束，无论访问控制规则或稍后处理它们的默认操作的日志记录配置如何。

当您通过访问控制规则允许流量时，可以使用关联的入侵或文件策略 （或二者），在流量可以达到其最终目标前，进一步检查流量和阻止入侵、受禁文件和恶意软件。然而，请注意，对于加密负载，文件和入侵检查已默认禁用。

将按以下方式记录与 Allow 访问控制规则匹配的流量的连接：

- 访问控制规则调用的入侵策略检测到入侵并生成入侵事件时，系统会将发生入侵连接结束自动记录至 防御中心数据库，无论该规则的日志记录配置如何。
- 访问控制规则调用的文件策略检测到受禁文件 （包括恶意软件）并生成文件或恶意软件事件时，系统会将检测到文件的连接结束自动记录至 数据库，而无论该访问控制规则的日志记录配置如何。防御中心
- 或者，对于所有允许的流量，包括系统视作安全的流量或您未使用入侵或文件策略检查的流量，您可以启用连接开始和连接结束日志记录。

对所有生成的连接事件， Action 和 Reason 字段均会反映为何记录事件；请参阅第 39-4 页上的 Action和第 39-7 页上的 Reason。请注意：

- `Allow` 操作代表达到其最终目标且被显示允许和用户绕过的交互式受阻连接。
- `Block` 操作代表首先被访问控制规则允许，但在其中检测到入侵、受禁文件或恶意软件的连接。

为允许的连接禁用文件和恶意软件事件日志记录

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

当您通过访问控制规则允许未加密或解密的流量时，可以使用关联的文件策略检查传输的文件，在其可以到达其目标前，阻止受禁文件和恶意软件；请参阅第 18-7 页上的调整的入侵防御性能。请注意，由于您无法在 DC500 上使用恶意软件许可证，也无法在 2 系列设备或用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此无法使用这些设备进行恶意软件防护。

当系统检测到受禁文件时，它会将以下事件类型之一自动记录至 防御中心数据库：

- *文件事件*，代表检测到或阻止的文件，包括恶意软件文件
- *恶意软件事件*，只代表被检测到或被阻止的恶意软件文件
- *可追溯的恶意软件事件*，其在之前检测到的文件的恶意软件性质变更时生成

如果您不想要记录文件或恶意软件事件，您可以通过清除访问控制规则编辑器的 Logging 选项卡上的 **Log Files** 复选框，来针对每条访问控制规则禁用此日志记录。有关完全禁用文件和恶意软件事件存储的信息，请参阅第 63-14 页上的配置控制面板事件限制。

注　思科建议您保持启用文件和恶意软件日志记录。

无论您是否保存文件和恶意软件事件，当网络流量违反文件策略时，系统均会自动将关联连接的结束记录至 防御中心数据库，而无论调用访问控制规则的日志记录配置如何；请参阅第 38-3 页上的与文件和恶意软件事件关联的连接。

连接记录的许可证和型号要求

许可证：因功能而异

因为您在访问控制和 SSL 策略中配置了连接日志记录，所以，您可以记录这些策略能够成功处理的任何连接。

虽然不管 防御中心上的许可证如何您均可创建访问控制和 SSL 策略，但访问控制的某些方面要求您先在目标设备上启用特定许可功能，然后才可能应用该策略。此外，一些功能仅在某些型号上可用。

请注意，利用防御中心随附的 FireSIGHT 许可证，您可以根据连接记录中的信息将主机、用户和应用数据添加到网络映射中以及查看与连接事件关联的危害表现 (IOC)。除了 DC500，您也可以查看与连接关联的地理位置数据 （源或目标国家/地区或大陆）。

下表说明您必须具备哪些许可证，才能成功配置 SSL 检查，从而记录由访问控制策略处理的连接。

表 38-2　访问控制策略中对于连接记录的许可证和型号要求

要记录连接...	许可证	支持的防御中心。	支持的设备
对使用网络、 VLAN、端口或文字 URL 条件处理的流量	任何环境	任何环境	任何设备，除了： • 2 系列设备无法执行 URL 过滤 • ASA FirePOWER 设备无法执行 VLAN 过滤
对使用地理定位数据处理的流量	FireSIGHT	除 DC500 外的所有型号	任何设备， 2 系列或 X -系列除外
关联于： • 声誉不良的 IP 地址 （安全情报过滤） • 未加密或解密流量中的入侵或受禁文件	保护	任何环境	任意设备，除了 2 系列设备不能执行安全情报过滤之外
与未加密或解密流量中检测到的恶意软件关联	恶意软件	除 DC500 外的所有型号	任何设备， 2 系列或 X -系列除外
对通过用户控制或应用控制处理的流量	可控性	除 DC500 外的所有型号	任何设备， 2 系列或 X -系列除外
对于系统使用 URL 类别和声誉数据进行过滤的流量，为受监控主机请求的 URL 显示 URL 类别和 URL 声誉信息	URL 过滤	除 DC500 外的所有型号	任何设备，除了 2 系列

下表说明您必须具备哪些许可证，才能成功配置 SSL 检查，从而记录由 SSL 策略处理的连接。请记住，即使已加密连接未被 SSL 策略记录 （甚至在已检查的情况下），仍可能因其他原因被记录。

表 38-3　　SSL 策略中对于连接记录的许可证和型号要求

要记录连接...	许可证	支持的防御中心。	支持的设备
对使用区域、网络、 VLAN、端口或 SSL 相关条件处理的已加密流量	任何环境	任何环境	3 系列
对使用地理定位数据处理的已加密流量	FireSIGHT	除 DC500 外的所有型号	3 系列
对使用应用或用户条件处理的已加密流量	可控性	除 DC500 外的所有型号	3 系列
对系统使用 URL 类别和信誉数据过滤的已加密流量	URL 过滤	除 DC500 外的所有型号	3 系列

记录安全情报 （黑名单）决策

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

作为抵御恶意互联网内容的第一道防线， FireSIGHT 系统包含安全情报功能，该功能可供您根据最新声誉情报立即将连接列入黑名单 （加以阻止），再也无需资源更密集的深入分析 。尽管该流量过滤确实发生在诸如使用快速路径的硬件级别处理之后，但是它会在基于策略的任何其他检查、分析或流量处理**之前**进行。

或者，如同被动部署中的建议，您可使用仅监控设置进行安全情报过滤。这使得系统可以进一步分析本应列入黑名单的连接，并仍将匹配项记录至黑名单。

注　如果想要根据安全情报信息创建流量量变曲线，或使用连接结束事件中的安全情报信息触发关联规则，则**必须**将该信息记录到防御中心数据库。首先，启用安全情报日志记录。然后，使用仅监控安全情报对象构建黑名单。有关详细信息，请参阅第 13-1 页上的使用安全情报 IP 地址信誉实施黑名单。

启用安全情报日志记录将会记录访问控制策略的目标设备处理的所有受阻和受监控的连接。然而，系统不会记录白名单匹配项；列入白名单的连接的记录取决于其最终的性质。

当系统由于安装情报过滤而记录连接事件时，它也会记录匹配的安全情报事件，这是一种您可以单独查看时和分析的特殊类型的连接事件。两种类型的事件均使用 **Action** 和 **Reason** 字段来反映黑名单匹配项。此外，您因此可以确定连接中列入黑名单的 IP 地址，列入黑名单和受监控的 IP 地址旁的主机图标在事件查看器中看上去稍有不同。

记录受阻且列入黑名单的连接

对于受阻连接，系统会记录连接开始安全情报和连接事件。因为列入黑名单的流量会被立即拒绝，无需进一步检查，所以，没有要记录的唯一连接结束。对于这些事件，操作为 `Block`，原因为 `IP Block`。

`IP 阻止`连接事件的每个唯一的发起方-响应方对都有 15 秒的阈值。换言之，一旦系统生成了其阻止连接的事件，在接下来的 15 秒内，无论端口或协议如何，对于这两个主机之间的额外的已阻止连接，系统不会生成另一连接事件。

记录受监控且列入黑名单的连接

对于安全情报功能监控而不是阻止的连接，系统会将连接结束安全情报和连接事件记录至 防御中心数据库。无论之后 SSL 策略、访问控制规则或访问控制默认操作如何处理连接，都会发生这种记录。

对于这些连接事件，操作取决于连接的最终性质。 **Reason** 字段包含 `IP Monitor` 以及连接可能已被记录的任何其他原因。

请注意，对于受监控的连接，系统还可能会生成连接开始事件，具体取决于稍后处理该连接的访问控制规则或默认操作中的日志记录设置。

要记录已列入黑名单的连接，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Security Intelligence 选项卡。

屏幕上将会显示访问控制策略的安全情报设置。

步骤 4　点击记录图标 ( )。

系统将显示 Blacklist Options 弹出窗口。

步骤 5　选择 **Log Connections** 复选框。

步骤 6　指定要将连接和安全情报事件发送到何处。有以下选项可供选择：

- 要将事件发送到防御中心，请选择**防御中心**。
- 要将事件发送至外部系统日志服务器，请选择 **Syslog**，然后从下拉列表选择系统日志警报响应。或者，您可以通过点击添加图标 ( ) 来添加系统日志警报响应；请参阅第 43-4 页上的创建系统日志警报响应。
- 要将连接事件发送至 SNMP 陷阱服务器，请选择 **SNMP Trap**，然后从下拉列表选择 SNMP 警报响应。或者，您可以通过点击添加图标 ( ) 来添加 SNMP 警报响应；请参阅第 43-3 页上的创建 SNMP 警报响应。

必须将事件发送至防御中心，如果要将已列入黑名单的对象设置为仅监控，或对安全情报过滤生成的连接事件执行任何其他基于防御中心的分析。有关详细信息，请参阅第 38-4 页上的将连接事件记录到防御中心或外部服务器中。

步骤 7　点击 **OK** 设置日志记录选项。

Security Intelligence 选项卡将会再次显示。

步骤 8　点击 **Save**。

只有应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

记录已加密连接

许可证：SSL

受支持的设备：3 系列

在访问控制过程中，通过 *SSL 检查*功能，您可以使用 SSL 策略解密已加密的流量以供访问控制规则进一步评估。您可以强制系统记录这些解密的连接，而无论系统之后如何处理或检查这些流量。您还可以在阻止已加密流量时或允许其传递至访问控制规则而不解密时，记录连接。

已加密会话的连接日志包含有关加密的详细信息，例如用于加密该会话的证书。您可以按每条 SSL 规则为 SSL 策略中已加密会话配置连接记录，以便仅记录关键连接。

有关详细信息，请参阅以下各节：

- 第 38-11 页上的记录可用 SSL 规则解密的连接
- 第 38-12 页上的为已加密和不可解密连接设置默认日志记录

记录可用 SSL 规则解密的连接

许可证：SSL

受支持的设备：3 系列

在 SSL 策略中，*SSL 规则*为处理多台受管设备上已加密流量提供了一种精细方法。这样，您可以仅记录关键连接，按每条 SSL 规则启用连接记录 - 如果您为某条规则启用连接记录，则系统会记录该规则处理的所有连接。

对于由 SSL 策略检查的已加密连接，可以将连接事件记录到防御中心数据库或外部系统日志或 SNMP 陷阱服务器。您可以仅记录连接结束事件，但是：

- 对于受阻连接 （Block、 Block with reset），系统会立即结束会话并生成事件
- 对于受监控连接 (Monitor) 和传递至访问控制规则 （Decrypt、 Do not decrypt）的连接，会话结束时，无论之后处理该连接的访问控制规则或默认操作的日志记录如何，系统都会生成事件

有关详细信息，请参阅第 38-5 页上的了解访问控制和 SSL 规则操作如何影响日志记录。

要记录可解密连接，请执行以下操作：

访问：管理员/访问管理员/网络管理员/安全审批人

步骤 1　选择 **Policies > SSL**。

系统将显示 SSL Policy 页面。

步骤 2　点击要编辑的 SSL 策略旁的编辑图标 ( )。

系统将显示 SSL 策略编辑器，以 Rules 选项卡为中心。

步骤 3　点击要配置日志记录所在规则旁的编辑图标 ( )。

系统将显示 SSL 规则编辑器。

步骤 4　选择 Logging 选项卡。

系统将显示 Logging 选项卡。

步骤 5　选择 **Log at End of Connection**。

步骤 6　指定将连接事件发送至何处。有以下选项可供选择：

- 要将连接事件发送到防御中心，请选择**防御中心**。当规则操作为 **Monitor** 时，您必须将连接记录到防御中心中。

- 要将事件发送至外部系统日志，请选择 **Syslog**，然后从下拉列表选择系统日志警报响应。或者，您可以通过点击添加图标 ( ) 来添加系统日志警报响应；请参阅第 43-4 页上的创建系统日志警报响应。
- 要将事件发送至 SNMP 陷阱服务器，请选择 **SNMP Trap**，然后从下拉列表选择 SNMP 警报响应。或者，您可以通过点击添加图标 ( ) 来添加 SNMP 警报响应；请参阅第 43-3 页上的创建 SNMP 警报响应。

如果要对这些连接事件执行基于防御中心的分析，您**必须**将事件发送至防御中心。有关详细信息，请参阅第 38-4 页上的将连接事件记录到防御中心或外部服务器中。

步骤 7　点击 **Add** 保存您的更改。

只有应用与 SSL 策略相关联的访问控制策略，才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

为已加密和不可解密连接设置默认日志记录

许可证：SSL

受支持的设备：3 系列

您可以为 SSL 策略默认操作处理的流量记录连接。这些日志记录设置还监管系统如何记录无法解密的会话。

SSL 策略默认操作决定着系统如何处理与策略中任何 SSL 规则均不匹配的已加密流量 （Monitor 规则除外，该规则匹配和记录流量，但不处理或检查流量）。如果您的 SSL 策略不包含任何 SSL 规则，则默认操作决定如何记录网络上所有已加密会话。有关详细信息，请参阅第 20-3 页上的为已加密流量设置默认处理和检查。

您可以将 SSL 策略默认操作配置为将连接事件记录到防御中心数据库或外部系统日志或 SNMP 陷阱服务器。您可以仅记录连接结束事件，但是：

- 对于受阻连接 （Block、 Block with reset），系统会立即结束会话并生成事件
- 对于您允许在未加密状态下传递至访问控制规则 (Do not decrypt) 的连接，系统会在会话结束时生成事件

请注意，即使您禁用 SSL 策略默认操作的日志记录，但当连接之前与至少一条 SSL Monitor 规则相匹配或之后与访问控制规则或访问控制策略默认操作相匹配时，系统仍然会将连接结束事件记录到防御中心数据库。

要设置已加密和无法解密流量的默认处理，请执行以下操作：

访问：管理员/访问管理员/网络管理员/安全审批人

步骤 1　选择 **Policies > SSL**。

系统将显示 SSL Policy 页面。

步骤 2　点击要编辑的 SSL 策略旁的编辑图标 ( )。

系统将显示 SSL 策略编辑器，以 Rules 选项卡为中心。

步骤 3　点击日志记录图标 ( )，该图标位于 **Default Action** 下拉列表旁。

屏幕上将会显示 Logging 弹出窗口。

步骤 4　选择 **Log at End of Connection**，以启用记录连接事件。

步骤 5　指定将连接事件发送至何处。有以下选项可供选择：

- 要将连接事件发送到防御中心，请选择**防御中心**。
- 要将事件发送至外部系统日志服务器，请选择 **Syslog**，然后从下拉列表选择系统日志警报响应。或者通过点击添加图标 ( ) 来配置系统日志警报响应，请参阅第 43-4 页上的创建系统日志警报响应。
- 要将事件发送至 SNMP 陷阱服务器，请选择 **SNMP Trap**，然后从下拉列表选择 SNMP 警报响应。或者通过点击添加图标 ( ) 来配置 SNMP 警报响应，请参阅第 43-3 页上的创建 SNMP 警报响应。

如果要对这些连接事件执行基于防御中心的分析，您**必须**将事件发送至防御中心。但请注意，系统将不进一步检查 SSL 策略默认操作处理的流量是否存在入侵、恶意软件或发现数据。有关详细信息，请参阅第 38-4 页上的将连接事件记录到防御中心或外部服务器中。

步骤 6　点击 **OK**，保存更改。

只有应用与 SSL 策略相关联的访问控制策略，才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

根据访问控制处理记录连接

许可证：任何环境

在访问控制策略中，访问控制规则为在多台受管设备之间处理网络流量提供了一种精细方法。因此您可以仅记录关键连接，针对每条访问控制规则启用连接记录，如果为规则启用连接记录，则系统会记录该规则处理的所有连接。

您也可以为访问控制策略默认操作处理的流量记录连接。默认操作确定系统如何处理与策略中所有访问控制规则均不匹配的流量 （Monitor 规则除外，这些规则匹配和记录，但不处理或检查流量）。

请注意，即便您为所有访问控制规则和默认操作禁用了日志记录，连接结束事件仍可能会被记录至 防御中心数据库，前提是该连接与访问控制规则相匹配且包含入侵尝试、受禁文件或恶意软件，或者其被系统解密且您在 SSL 策略中为该连接启用了日志记录。

取决于规则或默认策略操作以及您配置的关联检查选项，您的日志记录选项可能有所不同。有关详情，请参阅：

- 第 38-13 页上的记录与访问控制规则相匹配的连接
- 第 38-15 页上的记录访问控制默认操作处理的连接

记录与访问控制规则相匹配的连接

许可证：任何环境

要仅记录关键连接，您可以针对每条访问控制规则启用连接记录。如为某条规则启用日志记录，则系统会记录该规则处理的所有连接。

取决于规则操作及规则的入侵和文件检查配置，您的日志记录选项可能有所不同；请参阅第 38-5 页上的了解访问控制和 SSL 规则操作如何影响日志记录。另请注意，即便您为某条访问控制规则禁用日志记录，与该规则匹配的连接的连接结束事件仍可能被记录至 防御中心数据库，前提是该连接：

- 包含入侵尝试、受禁文件或恶意软件
- 由 SSL 策略检查和记录
- 以前至少与一条访问控制 Monitor 规则相匹配

要将访问控制规则配置为记录连接、文件和恶意软件信息，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要修改的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器，以 Rules 选项卡为中心。

步骤 3　点击要配置日志记录所在规则旁的编辑图标 ( )。

系统将显示访问控制规则编辑器。

步骤 4　选择 Logging 选项卡。

系统将显示 Logging 选项卡。

步骤 5　指定您是否想要选择 **Log at Beginning of Connection** 还是选择 **Log at End of Connection**。

要优化性能，请记录任何连接的开始或结束事件，而不是同时记录两者。

对于单一未受阻连接，连接结束事件限制包含连接开始事件中的所有信息，以及在会话期间收集到的信息。因为受阻流量会被立即拒绝，无需进一步检查，所以，您可仅记录 Block 规则的连接开始事件。

另请注意，因为 Monitor 规则的目的是记录匹配流量，所以，记录到防御中心数据库的连接结束日志记录功能会自动启用，而且您无法禁用该功能。有关详细信息，请参阅第 38-3 页上的记录连接的开始或结束事件。

步骤 6　使用 **Log Files** 复选框指定系统是否应记录与连接相关联的任何文件和恶意软件事件。

当您将文件策略与该规则关联以便执行文件控制或 AMP 时，系统会自动启用该选项。思科建议您保留启用此选项；请参阅第 38-7 页上的为允许的连接禁用文件和恶意软件事件日志记录。

步骤 7　指定将连接事件发送至何处。有以下选项可供选择：

- 要将连接事件发送到防御中心，请选择**防御中心**。您无法为 Monitor 规则禁用此选项。
- 要将事件发送至外部系统日志服务器，请选择 **Syslog**，然后从下拉列表选择系统日志警报响应。或者，您可以通过点击添加图标 ( ) 来添加系统日志警报响应；请参阅第 43-4 页上的创建系统日志警报响应。
- 要将事件发送至 SNMP 陷阱服务器，请选择 **SNMP Trap**，然后从下拉列表选择 SNMP 警报响应。或者，您可以通过点击添加图标 ( ) 来添加 SNMP 警报响应；请参阅第 43-3 页上的创建 SNMP 警报响应。

如果要对连接事件执行基于防御中心的分析，您**必须**将事件发送至数据库。有关详细信息，请参阅第 38-4 页上的将连接事件记录到防御中心或外部服务器中。

步骤 8　点击 **Save** 以保存规则。

您的规则保存成功。只有应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

记录访问控制默认操作处理的连接

许可证：任何环境

您也可以为访问控制策略默认操作处理的流量记录连接。默认操作确定系统如何处理与策略中所有访问控制规则均不匹配的流量（Monitor 规则除外，这些规则匹配和记录，但不处理或检查流量）；请参阅第 12-6 页上的设置对网络流量的默认处理和检查。

用于记录策略默认操作处理的连接的机制和选项与用于记录个别访问控制规则处理的连接的选项大致类似，如下表所述。也就是说，除了受阻流量，您可以记录连接的开始和结束，而且您可以将连接事件发送至 防御中心数据库或者外部系统日志或 SNMP 陷阱服务器。

表 38-4　　访问控制默认操作日志记录选项

默认操作	比较对象	请参阅.....
访问控制：阻止所有流量	Block 规则	第 38-6 页上的了解受阻和交互式受阻连接的记录
访问控制：信任所有流量	Trust 规则	第 38-6 页上的了解受信任连接的记录
入侵防御	带关联入侵策略的 Allow 规则	第 38-7 页上的了解受允许连接的记录
仅网络发现	不带关联入侵策略的 Allow 规则	

然而，记录访问控制规则处理的连接与记录默认操作处理的连接之间存在着一些差异：

- 默认操作没有文件日志记录选项。您不能使用默认操作执行文件控制或 AMP。
- 当与访问控制默认操作关联的入侵策略生成入侵事件时，系统**不会**自动记录相关连接结束事件。当您不想在入侵检测和仅限防御的部署中记录任何连接数据时，这很有帮助。

  如果启用了默认操作的连接开始日志记录，这一规则将不适用。在这种情况下，当关联的入侵策略触发时，除了记录连接开始事件外，系统还**会**日志记录连接结束事件。

请注意，即便您为默认操作禁用日志记录，与该规则匹配的连接的连接结束事件仍可能会被记录至 防御中心 数据库，前提是该连接以前至少与一条访问控制 Monitor 规则相匹配或由 SSL 策略进行检查和记录。

要记录访问控制默认操作处理的流量中的连接，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要修改的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器，以 Rules 选项卡为中心。

步骤 3　点击日志记录图标 ( )，该图标位于 **Default Action** 下拉列表旁。

屏幕上将会显示 Logging 弹出窗口。

步骤 4　指定您是否想要选择 **Log at Beginning of Connection** 还是选择 **Log at End of Connection**。

要优化性能，请记录这些连接的开始或结束，而不是同时记录两者。对于单一未受阻连接，连接结束事件限制包含连接开始事件中的所有信息，以及在会话期间收集到的信息。由于受阻流量会被立即拒绝，无需进一步检查，因此，您可以仅记录 Block All Traffic 默认操作的连接开始事件。

步骤 5　指定将连接事件发送至何处。有以下选项可供选择：

- 要将连接事件发送到防御中心，请选择**防御中心**。您无法为 Monitor 规则禁用此选项。
- 要将事件发送至外部系统日志服务器，请选择 **Syslog**，然后从下拉列表选择系统日志警报响应。或者，您可以通过点击添加图标 ( ) 来添加系统日志警报响应；请参阅第 43-4 页上的创建系统日志警报响应。
- 要将事件发送至 SNMP 陷阱服务器，请选择 **SNMP Trap**，然后从下拉列表选择 SNMP 警报响应。或者，您可以通过点击添加图标 ( ) 来添加 SNMP 警报响应；请参阅第 43-3 页上的创建 SNMP 警报响应。

如果要对连接事件执行基于防御中心的分析，您**必须**将事件发送至数据库。有关详细信息，请参阅第 38-4 页上的将连接事件记录到防御中心或外部服务器中。

步骤 6　点击 **Save** 以保存策略。

您的策略保存成功。只有应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

记录在连接中检测到的 URL

许可证：FireSIGHT

对于 HTTP 流量，当您将连接结束事件记录至防御中心数据库时，系统会记录在会话期间受监控主机请求的 URL。

默认情况下，系统会在连接日志中存储 URL 的前 1024 个字符。然而，您可以将系统配置为每个 URL 存储最多 4096 个字符，确保自己捕获受监控主机请求的完整 URL。或者，如果对访问的个别 URL 不感兴趣，可以通过存储 0 个字符来完全禁用 URL 存储。取决于网络流量，禁用 URL 字符存储或限制存储的 URL 字符的数量可以提高系统性能。

请注意，禁用 URL 日志记录不会影响 URL 过滤。访问控制规则会基于请求的 URL、其类别以及信誉来适当地过滤流量，即便系统不会记录这些规则处理的流量中请求的各个 URL。有关详细信息，请参阅第 16-7 页上的阻止 URL。

要自定义您存储的 URL 字符数，请执行以下操作：

访问：管理员/访问管理员/网络管理员

步骤 1　选择 **Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

屏幕上将会显示访问控制策略的高级设置。

步骤 4　点击 General Settings 旁的编辑图标 ( )。

系统将显示 General Settings 弹出窗口。

步骤 5　键入**连接事件中要存储的最大 URL 字符数**。

您可以指定从 0 至 4096 的任何数量。存储零字符将禁用 URL 存储，而不禁用 URL 过滤。

步骤 6　点击 **OK**。

屏幕上将会显示访问控制策略的高级设置。

步骤 7　点击 **Save** 以保存策略。

您的策略保存成功。只有应用访问控制策略才能使更改生效；请参阅第 12-13 页上的应用访问控制策略。

使用连接与安全情报数据

在受管设备监控网络主机生成的流量时，其可为其检测到的连接生成日志。访问控制和 SSL 策略中的各种设置可供您精细控制记录哪些连接、何时记录连接以及在何处存储数据。在大多数情况下，您均可记录连接的开始和/或结束。

当记录连接时，系统会生成*连接事件*。每当连接被列入黑名单（加以阻止）或被基于信誉的安全情报功能监控时，您还可以记录特殊类型的连接事件，称为*安全情报事件*。

连接日志，称为*连接事件*，包含有关检测到的会话的数据。您应根据贵组织的安全和合规需求记录连接；您可以记录除了在到达访问控制之前已在设备级别通过快速路径的连接以外的**任何**连接。

除了您配置的日志记录外，系统会自动记录检测到被禁止的文件、恶意软件或入侵尝试的大多数连接。除非您完全禁用连接事件存储，否则系统会将这些连接结束事件保存到防御中心数据库供进一步分析。有关配置连接日志记录的详细信息，请参阅第 38-1 页上的记录网络流量中的连接。

注 虽然可以使用任何设备和许可证记录连接，但可用于任何单个连接或安全情报事件的信息取决于若干因素，包括许可证。有关详细信息，请参阅第 38-8 页上的连接记录的许可证和型号要求。

要补充受管设备采集到的连接数据，您可以使用由 NetFlow 启用设备生成的记录来生成连接事件。如果将 NetFlow 启用设备部署在 FireSIGHT 系统受管设备无法监控的网络中，则此功能特别有用。

注 由于 NetFlow 数据收集与访问控制不相关，因此，您无法对想要记录的 NetFlow 连接进行精细控制。 FireSIGHT 系统受管设备检测由 NetFlow 启用设备导出的记录，依据这些记录中的数据生成单向连接结束事件，并最终将这些事件发送至防御中心，以便在数据库中进行记录。 NetFlow 记录无法生成安全情报事件，也不会记录到外部服务器。有关详细信息，请参阅第 45-14 页上的了解 NetFlow。

有关使用连接和安全情报事件的详细信息，请参阅：

了解连接和安全情报数据

许可证：任何环境

连接日志，称为*连接事件*，包含有关检测到的会话的数据。任何单个连接事件的可用信息取决于多种因素，但通常包括：

- 基本连接属性：时间戳、源和目标 IP 地址、入口和出口区域，处理连接的设备等
- 系统发现或推断的其他连接属性：应用、请求的 URL 或与连接关联的用户等
- 有关连接记录原因的元数据：哪个策略中的哪条访问控制规则（或其他配置）处理了流量，连接是被允许还是被阻止，以及有关已加密和已解密连接的详细信息等

访问控制和 SSL 策略中的各种设置可供您精细控制记录哪些连接、何时记录连接以及在何处存储数据。可以记录访问控制和 SSL 策略可成功处理的任何连接，这可能需要特定设备型号或许可的功能。在以下情况下可以启用连接日志记录：

- 当连接由基于信誉的安全情报功能列入黑名单（阻止）或监控时
- 当加密会话由 SSL 策略处理时
- 当连接由访问控制规则或访问控制默认操作处理时

除了您配置的日志记录外，系统会自动记录检测到被禁止的文件、恶意软件或入侵尝试的大多数连接。除非您使用系统策略完全禁用连接事件存储，否则无论您的其他日志记录配置如何，系统均将这些连接结束事件保存至防御中心数据库，以供进一步分析。

此外，当您启用安全情报日志记录时，黑名单匹配项会自动生成*安全情报事件*以及连接事件。安全情报事件是您可以单独查看和分析的一种特殊类型的事件，也可以单独存储和删除。有关配置连接日志记录的详细信息，包括安全情报黑名单决策，请参阅第 38-1 页上的记录网络流量中的连接。

提示 有关连接事件的一般信息也适合安全情报事件，除非另有说明。有关安全情报的详细信息，请参阅第 13-1 页上的使用安全情报 IP 地址信誉实施黑名单。

以下各节提供有关所检测到的连接的可用信息种类的其他详细信息：

了解连接摘要

许可证：任何环境

FireSIGHT 系统将五分钟间隔内采集到的连接数据汇总到连接摘要中，供系统生成连接图和流量量变曲线。或者，您可以基于连接摘要数据创建自定义工作流程，并以与基于单个连接事件的工作流程相同的方式来使用此类工作流程。

请注意，尽管相应的连接结束事件可以汇总到连接摘要数据中，但安全情报事件无任何特定的连接摘要。

多个连接必须满足以下条件才能汇总到连接摘要：

- 表示连接结束
- 具有相同的源 IP 地址和目标 IP 地址，并在响应方（目标）主机上使用相同的端口
- 使用相同的协议（TCP 或 UDP）

- 使用相同的应用协议
- 由相同的思科受管设备检测，或者由相同的 NetFlow 启用设备导出

每份连接摘要都包括总流量统计信息，以及摘要中连接的数量。因为 NetFlow 启用设备生成单向连接，所以对于每个基于 NetFlow 数据的连接而言，摘要中的连接数应乘以 2。

请注意，连接摘要中并未包含与摘要中汇总的连接相关联的所有信息。例如，在汇总连接以形成连接摘要时没有使用客户端信息，因此摘要中不包含客户端信息。

有关详细信息，请参阅以下各节：

- 第 39-3 页上的长期运行连接
- 第 39-3 页上的源于外部响应方的组合连接摘要
- 第 39-9 页上的连接和安全情报事件中的可用信息

长期运行连接

许可证：任何环境

如果汇总连接数据的受控会话跨越两个或多个 5 分钟时间间隔，那么该连接可视为*长期运行连接*。当计算连接摘要中的连接数时，系统仅累加启动长期运行连接的 5 分钟间隔内的连接数。

此外，当计算由长期运行连接中的发起方和响应方传输的数据包和字节数时，系统并不会报告每 5 分钟间隔中实际传输的数据包和字节数。相反，系统会假定一个固定传输比率，并基于传输的数据包和字节总数、连接长度及每 5 分钟间隔内发生的连接部分计算预估数字。

源于外部响应方的组合连接摘要

许可证：任何环境

要减少存储连接数据所需的空间并加快连接图的绘制，系统将在下列情况下合并连接摘要：

- 连接中涉及的其中一台主机并不在监控网络中
- 除了外部主机的 IP 地址外，摘要中的连接均满足第 39-2 页上的了解连接摘要列出的汇总条件：协议、应用协议、检测装置等

当在事件查看器中查看连接摘要并使用连接图时，系统将显示外部 IP 地址而非未监控主机的 IP 地址。

由于执行汇总的缘故，如果您尝试从涉及外部响应方的连接摘要或连接图深入了解连接数据的表视图 （即，访问单个连接的数据），该表视图将不包含任何信息。

了解连接和安全情报数据字段

许可证：因功能而异

受支持的设备：因功能而异

受支持的防御中心：因功能而异

每个连接表视图或连接图中都包含您正在查看的连接或连接摘要的信息，包括时间戳、 IP 地址、地理定位信息、应用等。安全情报事件视图中包含与连接事件视图相同的一般信息，但仅列出具有分配的 **Security Intelligence Category** 值的连接。

注　此外，可用于任何单个连接或安全情报事件的信息取决于若干因素，包括许可证和应用型号。有关详细信息，请参阅第 38-8 页上的连接记录的许可证和型号要求。

以下列表详细列明了由 FireSIGHT 系统记录的连接数据。有关确定任何单个连接或安全情报事件中所记录信息的因素的讨论，请参阅下一节：第 39-9 页上的连接和安全情报事件中的可用信息。

Access Control Policy

监控连接的访问控制策略。

Access Control Rule

处理连接的访问控制规则或默认操作，以及最多 8 条该连接匹配的监控规则。

如果连接匹配 1 条监控规则，则防御中心显示处理连接的规则名称，然后显示监控规则名称。如果连接匹配多个监控规则，则事件查看器显示所匹配的监控规则数量，例如，`Default Action + 2 Monitor Rules`。

要显示带有匹配连接的前 8 条监控规则列表的弹出窗口时，请点击 *N* **Monitor Rules**。

Action

与记录连接的访问控制规则或默认操作相关的操作：

- `Allow` 表示示确容许和用户忽略的被阻止连接。
- `Trust` 表示信任的连接。请注意，系统记录信任规则检测到的 TCP 连接的方式因设备而异。

  在 2 系列、虚拟设备以及用于 Blue Coat X-系列的思科 NGIPS中，第一个数据包的信任规则检测到的 TCP 连接仅会生成连接结束事件。系统会在最终会话数据包之后一小时生成事件。

  在 3 系列设备上，第一个数据包中的信任规则检测到的 TCP 连接会根据监控规则是否存在生成不同的事件。如果监控规则处于活动状态，系统评估数据包并生成连接开始和结束事件。如果没有监控规则处于活动状态，系统仅生成连接结束事件。
- `Block` 和 `Block with reset` 代表被阻止连接。系统还将 `Block` 操作与由安全情报列入黑名单的连接、受 SSL 规则阻止的连接、入侵策略检测到存在漏洞的连接及文件被文件策略阻止的连接相关联。
- `Interactive Block` 和 `Interactive Block with reset` 标记开始连接事件，您可以在系统利用交互式规则最初阻止用户的 HTTP 请求时进行记录。如果用户点击阅读系统显示的警告页面，则您为会话记录的任何其他连接事件均具有 `Allow` 操作。
- `Default Action` 表示连接采用默认操作处理。
- 对于受安全情报监控的连接，该项操作即为由连接触发的第一个非监控访问控制规则的操作，或者为默认操作。同样地，因为匹配监控规则的流量始终由后续规则或通过默认操作进行处理，所以与因监控规则原因记录的连接相关联的操作不可能为 `Monitor`。

Application Protocol

连接中检测到的表示主机之间通信的应用协议。

Application Risk

连接中检测到的应用流量相关风险：`Very High`、`High`、`Medium`、`Low` 或 `Very Low`。连接中检测的各类应用都有一个相关风险；该字段显示最高风险。有关详细信息，请参阅第 45-9 页上的表 45-2。

Business Relevance

连接中检测到的应用流量的业务相关性：`Very High`、`High`、`Medium`、`Low` 或 `Very Low`。连接中检测的各类应用都有相关业务相关性；该字段显示级别最低的业务相关性。有关详细信息，请参阅第 45-9 页上的表 45-2。

Category, Tag (Application Protocol, Client, Web Application)

展示了应用特征的标准，协助您了解应用功能。有关详细信息，请参阅第 45-9 页上的表 45-2。

Client 和 Client Version

在连接中检测到的客户端应用及版本。

如果系统无法识别连接中使用的具体客户端，则该字段将显示应用协议名称中追加的 `client`，以便提供通用名称，例如，`FTP client`。

Connections

连接摘要中的连接数。对于长期运行连接，即跨越多个连接摘要间隔的连接，只有第一个连接摘要间隔可递增。

Count

与每行显示的信息相匹配的连接数。注意，**Count** 字段仅在应用了创建两个或多个相同行的约束后才显示。

注　如果创建了自定义工作流程，但未在向下深入了解页面中添加 **Count** 列，则每个连接都将单独列出，且数据包和字节并不汇总。

Device

可检测连接或适用于 NetFlow 启用设备导出的连接的受管设备、处理 NetFlow 数据的受管设备。

Files

与连接相关的文件事件 （如有）。防御中心不显示文件列表，而是在该字段中显示视图文件图标 ()。图标上的数字表示连接中检测到或阻止的文件数量 （包括恶意软件文件）。

点击该图标显示一个弹出窗口。窗口中显示连接中检测到的文件列表及其类型、恶意软件查询处置情况 （如适用）。

请注意， DC500 防御中心及 2 系列设备均不支持基于网络的恶意软件文件检测功能。

有关详细信息，请参阅第 39-26 页上的查看连接中检测到的文件。

First Packet 或 Last Packet

查看会话的第一个或最后一个数据包的日期和时间。

HTTP Referrer

HTTP 来源地址，表示在连接中检测到的 HTTP 流量的请求 URL 来源地址 （例如提供到另一个 URL 的链接或从其导入链接的网站）。

Ingress Interface 或 Egress Interface

与连接相关的入口或出口接口。请注意，但是，如果您的部署包括异步路由配置，入口和出口接口可能属于同一接口集。

Ingress Security Zone 或 Egress Security Zone

与连接相关的入口或出口安全区。

Initiator Bytes 或 Responder Bytes

由会话发起方或会话响应方发送的总字节数。

Initiator Country 或 Responder Country

当检测到可路由 IP 时，该与发起会话的主机 IP 地址有关或与会话响应方有关的国家/地区。显示该国家/地区旗帜的图标，以及该国家/地区的 ISO 3166-1 alpha-3 国家/地区代码。将鼠标指针悬停在旗帜图标上可以查看该国家/地区的全名。

请注意， DC500 防御中心不支持此功能。

Initiator IP 或 Responder IP

发起或响应会话响应方的主机 IP 地址 （以及主机名，如果启用 DNS 解析）。黑名单 IP 地址旁边的主机图标会略有不同，因此，您可以在被列入黑名单的连接中识别黑名单 IP 地址。

Initiator Packets 或 Responder Packets

由会话发起方或会话响应方发送的总数据包数。

Initiator User

登录到会话发起方的用户。

Intrusion Events

与连接相关的入侵事件 （如有）。防御中心不显示事件列表，而是在该字段中显示视图入侵事件图标 （防御中心）。防御中心

点击该图标显示一个弹出窗口。窗口中显示与连接相关的入侵事件列表，以及事件的优先级和影响力。有关详细信息，请参阅第 39-26 页上的查看与连接有关的入侵事件。

IOC

事件是否对连接涉及的主机触发危害表现 (IOC)。有关 IOC 的详细信息，请参阅第 45-17 页上的了解危害表现。

NetBIOS Domain

会话中使用的 NetBIOS 域。

NetFlow Destination/Source Autonomous System

对于由 NetFlow 启用设备导出的连接，指连接中流量来源或目标的边界网关协议自治系统编号。

NetFlow Destination/Source Prefix

对于由 NetFlow 启用设备导出的连接，将来源或目标 IP 地址与来源或目标前缀掩码用 AND 连接。

NetFlow Destination/Source TOS

对于由 NetFlow 启用设备导出的连接，当连接流量进入或退出 NetFlow 启用设备时，服务类型 (TOS) 字节的设置。

NetFlow SNMP Input/Output

对于由 NetFlow 启用设备导出的连接，连接流量进入或退出 NetFlow 启用设备的接口的接口索引。

Network Analysis Policy

与事件生成相关的网络分析策略 (NAP)（如果有）。

Reason

在以下几种情况，连接被记录的原因：

- User Bypass 表示系统最初阻止了用户的 HTTP 请求，但用户选择通过点击警告页面继续访问原先请求的站点。User Bypass 原因始终与 Allow 操作匹配。
- IP Block 表示系统根据安全情报数据未经检查就拒绝连接。IP Block 原因始终与 Block 操作匹配。
- IP Monitor 表示系统根据安全情报数据本可拒绝连接，但您将系统配置为监控连接，而不是拒绝连接。
- File Monitor 表示系统在连接中检测到特定类型的文件。
- File Block 表示连接中包含系统禁止传输的文件或恶意软件文件。File Block 原因始终与 Block 操作匹配。
- File Custom Detection 表示连接中包含自定义检测列表上的系统禁止传输的文件。
- File Resume Allow 表示文件传输最初被 Block Files 或 Block Malware 文件规则阻止。应用允许文件的新访问控制策略后，会自动恢复 HTTP 会话。请注意，此原因只出现在内联部署中。
- File Resume Block 表示件传输最初被 Detect Files 或 Malware Cloud Lookup 文件规则允许。应用阻止文件的新访问控制策略后，会自动停止 HTTP 会话。请注意，此原因只出现在内联部署中。
- SSL Block 表示系统基于 SSL 检查配置阻止了加密连接。SSL Block 原因始终与 Block 操作匹配。
- Intrusion Block 表示系统阻止或本可阻止在连接中检测到的攻击程序（违反入侵策略）。Intrusion Block 原因与用于阻止攻击程序的 Block 操作和用于本可阻止的攻击程序的 Allow 操作相匹配。
- Intrusion Monitor 表示系统检测到但并未阻止连接中检测到的攻击程序。当触发的入侵规则状态设置为 **Generate Events** 时，会发生这种情况。

Referenced Host

如果连接的协议是 DNS、 HTTP 或 HTTPS，此字段显示各自协议使用的主机名。

Security Context

识别流量通过的虚拟防火墙组的元数据。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。

Security Intelligence Category

表示或包含连接中被列为黑名单的 IP 地址的黑名单对象名称。安全情报类别可以是网络对象或网络组、全局黑名单、自定义安全情报列表或源、或者情报源中一个类别的名称。请注意，只有在 **Reason** 是 IP Block 或 IP Monitor 时才填充该字段；安全情报事件视图中的条目始终显示原因。有关详细信息，请参阅第 13-1 页上的使用安全情报 IP 地址信誉实施黑名单。

另请注意，无论是 DC500 防御中心还是 2 系列设备都不支持此功能。

Source Device

导出连接数据的 NetFlow 启用设备的 IP 地址。如果受管设备检测到连接，则此字段包含 FireSIGHT 值。

Source Port/ICMP Type 或 Destination Port/ICMP Code

会话发起方或会话响应方使用的端口、 ICMP 类型或 ICMP 代码。

SSL Status

SSL 规则相关操作、默认操作或记录加密连接的不可解密流量操作：

- `Block` 和 `Block with reset` 代表被阻止的加密连接。
- `Decrypt (Resign)` 代表使用重签服务器证书解密的传出连接。
- `Decrypt (Replace Key)` 代表使用带替代公共密钥的自签服务器证书解密的传出连接。
- `Decrypt (Known Key)` 代表使用已知私有密钥解密的传入连接。
- `Do not Decrypt` 代表系统未解密的连接。

如果系统无法解密已加密的连接，则它会显示所采取的无法解密流量操作和失败原因。例如，如果系统检测到使用未知密码套件加密的流量并且未做进一步检查即允许了该流量，则此字段显示 `Do Not Decrypt (Unknown Cipher Suite)`。

点击锁图标 () 可查看证书详细信息。有关详细信息，请参阅第 39-27 页上的查看与加密连接相关的证书。

SSL Certificate Status

如果已加密流量与 SSL 规则相匹配，则此字段显示服务器证书状态。如果无法解密的流量与 SSL 规则相匹配，则此字段显示 `Not Checked`。有关详细信息，请参阅第 22-20 页上的按证书状态控制加密流量。

SSL Flow Error

当在 SSL 会话期间发生错误时，为错误名称和十六进制代码，如果未发生错误，则为 **Success**。

SSL Version

用来加密连接的 SSL 或 TLS 协议版本。

SSL Cipher Suite

用于加密连接的加密套件。

SSL Policy

处理连接的 SSL 规则。

SSL Rule

处理连接的 SSL 规则或默认操作，以及与连接匹配的第一个监控规则。如果连接匹配 1 条监控规则，则防御中心显示处理连接的规则名称，然后显示监控规则名称。

SSL Session ID

在 SSL 握手期间，在客户端与服务器之间协商的十六进制会话 ID。

SSL Ticket ID

在 SSL 握手期间发送的会话单信息的一个十六进制哈希值。

SSL Flow Flags

已加密连接的前十大调试级别标记。要查看所有标记，请点击省略号 (...)。

SSL Flow Messages

在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。

TCP Flags

在连接中检测到的 TCP 标志。

Time

系统用来在连接摘要中汇总连接的 5 分钟时间间隔的结束时间。

URL、 URL Category 和 URL Reputation

会话期间受控主机请求的 URL 以及 URL 类别和信誉 （如果有）。

如果系统识别或阻止 SSL 应用，而请求的 URL 位于加密流量中，系统会基于 SSL 证书识别流量。因此，对于 SSL 应用，此字段表示包含在证书中的通用名称。

请注意，无论是 DC500 防御中心还是 2 系列设备都不支持 URL 类别或信誉数据。

User Agent

从连接中检测到的 HTTP 流量提取的用户代理应用信息。

Web Application

表示连接中检测到的 HTTP 流量内容或请求的 URL 的网络应用。

如果网络应用不匹配事件的 URL，该流量大概是推荐流量，例如广告流量。如果系统检测到推荐流量，则会存储该推荐应用 （如果有），并将该应用列为网络应用。

如果系统不能在 HTTP 流量中识别特定的网络应用，该字段显示 `Web Browsing`。

连接和安全情报事件中的可用信息

许可证：因功能而异

受支持的设备：因功能而异

受支持的防御中心：因功能而异

可用于任何单个连接、连接摘要或安全情报事件的信息取决于多种因素。

Appliance Model 和 License

可以记录访问控制和 SSL 策略可成功处理的任何连接。但是，许多功能要求您启用目标设备上的特定许可功能，许多功能仅适用于某些型号。

例如， SSL 检查需要 3 系列设备。其他设备型号无法检查已加密流量；已记录的连接事件不包含有关已加密连接的信息。再如，在使用 DC500 的连接事件中无法查看地理定位数据。有关详细信息，请参阅第 38-8 页上的连接记录的许可证和型号要求。

Traffic Characteristics

系统仅报告在网络流量中展示 （并且可检测）的信息。例如，可能没有与发起人主机相关联的用户，或者在协议不是 DNS、 HTTP 或 HTTPS 的连接中未检测到引用的主机。

检测方法：FireSIGHT 系统 与 NetFlow

除了 TCP 标志和 NetFlow 自治系统、前缀和 TOS 数据，与通过受管设备监控网络流量产生的信息相比，从 NetFlow 记录中可获得的信息更加有限。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

记录方法：连接的开始或结束

当系统检测到连接时，您是在其开始时还是在其结束 （或两者）时记录它取决于您如何将系统配置为检测和处理它；请参阅第 38-3 页上的记录连接的开始或结束事件。

开始连接事件不具有必须通过检查会话持续时间内的流量来确定的信息 （例如，连接中传输数据的总量或最终数据包的时间戳）。也不保证开始连接事件拥有关于会话中应用或 URL 流量的信息，且该等事件不包含有关会话加密的任何详细信息。

检查方法：关联的 SSL、文件和入侵策略

只有 SSL 规则处理的加密连接在连接日志中才包含 SSL 相关信息。只有通过具有相关文件策略的访问控制规则记录的连接才包含文件信息。同样，您必须将入侵策略与访问控制规则或默认操作相关联才能查看连接日志中的入侵信息。

连接事件类型：个别与摘要

连接摘要不包含与汇总连接相关的所有信息。例如，在汇总连接以形成连接摘要时没有使用客户端信息，因此摘要中不包含客户端信息。

请记住，连接图基于连接摘要数据，并且只使用了结束连接记录。如果只记录了开始连接的数据，连接图和连接摘要事件视图将不包含任何数据。

其他配置

访问控制策略中控制系统在连接记录中为 HTTP 会话中受控主机请求的每个 URL 存储的字符数的高级设置。如果使用此设置禁用 URL 记录，系统不会在连接记录中显示每个 URL；但如果连接记录中存在类别和信誉数据，仍然可以查看。

此外，并非所有的连接事件都会有一个 **Reason**，该字段仅在特定情况下填充，例如当用户绕过交互阻止配置时；有关信息，请参阅第 39-7 页上的 Reason。

下表列出了各连接事件/安全情报事件字段，以及根据检测方法、记录方法和连接事件类型系统是否在字段中显示信息。请注意，因为安全情报事件永远不会汇总，所以 Summary 列仅指连接事件摘要。

提示 默认情况下，在连接事件和安全情报事件表视图中，有几个字段是隐藏的，包括每种应用类型的类别和标记字段、 NetFlow 相关字段、 SSL 相关字段和其他字段。要显示事件视图的隐藏字段，请展开搜索限制，然后点击 **Disabled Columns** 下的字段名称。

表 39-1　基于记录和检测方法的连接和安全情报数据

	检测方法：		记录方法：		连接事件：	
字段	FireSIGHT	NetFlow	开始	结束	单个	摘要
Time	是	是	否	是	否	是
First Packet	是	是	是	是	是	否
Last Packet	是	是	否	是	是	否
Action	是	否	是	是	是	否
Reason	是	否	是	是	是	否

表 39-1　基于记录和检测方法的连接和安全情报数据 （续）

	检测方法：		记录方法：		连接事件：	
字段	FireSIGHT	NetFlow	开始	结束	单个	摘要
Initiator IP	是	是	是	是	是	是
Initiator Country	是	否	是	是	是	是
Initiator User	是	是	是	是	是	是
Responder IP	是	是	是	是	是	是
Responder Country	是	否	是	是	是	是
Security Intelligence Category	是	否	是	是	是	否
Ingress Security Zone	是	否	是	是	是	是
Egress Security Zone	是	否	是	是	是	是
Source Port/ICMP Code	是	是	是	是	是	否
Destination Port/ICMP Type	是	是	是	是	是	是
SSL Status	是	否	否	是	是	否
SSL Certificate Status	是	否	否	是	是	否
SSL Version	是	否	否	是	是	否
SSL Policy	是	否	否	是	是	否
SSL Rule	是	否	否	是	是	否
SSL Cipher Suite	是	否	否	是	是	否
SSL Flow Flags	是	否	否	是	是	否
SSL Flow Messages	是	否	否	是	是	否
Application Protocol	是	是	如果有	是	是	是
Client	是	否	如果有	是	是	否
Client Version	是	否	如果有	是	是	否
Web Application	是	否	如果有	是	是	否
Category, Tag (Application Protocol, Client, Web Application)	是	否	如果有	是	是	否
Application Risk	是	否	如果有	是	是	否
Business Relevance	是	否	如果有	是	是	否
URL	是	否	如果有	是	是	否
URL Category	是	否	如果有	是	是	否
URL Reputation	是	否	如果有	是	是	否
VLAN ID	是	否	是	是	是	否
Referenced Host	是	否	否	是	是	否
User Agent	是	否	否	是	是	否
HTTP Referrer	是	否	否	是	是	否
IOC	是	否	是	是	是	否
Intrusion Events	是	否	否	是	是	否

表 39-1　基于记录和检测方法的连接和安全情报数据 （续）

字段	检测方法：		记录方法：		连接事件：	
	FireSIGHT	NetFlow	开始	结束	单个	摘要
Files	是	否	否	是	是	否
Intrusion Policy	是	否	是	是	是	否
Access Control Policy	是	否	是	是	是	否
Access Control Rule	是	否	是	是	是	否
Network Analysis Policy	是	否	是	是	是	否
Device	是	是	是	是	是	是
Ingress Interface	是	否	是	是	是	是
Egress Interface	是	否	是	是	是	是
Security Context (ASA only)	是	否	是	是	是	是
TCP Flags	否	是	否	是	是	否
NetFlow Destination/Source Autonomous System	否	是	否	是	是	否
NetFlow Destination/Source Prefix	否	是	否	是	是	否
NetFlow Destination/Source TOS	否	是	否	是	是	否
NetFlow SNMP Input/Output	否	是	否	是	是	否
Source Device	是	是	FireSIGHT	是	是	是
NetBIOS Domain	是	否	是	是	是	否
Initiator Packets	是	是	不实用	是	是	是
Responder Packets	是	是	不实用	是	是	是
Initiator Bytes	是	是	不实用	是	是	是
Responder Bytes	是	是	不实用	是	是	是
Connections	是	是	否	是	否	是
Count	是	是	是	是	是	否

查看连接和安全情报数据

许可证：因功能而异

受支持的设备：因功能而异

受支持的防御中心：因功能而异

为帮助您深入了解连接数据，系统可将连接数据以图形和表格的形式呈现出来。访问连接数据时看到的页面因所用的工作流程而有所不同。您可以使用一个预定义的工作流程或创建一个自定义工作流程，其中只显示符合特定需求的信息。

访问安全情报事件需要保护许可证，且仅以表格的形式显示。2 系列受管设备或 DC500 防御中心不支持安全情报数据。虽然安全情报事件对应的连接事件都可以图形的形式查看，但是您不能创建安全情报事件的数据图形。若要访问安全情报数据的交互式图形视图，可以查看情景管理器的“安全情报”小节。有关详细信息，请参阅第 56-15 页上的了解“安全情报”部分。

注　此外，可用于任何单个连接或安全情报事件的信息取决于若干因素，包括许可证和应用型号。有关详细信息，请参阅第 38-8 页上的连接记录的许可证和型号要求。

每个表视图或图形中都包含您正在查看的连接或连接摘要的信息，包括时间戳、 IP 地址、应用等。 FireSIGHT 系统检测到的任何单个连接的可用信息取决于多个因素，包括检测方法和记录选项。有关详细信息，请参阅第 39-3 页上的了解连接和安全情报数据字段和第 39-9 页上的连接和安全情报事件中的可用信息。

提示　连接摘要控制面板可提供系统记录的连接的概览视图，摘要控制面板显示安全情报事件数据。有关详细信息，请参阅第 55-1 页上的使用控制面板。

要查看连接或安全情报数据，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　此时您有两种选择：

- 要查看连接事件，请选择 **Analysis > Connections > Events**。
- 要查看安全情报事件，请选择 **Analysis > Connections > Security Intelligence Events**。

系统将显示默认连接或安全情报工作流程首页。对于连接事件，有两种可能性：

- 工作流程页面显示一个**图形**。有关可执行操作的信息，请参阅第 39-13 页上的使用连接图。
- 工作流程页面显示一个**表格**。有关可执行操作的信息，请参阅第 39-24 页上的使用连接和安全情报数据表。

对于安全情报事件，工作流程页面显示一个**表格**。

要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示任何事件，可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

使用连接图

许可证：任何环境

系统呈现连接数据的方式之一就是用图形。有三种不同类型的连接图：曲线图、条形图和饼形图。条形图和曲线图可以显示多个数据集；也就是说，它们可以在 y 轴为每个 x 轴数据点显示几个值。

可以各种方式操作连接图，包括：

- 改变图形显示的数据的类型
- 切换图形类型
- 对图形进行限制，使图形显示特定时间范围、主机、应用、端口和设备的数据

因为流量量变曲线基于连接数据 （参阅第 53-1 页上的创建流量量变曲线），所以可以将流量量变曲线视为曲线图。您可以操作其他任何连接图的方式操作这些图形，但会有一些限制。

虽然安全情报事件对应的连接事件都可以图形的形式查看，但是您不能创建安全情报事件的数据图形。若要访问安全情报数据的交互式图形视图，可以查看情景管理器的“安全情报”小节。有关详情，请参见第 56-15 页上的了解“安全情报”部分。

注　要查看流量量变曲线，您必须具有管理员访问权限。将其与其他连接图进行对比，您能够以任何安全分析师或管理员访问权限查看。

当您查看连接图时，如第 39-12 页上的查看连接和安全情报数据所述，您可以执行下表中所描述的基本操作。

访问：管理员/任何安全分析师

表 39-2　　连接图基本功能

要.....	您可以.....
了解有关显示数据的详细信息	在第 39-3 页上的了解连接和安全情报数据字段中获得详细信息。
修改时间和日期范围	在第 58-19 页上的设置事件时间限制中获得详细信息。
查看主机的配置文件	在按发起方或响应方显示连接数据的图形上，点击条形图的一条形或饼形图的一块，然后选择 **View Host Profile**。
使用一个不同的工作流程，包括一个自定义工作流程	通过工作流程标题点击 (**switch workflow**)。
在当前的工作流程页面之间导航	在第 58-16 页上的使用工作流程页面中获得详细信息。
导航至其他事件视图查看相关事件	在第 58-31 页上的在工作流程之间导航中获得详细信息。

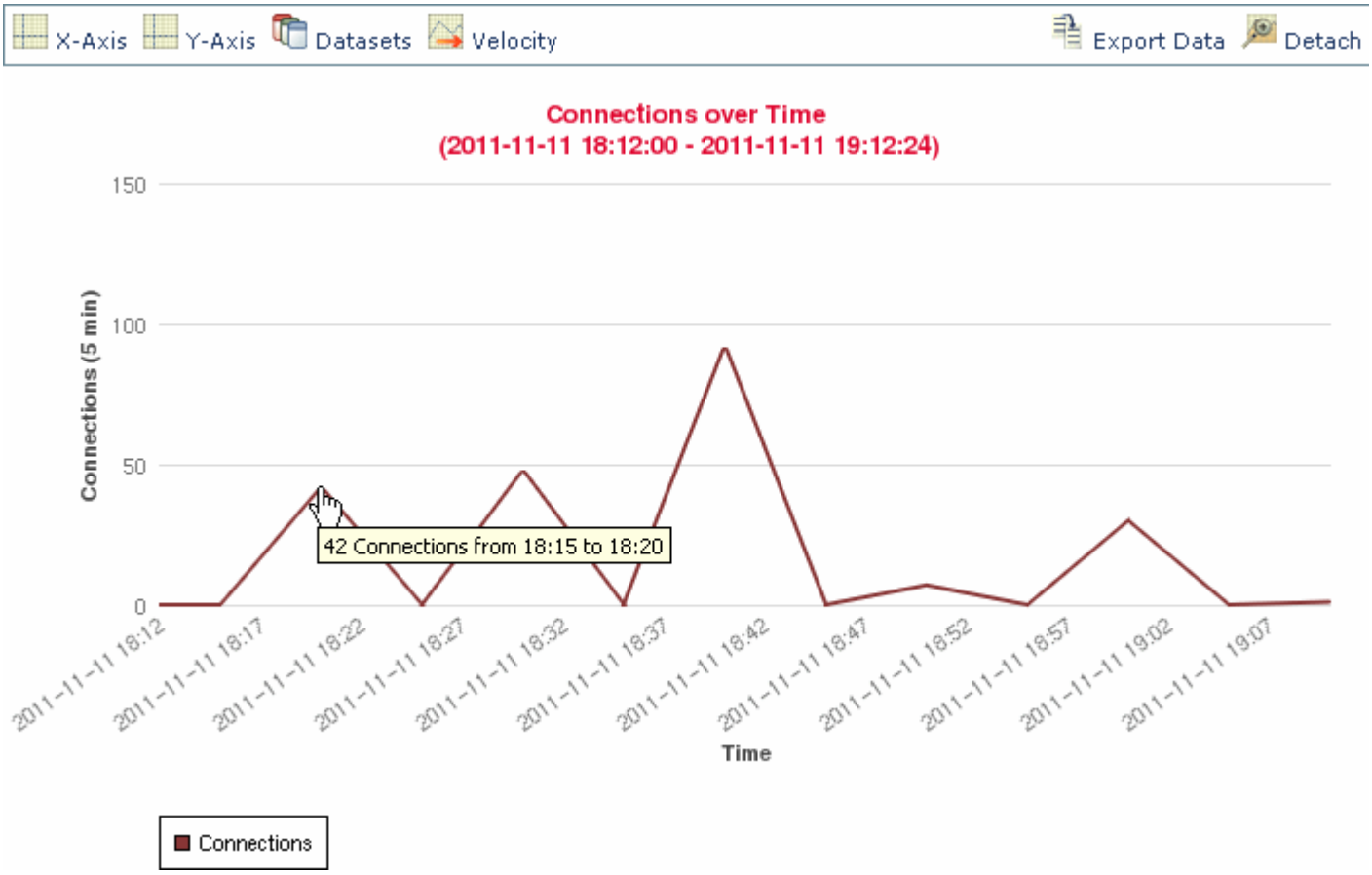
当深入分析连接数据时，还有许多其他的操作连接图的方式。有关详情，请参阅：

- 第 39-14 页上的更改图形类型介绍了如何在条形图与饼形图以及标准曲线图与速度曲线图之间进行切换。
- 第 39-17 页上的选择数据集介绍了如何为曲线图和条形图上的每个 x 轴数据点显示几个 y 轴值。
- 第 39-19 页上的查看有关汇总连接数据的信息介绍了如何获得图形上数据点的详细信息，或如何显示正在绘制统计数据的主机的配置文件。
- 第 39-20 页上的在工作流程页面上操作连接图介绍了如何在不进入工作流程下一页面的情况下限制连接图显示的数据。
- 第 39-20 页上的深入研究连接数据图介绍了如何在进入工作流程下一页面的情况下限制连接图显示的数据。
- 第 39-21 页上的重定曲线图的中心点和缩放介绍了如何在任一时间点范围内重新定位曲线图。
- 第 39-22 页上的选择数据进行绘图介绍了如何通过改变 X 轴或 Y 轴值来改变连接图显示的数据。
- 第 39-23 页上的分离连接图介绍了如何在不影响防御中心默认时间范围的情形下将连接图分离到新的浏览器窗口，以进一步分析连接图。
- 第 39-23 页上的导出连接数据介绍了如何将用于构造图形的连接数据导出为 CSV （逗号分隔值）文件。

更改图形类型

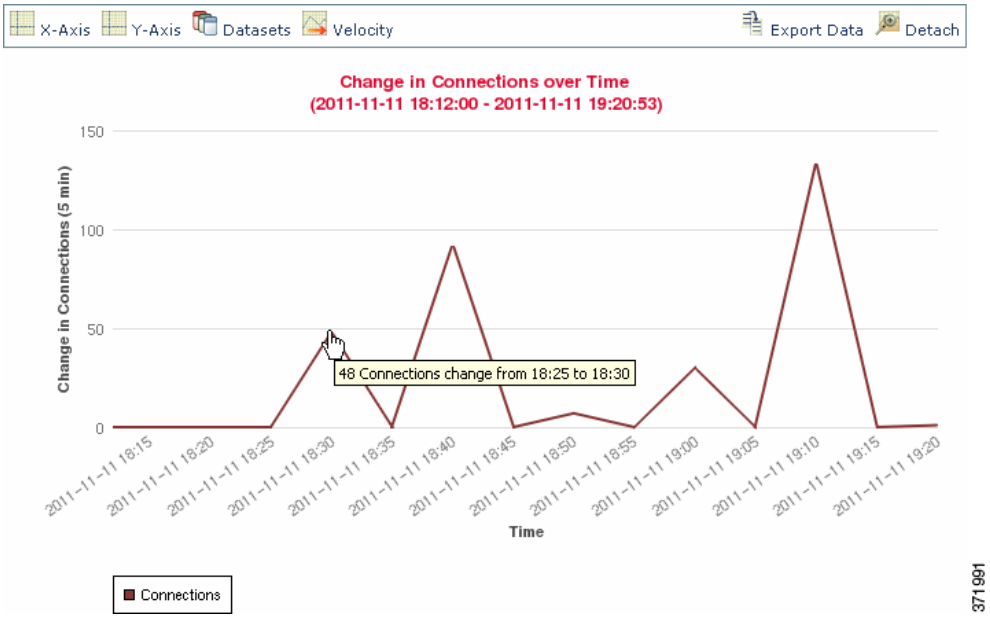
许可证：任何环境

有三种不同的连接图：曲线图、条形图和饼形图。*曲线图*可对一定时间内的数据绘制图表。例如，下面的曲线图显示了一个小时时间区间内监控网络上检测到的连接总数。流量量变曲线总是以曲线图的形式显示。

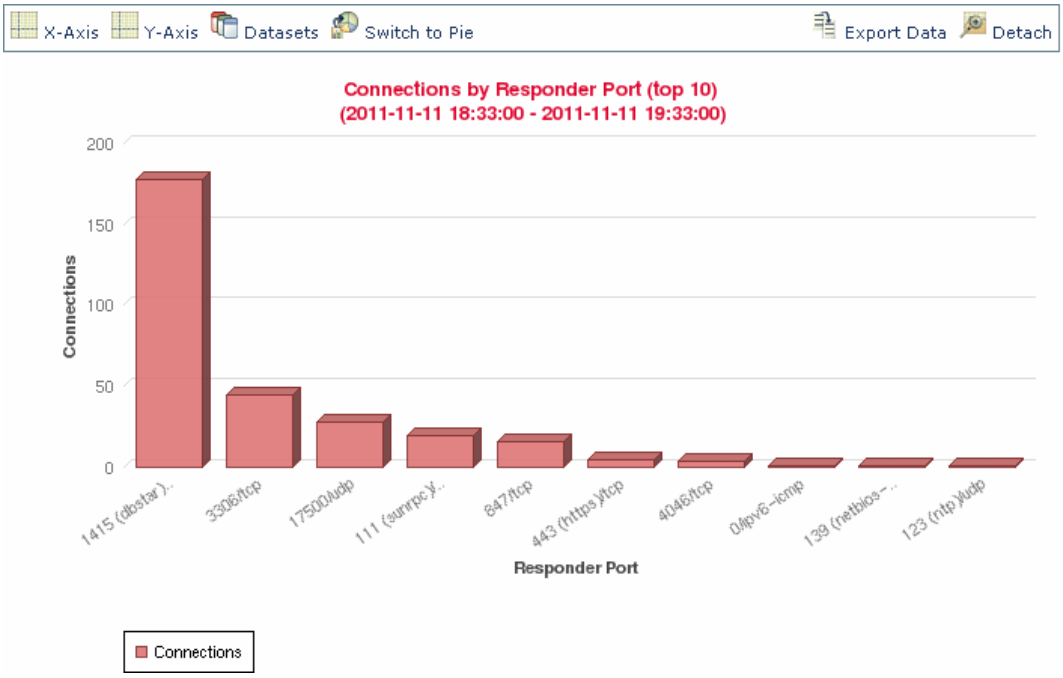


默认情况下，在*标准视图*中显示曲线图。标准曲线图每隔五分钟汇总数据、绘制汇总数据点，并连接这些数据点。

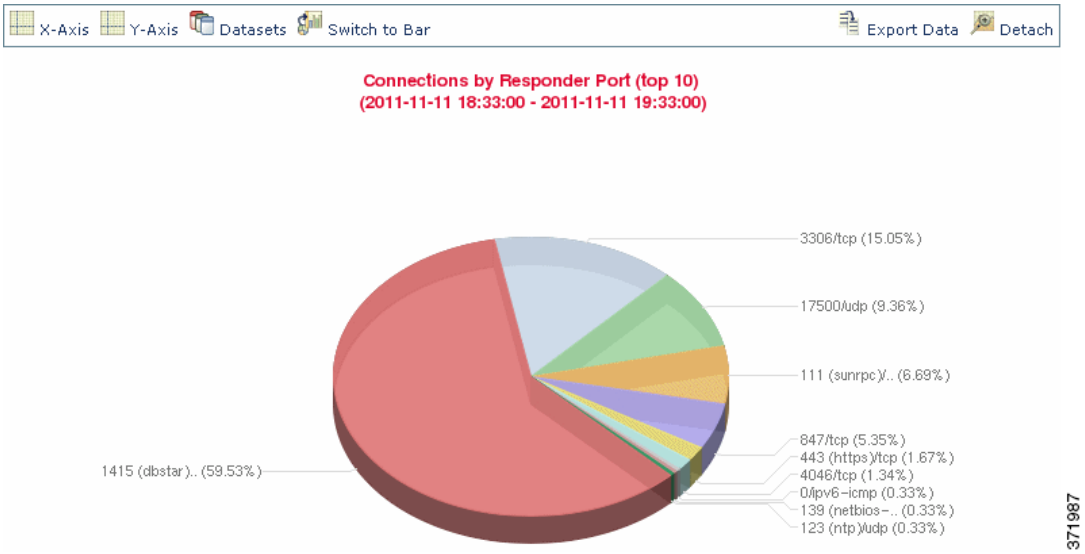
不过，您可将曲线图从标准视图切换至*速度视图*。速度曲线图会显示这些数据点之间的变化率。如果将以上图形更改为速度曲线图， y 轴会从表示连接数量转变为表示在一段时间内连接数量的变化。



*条形图*显示按各种类别分组的数据。例如，条形图可以显示在一个小时的时间区间内，在监控网络的 10 个最活跃端口上检测到的连接数。



饼形图，如条形图，也显示按各种类别分组的数据。下面的饼形图与上面的条形图显示的信息相同。



按照下表中的指示在标准曲线图与速度曲线图之间切换、在条形图和饼形图之间切换。

访问：管理员/任何安全分析师

表 39-3　　更改图形类型

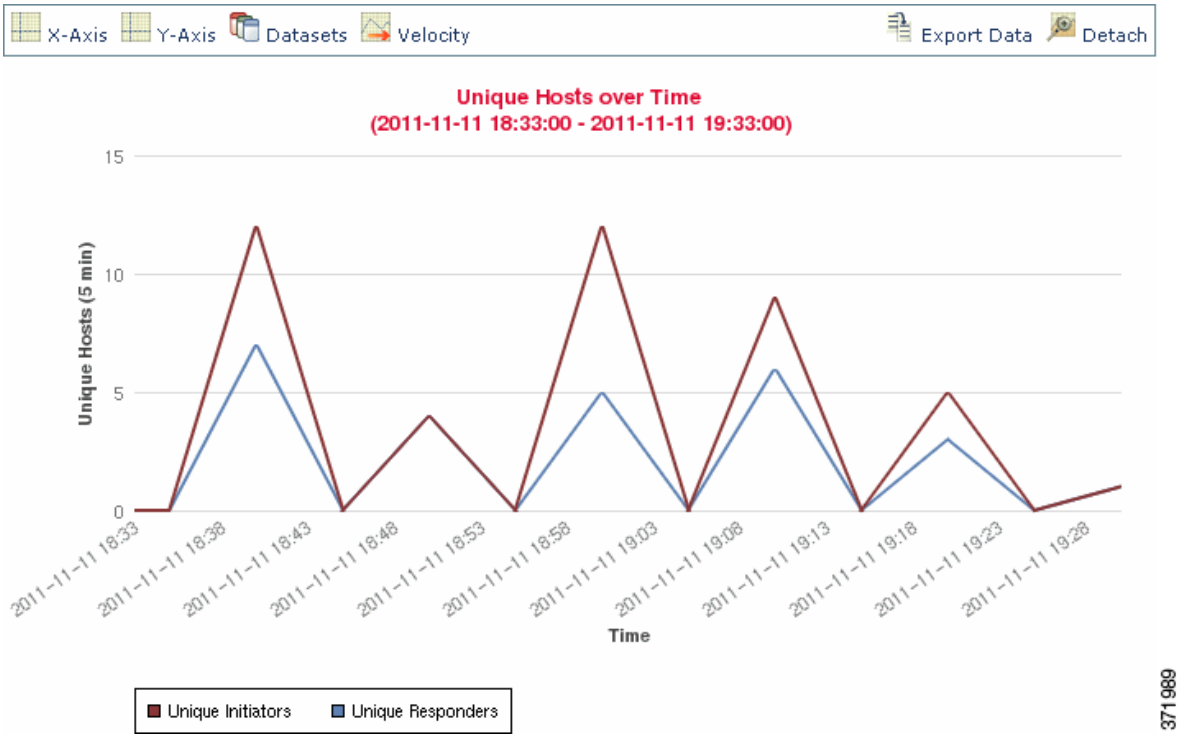
要更改.....	您可以.....
将条形图更改为饼形图	点击 **Switch to Pie**。 请注意，饼形图无法显示多个数据集；有关信息，请参阅第 39-17 页上的选择数据集。
将饼形图更改为条形图	点击 **Switch to Bar**。
将曲线图从标准曲线图更改为速度曲线图	点击 **Velocity** 并选择 **Velocity**。
将曲线图从速度曲线图更改为标准曲线图	点击 **Velocity** 并选择 **Standard**。

选择数据集

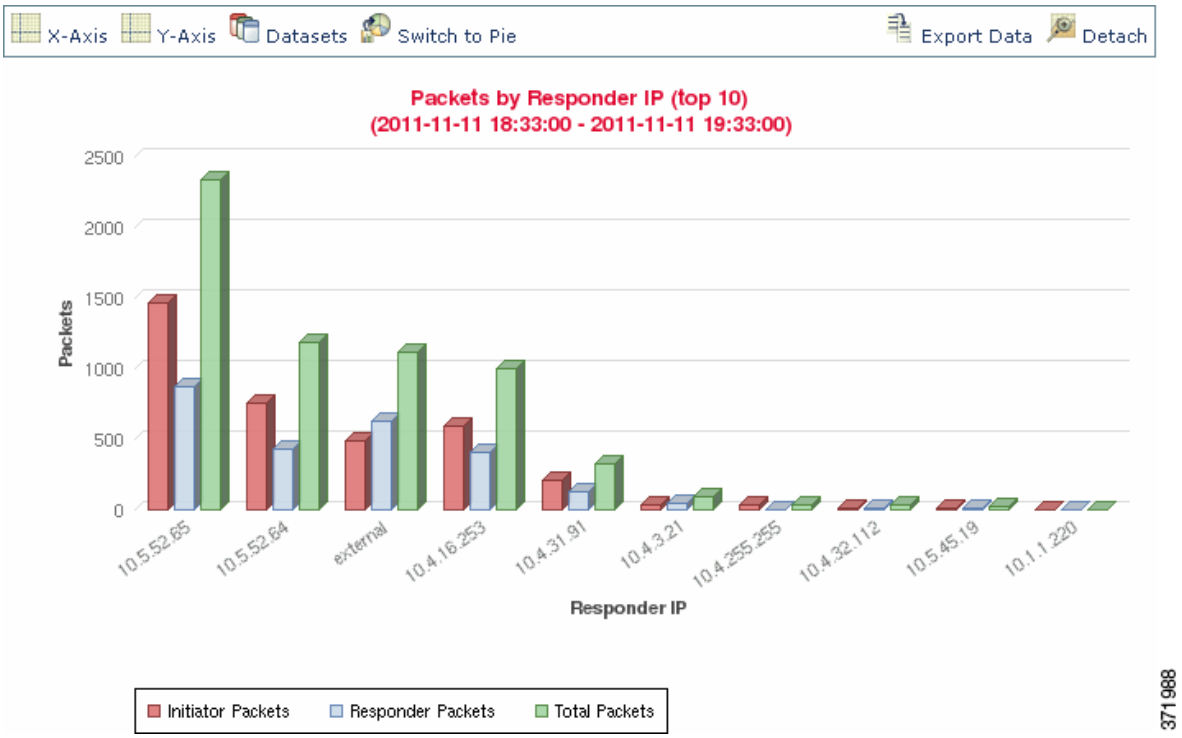
许可证：任何环境

条形图和曲线图可以显示多个数据集；也就是说，它们可以在 y 轴为每个 x 轴数据点显示几个值。例如，您可以显示独立发起方总数，而独立发起方总数饼形图只能显示一个数据集。

在曲线图上，多个数据集显示为多条线，每条线颜色不同。例如，下面的图形显示了在一个小时的时间区间内监控网络上检测到的独立发起方总数和独立响应方总数。



在条形图上，与 x 轴的各个数据点对应的多个数据集显示为一组彩色条形柱。例如，下面的条形图显示监控网络上传输的数据包总数、发起方传输的数据包总数以及响应方传输的数据包总数。



饼形图**不能**显示多个数据集。如果将具有多个数据集的条形图切换到饼形图，该饼形图只显示一个自动选择的数据集。当选择要显示的数据集时，防御中心会首选显示总统计数据，而不是发起方和响应方的统计数据；在显示发起方统计数据和响应方统计数据时，会首选显示发起方统计数据。下表介绍了在连接图 x 轴上可以显示的数据集。

表 39-4　　数据集选项

如果 y 轴显示.....	可以选为数据集的对象为.....
连接	仅默认数量，指在监控网络上检测到的连接数 (**Connections**) 这是流量剖面图的唯一选项。
KBytes	组合： • 监控网络上传输的总数据量 (**Total KBytes**) • 监控网络上的主机 IP 地址传输的数据量 (**Initiator KBytes**) • 监控网络上的主机 IP 地址收到的数据量 (**Responder KBytes**)
KBytes Per Second	仅默认数量，指在监控网络上每秒传输的总数据量 (**Total KBytes Per Second**)
数据包	组合： • 在监控网络上传输的数据包总数 (**Total Packets**) • 在监控网络上从主机 IP 地址传输的数据包总数 (**Initiator Packets**) • 在监控网络上主机 IP 地址收到的的数据包总数 (**Responder Packets**)
Unique Hosts	组合： • 在监控网络上独立会话发起方的数量 (**Unique Initiators**) • 在监控网络上独立会话响应方的数量 (**Unique Responders**)
Unique Application Protocols	仅默认数量，指监控网络上的独立应用协议的数量 (**Unique Application Protocols**)
Unique Users	仅默认数量，指登录到监控网络上会话发起方的独立用户的数量 (**Unique Initiator Users**)

要选择连接图上显示的数据集，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击 **Datasets**，然后选择想要绘制图形的数据集。

数据集选项表中介绍了可以选择的数据集。

查看有关汇总连接数据的信息

许可证：任何环境

连接图是基于每五分钟时间区间内汇总的数据 （也称为*连接摘要*）绘制的。有关用来构建连接图的具体连接摘要，您可获得详细信息。例如，在一段时间的连接图上，您可能想要知道在一个特定时间区间内究竟检测到了多少个连接。

要获得汇总的连接数据的详细信息，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　将光标移动至曲线图的某一点上、条形图的某一条上，或饼形图的某一块上。系统将显示一个提示框，其中提示构建该部分图形所用数据的详细信息。

在工作流程页面上操作连接图

许可证：任何环境

当打开连接数据工作流程时，最初数据仅受时间范围的限制。在不进入下一个工作流程页面的情况下，可使用其他标准限制连接图。

提示　以这种方式限制连接数据可以改变图形的 x 轴（在查看饼形图时也称为自变量）。要在不限制连接数据的情况下改变独立变量，请使用 **X-Axis** 和 **Y-Axis** 菜单。有关详细信息，请参阅第 39-22 页上的选择数据进行绘图。

要限制连接数据，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击曲线图上的某一点、条形图上的某一条，或饼形图上的某一块。

步骤 2　选择 **View by...** 选项。

可以基于 X 轴功能表中所列的任何标准对连接数据进行限制。

例如，思考一个长时间区间连接的图表。如果在按端口图形上应用时间点限制，系统会显示一个条形图，列出基于检测到的连接事件数目、同时受以所点击点为中心的 10 分钟时间区间限制的 10 个最活跃的端口。

如果通过点击条形图中的一个条柱并选择 **View by Initiator IP** 进一步限制该图形，系统将显示一个新的条形图。该条形图不仅受到与之前相同的 10 分钟时间区间的限制，还受到所点击条柱表示的端口的限制。

注　除非使用分离图形，否则以这种方式限制连接数据会改变时间范围。有关分离图的详细信息，请参阅第 39-23 页上的分离连接图。

深入研究连接数据图

许可证：任何环境

当打开连接数据工作流程时，最初数据仅受时间范围的限制。在进入下一个工作流程页面时，可以限制连接图。

要深入了解连接数据工作流程，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击曲线图上的某一点、条形图上的某一条，或饼形图上的某一块。

步骤 2　选择 **Drill-down**。

您可以向下深入了解下一个工作流程页面，使用点击的条目进行限制：

- 点击曲线图上的某个点可将下一个页面的时间范围限制为以所点击点为中心的 10 分钟时间区间。
- 点击条形图上的某一条或饼形图上的某一块，可基于该条或该块表示的标准限制下一个页面。例如，点击表示端口的条柱深入到下一个工作流程页面，该页面受所点击条柱表示的端口的限制。

重定曲线图的中心点和缩放

许可证：任何环境

您可以将任一时间点作为曲线图的中心时间点。可通过默认的时间范围重定中心，或选择不同的时间范围。

注　除非使用分离图，否则重定中心会改变默认的时间范围。有关分离图的详细信息，请参阅第 39-23 页上的分离连接图。

要使用默认的时间范围重定中心点，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在曲线图上点击要作为图形时间中心点的时间点，然后点击 **recenter**。

以所点击点为中心重新绘制该图，且时间区间与默认的时间范围相同。

要使用不同的时间范围重定中心点，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击想要重定图形中心的该点，然后点击 **Zoom**。

步骤 2　为新图形选择时间区间，该时间区间可长达一周也可短至一个小时。

系统将以所点击的时间点为中心、以选择的时间区间为时间区间，重新绘制图表。

选择数据进行绘图

许可证：任何环境

通过改变 x 轴、 y 轴或者 x 轴和 y 轴，可以在连接图上显示不同的数据。

请注意，在一个饼图上改变 x 轴可以改变自变量，改变 y 轴可以改变因变量。例如，考虑一个图形化显示各端口数据量的饼图。在这种情形下， x 轴是 **Responder Port**， y 轴是 **KBytes**。该饼图表示在一定时间区间内由监控网络发送的总数据量。该饼图的楔块表示在每端口上检测到的数据百分比。如果将该饼图 x 轴变更为 **Application Protocol**，该饼图仍然表示已传输的总数据量，但该饼图的楔块表示为每个已检测到应用协议传输的数据百分比。

然而，如果将第一个饼图的 y 轴改为 **Packets**，该饼图表示在一定时间区间内监控网络传输的数据包总数，而饼图的楔块表示每个端口上检测到的数据包在数据包总数中所占的百分比。

按照下表中指示变更连接图的 x 轴。

表 39-5　　X 轴功能

要按照如下标准图形化显示连接数据.....	您可以.....
按从检测到的连接事件数量来看监控网络上 10 个最活跃的应用协议。	点击 **X-Axis**，并选择 **Application Protocol**。
基于检测到的连接事件数量，在监控网络上利用10 个最活跃受管设备。	点击 **X-Axis**，并选择 **Device**。
按从检测到的连接事件数量来看监控网络上10 个最活跃的发起连接事务的主机 IP 地址。	点击 **X-Axis**，并选择 **Initiator IP**。
按从检测到的连接事件数量来看监控网络上 10 个最活跃的登录到发起连接事务的主机的用户。	点击 **X-Axis**，并选择 **Initiator User**。
按从检测到的连接事件数量来看监控网络上 10 个最活跃的地址为连接事务中响应方的主机 IP 地址。	点击 **X-Axis**，并选择 **Responder IP**。
按从检测到的连接事件数量来看监控网络上 10 个最活跃的主机为连接事务中响应方的端口。	点击 **X-Axis**，并选择 **Responder Port**。
按 10 个最活跃的源设备，其中包括已导出连接的相关连接数据的 NetFlow 启用设备以及名为 FireSIGHT 并适用于 思科受管设备检测到的所有连接的源设备。	点击 **X-Axis**，并选择 **Source Device**。
在一段时间内	点击 **X-Axis**，并选择 **Time**。

按照下表中指示变更连接图的 y 轴。

表 39-6　　Y 轴功能

要.....	您可以.....
按照您为 x 轴选择的标准，图形化显示监控网络上的连接数量	点击 **Y-Axis**，并选择 **Connections**。
按照您为 x 轴选择的标准，图形化显示监控网络上传输的总数据量	点击 **Y-Axis**，并选择 **KBytes**。
按照您为 x 轴选择的标准，图形化显示监控网络上每秒钟传输的总数据量	点击 **Y-Axis**，并选择 **KBytes Per Second**。
按照您为 x 轴选择的标准，图形化显示监控网络上传输的数据包总数	点击 **Y-Axis**，并选择 **Packets**。

表 39-6　　Y 轴功能 （续）

要.....	您可以.....
按照您为 x 轴选择的标准，图形化显示监控网络上检测到的独立主机总数	点击 **Y-Axis**，并选择 **Unique Hosts**。
按照您为 x 轴选择的标准，图形化显示监控网络上检测到的独立应用协议总数	点击 **Y-Axis**，并选择 **Unique Application Protocols**。
按照您为 x 轴选择的标准，图形化显示监控网络上检测到的独立用户总数	点击 **Y-Axis**，并选择 **Unique Users**。

分离连接图

许可证：任何环境

如果您想在不影响默认时间范围的情形下进一步分析连接图，可以将连接图分离到新的浏览器窗口。在分离的连接图上，您可以执行在嵌入连接图上执行的任何操作。通过点击 **Print**，您也可以打印已分离连接图。请注意，在默认情形下，流量剖面图是分离图形。

提示　如果您正在查看分离图，点击 **New Window** 在新的浏览器窗口中创建该分离图的另一份副本。然后，您可以在每个分离图上进行不同分析。

要分离图形，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击 **Detach**。

导出连接数据

许可证：任何环境

通过将连接数据导出为 CSV （逗号分隔值）文件，您就可以轻松地与他人共享连接数据。

提示　此外，通过右键单击连接图和遵循浏览器的提示，可以将连接图另存为图片。

要导出连接数据，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击 **Export Data**。

系统此时将弹出一个窗口，以表视图形式显示连接图上的数据。

步骤 2　点击 **Download CSV File**，并保存文件。

使用连接和安全情报数据表

许可证：因功能而异

受支持的设备：因功能而异

受支持的防御中心：因功能而异

FireSIGHT 系统事件查看器使您可以查看表中的连接数据，并根据分析相关信息利用事件视图。查看安全情报事件可让您专注于具有已确定的安全情报信誉的连接。（安全情报需要一个保护许可证，在 2 系列受管设备或者 DC500 防御中心上不予支持。）访问连接数据时所看到的页面因工作流程有所不同。工作流程只是一系列页面，您可以从广泛视图移动至更加突出重点的视图，使用这些页面评估事件。

注 此外，可用于任何单个连接或安全情报事件的信息取决于若干因素，包括许可证和应用型号。有关详细信息，请参阅第 38-8 页上的连接记录的许可证和型号要求。

提供的*连接事件*和*安全情报事件*工作流程提供基本连接和已检测到的应用信息相关摘要视图，然后，您可以展开到事件表视图。您还可以创建一个自定义工作流程，其中仅显示匹配特定需求的信息。

使用事件查看器，您可以：

- 搜索、分类和限制事件，以及变更已显示事件的时间范围
- 指定显示的列 （仅适用于表视图）
- 查看 IP 地址相关主机配置文件，或者与用户标识相关的用户详细信息和主机历史
- 查看连接中检测到的文件 （包括恶意软件文件）和入侵
- 查看与 IP 地址有关的地理定位信息
- 查看连接事件中的 URL 全文
- 查看用于加密会话的证书相关信息
- 查看已加密的会话详细信息
- 查看同一工作流程内使用不同工作流程页面的事件
- 集中查看使用不同工作流程的事件
- 展开工作流程内应用具体值限制的各个页面
- 给当前页加书签并进行限制，以便您在此后返回至相同数据 （假设该数据仍然存在）
- 使用当前限制创建报告模板
- 从数据库中删除事件
- 使用 IP 地址上下文菜单定制白名单、黑名单或者获取连接相关主机或 IP 地址的其他信息

请注意，当您在向下深入了解页面上约束连接事件时，来自相同事件的数据包和字节数将累加。然而，如果您正使用自定义工作流程，且没有将 **Count** 列添加到向下深入了解页面，则会单独列出事件，数据包和字节将不会累加。

以下各节包含有关查看及分析连接和安全情报事件表的信息：

- 第 58-1 页上的了解和使用工作流程提供有关使用事件查看器的详细说明。
- 第 58-17 页上的使用地理定位说明如何查看和解释与连接和安全情报事件相关联的地理定位信息。

- 第 71-3 页上的配置事件查看设置说明如何更改默认工作流程，以便查看连接和安全情报事件数据。
- 第 39-3 页上的了解连接和安全情报数据字段和第 39-9 页上的连接和安全情报事件中的可用信息提供连接和安全情报事件中数据的详细信息。
- 第 39-25 页上的使用监控规则相关的事件说明如何使用监控规则标准约束连接事件。
- 第 39-26 页上的查看连接中检测到的文件说明如何查看文件，包括连接中已检测或阻止的恶意软件文件。
- 第 39-26 页上的查看与连接有关的入侵事件说明如何查看连接相关的入侵事件。
- 第 39-27 页上的查看与加密连接相关的证书说明如何查看用于加密连接的证书相关详细信息。

使用监控规则相关的事件

许可证：任何环境

当您使用事件查看器查看已记录的连接时，防御中心显示用于处理每个连接的访问控制规则或者默认操作，并显示匹配这些连接中每个连接的最多 8 个监控规则。

如果连接匹配 1 条监控规则，则防御中心显示处理连接的规则名称，然后显示监控规则名称。如果连接匹配多个监控规则，则事件查看器显示所匹配的监控规则数量，例如，`Default Action + 2 Monitor Rules`。

您可以通过下面方式之一约束使用匹配的监控规则的连接事件视图：

- 处理该连接的访问控制规则或默认操作
- 连接匹配的单个监控规则

要使用监控规则匹配来约束连接事件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Connections > Events**。

系统将显示默认连接数据工作流程首页。

步骤 2　显示想要用于分析的工作流程。确保您正使用的向下深入了解页面或表视图显示 **Access Control Rule** 字段。

步骤 3　您希望如何约束事件？

- 要对处理连接的访问控制规则或默认操作进行约束，请点击规则名称或 **Default Action**。
- 要对匹配已记录连接的唯一监控规则进行约束，请点击监控规则名称。
- 要对匹配已记录连接的多个监控规则之一进行约束，请点击一个 *N* **Monitor Rules** 数值。例如，点击 **2 Monitor Rules**。

  系统将显示该连接事件的 Monitor Rules 弹出窗口，其中列出与该连接匹配的前 8 个监控规则。点击想要用于约束连接事件的监控规则名称。

事件受到约束。如果您正使用向下深入了解页面，事件视图转入工作流程中的下一页面。

查看连接中检测到的文件

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

如果将一个文件策略与一个或多个访问控制规则相关联，系统可以在匹配的流量中检测文件 （包括恶意软件）。通过使用事件查看器，您可以查看与这些规则所记录连接相关的文件事件 （如有）。

防御中心不显示文件列表，而是在 **Files** 列中显示视图文件图标 ( )。图标上的数字表示连接中检测到或阻止的文件数量 （包括恶意软件文件）。点击该图标将不会展开到下一工作流程页面或者约束连接事件，而是显示一个弹出窗口。窗口显示连接中检测到的文件列表及其类型、恶意软件查询处置情况 （如适用）。

在弹出窗口中，您可以点击：

- 文件视图图标 ( )，以便查看文件事件表视图中的详细信息。
- 恶意软件文件视图图标 ( )，以便查看恶意软件事件表视图中的详细信息。
- 文件轨迹图标 ( )，以便跟踪文件在网络中的传输情况。
- **View File Events** 或 **View Malware Events**，以便查看连接中已检测到的文件或基于网络的所有恶意软件事件详细信息。

提示 要快速查看与一个或多个连接相关联的文件或恶意软件事件，请在事件查看器中使用复选框选择连接，然后从 **Jump to** 下拉列表中选择 **Malware Events** 或 **File Events**。您可以使用类似方式查看用于传输文件的连接。有关详细信息，请参阅第 58-31 页上的在工作流程之间导航。

当您查看相关事件时，防御中心使用适用于该事件类型的默认工作流程。有关文件和恶意软件事件的详细信息，请参阅第 40-6 页上的使用文件事件和第 40-14 页上的使用恶意软件事件。有关使用网络文件轨迹功能的详细信息，请参阅第 40-30 页上的使用网络文件轨迹。

请注意，并非所有文件和恶意软件事件都与连接有关，如下说述：

- 基于终端的恶意软件事件与连接不相关。这些事件由 FireAMP 连接器生成，而并不是由检查网络流量的系统生成。
- 许多启用 IMAP 的邮件客户端使用单个 IMAP 会话，仅当用户退出应用时才结束。尽管长期运行的连接由系统进行记录 （请参阅第 39-3 页上的长期运行连接），但是直至会话结束，会话中下载的文件都不会与连接相关联。

还请注意， 2 系列、用于 Blue Coat X-系列的思科 NGIPS设备和 DC500 防御中心不支持基于网络的高级恶意软件防护。

查看与连接有关的入侵事件

许可证：保护

如果您将入侵策略与访问控制规则或默认操作相关联，系统可以检测匹配流量中的漏洞。通过使用事件查看器，您可以查看与已记录连接相关的入侵事件 （如有）。

防御中心不显示一份事件列表，而是将入侵事件查看图标 ( ) 显示在 **Intrusion Events** 列中。点击该图标将不会展开到下一工作流程页面或者约束连接事件，相反，将显示一个弹出窗口。窗口中显示与连接相关的入侵事件列表，以及事件的优先级和影响力。

在弹出窗口中，您可以点击列出事件的视图图标 ( )，以便在数据包视图中查看详细信息。您还可以点击 **View Intrusion Events** 查看与连接有关的所有入侵事件的详细信息。

提示 要快速查看与一个或多个连接相关联的入侵事件，请在事件查看器中使用复选框选择连接，然后从 **Jump to** 下拉列表中选择 **Intrusion Events**。您可以使用类似方式查看与入侵事件相关的连接。有关详细信息，请参阅第 58-31 页上的在工作流程之间导航。

当您查看相关事件时，防御中心使用默认的入侵事件工作流程。有关入侵事件的详细信息，请参阅第 41-1 页上的处理入侵事件。

查看与加密连接相关的证书

许可证：任何环境

如果配置 SSL 检查，可以记录已加密的连接。通过使用事件查看器，您可以查看用于加密连接的公共密钥证书详细信息，但前提是系统已对流量执行操作和该证书可用。

防御中心不显示证书本身，而是显示将锁形图标 ( ) 显示在 **SSL Status** 列中。点击该图标将显示一个弹出窗口，其中包含下表中所述的证书详细信息。

表 39-7　已加密连接的证书详细信息

属性	说明
Subject/Issuer Common Name	证书主体或证书颁发者的主机名和域名。
Subject/Issuer Organization	证书主体或证书颁发者的组织。
Subject/Issuer Organization Unit	证书主体或证书颁发者的组织单位。
Not Valid Before/After	证书有效日期。
Serial Number	由发行 CA 分配的序列号。
Certificate Fingerprint	用于验证证书的 SHA 哈希值。
Public Key Fingerprint	用于对证书内所含公钥进行身份验证的 SHA 哈希值。

通过双击标题，您可以在弹出窗口内展开或折叠区域。

请注意，如果系统已对加密流量执行操作，但证书不可用，那么锁形图标呈现灰色。例如，如果系统因连接包含 SSL 握手错误，且无法进行解密而阻止了该连接，那么系统不具有加密证书详细信息，并且该连接的锁形图标会灰显。

搜索连接和安全情报数据

许可证：任何环境

通过使用防御中心的 Search 页面，可以搜索特定连接事件、安全情报事件或连接摘要；在事件查看器中显示结果；并保存您的搜索条件以备稍后重复使用。自定义分析控制面板构件、报告模版和自定义用户角色也可以使用保存的搜索条件。

下文以已保存搜索列表中用（思科）标记的系统配套搜索条件作为示例。

由于连接图基于连接摘要，因此，约束连接摘要的相同标准也约束连接图。标有星号 (*) 的字段约束连接图、连接摘要以及单个连接或安全情报事件。

如果使用无效的搜索约束搜索连接摘要，并在自定义工作流程中使用连接摘要页面查看结果，那么无效约束将标记为不适用 (N/A)，并标有一根删除线，如下面图例中所示。

此外，请注意，搜索结果取决于正搜索事件中的可用数据。换言之，根据可用数据，搜索限制条件可能不适用。有关各连接数据字段中数据可用时间的信息，请参阅第 39-9 页上的连接和安全情报事件中的可用信息。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。指定字段中包含列出的任何值的记录与搜索条件相匹配。
- 所有字段都接受用引号引住的逗号分隔列表作为搜索值。
  - 对于可能仅包含一个值的字段，指定字段包含引号中指定的准确字符串的记录与搜索条件相匹配。例如，搜索 `A, B, "C, D, E"` 将匹配指定字段包含 `"A"`、`"B"` 或 `"C, D, E"` 的记录。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含引号引住的逗号分隔列表中的所有值的记录与搜索条件相匹配。
  - 对于可能同时包含多个值的字段，搜索条件可能包括单个值以及用引号引住的逗号分隔列表。例如，在可能包含一个或多个 `A, B, "C, D, E"` 字母的字段搜索这些字母时，将匹配指定字段包含 `A`、`B` 或同时包含 `C`、`D` 和 `E` 的记录。
- 搜索仅返回与为所有字段指定的搜索条件均匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 在任一字段指定 `n/a` 以便识别信息不适用于该字段的事件；使用 `!n/a` 识别字段填充事件。
- 使用设备字段搜索特定设备以及组、堆栈或集群中的设备。有关 FireSIGHT 系统如何处理搜索中设备字段的详细信息，请参阅第 60-6 页上的在搜索中指定设备。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

连接和安全情报数据专用搜索语法

为补充上文列出的通用搜索语法，以下列表介绍了用于连接和安全情报数据的一些专用搜索语法。

连接匹配的监控规则

使用 **Access Control Rule** 条件搜索匹配单个监控规则的连接。

由于匹配监控规则的流量始终由其他规则或默认操作进行后续处理，因此，您无法搜索与 `Monitor` 操作有关的连接。无论后续处理连接的规则或默认操作如何，搜索监控规则名称都会返回匹配该监控规则的所有连接。

带一个数值 （Bytes、 Packets 和 Connections）的条件

您可以将下列字符添加在该数值前面：大于 (>)、大于或等于(>=)、小于(<)、小于或等于(<=)或者等于 (=)。

提示　要查看通过 **Connections** 条件进行搜索获得的有意义结果，您必须使用具有连接摘要页面的自定义工作流程。

与连接相关的 Files 或 Intrusion Events

您无法使用连接/安全情报事件 Search 页面搜索与连接相关联的文件、恶意软件和入侵事件。有关查看这些相关事件的信息，请参阅第 39-26 页上的查看连接中检测到的文件和第 39-26 页上的查看与连接有关的入侵事件。

连接的 Initiator User 或 URL

系统执行部分匹配，即您可以搜索全部或部分字段内容而无需使用星号。

连接中使用的总流量 （字节）或传输协议

要确定连接表视图上是否存在协议或流量约束，请展开搜索限制。

要搜索特定协议，请使用 http://www.iana.org/assignments/protocol-numbers 中列出的名称或编号协议。

这些列不会显示在表视图中。

NetFlow 连接中的 TCP Flags

键入以逗号分隔的一列 TCP 标志，查看*至少*具有其中一个标志 （而不是全部）的所有连接。您也可以选择 **Only** 复选框搜索仅具有您所指定 TCP 标志的连接。

应用于连接的 SSL 加密

键入 `yes` 或 `no` 查看 SSL 加密或未加密连接。

此列不显示在安全情报或连接事件表视图中。

The SSL Status

键入为 **SSL Actual Action** 和 **SSL Failure Reason** 列出的一个或多个关键字，以查看系统对其应用操作或发生问题的已加密流量。此字段可能同时包含一个 **SSL Actual Action** 值和 **SSL Failure Reason** 值。

当解密成功时，安全情报和连接事件表视图在 **SSL Status** 列中显示 **SSL Actual Action** 的值。当系统解密流量失败时，安全情报和连接事件表视图在 **SSL Status** 列中同时显示 **SSL Actual Action** 和 **SSL Failure Reason**的值。

The SSL Actual Action taken

键入任何以下关键字，以查看系统已应用指定操作的已加密流量：

- `Do not Decrypt` 代表系统未解密的连接。
- `Block` 和 `Block with reset` 代表被阻止的加密连接。
- `Decrypt (Known Key)` 代表使用已知私有密钥解密的传入连接。
- `Decrypt (Replace Key)` 代表使用带替代公共密钥的自签服务器证书解密的传出连接。
- `Decrypt (Resign)` 代表使用重签服务器证书解密的传出连接。

当解密成功时，安全情报和连接事件表视图在 **SSL Status** 列中显示此值。当系统解密流量失败时，安全情报和连接事件表视图在 **SSL Status** 列中同时显示此值和 **SSL Failure Reason**。

The SSL Expected Action

键入以下任何关键字，以查看在 SSL 规则有效的情况下预期系统应以指定方式处理的已加密流量：

- `Do not Decrypt` 代表系统未解密的连接。
- `Block` 和 `Block with reset` 代表被阻止的加密连接。
- `Decrypt (Known Key)` 代表使用已知私有密钥解密的传入连接。
- `Decrypt (Replace Key)` 代表使用带替代公共密钥的自签服务器证书解密的传出连接。
- `Decrypt (Resign)` 代表使用重签服务器证书解密的传出连接。

此列不显示在安全情报或连接事件表视图中。

The SSL Failure Reason

键入以下任何关键字，以查看系统由于指定原因未能解密的已加密流量：

- `Unknown`
- `No Match`
- `Success`
- `Uncached Session`
- `Unknown Cipher Suite`
- `Unsupported Cipher Suite`
- `Unsupported SSL Version`
- `SSL Compression Used`
- `Session Undecryptable in Passive Mode`
- `Handshake Error`
- `Decryption Error`
- `Pending Server Name Category Lookup`
- `Pending Common Name Category Lookup`
- `Internal Error`
- `Network Parameters Unavailable`
- `Invalid Server Certificate Handle`
- `Server Certificate Fingerprint Unavailable`
- `Cannot Cache Subject DN`
- `Cannot Cache Issuer DN`
- `Unknown SSL Version`
- `External Certificate List Unavailable`
- `External Certificate Fingerprint Unavailable`
- `Internal Certificate List Invalid`
- `Internal Certificate List Unavailable`
- `Internal Certificate Unavailable`
- `Internal Certificate Fingerprint Unavailable`
- `Server Certificate Validation Unavailable`
- `Server Certificate Validation Failure`
- `Invalid Action`

当系统解密流量失败时，安全情报和连接事件表视图在 **SSL Status** 列中将此值与 **SSL Actual Action** 一起显示。

使用的 SSL 加密套件

键入表示用于连接加密的密码套件的宏值。有关密码套件值名称，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。

SSL 主体国家/地区

键入一个双字符 ISO 3166-1 二位字母国家/地区代码，查看与加密证书主体的国家/地区关联的已加密流量。

此列不显示在安全情报或连接事件表视图中。

SSL 颁发者国家/地区

输入一个双字符 ISO 3166-1 二位字母国家/地区代码，查看与加密证书主体国家/地区关联的已加密流量。

此列不显示在安全情报或连接事件表视图中。

SSL Certificate Fingerprint

键入或粘贴用于对证书进行身份验证的 SHA 哈希值，查看与该证书关联的流量。

此列不显示在安全情报或连接事件表视图中。

SSL Public Key Fingerprint

键入或粘贴用于对证书中包含的公用密钥进行身份验证的 SHA 哈希值，查看与该证书关联的流量。

此列不显示在安全情报或连接事件表视图中。

SSL Certificate Status

此字段仅在配置了证书状态规则条件时适用。键入下面列出的一个或多个关键字，查看与服务器证书状态关联的已加密流量。已加密流量可能同时与多个服务器证书状态值相匹配。

- `Not Checked`
- `Self Signed`
- `Valid`
- `Invalid Signature`
- `Invalid Issuer`
- `Expired`
- `Unknown`
- `Not Valid Yet`
- `Revoked`

SSL Flow Messages

键入以下任何关键字，查看与在 SSL 握手期间客户端与服务器之间交换的以下消息相关联的已加密流量：

- `HELLO_REQUEST`
- `CLIENT_ALERT`
- `SERVER_ALERT`
- `CLIENT_HELLO`
- `SERVER_HELLO`
- `SERVER_CERTIFICATE`
- `SERVER_KEY_EXCHANGE`
- `CERTIFICATE_REQUEST`
- `SERVER_HELLO_DONE`
- `CLIENT_CERTIFICATE`
- `CLIENT_KEY_EXCHANGE`
- `CERTIFICATE_VERIFY`
- `CLIENT_CHANGE_CIPHER_SPEC`

- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER

SSL Version

键入以下任何关键字，查看与指定的 SSL 或 TLS 协议版本相关联的已加密流量：

- Unknown
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TSLv1.2

SSL Serial Number

键入或粘贴由颁发 CA 分配给公共密钥证书的序列号。

此列不显示在安全情报或连接事件表视图中。

要搜索连接或安全情报数据，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　您有以下选项：

- 从表下拉列表中选择 **Connection Events**，以搜索连接数据。
- 从表下拉列表中选择 **Security Intelligence Events**，以搜索安全情报数据。

系统将用相应限制更新页面。

步骤 3　在相应字段输入搜索条件：

- 有关连接和安全情报事件表中字段的信息，请参阅第 39-3 页上的了解连接和安全情报数据字段。
- 有关公用密钥证书相关字段的信息，请参阅第 39-27 页上的查看与加密连接相关的证书。
- 有关用于连接和安全情报事件的特殊搜索语法的信息，请参阅第 39-28 页上的连接和安全情报数据专用搜索语法。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索另存为私有，这样只有您才能访问它。否则，请保持清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功（如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示输入搜索名称；请输入一个唯一搜索名称并点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认连接或安全情报工作流程中，受限于当前时间范围。

查看 Connection Summary 页面

许可证：任何环境

Connection Summary 页面以图形化形式提供按不同标准组织的监控网络中的活动。例如，Connections over Time 图表显示在选定时间期限内监控网络上的连接总数。

注　仅满足下面条件的用户可查看 Connection Summary 页面：已拥有受连接事件搜索限制的自定义角色，并已明确获得有关访问 Connection Summary 页面的授权。有关详细信息，请参阅第 61-51 页上的了解受限用户访问属性和第 61-48 页上的管理自定义用户角色。

下表介绍了您可以在 Connection Summary 页面上执行的各项操作。

表 39-8　Connection Summary 页面操作

要.....	您可以.....
修改用于 Connection Summary 页面的时间和日期范围	在第 58-19 页上的设置事件时间限制中获得详细信息。
处理连接图	在第 39-13 页上的使用连接图中获得详细信息。
从该页面中分离连接图	在想要分离的图形上点击 **View**。有关分离图的详细信息，请参阅第 39-23 页上的分离连接图。

如同连接图，您几乎可以在连接摘要图上执行完全一样的操作。然而，由于 Connection Summary 页面上的图形基于汇总数据，因此，您无法检查图形依赖的单个连接事件。换句话说，您无法从连接摘要图展开到连接数据表视图。

要查看 Connection Summary 页面，请执行以下操作：

访问：自定义

步骤 1　选择 **Overview > Summary > Connection Summary**。

系统将显示 Connection Summary 页面，并适用于您选择的防御中心当前时间范围。

步骤 2　从 **Select Device** 列表中，选择您需要查看其摘要的设备，或者选择 **All**，以查看所有设备摘要。

分析恶意软件和文件活动

防御中心将系统文件检查和处理的记录作为捕获文件、文件事件和恶意软件事件进行记录：

- *捕获文件*表示系统捕获的文件。
- *文件事件*表示系统在网络流量中检测到并或者被阻止的文件。
- *恶意软件事件*表示系统在网络流量中检测到并或者被阻止的恶意软件文件。
- *追溯性恶意软件事件*表示恶意软件文件的性质已更改的文件。

当系统基于对网络流量中恶意软件的检测或阻止生成恶意软件事件时，也会生成文件事件，因为要在文件中检测恶意软件，系统必须首先检测该文件本身。请注意， FireAMP 连接器 （请参阅第 37-6 页上的集成 FireAMP 与 FireSIGHT 系统）生成的基于终端的恶意软件事件不具备对应文件事件。同样，当系统在网络流量中捕获文件时，也会生成文件事件，因为系统将首先检测到该文件。

您可以使用防御中心查看、操作和分析捕获的文件、文件事件和恶意软件事件，然后与其他人交流您的分析结果。通过 Context Explorer、控制面板、事件查看器、上下文菜单、网络文件轨迹映射和报告功能，您可以更深入了解检测、捕获及阻止的文件和恶意软件。您也可以使用事件触发关联策略违规或者通过邮件、 SMTP 或系统日志向您发出警报。

由于您无法在 DC500 上使用恶意软件许可证，也无法在2 系列设备或用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此无法使用这些设备生成或分析与恶意软件云查找或与存档文件的内容相关联的捕获文件、文件事件和恶意软件事件。

有关详情，请参阅：

- 第 40-2 页上的使用文件存储
- 第 40-4 页上的使用动态分析
- 第 40-6 页上的使用文件事件
- 第 40-14 页上的使用恶意软件事件
- 第 40-25 页上的使用捕获的文件
- 第 40-30 页上的使用网络文件轨迹

有关配置系统以执行可以产生本章所讨论数据的恶意软件防护和文件控制操作的信息，请参阅第 37-1 页上的阻止恶意软件和禁止的文件。

使用文件存储

许可证：恶意软件

受支持的设备：任何设备， 2 系列或X -系列除外

受支持的防御中心：除 DC500 外的所有型号

根据文件策略配置，您可以使用文件控制功能检测和阻止文件。但是，来自可疑主机或网络的文件或者发送至您网络上受监控主机的多余文件可能需要进一步分析。通过文件存储功能，您可以捕获在流量中检测到的选定文件，并自动将其存储至设备硬盘驱动器或（如果已安装）恶意软件存储包内。

当设备在流量中检测到文件时，它可以捕获该文件。这将创建一个副本，系统可以存储或者提交该副本以进行动态分析。在设备捕获文件后，您有若干选择：

- 将捕获文件存储至设备硬盘驱动器中供后期分析使用。有关详情，请参见第 40-3 页上的了解捕获文件存储。
- 将存储的文件下载至本地计算机，以便进一步实施人工分析或存档。有关详情，请参见第 40-3 页上的将存储的文件下载至另一位置。
- 将捕获文件提交给综合安全智能云进行动态分析。有关详情，请参见第 40-4 页上的使用动态分析。

请注意，文件存储在设备中之后，如果未来检测到该文件且设备仍存有该文件，则不会再捕获该文件。

注 防御中心完成云查找后，首次检测到的文件将分配有一个性质。除非文件立即分配有一个性质，否则系统将生成一个文件事件，但是无法存储文件。

如果之前未检测到的文件与具有阻止恶意软件操作的文件规则相匹配，则随后的云查找将立即返回性质，从而使系统可以存储文件并生成事件。

如果之前未检测到文件与具有恶意软件云查找操作的文件规则相匹配，则系统将生成文件事件，但需要额外的时间执行云查找并返回性质。由于这种延迟，系统无法存储与具有恶意软件云查找操作的文件规则想匹配的文件，直到在网络上第二次看到这些文件。

无论系统捕获还是存储文件，您都可以：

- 从事件查看器中审查捕获文件的信息，包括文件是否存储或提交用于动态分析、文件性质和威胁评分，以便迅速查看网络中检测到的恶意软件潜在威胁。有关详情，请参见第 40-25 页上的使用捕获的文件。
- 查看文件轨迹，确定其如何穿过网络以及哪些主机有副本。有关详情，请参见第 40-32 页上的分析网络文件轨迹。
- 向清空列表或自定义检测列表添加文件，以便在未来检测过程中始终将该文件作为清空或恶意软件性质。有关详情，请参见第 3-29 页上的使用文件列表。

您可以在文件策略中配置文件规则，以便捕获并存储特定类型或者具有特定文件性质的文件（如有）。如果将该文件策略与访问控制策略相关联，并将其应用于设备上，则系统将捕获并存储流量中的匹配文件。还可以限制要存储的最小和最大文件大小。有关详细信息，请参阅第 18-17 页上的调整文件和恶意软件检查性能和存储和第 37-15 页上的使用文件规则。

文件存储需要设备上有足够的磁盘空间。如果设备主硬盘驱动器空间不足，而且未安装恶意软件存储包，则无法在设备上存储文件。

注意事项 请勿尝试在设备中安装思科未提供的硬盘驱动器。安装不受支持的硬盘驱动器可能会损坏设备。恶意软件存储包套件**仅**可从思科购买，而且**仅限**用于 8000 系列设备。如果需要恶意软件存储包方面的帮助，请与技术支持部门联系。有关详细信息，请参阅 《*FireSIGHT 系统恶意软件存储包指南*》。

请注意，由于您无法在 DC500 上使用恶意软件许可证，也无法在 2 系列设备或用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此，无法使用这些设备捕获或存储文件。

有关详情，请参阅：

- 第 40-3 页上的了解捕获文件存储
- 第 40-3 页上的将存储的文件下载至另一位置

了解捕获文件存储

许可证：恶意软件

受支持的设备：8000 系列

基于文件策略配置，设备可以将大量文件数据存储在硬盘驱动器中。您可以在设备上安装恶意软件存储包。系统将文件存储在恶意软件存储包内，允许主硬盘驱动器留出更多空间存储事件和配置文件。系统定期删除早期文件。

注意事项 请勿尝试在设备中安装思科未提供的硬盘驱动器。安装不受支持的硬盘驱动器可能会损坏设备。恶意软件存储包套件**仅**可从思科购买，而且**仅限**用于 8000 系列设备。如果需要恶意软件存储包方面的帮助，请与技术支持部门联系。有关详细信息，请参阅 《*FireSIGHT 系统恶意软件存储包指南*》。

在未安装恶意软件存储包时，如果将设备配置为存储文件，设备将分配一部分主硬盘驱动器空间专用于存储捕获文件。如果您在设备上安装恶意软件存储包并配置设备存储文件，设备将分配整个恶意软件存储包用于存储捕获文件。设备不会在恶意软件存储包中存储其他任何信息。

当分配的用于存储捕获文件的空间用尽时，系统删除最早的存储文件，直至分配空间达到系统定义的阈值。依据存储文件数量，在系统删除文件后，磁盘用量将大幅下降。

如果在安装恶意软件存储包时，设备已经存储文件，当您下次重启设备时，存储在主硬盘驱动器上的捕获文件将移至恶意软件存储包中。设备未来存储的文件都将存储至恶意软件存储包。如果设备主硬盘驱动器空间不足，也未安装恶意软件存储包，您将无法存储文件。

请注意，您不能将存储的文件置于系统备份文件中。有关详细信息，请参阅第 70-2 页上的创建备份文件。

将存储的文件下载至另一位置

许可证：恶意软件

受支持的设备：任何设备， 2 系列或 X -系列除外

受支持的防御中心：除 DC500 外的所有型号

设备存储文件后，只要防御中心可以与该设备保持通信并且未删除该文件，您就可以下载该文件。您可以人工分析该文件，或者将其下载至本地主机进行长期存储和分析。您可以从相关文件事件、恶意软件事件、捕获文件视图或文件轨迹中下载文件。有关详细信息，请参阅第 2-4 页上的使用上下文菜单和第 40-32 页上的概要信息。

由于恶意软件有害，默认情况下，您必须在每次下载文件时进行确认。但是您可以禁用文件下载确认提示。要重新启用确认，请参阅第 71-4 页上的文件首选项。

注意事项 思科强烈建议您**不要**下载恶意软件，否则可能造成不利后果。下载任何文件时请保持谨慎，这些文件可能包含恶意软件。确保您在下载文件前已采取各种必要预防措施保证下载目标安全。

因为性质为 Unknown 的文件可能包含恶意软件，当您下载文件时，系统会首先将该文件存档至 .zip 压缩包。.zip 文件名包含文件性质和文件类型（如有）以及 SHA-256 值。您可以对 .zip 文件采用密码保护以防意外解压缩。要编辑或删除默认 .zip 文件密码，请参阅第 71-4 页上的文件首选项。

使用动态分析

许可证：恶意软件

受支持的设备：任何设备， 2 系列或 X -系列除外

受支持的防御中心：除 DC500 外的所有型号

要增加云准确性并提供额外的恶意软件分析和威胁识别，可以向思科云提供合格捕获文件用于动态分析。云在测试环境中运行文件，并根据结果向防御中心返回威胁评分和动态分析总结报告。您也可以向云提交合格文件进行 Spero 分析，检查文件结构以便补充恶意软件识别。

能够将文件提交到云进行动态分析取决于捕获的文件类型，以及访问控制策略中配置的文件大小上限和下限。您可以：

- 自动提交文件进行动态分析 （如果文件规则在可执行文件上执行并且文件性质为 Unknown）
- 人工一次性提交最多二十五个文件进行动态分析 （如果这些文件已存储并且是受支持的文件类型，例如 PDF、 Microsoft Office 文档等）

提交后，文件会在云中排队等待分析。您可以查看捕获的文件和文件轨迹，判断文件是否提交用于动态分析。请注意，每次提交文件进行动态分析时，云都会分析该文件，即使首次分析已经产生结果。

有关详细信息，请参阅第 37-15 页上的使用文件规则和第 40-5 页上的提交文件进行动态分析。

注 系统会检查云，确定动态分析合格文件类型列表是否更新以及可提交的最小和最大文件大小 （不超过一日一次）。

云通过在沙盒环境中运行文件来对文件执行动态分析。它将返回：

- 威胁评分，详细介绍文件包含恶意软件的可能性。
- 动态分析总结报告，详细介绍云分配威胁评分的原因。

基于文件策略配置，您可以自动阻止威胁评分超过定义的阈值的文件。您也可以审查动态分析总结报告，以便更好地识别恶意软件、调整检测功能。

要补充动态分析，如果文件规则在可执行文件上执行恶意软件云查找，您可以自动提交该文件进行 Spero 分析。云将检查可执行文件结构 （包括元数据和标题信息），并确定文件为恶意软件。有关详情，请参见第 37-2 页上的了解恶意软件防护和文件控制。

请注意，由于无法在 DC500 上使用恶意软件许可证，也无法在 2 系列设备或用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，因此，无法使用这些设备提交文件供动态分析或 Spero 分析。

注　您可以配置受管设备，通过 HTTP 代理向思科云提交文件。要配置物理设备，请参阅第 64-8 页上的配置管理接口了解详细信息。要配置虚拟设备，请参阅第 D-32 页上的 http-proxy。用于 Blue Coat X-系列的思科 NGIPS不支持代理设置。

有关详情，请参阅：

- 第 40-5 页上的了解 Spero 分析
- 第 40-5 页上的提交文件进行动态分析
- 第 40-5 页上的审查威胁评分和动态分析总结

了解 Spero 分析

许可证：恶意软件

受支持的设备：任何设备， 2 系列或 X -系列除外

受支持的防御中心：除 DC500 外的所有型号

Spero 分析可补充 SHA-256 散列的分析结果，允许更完整地识别可执行文件内的恶意软件。Spero 分析需要设备检验文件结构特点，例如元数据和标题信息。基于该信息生成 Spero 签名后，设备会将其提交给思科云内的 Spero 启发式引擎。基于 Spero 签名，Spero 引擎返回文件是否为恶意软件的结果。如果是，并且当前文件的文件性质为未知，则系统分配 Malware 文件性质。有关文件性质的详细信息，请参阅第 37-2 页上的了解恶意软件防护和文件控制。

请注意，您只能在检测时提交可执行文件进行 Spero 分析；此后将无法人工提交文件。您可以提交文件进行 Spero 分析，而无需再提交这些文件进行动态分析。有关详细信息，请参阅第 37-15 页上的使用文件规则。

提交文件进行动态分析

许可证：恶意软件

受支持的设备：任何设备， 2 系列或 X -系列除外

受支持的防御中心：除 DC500 外的所有型号

从事件查看器上下文菜单或网络文件轨迹中，您可以人工提交文件进行动态分析。除了可执行文件，您也可以提交不适合自动提交的文件类型，例如 PDF、 Microsoft Office 文件等。有关详细信息，请参阅第 2-4 页上的使用上下文菜单和第 40-32 页上的概要信息。

要在事故后分析多个文件，无论文件性质如何，您都可以通过捕获文件视图一次性手动提交最多 25 个文件 （特定类型）。这样允许您更快速地分析多种文件，并准确确定事故具体成因。有关详细信息，请参阅第 40-25 页上的使用捕获的文件和第 58-30 页上的选择工作流程页面上的行。

审查威胁评分和动态分析总结

许可证：恶意软件

受支持的设备：任何设备， 2 系列或 X -系列除外

受支持的防御中心：除 DC500 外的所有型号

在您提交文件进行动态分析后，思科云分析文件签名并返回威胁评分和动态分析总结。这些有助您更密切地分析潜在恶意软件威胁并微调检测策略。

威胁评分

文件分为四个威胁评分等级，与文件含有恶意内容的可能性一一对应：

表 40-1　　威胁评分等级

威胁指数	图标	评级
低		1-25
中		26-50
高		51-75
极高		76-100

防御中心本地缓存文件威胁评分时间与文件性质时间相同。如果系统在后期检测到这些文件，将向用户显示缓存威胁评分而非再次查询思科云。根据文件策略配置，您可以自动向威胁评分超过定义的恶意软件阈值威胁评分的文件分配恶意软件文件性质。有关详细信息，请参阅第 37-14 页上的创建文件策略。

动态分析总结

如有动态分析总结，您可以点击威胁评分图标进行查看。动态分析总结介绍构成漏洞研究团队 (VRT) 文件分析分配的威胁评分总分的各部分等级以及云尝试运行该文件时启动的其他进程。

如果存在多份报告，该总结应当基于与精确威胁评分匹配的最新报告。如果没有报告与精确威胁评分匹配，则系统会显示威胁评分最高的报告。如果存在多份报告，您可以选择一个威胁评分查看各份报告。

总结将列明构成威胁评分的各部分威胁。各部分威胁都可以展开以详列 VRT 结果以及与该部分威胁相关的进程。

进程树显示云尝试运行该文件时启动的进程。这有助于识别是否有包含恶意软件的文件意外尝试访问进程和系统资源（例如，运行 Word 文档打开 Microsoft Word，接着启动 Explorer，然后启动 Java）。

列出的每个进程都包含一个进程标识符和 md5 校验和，以便您检验实际进程。进程树将以子节点显示因父进程而启动的进程。

从动态分析总结中，您可以点击 **View Full Report** 查看 VRT 分析报告，其中详细展示了 VRT 的完整分析，包括常规文件信息、对检测的所有进程的更深入了解、一份文件分析明细以及其他相关信息。

使用文件事件

许可证：保护

系统将按照当前适用文件策略记录当受管设备在网络流量中检测或阻止文件时生成的文件事件。请注意，无论调用访问控制规则采用何种日志记录配置，系统生成文件事件时，都会将相关连接的终止记录到防御中心数据库中。有关详细信息，请参阅第 37-8 页上的了解和创建文件策略。

注　FireSIGHT 系统在网络流量中检测到并确认为恶意软件的文件将生成一个文件事件和一个恶意软件事件。这是由于要在文件中检测恶意软件，系统必须首先检测文件本身。基于终端的恶意软件事件并不具备对应文件事件。有关详细信息，请参阅第 40-14 页上的使用恶意软件事件和第 40-25 页上的使用捕获的文件。

您可以使用防御中心事件查看器查看、搜索和删除文件事件。此外，文件控制面板还使用图表快速展示与网络上检测到的文件（包括恶意软件文件）相关的详细信息。网络文件轨迹可更加深入地展现单个文件，提供该文件相关摘要信息以及文件在一段时间内穿过网络的方式。使用文件识别数据，您可以触发关联规则并创建报告，报告将采用预定义文件报告模板或自定义报告模板。

有关详情，请参阅：

- 第 40-7 页上的查看文件事件
- 第 40-8 页上的了解文件事件表
- 第 58-17 页上的使用地理定位
- 第 40-11 页上的搜索文件事件

查看文件事件

许可证：保护

FireSIGHT 系统事件查看器使您可以在表中查看文件事件，并根据您的分析相关信息操作事件视图。请注意，可用于任何个别文件事件的信息取决于多种因素，包括许可证。有关详细信息，请参阅第 65-2 页上的许可证类型和限制。

在访问文件事件时看到的页面因工作流程有所不同。工作流程只是一系列页面，您可以从广泛视图移动至更加突出重点的视图，使用这些页面评估事件。系统配备以下预定义文件事件工作流程：

- *文件摘要*默认快速提供不同文件事件类别和类型明细以及相关恶意软件文件性质。
- *接收文件的主机*和*发送文件的主机*提供已经接收或发送文件的主机列表，该列表已按照这些文件的相关恶意软件性质进行分组。

注 只有系统已经完成恶意软件云查找的文件才会显示文件性质。有关信息，请参阅第 37-10 页上的文件规则操作和评估顺序。

您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关指定不同默认工作流程（包括自定义工作流程）的信息，请参阅第 71-3 页上的配置事件查看设置。

FireSIGHT 系统支持在所有网络界面区域显示和输入使用 Unicode (UTF-8) 字符的文件名，这些区域包括事件查看器、事件搜索、控制面板、情景管理器等等。但是请注意，您以 PDF 格式生成的报告不支持 Unicode；Unicode 文件名将在 PDF 报告中以转译形式显示。有关详细信息，请参阅第 57-24 页上的生成并查看报告。另请注意，SMB 协议会将 Unicode 文件名转换为可打印字符；您在 SMB 上检测到的使用 Unicode 文件名的文件在显示时会用句点 (.) 代替任何不可打印的字符。

使用事件查看器，您可以：

- 搜索、分类和限制事件，以及变更已显示事件的时间范围
- 指定显示的列（仅适用于表视图）
- 查看 IP 地址相关主机配置文件，或者与用户标识相关的用户详细信息和主机历史
- 查看检测到具体文件的连接
- 查看同一工作流程内使用不同工作流程页面的事件
- 集中查看使用不同工作流程的事件
- 展开工作流程内应用具体值限制的各个页面
- 给当前页加书签并进行限制，以便您在此后返回至相同数据（假设该数据仍然存在）
- 查看文件相关可路由 IP 地址的发送和接收国家/地区及洲

- 查看文件轨迹
- 向文件列表增加文件、下载文件、提交文件进行动态分析，或查看文件 SHA-256 值完整文本
- 查看文件动态分析总结报告 （如有）
- 查看存档文件中嵌套的文件
- 使用当前限制创建报告模板
- 从数据库中删除事件
- 使用 IP 地址上下文菜单定制白名单、黑名单或者获取文件事件相关主机或 IP 地址的其他可用信息

有关使用事件查看器的详细信息，包括创建自定义工作流程，请参阅第 58-1 页上的了解和使用工作流程。

要快速查看检测到具体文件的连接，使用事件查看器内复选框选择文件，然后从 **Jump to** 下拉列表中选择 **Connections Events**。有关详细信息，请参阅第 58-31 页上的在工作流程之间导航。

要查看文件事件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Files > File Events**。

系统将显示默认文件事件工作流程首页。有关所显示的列的信息，请参阅第 40-8 页上的了解文件事件表。

了解文件事件表

许可证：保护

防御中心将按照适用文件策略设置，在受管设备检测或阻止受监控网络流量内正在传送的文件时，记录文件事件。

文件事件表视图是预定义文件事件工作流程中的最终页面，您可以在自定义工作流程中该视图，视图中包括文件表内各字段的列。文件事件表视图内一些字段默认为禁用。要在会话期间启用一个字段，请点击展开箭头 ( ) 展开搜索限制，然后点击 **Disabled Columns** 下的列名。

请记住，可用于任何个别文件事件的信息取决于多种因素，包括许可证。例如，尽管您可以仅使用一个保护许可证执行文件控制，您也可以通过一个恶意软件许可证对特定文件类型执行高级恶意软件防护并跟踪网络中传送的文件。

下表介绍文件事件字段。

表 40-2　文件事件字段

字段	说明
时间	事件生成的日期和时间。
操作	检测文件的文件策略规则相关操作以及相关文件操作选项。
Sending IP	发送检测文件的主机 IP 地址。
Sending Country	发送检测文件的主机所在国家/地区。 请注意， DC500 防御中心不支持此功能。

表 40-2　　文件事件字段 （续）

字段	说明
Receiving IP	接收检测文件的主机 IP 地址。
Receiving Country	接收检测文件的主机所在国家/地区。 请注意， DC500 防御中心不支持此功能。
Sending Port	检测到文件的流量所用源端口。
Receiving Port	检测到文件的流量所用目标端口。
SSL Status	SSL 规则相关操作、默认操作或记录加密连接的不可解密流量操作： • `Block` 和 `Block with reset` 代表被阻止的加密连接。 • `Decrypt (Resign)` 代表使用重签服务器证书解密的传出连接。 • `Decrypt (Replace Key)` 代表使用带替代公共密钥的自签服务器证书解密的传出连接。 • `Decrypt (Known Key)` 代表使用已知私有密钥解密的传入连接。 • `Default Action` 表示连接采用默认操作处理。 • `Do not Decrypt` 代表系统未解密的连接。 如果系统无法解密已加密的连接，则它会显示所采取的无法解密流量操作和失败原因。例如，如果系统检测到使用未知密码套件加密的流量并且未做进一步检查就允许了该流量，则此字段将显示 `Do Not Decrypt (Unknown Cipher Suite)`。 点击锁图标 ( ) 可查看证书详细信息。有关详细信息，请参阅第 39-27 页上的查看与加密连接相关的证书。
用户	登录至文件所在主机 (**Receiving IP**) 的用户。 请注意，由于用户与目标主机关联，因此用户与其上传文件的文件事件不关联。
文件名	文件名称。
布置	可以为下列文件性质之一： • `Malware` 表示云将文件归类为恶意软件，或文件威胁评分超过文件策略定义的恶意软件阈值。 • `Clean` 表示云将文件归类为安全，或用户将文件添加到安全列表。 • `Unknown` 表示在云分配性质之前发生恶意软件云查找。文件未分类。 • `Custom Detection` 表示用户将文件添加到自定义检测列表。 • `Unavailable` 表示防御中心无法执行恶意软件云查找。您可能看到有一小部分事件具有此性质，这是预期行为。 • `N/A` 表示 Detect Files 或 Block Files 规则处理了文件，防御中心不执行恶意软件云查找。

表 40-2　　文件事件字段 （续）

字段	说明
SHA256	如果因以下原因检测到文件，则文件 SHA-256 哈希值以及网络文件轨迹图标代表最近检测到的文件事件和文件性质： • 启用了 **Store Files** 的 Detect Files 文件规则 • 启用了 **Store Files** 的 Block Files 文件规则 • Malware Cloud Lookup 文件规则 • Block Malware 文件规则 要查看网络文件轨迹，请点击轨迹图标。有关详细信息，请参阅第 40-32 页上的分析网络文件轨迹。
威胁指数	与此文件相关的最新威胁评分： • Low ( ) • Medium ( ) • High ( ) • Very High ( ) 要查看动态分析总结报告，请点击威胁评分图标。
类型	文件类型，例如 HTML 或 MSEXE。
类别	一般类别文件类型，例如：Office Documents、 Archive、 Multimedia、 Executables、 PDF files、 Encoded、 Graphics 或 System Files。
Size (KB)	文件大小 （千字节）。请注意，如果系统在完全接收文件前确定一个文件的文件类型，则可能不会计算文件大小，该字段为空。
URI	文件原始 URI，例如用户下载文件的 URL。
Archive Name	文件相关存档文件 （如有）名，例如 archive.zip。要查看存档文件内容，请右键单击该存档文件的事件查看器行，打开上下文菜单，然后点击 **View Archive Contents**。有关详细信息，请参阅第 37-19 页上的查看存档文件的内容。
Archive SHA256	文件相关存档文件 （如有） SHA-256 哈希值。
Archive Depth	文件嵌入存档文件的层级 （如有），例如 1 或 3。
Application Protocol	受管设备检测到文件的流量所用应用协议。
Application Protocol、 Client 或 Web Application Category 或 Tag	展示了应用特征的标准，帮助您了解应用的功能；请参阅第 45-9 页上的表 45-2。
客户端	连接中传送文件所用的客户端应用。
Web 应用程序	对于使用 HTTP 传送的文件，是指在连接中检测到并用于传送文件的网络应用（内容或请求的 URL）。
Application Risk	连接中检测到的应用流量相关风险：Very High、 High、 Medium、 Low 或 Very Low。连接中检测的各类应用都有一个相关风险；该字段显示最高风险。有关详细信息，请参阅第 45-9 页上的表 45-2。
业务相关性	连接中检测到的应用流量的业务相关性：Very High、 High、 Medium、 Low 或 Very Low。连接中检测的各类应用都有相关业务相关性；该字段显示级别最低的业务相关性。有关详细信息，请参阅第 45-9 页上的表 45-2。
通信	对于恶意软件性质已经变更的文件，即对于追溯恶意软件事件相关的文件，该字段显示性质变更时间和方式相关信息。

表 40-2　　文件事件字段 （续）

字段	说明
File Policy	检测文件的文件策略。
设备	检测文件的设备名称。
安全情景	识别流量通过的虚拟防火墙组的元数据。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
计数	与各行信息匹配的事件数量。当您应用了将创建两个或两个以上相同行的限制后将显示该字段。

搜索文件事件

许可证：保护

使用防御中心搜索页面，您可以搜索具体文件事件，在事件查看器中显示结果，并保存搜索条件以便后期重新使用。自定义分析控制面板构件、报告模版和自定义用户角色也可以使用保存的搜索条件。

请注意，搜索结果依赖于所搜索事件的可用数据。换言之，根据可用数据，搜索限制条件可能不适用。例如， **Disposition** 和 **SHA256** 字段仅针对防御中心执行恶意软件云查找的文件填充。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 在任一字段指定 `n/a` 以便识别信息不适用于该字段的事件；使用 `!n/a` 识别字段填充事件。
- 使用设备字段搜索特定设备以及组、堆栈或集群中的设备。有关 FireSIGHT 系统如何处理搜索中的设备字段的详细信息，请参阅第 60-6 页上的在搜索中指定设备。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

文件事件专用搜索语法

为补充上文所列通用搜索语法，以下列表介绍文件事件的一些专用搜索语法。

Sending/Receiving Continent

系统返回所有 **Sending Continent** 或 **Receiving Continent** 符合所指定洲的事件。

Sending/Receiving Country

系统返回 **Sending Country** 或 **Receiving Country** 符合您指定的国家/地区的所有事件。

Sending/Receiving IP

系统返回 **Sending IP** 或 **Receiving IP** 符合您指定 IP 地址的所有事件。

URI 或 Message

系统执行部分匹配，即您可以搜索全部或部分字段内容而无需使用星号。

File Storage

键入以下一项或多项：

- `Stored` 返回目前存储关联文件的所有事件。
- `Stored in connection` 返回系统捕获并存储关联文件的所有事件，无论目前是否已存储关联文件。
- `Failed` 返回系统未能存储关联文件的所有事件。

采取的 SSL 实际操作

键入以下任何关键字，查看系统将指定操作应用到的加密流量的文件事件：

- `Do not Decrypt` 代表系统未解密的连接。
- `Block` 和 `Block with reset` 代表被阻止的加密连接。
- `Decrypt (Known Key)` 代表使用已知私有密钥解密的传入连接。
- `Decrypt (Replace Key)` 代表使用带替代公共密钥的自签服务器证书解密的传出连接。
- `Decrypt (Resign)` 代表使用重签服务器证书解密的传出连接。

此列在文件事件表视图中不显示。

SSL 失败的原因

键入以下任何关键字，查看系统由于指定原因无法解密的加密流量的文件事件：

- `Unknown`
- `No Match`
- `Success`
- `Uncached Session`
- `Unknown Cipher Suite`
- `Unsupported Cipher Suite`
- `Unsupported SSL Version`
- `SSL Compression Used`
- `Session Undecryptable in Passive Mode`
- `Handshake Error`
- `Decryption Error`
- `Pending Server Name Category Lookup`
- `Pending Common Name Category Lookup`
- `Internal Error`
- `Network Parameters Unavailable`

- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

此列在文件事件表视图中不显示。

SSL 主体国家/地区

键入一个双字符 ISO 3166-1 二位字母国家/地区代码，查看与证书主体的国家/地区关联的加密流量的文件事件。

此列在文件事件表视图中不显示。

SSL 颁发者国家/地区

键入一个双字符 ISO 3166-1 二位字母国家/地区代码，查看与证书颁发者的国家/地区关联的加密流量的文件事件。

此列在文件事件表视图中不显示。

SSL Certificate Fingerprint

键入或粘贴用于验证证书的 SHA 哈希值，查看与该证书关联的流量的文件事件。

此列在文件事件表视图中不显示。

SSL 公共密钥指纹

键入或粘贴用于验证证书内包含的公共密钥的 SHA 哈希值，查看与该证书关联的流量的文件事件。

此列在文件事件表视图中不显示。

要搜索文件事件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **File Events**。

页面根据相应限制进行更新。

步骤 3　如以下各节所述，在相应字段中输入搜索条件：

- 有关文件事件表字段的信息，请参阅文件事件字段表。

- 有关文件事件的专用搜索语法，请参阅第 40-11 页上的文件事件专用搜索语法。
- 有关与公共密钥证书相关的字段，请参阅第 39-27 页上的查看与加密连接相关的证书。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save as New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果出现在默认文件事件工作流程内并受当前时间范围限制。

使用恶意软件事件

许可证：恶意软件或任意

受支持的设备：因功能而异

受支持的防御中心：因功能而异

在以下情况中系统将恶意软件事件记录在防御中心数据库内：

- 受管设备在网络流量中检测文件，并通过恶意软件云查找确认其为恶意软件
- 受管设备在网络流量中检测到自定义检测列表内的文件
- 系统发现文件的恶意软件性质已经变更，这些称为追溯性恶意软件事件
- 安装在您所在组织终端的 FireAMP 连接器检测到威胁并告知思科云

由于 FireAMP 恶意软件检测是在下载或执行时在终端执行，而受管设备在网络流量中检测文件，因此这些恶意软件事件中的信息有所不同。追溯性恶意软件事件所含数据与其他基于网络的恶意软件事件或基于终端的恶意软件事件也略有不同。

以下各节简要介绍不同类别恶意软件事件。有关整体恶意软件检测流程的信息，请参阅第 37-2 页上的了解恶意软件防护和文件控制。

基于终端 (FireAMP) 的恶意软件事件

如果您所在组织已有 FireAMP 订用，个人用户可以在其计算机和移动设备上安装 FireAMP 连接器。这些轻量级代理与思科云通信，云则与您的防御中心通信；请参阅第 37-21 页上的为 FireAMP 处理云连接。云可以发送威胁通知以及其他各类信息，包括扫描、隔离、阻止处置和云召回相关数据。防御中心将该信息作为恶意软件事件记录在其数据库上。

注 基于终端的恶意软件事件所报告的 IP 地址可能不在网络映射上 - 甚至可能完全不在监控的网络上。根据部署、合规水平以及其他因素，您所在组织内安装 FireAMP 连接器的终端可能与受管设备监控的主机不同。

基于网络流量的恶意软件事件

受支持的设备：任何设备， 2 系列或 X -系列除外

受支持的防御中心：除 DC500 外的所有型号

作为整体访问控制配置的一部分，受管设备可以通过恶意软件许可证在网络流量内检测到恶意软件；有关信息，请参阅第 37-8 页上的了解和创建文件策略。

以下情形可产生恶意软件事件：

- 如果受管设备检测一组具体文件类型之一，防御中心执行恶意软件云查找，向防御中心返回 `Malware`、 `Clean` 或 `Unknown` 文件性质。
- 如果防御中心不能与云建立连接，或者云因其他原因不可用，文件性质为 `Unavailable`。您可能看到有一小部分事件具有此性质，这是预期行为。
- 如果文件相关威胁评分超过检测该文件的文件策略定义的恶意软件威胁评分阈值，防御中心向该文件分配 `Malware` 文件性质。
- 如果受管设备检测到 SHA-256 值存储在自定义检测列表上的文件，防御中心向该文件分配 `Custom Detection` 文件性质。
- 如果受管设备检测到安全列表内文件，防御中心向该文件分配 `Clean` 文件性质。

防御中心将文件检测和性质记录以及其他上下文数据作为恶意软件事件进行记录。

注 FireSIGHT 系统在网络流量中检测到并确认为恶意软件的文件将生成一个文件事件和一个恶意软件事件。这是由于要在文件中检测恶意软件，系统必须首先检测文件本身。有关详细信息，请参阅第 40-6 页上的使用文件事件和第 40-25 页上的使用捕获的文件。

追溯性恶意软件事件

受支持的设备：3 系列、虚拟设备

受支持的防御中心：除 DC500 外的所有型号

对于在网络流量内检测到的恶意软件文件，文件性质可以变更。例如，思科云可以确定此前认定安全的文件现在是否识别为恶意软件，或者相反 - 识别为恶意软件的文件实际上属于安全文件。

如果您在上一周执行恶意软件查询的文件性质发生变更，云将向防御中心发出通知。然后将发生两件事情：

- 防御中心产生新追溯性恶意软件事件。

  新追溯性恶意软件事件代表上一周检测到的具备相同 SHA-256 哈希值的所有文件的性质发生变更。因此，这些事件包含限定信息：防御中心接到性质变更通知的日期和时间、新性质、文件 SHA-256 哈希值以及威胁名称。它们不包含 IP 地址或其他上下文信息。

- 防御中心变更此前检测到的具有追溯事件相关 SHA-256 哈希值的文件的文件性质。

  如果文件性质变更为 Malware，防御中心在其数据库内记录新恶意软件事件。除了新性质，新恶意软件事件信息与最初检测到文件时生成的文件事件中的信息都相同。

  如果文件性质变更为 Clean，防御中心不会从恶意软件表中删除该恶意软件事件。相反，该事件仅简单反应性质变更情况。这表示文件性质为安全的文件能够出现在恶意软件表中，前提是它们最初被视为恶意软件。从未识别为恶意软件的文件只会出现在文件表中。

在任一种情况下，恶意软件事件**消息**都会显示性质变更方式和时间，例如：

```
Retrospective Event, Mon Oct 1 20:44:00 2012 (UTC), Old Disp: Unknown, New Disp:
Malware
```

使用恶意软件事件

您可以使用防御中心事件查看器查看、搜索和删除恶意软件事件。此外，文件控制面板和 Context Explorer 还使用图表提供在网络上检测到的文件（包括恶意软件文件）相关详细信息大致概览。网络文件轨迹可更加深入地展现单个恶意软件文件，提供该文件相关信息摘要以及文件在一段时间内穿过网络的方式。使用恶意软件检测数据，您可以触发关联规则并创建报告，报告将采用预定义恶意软件报告模板或自定义报告模板。

有关详情，请参阅：

- 第 40-16 页上的查看恶意软件事件
- 第 40-17 页上的了解恶意软件事件表
- 第 40-22 页上的搜索恶意软件事件

查看恶意软件事件

许可证：恶意软件或任意

FireSIGHT 系统事件查看器使您可以在表中查看恶意软件事件，并根据分析相关信息使用事件视图。请注意，可用于任何个别恶意软件事件的信息取决于多种因素，包括许可证。有关详细信息，请参阅第 65-2 页上的许可证类型和限制。

在访问恶意软件事件时看到的页面因工作流程有所不同。工作流程只是一系列页面，您可以从广泛视图移至更加突出重点的视图，使用这些页面评估事件。系统配备以下预定义恶意软件事件工作流程：

- *恶意软件摘要*默认提供检测恶意软件列表并根据各项威胁分组。
- *恶意软件事件摘要*提供不同恶意软件事件类型和子类明细。
- *接收文件的主机*和*发送文件的主机*提供已经接收或发送文件的主机列表，该列表已按照这些文件的相关恶意软件性质进行分组。请注意，只有检测到的作为 Malware Cloud Lookup 或 Block Malware 文件规则结果的文件才会显示文件性质。
- *引入恶意软件的应用程序*提供访问或执行您所在组织终端检测到的恶意软件的客户端应用列表。您可以从该列表中深入探究每个父客户端访问的单独恶意软件文件。

您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关指定不同默认工作流程（包括自定义工作流程）的信息，请参阅第 71-3 页上的配置事件查看设置。

FireSIGHT 系统支持在所有网络界面区域显示和输入使用 Unicode (UTF-8) 字符的文件名，这些区域包括事件查看器、事件搜索、控制面板、 Context Explorer 等等。但是请注意，您以 PDF 格式生成的报告不支持 Unicode；Unicode 文件名将在 PDF 报告中以转译形式显示。有关详细信息，请参阅第 57-24 页上的生成并查看报告。

使用事件查看器，您可以：

- 搜索、分类和限制事件，以及变更已显示事件的时间范围
- 指定显示的列（仅适用于表视图）
- 查看 IP 地址相关主机配置文件，或者与用户标识相关的用户详细信息和主机历史
- 查看检测到具体恶意软件的连接（仅适用于基于网络的恶意软件事件）
- 查看同一工作流程内使用不同工作流程页面的事件

- 集中查看使用不同工作流程的事件
- 展开工作流程内应用具体值限制的各个页面
- 给当前页加书签并进行限制，以便您在此后返回至相同数据 （假设该数据仍然存在）
- 查看文件相关可路由定位 IP 地址的地理定位信息
- 查看文件轨迹
- 查看存档文件中嵌套的文件
- 使用当前限制创建报告模板
- 从数据库中删除事件
- 向文件列表增加文件、下载文件、提交文件进行动态分析，或查看文件 SHA-256 值完整文本
- 查看文件动态分析总结报告 （如有）
- 使用 IP 地址上下文菜单定制白名单、黑名单或者获取恶意软件事件相关主机或 IP 地址的其他可用信息

请注意， 2 系列设备、用于 Blue Coat X-系列的思科 NGIPS和 DC500 防御中心均不支持基于网络的恶意软件防护或存档文件检查，这可能影响显示的数据。例如，仅管理 2 系列设备的 3 系列防御中心只能显示基于终端的恶意软件事件。

有关使用事件查看器的详细信息，包括创建自定义工作流程，请参阅第 58-1 页上的了解和使用工作流程。

要查看恶意软件事件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Files > Malware Events**。

系统将显示默认恶意软件事件工作流程首页。有关所显示的列的信息，请参阅第 40-17 页上的了解恶意软件事件表。

了解恶意软件事件表

许可证：恶意软件或任意

受支持的设备：因功能而异

受支持的防御中心：因功能而异

当安装在您所在组织终端上的 FireAMP 连接器检测到威胁或受管设备在网络流量内检测到文件并通过恶意软件云查找识别为恶意软件时，系统将在防御中心数据库内记录恶意软件事件。系统在发现文件恶意软件性质变更时也会记录追溯性恶意软件事件。请注意， 2 系列 设备、用于 Blue Coat X-系列的思科 NGIPS和 DC500 防御中心均不支持基于网络的恶意软件防护，这可能影响显示的数据。例如，仅管理 2 系列设备的 3 系列防御中心只能显示基于终端的恶意软件事件。有关详细信息，请参阅第 37-2 页上的了解恶意软件防护和文件控制和第 40-14 页上的使用恶意软件事件。

恶意事件表视图是预定义恶意软件事件工作流程最终页面，您可以在自定义工作流程中添加该页面，包括文件表内各字段列。恶意软件事件表视图内一些字段默认为禁用。要在会话期间启用一个字段，请点击展开箭头 ( ) 展开搜索限制，然后点击 **Disabled Columns** 下的列名。

请记住，并非所有事件都会填充每个字段，不同类型恶意软件事件可以包括不同信息。例如，由于 FireAMP 恶意软件检测在终端在下载或执行时完成，所以基于终端的恶意软件事件包含文件路径、调用客户端应用等相关信息。相比之下，由于受管设备在网络流量中检测恶意软件文件，其相关恶意软件事件包含端口、应用协议和传送文件所用连接相关原始 IP 地址信息。

下表列出各恶意软件事件字段并根据恶意软件事件类型指示系统是否在该字段中显示信息。请注意， DC500 防御中心并不支持接收或发送洲或国家/地区的地理定位信息。

表 40-3　　恶意软件事件字段

字段	说明	网络	终端	云 追溯性
时间	事件生成的日期和时间。	是	是	是
操作	与匹配文件规则的规则操作相关的文件规则操作以及相关文件规则操作选项。	是	否	是
Sending IP	发送被检测恶意软件的主机的 IP 地址。	是	否	否
Sending Continent	发送被检测恶意软件的主机所在洲。	是	否	是
Sending Country	发送被检测恶意软件的主机所在国家/地区。	是	否	否
Receiving IP	对于基于网络的恶意软件事件，显示接收被检测恶意软件的主机的 IP 地址。 对于基于终端的恶意软件事件，显示安装 FireAMP 连接器终端的 IP 地址以及发生恶意软件事件的位置。	是	是	否
Receiving Continent	接收检测到的恶意软件的主机所在洲。	是	否	是
Receiving Country	接收检测到的恶意软件的主机所在国家/地区。	是	否	否
Sending Port	受管设备检测到恶意软件的流量所用源端口。	是	否	否
Receiving Port	受管设备检测到恶意软件的流量所用目标端口。	是	否	否
SSL Status	SSL 规则相关操作、默认操作或记录加密连接的不可解密流量操作： • `Block` 和 `Block with reset` 代表被阻止的加密连接。 • `Decrypt (Resign)` 代表使用重签服务器证书解密的传出连接。 • `Decrypt (Replace Key)` 代表使用带替代公共密钥的自签服务器证书解密的传出连接。 • `Decrypt (Known Key)` 代表使用已知私有密钥解密的传入连接。 • `Do not Decrypt` 代表系统未解密的连接。 如果系统无法解密已加密的连接，则它会显示所采取的无法解密流量操作和失败原因。例如，如果系统检测到使用未知密码套件加密的流量并且未做进一步检查就允许了该流量，则此字段将显示 `Do Not Decrypt (Unknown Cipher Suite)`。 点击锁图标 ( ) 可查看证书详细信息。有关详细信息，请参阅第 39-27 页上的查看与加密连接相关的证书。	是	否	否

表 40-3　　恶意软件事件字段 （续）

字段	说明	网络	终端	云 追溯性
用户	发生恶意软件事件主机 （**Receiving IP**）的用户。 对于基于网络的恶意软件事件，通过网络发现确定该用户。由于用户与目标主机关联，因此用户与其上传恶意软件文件的恶意软件事件无关联。 对于基于终端的恶意软件事件， FireAMP 连接器确定用户名。 FireAMP 用户**不受**用户发现或控制束缚。他们不会出现在用户表中，您也无法查看这些用户详细信息。	是	是	否
事件类型	恶意软件事件类型。要获得事件类型完整清单，请参阅第 40-21 页上的恶意软件事件类型。	是	是	是
Event Subtype	导致恶意软件检测的 FireAMP 操作，例如， `Create`、`Execute`、 `Move` 或 `Scan`。	否	是	否
Threat Name	被测恶意软件名称。	是	是	是
文件名	恶意软件文件名。	是	是	否
File Disposition	可以为下列文件性质之一： • `Malware` 表示云将文件归类为恶意软件，或文件威胁评分超过文件策略定义的恶意软件阈值。 • `Clean` 表示云将文件归类为安全，或用户将文件添加到安全列表。 • `Unknown` 表示在云分配性质之前发生恶意软件云查找。文件未分类。 • `Custom Detection` 表示用户将文件添加到自定义检测列表。 • `Unavailable` 表示防御中心无法执行恶意软件云查找。您可能看到有一小部分事件具有此性质，这是预期行为。 请注意，安全文件仅在变更为安全文件后才会出现在恶意软件表中；有关信息，请参阅第 40-15 页上的追溯性恶意软件事件。	是	否	是
File SHA256	文件的 SHA-256 哈希值以及显示最近检测文件事件和文件性质的网络文件轨迹图标。 要查看网络文件轨迹，请点击轨迹图标。有关详细信息，请参阅第 40-32 页上的分析网络文件轨迹。	是	是	是
威胁指数	与此文件相关的最新威胁评分： • `Low` ( ) • `Medium` ( ) • `High` ( ) • `Very High` ( ) 要查看动态分析总结报告，请点击威胁评分图标。	是	否	否
File Path	恶意软件文件的文件路径，不包括文件名。	否	是	否
文件类型	恶意软件文件的文件类型，例如 `HTML` 或 `MSEXE`。	是	是	否

表 40-3　恶意软件事件字段 （续）

字段	说明	网络	终端	云追溯性
File Type Category	一般类别文件类型，例如：Office Documents、 Archive、 Multimedia、 Executables、 PDF files、 Encoded、 Graphics 或 System Files。	是	是	否
File Timestamp	创建恶意软件文件的时间和日期。	否	是	否
File Size (KB)	恶意软件文件大小 （千字节）。	是	是	否
File URI	恶意软件文件原始 URI，例如用户下载文件的 URL。	是	否	否
Archive Name	恶意软件文件相关的存档文件 （如有）名，例如 archive.zip。	是	是	否
Archive SHA256	恶意软件文件相关的存档文件 （如有）的 SHA-256 哈希值。要查看存档文件的内容，请右键单击该存档文件的事件查看器行，打开上下文菜单，然后点击 **View Archive Contents**。有关详细信息，请参阅第 37-19 页上的查看存档文件的内容。	是	是	否
Archive Depth	文件嵌入存档文件的层级 （如有），例如 1 或 3。	是	是	否
Application File Name	检测期间访问恶意软件文件的客户端应用。这些应用与网络发现或应用控制无关联。	否	是	否
Application File SHA256	检测期间访问 FireAMP 检测或隔离文件的上级文件的 SHA-256 哈希值。	否	是	否
Application Protocol	受管设备检测到恶意软件文件的流量所用应用协议。	是	否	否
Application Protocol、Client 或 Web Application Category 或 Tag	展示了应用特征的标准，帮助您了解应用的功能；请参阅第 45-9 页上的表 45-2。	是	否	是
客户端	在主机上运行并依靠服务器发送文件的客户端应用。	是	否	是
Web 应用程序	代表连接内被检测 HTTP 流量内容或所请求 URL 的应用。	是	否	是
IOC	对于连接涉及的主机，恶意软件事件是否触发危险表现 (IOC)。当基于终端的恶意软件检测触发 IOC 规则时，将生成 FireAMP IOC 类型的完整恶意软件事件。有关 IOC 的详细信息，请参阅第 45-17 页上的了解危害表现。	是	是	是
Application Risk	连接中检测到的应用流量相关风险：Very High、 High、 Medium、 Low 或 Very Low。连接中检测的各类应用都有一个相关风险；该字段显示最高风险。有关详细信息，请参阅第 45-9 页上的表 45-2。	是	否	是
业务相关性	连接中检测到的应用流量的业务相关性：Very High、 High、 Medium、 Low 或 Very Low。连接中检测的各类应用都有相关业务相关性；该字段显示级别最低的业务相关性。有关详细信息，请参阅第 45-9 页上的表 45-2。	是	否	是
检测器	识别恶意软件的 FireAMP 检测器，例如 ClamAV、 Spero 或 SHA。	否	是	否

表 40-3　　恶意软件事件字段 （续）

字段	说明	网络	终端	云 追溯性
通信	恶意软件事件相关的任何其他信息。 对于基于网络的恶意软件事件，该字段仅在文件性质发生变更的文件中填充；有关信息，请参阅第 40-15 页上的追溯性恶意软件事件。	是	是	否
FireAMP Cloud	产生事件的 FireAMP 云名称。	否	是	否
设备	对于基于网络的恶意软件事件，显示检测到恶意软件文件的设备名称。 对于基于终端的恶意软件事件和云生成的追溯性恶意软件事件，显示防御中心名称。	是	是	是
安全情景	识别流量通过的虚拟防火墙组的元数据。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。	是	是	是
计数	与各行信息匹配的事件数量。当您应用了将创建两个或两个以上相同行的限制后将显示该字段。	不适用	不适用	不适用

恶意软件事件类型

许可证：恶意软件或任意

受支持的设备：因功能而异

受支持的防御中心：因功能而异

对于基于网络的恶意软件事件，事件类型可以是：

- 网络文件传送中检出威胁
- 网络文件传送 （回溯）中检出威胁

基于终端的恶意软件事件可能具有任何以下类型：

- 执行受阻
- 云召回隔离
- 云召回隔离尝试失败
- 开始云召回隔离
- 从隔离中恢复云召回
- 从隔离中恢复云召回失败
- 从隔离中恢复云召回启动
- FireAMP IOC
- 隔离失败
- 恢复隔离项目
- 恢复隔离失败
- 开始恢复隔离
- 扫描完成，未检出
- 扫描完成，检出
- 扫描失败

- 开始扫描
- Threat Detected
- 排除部分检出威胁
- 隔离威胁

如果文件轨迹映射包含恶意软件事件，这些事件是以下类型之一：网络文件传送检出威胁、网络文件传输 （回溯）检出威胁、检出威胁、排除部分检出威胁和隔离威胁。有关详情，请参见第 40-30 页上的使用网络文件轨迹。

请注意，2 系列 设备、用于 Blue Coat X-系列的思科 NGIPS和 DC500 防御中心均不支持基于网络的恶意软件防护，这可能影响显示的数据。例如，仅管理 2 系列设备的 3 系列防御中心只能显示基于终端的恶意软件事件。

搜索恶意软件事件

许可证：恶意软件或任意

使用防御中心搜索页面，您可以搜索具体恶意软件事件，在事件查看器中显示结果，并保存搜索条件以便后期重新使用。自定义分析控制面板构件、报告模版和自定义用户角色也可以使用保存的搜索条件。

下文以已保存搜索列表中用（思科）标记的系统配套搜索条件作为示例。

请注意，搜索结果依赖于所搜索事件的可用数据。换言之，根据可用数据，搜索限制条件可能不适用。例如，受管设备检查网络流量并不会生成基于终端的恶意软件事件，因此，这些事件不包含连接信息 （端口、应用协议等等）。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 在任一字段指定 `n/a` 以便识别信息不适用于该字段的事件；使用 `!n/a` 识别字段填充事件。
- 使用设备字段搜索特定设备以及组、堆栈或集群中的设备。有关 FireSIGHT 系统如何处理搜索中的设备字段的详细信息，请参阅第 60-6 页上的在搜索中指定设备。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

恶意软件事件的专用搜索语法

为补充上文所列通用搜索语法，以下列表介绍恶意软件事件的一些专用搜索语法。

Sending/Receiving IP

系统返回 **Sending IP** 或 **Receiving IP** 符合您指定 IP 地址的所有事件。

事件类型

当使用特定恶意软件事件类型 （参阅第 40-21 页上的恶意软件事件类型）搜索事件时，请用引号将事件类型引起，例如：`"Scan Completed With Detection"`。否则，系统执行部分匹配。即是，如果使用相同字符串但不使用引号进行搜索，系统返回以下几种类型事件：

- 扫描完成，未检出
- 扫描完成，检出

Initiator/Responder Continent

系统返回 **Initiator Continent** 或 **Responder Continent** 符合所指定洲的所有事件。

Initiator/Responder Country

系统返回 **Initiator Country** 或 **Responder Country** 符合所指定国家/地区的所有事件。

URI 或 Message

系统执行部分匹配，即您可以搜索全部或部分字段内容而无需使用星号。

采取的 SSL 实际操作

键入以下任何关键字，查看系统将指定操作应用到的加密流量的恶意软件事件：

- `Do not Decrypt` 代表系统未解密的连接。
- `Block` 和 `Block with reset` 代表被阻止的加密连接。
- `Decrypt (Known Key)` 代表使用已知私有密钥解密的传入连接。
- `Decrypt (Replace Key)` 代表使用带替代公共密钥的自签服务器证书解密的传出连接。
- `Decrypt (Resign)` 代表使用重签服务器证书解密的传出连接。

此列在恶意软件事件表视图中不显示。

SSL 失败的原因

键入以下任何关键字，查看系统由于指定原因无法解密的加密流量的恶意软件事件：

- `Unknown`
- `No Match`
- `Success`
- `Uncached Session`
- `Unknown Cipher Suite`
- `Unsupported Cipher Suite`
- `Unsupported SSL Version`
- `SSL Compression Used`
- `Session Undecryptable in Passive Mode`
- `Handshake Error`
- `Decryption Error`
- `Pending Server Name Category Lookup`
- `Pending Common Name Category Lookup`
- `Internal Error`

- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

此列在恶意软件事件表视图中不显示。

SSL 主体国家/地区

键入一个双字符 ISO 3166-1 二位字母国家/地区代码，查看与证书主体的国家/地区关联的加密流量的恶意软件事件。

此列在恶意软件事件表视图中不显示。

SSL 颁发者国家/地区

键入一个双字符 ISO 3166-1 二位字母国家/地区代码，查看与证书颁发者的国家/地区关联的加密流量。

此列在恶意软件事件表视图中不显示。

SSL Certificate Fingerprint

键入或粘贴用于对证书进行身份验证的 SHA 哈希值，查看与该证书关联的流量。

此列在恶意软件事件表视图中不显示。

SSL 公共密钥指纹

键入或粘贴用于对证书中包含的公用密钥进行身份验证的 SHA 哈希值，查看与该证书关联的流量。

此列在恶意软件事件表视图中不显示。

要搜索恶意软件事件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Malware Events**。

页面根据相应限制进行更新。

步骤 3　如以下各节所述，在相应字段中输入搜索条件：

- 有关恶意软件事件表字段的信息，请参阅恶意软件事件字段表。

- 有关恶意软件事件的专用搜索语法，请参阅第 40-23 页上的恶意软件事件的专用搜索语法。
- 有关与公共密钥证书相关的字段，请参阅第 39-27 页上的查看与加密连接相关的证书。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save as New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果出现在默认恶意软件事件工作流程内并受当前时间范围限制。

使用捕获的文件

许可证：恶意软件

受支持的设备：任何设备， 2 系列或 X -系列除外

受支持的防御中心：除 DC500 外的所有型号

当受管设备根据当前应用的文件策略规则捕获网络流量中检测到的文件时，系统记录日志。通过事件查看器可查看与捕获文件相关的信息，如与 SHA-256 值相关的最新文件名、文件性质和威胁评分、文件存储状态、存档检验状态以及是否手动提交文件用于动态分析。

注　因为捕获之前必须先检测到恶意软件，所以设备捕获包含恶意软件的文件后同时生成文件事件和恶意软件事件。有关详细信息，请参阅第 40-6 页上的使用文件事件和第 40-14 页上的使用恶意软件事件。

可以使用防御中心事件查看器查看和搜索捕获文件，以及提交捕获文件进行动态分析。此外，文件控制面板还使用图表快速展示与网络上检测到的文件 （包括恶意软件文件）相关的详细信息。

有关详情，请参阅：

- 第 40-26 页上的查看捕获的文件
- 第 40-27 页上的了解捕获的文件表
- 第 40-28 页上的搜索捕获文件

查看捕获的文件

许可证：恶意软件

FireSIGHT 系统事件查看器使您可以查看表中的文件事件，并根据分析相关信息使用事件视图。

在访问捕获的文件时看到的页面因工作流程有所不同。工作流程只是一系列页面，您可以使用这些页面从较宽泛的视图移动至更精细化的视图来评估事件。系统配备以下预定义捕获文件工作流程：

- *捕获文件概要*提供基于类型、类别和威胁评分的捕获文件明细 （默认工作流程）。
- *动态分析状态*依据捕获文件是否已提交用于动态分析提供此类文件计数。

您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关指定不同默认工作流程 （包括自定义工作流程）的信息，请参阅第 71-3 页上的配置事件查看设置。

FireSIGHT 系统支持在所有网络界面区域显示和输入使用 Unicode (UTF-8) 字符的文件名，这些区域包括事件查看器、事件搜索、控制面板、 Context Explorer 等等。但是请注意，您以 PDF 格式生成的报告不支持 Unicode；Unicode 文件名将在 PDF 报告中以转译形式显示。有关详细信息，请参阅第 57-24 页上的生成并查看报告。

使用事件查看器，您可以：

- 搜索、分类和限制事件，以及变更已显示事件的时间范围
- 指定显示的列 （仅适用于表视图）
- 查看同一工作流程内使用不同工作流程页面的事件
- 集中查看使用不同工作流程的事件
- 展开工作流程内应用具体值限制的各个页面
- 给当前页加书签并进行限制，以便您在此后返回至相同数据 （假设该数据仍然存在）
- 查看文件轨迹
- 查看存档文件内容及检查状态
- 向文件列表增加文件、下载文件、提交文件进行动态分析，或查看文件 SHA-256 值完整文本
- 查看文件动态分析总结报告 （如有）
- 一次最多提交 25 个文件用于动态分析
- 使用当前限制创建报告模板

请注意， 2 系列设备、用于 Blue Coat X-系列的思科 NGIPS和 DC500 防御中心均不支持基于网络的恶意软件防护或存档文件检查，这可能影响显示的数据。例如，仅管理 2 系列设备的 3 系列防御中心不能显示捕获的文件。

有关使用事件查看器的详细信息，包括创建自定义工作流程，请参阅第 58-1 页上的了解和使用工作流程。

要查看文件事件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Files > Captured Files**。

系统将显示默认文件事件工作流程首页。有关所显示的列的信息，请参阅第 40-27 页上的了解捕获的文件表。

了解捕获的文件表

许可证：恶意软件

当受管设备捕获正在受监控网络流量中传送的文件时，防御中心根据已应用文件策略设置记录日志。

捕获文件表视图是预定义捕获文件工作流程的最终页面，也可以添加到自定义工作流程中，且该视图为捕获文件表中的每个字段都准备了对应的列。捕获文件表视图中一些字段默认为禁用。要在会话期间启用一个字段，请点击展开箭头 ( ) 展开搜索限制，然后点击 **Disabled Columns** 下的列名。下表介绍捕获文件字段。

表 40-4　　捕获文件字段

字段	说明
Last Changed	上一次更新与该文件有关信息的时间。
文件名	最近检测到的与文件 SHA-256 哈希值相关的文件名。
布置	可以为下列文件性质之一： • `Malware` 表示云将文件归类为恶意软件，或文件威胁评分超过文件策略定义的恶意软件阈值。 • `Clean` 表示云将文件归类为安全，或用户将文件添加到安全列表。 • `Unknown` 表示在云分配性质之前发生恶意软件云查找。文件未分类。 • `Custom Detection` 表示用户将文件添加到自定义检测列表。 • `Unavailable` 表示防御中心无法执行恶意软件云查找。您可能看到有一小部分事件具有此性质，这是预期行为。 • `N/A` 表示 Detect Files 或 Block Files 规则处理了文件，防御中心不执行恶意软件云查找。
SHA256	文件的 SHA-256 哈希值以及显示最近检测文件事件和文件性质的网络文件轨迹图标。 要查看网络文件轨迹，请点击轨迹图标。有关详细信息，请参阅第 40-32 页上的分析网络文件轨迹。
威胁指数	与此文件相关的最新威胁评分： • `Low` ( ) • `Medium` ( ) • `High` ( ) • `Very High` ( ) 要查看动态分析总结报告，请点击威胁评分图标。
类型	文件类型，例如 `HTML` 或 `MSEXE`。
类别	一般类别文件类型，例如：`Office Documents`、`Archive`、`Multimedia`、`Executables`、`PDF files`、`Encoded`、`Graphics` 或 `System Files`。
Storage Status	该文件是否存储于受管设备。

表 40-4　捕获文件字段 （续）

字段	说明
Archive Inspection Status	对于存档文件，存档检查状态如下： • `Pending` 表示系统仍在检查存档文件及其内容。如果文件再次通过您的系统，就可以提供完整的信息。 • `Extracted` 表示系统能够提取和检查存档内容。 • 在极少数情况下，如果系统无法处理提取内容，会出现 `Failed` 状态。 • `Depth Exceeded` 表示存档包含超出最大允许深度的进一步嵌套存档文件。 • `Encrypted` 表示存档文件内容已加密，无法进行检查。 • `Not Inspectable` 表示系统未提取和检查存档内容。策略规则操作、策略配置和损坏文件是出现此状态的三个主要原因。 要查看存档文件内容，请右键单击文件事件查看器行，打开上下文菜单，然后选择 **View Archive Contents**。有关详细信息，请参阅第 37-18 页上的配置存档文件检查选项。
Analysis Status	是否已提交该文件用于动态分析。
Last Sent	最近一次向云提交文件进行动态分析的时间。

搜索捕获文件

许可证：恶意软件

使用防御中心搜索页面，您可以搜索具体捕获文件，在事件查看器中显示结果，并保存搜索条件以便后期重新使用。自定义分析控制面板构件、报告模版和自定义用户角色也可以使用保存的搜索条件。

请注意，搜索结果依赖于所搜索事件的可用数据。换言之，根据可用数据，搜索限制条件可能不适用。例如，如果文件从未被提交用于动态分析，可能没有与其关联的威胁评分。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (`!`)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (`*`) 作为通配符。

- 在任一字段指定 n/a 以便识别信息不适用于该字段的事件；使用 !n/a 识别字段填充事件。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

捕获文件的专用搜索语法

为补充上文所列通用搜索语法，下表介绍一些捕获文件的专用搜索语法。

表 40-5　捕获文件的专用搜索语法

搜索条件	专用语法
Storage Status	指定以下一项或多项内容： • File Stored - 返回设备存储的所有捕获文件 • Unable to Store File - 返回设备未存储的所有捕获文件
Dynamic Analysis Status	指定以下一项或多项内容： • Sent for Analysis - 返回排队等待进行动态分析的所有捕获文件 • Not Sent for Analysis - 返回未提交用于动态分析的所有捕获文件 • Analysis Complete - 返回提交用于动态分析且收到威胁评分和动态分析总结报告的所有捕获文件 • Previously Analyzed - 返回用户尝试再次提交用于动态分析且含有缓存的威胁评分的所有文件 • Failure (Analysis Timeout) - 返回提交用于动态分析，且云尚未返回结果的所有捕获文件 • Failure (Network Issue) - 返回因网络连接故障未提交用于动态分析的所有文件 • Failure (Cannot Run File) - 返回在测试环境中云不能运行的已提交用于动态分析的所有文件

要搜索捕获文件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Captured Files**。

页面根据相应限制进行更新。

步骤 3　在相应字段输入搜索条件。

有关捕获文件表字段的信息，请参阅捕获文件字段表。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save as New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果出现在默认的捕获文件工作流程内，并受当前时间范围限制。

使用网络文件轨迹

许可证：恶意软件或任意

受支持的设备：因功能而异

受支持的防御中心：因功能而异

网络文件轨迹功能映射出主机怎样在网络中传送文件，包括恶意软件文件。您可以使用此映射确定哪些主机可能已转移恶意软件、哪些主机存有风险并观察文件传送趋势。

轨迹映射以图表形式展示文件传输数据、文件性质以及是否阻止文件传送或是否隔离文件。构建映射的数据可来自基于网络的恶意软件事件 （系统执行恶意软件云查找并返回恶意软件性质的任何文件事件）和与检测和阻止恶意软件有关的基于终端的某些恶意软件事件 （任何检出威胁或隔离威胁的事件类型）。数据点之间的垂直线代表文件在主机之间传送。连接数据点的水平线表示随时间推移的主机文件活动。

对于系统可执行恶意软件云查找的任何文件类型，您可以跟踪该文件类型的传送。要直接访问文件轨迹，可使用 Network File Trajectory List 页面 (**Analysis > Files > Network File Trajectory**) 定位特定文件。此外，如果您正在分析入侵且需要审查相关文件的轨迹，您可以从 Context Explorer、控制面板或者连接、文件或恶意软件事件的事件视图中访问该文件轨迹。

单一轨迹映射显示的数据取决于设备中应用的许可证。下表列出了跟踪不同类型文件轨迹所必须的许可证。

表 40-6　　网络文件轨迹许可证要求

要查看.....	您需要以下许可证...
基于网络的文件和恶意软件轨迹	恶意软件
基于终端的威胁和隔离跟踪	任意 （您必须有一种 FireAMP 订用）

有关详情，请参见第 37-2 页上的了解恶意软件防护和文件控制。

请注意，因为您无法在 DC500 上使用恶意软件许可证，也无法在 2 系列设备或用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，所以，您无法使用这些设备捕获、存储或阻止个别文件、提交文件供动态分析、查看存档文件内容、或查看执行了恶意软件云查找的文件的轨迹。但是，您仍然可以查看基于终端的威胁和隔离跟踪文件轨迹

有关详细信息，请参阅以下各节：

- 第 40-31 页上的审核网络文件轨迹
- 第 40-32 页上的分析网络文件轨迹

审核网络文件轨迹

许可证：恶意软件或任意

受支持的设备：因功能而异

受支持的防御中心：因功能而异

当您审核捕获文件、文件事件和恶意软件事件时，您可以从 Context Explorer、正确配置的控制面板构件以及各种事件视图中查看文件轨迹映射。您还可以在 Network File Trajectory List 页面审核最近查看的网络文件轨迹和最近检测出的恶意软件。

有关详细信息，请参阅以下各节：

- 第 56-26 页上的查看“主要文件名”图形
- 第 56-38 页上的向下钻取 Context Explorer 数据
- 第 55-10 页上的了解 Custom Analysis 构件
- 第 37-18 页上的配置存档文件检查选项
- 第 40-8 页上的了解文件事件表
- 第 40-17 页上的了解恶意软件事件表
- 第 40-27 页上的了解捕获的文件表
- 第 39-9 页上的连接和安全情报事件中的可用信息
- 第 40-31 页上的访问网络文件轨迹

访问网络文件轨迹

许可证：恶意软件或任意

受支持的设备：因功能而异

受支持的防御中心：因功能而异

Network File Trajectory List 页面允许您定位具有 SHA-256 哈希值的文件，无论是用于分析最近检测出的恶意软件还是跟踪特定威胁。

该页面显示网络上最近检测出的恶意软件，以及最近查看过轨迹映射的文件。从这些列表中，可以查看最近在网络上查看文件的时间，该文件的 SHA-256 哈希值、名称、类型、当前文件性质、内容 （存档文件），以及与该文件相关联的事件的数量。有关字段的详细信息，请参阅第 40-8 页上的了解文件事件表。

该页面还包含一个可让您定位文件的搜索框，可基于 SHA-256 哈希值、文件名或传送或接收文件主机的 IP 地址进行查找。定位一个文件后，您可以点击 **File SHA256** 值，查看详细轨迹映射。有关详情，请参见第 40-32 页上的分析网络文件轨迹。

FireSIGHT 系统支持在所有网络界面区域显示和输入使用 Unicode (UTF-8) 字符的文件名，这些区域包括事件查看器、事件搜索、控制面板、 Context Explorer 等等。但是请注意，您以 PDF 格式生成的报告不支持 Unicode；Unicode 文件名将在 PDF 报告中以转译形式显示。有关详细信息，请参阅第 57-24 页上的生成并查看报告。

请注意，因为您无法在 DC500 上使用恶意软件许可证，也无法在 2 系列设备或用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，所以，您无法使用这些设备查看执行了恶意软件云查找的文件的轨迹。

要从 Network File Trajectory List 页面定位文件，请执行以下操作：

访问：任何环境

步骤 1　选择 **Analysis > Files > Network File Trajectory**。

系统将显示 Network File Trajectory List 页面，显示最近查看的文件和最近的恶意软件列表。

步骤 2　或者，您可以在搜索字段键入完整的 SHA-256 哈希值、主机 IP 地址或所要跟踪文件的文件名，然后按 Enter 键。

系统将显示 Query Results 页面，其中列出与搜索匹配的所有文件。如果只有一个结果匹配，系统将显示该文件的 Network File Trajectory 页面。

分析网络文件轨迹

许可证：恶意软件或任意

受支持的设备：因功能而异

受支持的防御中心：因功能而异

您可以通过查看网络文件详细轨迹在网络中跟踪文件。文件轨迹显示有关文件的概要信息、显示随时间推移的映射绘图数据点并且还列出了与表中数据点有关的事件数据。使用该表和映射，您可以准确定位特定文件事件、网络上传送或接收该文件的主机、映射中相关事件、表中受选定值限制的其他关联事件。

请注意，因为您无法在 DC500 上使用恶意软件许可证，也无法在 2 系列设备或用于 Blue Coat X-系列的思科 NGIPS上启用恶意软件许可证，所以，您无法使用这些设备查看执行了恶意软件云查找的文件的轨迹。

有关详细信息，请参阅以下各节：

- 第 40-32 页上的概要信息
- 第 40-34 页上的轨迹映射
- 第 40-37 页上的事件表

概要信息

许可证：恶意软件或任意

受支持的设备：因功能而异

受支持的防御中心：因功能而异

文件的轨迹页面显示有关文件的基本信息，包括文件识别信息、首次及最近一次在网络上查看文件的时间、与该文件相关的事件和主机数量以及该文件的当前性质。从本节开始，如果受管设备已存储文件，您可以进行本地下载、提交文件进行动态分析或将文件添加至文件列表。

提示　要查看相关文件事件，请点击字段值链接。在新窗口中打开文件事件默认工作流程首页，显示包含选定值的所有文件事件。

下表介绍了概要信息字段。

表 40-7　网络文件轨迹概要信息字段

字段名称	说明
File SHA256	文件的 SHA-256 哈希值。 默认情况下以压缩格式显示哈希值。要查看完整哈希值，请将指针悬停在上方。如果一个文件名与多个 SHA-256 哈希值关联，将指针悬停在链接上方查看全部哈希值。 点击下载文件图标 ( ) 将文件下载到本地计算机。如弹出提示，请确认您要下载该文件。按照浏览器提示保存文件。如果该文件不支持下载，则图标将灰显。 **注意事项** 思科强烈建议您**不要**下载恶意软件，否则可能造成不利后果。下载任何文件时请保持谨慎，这些文件可能包含恶意软件。确保您在下载文件前已采取各种必要预防措施保证下载目标安全。
文件名	事件关联文件的名称，如网络上所示。 如果一个 SHA-256 哈希值与多个文件名关联，列出最近检测到的文件名。您还可通过点击 `more` 将其展开以查看其余文件名。
文件类型	文件类型，例如 `HTML` 或 `MSEXE`。
File Category	文件类型的一般类别，例如 `Office Documents` 或 `System Files`。
Parent Application	检测期间访问恶意软件文件的客户端应用。这些应用与网络发现或应用控制**无**关联。 只为基于终端的恶意软件事件显示此字段。
First Seen	受管设备或 FireAMP 连接器首次检测到该文件和首次上传该文件的主机 IP 地址的时间。
Last Seen	受管设备或 FireAMP 连接器最近一次检测到该文件和最近一次下载该文件主机的 IP 地址的时间。
Event Count	网络上看到的与该文件相关事件的数量，以及如检测到超过 250 个事件时映射中显示的事件数量。
Seen On	发送或接收文件的主机数量。因为一台主机可以在不同时间上传和下载文件，在 `Seen On Breakdown` 字段中的主机总数可能与发送方总数加上接收方总数之和并不匹配。
Seen On Breakdown	发送文件的主机数量，然后紧接接收文件的主机数量。
Current Disposition	可以为下列文件性质之一： • `Malware` 表示云将文件归类为恶意软件，或文件威胁评分超过文件策略定义的恶意软件阈值。 • `Clean` 表示云将文件归类为安全，或用户将文件添加到安全列表。 • `Unknown` 表示在云分配性质之前发生恶意软件云查找。文件未分类。 • `Custom Detection` 表示用户将文件添加到自定义检测列表。 • `Unavailable` 表示防御中心无法执行恶意软件云查找。您可能看到有一小部分事件具有此性质，这是预期行为。 • `N/A` 表示 Detect Files 或 Block Files 规则处理了文件，防御中心不执行恶意软件云查找。 点击编辑图标 ( ) 从安全列表或自定义检测列表中添加或删除文件。 只为基于网络的恶意软件事件显示此字段。

表 40-7　网络文件轨迹概要信息字段 （续）

字段名称	说明
Archive Contents	对已检查存档文件，指存档文件包含的文件数量。点击视图图标 ( ) 查看有关 Archive Contents 窗口中内容文件的信息。 有关存档文件检查的详细信息，请参阅第 37-18 页上的配置存档文件检查选项。
Threat Name	与文件相关的恶意软件威胁名称。 只为基于终端的恶意软件事件显示此字段。
威胁指数	文件威胁评分： • Low ( ) • Medium ( ) • High ( ) • Very High ( )。 点击威胁评分图标查看动态分析总结报告，点击威胁评分图标。 点击威胁评分链接查看具有该威胁评分的所有捕获文件。 点击云图标 ( ) 将文件提交至云进行动态分析。如果该文件无法提交或您无法连接到云，图标将灰显。

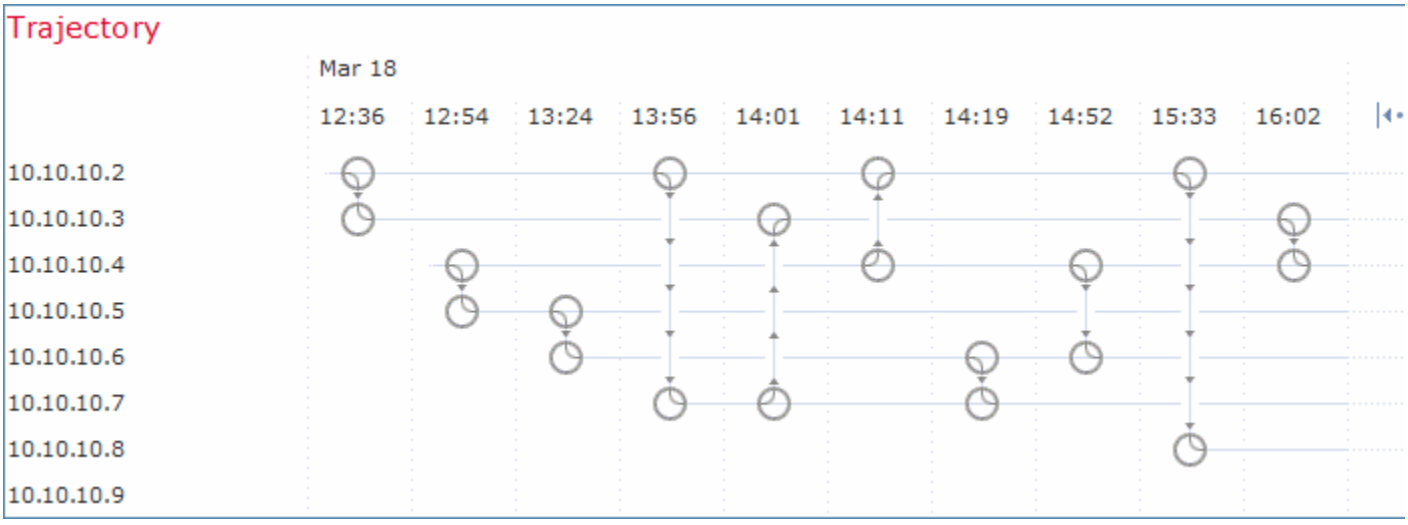
轨迹映射

许可证：恶意软件或任意

受支持的设备：因功能而异

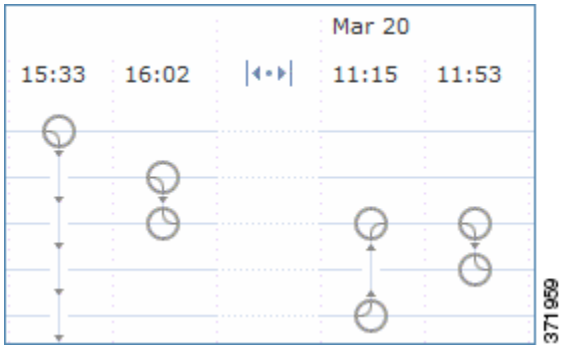
受支持的防御中心：因功能而异

文件轨迹映射直观地跟踪从网络上第一次检测到文件至最近一次检测到该文件的情况。该映射显示出主机传送或接收文件的时间、传送文件频率和阻止或隔断文件的时间。该映射还显示文件出现文件事件的频率，以及系统为文件分配性质或回溯性质的时间。您可以在映射中选择数据点，并突出显示追溯至主机第一次传输该文件的事例的轨迹；此轨迹还将贯穿每次主机作为该文件接收方或发送方的事例。下图显示了一个轨迹映射示例：



映射 y 轴包含与该文件交互的所有主机 IP 地址列表。 IP 地址按照系统在主机上首次检测到该文件的时间降序排列。每行都包含与该 IP 地址相关的所有事件，无论是单一文件事件、文件传送还是回溯事件。 x 轴包含系统检测到各个事件的日期和时间。时间戳按时间顺序排列。如果一分钟内发生多个事件，在同一栏中列出所有事件。您可以水平或垂直滚动映射，以查看其他事件和 IP 地址。

映射中显示多达 250 个与文件 SHA-256 哈希值有关的事件。如有超过 250 个事件，则映射上只显示前十个，并用箭头图标 (|◂•▸|) 截略其他事件。然后映射显示剩下 240 个事件。下图显示箭头图标截略事件：

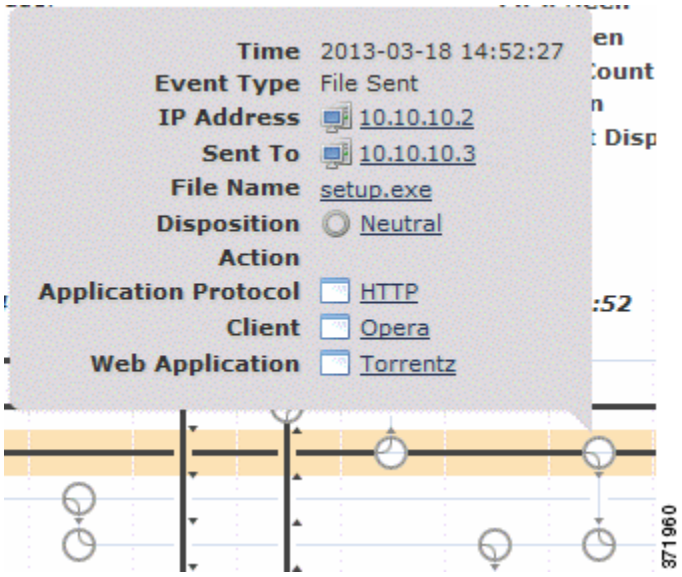


您可以通过点击箭头图标 (|◂•▸|) 查看文件概要事件视图中未显示的所有事件。将在新窗口中显示文件事件默认工作流程的首页，同时显示所有基于文件类型受限的其他事件。如果未显示基于终端的恶意软件事件，您必须切换到 Malware Events 表进行查看。

每个数据点代表一个事件及其文件性质，如在映射下方图例所述。例如， Malware Block 事件图标结合了 Malicious Disposition 图标和 Block Event 图标。

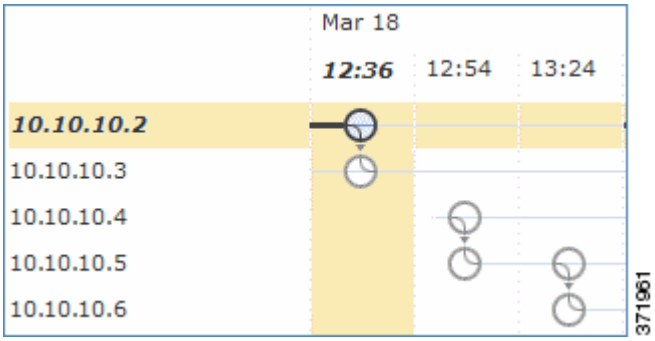
基于终端的恶意软件事件包含一个图标。回溯事件在栏中为各检测到文件的主机显示一个图标。文件传送事件始终包括两个图标，一个文件发送图标和一个文件接收图标，两者之间用垂直线连接。箭头表示从发送方到接收方的文件传送方向。

您可以通过将鼠标指针悬停在事件图标 (◔) 上来查看概要信息。所显示概要信息与事件表中显示信息相匹配。下图显示一个事件图标的概要信息：



如果点击任何事件概要信息链接，则在新窗口中显示文件事件默认工作流程首页以及基于文件类型的所有其他受限事件。在新窗口中打开文件概要事件视图，显示符合所点击标准值的所有文件事件。

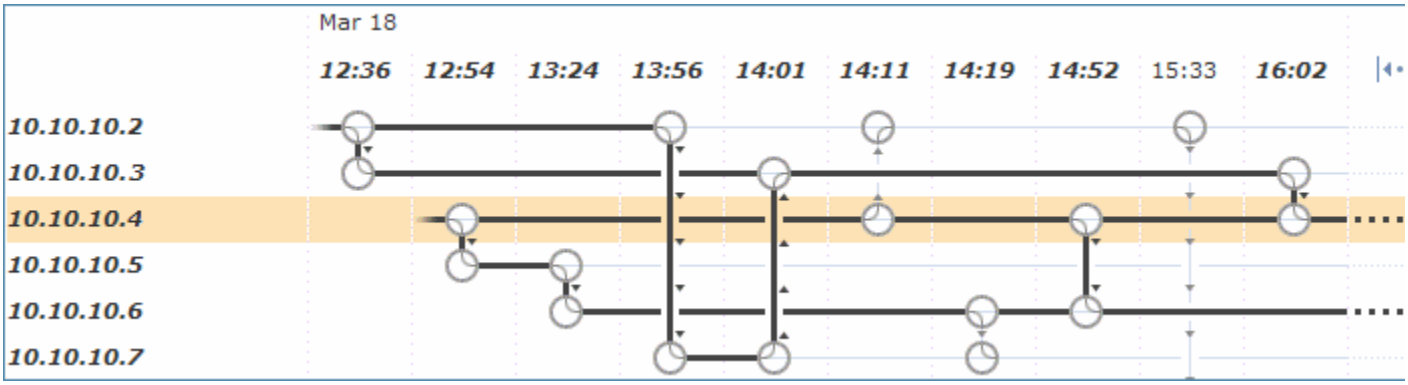
要定位涉及 IP 地址的第一例文件事件，请点击该地址。突出显示连至该数据点的轨迹，以及与第一个文件事件相关的任何介于其间的文件事件和 IP 地址。同时突出显示事件表中相应事件。如当前不可见，映射会滚动至该数据点。下图显示点击 IP 地址后突出显示的轨迹：



要跟踪文件在网络中的历程，可以点击任意数据点突出显示一个轨迹，其中包括与选定数据点相关的所有数据点。这包括与下列类型的事件相关的数据点：

- 无论关联 IP 地址作为发送方还是接收方的任何文件传送
- 涉及关联 IP 地址的任何基于终端的恶意软件事件
- 如果涉及另一个 IP 地址，无论该关联 IP 地址作为发送方还是接收方的所有文件传送
- 如果涉及另一个 IP 地址，涉及该 IP 地址的基于终端的任何恶意软件事件

下图显示点击一个事件图标后突出显示的轨迹：



同时突出显示与任何突出显示数据点相关的所有 IP 地址和时间戳。同时突出显示事件表中相应事件。如果一条轨迹中包含截略事件，则用虚线突出显示轨迹本身。可能有截略事件与轨迹相交，但并不在映射中进行显示。

事件表

许可证：恶意软件或任意

受支持的设备：因功能而异

受支持的防御中心：因功能而异

事件表为映射中各数据点列出事件信息。您可以点击列标题按升序或降序排列事件。您可以通过选择表格行来突出显示映射中的数据点。如当前不可见，映射会滚动至选定文件事件并显示该事件。有关字段的详细信息，请参阅第 40-8 页上的了解文件事件表。

处理入侵事件

FireSIGHT 系统可帮助监控网络中可能影响主机及其数据的可用性、完整性和机密性的流量。通过将受管设备放在关键网段，可以检查流经网络的数据包是否包含恶意活动。系统通过使用多个机制查找攻击者开发的众多漏洞。

如果系统识别出潜在的入侵，会生成*入侵事件*；入侵事件是包含攻击的日期、时间、漏洞类型以及有关攻击的来源和目标的情境信息的记录。对于基于数据包的事件，还会记录触发事件的一个或多个数据包的副本。受管设备将其事件传输到防御中心，在其中可以查看聚合数据并更好地了解针对网络资产的攻击。

还可以将受管设备部署为内联式、交换式或路由式入侵系统，以便将设备配置为会丢弃或替换已知有害的数据包。

FireSIGHT 系统还提供必要的工具，可以用来审查入侵事件并评估它们在网络环境中以及对于安全策略是否重要。这些工具包括：

- 事件摘要页面，提供受管设备上当前活动的概览
- 基于文本和图表的报告，可以针对所选的任何时间段生成此类报告；还可以自行设计报告并将其配置为按预定的时间间隔运行
- 可用来收集与攻击相关的事件数据的事故处理工具；还可以添加注释以便跟踪调查和响应
- 可以为 SNMP、邮件和系统日志配置的自动警报
- 可用于响应和处理特定入侵事件的自动关联策略
- 预定义和自定义工作流程，可用于向下钻取以识别要进一步调查的事件

有关详细信息，请参阅以下各节：

- 第 41-2 页上的查看入侵事件统计信息介绍 Intrusion Event Statistics 页面，该页面提供设备运行状况概览和网络重大威胁的摘要。
- 第 41-4 页上的查看入侵事件性能介绍如何生成入侵事件性能统计信息图表。
- 第 41-7 页上的查看入侵事件图表介绍如何生成显示事件趋势随时间推移变化情况的图表。
- 第 41-7 页上的查看入侵事件介绍如何使用网络界面查看和调查入侵事件。
- 第 41-15 页上的了解入侵事件的工作流程页面介绍在入侵事件工作流程中可供使用的各个页面，并说明如何使用它们来分析入侵事件。
- 第 41-16 页上的使用下钻式页面和表视图页面介绍入侵事件工作流程中两类页面的功能。
- 第 41-19 页上的使用数据包视图介绍如何使用入侵事件的数据包视图。
- 第 41-32 页上的使用影响级别评估事件说明如何使用影响级别评估入侵事件。
- 第 41-33 页上的解读预处理器事件说明如何解读预处理器规则生成的事件。
- 第 41-36 页上的搜索入侵事件说明如何使用搜索功能对入侵事件列表应用特定限制条件。

- 第 41-42 页上的使用剪贴板说明如何将入侵事件添加到一个称为剪贴板的保留区域，以便日后将这些事件添加到事故。本节还介绍如何根据剪贴板内容生成事件报告。

另请参阅：

- 第 42-1 页上的事故处理，以了解有关事故处理以及如何使用事故来跟踪事件分析进度的信息。
- 第 44-1 页上的配置入侵规则的外部警报，以了解有关自动警报的详细信息。
- 第 57-1 页上的使用报告，以了解有关入侵事件报告的详细信息。
- 第 58-17 页上的使用地理定位，以了解有关入侵事件中的地理定位信息的详细信息。

查看入侵事件统计信息

许可证：保护

Intrusion Event Statistics 页面提供设备当前状态和网络生成的所有入侵事件的简要摘要。

Intrusion Event Statistics 页面有三个主要区域：

- 第 41-3 页上的主机统计信息介绍 Host Statistics 章节，提供有关设备 （对于 防御中心，还包括其受管设备）的信息。
- 第 41-3 页上的事件概述介绍 Event Overview，提供事件数据库中信息的概述。
- 第 41-3 页上的事件统计信息介绍 Event Statistics ，提供有关事件数据库中信息的更具体信息，例如，前 10 大事件类型。

页面上的每个 IP 地址、端口、协议和事件消息等均为链接。点击任意链接可查看相关的事件信息。例如，如果前 10 大目标端口之一是 `80 (http)/tcp`，点击该链接会显示默认入侵事件工作流程的第一个页面，并列出以该端口为目标的事件。请注意，只会显示当前时间范围内的事件 （以及生成事件的受管设备）。此外，标记为“已审核”的入侵事件会继续显示在统计信息中。例如，如果当前时间范围是过去一小时，但第一个事件是在五小时前生成的，当点击 **First Event** 链接时，打开的事件页面将不会显示事件，直至时间范围被更改。

要查看入侵事件统计信息，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Overview > Summary > Intrusion Event Statistics**。

系统将显示 Intrusion Event Statistics 页面。

步骤 2　从页面顶部的两个选择框选择要查看其统计信息的区域和设备，或者选择 **All Security Zones** 和 **All Devices** 以查看收集入侵事件的所有设备的统计信息。

步骤 3　点击 **Get Statistics**。

Intrusion Event Statistics 页面刷新，以显示来自所选设备的数据。

提示　要查看自定义时间范围内的数据，请点击页面右上角区域的链接并按照第 58-19 页上的设置事件时间限制中的指示操作。

步骤 4　有关显示在 Intrusion Event Statistics 页面上的统计信息的详细信息，请参阅以下各节：

- 第 41-3 页上的主机统计信息
- 第 41-3 页上的事件概述
- 第 41-3 页上的事件统计信息

主机统计信息

许可证：保护

Intrusion Event Statistics 页面的 Host Statistics 节提供有关设备本身的信息。在防御中心上，此节还提供有关所有受管设备的信息。

这些信息包括以下内容：

- **Time** 显示设备上的当前时间。
- **Uptime** 显示设备本身重新启动以来的天数、小时数和分钟数。在防御中心上， Uptime 还显示每个受管设备上一次重新启动的时间、已登录用户数和平均负载。
- **Disk Usage** 显示使用中磁盘所占的百分比。
- **Memory Usage** 显示已使用系统内存所占的百分比。
- **Load Average** 显示过去 1 分钟、 5 分钟和 15 分钟内 CPU 队列中的平均进程数。

事件概述

许可证：保护

Intrusion Event Statistics 页面的 Event Overview 章节提供入侵事件数据库中信息的概述。

这些统计信息包括以下内容：

- **Events** 显示入侵事件数据库中的事件数。
- **Events in Time Range** 显示当前选定的时间范围以及数据库中属于该时间范围的事件数量和所占百分比。
- **First Event** 显示事件数据库中第一个事件的事件消息。
- **Last Event** 显示事件数据库中最后一个事件的事件消息。

注　请注意，在防御中心上，如果选择受管设备，将会显示该设备的 Event Overview 部分。

事件统计信息

许可证：保护

Intrusion Event Statistics 页面的 Event Statistics 部分提供有关入侵事件数据库中信息的更具体信息。

这些信息包括以下方面的详细信息：

- 前 10 大事件类型
- 前 10 大源 IP 地址
- 前 10 大目标 IP 地址
- 前 10 大目标端口
- 具有最大数量事件的协议、入口安全区域、出口安全区域和设备

查看入侵事件性能

许可证：保护

Intrusion Event Performance 页面允许生成说明入侵事件在特定时间段内的性能统计信息的图表。可以生成图表来反映每秒入侵事件数、每秒兆位数、每个数据包的平均字节数、 Snort 未检查的数据包百分比以及因 TCP 标准化而被阻止的数据包数量。这些图表可以显示过去一小时、前一天、上一周或上个月的运行统计信息。

有关详细信息，请参阅第 41-4 页上的生成入侵事件性能统计信息图表。

要查看入侵事件性能统计信息，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **Overview > Summary > Intrusion Event Performance**。

系统将显示 Intrusion Event Performance 页面。

生成入侵事件性能统计信息图表

许可证：保护

可以基于以下数据生成说明防御中心或受管设备性能统计信息的图表：每秒事件数、每秒兆位数、每个数据包的平均字节数、 Snort 未检查的数据包百分比以及因 TCP 标准化而被阻止的数据包数量。

注　新数据将进行累计，统计信息图表每五分钟更新一次。因此，如果快速重新加载图表，直到下一次五分钟更新间隔之前数据可能不会更改。

下表列出了可用的图表类型。请注意，如果图表类型填充的数据受网络分析策略 **Inline Mode** 设置影响，则图表类型显示会有所不同。如果禁用 **Inline Mode**，网络界面上标有星号 (*) 的图表类型（在下面的栏中标有 `yes`）会用关于流量的数据进行填充；如果禁用 **Inline Mode** ，则系统会修改或丢弃数据。有关 **Inline Mode** 设置的详细信息，请参阅第 26-4 页上的允许预处理器影响内联部署中的流量。

有关所需的选项和设置的详细信息，请参阅第 29-6 页上的规范化内联流量、第 26-4 页上的允许预处理器影响内联部署中的流量和第 31-5 页上的在内联部署中设置丢弃行为。

表 41-1　　入侵事件性能图表类型

要为以下项生成数据：	您必须.....	代表含义.....	是否受 Inline Mode 影响？
平均字节/数据包	不适用	每个数据包中包含的平均字节数。	否
在 TCP 流量/数据包中规范化的 ECN 标志	启用 **Explicit Congestion Notification** 并选择 **Packet**	无论是否协商，以数据包为单位，已为其清除 ECN 标记的数据包的数量。	是
在 TCP 流量/会话中规范化的 ECN 标记	启用 **Explicit Congestion Notification** 并选择 **Stream**	未协商使用 ECN 使用时，以数据流为单位， ECN 标记被清除的次数。	是
事件/秒	不适用	设备上每秒生成的事件数。	否

表 41-1　　入侵事件性能图表类型（续）

要为以下项生成数据：	您必须.....	代表含义.....	是否受 Inline Mode 影响？
ICMPv4 回显规范化	启用 **Normalize ICMPv4**	回显（请求）或回显回复消息中 8 位 Code 字段被清除的 ICMPv4 数据包的数量。	是
ICMPv6 回显规范化	启用 **Normalize ICMPv6**	回显（请求）或回显回复消息中 8 位 Code 字段被清除的 ICMPv6 数据包的数量。	是
IPv4 DF 标记规范化	启用 **Normalize IPv4** 和 **Normalize Don't Fragment Bit**	IPv4 Flags 报头字段的一位 Don't Fragment 子字段被清除的 IPv4 数据包的数量。	是
IPv4 选项规范化	启用 **Normalize IPv4**	选项八位字节被设置为 1 (No Operation) 的 IPv4 数据包的数量。	是
IPv4 保留标记规范化	启用 **Normalize IPv4** 和 **Normalize Reserved Bit**	IPv4 Flags 报头字段的一位 Reserved 子字段被清除的 IPv4 数据包的数量。	是
IPv4 调整大小规范化	启用 **Normalize IPv4**	已按照 IP 报头中指定数据报长度截断多余长度负载的 IPv4 数据包的数量。	是
IPv4 TOS 规范化	启用 **Normalize IPv4** 和 **Normalize TOS Bit**	单字节 Differentiated Services (DS) 字段（之前叫做 Type of Service (TOS) 字段）被清除的 IPv4 数据包的数量。	是
IPv4 TTL 规范化	启用 **Normalize IPv4**、 **Maximum TTL** 和 **Reset TTL**	IPv4 生存时间规范化的数量。	是
IPv6 选项规范化	启用 **Normalize IPv6**	Hop-by-Hop Options 或 Destination Options 扩展报头中 Option Type 字段设置为 `00`（跳过并继续处理）的 IPv6 数据包的数量。	是
IPv6 TTL 规范化	启用 **Normalize IPv6**、**Minimum TTL** 和 **Reset TTL**	IPv6 跳数限制 (TTL) 规范化的数量。	是
兆位/秒	不适用	每秒通过设备的流量兆位数。	否
调整大小以适应 MSS 的数据包规范化	启用 **Trim Data to MSS**	负载长于 TCP Data 字段，因而被调整至 Maximum Segment Size 的数据包的数量。	是
调整大小以适应 TCP 窗口的数据包规范化	启用 **Trim Data to Window**	TCP Data 字段被调整以适应接收主机的 TCP 窗口的数据包的数量。	是
丢包率	不适用	所有选定设备上未经检查的数据包的平均百分比。例如，如果选择两个设备，那么平均百分比 50% 可能表示一个设备的丢包率为 90%，另一个的丢包率为 10%。也可能表示这两个设备的丢包率均为 50%。当选择一个设备时，此图表仅表示总丢包率。	否
数据条带化的 RST 数据包规范化	启用 **Remove Data on RST**	数据被从 TCP 重置 (RST) 数据包移除的数据包的数量。	是
数据条带化的 SYN 数据包规范化	启用 **Remove Data on SYN**	当 TCP 操作系统不是 Mac OS 时数据被从 SYN 数据包移除的数据包的数量。	是
TCP 报头填充规范化	启用 **Normalize/Clear Option Padding Bytes**	选项填充字节设置为 0 的 TCP 数据包的数量。	是
无选项 TCP 规范化	启用 **Allow These TCP Options** 并设置为 `any` 之外的任意选项	Time Stamp 选项条带化的数据包的数量。	是

表 41-1　　入侵事件性能图表类型 （续）

要为以下项生成数据：	您必须.....	代表含义.....	是否受 Inline Mode 影响？
TCP NS 标记规范化	启用 **Explicit Congestion Notification** 并选择 **Packet**	ECN Nonce Sum (NS) 选项规范化的数量。	是
TCP 选项规范化	启用 **Allow These TCP Options** 并设置为 any 之外的任意选项	选项字段设置为 No Operation (TCP Option 1) 的选项的数量 （MSS、 Window Scale、 Time Stamp 以及明确允许的选项除外）。	是
TCP 数据包阻止条件规范化	启用 **Normalize TCP Payload**（分段重组必须失败）	因为 TCP 分段无法正确重组而被丢弃的数据包的数量。	是
TCP 保留标记规范化	启用 **Normalize/Clear Reserved Bits**	Reserved 位被清除的 TCP 数据包的数量。	是
TCP 分段重组规范化	启用 **Normalize TCP Payload**（分段重组必须成功）	TCP Data 字段已规范化以确保重传传输的数据的一致性的数据包数量 （无法正确重组的所有片段都被丢失）。	是
TCP SYN 选项规范化	启用 **Allow These TCP Options** 并设置为 any 之外的任意选项	由于未设置 SYN 控制位， Maximum Segment Size 或 Window Scale 选项被设置为 No Operation (TCP Option 1) 的选项的数量。	是
TCP 时间戳 ECR 规范化	启用 **Allow These TCP Options** 并设置为 any 之外的任意选项	Time Stamp Echo Reply (TSecr) 选项字段由于未设置 Acknowledgment (ACK) 控制位而被清除的数据包的数量。	是
TCP 紧急指针规范化	启用 **Normalize Urgent Pointer**	双字节 TCP 报头 Urgent Pointer 字段大于负载长度，因而被设置成负载长度的数据包的数量。	是
被阻止的地址块总数	配置 **Inline Mode** 或 **Drop when Inline**	丢弃的数据包总数，包括规则、解码器和预处理器丢弃。	否
总计注入的数据包	配置 **Inline Mode**	在重新传输前调整大小的数据包的数量。	否
总 TCP 过滤的数据包	配置 TCP Stream Preprocessing	由于 TCP 端口过滤而被数据流跳过的数据包的数量。	否
总 UDP 过滤的数据包	配置 UDP Stream Preprocessing	由于 UDP 端口过滤而被数据流跳过的数据包的数量。	否
紧急标记清除规范化	启用 **Clear URG if Urgent Pointer is Not Set**	因为未设置紧急指针， TCP 报头 URG 控制位被清除的数据包的数量。	是
紧急指针和紧急标记清除规范化	启用 **Clear Urgent Pointer/URG on Empty Payload**	TCP 报头 Urgent Pointer 字段和 URG 控制位由于没有负载而被清除的数据包的数量。	是
紧急指针清除规范化	启用 **Clear Urgent Pointer if URG=0**	16 位 TCP 报头 Urgent Pointer 字段由于未设置紧急 (URG) 控制位而被清除的数据包的数量。	是

要生成入侵事件性能图表，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **Overview > Summary > Intrusion Event Performance**。

系统将显示 Intrusion Event Performance 页面。

步骤 2　从 **Select Device** 列表中，选择要查看其数据的设备。

步骤 3　从 **Select Graph(s)** 列表中，选择要创建的图表类型。

步骤 4　从 **Select Time Range** 列表中，选择要用于图表的时间范围。

可供选择的时间范围有：过去一小时、前一天、上一周和上个月。

步骤 5　点击 **Graph**。

系统显示图表，其中显示您指定的信息。

步骤 6　要保存图表，请右键单击它并按照浏览器的指示保存图像。

查看入侵事件图表

许可证：保护

FireSIGHT 系统提供显示入侵事件随时间推移变化趋势的图表。可以为以下对象生成随时间推移变化范围为过去一小时至上个月的入侵事件图表：

- 一个或所有受管设备
- 前 10 大目标端口
- 前 10 大源 IP 地址
- 前 10 大事件消息

要生成事件图表，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Overview > Summary > Intrusion Event Graphs**。

系统将显示 Intrusion Event Graphs 页面。页面顶部的三个选择框控制生成哪个图表。

步骤 2　在 **Select Device** 下，选择 **all** 以包括所有设备，或选择要包括在图表中的特定设备。

步骤 3　在 **Select Graph(s)** 下，选择要生成的图表类型。

步骤 4　在 **Select Time Range** 下，选择图表的时间范围。

步骤 5　点击 **Graph**。

成功生成图表。

查看入侵事件

许可证：保护

当系统识别到可能有恶意行为的数据包时，会生成入侵事件并将该事件添加到数据库。

初始入侵事件视图根据用于访问页面的工作流程而不同。可以使用其中一个预定义工作流程（其中包括一个或更多下钻式页面、入侵事件表视图和一个终止数据包视图），或者也可以创建自己的工作流程。还可以查看基于自定义表的工作流程，该表可能包括入侵事件。请注意，如果事件视图包含大量 IP 地址且已启用 **Resolve IP Addresses** 事件视图设置，事件视图可能显示得很慢。有关详细信息，请参阅第 71-3 页上的配置事件查看设置。

可以查看入侵事件来确定其是否会对网络安全构成威胁。如果确信入侵事件不是恶意的，可以将其标记为“已审核”。您的姓名将显示为审核员，已审核的事件不再列出在默认入侵事件视图中。可以将已审核的事件返回到默认入侵事件视图，方法是将该事件标记为“未审核”。

可以查看标记为“已审核”的入侵事件。已审核事件存储在数据库中并包括在事件摘要统计信息中，但不再显示在默认事件页面中。有关详细信息，请参阅第 41-14 页上的审核入侵事件。

如果执行备份然后删除已审核的入侵事件，恢复备份会恢复已删除的入侵事件，但不能恢复其“已审核”状态。可在 Intrusion Events （而不是 Reviewed Events）下查看这些恢复的入侵事件。

要快速查看与一个或多个入侵事件相关的连接事件，请使用事件查看器中的复选框选择入侵事件，然后从 **Jump to** 下拉列表选择 **Connections**。在事件的表视图之间导航时，此方法最有用。还可以使用类似方法查看与特定连接相关的入侵。

有关详细信息，请参阅以下各节：

- 第 41-8 页上的了解入侵事件
- 第 58-34 页上的创建自定义工作流程
- 第 41-16 页上的使用下钻式页面和表视图页面
- 第 41-19 页上的使用数据包视图
- 第 41-13 页上的查看与入侵事件相关的连接数据
- 第 41-14 页上的审核入侵事件
- 第 59-8 页上的根据自定义表查看工作流程

要查看入侵事件，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Analysis > Intrusions > Events**。

系统显示默认入侵事件工作流程的第一个页面。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示任何事件，可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

提示　如果使用不包括入侵事件表视图的自定义工作流程，请点击工作流程标题旁边的 **(switch workflow)** 以选择随设备提供的任意预定义工作流程。

有关入侵事件视图中显示的事件的详细信息，请参阅第 41-8 页上的了解入侵事件。请参阅第 41-15 页上的了解入侵事件的工作流程页面，以了解有关如何将视图缩小至对分析非常重要的入侵事件的详细信息。

了解入侵事件

许可证：保护

系统检查网络上传输的数据包是否存在可能影响主机及其数据的可用性、完整性和机密性的恶意活动。如果系统识别出潜在的入侵，会生成*入侵事件*；入侵事件是包含攻击的日期、时间、漏洞类型以及有关攻击的来源和目标的情境信息的记录。对于基于数据包的事件，还会记录触发事件的一个或多个数据包的副本。请注意，对于任何单个入侵事件可提供的信息取决于许可证等多种因素。有关详细信息，请参阅第 65-2 页上的许可证类型和限制。

以下列表说明入侵事件中包含的信息。请注意，默认情况下，入侵事件表视图中的某些字段已禁用。要在会话期间启用一个字段，请点击展开箭头 ( ) 展开搜索限制，然后点击 **Disabled Columns** 下的列名。

时间

事件的日期和时间。

优先级

事件优先级由思科 VRT 确定。

影响

此字段中的影响级别指示入侵数据、网络发现数据和漏洞信息之间的相关性。有关详细信息，请参阅第 41-32 页上的使用影响级别评估事件。

请注意，对于基于 NetFlow 数据添加到网络映射的主机，没有任何操作系统信息可用，因此，防御中心无法为涉及这些主机的入侵事件分配 Vulnerable （影响级别 1：红色）影响级别，除非您使用主机输入功能手动设置主机操作系统身份。

Inline Result

以下之一：

- 一个黑色向下箭头，表明系统已丢弃触发规则的数据包
- 一个灰色向下箭头，表明如果已启用 **Drop when Inline** 入侵策略选项 （在内联部署中），或者在系统进行修剪时一个 Drop and Generate 规则生成了该事件，那么 IPS 应该已丢弃数据包
- 空白，表明触发规则未设置为 Drop and Generate Events

请注意，无论入侵策略的规则状态或内联丢弃行为如何，系统都不会丢弃被动部署中的数据包，当内联接口处于分路模式时也是如此。

源 IP：

发送主机使用的 IP 地址。

Source Country

发送主机的国家/地区。

目标 IP：

接收主机使用的 IP 地址。

Destination Country

接收主机的国家/地区。

Original Client IP

提取自 X-Forwarded-For (XFF)、True-Client-IP 或自定义的 HTTP 报头的原始客户端 IP 地址。要显示此字段的值，必须在网络分析策略中启用 HTTP 预处理器 **Extract Original Client IP Address** 选项。或者，在网络分析策略的同一区域，还可以指定最多六个自定义客户端 IP 报头，并设置系统选择原始客户端 IP 事件字段值的优先顺序。有关详细信息，请参阅第 27-28 页上的选择服务器级别 HTTP 规范化选项。

默认情况下会启用此字段。

Source Port/ICMP Type

发送主机上的端口号。对 ICMP 流量，当没有端口号时，系统显示 ICMP 类型。

Destination Port/ICMP Code

接收流量的主机的端口号。对 ICMP 流量，当没有端口号时，系统显示 ICMP 代码。

SSL Status

SSL 规则相关操作、默认操作或记录加密连接的不可解密流量操作：

- `Block` 和 `Block with reset` 代表被阻止的加密连接。
- `Decrypt (Resign)` 代表使用重签服务器证书解密的传出连接。
- `Decrypt (Replace Key)` 代表使用带替代公共密钥的自签服务器证书解密的传出连接。
- `Decrypt (Known Key)` 代表使用已知私有密钥解密的传入连接。
- `Do not Decrypt` 代表系统未解密的连接。

如果系统无法解密加密连接，则会显示所采取的不可解密流量操作和失败原因。例如，如果系统检测到使用未知密码套件加密的流量并且未做进一步检查即允许了该流量，此字段显示 `Do Not Decrypt (Unknown Cipher Suite)`。

点击锁图标 () 可查看证书详细信息。有关详细信息，请参阅第 39-27 页上的查看与加密连接相关的证书。

VLAN ID

与触发入侵事件的数据包相关的最内部的 VLAN ID。

MPLS Label

与触发此入侵事件的数据包相关的多多协议标记交换标记。

默认情况下，此字段处于禁用状态。

通信

事件的说明文本。对于基于规则的入侵事件，事件消息提取自规则。对于基于解码器和预处理器的事件，事件消息采用硬编码。

分类

生成事件的规则所属的分类。有关规则分类名称和编号，请参阅规则分类表。

发电机

生成事件的组件。有关入侵事件生成器 ID 的列表，请参阅第 41-34 页上的表 41-7。

Source User

登录源主机的任何已知用户的用户 ID。

Destination User

登录目标主机的任何已知用户的用户 ID。

Application Protocol

应用协议 （如果有），代表在触发入侵事件的流量中检测到的主机之间的通信。有关系统 如何识别在防御中心网络界面中检测到的应用程序协议的信息，请参阅第 45-11 页上的表 45-3。

客户端

客户端应用 （如果有），代表在触发入侵事件的流量中检测到的受监控主机上运行的软件。

Web 应用程序

网络应用，代表在触发入侵事件流量中检测到的 HTTP 流量的内容或请求的 URL。

请注意，如果系统检测到 HTTP 应用协议，但无法检测到特定网络应用，系统会在此处提供通用的 网络浏览应用。

IOC

触发入侵事件的流量是否也触发了危害表现 (IOC)。有关 IOC 的详细信息，请参阅第 45-17 页上的了解危害表现。

Category, Tag (Application Protocol, Client, Web Application)

展示了应用特征的标准，帮助您了解应用功能；请参阅第 45-9 页上的表 45-2。

Application Risk

与在触发入侵事件的流量中检测到的应用相关的风险。在连接中检测的各种类型的应用都有相关的风险；此字段显示当中的最高风险。有关详细信息，请参阅第 45-9 页上的表 45-2。

业务相关性

与在触发入侵事件的流量中检测到的应用相关的业务相关性。连接中检测的各类应用都有相关业务；此字段显示当中最低 （相关性最小）的业务相关性。有关详细信息，请参阅第 45-9 页上的表 45-2。

Ingress Security Zone

触发事件的数据包的入口安全区域。在被动部署中仅填充此安全区域字段。请参阅第 3-34 页上的使用安全区域。

Egress Security Zone

对于内联部署，触发事件的数据包的出口安全区域。在被动部署中不填充此安全区域字段。请参阅第 3-34 页上的使用安全区域。

设备

应用访问控制策略的受管设备。请参阅第 4-1 页上的管理设备。

安全情景

识别流量通过的虚拟防火墙组的元数据。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。

Ingress Interface

触发事件的数据包的入口接口。对于被动接口，仅填充此接口列。请参阅第 4-52 页上的配置感应接口。

Egress Interface

对于内联部署，触发事件的数据包的出口接口。对于被动接口，不填充此接口列。请参阅第 4-52 页上的配置感应接口。

Intrusion Policy

启用了生成事件的入侵规则、预处理器规则或解码器规则的入侵策略。可以选择入侵策略作为访问控制策略的默认操作，也可以将入侵策略与访问控制规则关联起来。请参阅第 12-6 页上的设置对网络流量的默认处理和检查和第 18-5 页上的配置访问控制规则以执行入侵防御。

访问控制策略

包含启用了生成事件的入侵规则、预处理器规则或解码器规则的入侵策略的访问控制策略；请参阅第 12-9 页上的管理访问控制策略。

Access Control Rule

调用生成事件的入侵策略的访问控制规则；请参阅第 18-5 页上的配置访问控制规则以执行入侵防御。`Default Action` 指出启用了规则的入侵政策未与特定访问控制规则关联，但被配置为访问控制策略的默认操作；请参阅第 12-6 页上的设置对网络流量的默认处理和检查。

如果入侵检查既未与访问控制规则关联，也未与默认操作关联，例如数据包由默认入侵策略检查，则该字段留空。有关详细信息，请参阅第 25-1 页上的设置用于访问控制的默认入侵策略。

网络分析策略

与事件生成相关的网络分析策略 (NAP) （如有）；请参阅第 26-1 页上的网络分析策略使用入门。

HTTP Hostname

提取自 HTTP 请求主机报头的主机名 （如果有）。请注意，请求数据包并非总是包含主机名。

要显示主机名，必须启用 HTTP 检查预处理器 **Log Hostname** 选项。有关详细信息，请参阅第 27-28 页上的选择服务器级别 HTTP 规范化选项。

此列显示提取的主机名的前五十个字符。将光标悬停在缩写主机名的显示部分上可显示完整名称 （最多包含 256 个字节）。还可以在数据包视图中显示完整主机名 （最多包含 256 个字节）。有关详细信息，请参阅第 41-20 页上的查看事件信息。

默认情况下，此字段处于禁用状态。

HTTP URI

与触发入侵事件的 HTTP 请求数据包相关的原始 URI （如果有）。请注意，请求数据包并非总是包含 URI。

要显示提取的 URI，必须启用 HTTP 检查预处理器 **Log URI** 选项。有关详细信息，请参阅第 27-28 页上的选择服务器级别 HTTP 规范化选项。

要查看与 HTTP 响应触发的入侵事件相关的 HTTP URI，应配置 **Perform Stream Reassembly on Both Ports** 选项中的 HTTP 服务器端口；但请注意，这样会增加流量重组的资源需求。请参阅第 29-23 页上的选择数据流重组选项。

此列显示提取的 URI 的前五十个字符。将光标悬停在缩略 URI 的显示部分上可显示完整 URI （最多包含 2048 个字节）。还可以在数据包视图中显示完整 URI （最多包含 2048 个字节）。有关详细信息，请参阅第 41-20 页上的查看事件信息。

默认情况下，此字段处于禁用状态。

Email Sender

提取自 SMTP MAIL FROM 命令的邮件发件人的地址。要显示此字段的值，必须启用 SMTP 预处理器 **Log From Addresses** 选项。支持多个发件人地址。有关详细信息，请参阅第 27-51 页上的了解 SMTP 解码。

默认情况下，此字段处于禁用状态。

Email Recipient

提取自 SMTP RCPT TO 命令的邮件收件人的地址。要显示此字段的值，必须启用 SMTP 预处理器 **Log To Addresses** 选项。支持多个收件人地址。有关详细信息，请参阅第 27-51 页上的了解 SMTP 解码。

默认情况下，此字段处于禁用状态。

电子邮件附件

提取自 MIME Content-Disposition 报头的 MIME 附件文件名。要显示附件文件名，必须启用 SMTP 预处理器 **Log MIME Attachment Names** 选项。支持多个附件文件名。有关详细信息，请参阅第 27-51 页上的了解 SMTP 解码。

默认情况下，此字段处于禁用状态。

Reviewed By

审核事件的用户的名称。请参阅第 41-14 页上的审核入侵事件。

计数

与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

查看与入侵事件相关的连接数据

许可证：保护

系统可以记录在其中检测到入侵事件的连接。虽然会对与访问控制规则关联的入侵策略自动执行这种记录，但必须手动启用连接记录才能查看与默认操作关联的连接数据；请参阅第 38-13 页上的根据访问控制处理记录连接。

注 任何单个连接或安全情报事件的可用信息取决于多种因素，包括许可证和设备型号。有关详细信息，请参阅第 38-8 页上的连接记录的许可证和型号要求。

要查看与一个或多个入侵事件相关的连接数据，请执行以下操作：

访问：管理

步骤 1 选择 **Analysis > Intrusions > Events**。

系统显示默认入侵事件工作流程的第一个页面。

在事件的表视图之间导航时，查看相关数据最有用。请参阅第 41-15 页上的了解入侵事件的工作流程页面，以了解有关如何将视图缩小至对分析非常重要的入侵事件的详细信息。

步骤 2 使用事件查看器中的复选框选择入侵事件，然后从 **Jump to** 下拉列表选择 **Connections**。

可以使用类似方法查看与特定连接相关的入侵事件。有关详细信息，请参阅第 58-31 页上的在工作流程之间导航。

查看相关事件时，防御中心使用默认连接数据工作流程。有关连接数据的详细信息，请参阅第 39-1 页上的使用连接与安全情报数据。

提示 如果使用不包括入侵事件表视图的自定义工作流程，请点击工作流程标题旁边的 **(switch workflow)** 以选择随设备提供的任意预定义工作流程。

审核入侵事件

许可证：保护

如果检查了某个入侵事件并确信其不对网络安全构成威胁 （或许是因为您知道网络中的所有主机均不易受检测到的漏洞攻击），那么可以将事件标记为“已审核”。您的姓名将显示为审核员，已审核的事件不再列出在默认入侵事件视图中。被标记为“已审核”的事件将保留在事件数据库中，但不会再显示在入侵事件视图中。

要将入侵事件标记为“已审核”，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在显示入侵事件的页面上，您有两个选择：

- 要标记事件列表中的一个或多个入侵事件，请选择事件旁边的复选框并点击 **Review**。
- 要标记事件列表中的所有入侵事件，请点击 **Review All**。

系统显示成功消息，并且更新已审核事件的列表。

有关入侵事件视图中显示的事件的详细信息，请参阅第 41-8 页上的了解入侵事件。请参阅第 41-15 页上的了解入侵事件的工作流程页面，以了解有关如何将视图缩小至对分析非常重要的入侵事件的详细信息。

注　已审核事件会包括在事件摘要统计信息中，但不显示在与入侵事件相关的工作流程页面上。

要查看以前标记为“已审核”的事件，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Analysis > Intrusions > Reviewed Events**。

系统显示默认已审核入侵事件工作流程的第一个页面。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示任何事件，可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

提示　如果使用不包括入侵事件表视图的自定义工作流程，请点击工作流程标题旁边的 **(switch workflow)** 以选择随设备提供的任意预定义工作流程。

请参阅第 41-8 页上的了解入侵事件，以了解有关已审核入侵事件视图中显示的事件的详细信息。请参阅第 41-15 页上的了解入侵事件的工作流程页面，以了解有关如何将视图缩小至对分析非常重要的入侵事件的详细信息。

要将已审核事件标记为“未审核”，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在显示已审核事件的页面上，您有两个选择：

- 要移除已审核事件列表中的单个入侵事件，请选择事件旁边的复选框并点击 **Unreview**。
- 要从已审核事件列表移除所有入侵事件，请点击 **Unreview All**。

系统显示成功消息，并且更新已审核事件的列表。

了解入侵事件的工作流程页面

许可证：保护

如果监控的流量违反策略，当前入侵策略中启用的预处理器规则、解码器规则和入侵规则就会生成入侵事件。

FireSIGHT 系统提供一系列填充了事件数据的预定义工作流程，这些工作流程可用于查看和分析入侵事件。每个这些工作流程都会引导您浏览一系列页面，从而帮助您要确定要评估的入侵事件。

预定义的入侵事件工作流程包含三种不同类型的页面 （又称为事件视图）：

- 一个或多个下钻式页面
- 入侵事件的表视图
- 数据包视图

*下钻式页面*通常在一个表中包含两列或更多列 （对于某些下钻式视图，还可能有多于一个表），允许查看一种特定类型的信息。

“向下钻取”以查找有关一个或多个目标端口的详细信息时，将会自动选择这些事件，然后显示工作流程中的下一页。这样，下钻式表就能够帮助减少一次分析的事件数。

入侵事件的初始的*表视图*在其自身的行中列出每个入侵事件。表中的各列列出各种信息，例如，时间、源 IP 地址、源端口、目标 IP 地址、目标端口、事件优先级和事件消息，等等。

选择表视图中的事件时，可以先不选择事件并显示工作流程中的下一页，而是为事件添加*限制条件*。限制条件是对要分析的事件类型施加的限制。

例如，如果点击任何列中的关闭列图标 (✖) 并从下拉列表清除 **Time**，可以将 Time 作为一列移除。要减少分析中事件列表的事件数，可以点击表视图中任何行中某个值的链接。例如，要将分析范围缩小为从其中一个源 IP 地址 （假设是潜在攻击者）生成的事件，请点击 **Source IP Address** 列中的 IP 地址。

如果选择表中的一行或多行，然后点击 **View**，将会显示数据包视图。*数据包视图*提供有关触发生成事件的规则或预处理器的数据包的信息。数据包中的每个部分都包含有关数据包中特定层的信息。可以展开折叠的部分以了解详细信息。

注　由于每个端口扫描事件均由多个数据包触发，因此，端口扫描事件使用特殊版本的数据包视图。有关详细信息，请参阅第 34-2 页上的检测端口扫描。

如果预定义工作流程不能满足您的特定需求，您可以创建自定义工作流程，在其中仅显示您感兴趣的信息。自定义入侵事件工作流程可以包括下钻式页面和/或事件表视图；系统会自动包括数据包视图作为最后一页。根据调查事件的需要，您可以轻松地在预定义工作流程和自定义工作流程之间切换。

提示　第 58-1 页上的了解和使用工作流程说明如何使用工作流程以及通用于所有工作流程页面的功能。本章还介绍如何创建和使用自定义入侵事件工作流程。

有关详情，请参阅：

- 第 41-16 页上的使用下钻式页面和表视图页面，其中说明如何使用下钻式页面和事件表视图（两者共享许多常见功能）。
- 第 41-19 页上的使用数据包视图，其中说明如何使用数据包视图中的功能。
- 第 41-36 页上的搜索入侵事件说明如何搜索事件数据库以查找特定入侵事件。

使用下钻式页面和表视图页面

许可证：保护

可用于调查入侵事件的工作流程使用三种不同类型的页面：

- 下钻式页面
- 入侵事件的表视图
- 数据包视图

第 41-15 页上的了解入侵事件的工作流程页面中介绍了这三种页面。

事件的下钻式视图和表视图共享一些常见功能，这些功能可用于缩小事件列表，以便将分析焦点集中到一组相关事件上。下表介绍了这些功能。

表 41-2　　入侵事件常见功能

要.....	您可以.....
了解有关显示的列的详细信息	在第 41-8 页上的了解入侵事件中获得详细信息。
查看主机的配置文件	点击显示在主机 IP 地址旁边的配置文件图标 ()。
查看地理定位详细信息	点击 Source Country 或 Destination Country 列中显示的旗帜图标。
修改所显示事件的时间和日期范围	在第 58-19 页上的设置事件时间限制中获得详细信息。 请注意，如果以时间限制事件视图，在为设备配置的时间段（无论是全局还是特定于事件）之外生成的事件也可能显示在事件视图中。即使已经为设备配置一个滑动时间窗，这种情况仍然可能发生。
对当前工作流程页面上的事件进行排序和限制	在以下表中查找详细信息： • 第 58-29 页上的对向下钻取工作流程页面进行排序 • 限制下钻式页面上的事件表 • 限制事件表视图中的事件表
在当前工作流程页面中导航	在第 58-30 页上的导航到工作流程中的其他页面中获得详细信息。 **提示**　为了避免在不同的工作流程页面上显示相同的入侵事件，当您点击位于页面底部的链接显示另一页事件时，事件范围会暂停；当您在后续页面上点击以执行任何其他操作时，事件范围将会继续。有关详细信息，请参阅第 58-19 页上的设置事件时间限制。
在当前工作流程中的页面之间导航，同时保留当前限制条件	点击工作流程页面左上角的相应页面链接。有关详细信息，请参阅第 58-16 页上的使用工作流程页面。

表 41-2　　入侵事件常见功能 （续）

要.....	您可以.....
将事件添加到剪贴板，以便以后将其传输到事故	可使用以下其中一种方法： • 要将工作流程页面上的多个入侵事件复制到剪贴板，请选择要复制的事件旁边的复选框，然后点击 **Copy**。 • 要将当前受限制视图中的所有入侵事件复制剪贴板，请点击 **Copy All**。 剪贴板可为每个用户存储最多 25000 个事件。有关详细信息，请参阅第 41-42 页上的使用剪贴板。
从事件数据库删除事件	可使用以下其中一种方法： • 要删除选定的入侵事件，请选择要删除的事件旁边的复选框，然后点击 **Delete**。 • 要删除当前受限制视图中的所有入侵事件，请点击 **Delete All**，然后确认要删除所有事件。
将事件标记为“已审核”以其从入侵事件页面上移除，但不将其从事件数据库中移除	可使用以下其中一种方法： • 要审核选定的入侵事件，请选择要审核的事件旁边的复选框，然后点击 **Review**。 • 要审核当前受限制视图中的所有入侵事件，请点击 **Review All**。 有关详细信息，请参阅第 41-14 页上的审核入侵事件。
下载触发每个选定事件的数据包（数据包以 libpcap 格式捕获文件）的本地副本	可使用以下其中一种方法： • 要下载触发选定入侵事件的数据包，请选择要下载的数据包所触发的事件旁边的复选框，然后点击 **Download Packets**。 • 要下载触发当前受限制视图中的入侵事件的所有数据包，请点击 **Download All Packets**。 捕获的数据包以 libpcap 格式保存。多个常用的协议分析器均使用此格式。
导航至其他事件视图查看相关事件	在第 58-31 页上的在工作流程之间导航中获得详细信息。
暂时使用不同的工作流程	点击 **(switch workflow)**。有关详细信息，请参阅第 58-14 页上的选择工作流程。
为当前页面添加书签以便快速返回到该页面	点击 **Bookmark This Page**。有关详细信息，请参阅第 58-32 页上的使用书签。
查看 Summary 控制面板的 Intrusion Events 部分	点击 **Dashboards**。有关详细信息，请参阅第 55-31 页上的使用控制面板。
导航到书签管理页面	点击 **View Bookmarks**。有关详细信息，请参阅第 58-32 页上的使用书签。
根据当前视图中的数据生成报告	点击 **Report Designer**。有关详细信息，请参阅第 57-8 页上的从事件视图创建报告模板。

事件视图中显示的入侵事件数可能很大，具体取决于：

- 选择的时间范围
- 网络流量
- 应用的入侵策略

为了便于分析入侵事件，可以对事件页面施加限制。对于下钻式视图和表视图，限制过程略有不同。

提示　当您点击入侵事件工作流程页面底部的其中一个链接导航到其他页面时，时间范围会暂停，当您在后续页面上点击以执行其他操作 （包括退出工作流程）时，时间范围将会继续；这样可降低发生这样一种情况的可能性：导航到其他页面查看更多事件却仍看到原来的事件。有关详细信息，请参阅第 58-19 页上的设置事件时间限制和第 58-30 页上的导航到工作流程中的其他页面。

下表介绍如何使用下钻式页面。

表 41-3　限制下钻式页面上的事件

要.....	您可以.....
向下钻取到下一个限制特定值的工作流程页面	点击该值。 例如，在 Destination Port 工作流程中，要将事件限制为目标端口为 80 端口的事件，请点击 **DST Port/ICMP Code** 列中的 **80/tcp**。屏幕上将会显示工作流程的下一页 （Events 页面），其中仅包含 80/tcp 端口事件。
向下钻取到下一个限制选定事件的工作流程页面	选择要在下一个工作流程页面上查看的事件旁边的复选框，然后点击 **View**。 例如，在 Destination Port 工作流程中，要将事件限制为目标端口为 20/tcp 和 21/tcp 端口的事件，请选择这些端口对应行旁边的复选框，然后点击 **View**。屏幕上将会显示工作流程的下一页 （Events 页面），其中仅包含 20/tcp 和 21/tcp 端口事件。 **注**　如果对多行施加限制，并且表不止包含一列 （Count 列不算在内），将会产生“复合限制条件”。复合限制条件确保仅将计划内的事件纳入限制中。例如，如果使用 Event and Destination 工作流程，在第一个向下钻取页面上选择的每一行都会创建一个复合限制条件。如果选择目标 IP 地址为 10.10.10.100 的事件 1:100，并且选择目标 IP 地址为 192.168.10.100 的事件 1:200，那么，复合限制条件确保您不会选择事件类型为 1:100 且目标 IP 地址为 192.168.10.100 的事件或事件类型为 1:200 且目标 IP 地址为 10.10.10.100 的事件。
向下钻取到下一个保留当前限制的工作流程页面	点击 **View All**。

下表介绍如何使用表视图。

表 41-4　限制事件表视图中的事件

要.....	您可以.....
将视图限制为仅显示具有单个属性的事件	点击该属性。 例如，要将视图限制为仅显示目标端口为 80 端口的事件，请点击 **DST Port/ICMP Code** 列中的 **80/tcp**。
从表中移除列	在要隐藏的列标题中点击关闭图标 (✖)。在显示的弹出窗口中，点击 **Apply**。 **提示**　要隐藏或显示其他列，选择或清除相应的复选框，然后点击 **Apply**。要将已禁用的列重新添加到视图中，点击展开箭头 (▶) 展开搜索条件，然后点击 **Disabled Columns** 列下的列名。
查看与一个或多个事件相关的数据包	执行以下其中一种操作： • 点击要查看的数据包的事件旁边的向下箭头图标 (⬇)。 • 选择要查看的一个或多个数据包，然后点击页面底部的 **View**。 • 在页面底部，点击 **View All** 查看与当前限制条件匹配的所有事件。

提示　在操作过程中，可以随时将限制条件保存为一组搜索条件。例如，如果您发现几天内您的网络被来自某个 IP 地址的攻击者探测，您可以在调查期间保存限制条件，以供日后再次使用。但是，不能将复合限制条件保存为一组搜索条件。有关详细信息，请参阅第 60-1 页上的执行和保存搜索。

提示　如果入侵事件未显示在事件视图中，调整选定时间范围可能会返回结果。建议不要选择旧的时间范围，因为旧时间范围内的事件可能已被删除。调整规则阈值配置可能生成事件。

使用数据包视图

许可证：保护

数据包视图提供有关触发生成入侵事件的规则的数据包的信息。

提示　如果检测事件的设备的 **Transfer Packet** 选项处于禁用状态，防御中心 上的数据包视图不包含数据包信息。

数据包视图通过提供有关数据包触发的入侵事件的信息指示捕获特定数据包的原因，这些信息包括事件的时间戳、消息、分类和优先级 （如果事件由标准文本规则生成，还包括生成事件的规则）。数据包视图还提供有关数据包的一般信息 （例如大小）。

此外，数据包视图还有一个介绍数据包中每一层 （数据链路层、网络层和传输层）的部分，以及一个介绍组成数据包的字节的部分。如果系统已解密数据包，可以查看解密的字节。可以展开折叠的部分以显示详细信息。

注　由于每个端口扫描事件均由多个数据包触发，因此，端口扫描事件使用特殊版本的数据包视图。有关详细信息，请参阅第 34-2 页上的检测端口扫描。

下表介绍在数据包视图中可以执行的操作。

表 41-5　数据包视图操作

要.....	您可以.....
修改数据包视图中的日期和时间范围	在第 58-19 页上的设置事件时间限制中获得详细信息。
了解有关数据包视图中所显示信息的详细信息	在以下表中查找详细信息： • 第 41-20 页上的查看事件信息 • 第 41-26 页上的查看帧信息 • 第 41-27 页上的查看数据链路层信息 • 第 41-27 页上的查看网络层信息 • 第 41-29 页上的查看传输层信息 • 第 41-32 页上的查看信息包字节信息

表 41-5　　数据包视图操作（续）

要.....	您可以.....
将事件添加到剪贴板，以便以后将其传输到事故	执行以下其中一种操作： • 点击 **Copy** 以复制正在查看其数据包的事件 • 点击 **Copy All** 以复制之前选择了其数据包的所有事件 剪贴板可为每个用户存储最多 25000 个事件。有关剪贴板的详细信息，请参阅第 41-42 页上的使用剪贴板。
从事件数据库删除事件	执行以下其中一种操作： • 点击 **Delete** 以删除正在查看其事件的数据包 • 点击 **Delete All** 以删除之前选择了其数据包的所有事件
将事件标记为“已审核”会将其从事件视图中移除，但不会将其从事件数据库中移除	执行以下其中一种操作： • 点击 **Review** 以审核正在查看其事件的数据包 • 点击 **Review All** 以审核之前选择了其数据包的所有事件 有关详细信息，请参阅第 41-14 页上的审核入侵事件。请注意，已审核事件将继续包括在 Intrusion Event Statistics 页面的事件统计信息中。
下载触发事件的数据包（数据包以 libpcap 格式捕获文件）的本地副本	执行以下其中一种操作： • 点击 **Download Packet** 以保存为正在查看的事件捕获的数据包的副本。 • 点击 **Download All Packets** 以保存为之前选择了其数据包的所有事件捕获的数据包的副本 捕获的数据包以 libpcap 格式保存。多个常用的协议分析器均使用此格式。 请注意，无法下载端口扫描数据包，因为单个端口扫描事件基于多个数据包；但端口扫描视图提供所有可用的数据包信息。有关详细信息，请参阅第 34-6 页上的了解端口扫描事件。 请注意，要下载，必须至少有 15% 的可用磁盘空间。
展开或折叠页面部分	点击要展开或折叠的部分旁边的箭头。

要显示数据包视图，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在入侵事件的表视图中，选择要查看的数据包。有关详细信息，请参阅限制事件表视图中的事件表。

系统显示数据包视图。如果选择多个事件，可以使用页面底部的页码来浏览多个页面上的数据包。

查看事件信息

许可证：保护

在数据包视图上，可以查看有关 Event Information 部分中数据包的信息。

Event

事件消息。对于基于规则的事件，这相当于规则消息。对于其他事件，这取决于解码器或预处理器。

事件 ID 以 *(GID:SID:Rev)* 格式附加在消息后面。*GID* 是生成事件的规则引擎、解码器或预处理器的生成器 ID。*SID* 是规则、解码器消息或预处理器消息的标识符。*Rev* 是规则的修订号。有关详细信息，请参阅第 41-34 页上的解读预处理器生成器 ID。

Timestamp

捕获数据包的时间。

Classification

事件分类。对于基于规则的事件，这相当于规则分类。对于其他事件，这取决于解码器或预处理器。

Priority

事件优先级。对于基于规则的事件，这相当于 `priority` 关键字或 `classtype` 关键字的值。对于其他事件，这取决于解码器或预处理器。

Ingress Security Zone

触发事件的数据包的入口安全区域。在被动部署中仅填充此安全区域字段。请参阅第 3-34 页上的使用安全区域。

Egress Security Zone

对于内联部署，触发事件的数据包的出口安全区域。请参阅第 3-34 页上的使用安全区域。

设备

应用访问控制策略的受管设备。请参阅第 4-1 页上的管理设备。

安全情景

识别流量通过的虚拟防火墙组的元数据。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。

Ingress Interface

触发事件的数据包的入口接口。对于被动接口，仅填充此接口列。请参阅第 4-52 页上的配置感应接口。

Egress Interface

对于内联部署，触发事件的数据包的出口接口。请参阅第 4-52 页上的配置感应接口。

Source/Destination IP

触发事件的数据包源自的 （源）主机 IP 地址或域名，或触发事件的流量的目标主机。

请注意，要显示域名，必须启用 IP 地址解析；有关详细信息，请参阅第 71-3 页上的配置事件查看设置。

点击地址或域名查看上下文菜单，然后选择 **Whois** 可在主机上执行 whois 搜索，选择 **View Host Profile** 可查看主机信息，选择 **Blacklist Now** 或 **Whitelist Now** 可将地址添加到全局黑名单或白名单。请参阅第 49-1 页上的使用主机配置文件和第 3-6 页上的使用全局白名单和黑名单。

Source Port/ICMP Type

触发事件数据包的源端口。对 ICMP 流量，当没有端口号时，系统显示 ICMP 类型。

Destination Port/ICMP Code

接收流量的主机的端口号。对 ICMP 流量，当没有端口号时，系统显示 ICMP 代码。

Email Headers

提取自邮件报头的数据。请注意，邮件报头不显示在入侵事件表视图中，但可以将邮件报头数据作为搜索条件。

要将邮件报头与 SMTP 流量的入侵事件相关联，必须启用 SMTP 预处理器 **Log Headers** 选项。有关详细信息，请参阅第 27-51 页上的了解 SMTP 解码。对基于规则的事件，提取邮件数据时会显示此行。

HTTP Hostname

提取自 HTTP 请求主机报头的主机名 （如果有）。此行显示完整的主机名 （最多包含 256 个字节）。如果主机名超过一行，点击展开箭头 ( ) 可显示完整的主机名。

要显示主机名，必须启用 HTTP 检查预处理器 **Log Hostname** 选项。有关详细信息，请参阅第 27-28 页上的选择服务器级别 HTTP 规范化选项。

请注意，HTTP 请求数据包并非总是包含主机名。对于基于规则的事件，当数据包包含 HTTP 主机名或 HTTP URI 时，会显示此行。

HTTP URI

与触发入侵事件的 HTTP 请求数据包相关的原始 URI （如果有）。此行显示完整 URI （最多包含 2048 个字节）。如果完整 URI 超过一行，点击展开箭头 ( ) 可显示完整 URI。

要显示 URI，必须启用 HTTP 检查预处理器 **Log URI** 选项。有关详细信息，请参阅第 27-28 页上的选择服务器级别 HTTP 规范化选项。

请注意， HTTP 请求数据包并非总是包含 URI。对于基于规则的事件，当数据包包含 HTTP 主机名或 HTTP URI 时，会显示此行。

要查看与 HTTP 响应触发的入侵事件相关的 HTTP URI，应配置 **Perform Stream Reassembly on Both Ports** 选项中的 HTTP 服务器端口；但请注意，这样会增加流量重组的资源需求。请参阅第 29-23 页上的选择数据流重组选项。

Intrusion Policy

启用了生成入侵事件的入侵规则、预处理器规则或解码器规则的入侵策略 （如果有）。可以选择入侵策略作为访问控制策略的默认操作，也可以将入侵策略与访问控制规则关联起来。请参阅第 12-6 页上的设置对网络流量的默认处理和检查和第 18-5 页上的配置访问控制规则以执行入侵防御。

访问控制策略

包含启用了生成事件的入侵规则、预处理器规则或解码器规则的入侵策略的访问控制策略。请参阅第 12-9 页上的管理访问控制策略。

Access Control Rule

与生成事件的入侵规则相关的访问控制规则；请参阅第 18-5 页上的配置访问控制规则以执行入侵防御。 `Default Action` 指出启用了规则的入侵政策未与访问控制规则关联，但被配置为访问控制策略的默认操作；请参阅第 12-6 页上的设置对网络流量的默认处理和检查。

Rule

对于标准文本规则事件，生成事件的规则。

请注意，如果事件基于共享对象规则、解码器或预处理器，规则不可用。

由于规则数据可能包含有关网络的敏感信息，管理员可以使用用户角色编辑器中的 View Local Rules 权限来设置用户查看数据包视图中的规则信息的权限。有关详细信息，请参阅第 61-50 页上的修改用户权限和选项。

行动

对于标准文本规则事件，展开 **Actions** 以对触发事件的规则执行下列任一操作：

- 编辑规则
- 查看有关规则修订的文档
- 向规则添加注释
- 更改规则的状态
- 设置规则的阈值
- 抑制规则

有关详细信息，请参阅第 41-23 页上的使用数据包视图操作、第 41-24 页上的在数据包视图内设置阈值选项和第 41-25 页上的在数据包视图中设置抑制选项。

请注意，如果事件基于共享对象规则、解码器或预处理器，规则不可用。

使用数据包视图操作

许可证：保护

在数据包视图中，可以对触发事件的规则执行 Event Information 部分中的多个操作。请注意，如果事件基于共享对象规则、解码器或预处理器，规则不可用。必须展开 **Actions** 显示规则操作。

编辑

对于标准文本规则事件，点击 **Edit** 可修改生成事件的规则。

请注意，如果事件基于共享对象规则、解码器或预处理器，规则不可用。

注 如果编辑由思科提供的规则（而不是自定义标准文本规则），实际上会创建新的本地规则。请确保将本地规则设置为生成事件，并禁用当前入侵策略中的原始规则。但请注意，**不能**启用默认策略中的本地规则。有关详细信息，请参阅第 36-95 页上的修改现有规则。

View Documentation

对于标准文本规则事件，点击 **View Documentation** 了解有关生成事件的规则修订版的详细信息。

Rule Comment

对于标准文本规则事件，点击 **Rule Comment** 可以向生成事件的规则添加文本注释。

这样做可以提供有关规则以及其识别出的漏洞或策略违规的额外上下文和信息。还可以在规则编辑器中添加和查看规则注释。有关详细信息，请参阅第 36-96 页上的向规则添加注释。

Disable this rule

如果事件由标准文本规则生成，必要时可以禁用此规则。可以在能够在本地编辑的所有策略中设置此规则。或者，如果您能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置此规则。

有关详细信息，请参阅第 32-18 页上的设置规则状态。

请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认策略。

注 **不能**从数据包视图禁用共享对象规则，也不能禁用默认策略中的规则。

Set this rule to generate events

如果事件由标准文本规则生成，可以在能够在本地编辑的所有策略中设置此规则以生成事件。或者，如果您能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置此规则。

有关详细信息，请参阅第 32-18 页上的设置规则状态。

请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认策略。

注　不能从数据包视图设置共享对象规则以生成事件，也不能禁用默认策略中的规则。

Set this rule to drop

如果受管设备在网络中以内联方式部署，可以在能够在本地编辑的所有策略中将触发事件的规则设置为丢弃触发该规则的数据包。或者，如果您能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置此规则。

请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认策略。请注意，仅在当前策略中启用了 **Drop when Inline** 的情况下，才会显示此选项。有关详细信息，请参阅第 31-5 页上的在内联部署中设置丢弃行为。

Set Thresholding Options

可以使用此选项在能够在本地编辑的所有策略中为触发此事件的规则创建阈值。或者，如果能够在本地编辑当前策略，可以仅为当前策略（即，生成事件的策略）创建阈值。

第 41-24 页上的在数据包视图内设置阈值选项中介绍了阈值选项。

请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认入侵策略。

Set Suppression Options

可以使用此对象在能够在本地编辑的所有策略中抑制触发此事件的规则。或者，如果能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中抑制此规则。

第 41-25 页上的在数据包视图中设置抑制选项中介绍了抑制选项。

请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认策略。

在数据包视图内设置阈值选项

许可证：保护

通过在入侵事件的数据包视图中设置阈值选项，可以控制每个规则随时间推移生成的事件数。可以在能够在本地编辑的所有策略中设置阈值选项；或者，如果能够在本地编辑策略，可以仅在当前策略（即，导致事件生成的策略）中设置阈值选项。

要在数据包视图中设置阈值选项，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在入侵规则生成的入侵事件的数据包视图中，展开 Event Information 部分的 **Actions**；展开 **Set Thresholding Options** 并选择以下两个选项之一：

- **in the current policy**
- **in all locally created policies**

请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认策略。

系统显示阈值选项。

步骤 2　选择要设置的阈值的类型。

- 选择 **limit** 以将通知限制为每个时间段内仅为指定数目的事件实例提供通知。
- 选择 **threshold** 为每个时间段内每发生指定数目的事件实例提供通知。
- 选择 **both** 在每个时间段内发生指定数目的事件实例后提供一次通知。

步骤 3　选择适当的单选按钮，以指明是要按**源**还是**目标** IP 地址跟踪事件实例。

步骤 4　在 **Count** 字段中，键入要用作阈值的事件实例数。

步骤 5　在 **Seconds** 字段中，键入一个 1 和 86400 之间的数字来指定跟踪事件实例的时间段。

步骤 6　如果要覆盖现有入侵策略中的规则的所有当前阈值，请选择 **Override any existing settings for this rule**。

步骤 7　点击 **Save Thresholding**。

系统添加阈值并显示成功消息。如果选择不覆盖现有设置，屏幕上将会显示一条消息，通知您出现冲突。

在数据包视图中设置抑制选项

许可证：保护

可以使用抑制选项抑制全部入侵事件或者基于源或目标 IP 地址抑制入侵事件。可在在能够在本地编辑的所有策略中设置抑制选项。或者，如果能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置抑制选项。

要在数据包视图中抑制入侵事件，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　在入侵规则生成的入侵事件的数据包视图中，展开 Event Information 部分的 **Actions**；展开 **Set Suppression Options** 并点击以下两个选项之一：

- **in the current policy**
- **in all locally created policies**

请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认策略。

系统显示抑制选项。

步骤 2　选择以下其中一个 **Track By** 选项：

- 要完全抑制触发此事件的规则的事件，请选择 **Rule**。
- 要抑制由源自指定源 IP 地址的数据包生成的事件，请选择 **Source**。
- 要抑制发送到指定目标 IP 地址的数据包生成的事件，请选择 **Destination**。

步骤 3　在 **IP address or CIDR block** 字段中，输入要指定为源或目标 IP 地址的 IP 地址或 CIDR 块/前缀长度。

有关在 FireSIGHT 系统中使用 CIDR 表示法和前缀长度的信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 4　点击 **Save Suppression**。

系统会根据您的选择修改入侵策略中的抑制选项。如果选择不覆盖现有设置，屏幕上将会显示一条消息，通知您出现冲突。

查看帧信息

许可证：保护

在数据包视图中，点击 **Frame** 旁边的箭头可查看捕获的帧的信息。数据包视图可以显示单个帧或多个帧。每个帧提供有关单个网络数据包的信息。您会看到多个帧，例如，对于已标记的数据包或重组的 TCP 数据流中的数据包。有关已标记的数据包的信息，请参阅第 36-81 页上的评估攻击后流量。有关重组的 TCP 数据流的信息，请参阅第 29-23 页上的重组 TCP 数据流。

Frame n

捕获的帧，其中，*n* 为 1 （对于单帧数据包）或递增帧编号 （对于多帧数据包）。帧中捕获的字节数将附加到帧编号后面。

Arrival Time

捕获帧的日期和时间。

Time delta from previous captured frame

对于多帧数据包，表示自捕获上一个帧以来经过的时间。

Time delta from previous displayed frame

对于多帧数据包，表示自显示上一个帧以来经过的时间。

Time since reference or first frame

对于多帧数据包，表示自捕获第一个帧以来经过的时间。

Frame Number

递增的帧编号。

Frame Length

帧的长度，以字节为单位。

Capture Length

捕获的帧的长度，以字节为单位。

Frame is marked

帧是否被标记 （true 或 false）。

Protocols in frame

帧中包括的协议。

查看数据链路层信息

许可证：保护

在数据包视图中，点击数据链路层协议（例如，**Ethernet II**）旁边的箭头可查看有关数据包的数据链路层信息，这些信息包括源主机和目标主机的 48 位介质访问控制 (MAC) 地址。它还可能显示有关数据包的其它信息，取决于硬件协议。

注　请注意，本示例讨论以太网链路层信息；也可能出现其他协议。

数据包视图反映数据链路层使用的协议。以下列表说明在数据包视图中可能会看到的以太网 II 或 IEEE 802.3 以太网数据包的信息。

目标

目标主机的 MAC 地址。

注　以太网还可以使用组播地址和广播地址作为目标地址。

信息来源

源主机的 MAC 地址。

类型

对于以太网 II 数据包，代表在以太网帧中封装的数据包的类型；例如，IPv6 或 ARP 数据报。请注意，此项目仅对以太网 II 数据包显示。

长度

对于 IEEE 802.3 以太网数据包，代表数据包的长度（以字节为单位，不包括校验和）。请注意，此项目仅对 IEEE 802.3 以太网数据包显示。

查看网络层信息

许可证：保护

在数据包视图中，点击网络层协议（例如，**Internet Protocol**）旁边的箭头可查看有关与数据包相关的网络层的更多详细信息。

注　请注意，本示例讨论 IP 数据包；也可能出现其他协议。

有关详细信息，请参阅以下各节：

- 第 41-28 页上的查看 IPv4 网络层信息
- 第 41-29 页上的查看 IPv6 网络层信息

查看 IPv4 网络层信息

许可证：保护

以下列表说明在 IPv4 数据包中可能显示的特定于协议的信息。

版本

互联网协议的版本号。

Header Length

报头 （包括任何 IP 选项）中的字节数。不带选项的 IP 报头的长度为 20 字节。

Differentiated Services Field

差分服务的值，用以指明发送主机如何支持显式堵塞通知 (ECN)：

- `0x0` - 不支持具有 ECN 功能的传输 (ECT)
- `0x1` 和 `0x2` - 支持 ECT
- `0x3` - 堵塞情况 (CE)

Total Length

IP 数据包的长度 （以字节为单位，不包括 IP 报头在内）。

确定

唯一标识源主机发送的 IP 数据报的值。此值用于跟踪同一数据报的数据分片。

Flags

控制 IP 分片的值，其中：

Last Fragment 标志的值指明是否有更多与数据报相关的分片。

- `0` - 没有更多与数据报相关的分片
- `1` - 有更多与数据报相关的分片

Don’t Fragment 标志的值控制数据报是否可以分片：

- `0` - 数据报可以分片
- `1` - 数据报不可分片

Fragment Offset

自数据报开始以来分片偏移量的值。

Time to Live (ttl)

数据包在过期之前可以在路由器之间跳转的剩余跳数。

协议

封装在 IP 数据报中的传输协议；例如， ICMP、 IGMP、 TCP 或 UDP。

Header Checksum

指明 IP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏或可能正被用于躲避入侵。

Source/Destination

源（或目标）主机的 IP 地址或域名。

请注意，要显示域名，必须启用 IP 地址解析；有关详细信息，请参阅第 71-3 页上的配置事件查看设置。

点击地址或域名查看上下文菜单，然后选择 **Whois** 可在主机上执行 whois 搜索，选择 **View Host Profile** 可查看主机信息，选择 **Blacklist Now** 或 **Whitelist Now** 可将地址添加到全局黑名单或白名单。请参阅第 49-1 页上的使用主机配置文件和第 3-6 页上的使用全局白名单和黑名单。

查看 IPv6 网络层信息

许可证：保护

以下列表说明在 n IPv6 数据包中可能出现的特定于协议的信息。

Traffic Class

IPv6 报头中的试验性 8 位字段，用于识别 IPv6 数据包类别或优先级，类似于 IPv4 提供的差分服务功能。未使用时，此字段设为零。

Flow Label

可选的 20 位 IPv6 十六进制值（从 1 到 FFFFF），用于识别特殊流（例如，非默认服务质量和实时服务）。未使用时，此字段设为零。

Payload Length

表示 IPv6 负载中八位组数的 16 位字段，负载由 IPv6 报头后面的所有数据包组成，包括任何扩展报头。

Next Header

表示紧随 IPv6 报头之后的报头类型的 8 位字段，使用与 IPv4 协议字段相同的值。

Hop Limit

一个 8 位十进制整数，其中用于转发数据包的每个节点每次减 1。如果递减的值达到零，则丢弃数据包。

信息来源

源主机的 128 位 IPv6 地址。

目标

目标主机的 128 位 IPv6 地址。

查看传输层信息

许可证：保护

在数据包视图中，点击传输层协议（例如，**TCP**、**UDP** 或 **ICMP**）旁边的箭头可查看有关数据包的详细信息。

提示 点击 **Data**（如果显示）可在紧接其上方的数据包视图的 Packet Information 部分中查看协议负载的前二十四个字节。

以下协议的传输层的内容如下所述：

- 第 41-30 页上的 TCP 数据包视图
- 第 41-31 页上的 UDP 数据包视图
- 第 41-31 页上的 ICMP 数据包视图

注　请注意，这些示例讨论 TCP、 UDP 和 ICMP 数据包；也可能出现其他协议。

TCP 数据包视图

许可证：保护

本节介绍 TCP 数据包的特定于协议的信息。

Source port

用于识别发起应用协议的编号。

目标端口

用于识别接收应用协议的编号。

Sequence number

当前 TCP 分段中第一个字节的值，包含在 TCP 数据流中的初始序列号中。

Next sequence number

在响应数据包中，要发送的下一个数据包的序列号。

Acknowledgement number

TCP 确认，包含在之前接受的数据的序列号中。

Header Length

报头中的字节数。

Flags

六位，表示 TCP 分段的传输状态：

- U - 紧急指针有效
- A - 确认号有效
- P - 接收方应推送数据
- R - 重置连接
- S - 同步序列号以开始新连接
- F - 发送方完成发送数据

Window size

接收主机将接受的未确认数据数量 （以字节为单位）。

Checksum

指明 TCP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏或可能正被用于躲避入侵。

Urgent Pointer

TCP 分段中发送紧急数据的位置 （如果存在）。与 u 标记一起使用。

选项

TCP 选项的值 （如果有）。

UDP 数据包视图

许可证：保护

本节介绍 UDP 数据包的特定于协议的信息。

Source port

用于识别发起应用协议的编号。

目标端口

用于识别接收应用协议的编号。

长度

UDP 报头和数据的总长度。

Checksum

指明 UDP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏。

ICMP 数据包视图

许可证：保护

本节介绍 ICMP 数据包的特定于协议的信息。

类型

ICMP 消息的类型：

- 0 - 回应应答
- 3 - 目标不可达
- 4 - 源抑制
- 5 - 重定向
- 8 - 回应请求
- 9 - 路由器通告
- 10 - 路由器请求
- 11 - 超时
- 12 - 参数问题
- 13 - 时间戳请求

– 14 - 时间戳应答
– 15 - 信息请求 （过时）
– 16 - 信息应答 （过时）
– 17 - 地址掩码请求
– 18 - 地址掩码应答

代码

ICMP 消息类型随附的代码。 ICMP 消息类型 3、 5、 11 和 12 都有一个相应的代码，如 RFC 792 中所述。

Checksum

指名 ICMP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏。

查看信息包字节信息

许可证：保护

在数据包视图中，点击 **Packet Bytes** 旁边的箭头可查看构成数据包的字节的十六进制和 ASCII 版本。如果系统已解密流量，可以查看解密的数据包字节。

使用影响级别评估事件

许可证：保护

为了帮助评估事件对网络的影响，防御中心在入侵事件的表视图中显示影响级别。对于每一个事件，防御中心都会添加影响级别图标，其颜色表示入侵数据、网络发现数据和漏洞信息之间的相关性。

注 对于基于 NetFlow 数据添加到网络映射的主机，没有任何操作系统信息可用，因此，防御中心无法为涉及这些主机的入侵事件分配 Vulnerable （影响级别 1：红色）影响级别，除非您使用主机输入功能手动设置主机操作系统身份。

下表介绍了影响级别的可能值。

表 41-6　　影响级别

影响级别	漏洞	颜色	说明
0	未知	灰色	源主机和目标主机都不在由网络发现监控的网络上。
1	较弱	红色	存在以下其中一种情况： • 源主机或目标主机在网络映射中，并且漏洞已映射到主机 • 源主机或目标主机可能已被病毒、特洛伊木马或其他恶意软件感染；有关详细信息，请参阅第 36-41 页上的设置影响级别 1

表 41-6　影响级别（续）

影响级别	漏洞	颜色	说明
2	Potentially Vulnerable	橙色	源主机或目标主机在网络映射中，并且下列情况之一属实： • 对于面向端口的流量，端口正在运行服务器应用协议 • 对于非面向端口的流量，主机使用该协议
3	Currently Not Vulnerable	yellow	源主机或目标主机在网络映射中，并且下列情况之一属实： • 对于面向端口的流量（例如 TCP 或 UDP），端口不处于打开状态 • 对于非面向端口的流量（例如 ICMP），主机不使用该协议
4	Unknown Target	蓝色	源主机或目标主机在受监控网络上，但网络映射中没有该主机的条目。

要使用表视图上的影响级别评估事件，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Analysis > Intrusions > Events**。

系统显示默认入侵事件工作流程的第一个页面。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示任何事件，可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

步骤 2　限制事件视图仅查看要评估的那些事件。

有关详细信息，请参阅第 41-16 页上的使用下钻式页面和表视图页面。

步骤 3　点击页面顶部的 **Table View of Events**。

系统显示事件的表视图 **Impact** 可以是影响级别表中所述的任何值。

步骤 4　要按影响级别对表格进行排序，请点击 **Impact**。

事件将按影响级别排序。

提示　要反转排序顺序，请再次点击 **Impact**。

解读预处理器事件

许可证：保护

预处理器提供两项功能：对数据包执行指定的操作（例如，解码和规范化 HTTP 流量）以及报告指定的预处理器选项的执行情况；其做法是，每当数据包触发该预处理器选项并且已启用相关预处理器规则时就生成事件（例如，可以启用 `Double Encoding` HTTP 检查选项以及具有 HTTP 检查生成器ID (GID) 为 119 且 Snort ID (SID) 未 2 的相关预处理器规则，以在预处理器遇到 IIS 双编码流量时生成事件）。生成事件来报告预处理器的执行情况有助于检测异常协议漏洞攻击。例如，攻击者可以制造重叠的 IP 片段来对主机进行 DoS 攻击。 IP 分片重组预处理器可以检测此类攻击并为之生成入侵事件。

有关详细信息，请参阅以下各节：

- 第 41-34 页上的了解预处理器事件数据包显示介绍预处理器生成的事件中包含的信息。
- 第 41-34 页上的解读预处理器生成器 ID 详细介绍预处理器生成器 ID 提供的信息。

了解预处理器事件数据包显示

许可证：保护

预处理器事件与规则事件的不同之处在于，数据包显示不包含对事件的详细规则说明。相反，数据包显示的是事件消息、生成器 ID、 Snort ID、数据包报头数据和数据包负载。这让您可以分析数据包的报头信息，确定数据包的报头选项是否正在使用以及它们是否会令系统出现漏洞，并检查数据包负载。预处理器分析每个数据包后，规则引擎对其执行适当的规则 （如果预处理器能够整理数据包并将其作为有效会话的一部分），进一步分析潜在内容级别的威胁并提供相关报告。

解读预处理器生成器 ID

许可证：保护

每个预处理器都有自己的生成器 ID （即 GID），用以指明数据包触发的是哪个预处理器。某些预处理器还具有相关 SID，这是用于对潜在攻击进行分类的 ID 编号。这有助于通过对事件类型进行分类从而更有效地分析事件，就像规则的 Snort ID (SID) 能提供数据包触发规则的上下文一样。可以在入侵策略“规则”页面的“预处理器”筛选组中按预处理器列出预处理器规则；还可以在“类别”筛选组的预处理器和数据包解码器子组中列出预处理器规则。有关详细信息，请参阅第 32-1 页上的使用规则调整入侵策略和第 32-2 页上的表 32-1。

注　由标准文本规则生成的事件带有生成器 ID 1。事件的 SID 指明触发的是哪条具体规则。对于共享对象规则，事件带有一个生成器 ID 3 和一个用以指明触发了哪条具体规则的 SID。

下表介绍了生成每个 GID 的事件的类型。

表 41-7　　生成器 ID

ID	组件	说明	有关详细信息，请参阅.....
1	标准文本规则	数据包触发标准文本规则时生成此事件。	第 32-2 页上的表 32-1
2	带标记数据包	事件由标记生成器生成 （标记生成器会根据带标记会话生成数据包）。使用 `tag` 规则选项时会出现这种情况。	第 36-81 页上的评估攻击后流量
3	共享对象规则	数据包触发共享对象规则时生成此事件。	第 32-2 页上的表 32-1
102	HTTP 解码器	解码器引擎解码数据包中的 HTTP 数据。	第 27-26 页上的解码 HTTP 流量
105	Back Orifice 检测器	Back Orifice 检测器检测到与数据包关联的一个 Back Orifice 攻击。	第 34-1 页上的检测 Back Orifice
106	RPC 解码器	RPC 解码器解码数据包。	第 27-39 页上的使用 Sun RPC 预处理器
116	数据包解码器	事件由数据包解码器生成。	第 29-14 页上的了解数据包解码

表 41-7　　生成器 ID （续）

ID	组件	说明	有关详细信息，请参阅.....
119、120	HTTP 检查预处理器	事件由 HTTP 检查预处理器生成。 GID 120 规则与服务器特定 HTTP 流量相关。	第 27-26 页上的解码 HTTP 流量
122	端口扫描检测器	事件由端口扫描流量检测器生成。有关详细信息，请参阅	第 34-2 页上的检测端口扫描
123	IP 分片重组器	分片的 IP 数据报不能正确重组时生成事件。	第 29-10 页上的对 IP 数据包进行分片重组
124	SMTP 解码器	SMTP 预处理器检测到针对 SMTP 谓词的漏洞时生成事件。	第 27-51 页上的了解 SMTP 解码
125	FTP 解码器	FTP/Telnet 解码器检测到 FTP 流量中有漏洞时生成事件。	第 27-19 页上的了解服务器级别 FTP 选项 第 27-24 页上的了解客户端级别 FTP 选项
126	Telnet 解码器	FTP/Telnet 解码器检测到 Telnet 流量中有漏洞时生成事件。	第 27-16 页上的解码 FTP 和 Telnet 流量
128	SSH 预处理器	SSH 预处理器检测到 SSH 流量中的漏洞时生成事件。	第 27-57 页上的使用 SSH 预处理器检测攻击
129	数据流预处理器	在数据流预处理器对数据流进行预处理期间生成事件。	第 29-18 页上的使用 TCP 数据流预处理
131	DNS 预处理器	事件由 DNS 预处理器生成。	第 27-13 页上的检测 DNS 域称服务器响应中的漏洞
133	DCE/RPC 预处理器	事件由 DCE/RPC 预处理器生成。	第 27-2 页上的解码 DCE/RPC 流量
134	规则延迟 数据包延迟	规则延迟暂停 (134:1) 或重新启用 (134:2) 一组入侵规则时，或者由于超出数据包延迟阈值而使系统停止检查数据包 (134:3) 时，生成事件。	第 18-10 页上的配置数据包和入侵规则延迟阈值
135	基于速率的攻击检测器	基于速率的攻击检测器识别到网络上的主机存在过多连接时生成事件。	第 34-8 页上的防御基于速率的攻击
138、139	敏感数据预处理器	事件由敏感数据预处理器生成。	第 34-17 页上的检测敏感数据
140	SIP 预处理器	事件由 SIP 预处理器生成。	第 27-40 页上的解码会话发起协议
141	IMAP 预处理器	事件由 IMAP 预处理器生成。	第 27-45 页上的解码 IMAP 流量
142	POP 预处理器	事件由 POP 预处理器生成。	第 27-48 页上的解码 POP 流量
143	GTP 预处理器	事件由 GTP 预处理器生成。	第 27-44 页上的配置 GTP 命令通道
144	Modbus 预处理器	事件由 Modbus SCADA 预处理器生成。	第 28-1 页上的配置 Modbus 预处理器
145	DNP3 预处理器	事件由 DNP3 SCADA 预处理器生成。	第 28-3 页上的配置 DNP3 预处理器

搜索入侵事件

许可证：保护

可以使用随 FireSIGHT 系统提供的预定义搜索或创建您自己的搜索条件来搜索特定入侵事件。

预定义搜索用作示例，可用于快速访问关于网络的重要信息。您可能想要修改默认搜索中的特定字段，以根据网络环境对它们进行自定义，然后保存以便日后重复使用。请注意，搜索结果依赖于所搜索事件的可用数据。换言之，根据可用数据，搜索限制条件可能不适用。例如，只有加密流量上触发的入侵事件才包含 SSL 信息。

提示 有关在入侵事件搜索中指定 IP 地址和端口的语法的信息，请参阅第 60-6 页上的在搜索中指定 IP 地址和第 60-7 页上的在搜索中指定端口。

有关搜索的详细信息，包括如何加载和删除已保存搜索，请参阅第 60-1 页上的搜索事件。

以下列表介绍了可使用的搜索条件：

优先级

指定要查看的事件的优先级。优先级对应于 `priority` 关键字或 `classtype` 关键字的值。对于其他入侵事件，优先级由解码器或预处理器决定。有效值为 `high`、`medium` 和 `low`。

影响

指定根据入侵数据与网络发现数据的相关性对入侵事件分配的影响级别。有效值 （不区分大小写）包括 `Impact 0`、`Impact Level 0`、`Impact 1`、`Impact Level 1`、`Impact 2`、`Impact Level 2`、 `Impact 3`、 `Impact Level 3`、 `Impact 4` 和 `Impact Level 4`。

请勿使用影响图标颜色或部分字符串 （例如，请勿使用 `blue`、 `level 1` 或 `0`）。

有关详细信息，请参阅第 41-32 页上的使用影响级别评估事件。

Inline Result

键入以下内容之一：

- `dropped`，指定在内联部署中是否丢弃数据包
- `would have dropped`，指定是否已丢弃数据包 （如果入侵策略设置为在内联部署中丢弃数据包）

请注意，无论入侵策略的规则状态或内联丢弃行为如何，系统都不会丢弃被动部署中的数据包，当内联接口处于分路模式时也是如此。

源 IP：

指定入侵事件中涉及的源主机使用的 IP 地址。

目标 IP：

指定入侵事件中涉及的目标主机使用的 IP 地址。

Source/Destination IP

指定要查看其入侵事件的主机使用的源或目标 IP 地址。

Source Country

指定入侵事件中涉及的源主机所在的国家/地区。

Destination Country

指定入侵事件中涉及的目标主机所在的国家/地区。

Source/Destination Country

指定要查看的入侵事件所涉及的源主机或目标主机所在的国家/地区。

Source Continent

指定入侵事件中涉及的源主机所在的大洲。

Destination Continent

指定入侵事件中涉及的目标主机所在的大洲。

Source/Destination Continent

指定要查看的入侵事件所涉及的源主机或目标主机所在的大陆。

Original Client IP

指定提取自 X-Forwarded-For (XFF)、 True-Client-IP 或自定义 HTTP 报头的原始客户端 IP 地址。要为入侵事件中的此字段提取值，必须启用 HTTP 预处理器 **Extract Original Client IP Address** 选项。或者，在网络分析策略的同一区域，还可以指定最多六个自定义客户端 IP 报头，并设置系统选择原始客户端 IP 事件字段值的优先顺序。有关详细信息，请参阅第 27-28 页上的选择服务器级别 HTTP 规范化选项。

协议

键入连接中使用的传输协议的名称或编号，如 http://www.iana.org/assignments/protocol-numbers 中所列。

请注意，在入侵事件表视图中没有 Protocol 列。这是与源端口和目标端口/ICMP 列相关的协议。

Source Port/ICMP Type

指定与入侵事件相关联的源端口。

提示 对于没有目标端口的 ICMP 流量，可以使用此字段搜索具有特定 ICMP 类型的事件。

Destination Port/ICMP Code

指定与入侵事件相关联的目标端口。

提示 对于没有目标端口的 ICMP 流量，可以使用此字段搜索具有特定 ICMP 代码的事件。

VLAN ID

指定与触发入侵事件的数据包相关联的最内部的 VLAN ID。

MPLS Label

指定与触发入侵事件的数据包相关的多协议标记交换标记。

通信

指定要查看事件的全部或部分消息。

分类

为生成要查看的事件的规则输入分类编号或者完整或部分的分类名称或描述。也可以输入编号、名称或描述的以逗号分隔列表。最后，如果添加自定义分类，还可以使用其完整或部分的名称或描述进行搜索。有关分类编号、名称和描述的列表，请参阅规则分类表。

发电机

指定生成要查看的事件的组件，如第 41-34 页上的表 41-7中所列。

Snort ID

指定生成事件的规则的 Snort ID (SID)，或者指定规则的生成器 ID (GID) 和 SID 的组合，GID 和 SID 之间用冒号 (:) 隔开，格式为 GID:SID。可指定下表中的任何值：

表 41-8　Snort ID 搜索值

价值	示例
单个 SID	10000
SID 范围	10000 - 11000
大于某个 SID	>10000
大于或等于某个 SID	>=10000
小于某个 SID	<10000
小于或等于某个 SID	<=10000
以逗号分隔的 SID 值列表	10000,11000,12000
单个 GID:SID 组合	1:10000
以逗号分隔的 GID:SID 组合列表	1:10000,1:11000,1:12000
以逗号分隔的 SID 和 GID:SID 组合列表	10000,1:11000,12000

有关详细信息，请参阅第 41-34 页上的解读预处理器生成器 ID。

请注意， Snort ID 列不显示在搜索结果中；正在查看的事件的 SID 列示在 Message 列中。

Source User

指定登录源主机的用户的用户 ID。

Destination User

指定登录目标主机的用户的用户 ID。

Source/Destination User

指定登录源主机或目标主机的用户的用户 ID。

Application Protocol

键入在触发入侵事件的流量中检测到的应用协议的名称 （它代表主机之间的通信）。

Client

键入在触发入侵事件的流量中检测到的客户端应用的名称 （它表示在受监控主机上运行的软件）。

Web Application

键入网络应用的名称 （它表示在触发入侵事件的流量中检测到的 HTTP 流量的内容或请求 URL）。

Category, Tag (Application Protocol, Client, Web Application)

键入与在会话中检测到的应用相关的类别或标记。使用逗号隔开多个类别或标记。这些字段不区分大小写。

Application Risk

键入与在会话中检测到的应用相关的最高风险。有效条件为：`Very High`、`High`、`Medium`、`Low` 和 `Very Low`。这些字段不区分大小写。

Business Relevance

键入与在会话中检测到的应用相关的最低的业务相关性。有效条件为：`Very High`、`High`、`Medium`、`Low` 和 `Very Low`。这些字段不区分大小写。

Security Zone (Ingress, Egress, Ingress/Egress)

键入与触发事件的数据包相关的安全区域的名称。这些字段不区分大小写。请参阅第 3-34 页上的使用安全区域。

Device

键入设备名称或 IP 地址或设备组、堆栈或集群名称，将搜索限制于已应用访问控制规则的特定设备。有关 FireSIGHT 系统如何处理搜索中的设备字段的详细信息，请参阅第 60-6 页上的在搜索中指定设备。

请注意，堆叠配置中的主设备和辅助设备会单独报告入侵事件。有关详细信息，请参阅第 4-37 页上的管理堆叠设备。

Security Context

键入识别流量通过的虚拟防火墙组的安全上下文名称。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。

Interface (Ingress, Egress)

键入与触发事件的数据包相关联的接口名称；请参阅第 4-52 页上的配置感应接口。

Intrusion Policy

键入与事件相关联的入侵策略的名称；请参阅第 31-3 页上的管理入侵策略。

访问控制策略

键入与事件相关联的访问控制策略的名称；请参阅第 12-9 页上的管理访问控制策略。

Access Control Rule

键入与事件相关联的访问控制规则的名称；请参阅第 14-1 页上的使用访问控制规则调整流量。

HTTP Hostname

指定从 HTTP 请求主机报头提取的单个主机名。

要将主机名与 HTTP 客户端流量的入侵事件相关联，必须启用 HTTP 检查预处理器 **Log Hostname** 选项。有关详细信息，请参阅第 27-28 页上的选择服务器级别 HTTP 规范化选项。

HTTP URI

指定与触发入侵事件的 HTTP 请求数据包相关联的单个 URI。

要将 URI 与 HTTP 客户端流量的入侵事件相关联，必须启用 HTTP 检查预处理器 **Log URI** 选项。有关详细信息，请参阅第 27-28 页上的选择服务器级别 HTTP 规范化选项。

Email Sender

指定提取自 SMTP MAIL FROM 命令的邮件发件人的地址。也可以输入逗号隔开列表，搜索与任何指定的地址相关联的事件。有关详细信息，请参阅第 41-8 页上的了解入侵事件。

Email Recipient

指定提取自 SMTP RCPT TO 命令的邮件收件人的地址。也可以输入逗号隔开列表，搜索与任何指定的地址相关联的事件。有关详细信息，请参阅第 41-8 页上的了解入侵事件。

Email Attachments

指定提取自 MIME Content-Disposition 报头的 MIME 附件文件名。输入逗号隔开列表，搜索与列表中任何附件文件名相关联的事件。有关详细信息，请参阅第 41-8 页上的了解入侵事件。

Email Headers

指定提取自邮件报头的数据。请注意，邮件报头不显示在入侵事件表视图中，但可以将邮件报头数据作为搜索条件。

要将邮件报头与 SMTP 流量的入侵事件相关联，必须启用 SMTP 预处理器 **Log Headers** 选项。有关详细信息，请参阅第 27-51 页上的了解 SMTP 解码。

Reviewed By

指定审核事件的用户的名称。请参阅第 41-14 页上的审核入侵事件。

提示 可以输入 `unreviewed` 搜索尚未审核的事件。

入侵事件的专用搜索语法

为补充上文所列通用搜索语法，以下列表介绍一些入侵事件专用搜索语法。

SSL 实际操作

键入以下任何关键字，查看系统向其应用指定操作的加密流量的入侵事件：

- `Do not Decrypt` 代表系统未解密的连接。
- `Block` 和 `Block with reset` 代表被阻止的加密连接。
- `Decrypt (Known Key)` 代表使用已知私有密钥解密的传入连接。
- `Decrypt (Replace Key)` 代表使用带替代公共密钥的自签服务器证书解密的传出连接。
- `Decrypt (Resign)` 代表使用重签服务器证书解密的传出连接。

此列在入侵事件表视图中不显示。

SSL 失败的原因

键入以下任何关键字，查看系统由于指定原因无法解密的加密流量的入侵事件：

- 未知
- 无匹配
- 成功

- Uncached Session
- Unknown Cipher Suite
- Unsupported Cipher Suite
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

此列在入侵事件表视图中不显示。

SSL 使用者国家/地区

键入一个双字符 ISO 3166-1 二位字母国家/地区代码，查看与证书使用者国家/地区关联的加密流量的入侵事件。

此列在入侵事件表视图中不显示。

SSL 颁发者国家/地区

键入一个双字符 ISO 3166-1 二位字母国家/地区代码，查看与证书颁发者国家/地区关联的加密流量的入侵事件。

此列在入侵事件表视图中不显示。

SSL 证书指纹

键入或粘贴用于验证证书的 SHA 哈希值，查看与该证书关联的流量的入侵事件。

此列在入侵事件表视图中不显示。

SSL 公共密钥指纹

键入或粘贴用于验证证书内包含的公共密钥的 SHA 哈希值，查看与该证书关联的流量的入侵事件。

此列在入侵事件表视图中不显示。

要搜索入侵事件，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Analysis > Search**。

系统将显示 Intrusion Events 搜索页面。

查看入侵事件的列表时，也可以点击 **Search** （**Analysis > Intrusions > Events**）。

步骤 2　在相应字段中输入搜索条件，如前面的列表中所述。

- 有关搜索语法 （包括在搜索中使用对象）的详细信息，请参阅第 60-1 页上的搜索事件。
- 有关与公共密钥证书相关的字段，请参阅第 39-27 页上的查看与加密连接相关的证书。
- 有关入侵事件的专用搜索语法，请参阅第 41-40 页上的入侵事件的专用搜索语法。

步骤 3　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 4　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save as New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 5　点击 **Search** 开始搜索。

搜索结果显示在默认入侵事件工作流程中 （限制为当前时间范围）。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

使用剪贴板

许可证：保护

剪贴板是一个保留区域，可从任何入侵事件视图复制入侵事件到其中。有关如何向剪贴板添加事件的信息，请参阅第 41-16 页上的使用下钻式页面和表视图页面和第 41-19 页上的使用数据包视图。

剪贴板的内容按生成事件的日期和时间排序。在将入侵事件添加到剪贴板之后，可以将它们从剪贴板删除以及根据剪贴板内容生成报告。

还可以将剪贴板中的入侵事件添加到事故 （怀疑涉及到对安全策略的可能违反的事件的集合）。有关将剪贴板中的事件添加到事故的详细信息，请参阅第 42-4 页上的创建事故。

有关详细信息，请参阅以下各节：

- 第 41-43 页上的生成剪贴板报告
- 第 41-43 页上的从剪贴板删除事件

生成剪贴板报告

许可证：保护

可以为剪贴板中的事件生成报告，就像从任何事件视图中执行此操作一样。

要为剪贴板中的入侵事件生成报告，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　将一个或多个事件添加到剪贴板：

- 有关如何从事件的向下钻取页面或表视图向剪贴板添加事件的信息，请参阅第 41-16 页上的使用下钻式页面和表视图页面。
- 有关如何从数据包视图向剪贴板添加事件的信息，请参阅第 41-19 页上的使用数据包视图。

步骤 2　选择 **Analysis > Intrusions > Clipboard**。

系统显示剪贴板。

步骤 3　您有以下选项：

- 要包括剪贴板上某个页面中的特定事件，请导航到该页面，选择该事件旁边的复选框，然后点击 **Generate Report**。
- 要包括剪贴板中的所有事件，点击 **Generate Report All**。

在这两种情况下，系统都显示 Report Templates 页面。

步骤 4　指定报告布局，然后点击 **Generate**。

系统将显示 Generate Report 弹出对话框。

步骤 5　选择一种或多种输出格式 （HTML、 PDF 和 CSV），或者，修改任何其他设置。

提示　有关使用 Report Designer 的详细信息，请参阅第 57-1 页上的使用报告。

步骤 6　点击 **Generate**，然后点击 **Yes**。

系统将显示 Report Generation Complete 弹出窗口，其中包括可查看报告的链接。

步骤 7　点击以下其中一项：

- 报告链接，用于打开新窗口以显示所选的报告。
- **OK**，返回到 Report Templates 页面，可在其中修改报告设计。

从剪贴板删除事件

许可证：保护

如果在剪贴板上有不想添加到事故的入侵事件，可以删除事件。

注　从剪贴板删除事件**不会**从事件数据库删除该事件。但是，从事件数据库删除事件会从剪贴板删除该事件。

要从剪贴板删除事件，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Analysis > Intrusions > Clipboard**。

系统显示剪贴板。

步骤 2　您有以下选项：

- 要删除剪贴板上某个页面中的特定入侵事件，导航至该页面，选择事件旁边的复选框，然后点击 **Delete**。

  事件成功删除。

- 要删除剪贴板中的所有入侵事件，点击 **Delete All**。

  从剪贴板中成功删除所有事件。请注意，如果选择 Event Preferences 中的 **Confirm 'All' Actions** 选项，系统首先会提示您确认要删除所有事件。

事故处理

事故处理是指一个组织在怀疑存在违反组织安全策略的情况下做出的响应。 FireSIGHT 系统包括很多功能，在您收集和处理与事故调查相关的信息时为您提供支持。您可以使用这些功能收集可能与事故相关的入侵事件和数据包数据。您还可以将事故当做一个存储库，存储您从 FireSIGHT 系统提取的任何活动的相关备注，缓解攻击造成的影响。例如，如果安全策略要求隔离来自您网络的受危害主机，您就可以注意到事故中这种情况。

FireSIGHT 系统 还提供整个事故周期支持，让您可以在对攻击做出响应的过程中修改事故状态。处理完事故时，您可以注意到根据所学到的经验已经对安全策略进行的任何修改。

有关处理 FireSIGHT 系统中事故的详细信息，请参阅以下各节。

事故处理基本信息

许可证：保护

每个组织可能都有自己发现、定义和响应违反其安全策略情况的流程。以下各节介绍一些事故处理基本信息以及如何将 FireSIGHT 系统纳入您的事故响应计划：

事故的定义

许可证：保护

通常，*事故*指您怀疑可能涉及违反安全政策的一个或多个入侵事件。思科也使用本术语描述您在 FireSIGHT 系统中使用的以跟踪您对事故的响应的功能。

按照第 41-1 页上的处理入侵事件中的说明，对网络资产可用性、机密性和完整性而言，某些入侵事件比其他入侵事件更加重要。例如， FireSIGHT 系统提供的端口扫描检测功能可让您了解网络上的端口扫描活动。但是，您的安全策略可能未明确禁止端口扫描或将其视为高优先级威胁，因此，您可能不会采取任何直接行动，而只想保留全部端口扫描的日志以供日后调查研究之用。

另一方面，如果系统生成表明您网络中的主机已受到危害并且正在参与分布式拒绝服务 (DDoS) 攻击的事件，那么这个活动就可能明显违反安全策略，您应在 FireSIGHT 系统中创建一个事故来帮助跟踪对这些事件的调查。

常规事故处理流程

许可证：保护

每个组织都可能确定了自己处理安全事故的流程。大多数方法都包括以下部分或全部阶段：

- 第 42-2 页上的准备
- 第 42-2 页上的检测和通知
- 第 42-2 页上的调查和资格审批
- 第 42-3 页上的沟通
- 第 42-3 页上的控制和恢复
- 第 42-3 页上的学习到的经验

这些阶段都将在后续各节中逐一说明。这些说明还会解释如何将 FireSIGHT 系统纳入每个阶段。

准备

您可以通过两种方式为事故做准备：

- 落实明确和全面的安全策略以及强化这些策略的硬件和软件资源
- 制定一个清晰明确的事故响应计划，并配备一个可以实施此计划的训练有素的团队

事故处理的关键部分在于了解网络的哪些部分面临最大的风险。在这些网段部署 FireSIGHT 系统组件，可以提高对于事故发生时间和状况的了解。此外，花时间仔细调整每个受管设备的入侵策略，可以确保生成的事件具有最高的质量。

检测和通知

您必须能检测到事故，才能响应事故。事故处理流程应注意您可以检测到的安全相关事件的类型以及您可用于检测这些类型事件的软件和硬件机制。您还应该注意会在何处检测到违反安全策略的活动。如果网络包括没有被主动或被动监控的网段，则需要特别注意。

您在网络中部署的受管设备负责分析安装了这些设备的网段的流量、检测入侵以及生成描述入侵的事件。记住：您在每个受管设备上应用的访问控制策略控制这些设备可以检测哪些类型的活动以及如何确定其优先级。您还可以设置特定类型入侵事件的通知选项，从而让事故团队无需筛查数百个事件。您可以指定在检测到特定高优先级、高敏感性事件时自动获得通知。

调查和资格审批

您的事故处理流程应指定检测到安全事故之后如何执行调查。某些组织中，初级团队成员负责将所有事故分类并处理严重程度或优先级较低的事故。高严重程度和高优先级事故则由更高级的团队成员来处理。您应该认真确定升级流程，让每个团队成员都了解提高事故重要性的标准。

升级流程的一部分在于了解检测到的事件会如何影响网络资产的安全性。例如，运行 Microsoft SQL Server 的主机的攻击对于使用不同数据库服务器的组织来说优先级并不高。同样，如果网络中使用的是 SQL Server，但是您确信所有服务器都已打补丁并且不容易受到攻击，那么这种攻击对您来说重要性也会降低。但是，如果有人最近安装了一个易受攻击的版本的软件 （可能是为了进行测试），您所遇到的问题可能会比粗略调查反映的问题更严重。

FireSIGHT 系统特别适合支持调查和资格审批流程。您可以创建自己的事件分类，然后以最充分描述网络漏洞的方式应用这些分类。网络上的流量触发事件时，系统将自动划分事件的优先级和类别，并向您提供表明哪些攻击是针对已知易受攻击的主机的具体指标。

FireSIGHT 系统中的事故跟踪功能还包括状态标记，您可以修改此状态标记，指出哪些事故已经升级。

沟通

所有事故处理流程都应指定事故处理团队和内外受众之间进行事故沟通的方式。例如，您应该考虑哪些类型的事故需要管理人员干涉以及需要哪个级别的管理人员干涉。此外，流程应该规定如何及何时与外部组织沟通。某些事故是否需要通知执法机构？如果您的主机正在参加针对远程站点的分布式拒绝服务 (DDoS)，您是否要通知它们？您是否希望与计算机紧急事故响应小组协调中心 (CERT/CC) 或 事故响应与安全组织论坛 (FIRST) 共享信息？

FireSIGHT 系统具备可用于收集诸如 HTML、 PDF、 CSV（逗号分隔值）等标准格式入侵数据的功能，让您能够轻松与他人共享入侵数据。

例如， CERT/CC 在其网站上收集有关安全事故的标准信息。 CERT/CC 寻找可以从 FireSIGHT 系统轻松提取的各类型的信息，例如：

- 有关受影响的机器的信息，包括：
- 主机名和 IP 地址
- 时区
- 主机的用途或功能
- 有关攻击源的信息，包括：
- 主机名和 IP 地址
- 时区
- 您是否与攻击者有任何接触
- 处理事故的估算成本
- 事故的描述，包括：
- 日期
- 入侵方法
- 涉及的入侵者工具
- 软件版本和补丁级别
- 任何入侵者工具输出
- 被利用的漏洞的详细信息
- 攻击源
- 任何其他相关信息

您还可以使用事故的备注部分记录您何时以及与谁沟通了这些问题。

控制和恢复

您的事故处理流程应明确指出主机或其他网络组件受到危害时采取哪些措施。控制范围和恢复选项包括从向易受攻击的主机应用补丁到关闭目标并将其从网络移除。您还应该按照攻击的性质和严重性考虑保留证据的重要性，以备提出刑事指控。

您可以使用 FireSIGHT 系统的事故功能记录您在事故的控制和恢复阶段采取的行动。

学习到的经验

每个安全事故，无论是否攻击成功，都是一个审核安全策略的机会。您是否需要更新防火墙规则？您是否需要采取更加结构化的补丁管理方法？未授权无线接入点是否构成新的安全问题？每个学到的经验都应反馈到安全策略中并帮助您更好地准备处理下一事故。

FireSIGHT 系统中的事故类型

许可证：保护

您可以为创建的每个事故指定一个事故类型。在 FireSIGHT 系统中默认情况下支持以下类型：

- 入侵
- 拒绝服务攻击
- 未经授权的管理员访问权限
- 网站篡改
- 系统完整性危害
- 欺诈
- 盗窃
- 损坏
- 未知

您还可以创建自己的事故类型，详见第 42-6 页上的创建定制事故类型所述。

创建事故

许可证：保护

本节介绍如何创建事故。

要创建事故，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Analysis > Intrusions > Incidents**。

系统将显示 Incidents 页面。

步骤 2　点击 **Create Incident**。

系统将显示 Create Incident 页面。

如果您以前已将入侵事件复制到剪贴板，它们会显示在页面底部。有关使用剪贴板的详细信息，请参阅第 41-42 页上的使用剪贴板。

步骤 3　从 **Type** 下拉菜单中选择最能描述事故的选项。

步骤 4　在 **Time Spent** 字段中，按照 #d #h #m #s 格式输入您在此事故上花费的时间，其中 # 代表天数、小时数、分钟数或秒数。

步骤 5　在 **Summary** 文本框中，键入对事故的简要说明 （至多 255 个字母数字字符、空格和符号）。

步骤 6　在 **Add Comment** 文本框中，键入对事故更完整的说明 （至多 8191 个字母数字字符、空格和符号）。

步骤 7　是否要向事故添加事件？

- 如果**是**，请在剪贴板选择事件并点击 **Add to Incident**。

  您还可以通过点击 **Add All to Incident** 添加剪贴板上的全部事件。
- 如果**不是**，请点击 **Save**。

无论如何，事故会连同您输入的信息一起保存。

注　如果想要添加来自剪贴板上多个页面的各个事件，您必须单独添加来自一个页面的事件，再添加来自其他页面的事件。

编辑事故

许可证：保护

收集到更多信息时，您可以更新事故。调查进行过程中，您还可以向事故添加或从中删除事件。

要编辑事故，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Analysis > Intrusions > Incidents**。

系统将显示 Incidents 页面。

步骤 2　点击要编辑的事故旁的编辑图标 ( )。

步骤 3　您可以编辑事故的以下任何方面：

- 更改状态
- 更改类型
- 从剪贴板添加事件
- 删除事件

步骤 4　在 **Time Spent** 字段中，输入在事故上额外花费的时间量。

步骤 5　在 **Add Comment** 文本框中，指出您对事故的更改 （至多 8191 个字母数字字符、空格和符号）。

步骤 6　或者，您可以给事故添加或删除事件：

- 要添加剪贴板上的事件，请选择剪贴板上的事件，并点击 **Add to Incident**。
- 要添加剪贴板上的全部事件，请点击 **Add All to Incident**。
- 要删除事故的特定事件，请选择事件并点击 **Delete**。
- 要删除事故的所有事件，请点击 **Delete All**。
- 要更新事故而不添加或删除事件，请点击 **Save**。

对事故的更改保存成功。

生成事故报告

许可证：保护

您可以使用 FireSIGHT 系统生成事故报告，其中包含事故摘要、事故状态和注释以及您添加到事故上的事件的信息。您还可以指定是否要在报告中包括事件摘要信息。

要生成事故报告，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Analysis > Intrusions > Incidents**。

系统将显示 Incidents 页面。

步骤 2　点击您想要包含在报告中的事故旁的编辑图标 ( )。

步骤 3　此时您有两种选择：

- 要将事故的所有事件都包括在报告中，请点击 **Generate Report All**。
- 要将事故的特定事件包括在报告中，请选择要包括的事件旁的复选框并点击 **Generate Report**。

无论哪种情况，系统都会显示 Generate Report 页面，其中包括事故报告选项。

步骤 4　为此报告输入一个名称。您可以使用字母数字字符、点号和空格。

步骤 5　在 **Incident Report Sections** 中，选择要包含在报告中的事故部分的复选框：**status**、 **summary** 和 **comments**。

步骤 6　如果要在报告中包括事件信息，请选择您要使用的工作流程，然后在 **Report Sections** 中指定是否要包括事件摘要信息。

步骤 7　选择报告中要包括的工作流程页面旁的复选框。

步骤 8　选择要用于报告的输出格式旁边的复选框：**PDF**、 **HTML** 和 **CSV**。

注　基于 CSV 的事故报告仅包括事件信息。它们不包括事故的状态、摘要或备注。

步骤 9　点击 **Generate Report** 并确认您要更新报告配置文件。

报告即已生成。

创建定制事故类型

许可证：保护

FireSIGHT 系统提供以下可用于给事故分类的事故类型：

- 系统完整性危害
- 损坏
- 拒绝服务攻击
- 欺诈
- 入侵
- 盗窃
- 未经授权的管理员访问权限
- 未知
- 网站篡改

如果这些事故类型不能满足您的需求，您可以添加自己的类型。请注意，您不能删除任何定制事故类型。

要创建新的事故类型，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Analysis > Intrusions > Incidents**。

系统将显示 Incident 页面。

步骤 2　点击 **Create Incident**。

系统将显示 Create Incident 页面。

步骤 3　在 **Type** 区域，点击 **Types**。

系统将显示事故管理 Types 页面。默认事故类型列在页面底部。

步骤 4　在 **Incident Type Name** 字段中，输入新的事故类型名称。

使用字母数字字符和空格。

步骤 5　点击 **Add**。

新的事故类型添加成功。

步骤 6　点击 **Done** 关闭弹出窗口并返回到 Incidents 页面。

下次创建或编辑事故时，您就可以使用新的事故类型。

配置外部警报

尽管 FireSIGHT 系统在络界面中提供了各种事件视图，但您仍可能想要配置外部事件通知，以简化对关键系统的持续监控。可将 FireSIGHT 系统配置为生成警报，在发生以下某一事件时通过邮件、 SNMP 陷阱或系统日志发送通知：

- 带有特定影响标志的入侵事件
- 特定类型的发现事件
- 基于网络的恶意软件事件或回溯性恶意软件事件
- 由特定的关联策略违规触发的相关性事件
- 由特定的访问控制规则触发的连接事件
- 运行状况策略中某一模块的特定状态变化

要让系统发送这些警报，必须先创建一个*警报响应*，这是一组配置，允许 FireSIGHT 系统与计划发送警报的外部系统进行交互。例如，这些配置可以指定邮件中继主机、 SNMP 警报参数或系统日志设备和优先级。

创建警报响应之后，可将其与要用于触发警报的事件关联起来。请注意，在将警报响应与事件进行关联时，具体流程因事件类型而异：

- 可使用各类事件自己的配置页面，将警报响应与影响标记、发现事件和恶意软件事件关联起来。
- 在关联策略中，可将相关性事件与警报响应（和补救响应；参阅第 54-1 页上的创建补救）关联起来。
- 通过使用访问控制规则和策略，可将 SNMP 和系统日志警报响应与已记录的连接关联起来。对于已记录的连接，系统不支持邮件警报。
- 通过使用运行状况监控程序，可将警报响应与运行状况模块状态变化关联起来。

还可在 FireSIGHT 系统中执行另外一种警报，即为单个的入侵事件配置邮件、 SNMP 和系统日志入侵事件通知，不管影响标志如何。可在入侵策略中配置这些通知；请参阅第 44-1 页上的配置入侵规则的外部警报和第 32-29 页上的添加 SNMP 告警。下表介绍了生成警报时必须拥有的许可证。

表 43-1 生成警报时的许可证要求

要基于以下内容生成警报...	您需要该许可证.....
带有特定影响标志的入侵事件	FireSIGHT + 保护
特定类型的发现事件	FireSIGHT
基于网络的恶意软件事件	恶意软件
关联策略违规	触发策略违规所需许可证

表 43-1　　生成警报时的许可证要求 （续）

要基于以下内容生成警报...	您需要该许可证.....
连接事件	记录连接所需许可证
运行状况模块状态变化	任何环境

有关详情，请参阅：

- 第 43-2 页上的使用警报响应
- 第 43-7 页上的配置影响标志警报
- 第 43-8 页上的配置发现事件警报
- 第 43-8 页上的配置高级恶意软件防护警报
- 第 51-45 页上的将响应添加至规则和白名单
- 第 38-1 页上的记录网络流量中的连接
- 第 68-35 页上的配置运行状况监视警报

使用警报响应

许可证：任何环境

配置外部警报时，首先要创建一个警报响应，这是一组配置，允许 FireSIGHT 系统与计划发送警报的外部系统进行交互。可创建警报响应以通过邮件、简单网络管理协议 (SNMP) 陷阱或系统日志 (syslog) 发送警报。

在警报中收到的信息取决于触发警报的事件类型。例如，影响标志警报包含时间戳、入侵规则、影响标志和事件说明信息。又例如，发现事件警报也包含时间戳和说明信息，以及发现事件类型信息。

如果在关联策略中使用了警报响应，则警报中的信息取决于触发关联策略违规的事件的类型。

注　如将警报配置为对包含连接跟踪程序的关联规则的响应，则收到的警报信息与流量配置文件变化警报相同，即使关联规则本身基于不同类型的事件。

创建警报响应时，它将自动启用。只有已启用的警报响应才能生成警报。要阻止生成警报，可暂时禁用警报响应，而非删除配置。

可在 Alerts 页面 (**Policies > Actions > Alerts**) 上管理警报响应。每个警报响应旁的滑块指明该响应是否处于活动状态；只有已启用的警报响应才能生成警报。该页面也指明警报响应目前是否用于某一配置中，例如，在访问控制规则中记录连接。可点击名称、类型、使用状态和启用/禁用状态以按相应的列标题对警报响应排序；再次点击列标题可以反向排序。

有关详情，请参阅：

- 第 43-3 页上的创建邮件警报响应
- 第 43-3 页上的创建 SNMP 警报响应
- 第 43-4 页上的创建系统日志警报响应
- 第 43-6 页上的修改警报响应
- 第 43-7 页上的删除警报响应
- 第 43-7 页上的启用和禁用警报响应

创建邮件警报响应

许可证：任何环境

请注意，**不能**在访问控制策略中对已记录的连接执行邮件警报。

创建邮件警报响应之前，应确保防御中心可反向解析其自身的 IP 地址。还应按第 63-17 页上的配置邮件中继主机和通知地址中所述，配置自己的邮件中继主机。

要创建邮件警报响应，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Actions > Alerts**。

系统将显示 Alerts 页面。

步骤 2　从 **Create Alert** 下拉菜单，选择 **Create Email Alert**。

系统将显示 Create Email Alert Configuration 弹出窗口。

步骤 3　在 **Name** 字段中，键入要用于标识警报响应的名称。

步骤 4　在 **To** 字段中，键入要发送警报的邮件地址。

用逗号隔开邮件地址。

步骤 5　在 **From** 字段中，键入要作为警报发件人的邮件地址。

步骤 6　在 **Relay Host** 旁，验证列出的邮件服务器是要用于发送警报的服务器。

要更改服务器，或如果尚未配置中继主机，请点击编辑图标 () 以在弹出窗口中显示 System Policy 页面，然后按照第 63-17 页上的配置邮件中继主机和通知地址中的指示操作。必须应用编辑后的系统策略，更改才能生效。

步骤 7　点击 **Save**。

警报响应保存成功并自动启用。

创建 SNMP 警报响应

许可证：任何环境

可使用 SNMPv1、 SNMPv2 或 SNMPv3 创建 SNMP 警报响应。

注　如果想要使用 SNMP 监控 64 位值，则必须使用 SNMPv2 或 SNMPv3。SNMPv1 不支持 64 位监控。

如果网络管理系统需要防御中心的管理信息库 (MIB) 文件，则可在 `/etc/sf/DC EALERT.MIB` 处获取该文件。

要创建 SNMP 警报响应，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Actions > Alerts**。

系统将显示 Alerts 页面。

步骤 2　从 **Create Alert** 下拉菜单，选择 **Create SNMP Alert**。

系统将显示 Create SNMP Alert Configuration 弹出窗口。

步骤 3　在 **Name** 字段中，键入要用于标识 SNMP 响应的名称。

步骤 4　在 **Trap Server** 字段中，使用字母数字字符键入 SNMP 陷阱服务器的主机名或 IP 地址。

请注意，如在此字段中输入了无效的 IPv4 地址 （例如 192.169.1.456），则系统**不会**发出警告。相反，无效地址会被视为主机名。

步骤 5　从 **Version** 下拉列表中，选择要使用的 SNMP 版本。

SNMP v3 是默认值。如果选择 SNMP v1 或 SNMP v2，系统会显示不同的选项。

步骤 6　您选择了哪个版本的 SNMP？

- 对于 SNMP v1 或 SNMP v2，在 **Community String** 字段中，使用字母数字字符或特殊符号 `*` 或 `$` 键入 SNMP 团体名称，然后跳至第 12 步。
- 对于 SNMP v3，在 **User Name** 字段中，键入要使用 SNMP 服务器对其进行身份验证的用户的名称并继续下一步。

步骤 7　从 **Authentication Protocol** 下拉列表中，选择要用于身份验证的协议。

步骤 8　在 **Authentication Password** 字段中，键入使用 SNMP 服务器进行身份验证所需的密码。

步骤 9　从 **Privacy Protocol** 列表中，选择 **None** 以不使用隐私协议或选择 **DES** 以使用 Data Encryption Standard 作为隐私协议。

步骤 10　在 **Privacy Password** 字段中，键入 SNMP 服务器要求的隐私密码。

步骤 11　在 **Engine ID** 字段中，使用偶数数字 （十六进制形式）键入 SNMP 引擎的标识符。

使用 SNMPv3 时，系统使用引擎 ID 值对消息进行编码。 SNMP 服务器需要使用该值解码消息。

思科建议您使用防御中心的 IP 地址的十六进制版本。例如，如果防御中心的 IP 地址是 `10.1.1.77`，请使用 `0a01014D0`。

步骤 12　点击 **Save**。

警报响应保存成功并自动启用。

创建系统日志警报响应

许可证：任何环境

配置系统警报响应时，可指定与系统日志消息相关联的严重性和设备，以确保它们得到系统日志服务器的正确处理。设备指明创建消息的子系统，严重性界定消息的严重性。设备和严重性不显示在系统日志中的实际消息中，而是告知接收系统日志消息的系统如何对消息进行归类。

提示　有关系统日志如何运行及如何对其进行配置的更多详细信息，请参阅系统文档。在 UNIX 系统上，`syslog` 和 `syslog.conf` 的 `man` 页面提供了概念信息和配置说明。

虽然在创建系统日志警报响应时可选择任一种设备，但您还是应该根据自己的系统日志服务器选择适合的一个；并非所有系统日志服务器都支持所有设备。对于 UNIX 系统日志服务器，`syslog.conf` 文件应指示哪些设备保存到了服务器的哪些日志文件上。

下表列出了可选择的系统日志设备。

表 43-2　可选用的系统日志设施

设施	说明
ALERT	警报消息。
审计	审计子系统生成的消息。
AUTH	与安全和授权相关的消息。
AUTHPRIV	与安全和授权相关的访问限制消息。很多系统会将这些消息转发到一个安全的文件中。
CLOCK	时钟后台守护程序生成的消息。 请注意，运行 Windows 操作系统的系统日志服务器将使用 CLOCK 设备。
CRON	时钟后台守护程序生成的消息。 请注意，运行 Linux 操作系统的系统日志服务器将使用 CRON 设备。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
MAIL	邮件系统生成的消息。
新闻	网络新闻子系统生成的消息。
NTP	NTP 守护程序生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
用户	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

下表列出了可选择的标准系统日志严重性级别。

表 43-3　系统日志严重性级别

功率水平	说明
ALERT	应立即更正的状况。
CRIT	临界状况。
DEBUG	包含调试信息的消息。
EMERG	向所有用户广播的紧急状况。
ERR	错误状况。
INFO	信息性消息
请注意！	需要注意但非错误的状况。
警告	警告消息。

开始发送系统日志警报之前，请确保系统日志服务器可接受远程消息。

要创建系统日志警报，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Actions > Alerts**。

系统将显示 Alerts 页面。从 **Create Alert** 下拉菜单中，选择 **Create Syslog Alert**。

系统将显示 Create Syslog Alert Configuration 弹出窗口。

步骤 2　在 **Name** 字段中，键入要用于标识已保存响应的名称。

步骤 3　在 **Host** 字段中，键入系统日志服务器的主机名 或 IP 地址。

请注意，如在此字段中输入了无效的 IPv4 地址 （例如 192.168.1.456），则系统**将不**发出警告。相反，无效地址会被视为主机名。

步骤 4　在 **Port** 字段中，键入服务器用于系统日志消息的端口。

默认情况下，此值为 514。

步骤 5　从 **Facility** 列表中，选择设备。

请参阅可选用的系统日志设施表，了解可用设备列表。

步骤 6　从 **Severity** 列表中，选择严重性。

请参阅系统日志严重性级别表，了解可用严重性列表。

步骤 7　在 **Tag** 字段中，键入想要与系统日志消息一起显示的标记名称。

标记名称只能使用字母数字字符。**不能**使用空格或下划线。

例如，如果想在发送至系统日志的所有消息前加上 `FromDC`，请在该字段中键入 `FromDC`。

步骤 8　点击 **Save**。

警报响应保存成功并自动启用。

修改警报响应

许可证：任何环境

对于大多数类型的警报，如果某一警报响应已启用且在使用中，则对该警报响应做出的更改将立即生效。但对于访问控制规则中用于记录连接事件的警报响应而言，只有重新应用了访问控制策略，所做的更改才能生效。

要编辑警报响应，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Actions > Alerts**。

系统将显示 Alerts 页面。

步骤 2　在要编辑的警报响应旁，点击编辑图标 ( )。

系统显示与该警报响应对应的配置弹出窗口。

步骤 3　根据需要进行更改。

步骤 4　点击 **Save**。

警报响应保存成功。

删除警报响应

许可证：任何环境

可删除未使用的任何警报响应。

要删除警报响应，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Actions > Alerts**。

系统将显示 Alerts 页面。

步骤 2　在要删除的警报响应旁，点击删除图标 ( )。

步骤 3　确认要删除该警报响应。

警报响应删除成功。

启用和禁用警报响应

许可证：任何环境

只有已启用的警报响应才能生成警报。要阻止生成警报，可暂时禁用警报响应，而非删除配置。请注意，如在禁用某警报时该警报正在使用中，则该警报禁用后仍被视为在使用。

要启用或禁用警报响应，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Actions > Alerts**。

系统将显示 Alerts 页面。

步骤 2　在要启用或禁用的警报响应旁，点击启用/禁用滑块。

如果警报响应已启用，则将其禁用。如果连接已禁用，点击该滑块将会启用连接。

配置影响标志警报

许可证：保护

可将系统配置为只要出现带有特定影响标志的入侵事件就会发出警报。影响标记可通过将入侵数据、网络发现数据和漏洞信息相关联来帮助评估入侵对网络的影响。有关详细信息，请参阅第 41-32 页上的使用影响级别评估事件。

要配置影响标志警报，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Actions > Alerts**，然后选择 **Impact Flag Alerts** 选项卡。

系统将显示 Impact Flag Alerts 页面。

步骤 2　在 Alerts 部分，为每种警报类型选择要使用的警报响应。

要新建警报响应，从任一下拉列表选择 **New**。有关详细信息，请参阅第 43-2 页上的使用警报响应。

步骤 3　在 Impact Configuration 部分，选择与要为每个影响标志接收的警报相应的复选框。

步骤 4　点击 **Save**。

影响标志警报设置保存成功。

配置发现事件警报

许可证：FireSIGHT

可将系统配置为只要出现特定类型的发现事件就会发出警报。有关不同事件类型的信息，请参阅第 50-8 页上的了解发现事件类型和第 50-11 页上的了解主机输入事件类型。

请注意，要根据发现事件类型生成警报，必须将网络发现策略配置为记录该事件类型；请参阅第 45-31 页上的配置发现事件日志记录。默认情况下，已为所有事件类型启用日志记录功能。

要配置发现事件警报，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Actions > Alerts**，然后选择 **Discovery Event Alerts** 选项卡。

系统将显示 Discovery Event Alerts 页面。

步骤 2　在 **Alerts** 部分，为每种警报类型选择要使用的警报响应。

要新建警报响应，从任一下拉列表选择 **New**。有关详细信息，请参阅第 43-2 页上的使用警报响应。

步骤 3　在 **Events Configuration** 部分，选择与要为每种发现事件类型接收的警报相应的复选框。

步骤 4　点击 **Save**。

发现事件警报设置保存成功。

配置高级恶意软件防护警报

许可证：恶意软件

受支持的设备：3 系列或虚拟

受支持的防御中心：除 DC500 外的所有型号

可将系统配置为只要生成任何基于网络的恶意软件事件 （包括回溯性事件）就发出警报。不过，无法就基于终端的 (FireAMP) 恶意软件事件发送警报。有关恶意软件事件的信息，请参阅第 40-14 页上的使用恶意软件事件。

要根据恶意软件事件生成警报，必须创建一个用于执行恶意软件云查找的文件策略，然后将该策略与访问控制规则相关联。有关详细信息，请参阅第 18-1 页上的使用入侵和文件策略控制流量。

要配置恶意软件事件警报，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Actions > Alerts**，然后选择 **Advanced Malware Protections Alerts** 选项卡。

系统将显示 Advanced Malware Protection Alerts 页面。

步骤 2　在 **Alerts** 部分，为每种警报类型选择要使用的警报响应。

要新建警报响应，从任一下拉列表选择 **New**。有关详细信息，请参阅第 43-2 页上的使用警报响应。

步骤 3　在 **Events Configuration** 部分，选择与要为每种恶意软件事件类型接收的警报相应的复选框。

请注意， **All network-based malware events** 包括 **Retrospective Events**。

步骤 4　点击 **Save**。

恶意软件事件警报设置保存成功。

配置入侵规则的外部警报

虽然 FireSIGHT 系统在网络界面内提供各种入侵事件视图，但一些企业更喜欢通过定义外部入侵事件通知对关键系统实施持续监控。如果想要立即通知关键事件的特定联系人，可以设置邮件警报进行操作。也可以记录日志到系统日志设施或将事件数据发送到 SNMP 陷阱服务器。

您可以为每个入侵策略指定入侵事件通知限制、设置发送到外部日志记录设施的入侵事件通知，也可以配置入侵事件的外部响应。

提示 一些分析师并不希望收到同一入侵事件的多个警报，但却希望控制收到特定入侵事件通知的频率。有关详情，请参见第 32-20 页上的按策略过滤入侵事件通知。

除了入侵策略， FireSIGHT 系统还可以执行另外一种警报。对于其他类型事件，可以配置邮件、SNMP 和系统日志警报响应活动。这些事件包括带有特定影响标记的入侵事件或采用特定访问控制规则记录的连接事件。有关详细信息，请参阅第 43-1 页上的配置外部警报。

有关外部入侵事件通知的详细信息，请参阅以下章节。

- 第 44-1 页上的使用 SNMP 响应介绍用于将事件数据发送到指定 SNMP 陷阱服务器的配置选项，并提供指定 SNMP 警报选项的程序。
- 第 44-4 页上的使用系统日志响应介绍用于将事件数据发送到外部系统日志的配置选项，并提供指定系统日志警报选项的程序。
- 第 44-6 页上的了解邮件警报介绍通过邮件发送入侵事件通知的配置选项。

使用 SNMP 响应

许可证：保护

*SNMP 陷阱*是一种网络管理通知。将设备配置为以 SNMP 陷阱（又称为 *SNMP 警报*）的形式发送入侵事件通知。每个 SNMP 警报都包括以下内容：

- 生成陷阱的服务器的名称
- 检测到入侵事件的设备的 IP 地址
- 检测到入侵事件的设备的名称
- 事件数据

可以设置 SNMP 警报的多种参数。可设定的参数因所用的 SNMP 版本而有所不同。有关启用和禁用 SNMP 警报的详细信息，请参阅第 31-6 页上的在入侵策略中配置高级设置。

提示 如果网络管理系统要求使用管理信息库文件 (MIB)，您可以从防御中心中获取，具体位置为 `/etc/sf/DCEALERT.MIB`。

SNMP v2 选项

对于 SNMP v2，您可指定下表中介绍的选项。

表 44-1　SNMP v2 选项

选项	说明
Trap Type	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则可以选择 **as Binary**。否则，应选择 **as String**。例如， HP Openview 就需要选择字符串类型。
Trap Server	收到 SNMP 陷阱通知的服务器。 可指定一个唯一的 IP 地址或主机名。
Community String	社区名称。

SNMP v3 选项

对于 SNMP v3，您可指定下表中介绍的选项。

注 当您使用 SNMP v3 时，设备会使用一个 Engine ID 值编码消息。SNMP 服务器需要使用该值解码消息。目前，该 Engine ID 值始终采用设备 IP 地址的十六进制形式，且该字符串的末尾为 `01`。例如，如果发送 SNMP 警报的设备有一个 IP 地址为 `172.16.1.50`，则 Engine ID 为 `0xAC10013201`，而如果设备有一个 IP 地址为 `10.1.1.77`，则 `0x0a01014D01` 就用作 Engine ID。

表 44-2　SNMP v3 选项

选项	说明
Trap Type	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则可以选择 **as Binary**。否则，应选择 **as String**。例如， HP Openview 就需要选择字符串类型。
Trap Server	收到 SNMP 陷阱通知的服务器。 可指定一个唯一的 IP 地址或主机名。
Authentication Password	用于身份验证的密码。SNMP v3 使用消息摘要 5 (MD5) 哈希函数或安全哈希算法 (SHA) 哈希函数进行密码加密，具体取决于配置。 一旦指定身份验证密码，身份验证即可启用。
Private Password	用于保护隐私的 SNMP 密钥。SNMP v3 采用数据加密标准 (DES) 分组密码对密码进行加密。 一旦指定私有密码，隐私功能即可启用。指定私有密码后，还必须指定身份验证密码。
用户名	SNMP 用户名。

有关配置 SNMP 警报的信息，请参阅第 44-3 页上的配置 SNMP 响应。

配置 SNMP 响应

许可证：保护

您可以配置入侵策略中的 SNMP 警报。应用访问控制策略中的入侵策略后，一旦系统检测到任何入侵事件，就会通过 SNMP 陷阱发送通知。有关 SNMP 警报的详细信息，请参阅第 44-1 页上的使用 SNMP 响应。

要配置 SNMP 警报选项，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies> Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　根据 External Responses 中 **SNMP Alerting** 的启用情况，您有两种选择：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 SNMP Alerting 页面。

页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　指定在警报中显示的 IP 地址所用的陷阱类型格式，可选择 **as Binary** 或 **as String**。

注　如果网络管理系统正常显现 INET_IPV4 地址类型，则可以使用 **as Binary** 选项。否则，应使用 **String** 选项。例如， HP Openview 需要选择 **as String** 选项。

步骤 6　选择 SNMP v2 或 SNMP v3：

- 要配置 SNMP v2，请在相应字段中输入要使用的陷阱服务器的 IP 地址和社区名称。请参阅第 44-2 页上的 SNMP v2 选项。
- 要配置 SNMP v3，请在相应字段中输入要使用的陷阱服务器的 IP 地址、身份验证密码、私有密码和用户名。有关详情，请参见第 44-2 页上的 SNMP v3 选项。

注　必须选择 SNMP v2 **或** SNMP v3。

注　输入 SNMP v3 密码后，初始配置期间的密码会以明文显示，但以加密格式保存。

步骤 7　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

使用系统日志响应

许可证：保护

系统日志 (*syslog*) 是网络事件记录的标准记录机制。您可以将表示入侵事件通知的*系统日志警报*发动到设备的系统日志中。系统日志使您能够按照优先级和设施对信息进行分类。*优先级*反映的是警报的严重程度，*设施*显示的是生成警报的子系统。设施和优先级并不会在系统日志的实际消息内显示，而是用于规定系统对系统日志消息进行分类的方法。

系统日志警报包含以下信息：

- 生成警报的日期和时间
- 事件消息
- 事件数据
- 触发事件的生成器 ID
- 触发事件的 Snort ID
- 修订

您可以打开入侵策略中的系统日志警报、指定与系统日志中入侵事件通知有关的系统日志优先级和设施。应用了访问控制策略中的入侵策略后，如果检测到入侵事件，系统会发送系统日志警报给策略中指定的本地主机或日志记录主机上的系统日志设施。接收警报的主机会采用配置系统日志警报分类时设置的设施和优先级信息。

下表列出了在配置系统日志警报时可选择的设施。务必要根据所用远程系统日志服务器的配置情况来合理配置设施。远程系统中的 `syslog.conf` 文件（如果将系统日志消息记录到基于 UNIX 或 Linux 的系统）指示哪些设施保存在服务器的哪些日志文件中。

表 44-3　　可选用的系统日志设施

设施	说明
AUTH	与安全和授权相关的消息。
AUTHPRIV	与安全和授权相关的访问限制消息。很多系统会将这些消息转发到一个安全的文件中。
CRON	时钟后台守护程序生成的消息。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
MAIL	邮件系统生成的消息。
新闻	网络新闻子系统生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
用户	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

选择以下标准系统日志优先级之一，显示在该警报生成的所有通知中：

表 44-4　　系统日志优先级

功率水平	说明
EMERG	紧急状况，向所有用户广播
ALERT	需要立即更正的状况
CRIT	严重的状况
ERR	错误状况
警告	警告消息
请注意！	并未出现错误，但需引起注意的状况
INFO	参考消息
DEBUG	包含调试信息的消息

有关系统日志工作方式和配置方法的详细信息，请参阅系统随附的文档。如果您在基于 UNIX 或 Linux 的系统日志中记录数据，`syslog.conf` man 文件（在命令行键入 `man syslog.con`）和系统日志 man 文件（在命令行键入 `man syslog`）提供有关系统日志工作方式和配置方法的信息。

配置系统日志响应

许可证：保护

您可以配置入侵策略中的系统日志警报。应用访问控制策略中的入侵策略后，一旦系统检测到任何入侵事件，就会通过系统日志发送通知。有关系统日志警报的详细信息，请参阅第 44-4 页上的使用系统日志响应。

要配置系统日志警报选项，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　根据 External Responses 中 **Syslog Alerting** 的启用情况，您有两种选择：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Syslog Alerting 页面。

页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 24-1 页上的在网络分析或入侵策略中使用层。

步骤 5　或者，在 **Logging Hosts** 字段中输入想要指定为日志记录主机的远程访问 IP 地址。用逗号分隔多个主机。

步骤 6　从下拉列表中选择设施和优先级。

有关设施和优先级选项的详细信息，请参阅第 44-4 页上的使用系统日志响应。

步骤 7　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

了解邮件警报

许可证：保护

*邮件警报*是通过邮件发送的入侵事件通知。邮件警报包括以下信息：

- 数据库中的警报总数
- 上一邮件时间 （系统生成上一次邮件报告的时间）
- 当前时间 （系统生成当前邮件报告的时间）
- 新警报总数
- 与指定邮件过滤器相匹配的事件数量 （根据指定规则配置事件的情况下）
- （Summary Output 关闭时）每个事件的时间戳、协议、事件消息和会话信息 （源和目标 IP 地址及端口，显示流量方向）

注　如果多个入侵事件源自同一源 IP，事件下方会出现一则通知，显示其他事件的总数。

- 每个目标端口的事件总数
- 每个源 IP 的事件总数

可以为每个规则或规则组启用或禁用入侵事件邮件警报。不论设备应用了访问控制策略中的哪项入侵策略，都可以使用邮件警报设置。

下表介绍了邮件警报可供设置的参数。

On/Off

启用或禁用邮件通知。

From Address

指定系统发送入侵事件的一个或多个邮件地址。

To Address

指定系统接收入侵事件的邮件地址。要发送邮件给多个收件人，请使用逗号分隔邮件地址。例如：

```
user1@example.com, user2@example.com
```

Max Alerts

指定系统在按 Frequency (seconds) 计算的指定时间段内通过邮件发送的入侵事件最大数量。

Frequency (seconds)

指定系统发送入侵事件的频率。 Frequency 设置也可以指定保存邮件设置的频率。

最低频率：300 秒
最高频率：40 亿秒

Coalesce Alerts

启用或禁用按照源 IP 和事件对入侵事件分组，这样如果同一个源 IP 生成多个相同的入侵事件，页面只会显示一个事件。

请注意，事件过滤后才会执行警报组合 （分组）。因此，如果按照特定规则配置邮件警报，只会接收与 Mail Alerting Configuration 中指定规则相匹配的事件列表。

Summary Output

启用或禁用简要邮件警报，适用于有文字数量限制的设备，例如传呼机。简要邮件警报包含以下内容：

- 事件时间戳
- 对于防御中心，生成事件设备的 IP 地址
- 事件协议
- 源 IP 和端口
- 目标 IP 和端口
- 事件消息
- 同一个源 IP 生成的入侵事件数量

例如：

```
2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0
snort_decoder: Unknown Datagram decoding problem!(116:108)
```

Email Alerting on Specific Rules Configuration

指定将事件发送到一个或多个指定邮件地址的规则或规则组。

有关配置邮件警报的信息，请参阅第 44-7 页上的配置邮件警报。

配置邮件警报

许可证：保护

配置邮件警报后，特定规则或规则组下的入侵事件一旦发生，设备就会发出通知。

接收邮件警报前，您**必须：**

- 配置邮件主机，以便接收邮件警报 （请参阅第 63-17 页上的配置邮件中继主机和通知地址）
- 确保受管设备和防御中心都可反向解析自身 IP 地址

要配置邮件警报选项，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Policies > Intrusion > Email**。

系统将显示 Email Alerting 页面。

步骤 2　选择 **State** 旁边的 **on**，启用邮件警报。

步骤 3　在 **From Address** 字段中，键入邮件警报 From 字段要显示的地址。

步骤 4　在 **To Address** 字段，键入要接收邮件警报的地址。

步骤 5　在 **Max Alerts** 字段中，键入一个邮件中要包含的最大事件数量。

步骤 6　在 **Min Frequency** 字段中，键入要接收邮件警报的最低频率，以秒数计算。

步骤 7　要按 IP 地址给事件分组，请选择 **Coalesce Alerts** 旁边的 **on**。

步骤 8　要发送简要邮件警报，请选择 **Summary Output** 旁边的 **on**。

提示　如果启用了 **Summary Output**，为了减少生成的警报数量，可以考虑启用 **Coalesce Alerts**。也可以考虑将 **Max Alerts** 设置为 1，从而避免设备文本消息缓冲区溢出。

步骤 9　在 **Time Zone** 字段中，从下拉列表中选择相应的时区。

步骤 10　要按规则启用邮件警报，请点击 **Email Alerting per Rule Configuration**。

系统将显示规则组。

提示　要接收所有类别规则的邮件警报，请选择 **Select All**。

步骤 11　执行下列一项或两项操作：

- 如果想要接受某个类别规则的所有邮件警报，点击规则类别旁边的 **All**。
- 如果想要指定该类别单个规则下的邮件警报，点击类别文件夹，然后启用接收邮件警报的规则。

步骤 12　点击 **Save**。

系统将保存邮件警报配置。当适用的入侵事件发生时，就会收到邮件警报。

网络发现简介

FireSIGHT 系统使用称为*网络发现*的功能来监控网络中的流量并构建网络资产的全面映射。

由于受管设备被动观察指定网段上的流量，因此，系统会根据既定的定义（称为*指纹*）比较特定数据包报头值以及来自网络流量的其他唯一数据，以确定网络上主机（包括网络设备）的数量和类型以及这些主机上的操作系统、活动应用和开放端口。

还可以配置 FireSIGHT 系统受管设备来监控网络上的用户活动，以便识别策略违规、攻击或网络漏洞的来源。

要补充系统收集的数据，可以导入由支持 NetFlow 的设备、 Nmap 主动扫描、主机输入功能和用户代理（用户代理驻留在 Microsoft Active Directory 服务器上，会报告 LDAP 身份验证）生成的记录。FireSIGHT 系统将这些记录与其通过直接网络流量观察（按受管设备）收集到的信息整合到一起。

系统可关联网络主机上发生的某些类型的入侵、恶意软件及其他事件，以确定主机何时可能受到危害，并会使用*危害表现* (IOC) 标记来标记这些主机。 IOC 数据使您可以清楚、直接地了解试图攻击受监控网络上主机的威胁。

系统使用所有这些信息帮助执行取证分析、行为分析和访问控制，以及减少和应对组织容易遇到的漏洞和攻击。

有关详情，请参阅：

- 第 45-1 页上的了解发现数据收集
- 第 45-14 页上的了解 NetFlow
- 第 45-17 页上的了解危害表现
- 第 45-19 页上的创建网络发现策略

了解发现数据收集

许可证：FireSIGHT

发现数据包括关于网络主机以及这些主机上的操作系统、活动应用和用户活动的信息。

要开始收集发现数据，必须首先应用访问控制策略。访问控制策略定义允许的流量以及因而可使用网络发现监控的流量。请注意，这意味着，如果使用访问控制阻止某些流量，系统将无法检查主机、用户和应用活动的流量。例如，如果阻止对社交网络应用的访问，系统将不会提供关于社交网络应用的任何发现数据。

应用访问控制策略后，必须配置和应用网络发现策略，后者指定要使用受管设备监控的网段和端口以及要收集的数据类型。应用网络发现政策后，系统开始生成发现数据（可以使用防御中心网络界面查看和分析这些数据）。

系统将网络发现数据存储在防御中心数据库中；有关存储限制的信息，请参阅第 63-14 页上的配置控制面板事件限制。除了数据库限制之外，防御中心可存储的检测到的主机和用户总数取决于 FireSIGHT 许可证。

如果达到许可的用户限值，多数情况下，系统会停止向数据库添加新用户。要添加新用户，必须手动从数据库中删除旧的或非活动用户，或者清除数据库中的所有用户。另一方面，如果达到许可的主机限制，可以将系统配置为会采取以下行动之一：停止向数据库添加新主机；替换进入非活动状态最长时间的主机。

要补充系统收集的数据，可以导入由支持 NetFlow 的设备、 Nmap 主动扫描、主机输入功能和用户代理 （用户代理驻留在 Microsoft Active Directory 服务器上，会报告 LDAP 身份验证）生成的记录。 FireSIGHT 系统将这些记录与其通过直接网络流量观察 （按受管设备）收集到的信息整合到一起。

有关详情，请参阅：

- 第 45-2 页上的了解主机数据收集
- 第 45-3 页上的了解用户数据收集
- 第 45-9 页上的了解应用检测
- 第 45-17 页上的了解危害表现
- 第 45-13 页上的导入第三方发现数据
- 第 45-13 页上的发现数据的用途

了解主机数据收集

许可证：FireSIGHT

由于系统被动监控流经网络的流量，因此，系统会根据既定的定义 （称为*指纹*）比较特定数据包报头值以及来自网络流量的其他唯一数据，以确定关于网络主机的以下信息，包括：

- 主机的数量和类型 （包括网络设备，例如网桥、路由器、负载均衡器和 NAT 设备）
- 基本网络拓扑数据 （包括从网络上的发现点到主机之间的跳数）。
- 主机上运行的操作系统
- 主机上的应用以及与这些应用关联的用户

如果系统无法识别主机的操作系统，可以使用自定义指纹功能创建自定义客户端或服务器指纹。系统将会使用这些指纹来识别新主机。可以将指纹映射到漏洞数据库 (VDB) 中的系统，以便在使用自定义指纹识别主机时显示适当的漏洞信息。有关详细信息，请参阅第 46-6 页上的使用自定义指纹技术。

还可以通过主机输入功能添加或更新主机和操作系统数据。此外，如果创建启用了主机检测的支持 NetFlow 的发现规则，可以从 NetFlow 数据将主机添加到网络映射。

可以使用防御中心网络界面查看系统检测到的主机。

- 有关使用事件查看器查看和搜索主机的信息，请参阅第 50-17 页上的使用主机。
- 有关查看网络映射 （是对网络资产和拓扑的详细表示）的信息，请参阅第 48-1 页上的使用网络映射。
- 有关查看主机配置文件 （配置文件可完整展示检测到的主机的所有可用信息）的信息，请参阅第 49-1 页上的使用主机配置文件。

了解用户数据收集

许可证：FireSIGHT

可以使用 FireSIGHT 系统监控网络上的用户活动，以便将威胁、终端和网络智能与用户身份信息关联起来。通过将网络行为、流量和事件直接与单个用户相关联，系统可帮助您识别策略违规、攻击或网络漏洞的来源。换句话说，系统会告诉您“谁”做了“什么事”。例如，您可以确定：

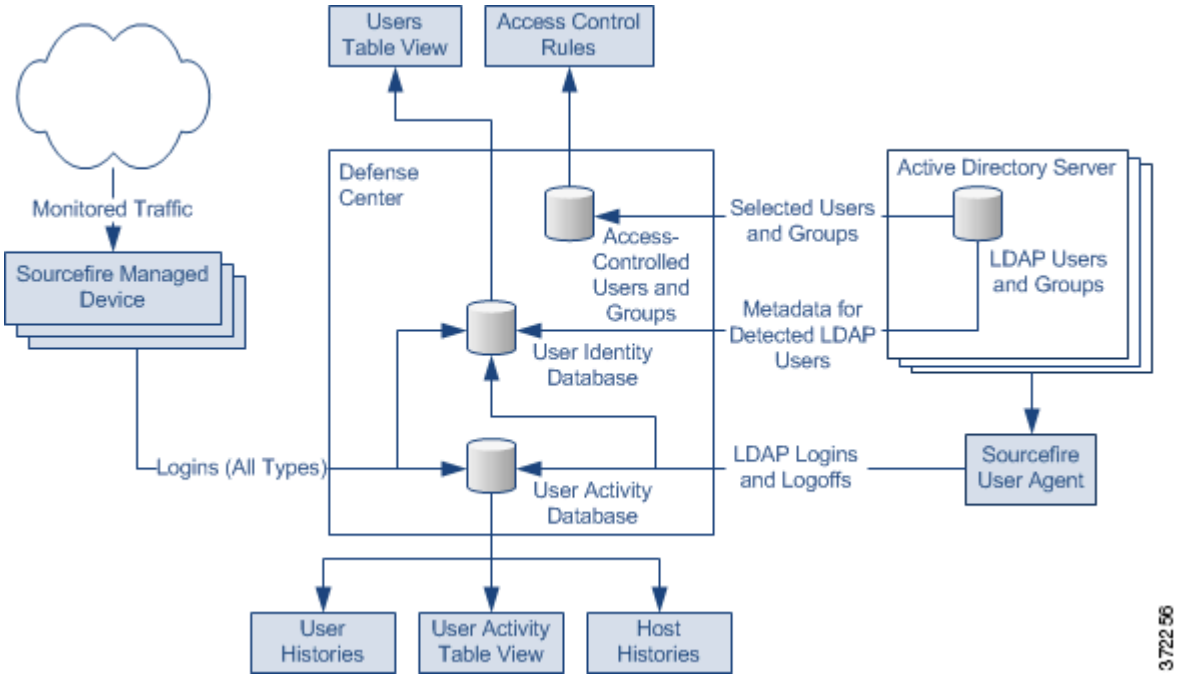
- 谁拥有作为影响程度为 Vulnerable （级别 1：红色）的入侵事件的目标的主机
- 谁发起了内部攻击或端口扫描
- 谁正在尝试未授权访问具有高主机重要性的服务器
- 谁正在耗用异常大量的带宽
- 谁尚未应用关键操作系统更新
- 谁正在使用即时消息软件或 P2P 文件共享应用，而这样做是违反公司的 IT 策略的

借助这些信息，可以采用有针对性的方法降低风险，阻止用户或用户活动，以及采取措施防止其他人的活动中断。这些功能还可以大大改善审核控制并提高合规性。

系统根据 LDAP 连接中的用户感知设置，从 Microsoft Active Directory LDAP 服务器下载用于访问控制策略的用户。用户代理为这些用户将提供登录数据，这些用户将被添加到用户数据库。这些用户称为*访问受控用户*。编写包含用户条件的访问控制策略时，请根据访问控制用户编写这些条件。有关详细信息，请参阅第 17-2 页上的向访问控制规则添加用户条件。

系统从用户登录 （从用户代理、在流量中检测到的应用数据或者从通过 POP3、 SMTP 或 IMAP 进行的邮件登录）检测用户数据时，会根据用户列表检查登录用户。如果登录用户与代理报告的现有用户匹配，登录数据将会分配给该用户。如果登录与现有用户不匹配，会导致创建新用户，除非登录是在 SMTP 流量中。 SMTP 流量中不匹配的登录将被丢弃。

下图说明 FireSIGHT 系统如何收集和存储用户数据。



如图所示，有三种用户数据来源，有三个存储数据的位置。有关用户数据收集的详细信息，请参阅：

托管设备

许可证：FireSIGHT

可以使用网络发现策略配置受管设备，以使它们被动检测在您指定的网络上的 LDAP、 AIM、 POP3、 IMAP、 Oracle、 SIP (VoIP)、 FTP、 HTTP、 MDNS 和 SMTP 登录。请注意，如果在网络发现规则中启用用户发现，将会自动启用主机发现。

注 受管设备仅将用于 LDAP 连接的 Kerberos 登录解释为 LDAP 身份验证。受管设备无法检测使用协议 （例如 SSL 或 TLS）的加密 LDAP 身份验证。

设备检测登录时，它会将以下信息发送到防御中心 （这些信息将被记录为用户活动）：

- 识别出的登录用户名
- 登录时间
- 登录使用的 IP 地址，可能是用户的主机 （用于 LDAP、 POP3、 IMAP 和 AIM 登录）、服务器 （用于 HTTP、 MDNS、 FTP、 SMTP 和 Oracle 登录）或会话发起方 （用于 SIP 登录）的 IP 地址
- 用户的邮件地址 （用于 POP3、 IMAP 和 SMTP 登录）
- 检测到登录的设备名称

如果之前已检测到该用户，防御中心会更新该用户的登录历史记录。请注意，防御中心可以使用 POP3 和 IMAP 登录中的邮件地址与 LDAP 用户 关联。这意味着，举例来说，如果防御中心检测到新的 IMAP 登录，且 IMAP 登录中的邮件地址与某个现有 LDAP 用户的邮件地址匹配，则 IMAP 登录不会创建新用户，而是会更新该 LDAP 用户的历史记录。

如果之前从未检测到该用户，防御中心会将该用户添加到用户数据库。唯一的 AIM、 SIP 和 Oracle 登录始终会创建新用户记录，因为这些登录事件中没有防御中心可与其他登录类型关联的数据。

在以下情况下，防御中心**不**会记录用户活动或用户身份：

- 网络发现策略被配置为忽略登录类型，如第 45-25 页上的限制用户日志记录中所述
- 受管设备检测到 SMTP 登录，但用户数据库不包含之前使用匹配的邮件地址检测到的 LDAP、 POP3 或 IMAP 用户

用户代理

许可证：FireSIGHT

如果组织使用 Microsoft Active Directory LDAP 服务器，思科建议安装用户代理，以便通过 Active Directory 服务器监控用户活动。如果要执行用户控制，**必须**安装和使用用户代理；代理将用户与 IP 地址关联，从而允许将访问控制规则与要触发的用户条件关联。使用一个代理可监控最多五台 Active Directory 服务器上的用户活动。

要使用代理，必须配置连接到代理的每个防御中心与监控的 LDAP 服务器之间的连接。此连接不仅允许检索用户代理检测到的登录和注销用户的元数据，还可用于指定在访问控制规则中使用的用户和组。有关针对用户发现配置 LDAP 服务器的详细信息，请参阅第 17-4 页上的检索访问受控用户和 LDAP 用户元数据。

每个代理均可通过定期按计划轮询或实时监控来监控使用加密流量的登录。用户登录计算机时（无论是在工作站登录还是通过远程桌面登录），Active Directory 服务器会生成登录。

代理还可以监控和报告用户注销情况。当检测到用户从主机 IP 地址注销时，代理会生成注销。当检测到登录主机的用户已更改时（在 Active Directory 服务器报告用户已更改之前），代理也会生成注销。将注销数据与登录数据结合起来，便对登录到网络的用户有了更全面的了解。

轮询 Active Directory 服务器允许代理在定义的轮询时间间隔批量检索用户活动数据。一旦 Active Directory 接收到用户活动数据，实时监控就会将这些数据传输到代理。

可以将代理配置为不报告与特定用户名或 IP 地址相关的登录或注销。这项配置很有用，例如，排除共享服务器上（如文件共享和打印服务器）的重复登录，以及排除为排除故障登录设备的用户。

代理将所有检测到的登录和注销（不包括排除的用户名或 IP 地址）发送到防御中心，作为用户活动进行记录和报告。代理检测 防御中心 版本并以适当的数据格式发送登录记录。对受管设备直接检测到的用户活动提供补充。用户代理报告的登录将用户与 IP 地址相关联，从而允许触发包含用户条件的访问控制规则。

用户代理在用户登录网络或者账户因其他原因使用 Active Directory 凭证进行身份验证时，对用户活动进行监控。版本 2.1 用户代理对主机上的交互式用户登录、远程桌面登录、文件共享身份验证、计算机帐户登录、用户注销以及用户已从其注销的远程桌面会话进行监测。

检测到的登录类型决定代理如何报告登录，以及主机配置文件中登录的显示方式。主机的*授权用户登录*会导致映射到主机 IP 地址的当前用户更改为新登录的用户。其他类型的登录不会更改主机的当前用户，或者仅当主机上的现有用户没有该主机的授权用户登录时，才会更改该主机的当前用户。在这些情况下，如果预期的用户不再处于登录状态，代理会生成该用户的注销。仅在主机上的现有用户没有该主机的授权用户登录时，网络发现检测到的用户登录才会更改该主机的当前用户。代理检测到的登录对网络映射有下列影响：

- 当代理检测到用户对主机的交互式登录或检测到远程桌面登录时，该代理报告主机的授权用户登录并将主机的当前用户更改为新用户。
- 如果代理检测到使用文件共享身份验证的登录，则报告主机的用户登录活动，但不更改主机的当前用户。
- 如果代理检测到计算机帐户登录主机，则生成 NetBIOS 名称更改发现事件，主机配置文件也会反映对 NetBIOS 名称的更改。
- 如果代理检测到一个已排除用户名的登录活动，则不向防御中心报告此登录活动。

发生登录或其他身份验证活动时，代理会向防御中心发送以下信息：

- 用户的 LDAP 用户名
- 发生登录或其他身份验证的时间
- 用户主机的 IP 地址和本地链路地址（如果代理计算机帐户登录报告的是 IPv6 地址）

防御中心将登录和注销消息记录为用户活动。当用户代理报告来自用户登录或注销的用户数据时，会将所报告的用户与用户列表进行比对。如果所报告的用户与代理所报告的现有用户匹配，报告的数据将分配给该用户。如果所报告的用户与现有用户不匹配，则会导致创建一个新用户。

即使不会报告与一个已排除用户名相关的用户活动，但可能仍将报告相关的用户活动。如果代理检测到用户登录机器，然后该代理检测到第二个用户登录，并且您已排除与第二次用户登录相关的用户名的报告，则代理会报告原始用户的注销。但是，不会报告第二个用户的登录活动。因此，不会将任何用户映射到 IP 地址，即使有排除的用户已登录主机。

请注意，代理检测到的用户名具有以下限制：

- 向防御中心报告的以美元符号 ($) 结束的用户名会更新网络映射，但不会显示为用户登录。
- 防御中心对包含 Unicode 字符的用户名显示可能有限制。

防御中心可存储的检测用户的总数取决于 FireSIGHT 许可证。如果达到许可的用户限制，多数情况下，系统会停止向数据库添加新用户。要添加新用户，必须手动从数据库中删除旧的或非活动用户，或者清除数据库中的所有用户。

防御中心-LDAP 服务器连接

许可证：FireSIGHT

防御中心-LDAP 服务器连接使您可以检索某些检测到的用户的元数据。不管 LDAP 用户的登录是受管设备还是用户代理检测到的，都可以检索这些用户的元数据；如果这些用户与 LDAP 用户具有相同的邮件地址，您还可以检索 POP3 和 IMAP 用户的元数据。

如果组织使用 Microsoft Active Directory 服务器，此连接还允许指定要在访问控制规则中使用的 LDAP 用户和用户组。如果要执行用户控制，**必须**配置防御中心与 Active Directory 服务器之间的连接。如果组织不使用 Active Directory，仍可以使用受管设备检测用户登录，还可以从 Oracle 或 OpenLDAP 服务器获取某些用户的元数据。但是，不可以根据这些用户或其活动执行用户控制。

防御中心从 LDAP 服务器获取关于每个用户的以下信息和元数据：

- LDAP 用户名
- 名和姓
- email address
- department
- 电话号码

用户数据库

许可证：FireSIGHT

用户数据库包含受管设备或用户代理检测到的每个用户的记录。防御中心可存储的检测用户的总数取决于 FireSIGHT 许可证。如果达到许可的限制，多数情况下，系统会停止向数据库添加新用户。要添加新用户，必须手动从数据库中删除旧的或非活动用户，或者清除数据库中的所有用户。

但是，系统会优先接受授权用户登录。如果已达到用户数量限制，并且系统检测到之前未检测到的用户的授权用户登录，系统将删除保持非活动状态时间最长的未授权用户，并将其替换为新用户。

可以使用防御中心网络界面查看用户数据库的内容。有关查看、搜索和删除检测到的用户的信息，请参阅第 50-52 页上的使用用户。

用户活动数据库

许可证：FireSIGHT

用户活动数据库包含网络中用户活动的记录，记录可来自受用户代理监控的 Active Directory LDAP 服务器的连接或是通过网络发现得到。系统会在以下情况下记录事件：

- 系统检测到单独的登录或注销
- 系统检测到新用户
- 您手动删除用户
- 系统检测到不在数据库中的用户，但因已达到FireSIGHT许可限制而无法添加该用户

可以使用防御中心网络界面查看系统检测到的用户活动。有关查看、搜索和删除用户活动的信息，请参阅第 50-57 页上的使用用户活动。如果要使用版本 2.1 的用户代理将 LDAP 登录数据发送到防御中心，必须在您想要让代理连接的每个防御中心上为每个代理配置连接。该连接允许代理在与 防御中心 之间建立一个安全的连接，代理可以通过此连接发送登录数据。如果代理配置为排除特定用户名，那么这些用户名的登录数据不会报告给 防御中心。

此外，如果您正计划实施用户访问控制，则必须设置代理与待收集数据的每个 Microsoft Active Directory 服务器之间的连接，并配置用户感知参数。

FireSIGHT 系统会尽可能地将用户活动与其他类型的事件关联。例如，入侵事件可以指出在事件发生时登录源主机和目标主机的用户。

系统还使用用户活动生成*主机历史记录*（跟踪每个用户登录到的主机）和*用户历史记录*（跟踪登录到每个主机的用户）。系统以图形表示过去 24 小时里每个用户的活动和每个主机的登录情况。有关详细信息，请参阅第 50-55 页上的了解用户详细信息和主机历史记录和第 49-19 页上的使用主机配置文件中的用户历史。

访问受控用户数据库

许可证：可控性

访问受控用户数据库包含可在访问控制规则中使用的用户和组，因此，可使用 FireSIGHT 系统执行用户控制。这些用户可以是以下两种类型之一：

- *访问受控用户*为可以添加到访问控制规则以执行用户控制的用户。在配置防御中心-LDAP 服务器连接时，可指定访问受控用户必须所在的组。
- *非访问受控用户*是其他检测到的用户。

在配置防御中心-LDAP 服务器连接时，可指定访问受控用户必须所在的组，如第 17-4 页上的检索访问受控用户和 LDAP 用户元数据中所述。

如果要使用版本 2.1 的用户代理将 LDAP 登录和注销数据发送到版本 5.x 的防御中心，必须在您想要让代理连接的每个防御中心上为每个代理配置连接。该连接允许代理在与 防御中心 之间建立一个安全的连接，代理可以通过此连接发送用户活动数据。

如果代理配置为排除特定用户名，那么这些用户名的用户活动数据将不会报告给防御中心。这些已排除的用户名仍保留在数据库中，但不与 IP 地址关联。

此外，如果您正计划实施用户访问控制，则必须设置代理与待收集数据的每个 Microsoft Active Directory 服务器之间的连接，并配置用户感知参数。

可在访问控制中使用的最大用户数取决于 FireSIGHT 许可证。配置防御中心-LDAP 服务器连接时，请确保所包含的用户总数小于 FireSIGHT 用户许可证数量。有关详情，请参见第 65-6 页上的了解 FireSIGHT 主机和用户许可证限制。

用户数据收集限制

许可证：FireSIGHT

下表介绍了用户数据收集的限制。

表 45-1　　用户感知限制

限制	说明
用户控制	要执行用户控制，组织**必须**使用 Microsoft Active Directory LDAP 服务器。系统从 Active Directory 获取可在访问控制规中使用的用户和组，并使用安装在 Active Directory 服务器上的用户代理所报告的登录和注销数据将用户与 IP 地址进行绑定。
用于 LDAP 连接的非 Kerberos 登录	受管设备仅将用于 LDAP 连接的 Kerberos 登录解释为 LDAP 身份验证。受管设备无法检测到加密的 LDAP 身份验证 （如果它们使用其他协议，例如 SSL 或 TLS）。 另一方面，用户代理使用 Active Directory 服务器上的安全日志收集用户登录数据，且无此类限制。
登录检测	如果要检测 Active Directory 服务器上的登录，必须用服务器 IP 地址配置 Active Directory 服务器连接。有关详细信息，请参阅 《*用户代理配置指南*》。 如果有多个用户使用远程会话登录主机，代理可能无法正常检测到该主机上的登录。有关如何防止这种情况的详细信息，请参阅 《*用户代理配置指南*》。
注销检测	注销可能不会立即被检测到。与注销关联的时间戳反映代理检测到用户不再映射到主机 IP 地址的时间，此时间可能与实际的用户注销主机的时间不一致。 当检测到用户从主机 IP 地址注销时，代理会生成注销。当检测到登录主机的用户已更改时 （在 Active Directory 服务器报告用户已更改之前），代理也会生成注销。
实时数据检索	Active Directory 服务器必须运行 Windows Server 2008 或 Windows Server 2012。
不同用户多次登录到同一主机	系统假设一次只有一个用户登录任何给定主机，且主机的当前用户是最后一次授权用户登录。如果只有未授权登录用户登录到主机，最后的未授权登录用户将被视为当前用户。如果有多个用户通过远程会话登录， Active Directory 服务器报告的最后用户是报告给防御中心的用户。
同一用户多次登录到同一主机	系统记录用户在特定主机的首次登录并忽略后续的登录。如果单个用户是唯一登录到特定主机的人员，则系统唯一记录的登录为原始登录。 然而，如果另一用户登录到该主机，则系统会记录新的登录。如果原始用户再次登录，将会记录其新的登录。
Unicode 字符	用户界面可能无法正确显示包含 Unicode 字符的用户名。
用户数据库中的 LDAP 用户帐户	如果从 LDAP 服务器上移除或禁用某个 LDAP 用户，或者排除向防御中心报告该用户名，防御中心不会从用户数据库中删除该用户，该用户继续被算在数据库所列用户许可数量限制内。必须从数据库中手动清除该用户。 请注意，用户许可证限制对访问受控用户同时应用；访问受控用户的用户计数取决于 LDAP 配置检索到的用户数量。
AOL Instant Messenger (AIM) 登录检测	受管设备只能检测使用 OSCAR 协议的 AIM 登录。尽管大多数 AIM 客户端使用 OSCAR，但是有些使用 TOC2。

了解应用检测

许可证：FireSIGHT

FireSIGHT 系统分析 IP 流量时，会尝试识别网络上常用的应用。应用感知是执行基于应用的访问控制的关键。

系统检测的应用有三种类型：

- *应用协议*（例如 HTTP 和 SSH），代表主机之间的通信
- *客户端*（例如 网络浏览器和邮件客户端），代表在主机上运行的软件
- *网络应用*（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL

系统使用数据包报头中的 ASCII 或十六进制模式或者流量使用的端口来识别网络流量中的应用。有些应用检测器会同时使用端口和特征这两种方式进行检测，以提高正确识别特定应用流量的可能性。此外，安全套接字层 (SSL) 协议检测程序使用安全会话的信息来识别会话中的应用。FireSIGHT 系统中有两种应用检测程序来源：

- *思科提供的检测程序*，用于检测网络应用、客户端和应用协议

  思科提供的应用检测程序 （和操作系统，请参阅第 45-2 页上的了解主机数据收集）的可用性取决于 FireSIGHT 系统的版本和已安装的 VDB 的版本。版本说明和公告包含关于新的和更新的检测程序的信息。也可以导入专业服务开发的单个检测程序。有关所检测到的应用的完整列表，请参阅支持站点。

- *用户定义的应用检测程序*，您可以创建此类检测程序，以增强系统的应用协议检测能力

还可以通过*隐含应用协议检测*来检测应用协议，这种检测根据对客户端的检测暗示应用协议的存在。

系统使用下表中所述的条件来展示其检测到的每个应用的特征。系统使用这些特征创建应用过滤器或应用组。您可以使用这些过滤器和您自己创建的过滤器执行访问控制，以及限制搜索、报告和控制面板构件。有关详细信息，请参阅第 3-13 页上的使用应用过滤器。

表 45-2　　应用特征

特征	说明	示例
类型	应用类型： • **Application Protocols** 代表主机之间的通信。 • **客户端**代表主机上运行的软件。 • **Web Applications** 代表 HTTP 流量的内容或请求的 URL。	HTTP 和 SSH 是应用协议。网络浏览器和邮件客户端是客户端。 MPEG 视频和 Facebook 是网络应用。
风险	应用被用于可能违反组织安全策略之目的的可能性。应用风险的取值范围为 **Very Low** 到 **Very High**。	P2P 应用的风险通常很高。
业务相关性	应用被用于组织的企业运营中 （而不是被用于娱乐目的）的可能性。应用的业务相关性的取值范围为 **Very Low** 到 **Very High**。	游戏应用的业务相关性通常很低。
类别	说明应用的最基本功能的应用通用分类。每个应用都至少归属于一个类别。	Facebook 属于**社交网络**类别。
标记	有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。	视频流网络应用通常标记为**高带宽**和**展示广告**。

为了补充系统生成的应用数据，您可以使用由支持 NetFlow 的设备、 Nmap 主动扫描和主机输入功能生成的记录。

有关详情，请参阅：

- 第 45-10 页上的了解应用协议检测过程
- 第 45-11 页上的通过客户端检测进行隐含应用协议检测
- 第 45-12 页上的有关应用协议检测的特殊注意事项：Squid
- 第 45-12 页上的特殊注意事项：SSL 应用检测
- 第 45-12 页上的特殊注意事项：被推荐网络应用
- 第 46-14 页上的使用应用检测器
- 第 45-13 页上的导入第三方发现数据
- 第 45-14 页上的了解 NetFlow

了解应用协议检测过程

许可证：FireSIGHT

当系统检测应用流量时，它首先确定应用协议是否在使用该特定端口作为唯一的检测条件的检测程序识别出的端口上运行。如果应用协议在这些端口之一上运行，系统会使用已知的端口检测程序正确识别应用协议。

注 由于可以创建并激活在思科提供的检测程序使用的端口上用户定义的基于端口的应用协议检测程序，因此可能会覆盖思科的检测功能。例如，如果用户定义的检测程序将端口 22 上的所有应用协议流量识别为 `myapplication` 应用协议，端口 22 上的 SSH 流量将被错误识别为 `myapplication` 流量。

如果应用协议不是在这些端口之一上运行，系统会使用更强大的方法根据匹配的端口和模式对其进行识别。如果两个检测程序都正确识别流量，使用较长的模式匹配的检测程序将会优先。同样，有多个模式匹配的检测程序优先于单一模式匹配。

请注意，如在网络发现策略中所定义，系统仅识别监控网络的主机上运行的应用协议。例如，如果内部主机访问未受监控的远程站点的 FTP 服务器，系统不会将应用协议识别为 FTP。另一方面，如果远程或内部主机访问正受监控主机上的 FTP 服务器，系统能够正确识别应用协议。

如果系统可识别未受监控的服务器与受监控主机之间的访问连接中使用的客户端，可能会发生异常。在这种情况下，系统可正确识别与连接的客户端对应的适当应用协议，但不会将应用协议添加到网络映射。有关详细信息，请参阅第 45-11 页上的通过客户端检测进行隐含应用协议检测。请注意，客户端会话必须包括来自要发生应用检测的服务器的响应。

下表概括了 FireSIGHT 系统如何识别在防御中心网络界面 （网络映射、主机配置文件、事件视图等）中检测到的应用协议。

表 45-3　FireSIGHT 系统对应用协议的标别

应用	说明
应用协议名称	如果应用协议属于以下情况，防御中心将会使用应用协议名称来识别应用协议： • 由系统正确识别出 • 使用 NetFlow 数据识别出，并且 `/etc/sf/services` 中有端口应用协议关联 • 使用主机输入功能手动识别出 • 由 Nmap 或其他活动源识别出
`pending`	如果系统既不能正确识别也不能错误识别应用，防御中心会将应用协议识别为 `pending`。 大多数情况下，系统需要收集和分析更多连接数据 （识别出的应用所在的数据），然后才能识别待处理应用。 在应用详细信息表、服务器表和主机配置文件中，只会对在其中检测到 （而不是由检测到的客户端或网络应用流量暗示）特定应用协议流量的应用协议显示 `pending` 状态。
`unknown`	如果应用属于以下情况，防御中心会将应用协议识别为 `unknown`： • 不匹配系统的任何检测程序 • 应用协议是使用 NetFlow 数据识别出的，但 `/etc/sf/services` 中没有端口应用协议关联
空白	已检查检测到的所有可用数据，并且没有识别出应用协议。在应用详细信息表、服务器表中和主机配置文件中，对于在其中没有检测到应用协议的非 HTTP 通用客户端数据流量，应用协议留空。

通过客户端检测进行隐含应用协议检测

许可证：FireSIGHT

如果系统可识别未受监控的服务器与受监控主机之间的访问连接中使用的客户端，防御中心会推断该连接使用与该客户端对应的应用协议。（由于系统仅跟踪监控网络上的应用，因此，连接日志通常不包含有关监控主机用于访问未受监控的服务器的连接的应用协议信息。）

通过客户端检测进行隐含应用协议检测有几种后果：

- 由于系统不会为这些服务器生成新的 TCP 端口或新的 UDP 端口事件，因此，服务器不会显示在服务器表中。此外，不能将对这些应用协议的检测作为条件来触发事件警报或关联规则。
- 由于应用协议未与主机关联，因此，不能查看主机配置文件中的详细信息，不能设置其服务器身份，也不能使用流量量变曲线或关联规则的主机配置文件限定条件中的信息。此外，系统不会根据此类检测将漏洞与主机关联。

但是，可以触发关于连接中的应用协议信息的关联事件。还可以使用连接日志中的应用协议信息创建连接跟踪程序和流量量变曲线。

主机限制和发现事件日志记录

许可证：FireSIGHT

如果系统检测到客户端、服务器或网络应用，它会生成发现事件，除非关联的主机已达到客户端、服务器或网络应用的最大数量。

主机配置文件最多为每个主机显示 16 个客户端、 100 个服务器和 100 个网络应用。有关详细信息，请参阅第 49-13 页上的使用主机配置文件中的服务器和第 49-17 页上的查看主机配置文件中的应用。

请注意，依赖于客户端、服务器或网络应用检测的操作不受此限制的影响。例如，经配置要在服务器上触发的访问控制规则仍会记录连接事件。

有关应用协议检测的特殊注意事项：Squid

许可证：FireSIGHT

在以下情况下，系统会正确识别 Squid 服务器流量：

- 系统检测监控网络上主机与启用了代理身份验证的 Squid 服务器之间的连接；或
- 系统检测监控网络上 Squid 代理服务器与目标系统 （即，客户端正在其中请求信息或其他资源的目标服务器）之间的连接

但是，在以下情况下，系统无法识别 Squid 业务流量：

- 监控网络上的主机连接到已禁用代理身份验证的 Squid 服务器；或
- Squid 代理服务器被配置为会从其 HTTP 响应中移除 Via: 报头字段

特殊注意事项：SSL 应用检测

许可证：FireSIGHT

FireSIGHT 系统提供的检测器可以使用安全套接字层 (SSL) 会话中的信息确定会话中的应用协议、客户应用或 Web 应用。

如果系统检测到加密连接，它会将该连接标记为通用 HTTPS 连接或更为具体的安全协议，例如 SMTPS （如果适用）。如果系统检测到 SSL 会话，它会将 `SSL client` 添加到该会话的连接事件中的 **Client** 字段。如果识别到会话的 Web 应用，系统会为该流量生成发现事件。

对于 SSL 应用流量，受管设备还可以检测服务器证书中的公用名并将其与 SSL 主机模式的客户端或 Web 应用比对。当系统识别到特定客户端时，会将 `SSL 客户端`替换为该客户端的名称。

由于 SSL 应用流量已加密，因此，系统只能使用证书中的信息 （而不是加密数据流中的应用数据）进行识别。为此， SSL 主机模式有时只能识别作为应用编写者的公司，因此，同一公司开发的 SSL 应用可能有相同的标别。

在某些情况下，例如 HTTPS 会话是从 HTTP 会话内部发起时，受管设备会从客户端数据包中的客户端证书检测服务器名称。

要启用 SSL 应用标别，必须创建监控响应方流量的访问控制规则。这些规则必须包含适用于 SSL 应用的应用条件或者使用来自 SSL 证书的 URL 的 URL 条件。对于网络发现，响应方 IP 地址必须位于要在网络发现策略中监控的网络上；访问控制策略配置决定是否识别流量。在应用检测程序列表中或在访问控制规则中添加应用条件时，可以按 `SSL protocol` 标记进行过滤，以识别 SSL 应用的检测程序。

特殊注意事项：被推荐网络应用

网络服务器有时会将流量推荐到其他网站，这些网站通常为广告服务器。为了帮助更好地了解网络上发生的被推荐流量的上下文，系统会在被推荐会话事件的 Web Application 字段中列出推荐流量的网络应用。VDB 包含已知被推荐站点的列表。如果系统检测到来自这些站点之一的流量，会将推荐站点连同该流量的事件一起存储。例如，如果通过 Facebook 访问的广告实际在 Advertising.com 上托管，检测到的 Advertising.com 流量与 Facebook网络应用相关。系统还可以检测到 HTTP 流量中的推荐 URL，例如当网站提供与另一站点的简单链接时；在这种情况下，推荐 URL 出现在 HTTP Referrer 事件字段。

在事件中，如果存在推荐应用，它将被列为流量的网络应用，而 URL 则是被推荐站点的 URL。在上述示例中，用于流量的连接事件的网络应用是 Facebook，但 URL 是 Advertising.com。如果未检测到推荐网络应用，如果主机推荐自身，或者如果存在推荐链，被推荐应用在事件中可能会显示为网络应用。在控制面板中，网络应用的连接和字节数包括网络应用与该应用推荐的流量相关的会话。

请注意，如果创建专门针对被推荐流量的规则，应该为被推荐应用 （而不是为推荐应用）添加条件。例如，要阻止从 Facebook 推荐的 Advertising.com 流量，可以向 Advertising.com 应用的访问控制规则添加应用条件。

导入第三方发现数据

许可证：FireSIGHT

可使用 Nmap 主动扫描添加关于操作系统、应用和漏洞的信息，以此补充系统收集到的数据。有关 Nmap 扫描和扫描结果的详细信息，请参阅第 47-1 页上的了解 Nmap 扫描。

还可以使用主机输入功能来补充系统通过监控网络流量收集到的信息，具体做法是，将通过 API 将第三方应用配置为可与 FireSIGHT 系统交互，或者手动添加数据。可以创建产品、漏洞和修复程序映射，以将第三方数据映射到思科定义，从而实现操作系统和服务器的影响关联。有关主机输入功能和映射第三方数据的详细信息，请参阅 *《FireSIGHT 系统主机输入 API 指南》*和第 46-26 页上的导入主机输入数据。

系统会协调收集到的关于操作系统和服务器身份的数据，并根据指纹源优先级值、身份冲突解决设置和收集时间确定每个身份。

还可以配置网络映射以使用来自支持 NetFlow 设备的数据，从而改进网络映射和事件表。有关详细信息，请参阅第 45-14 页上的了解 NetFlow。

发现数据的用途

许可证：FireSIGHT

记录发现数据使得可以利用 FireSIGHT 系统中的许多功能，包括：

- 查看网络映射 （网络映射是对网络资产和拓扑的详细表示，可通过对主机和网络设备、主机属性、应用协议或漏洞进行分组来查看）；请参阅第 48-1 页上的使用网络映射
- 查看主机配置文件 （配置文件可完整展示检测到的主机的所有可用信息）；请参阅第 49-1 页上的使用主机配置文件
- 查看控制面板，（控制面板提供有关网络资产和用户活动的概览及其他功能）；请参阅第 55-1 页上的使用控制面板
- 查看关于系统记录的发现事件和用户活动的详细信息；请参阅第 50-1 页上的使用发现事件
- 根据发现数据创建报告；请参阅第 57-1 页上的使用报告
- 执行应用和用户控制，也就是说，使用应用条件和用户条件编写访问控制规则；请参阅第 16-2 页上的控制应用流量和第 17-2 页上的向访问控制规则添加用户条件
- 将主机及其运行的任何服务器或客户端与它们容易受到的攻击关联，这样可识别和减少漏洞，评估入侵事件对网络的影响，以及调整入侵规则状态以使它们能够为网络资产提供最大程度的保护；请参阅第 49-23 页上的使用主机配置文件中的漏洞、第 41-32 页上的使用影响级别评估事件、第 45-17 页上的了解危害表现和第 33-1 页上的为您的网络资产定制入侵防御
- 在系统生成有特定影响标记的入侵事件或特定类型的发现事件时，通过邮件、 SNMP 陷阱或系统日志向您发出警报；请参阅第 43-1 页上的配置外部警报

- 监控组织是否遵守允许的操作系统、客户端、应用协议和协议的白名单；请参阅第 52-1 页上的将 FireSIGHT 系统用作一个合规工具
- 在系统生成发现事件或检测用户活动时，创建具有会触发和生成关联事件的规则的关联策略；请参阅第 51-1 页上的配置关联策略和规则
- 如果记录 NetFlow 连接，使用这些连接数据；请参阅第 38-4 页上的将连接事件记录到防御中心或外部服务器中

了解 NetFlow

许可证：FireSIGHT

NetFlow 是思科 IOS 软件中一个展示网络操作特征的嵌入式工具。通过 RFC 流程实现标准化后，NetFlow 不仅可在思科网络设备上使用，也可以嵌入到 Juniper、 FreeBSD 和 OpenBSD 设备中。

支持 NetFlow 的设备非常广泛地用于捕获和导出关于流经这些设备的流量的数据。支持 NetFlow 的设备拥有称为 NetFlow 缓存 （存储流经设备的数据流的记录）的数据库。数据流 （在 FireSIGHT 系统中称为*连接*）是数据包序列，代表使用特定端口、协议和应用协议的源主机和目标主机之间的会话。

对于指定的网络， FireSIGHT 系统受管设备检测支持 NetFlow 的设备导出的记录，根据这些记录中的数据生成连接事件，最后将这些事件发送到防御中心以供记录在数据库中。还可以根据 NetFlow 连接中的信息来配置系统，以将主机和应用协议信息添加到数据库。

可以使用这些发现和连接数据补充受管设备直接收集到的数据。如果在受管设备无法监控的网络上部署了支持 NetFlow 的设备，这尤其有用。

可以使用网络发现策略中的规则来配置 NetFlow 数据收集 （包括连接日志记录）。可以将这种数据收集与FireSIGHT 系统受管设备 （根据访问控制规则进行配置）检测到的连接的连接日志记录进行比较，如第 38-13 页上的根据访问控制处理记录连接中所述。由于 NetFlow 数据收集与网络而不是访问控制规则相关联，因此，您不能非常精细地控制要记录哪些连接。此外，系统会自动将所有基于 NetFlow 的连接事件保存到防御中心连接事件数据库；您不能将这些连接发送到系统日志或 SNMP 陷阱服务器。

有关详情，请参阅：

- 第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异
- 第 45-16 页上的准备分析 NetFlow 数据
- 第 45-13 页上的发现数据的用途
- 第 38-4 页上的将连接事件记录到防御中心或外部服务器中

NetFlow 与 FireSIGHT 数据之间的差异

许可证：FireSIGHT

NetFlow 记录中可用的信息比通过使用受管设备监控网络流量而生成的信息有更多限制，但有一种例外情况 （TCP 标记）。由于系统无法直接分析 NetFlow 数据表示的流量，因此在系统处理 NetFlow 记录时，它会使用多种方法将数据转换为连接日志以及主机和应用协议记录。

转换后的 NetFlow 数据与受管设备直接收集到的发现数据和连接数据之间存在一些差异。在执行具有以下要求的分析时，应记住这些差异：

- 需要检测到的连接次数的统计信息
- 需要与操作系统及其他主机相关的信息 （包括漏洞）

- 需要应用数据，包括客户端信息、网络应用信息以及供应商和版本服务器信息
- 需要知道连接中的主机哪个是发起方，哪个是响应方

提示 对于连接事件中的每个字段，第 39-10 页上的表 39-1表指出，可用数据取决于连接是否由 FireSIGHT 系统受管设备直接检测出，或者连接事件是否基于 NetFlow 数据。

每个受监控会话生成的连接事件的数量

对于受管设备直接检测到的连接，可在连接开始和/或结束时记录双向连接事件，具体取决于访问控制规则操作。

但是，由于支持 NetFlow 的设备导出单向连接数据，因此，系统会始终为支持 NetFlow 的设备检测到的每次连接至少生成两个连接事件，具体取决于设备如何配置。这也意味着，对于基于 NetFlow 数据的每次连接，摘要的连接数会每次递增 2，从而提供网络上实际发生的快速增长的连接数量。

请注意，如果将支持 NetFlow 的设备配置为仅在连接结束时输出记录，系统将为该会话生成两个连接事件。另一方面，如果将支持 NetFlow 的设备配置为即使在仍有连接的情况下也会按固定时间间隔输出记录，系统将为设备导出的每个记录生成一个连接事件。例如，如果将支持 NetFlow 的设备配置为每 5 分钟输出一次长期连接的记录，且特定连接持续 12 分钟，那么系统将会为该会话生成 6 个连接事件：

- 前 5 分钟生成一对事件
- 第二个 5 分钟生成一对事件
- 连接终止时生成最后一对事件

为此，思科**强烈**建议将支持 NetFlow 的设备配置为仅在受监控会话关闭时输出记录。

主机和操作系统数据

虽然可以配置网络发现策略以根据 NetFlow 记录将主机添加到网络映射，但主机配置文件不包含连接中主机的任何操作系统或 NetBIOS 数据，系统也无法识别主机是否为网络设备 （网桥、路由器、 NAT 设备或负载均衡器）。但是，可以使用主机输入功能手动设置主机的操作系统身份。

应用程序数据

对于受管设备直接检测到的连接，系统可以通过检查连接中的数据包来识别应用协议、客户端和网络应用。

系统处理 NetFlow 记录时，会使用 `/etc/sf/services` 中的端口关联来推断应用协议身份。但是，这些应用协议不包含供应商或供应商信息，而且连接日志不包含关于会话中使用的客户端或网络应用的信息。但是，可以使用主机输入功能手动提供这些信息。

请注意，简单端口关联意味着在非标准端口上运行的应用协议可能不会被识别或被错误识别。此外，如果不存在关联，系统会在连接日志中将应用协议标记为 `unknown`。

漏洞映射

FireSIGHT 系统无法确定哪些漏洞可能会影响根据 NetFlow 记录添加到网络映射的主机，除非使用主机输入功能手动设置主机操作系统的身份或应用协议身份。请注意，由于 NetFlow 连接中没有客户端信息，因此您无法将客户端漏洞与 NetFlow 主机关联。

连接中发起方和响应方信息

对于受管设备直接检测到的连接，系统可确定哪个主机是发起方 （即，源），哪个主机是响应方（即，目标）。但是， NetFlow 数据不包含发起方或响应方信息。

当系统处理 NetFlow 记录时，它会根据各主机正在使用的端口以及此类端口是否为公认端口来使用一种算法确定该信息：

- 如果使用的两个端口都不是公认端口，系统会将端口号较小的那个主机视为响应方。
- 如果只有一个主机在使用公认端口，系统会将该主机视为响应方。

为此，公认端口是编号为 1 到 1023 的任意端口，或包含受管设备上 `/etc/sf/services` 中应用协议信息的端口。

准备分析 NetFlow 数据

许可证：FireSIGHT

在配置 FireSIGHT 系统以分析 NetFlow 数据之前，必须在路由器或要使用的其他支持 NetFlow 的设备上启用 NetFlow 功能，并将这些设备配置为可将 NetFlow 版本 5 数据导出到连接了受管设备感应接口的目标网络。

请注意，系统可以分析 NetFlow 版本 5 和 NetFlow 版本 9 的记录。如果要将支持 NetFlow 的设备与 FireSIGHT 系统部署配合使用，这些设备**必须**使用这些版本之一。此外，系统要求特定字段必须位于支持 NetFlow 的设备广播的模板和记录中。如果支持 NetFlow 的设备使用版本 9（可自定义），**必须**确保这些设备广播的模板和记录包含以下字段（可以是任意顺序）：

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

由于 FireSIGHT 系统使用受管设备分析 NetFlow 数据，因此，部署必须至少包括一个可监控支持 NetFlow 的设备的受管设备。受管设备上至少要有一个感应接口必须与网络连接，以便能够从该网络收集支持 NetFlow 的设备导出的数据。由于受管设备上的感应接口通常不具有 IP 地址，因此系统不支持直接收集 NetFlow 记录。

此外，**思科强烈**建议将支持 NetFlow 的设备配置为仅在受监控会话关闭时输出记录。如果将支持 NetFlow 的设备配置为按固定时间间隔输出记录，对 NetFlow 记录派生的连接数据的分析可能会更为复杂；请参阅第 45-15 页上的每个受监控会话生成的连接事件的数量。

最后，请注意，在某些支持 NetFlow 的设备上可用的采样 NetFlow 功能只会收集流经设备的数据包子集中的 NetFlow 统计信息。尽管启用此功能可以提高支持 NetFlow 的设备上的 CPU 利用率，但可能会影响收集以供系统分析的数据。

了解危害表现

许可证：FireSIGHT

作为网络发现的一部分， FireSIGHT 系统的数据相关器可以将各种类型的数据 （入侵事件、安全情报、连接事件和恶意软件事件）与主机关联，以确定监控网络上的主机是否可能遭受恶意侵害。这些关联称为危害表现 (IOC)。可以通过在发现策略编辑器中启用此功能以及思科预定义的众多 *IOC 规则*当中的任意一个来激活此功能。启用此功能后，还可以编辑主机配置文件中单个主机的规则状态。每个 IOC 规则都对应于主机关联的一个特定 *IOC 标记*。

除数据相关器外，思科的基于终端的综合安全智能云数据也可以从 IOC 规则生成 IOC 标记。由于这些数据检查主机本身上的活动 （例如，单个程序执行的操作），因此，通过这些数据可了解到纯网络数据无法洞察到的可能威胁。来自终端的 FireAMP IOC 数据通过 思科 云连接进行传输。

带有活动 IOC 标记的主机显示在事件视图的 IP Address 列，同时显示受危害主机图标 () 而不是正常主机图标 ()。可触发 IOC 标记的事件的事件视图指出事件是否已触发 IOC。

了解危害表现类型

许可证：FireSIGHT

有很多威胁表现 (IOC) 规则和标记类型。这些类型全部由思科预定义，一个 IOC 规则对应于一个 IOC 标记。由于 IOC 规则根据 FireSIGHT 系统的其他功能 （对于某些事件，根据 思科 云）提供的数据触发，这些功能对于要设置 IOC 标记的 IOC 规则必须可用且处于活动状态。在思科开发新的基于终端的恶意软件事件 IOC 类型时，系统通过云自动下载并开始使用它们。以下列表详细介绍了 IOC 规则类型、与这些类型相关的功能以及任何其他许可要求 （除了网络发现所需的 FireSIGHT 许可证之外）：

- 第 45-17 页上的基于终端的恶意软件事件 IOC 类型
- 第 45-18 页上的入侵事件 IOC 类型
- 第 45-18 页上的安全情报事件 IOC 类型

基于终端的恶意软件事件 IOC 类型

许可证：FireSIGHT

以下列表包含的 IOC 类型示例与基于终端的恶意软件事件相关联，这些类型需要订用思科云。除了下面列出的 IOC 类型外，思科定期开发新型，系统通过到云的连接自动下载和实施新类型。

有关配置基于终端的恶意软件防护的详细信息，请参阅第 37-21 页上的为 FireAMP 处理云连接和第 37-7 页上的基于网络的 AMP 与基于终端的 FireAMP。

- Adobe Reader 危害 - Adobe Reader 启动了外壳程序
- Adobe Reader 危害 - FireAMP 检测到的 PDF 危害
- CnC 已连接 - FireAMP 检测到的可疑僵尸网络
- 植入程序感染 - FireAMP 检测到的植入程序感染
- Excel 危害 - FireAMP 检测到的 Excel 危害
- Excel 危害 - Excel 启动了外壳程序
- FireAMP 检测到的通用 IOC
- Java 危害 - FireAMP检测到的 Java 危害
- Java 危害 - Java 启动了外壳程序

- 检测到恶意软件 - FireAMP 检测到的威胁 - 未执行
- 检测到恶意软件 - 在文件传输中检测到的威胁
- 执行的恶意软件 - FireAMP 检测到的威胁 - 已执行
- Microsoft 计算器危害 - FireAMP 检测到的 Microsoft 计算器危害
- Microsoft 记事本危害 - FireAMP 检测到的 Microsoft 计算器危害
- PowerPoint 危害 - FireAMP 检测到的 PowerPoint 危害
- PowerPoint 危害 - PowerPoint 启动了外壳程序
- QuickTime 危害 - FireAMP 检测到的 QuickTime 危害
- QuickTime 危害 - QuickTime 启动了外壳程序
- Word 危害 - FireAMP 检测到的 Word 危害
- Word 危害 - Word 启动了外壳程序

入侵事件 IOC 类型

许可证：FireSIGHT+保护

以下 IOC 类型与入侵事件相关（此类事件需要保护许可证）。有关查看入侵事件以及配置入侵检测和防护的详细信息，请参阅第 18-1 页上的使用入侵和文件策略控制流量和第 41-7 页上的查看入侵事件。

- CnC 已连接 - 入侵事件 - malware-backdoor
- CnC 已连接 - 入侵事件 - malware-cnc
- 攻击包 - 入侵事件 - exploit-kit
- 影响 1 攻击 - 影响 1 入侵事件 - attempted-admin
- 影响 1 攻击 - 影响 1 入侵事件 - attempted-user
- 影响 1 攻击 - 影响 1 入侵事件 - successful-admin
- 影响 1 攻击 - 影响 1 入侵事件 - successful-user
- 影响 1 攻击 - 影响 1 入侵事件 - web-application-attack
- 影响 2 攻击 - 影响 2 入侵事件 - attempted-admin
- 影响 2 攻击 - 影响 2 入侵事件 - attempted-user
- 影响 2 攻击 - 影响 2 入侵事件 - successful-admin
- 影响 2 攻击 - 影响 2 入侵事件 - successful-user
- 影响 2 攻击 - 影响 2 入侵事件 - web-application-attack

安全情报事件 IOC 类型

许可证：FireSIGHT+保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

已连接 CnC — 安全情报事件 - CnC 类型 与安全情报事件关联，这是一种连接事件。安全情报功能需要保护许可证。有关配置安全情报以及查看安全情报事件的详细信息，请参阅第 13-1 页上的使用安全情报 IP 地址信誉实施黑名单和第 39-12 页上的查看连接和安全情报数据。

查看和编辑危害表现数据

许可证：FireSIGHT

在网络发现策略之外，可以在 FireSIGHT 系统网络界面的其他几个部分中查看和编辑危害表现 (IOC) 数据：

- 在控制面板中，默认情况下， Summary Dashboard 的 Threats 选项卡会按一段时间内触发的主机和新 IOC 规则显示 IOC 标记。Custom Analysis 构件根据 IOC 数据提供预设。有关信息，请参阅第 55-1 页上的使用控制面板和第 55-13 页上的配置 Custom Analysis 构件。
- Context Explorer 的 Indications of Compromise 部分按 IOC 类别显示主机图，按主机显示 IOC 类别。有关信息，请参阅第 56-3 页上的了解“危害表现”部分。
- 发现 (IOC) 事件、连接事件、安全情报事件、入侵事件和恶意软件事件的事件视图 （在 IOC 列中）显示事件是否触发了 IOC 规则。触发 IOC 规则的基于终端的恶意软件事件的事件类型为FireAMP IOC，并同时显示指明危害的事件子类型。可以根据事件查看器中显示的所有 IOC 数据编写合规性规则。有关详细信息，请参阅：
- 第 39-12 页上的查看连接和安全情报数据
- 第 41-7 页上的查看入侵事件
- 第 40-14 页上的使用恶意软件事件
- 第 50-28 页上的使用危害表现
- 第 51-1 页上的配置关联策略和规则
- 网络映射的 Indications of Compromise 选项卡列出监控网络上的主机 （这些主机按 IOC 标记进行分组）。有关信息，请参阅第 48-4 页上的使用危害表现网络映射。
- 在可能受到危害的主机的主机配置文件视图中，可以查看与该主机关联的所有 IOC 标记，解析该主机的任何或所有 IOC 标记，以及配置 IOC 规则状态。有关信息，请参阅第 49-7 页上的使用主机配置文件中的危害表现。

创建网络发现策略

许可证：FireSIGHT

防御中心上的网络发现策略控制系统如何收集有关组织网络资产以及哪些网段和端口受监控的数据。

策略中的发现规则指定 FireSIGHT 系统监控哪些网络和端口来根据流量中的网络数据生成发现数据，以及策略适用于哪些区域。在规则中，可以配置是否发现主机、应用和用户。可以创建规则来将网络和区域排除在发现范围外。从 NetFlow 设备创建发现规则时，可以选择只记录连接。

网络发现策略有一个默认规则，被配置为会发现 0.0.0.0/0 网络上任何 IPv4 流量中的应用。请注意，必须将访问控制策略应用于目标设备，才可应用网络发现策略。该规则不排除任何网络、区域和端口，未配置主机和用户发现，并且未配置 NetFlow 设备。请注意，默认情况下，网络发现策略应用于已注册到防御中心的任何受管设备。要开始收集主机或数据，必须添加或修改发现规则并将策略重新应用于设备。

请记住，访问控制策略定义允许的流量以及因此可使用网络发现监控的流量。请注意，这意味着，如果使用访问控制阻止某些流量，系统将无法检查主机、用户和应用活动的流量。例如，如果在访问控制策略中阻止对社交网络应用的访问，系统将不会提供关于这些应用的任何发现数据。

如果要调整网络发现范围，可以创建其他发现规则，并修改或移除默认规则。可以从 NetFlow 设备配置数据发现，还可以限制用于网络上发现的用户数据所在流量的协议。

如果要使用 FireSIGHT 系统执行入侵检测和防御，但不需要利用发现数据，可以通过禁用新发现优化性能。首先，确保已应用的访问控制策略不包含带有用户条件、应用条件或 URL 条件的规则。然后，从网络发现策略中移除所有规则，并将策略应用于受管设备。有关配置访问控制规则的详细信息，请参阅第 14-1 页上的使用访问控制规则调整流量。

如果在发现规则中启用用户发现，可通过使用一组应用协议的流量中的用户登录活动来检测用户。如有需要，可以禁用用于所有规则的特定协议中的发现。禁用某些协议有助于避免达到与 FireSIGHT 许可证相关的用户限制，从而为来自其他协议的用户保留可用用户数。

借助高级网络发现设置，可以管理记录哪些数据、如何存储发现数据、哪些危害表现 (IOC) 规则处于活动状态、哪些漏洞映射用于影响评估，以及如果源提供冲突发现数据将会发生什么情况。也可以为主机输入添加 NetFlow 设备和源。

有关详情，请参阅：

- 第 45-20 页上的使用发现规则
- 第 45-25 页上的限制用户日志记录
- 第 45-26 页上的配置高级网络发现选项
- 第 45-32 页上的应用网络发现策略

使用发现规则

许可证：FireSIGHT

发现规则允许您灵活调整为网络映射发现的信息，以仅包括所需的特定数据。网络发现策略中的规则按顺序接受评估。请注意，尽管可使用重叠的监控条件创建规则，但这样做可能会影响系统性能。

将主机或网络排除在监控范围外之后，被排除的主机或网络将不会显示在网络映射中，系统也不会为其报告事件。思科建议将负载均衡器（或负载均衡器上的特定端口）和 NAT 设备排除在监控范围外。这些设备可能会创建过量并有误导性的事件，从而填充数据库并使防御中心过载。例如，受监控的 NAT 设备可能会在短时间内显示其操作系统的多个更新。如果知道负载均衡器和 NAT 设备的 IP 地址，可以将它们排除在监控范围外。

提示 系统可通过检查网络流量识别许多负载均衡器和 NAT 设备。要确定网络上的哪些主机是负载均衡器和 NAT 设备，请应用网络发现策略，等待系统填充网络映射，然后执行限制主机类型的主机搜索。

此外，如果需要创建自定义服务器指纹，应暂时禁止监控用于与正在创建指纹的主机通信的 IP 地址。否则，网络映射和发现事件视图中将会出现大量关于该 IP 地址代表的主机的不准确信息。创建指纹后，可以配置策略，以便再次监控该 IP 地址。有关详细信息，请参阅第 46-9 页上的指纹技术服务器。

此外，思科建议**不要**监控支持 NetFlow 的设备和FireSIGHT 系统受管设备所在的网段。尽管在理想情况下应使用不重叠的规则来配置网络发现政策，但系统不会丢弃受管设备生成的重复连接日志。请注意，**不能**丢弃关于受管设备和支持 NetFlow 的设备检测到连接的重复连接日志。

有关详细信息，请参阅：

- 第 45-21 页上的了解设备选择
- 第 45-21 页上的了解操作和发现的资产
- 第 45-21 页上的了解受监控网络
- 第 45-22 页上的了解网络发现策略中的区域

了解设备选择

许可证：FireSIGHT

如果选择某个发现规则中的 NetFlow 设备，该规则将被限制为为指定网络发现 NetFlow 数据。应先选择 NetFlow 设备再配置规则行为的其他方面，因为选择 NetFlow 设备时可用规则操作会更改。此外，不能为 NetFlow 流量配置端口排除。

在选择网络发现规则中的 NetFlow 设备之前，必须在网络发现高级设置中配置与 NetFlow 设备的连接。有关详细信息，请参阅第 45-29 页上的添加支持 NetFlow 的设备。

了解操作和发现的资产

许可证：FireSIGHT

配置发现规则时，必须为规则选择操作。操作确定在系统处理规则时发现或排除哪些资产。但请注意，规则操作的影响取决于规则是用于从受管设备还是支持 NetFlow 的设备发现数据。

请注意，如果创建不带有用于发现主机或用户的任何规则的网络发现策略，应用该策略将会禁用对设备的新发现。要在将受管设备只用于入侵防御时优化性能，请从策略中移除所有发现规则，并将其应用于主用设备。

下表说明了规则使用这两种方案中指定的操作设置发现的资产。

表 45-4　　发现规则操作

操作	受管设备	NetFlow
排除	将指定网络排除在监控范围外。如果用于连接的源主机或目标主机已被排除在发现范围外，会记录连接，但不会为排除的主机创建发现事件。	
发现：主机	根据发现事件将主机添加到网络映射。（可选操作；如果启用了用户发现，则为必要操作。）	根据 NetFlow 记录将主机添加到网络映射。（必要操作）
发现：应用	根据应用检测程序将应用添加到网络映射。请注意，在没有发现应用的情况下，无法发现规则中的主机或用户。（必要操作）	根据 NetFlow 记录和 `/etc/sf/services` 中的端口应用协议关联将应用协议添加到网络映射。（选填）
发现：用户	将用户添加到用户表，并根据与网络发现策略中配置的用户协议匹配的流量中检测到的活动记录用户活动。（选填）	不适用
记录 NetFlow 连接	不适用	仅记录 NetFlow 连接。不发现主机或应用。

了解受监控网络

许可证：FireSIGHT

发现规则仅用于发现指定网络上主机收到和发出的流量中的受监控资产。对于发现规则，会为符合以下条件的连接执行发现：在指定的网络中至少有一个 IP 地址；且只为要监控的网络中的 IP 地址生成事件。默认发现规则只会发现 `0.0.0.0/0` 和 `::/0` 网络上的应用。

对于启用了指定 NetFlow 设备和 **Log Network Connections** 选项的规则，也会记录发向和来自指定网络中 IP 地址的连接。请注意，网络发现规则提供记录 NetFlow 网络连接的唯一方法。

也可以使用网络对象或对象组指定要监控的网络。如果修改网络发现策略中使用的网络对象，必须重新应用策略，所做的更改才会对发现生效。

了解网络发现策略中的区域

许可证：FireSIGHT

出于性能方面的考虑，应配置每个发现规则，以便规则中的区域包括物理连接到规则中要监控网络的受管设备上的感应接口。

但是，系统可能并不总是告知您网络配置的更改情况。网络管理员可以通过路由或主机更改修改网络配置而无需告知您，这可能会导致您难以随时了解正确的网络发现策略配置。如果您不知道受管设备上的感应接口如何与网络物理连接，请将区域配置保留为默认设置，这可将发现规则应用于部署中的所有区域。（如果没有区域被排除，发现策略将应用于所有区域。）

了解端口排除

许可证：FireSIGHT

可以将特定端口排除在监控范围外，就像将主机排除在监控范围外一样 （请参阅第 45-21 页上的了解操作和发现的资产）。

例如，负载均衡器可在短时间内报告同一端口上的多个应用。可以配置网络发现策略，以便将该端口排除在监控范围外，例如，排除处理 Web 场的负载均衡器上的端口 80。

另一种情况是，组织可以使用采用特定端口范围的自定义客户端。如果来自该客户端的流量生成过多有误导性的事件，可以排除对这些端口的监控。同样，可以决定是否要监控 DNS 流量。在这种情况下，可以将策略配置为不监控端口 53。

添加要排除的端口时，可以决定是使用 Available Ports 列表中的可重用端口对象，将端口直接添加到源或目标排除列表，还是创建新的可重用端口然后将其移至排除列表。

请注意，不能将支持 NetFlow 的设备配置为会将端口排除在监控范围外。

添加发现规则

许可证：FireSIGHT

可以配置发现规则，以根据自身需求定制主机和应用数据的发现。请注意，修改规则中引用的对象后，必须重新应用网络发现策略，所做的更改才会生效。

要添加发现规则，请执行以下操作：

访问：管理员/发现管理员

步骤 1　检查访问控制政策，以确保正在为要在其中发现网络数据的流量记录必要的记录。

有关详细信息，请参阅第 38-13 页上的根据访问控制处理记录连接。要发现大多数数据，请在要发现的流量的连接结束时进行记录。

步骤 2　选择 **Policies > Network Discovery**。

系统将显示 Network Discovery Policy 页面。

步骤 3　点击 **Add Rule**。

系统将显示 Add Rule 弹出窗口。

步骤 4　此时您有两种选择：

- 如果要在 Add Rule 弹出窗口中使用规则监控 NetFlow 流量，请点击 **NetFlow Device**。

  系统将显示 NetFlow Device 页面。

  请注意，仅在 NetFlow 设备已添加到发现政策的情况下， NetFlow 页面才可用。有关详细信息，请参阅第 45-29 页上的添加支持 NetFlow 的设备。

- 如果要使用规则监控受管设备，请跳至第 6 步。

有关详细信息，请参阅第 45-14 页上的NetFlow 与 FireSIGHT 数据之间的差异和第 45-21 页上的了解设备选择

步骤 5　从下拉列表中选择要使用的 NetFlow 设备的 IP 地址。

步骤 6　设置规则操作：

- 要从网络发现中排除与规则匹配的所有流量，请选择 **Exclude**。请注意，选择此规则操作后，Port Exclusions 选项卡会被禁用。
- 要在与规则匹配的流量中发现选定类型的数据，请选择 **Discovery**，并选中或取消选中相应的数据类型复选框。

  如果监控受管设备流量，需要记录应用。如果监控用户，需要记录主机。请注意，如果监控 NetFlow 流量，将不能记录用户，记录应用则是可选操作。

- 如果监控 NetFlow 流量，要使用规则记录 NetFlow 流量中的连接，请选择 **Log NetFlow Connections**。请注意，只在选择了规则中的 NetFlow 设备后，此选项才会显示。

注　系统根据网络发现策略设置检测 NetFlow 流量中的连接。可在访问控制策略中配置受管设备流量中的连接日志记录。有关详细信息，请参阅第 38-1 页上的记录网络流量中的连接。

有关规则操作和资产发现的详细信息，请参阅第 45-21 页上的了解操作和发现的资产

步骤 7　每个发现规则必须至少包含一个网络。或者，要限制对于特定网络的规则操作，请点击 **Networks** 选项卡，从 **Available Networks** 列表中选择网络，然后点击 **Add**，或者在 Networks 列表下键入网络并点击 **Add**。

有关网络监控的信息，请参阅第 45-21 页上的了解受监控网络。有关将网络对象添加到 Available Networks 列表的信息，请参阅第 45-24 页上的创建网络对象。请注意，如果修改网络发现策略中使用的网络对象，必须重新应用策略，所做的更改才会对发现生效。

步骤 8　或者，要限制对于特定区域中流量的规则操作，请点击 **Zones**，从 **Available Zones** 列表中选择一个区域或多个区域，然后点击 **Add**。

有关选择要监控的区域的信息，请参阅第 45-22 页上的了解网络发现策略中的区域。

步骤 9　要将端口排除在监控范围外，请点击 **Port Exclusions**。

系统将显示 Port Exclusions 页面。

步骤 10　要将特定源端口排除在监控范围外，您有两种选择：

- 从 **Available Ports** 列表中选择一个或多个端口，然后点击 **Add to Source**。
- 要在不添加端口对象的情况下排除来自特定源端口的流量，在 **Selected Source Ports** 列表下，从 **Protocol** 下拉列表中选择相应的协议，在 **Port** 字段中键入一个 1 到 65535 之间的端口号，然后点击 **Add**。

  有关将端口排除在监控范围外的信息，请参阅第 45-22 页上的了解端口排除。有关将端口对象添加到 Available Ports 列表的信息，请参阅第 45-24 页上的创建端口对象。请注意，如果修改网络发现策略中使用的端口对象，必须重新应用策略，所做的更改才会对发现生效。

步骤 11　要将特定目标端口排除在监控范围外，您有两种选择：

- 从 **Available Ports** 列表中选择一个或多个端口，然后点击 **Add to Destination**。
- 要在不添加端口对象的情况下排除来自特定目标端口的流量，在 **Selected Destination Ports** 列表下，从 **Protocol** 下拉列表中选择相应的协议，在 **Port** 字段中键入一个 1 到 65535 之间的端口号，然后点击 **Add**。

步骤 12　规则编辑完毕后，点击 **Save** 返回到发现策略规则列表。

必须应用网络发现策略，所做的更改才会生效。有关详细信息，请参阅第 45-32 页上的应用网络发现策略。

创建网络对象

许可证：FireSIGHT

发现规则中显示的可用网络列表包含可在 FireSIGHT 系统的任何位置使用的可重用网络对象和对象组。可以将新的网络对象添加到该列表。请注意，修改规则中引用的对象后，必须重新应用网络发现策略，所做的更改才会生效。

要创建新的网络对象，请执行以下操作：

管理员/发现管理员

步骤 1　选择 **Policies > Network Discovery**。

系统将显示 Network Discovery Policy 页面。

步骤 2　点击 **Add Rule**。

系统将显示 Add Rule 弹出窗口。

步骤 3　在 Networks 页面上，点击添加图标 ( )。

系统将显示 Network Objects 弹出窗口。

步骤 4　在 **Name** 字段中为网络对象键入名称。您可以使用除小竖线 (|) 或花括号({}) 之外的任何可打印标准 ASCII 字符。

步骤 5　为要添加到网络对象的每个 IP 地址、 CIDR 块和前缀长度键入一个值，然后点击 **Add**。

步骤 6　点击 **Save** 以将网络对象添加到 Available Networks 列表。

提示　如果添加的网络没有立即显示在列表中，请点击刷新图标 ( )。

创建端口对象

许可证：FireSIGHT

发现规则中显示的可用端口列表包含可在 FireSIGHT 系统的任何位置使用的可重用端口对象和对象组。可以将新的端口对象添加到该列表。请注意，修改规则中引用的对象后，必须重新应用网络发现策略，所做的更改才会生效。

要创建新的端口对象，请执行以下操作：

管理员/发现管理员

步骤 1　点击 **Port Exclusions**。

系统将显示 Port Exclusions 页面。

步骤 2　要将端口添加到 Available Ports 列表，请点击添加对象图标 ( )。

系统将显示 Port Objects 弹出窗口。

步骤 3　在 **Name** 字段中为端口对象提供名称。您可以使用除小竖线 (|) 或花括号({}) 之外的任何可打印标准 ASCII 字符。

步骤 4　在 **Protocol** 字段中，指定要排除的流量协议。

选择 **TCP**、 **UDP** 或 **Other**，然后从下拉列表中选择一个选项以选择协议，或者选择 **All**。

步骤 5　在 **Port(s)** 字段中，输入要排除在监控范围外的端口。

可以指定单个端口、用破折线 (-) 分隔的一系列端口或者用逗号分隔的端口和端口范围列表。允许的端口值介于 1 到 65535 之间。

步骤 6　点击 **Save** 以将端口添加到 Available Ports 列表。

提示　如果添加的端口没有立即显示在列表中，请点击刷新图标 ( )。

限制用户日志记录

许可证：FireSIGHT

如果应用的网络发现策略带有可发现用户的规则，则将会在使用 AIM、 IMAP、 LDAP、 Oracle、 POP3、 SMTP、 FTP、 HTTP、 MDNS 和 SIP 协议的流量中发现用户。这些用户已添加到用户表，可通过 Analysis 菜单访问。可以限制在其中发现用户活动的协议，以减少检测到的用户的总数，以便将重点放在可能提供最完整用户信息的用户。

防御中心可存储的检测用户的总数取决于 FireSIGHT 许可证。如果达到许可的限制，多数情况下，系统会停止向数据库添加新用户。要添加新用户，必须手动从数据库中删除旧的或非活动用户，或者清除数据库中的所有用户。限制协议检测有助于最大程度地减少用户名混乱以及保留 FireSIGHT 用户许可证。

例如，如果通过协议 （例如 AIM、 POP3 和 IMAP）获取用户名，可能会由于承包商、访客及其他访客的网络访问而引入与组织无关的用户名。

再如， AIM、 Oracle 和 SIP 登录可能会创建外来用户记录。之所以会发生这种情况，是因为这些登录类型没有与系统从 LDAP 服务器获取的任何用户元数据关联，也没有与受管设备会检测的其他类型登录中包含的任何信息关联。因此，防御中心无法将这些用户与其他类型的用户关联。

请记住，只有受管设备可以检测非 LDAP 用户登录。如果仅使用安装在 Microsoft Active Directory 服务器上的用户代理检测用户活动，限制非 LDAP 登录将不起作用。此外，也不能限制 SMTP 日志记录。这是因为未根据 SMTP 登录将用户添加到数据库；虽然系统会检测 SMTP 登录，这些登录不会被记录下来，除非数据库中包含已具有匹配邮件地址的用户。

可以选择是否记录在 LDAP、POP3、FTP 或 IMAP 流量中检测到的失败用户登录尝试。如果登录尝试失败，不会将新用户添加到数据库的用户列表中。请注意，用户代理不报告失败的登录活动。检测到的失败登录活动的用户活动类型是 Failed User Login。

请注意，系统无法区分失败和成功的 HTTP 登录。要查看 HTTP 用户信息，您必须启用 **Capture Failed Login Attempts**。

要限制在其中检测用户登录的协议，请执行以下操作：

管理员/发现管理员

步骤 1　选择 **Policies > Network Discovery**。

系统将显示 Network Discovery Policy 页面。

步骤 2　点击 **User**。

系统将显示 User 页面。

步骤 3　选中要检测登录的协议的复选框，或取消选中不要检测登录的协议的复选框。

步骤 4　或者，要记录在 LDAP、POP3、FTP 或 IMAP 流量中检测的失败登录尝试，或捕获 HTTP 登录的用户信息，请启用 **Capture Failed Login Attempts**。

步骤 5　点击 **Save** 以保存网络策略。

必须应用网络发现策略，所做的更改才会生效。有关详细信息，请参阅第 45-32 页上的应用网络发现策略。

配置高级网络发现选项

许可证：FireSIGHT

可以使用网络发现策略的 Advanced 选项卡来配置策略范围的设置，以指定要检测的事件、发现数据的保留时间长度和更新频率、用于影响关联的漏洞映射，以及如何解决操作系统和服务器身份冲突。此外，还可以添加主机输入源和支持 NetFlow 的设备，以允许从其他源导入数据。

请注意，可在系统策略中设置发现和用户活动事件的数据库事件限制。有关详细信息，请参阅第 63-14 页上的配置控制面板事件限制。

要配置高级设置，请执行以下操作：

管理员/发现管理员

步骤 1　选择 **Policies > Network Discovery**。

系统将显示 Network Discovery Policy 页面。

步骤 2　点击 **Advanced**。

系统将显示 Advanced 页面。

步骤 3　根据需要编辑高级设置：

- 第 45-27 页上的配置常规设置
- 第 45-27 页上的配置身份冲突解决
- 第 45-28 页上的启用漏洞影响评估映射
- 第 45-29 页上的设置危害表现规则
- 第 45-29 页上的添加支持 NetFlow 的设备
- 第 45-30 页上的配置数据存储

- 第 45-31 页上的配置发现事件日志记录
- 第 45-32 页上的添加身份源

步骤 4　完成配置设置后，点击 **Save** 保存策略。

步骤 5　完成并保存策略后，应用策略以使更新后的设置生效。有关详细信息，请参阅第 45-32 页上的应用网络发现策略。

配置常规设置

许可证：FireSIGHT

常规设置控制系统更新网络映射中信息的频率以及是否在发现过程中捕获服务器横幅。

Capture Banners

如果希望系统存储来自播发服务器供应商和版本的网络流量的报头信息（“横幅”），请选中此复选框。这些信息可提供有关收集的信息的其他上下文。可以通过访问服务器详细信息来访问为主机收集的服务器横幅。

更新间隔

系统更新信息（例如，上一次显示任何主机的 IP 地址的时间、使用应用的时间或应用的点击次数）的时间间隔。默认设置为 3600 秒（1 小时）。

请注意，为更新超时设置较小的时间间隔可在主机显示中提供更准确的信息，但会生成更多网络事件。

要更新常规设置，请执行以下操作：

管理员/发现管理员

步骤 1　点击 **General Settings** 旁的编辑图标 ( )。

系统将显示 General Settings 弹出窗口。

步骤 2　根据需要更新设置。

步骤 3　点击 **Save**，以保存常规设置并返回到网络发现策略的 Advanced 选项卡。

必须应用网络发现策略，所做的更改才会生效。有关详细信息，请参阅第 45-32 页上的应用网络发现策略。

配置身份冲突解决

许可证：FireSIGHT

系统根据流量模式匹配操作系统和服务器的指纹，以确定在特定主机上运行的操作系统和应用。为了提供最可靠的操作系统和服务器身份信息，系统会核对来自多个源的指纹信息。

系统使用所有被动数据来推导操作系统身份并分配置信度值。有关当前身份以及系统如何选择当前身份的详细信息，请参阅第 46-3 页上的增强网络映射。

默认情况下，由扫描程序或第三方应用添加的身份数据会覆盖 FireSIGHT 系统检测到的身份数据，除非存在身份冲突。可以使用 Identity Sources 设置按优先级对扫描程序和第三方应用指纹源进行评级。系统为每个源保留一个身份，但只有优先级最高的第三方应用或扫描程序源中的数据可用作当前身份。但请注意，用户输入数据会覆盖扫描程序和第三方应用数据，无论后者的优先级如何。

身份冲突是指系统检测到某个身份与来自 Identity Sources 设置中列出的活动扫描程序或第三方应用源或者来自 FireSIGHT 系统用户的现有身份相冲突。默认情况下，身份冲突不会自动解决，必须通过主机配置文件，或者通过重新扫描主机或重新添加新的身份数据覆盖被动身份来解决冲突。但是，可以将系统设置为通过保留被动身份自动解决冲突，或始终通过保留主动身份解决冲突。

Generate Identity Conflict Event

启用此选项将会在网络映射中主机上发生身份冲突时生成事件。

Automatically Resolve Conflicts

您有以下选项：

- 要手动强制解决身份冲突，请从 **Automatically Resolve Conflicts** 下拉列表中选择 **Disabled**。
- 要在发生身份冲突时使用被动指纹，请从 **Automatically Resolve Conflicts** 下拉列表中选择 **Identity**。
- 要在发生身份冲突时使用优先级最高的活动源中的当前身份，请从 **Automatically Resolve Conflicts** 下拉列表中选择 **Keep Active**。

要更新身份冲突解决设置，请执行以下操作：

管理员/发现管理员

步骤 1　点击 **Identity Conflict Settings** 旁边的编辑图标 ( )。

系统将显示 Edit Identity Conflict Settings 弹出窗口。

步骤 2　根据需要更新设置。

步骤 3　点击 **Save**，以保存身份冲突设置并返回到网络发现策略的 **Advanced** 选项卡。

必须应用网络发现策略，所做的更改才会生效。有关详细信息，请参阅第 45-32 页上的应用网络发现策略。

启用漏洞影响评估映射

许可证：FireSIGHT

可以配置 FireSIGHT 系统如何对入侵事件执行关联影响。有以下选项可供选择：

- 如果要使用基于系统的漏洞信息执行影响关联，请选择 **Use Network Discovery Vulnerability Mappings**。
- 如果要使用第三方漏洞引用执行关联影响，请选择 **Use Third-Party Vulnerability Mappings**。有关详细信息，请参阅第 46-30 页上的映射第三方漏洞或《*FireSIGHT 系统主机输入 API 指南*》。

可以同时选中这两个复选框或选中其中之一。如果系统生成入侵事件，且该事件涉及的主机所拥有的服务器或操作系统包含所选漏洞映射集中的漏洞，则该入侵事件将带有 Vulnerable （级别 1：红色）影响图标。请注意，对于没有供应商或版本信息的任何服务器，需要在系统策略中配置漏洞映射。有关详细信息，请参阅第 63-27 页上的映射服务器的漏洞。

如果取消选中这两个复选框，入侵事件将**不会**带有 Vulnerable （级别 1：红色）影响图标。有关详细信息，请参阅第 41-32 页上的使用影响级别评估事件。

要更新漏洞设置，请执行以下操作：

管理员/发现管理员

步骤 1　点击 **Vulnerabilities to use for Impact Assessment** 旁边的编辑图标 ( )。

系统将显示 Edit Vulnerability Settings 弹出窗口。

步骤 2　根据需要更新设置。

步骤 3　点击 **Save**，以保存漏洞设置并返回到网络发现策略的 Advanced 选项卡。

必须应用网络发现策略，所做的更改才会生效。有关详细信息，请参阅第 45-32 页上的应用网络发现策略。

设置危害表现规则

许可证：FireSIGHT

要使系统检测和标记危害表现 (IOC)，必须首先在发现规则中至少激活一个 IOC 规则。每个 IOC 规则对应于一种类型的 IOC 标记，所有 IOC 规则均由思科预定义；您不能创建原始规则。可根据网络和组织需要启用任何或全部规则。例如，如果使用诸如 Microsoft Excel 等软件的主机从未出现在监控网络上，可决定不启用与基于 Excel 的威胁相关的 IOC 。有关 IOC 功能的详细信息，请参阅第 45-17 页上的了解危害表现。

启用 IOC 规则后，必须启用与之相关的 FireSIGHT 系统功能 （例如，入侵防御和恶意软件防护）；如果未启用规则的相关功能，将不会收集相关数据，规则也将无法触发。有关 IOC 规则类型及其相关功能的详细信息，请参阅第 45-17 页上的了解危害表现类型。

要设置发现策略中的危害表现规则，请执行以下操作：

管理员/发现管理员

步骤 1　点击 **Indications of Compromise Settings** 旁边的编辑图标 ( )。

系统将显示 Edit Indications of Compromise Settings 弹出窗口。

步骤 2　要关闭或关闭整个 IOC 功能，请点击 **Enable IOC** 旁边的滑块。

步骤 3　要启用或禁用单个 IOC 规则，请点击相应规则的 **Enabled** 列中的滑块。

步骤 4　点击 **Save**，以保存 IOC 规则设置并返回到发现策略的 Advanced 选项卡。

已保存您的更改。

必须应用网络发现策略，所做的更改才会生效。有关详细信息，请参阅第 45-32 页上的应用网络发现策略。

添加支持 NetFlow 的设备

许可证：FireSIGHT

如果已启用支持 NetFlow 的设备上的 NetFlow 功能，可以使用这些设备导出的连接数据来补充思科设备收集的连接数据。

在发现规则中使用支持 NetFlow 的设备之前，必须配置要使用的设备 （请参阅第 45-16 页上的准备分析 NetFlow 数据），然后将它们添加到网络发现策略。

有关将 NetFlow 数据与 FireSIGHT 系统配合使用的详细信息 （包括有关其他先决条件的信息），请参阅第 45-14 页上的了解 NetFlow。

要添加用于连接数据收集的支持 NetFlow 的设备，请执行以下操作：

管理员/发现管理员

步骤 1　选择 **Policies > Network Discovery**。

系统将显示 Network Discovery Policy 页面。

步骤 2　点击 **Advanced**。

系统将显示 Advanced 页面。

步骤 3　点击 NetFlow Devices 旁边的添加图标 ( )。

系统将显示 Add NetFlow Device 弹出窗口。

步骤 4　在 **IP Address** 字段中，输入要用于收集连接数据的支持 NetFlow 设备的 IP 地址。

步骤 5　要添加其他支持 NetFlow 的设备，请重复第 3 步和第 4 步。

提示　要移除支持 NetFlow 的设备，请选择要移除的设备旁边的删除图标 ( )。请记住，如果使用发现规则中支持 NetFlow 的设备，必须先删除规则，才能从 Advanced 页面删除设备。有关详细信息，请参阅第 45-20 页上的使用发现规则。

步骤 6　点击 **Save**。

设备将显示在支持 NetFlow 的设备列表中。

必须应用网络发现策略，所做的更改才会生效。有关详细信息，请参阅第 45-32 页上的应用网络发现策略。

配置数据存储

许可证：FireSIGHT

数据存储设置控制数据库中存储的数据类型，进而确定 FireSIGHT 系统可使用的数据。这些设置还控制数据在网络映射中保留多长时间。

以下选项包含网络发现数据存储设置。

When Host Limit Reached

可以控制如果防御中心达到其主机限制 （取决于 FireSIGHT 许可证）且网络映射已满，将会如何处理主机。如果希望防止欺骗主机代替网络映射中有效的主机，此选项特别有用。要丢弃旧主机，请从 **When Host Limit Reached** 下拉列表中选择 **Drop hosts**。要丢弃新主机，请从 **When Host Limit Reached** 下拉列表中选择 **Don't insert new hosts**。有关详细信息，请参阅第 65-6 页上的了解 FireSIGHT 主机和用户许可证限制。

Host Timeout

系统在网络映射丢弃进入非活动状态的来自网络映射主机前允许它们存在的时间 （以分钟为单位）。默认设置为 10080 分钟 （7 天）。单个主机 IP 和 MAC 地址可以单独超时，但是，只有所有相关地址已超时的情况下主机才会从网络映射中消失。

为避免主机提前超时，请确保主机超时值大于网络发现政策中的更新时间间隔。有关更新时间间隔的详细信息，请参阅第 45-27 页上的配置常规设置。

服务器超时

系统在丢弃进入非活动状态的服务器前允许它们存在的时间 （以分钟为单位）。默认设置为 10080 分钟 （7 天）。

为避免服务器提前超时，请确保服务器超时值大于网络发现政策中的更新时间间隔。有关详细信息，请参阅第 45-27 页上的配置常规设置。

Client Application Timeout

系统在丢弃进入非活动状态的客户端前允许它们存在的时间 （以分钟为单位）。默认设置为 10080 分钟 （7 天）。

应确保客户端超时值大于网络发现策略中的更新时间间隔。有关详细信息，请参阅第 45-27 页上的配置常规设置。

要更新数据存储设置，请执行以下操作：

管理员/发现管理员

步骤 1　点击 **Data Storage Settings** 旁边的编辑图标 ( )。

系统将显示 Data Storage Settings 弹出窗口。

步骤 2　根据需要更新设置。

步骤 3　点击 **Save**，以保存数据存储设置并返回到网络发现策略的 Advanced 选项卡。

必须应用网络发现策略，所做的更改才会生效。有关详细信息，请参阅第 45-32 页上的应用网络发现策略。

配置发现事件日志记录

许可证：FireSIGHT

事件日志记录设置控制是否记录发现和主机输入事件。如果不记录事件，将无法在事件视图中检索事件，也不能将事件用于触发关联规则。

要设置事件日志记录设置，请执行以下操作：

管理员/发现管理员

步骤 1　点击 **Event Logging Settings** 旁边的编辑图标 ( )。

系统将显示 Event Logging Settings 弹出窗口。

步骤 2　选中或取消选中要在数据库中记录的发现和主机输入事件类型旁边的复选框。有关每种事件类型的信息，请参阅第 50-8 页上的了解发现事件类型和第 50-11 页上的了解主机输入事件类型。

步骤 3　点击 **Save**，以保存事件日志记录设置并返回到网络发现策略的 Advanced 选项卡。

必须应用网络发现策略，所做的更改才会生效。有关详细信息，请参阅第 45-32 页上的应用网络发现策略。

添加身份源

许可证：FireSIGHT

可以通过此页面添加新的活动源，或者更改现有源的优先级或超时设置。请注意，将扫描程序添加到此页面不会添加 Nmap 扫描程序已有的完整集成功能，但允许集成导入的第三方应用或扫描结果。如果从第三方应用或扫描程序导入数据，请务必确保将源中的漏洞映射到网络映射中的漏洞。有关详细信息，请参阅第 46-30 页上的映射第三方漏洞。

要添加身份源，请执行以下操作：

管理员/发现管理员

步骤 1　点击 **OS and Server Identity Sources** 旁边的编辑图标 ( )。

系统将显示 Edit OS and Server Identity Sources 弹出窗口。

步骤 2　要添加新源，请点击 **Add Source**。

系统将显示 Add Identity Source 弹出窗口。

步骤 3　在 **Name** 字段中为源键入名称。

步骤 4　从 **Type** 下拉列表中选择输入源类型：

- 如果要使用 AddScanResult 函数导入扫描结果，请选择 **Scanner**。
- 如果不打算导入扫描结果，请选择 **Application**。

步骤 5　要指定从该源将某个身份添加到网络映射到删除该身份之间的持续时间，请从 **Timeout** 下拉列表中选择 **Hours**、 **Days** 或 **Weeks**，并键入适当的持续时间。

提示　要删除已添加的源，请点击源旁边的删除图标 ( )。

步骤 6　或者，要升级某个源并使用操作系统和应用身份以支持列表中该源下面的源，请选择该源并点击向上箭头。

步骤 7　或者，要降级某个源并且只有列表中该源上面的源没有提供身份时才会使用操作系统和应用身份，请选择改源并单击向下箭头。

步骤 8　点击 **Save**，以保存身份源设置并返回到网络发现策略的 Advanced 选项卡。

必须应用网络发现策略，所做的更改才会生效。有关详细信息，请参阅第 45-32 页上的应用网络发现策略。

应用网络发现策略

许可证：FireSIGHT

默认情况下，网络发现策略应用于已在防御中心中注册的受管设备上的任何目标区域。应用网络发现策略使系统可以根据规范监控网络。如果更改了网络发现策略，必须重新应用该策略，所做的更改才会生效。

如果重新应用网络发现策略：

- 系统会删除并重新发现监控网络上主机的网络映射中的 MAC 地址、 TTL 和跳数信息。
- 受影响的受管设备会丢弃任何尚未发送到防御中心的发现数据

应用网络发现策略时，请确保已将访问控制策略应用于受防御中心管理的所有设备。如果尚未将访问控制策略应用于每台设备，则网络发现策略应用将会失败。请主机，不能将网络发现策略应用于未安装 FireSIGHT 许可证的防御中心。

如果修改网络发现策略中使用的网络对象或端口对象，必须重新应用策略，所做的更改才会对发现生效。

请注意，不能将网络发现应用于运行不同版本 FireSIGHT 系统的堆叠设备 （例如，如果其中一个设备的升级失败）。

要应用网络发现策略，请执行以下操作：

管理员/安全审批者

步骤 1　选择 **Policies > Network Discovery**。

系统将显示 Network Discovery Policy 页面。

步骤 2　点击**应用 (Apply)**。

系统将显示一条消息，要求您确认是否要将策略应用于防御中心上访问控制策略所针对的所有区域。

步骤 3　点击 **Yes** 应用策略。

增强网络发现

FireSIGHT 系统收集的有关网络流量的信息对您最有价值，因为系统可以参考该信息来识别网络上最易受攻击和最重要的主机。

例如，如果网络上有多个运行自定义版本的 SuSE Linux 的设备，系统无法识别操作系统，因此无法将漏洞映射至主机。然而，知道系统拥有 SuSE Linux 的漏洞列表，您可能想要为某个主机创建自定义的指纹，以便随后可将该指纹用来识别运行相同操作系统的其他主机。可将 SuSE Linux 漏洞列表的映射纳入指纹中，以便将该列表与匹配指纹的每个主机关联。

系统还允许使用主机输入功能，将来自第三方系统的主机数据直接输入至网络映射。然而，第三方操作系统或应用数据不会自动映射至漏洞信息。如果想要为使用第三方操作系统、服务器和应用协议数据的主机查看漏洞并执行影响关联，必须将来自第三方系统的供应商和版本信息映射至漏洞数据库 (VDB) 中列出的供应商和版本。您也可能想要持续维护主机输入数据。请注意，即使将应用数据映射至 FireSIGHT 系统供应商和版本定义，导入的第三方漏洞也不用于客户端或网络应用的影响评估。

如果系统无法识别网络主机上运行的应用协议，则可创建用户定义的应用协议检测器以便系统根据端口或模式识别应用。还可以导入、激活和停用某些应用检测器，以便进一步自定义 FireSIGHT 系统的应用检测功能。

还可使用 Nmap 主动扫描器的扫描结果替换操作系统和应用数据的检测，或者使用第三方漏洞来扩充漏洞列表。系统可以协调来自多个源的数据，从而确定应用的标识。有关系统如何执行此操作的详细信息，请参阅第 46-4 页上的了解当前标识。有关主动扫描的详细信息，请参阅第 47-1 页上的配置主动扫描。

有关详细信息，请参阅以下各节：

评估检测策略

许可证：FireSIGHT

在对系统的默认检测功能进行任何更改之前，应分析哪些主机未被正确地识别以及原因，以便可以决定实施哪些解决方案。请使用以下信息作为决策指南：

受管设备是否正确布置？

许可证：FireSIGHT

如果诸如负载均衡器、代理服务器或 NAT 设备的网络设备位于受管设备和未识别或错误识别的主机之间，请将受管设备布置在更靠近错误识别的主机的位置，而不是使用自定义指纹技术。思科不建议在这种情况下使用自定义指纹技术。

未识别的操作系统是否拥有唯一的 TCP 堆栈？

许可证：FireSIGHT

如果系统错误地识别主机，应调查主机为何被错误地识别，以便帮助您做出以下决择：是创建和激活自定义指纹，还是用 Nmap 或主机输入数据替代发现数据。

注意事项　如果遇到错误识别的主机，请在创建自定义指纹之前联系支持代表。

如果主机正在运行的操作系统未被系统默认检测到而且不与已检测的现有操作系统共享识别性 TCP 堆栈特征，应创建自定义指纹。

例如，如您拥有的 Linux 自定义版本带有系统无法识别的唯一 TCP 堆栈，则创建自定义指纹将让您受益，因为，这可使系统识别并继续监控主机，而不必使用扫描结果或第三方数据，进而无需持续自行主动更新数据。

请注意，许多开源 Linux 发行版本使用相同的内核，同样，系统将使用 Linux 内核名称来识别它们。如为 Red Hat Linux 系统创建自定义指纹，可能会看到识别为 Red Hat Linux 的其他操作系统（如 Debian Linux、 Mandrake Linux、 Knoppix 等），因为相同的指纹与多个 Linux 发行版本匹配。

不应在每种情况下都使用指纹。例如，可能对主机的 TCP 堆栈做出了修改，以使其与另一操作系统类似或相同。例如， Apple Mac OS X 主机已修改，使其指纹与 Linux 2.4 主机相同，从而导致系统将其识别为 Linux 2.4 而不是 Mac OS X。如果为 Mac OS X 主机创建自定义指纹，可能导致将所有合法的 Linux 2.4 主机错误地识别为 Mac OS X 主机。在这种情况下，如果 Nmap 正确地识别主机，应为该主机安排定期的 Nmap 扫描。

如果使用主机输入从第三方系统导入数据，则必须将第三方用于描述服务器和应用协议的供应商、产品和版本字符串映射至这些产品的思科定义。有关详细信息，请参阅第 46-27 页上的管理第三方产品映射。请注意，即使将应用数据映射至 FireSIGHT 系统供应商和版本定义，导入的第三方漏洞也不用于客户端或网络应用的影响评估。

系统可以协调来自多个源的数据，以便确定操作系统或应用的当前标识。有关系统如何执行此操作的详细信息，请参阅第 46-4 页上的了解当前标识。

对于 Nmap 数据，可安排定期 Nmap 扫描。对于主机输入数据，可定期运行用于导入的 Perl 脚本或命令行实用程序。然而，请注意，主动扫描数据和主机输入数据可能不会随发现数据的频率进行更新。

FireSIGHT 系统能否识别所有应用？

许可证：FireSIGHT

如果主机已由系统正确识别，但有未识别的应用，则可创建用户定义的检测器来向系统提供端口和模式匹配信息以帮助识别应用。有关详细信息，请参阅第 46-16 页上的创建用户定义的应用协议检测器。

是否已应用可修复漏洞的修补程序？

许可证：FireSIGHT

如果系统已正确识别主机，但未反映已应用的修补，则可使用主机输入功能导入修补程序信息。导入修补程序信息时，必须将修补程序的名称映射至数据库中的修补程序。有关详细信息，请参阅第 46-29 页上的映射第三方产品修补程序。

是否想要跟踪第三方漏洞？

许可证：FireSIGHT

如果拥有想要用于影响关联的第三方系统的漏洞信息，则可将服务器和应用协议的第三方漏洞标识符映射至思科数据库中的漏洞标识符，然后使用主机输入功能导入漏洞。有关使用主机输入功能的详细信息，请参阅《*FireSIGHT 系统主机输入 API 指南*》。有关映射第三方漏洞的详细信息，请参阅第 46-30 页上的映射第三方漏洞。请注意，即使将应用数据映射至 FireSIGHT 系统供应商和版本定义，导入的第三方漏洞也不用于客户端或网络应用的影响评估。

增强网络映射

许可证：FireSIGHT

FireSIGHT 系统使用其通过被动分析流量检测的数据构建网络映射。它还使用通过主机输入功能和 Nmap 扫描器等主动源添加的数据。了解系统如何确定哪些数据用于应用或者操作系统标识有助于确定如何最佳地使用主动输入源扩充系统的被动检测功能。

有关详细信息，请参阅以下主题：

了解被动检测

许可证：FireSIGHT

*被动检测*通过分析系统被动收集的流量对主机操作系统、客户端和应用信息进行检测。系统使用 VDB 中的信息来帮助识别网络资产。

如果系统无法识别主机上的操作系统，则可对其进行手动确定，然后创建自定义服务器或客户端指纹来帮助系统识别其他主机上有着类似操作系统特征的操作系统。

系统可使用为主机操作系统收集的所有被动指纹来创建*派生指纹*。系统通过应用公式来创建派生指纹，该公式使用每个收集的指纹的置信值和标识之间的证实指纹数据的数量来计算最有可能的标识。常见元素在标识之间进行识别

如果在网络上使用用户定义的应用检测器，则可通过创建自定义检测器来扩充系统的应用检测功能，自定义检测器可向系统提供其识别这些应用所需的信息。 NetFlow 还可将被动检测的应用信息添加至网络映射。

请注意，系统不会使用分类为*未知*的应用协议和操作系统数据，因为其无法解释数据。受管设备会将该标识向防御中心报告为未知，标识数据将不用于派生指纹。

了解主动检测

许可证：FireSIGHT

*主动检测*是对网络映射的补充，是通过主动源收集的数据，如主机操作系统和应用信息。例如，可使用 Nmap 扫描器仪主动扫描网络上的目标主机。 Nmap 可发现主机上的操作系统和应用。

此外，主机输入功能可用于将*主机输入数据*主动添加至网络映射。有两种不同类别的主机输入数据：

- 可以 FireSIGHT 系统用户界面修改主机操作系统或应用标识 通过接口添加的数据为*用户输入数据*。
- 还可使用命令行实用程序导入数据。导入的数据为*主机导入输入数据*。

系统将为每个主动源保留一个标识。如果运行 Nmap 扫描实例，例如，先前的扫描结果将替代为新的扫描结果。然而，如果运行 Nmap 扫描，然后用结果通过命令行导入的客户端的数据替代这些结果，系统将同时保留来自 Nmap 结果的标识以及来自导入客户端的标识。然后，系统会使用系统策略中设置的优先级来确定哪个主动标识用作当前标识。

请注意，用户输入视为一个源，即使其来自不同的源。例如，如果用户 A 通过主机配置文件设置操作系统，然后用户 B 通过主机配置文件更改该定义，用户 B 设置的定义将保留，而用户 A 设置的定义将丢弃。此外，请注意，用户输入会覆盖所有其他的主动源，并会用作当前标识（如果其存在）。

了解当前标识

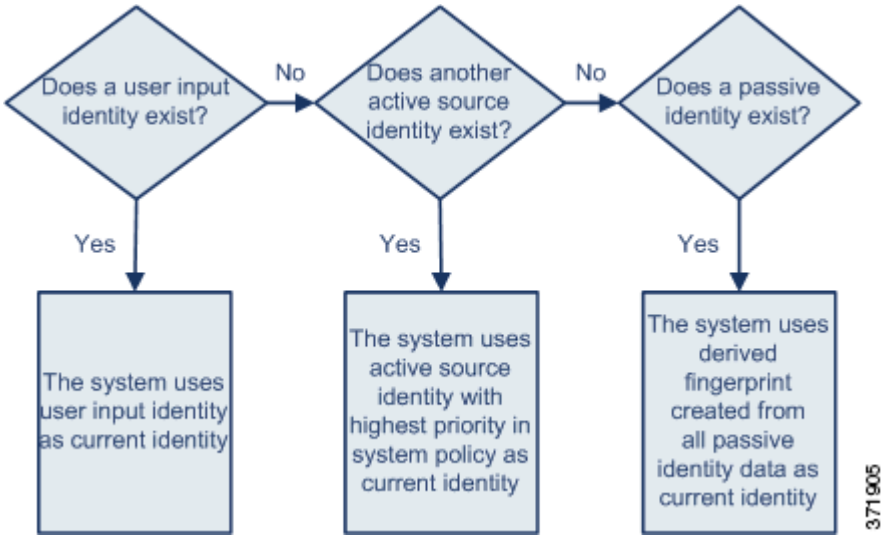
许可证：FireSIGHT

主机上的应用或操作系统的*当前标识*是系统发现最有可能正确的标识。

系统会将操作系统或应用的当前标识用于以下用途：

- 分配漏洞至主机
- 影响评估
- 评估针对操作系统标识、主机配置文件合格性以及合规性白名单写入的相关性规则
- 在工作流程的“主机和服务器”表格视图中进行显示
- 在主机配置文件中进行显示
- 在 Discovery Statistics 页面上计算操作系统和应用统计

系统会使用源优先级来确定哪个主动标识应该用作应用或操作系统的当前标识。



例如，如果用户在主机上将操作系统设置为 Windows 2003 Server，则 Windows 2003 Server 为当前标识。针对该主机上的 Windows 2003 Server 漏洞的攻击将被赋予更高的影响，而主机配置文件中为该主机列出的漏洞包括 Windows 2003 Server 漏洞。

对于主机上的操作系统或特定应用，数据库可能保留来自多个源的信息。

如果数据的源拥有最高的源优先级，系统会将操作系统或应用标识视作当前标识。可能的源拥有以下的优先级顺序：

1. 用户
2. 扫描器和应用 （在网络发现策略中设置）
3. 受管设备
4. NetFlow

请注意，如果优先级更高的新应用标识拥有的详细信息比当前标识少，则将不覆盖当前应用标识。

此外，请注意，如果出现标识冲突，冲突的解决取决于网络发现策略中的设置或者手动解决，如第 46-5 页上的了解标识冲突中所述。

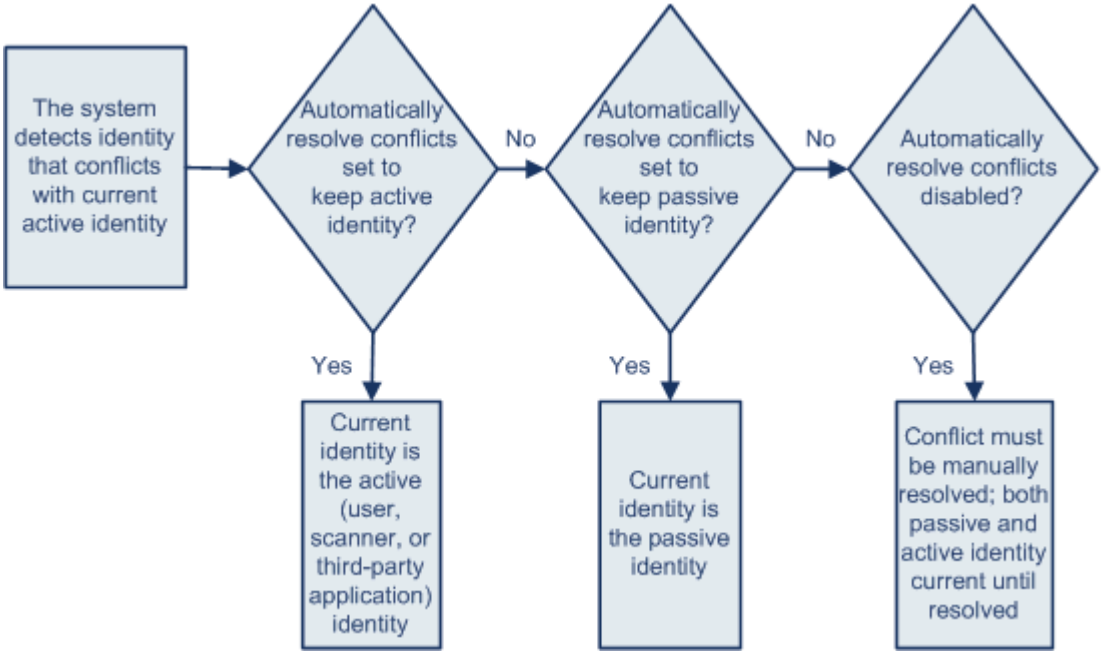
了解标识冲突

许可证：FireSIGHT

如果系统报告新的被动标识与当前主动标识和先前报告的被动标识冲突，就会发生*标识冲突*。例如，如将操作系统先前的被动标识报告为 Windows 2000，则主动标识 Windows XP 成为当前标识。接下来，系统检测到新的被动标识 Ubuntu Linux 8.04.1。标识 Windows XP 和 Ubuntu Linux 发生冲突。

如果主机的操作系统或主机上的某个应用存在标识冲突，系统会将两个冲突的标识均列为当前标识，并将二者用于影响评估，直到冲突解决。

有管理员权限的用户可自动解决标识冲突，只需选择始终使用被动标识或始终使用主动标识。除非禁用标识冲突的自动解决，否则标识冲突始终会自动解决。



有管理员权限的用户还可配置系统，从而在标识冲突发生时生成事件。然后，该用户可设置带有相关性规则的关联策略，规则将 Nmap 扫描用作相关性响应。如果事件发生， Nmap 会扫描主机以获取经过更新的主机操作系统和应用数据。

使用自定义指纹技术

许可证：FireSIGHT

FireSIGHT 系统包含有操作系统*指纹*，系统进行检测时，将其用于识别每个主机上的操作系统。然而，有时系统会因为不存在与操作系统匹配的指纹而无法识别主机操作系统，或者错误地识别主机操作系统。要纠正此问题，可创建*自定义指纹*，指纹提供未知或识别错误的操作系统所独有的操作系统特征模式，以便提供用于标识的操作系统名称。

如果系统无法匹配主机操作系统，则无法识别主机漏洞，因为系统通过其操作系统指纹为每个主机派生漏洞列表。例如，如果系统检测到运行 Microsoft Windows 的主机，则表明系统存储了 Microsoft Windows 漏洞列表，其根据检测到的 Windows 操作系统将该列表添加至该主机的主机配置文件。

例如，如果网络上有多个运行新试用版 Microsoft Windows 的设备，系统无法确定操作系统，因此无法将漏洞映射至主机。然而，知道系统拥有 Microsoft Windows 的漏洞列表，您可能想要为某个主机创建自定义的指纹，以便随后可将该指纹用来识别运行相同操作系统的其他主机。可将 Microsoft Windows 漏洞列表的映射纳入指纹中，以便将该列表与匹配指纹的每个主机关联。

创建自定义指纹时，可添加操作系统信息的自定义显示，而且可为操作系统选择其供应商、产品名称和产品版本，操作系统应将该等信息用作指纹漏洞列表的模型。防御中心将为运行相同操作系统的任何主机列出与该指纹关联的漏洞集。如果创建的自定义指纹没有任何漏洞映射，则系统将使用该指纹来分配在其中提供的自定义操作系统信息。如果系统发现的新流量源自已检测到而且目前驻留在网络映射中的主机，系统会使用新的指纹信息来更新主机。首次检测到使用该操作系统的任何新主机时，系统还会使用新的指纹来识别这些主机。

在尝试设置主机指纹前，应确定为何主机未被正确识别，从而决定自定义指纹技术是否为可行的解决方案。有关详细信息，请参阅第 46-1 页上的评估检测策略。

可使用系统创建两种类型的指纹：

- 客户端指纹，这种指纹根据 SYN 数据包识别操作系统，主机连接网络上的另一主机上运行的 TCP 应用时，会发送这种数据包。

  有关如何获取主机的客户端指纹的信息，请参阅第 46-7 页上的设置客户端指纹。

- 服务器指纹，这种指纹根据 SYN-ACK 数据包识别操作系统，主机使用这种数据包来响应通向运行的 TCP 应用的传入连接。

  有关如何获取主机的服务器指纹的信息，请参阅第 46-9 页上的指纹技术服务器。

创建指纹后，必须先将其激活，然后系统才可以将其与主机关联。有关详情，请参见第 46-11 页上的管理指纹。

注　如果客户端和服务器指纹均与相同的主机匹配，将会使用客户端指纹。

设置客户端指纹

许可证：FireSIGHT

客户端指纹根据 SYN 数据包识别操作系统，主机连接网络上的另一主机上运行的 TCP 应用时，会发送这种数据包。

如果防御中心不与受监控的主机直接联系，指定客户端指纹属性时，可以指定防御中心管理的离想要为其设置指纹的主机最近的设备。

开始指纹设置流程之前，获取想要为其设置指纹的主机的以下相关信息：

- 主机与防御中心或用于获取指纹的设备之间的网络跳数。（思科强烈建议将防御中心或设备直接连接至于主机所连接至的相同子网）。
- 连接至主机所在网络的 （防御中心或设备上的）网络接口。
- 主机的实际的操作系统供应商、产品和版本。
- 访问主机以便生成客户端流量。

要获取主机的客户端指纹，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies** > **Network Discovery**，然后点击 **Custom Operating Systems**。

系统将显示 Custom Fingerprint 页面。

步骤 2　点击 **Create Custom Fingerprint**。

系统将显示 Create Custom Fingerprint 页面。

步骤 3　从 **Device** 下拉列表，选择要用于收集指纹的防御中心或设备。

步骤 4　在 **Fingerprint Name** 字段中，键入指纹的标识名称。

步骤 5　在 **Fingerprint Description** 字段中，键入指纹描述。

步骤 6　从 **Fingerprint Type** 列表，选择 **Client**。

步骤 7　在 **Target IP Address** 字段中，键入要为其设置指纹的主机的 IP 地址。请注意，指纹仅会基于流向和来自您指定的主机 IP 地址的流量，而不是主机的任何其他 IP 地址 （如果其拥有）。

注意事项　有关在受管设备和防御中心上启用 IPv6 的信息，请参阅第 64-8 页上的配置管理接口。

步骤 8　在 **Target Distance** 字段中，输入主机和在第 3 步中选择的用于收集指纹的设备之间的网络跳数。

注意事项　此跳数必须是至主机的实际物理网络跳数，与系统检测到的跳数不一定相同。

步骤 9　从 **Interface** 列表，选择连接至主机所在网段的网络接口。

注意事项　思科建议**不要**将受管设备上的传感接口用于设置指纹，这是因为以下多个原因。首选，如果传感接口位于镜像端口之上，指纹技术将不起作用。另外，如果使用设备上的传感接口，设备在其收集指纹所花的时间内会停止监控网络。然而，可使用管理接口或任何其他可用接口来执行指纹收集。如果不知道哪个接口是设备上的传感接口，请参阅用于设置指纹的特定型号的 《*安装指南*》。

步骤 10　如果想要在设置指纹的主机的主机配置文件中显示自定义信息 （或者如果想要设置指纹的主机不在 OS Vulnerability Mappings 部分中），在 Custom OS Display 部分中选择 **Use Custom OS Display**，并对于以下项提供想要在主机配置文件中显示的值：

- 在 **Vendor String** 字段中，键入操作系统的供应商名称。例如， Microsoft Windows 的供应商为 Microsoft。
- 在 **Product String** 字段中，键入操作系统的产品名称。例如， Microsoft Windows 2000 的产品名称为 Windows。
- 在 **Version String** 字段中，键入操作系统的版本号。例如，Microsoft Windows 2000 的版本号为 2000。

步骤 11　在 OS Vulnerability Mappings 部分中，选择想要用于漏洞映射的操作系统、产品和版本。

例如，如果想要自定义指纹将 Redhat Linux 9 的漏洞列表分配至匹配主机，请选择 **Redhat, Inc.** 作为供应商、 **Redhat Linux** 作为产品以及 **9** 作为主版本。

提示　创建指纹时，可为指纹分配单个漏洞映射。指纹创建并激活后，可为操作系统的其他版本添加额外漏洞映射。有关详情，请参见第 46-14 页上的编辑活动指纹。

如果想要使用指纹来识别匹配主机的漏洞，或者如果不分配自定义的操作系统显示信息，必须在此部分指定供应商和产品名称。要为所有版本的操作系统映射漏洞，请仅指定供应商和产品名称。例如，要添加所有版本的 Palm OS，将从 **Vendor** 列表选择 **PalmSource, Inc.**，从 **Product** 列表选择 **Palm OS**，并让所有其他列表保持其默认设置。

注　并非 **Major Version**、**Minor Version**、**Revision Version**、**Build**、**Patch** 和 **Extension** 下拉列表中的所有选项均可应用至选择的操作系统。此外，如果列表中没有显示与想要设置指纹的操作系统匹配的定义，可将这些值留空。请注意，如果不在指纹中创建任何操作系统漏洞映射，则系统无法使用指纹来为指纹识别的主机分配漏洞列表。

步骤 12　点击**创建**。

系统将重新显示 Custom Fingerprint 状态页面。状态页面每隔 10 秒进行刷新，直到其收到来自所述主机的数据。

提示　如果点击 **Create**，状态会短暂显示 `New`，然后切换至 `Pending`，此状态会保持不变，直到发现匹配指纹的流量，然后状态会切换至 `Ready`。

步骤 13　将指定的 IP 地址用作目标 IP 地址，访问您尝试为其设置指纹的主机，并发起至设备的 TCP 连接。

例如，从想要为其设置指纹的主机访问防御中心的网络界面，或者从主机使用 SSH 登录至防御中心。如在使用 SSH，请使用以下的命令：

```
ssh -b localIPv6address DCmanagementIPv6address
```

其中，*`localIPv6address`* 是在第 7 步中指定的目前已分配至主机的 IPv6 地址，*`DCmanagementIPv6address`* 是防御中心的管理 IPv6 地址。

然后，Custom Fingerprint 页面重新加载，其状态为“就绪”。

注　要创建准确的指纹，收集指纹的设备**必须**发现流量。如果通过交换机进行连接，系统可能不会发现流向系统而不是设备的流量。

步骤 14　指纹创建后，必须先将其激活，然后防御中心才可以使用其来识别主机。有关详情，请参见第 46-11 页上的管理指纹。

指纹技术服务器

许可证：FireSIGHT

服务器指纹根据 SYN-ACK 数据包识别操作系统，主机使用这种数据包来响应通向运行的 TCP 应用的传入连接。在开始之前，应获取关于想要为其设置指纹的主机的以下信息：

- 主机与用于获取指纹的设备之间的网络跳数。思科强烈建议将设备上不使用的接口直接连接至主机所连接至的相同子网。
- 连接至主机所在网络的 （设备上的）网络接口。
- 主机的实际的操作系统供应商、产品和版本。
- 未在使用的 IP 地址，并在主机所在网络上得到授权。

提示　如果防御中心不与受监控的主机直接联系，指定服务器指纹属性时，可以指定离想要为其设置指纹的主机最近的受管设备。

要获取主机的服务器指纹，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies** > **Network Discovery**，然后点击 **Custom Operating Systems**。

系统将显示 Custom Fingerprint 页面。

步骤 2　点击 **Create Custom Fingerprint**。

系统将显示 Create Custom Fingerprint 页面。

步骤 3　从 **Device** 列表，选择想要用于收集指纹的防御中心或受管设备。

步骤 4　在 **Fingerprint Name** 字段中，键入指纹的标识名称。

步骤 5　在 **Fingerprint Description** 字段中，键入指纹描述。

步骤 6　从 **Fingerprint Type** 列表，选择 **Server**。

系统将显示服务器指纹技术选项。

步骤 7　在 **Target IP Address** 字段中，键入要为其设置指纹的主机的 IP 地址。请注意，指纹仅会基于流向和来自您指定的主机 IP 地址的流量，而不是主机的任何其他 IP 地址 （如果其拥有）。

注意事项　仅对于运行 FireSIGHT 系统 5.2 和更高版本的设备，可以捕获 IPv6 指纹。

步骤 8　在 **Target Distance** 字段中，输入主机和在第 3 步中选择的用于收集指纹的设备之间的网络跳数。

注意事项　此跳数必须是至主机的实际物理网络跳数，与系统检测到的跳数不一定相同。

步骤 9　从 **Interface** 列表，选择连接至主机所在网段的网络接口。

注意事项　思科建议**不要**将受管设备上的传感接口用于设置指纹，这是因为以下多个原因。首选，如果传感接口位于镜像端口之上，指纹技术将不起作用。另外，如果使用设备上的传感接口，设备在其收集指纹所花的时间内会停止监控网络。然而，可使用管理接口或任何其他可用接口来执行指纹收集。如果不知道哪个接口是设备上的传感接口，请参阅用于设置指纹的特定型号的 《*安装指南*》。

步骤 10　点击 **Get Active Ports**。

如果系统检测到了主机上的任何开放端口，它们会在下拉列表中显示。

步骤 11　在 **Server Port** 字段中，键入想要设备选择用于收集指纹以便向其发起联系的端口，或者从 **Get Active Ports** 下拉列表选择端口。

可使用主机上已知开放的任何服务器端口 （例如， 80，如果主机正在运行网络服务器）。

步骤 12　在 **Source IP Address** 字段中，键入应用于尝试与主机通信的 IP 地址。

应使用经授权可在网络上使用，但目前未在使用的源 IP 地址，例如，当前未在使用的 DHCP 池地址。创建指纹时，这可防止临时访问另一离线主机。

此外，创建指纹时，应从网络发现策略的监控中排除该 IP 地址。否则，网络映射和发现事件视图中将会出现大量关于该 IP 地址代表的主机的不准确信息。有关详细信息，请参阅第 45-1 页上的了解发现数据收集。

步骤 13　在 **Source Subnet Mask** 字段中，键入正在使用的 IP 地址的子网掩码。

步骤 14　如果 **Source Gateway** 字段显示，输入应用于建立至主机的路由的默认网关 IP 地址。

如果目标距离 （跳数）为 1 或更大，而且正在使用非管理接口连接至主机所在的网络，系统将显示 **Source Gateway** 字段。

步骤 15　如果想要在设置指纹的主机的主机配置文件中显示自定义信息，或者如果想要使用的指纹名称在 OS Definition 部分中不存在，可以在 Custom OS Display 部分中选择 **Use Custom OS Display**。

对于以下项提供想要在主机配置文件中显示的值：

- 在 **Vendor String** 字段中，键入操作系统的供应商名称。例如， Microsoft Windows 的供应商为 Microsoft。
- 在 **Product String** 字段中，键入操作系统的产品名称。例如， Microsoft Windows 2000 的产品名称为 Windows。
- 在 **Version String** 字段中，键入操作系统的版本号。例如，Microsoft Windows 2000 的版本号为 2000。

步骤 16　在 OS Vulnerability Mappings 部分中，选择想要用于漏洞映射的操作系统、产品和版本。例如，如果想要自定义指纹将 Redhat Linux 9 的漏洞列表分配至匹配主机，选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

提示　创建指纹时，可为指纹分配单个漏洞映射。指纹创建并激活后，可为操作系统的其他版本添加额外漏洞映射。有关详情，请参见第 46-14 页上的编辑活动指纹。

如果想要使用指纹来识别匹配主机的漏洞，或者如果不分配自定义的操作系统显示信息，必须在此部分指定供应商和产品名称。要为所有版本的操作系统映射漏洞，请仅指定供应商和产品名称。例如，要添加所有版本的 Palm OS，将从 **Vendor** 列表选择 **PalmSource, Inc.**，从 **Product** 列表选择 **Palm OS**，并让所有其他列表保持其默认设置。

注　并非 **Major Version**、**Minor Version**、**Revision Version**、**Build**、**Patch** 和 **Extension** 下拉列表中的所有选项均可应用至选择的操作系统。此外，如果列表中没有显示与想要设置指纹的操作系统匹配的定义，可将这些值留空。请注意，如果不在指纹中创建任何操作系统漏洞映射，则系统无法使用指纹来为指纹识别的主机分配漏洞列表。

步骤 17　点击**创建**。

步骤 18　系统将显示 Custom Fingerprint 状态页面。该页面应每隔 10 秒以“就绪”状态重新加载。

注　如果目标系统在设置指纹的过程中停止响应，状态将会显示 `ERROR: No Response` 消息。如果看到此消息，请再次提交指纹。等待 3 至 5 分钟（时长可能因目标系统而异），点击编辑图标 ( ) 访问 Custom Fingerprint 页面，然后点击 **Create**。

步骤 19　指纹创建后，将其激活，或者，添加漏洞映射。有关详情，请参见第 46-11 页上的管理指纹。

管理指纹

许可证：FireSIGHT

可以激活、停用、删除、查看和编辑自定义指纹。创建指纹时，可为指纹分配单个漏洞映射。有关创建指纹的详细信息，请参阅第 46-7 页上的设置客户端指纹和第 46-9 页上的指纹技术服务器。指纹创建和激活后，可编辑指纹以便做出更改或添加漏洞映射。

要访问 Custom Fingerprints 页面，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies** > **Network Discovery**，然后点击 **Custom Operating Systems**。

系统将显示 Custom Fingerprint 页面。

如果系统正在等待数据以便创建指纹，将会每 10 秒自动刷新页面，直到指纹已创建。

有关详细信息，请参阅以下各节：

激活指纹

许可证：FireSIGHT

创建自定义指纹后，必须先将其激活，然后系统才可将其用于识别主机。新指纹激活后，系统会将其用于重新识别先前发现的主机并发现新的主机。

要激活指纹，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies** > **Network Discovery**，然后点击 **Custom Operating Systems**。

系统将显示 Custom Fingerprint 页面。

步骤 2　点击想要激活的指纹旁的滑块。

注　激活选项仅当创建的指纹有效时才可用。如果滑块不可用，请尝试再次创建指纹。

防御中心将激活指纹，并将其传播至所有受管设备。指纹名称旁的图标将会变化，以表示指纹处于活动状态。

停用指纹

许可证：FireSIGHT

如果想要停止使用指纹，可将其停用。停用指纹后，其就不再可用，但仍保留其在系统上。停用指纹后，对于使用该指纹的主机，操作系统被标记为未知。如果再次检测到这些主机，并且这些主机与不同的活动指纹匹配，则该活动指纹将对其进行识别。

删除指纹会将其从系统中完全删除。停用指纹后，即可将其删除。

要停用活动指纹，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies** > **Network Discovery**，然后点击 **Custom Operating Systems**。

系统将显示 Custom Fingerprint 页面。

步骤 2　点击想要停用的活动指纹旁的滑块。

防御中心将停用指纹，并将停用传播至所有受管设备。

删除指纹

许可证：FireSIGHT

如果不再使用指纹，可将其从系统中删除。请注意，必须先停用指纹，然后才可将其删除。

要删除指纹，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies** > **Network Discovery**，然后点击 **Custom Operating Systems**。

系统将显示 Custom Fingerprint 页面。

步骤 2　如果想要删除的指纹处于活动状态，请点击每个指纹旁的滑块图标以便将其停用。

步骤 3　点击想要删除的指纹旁的删除图标 ( )。

步骤 4　点击 **OK**，以便确认想要删除指纹。

指纹删除成功。

编辑指纹

许可证：FireSIGHT

创建指纹后，即可查看或编辑它。这样，您就可更改并重新提交指纹，或向其添加额外的漏洞映射。无论指纹是处于活动状态还是非活动状态，均可对其进行修改，但取决于指纹的状态，可修改的内容有所不同。

如果指纹处于*非活动*状态，可修改指纹的所有元素，并将其重新提交至防御中心。这包括创建指纹时指定的所有属性，如指纹类型、目标 IP 地址与端口、漏洞映射等。编辑非活动指纹并将其提交时，会将它重新提交至系统，如果指纹是客户端指纹，必须先将流量重新发送至设备，然后才可以将其激活。请注意，对于非活动指纹，仅可选择单一漏洞映射。激活指纹后，可将额外的操作系统和版本映射至其漏洞列表。

如果指纹处于*活动*状态，可修改指纹名称、描述、自定义操作系统显示，并向其映射额外的漏洞。

有关详细信息，请参阅以下各节：

- 第 46-13 页上的编辑非活动指纹
- 第 46-14 页上的编辑活动指纹

编辑非活动指纹

许可证：FireSIGHT

如果指纹处于非活动状态，可修改其属性，并将其重新提交至系统。这包括对需要使用的指纹类型、指纹目标系统等进行更改。

要编辑非活动指纹，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies** > **Network Discovery**，然后点击 **Custom Operating Systems**。

系统将显示 Custom Fingerprint 页面。

步骤 2　点击想要编辑的指纹旁的编辑图标 ( )。

系统将显示 Edit Custom Fingerprint 页面。

步骤 3　请在必要时更改指纹：

- 如在修改客户端指纹，请参阅第 46-7 页上的设置客户端指纹，了解有关可配置选项的详细信息。
- 如在修改服务器指纹，请参阅第 46-9 页上的指纹技术服务器，了解有关可配置选项的详细详细信息。

步骤 4　点击 **Save**，以重新提交指纹。

注　如已修改客户端指纹，切记将流量从主机发送至收集指纹的设备。

编辑活动指纹

许可证：FireSIGHT

指纹处于活动状态时，可更改其名称、描述和显示标记。此外，可管理漏洞映射，包括添加和删除漏洞映射。

要编辑活动指纹，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies** > **Network Discovery**，然后点击 **Custom Operating Systems**。

系统将显示 Custom Fingerprint 页面。

步骤 2　点击想要编辑的指纹旁的编辑图标 ( )。

系统将显示 Edit Custom Fingerprint Product Mappings 页面。

步骤 3　必要时修改指纹名称、描述和自定义操作系统显示。

步骤 4　如果想要删除漏洞映射，请点击页面的 Pre-Defined OS Product Maps 部分中映射旁的 **Delete**。

步骤 5　如果想要为漏洞映射添加额外的操作系统，请选择 **Product**， **Major Version**、 **Minor Version**、 **Revision Version**、 **Build**、 **Patch** 和 **Extension** （如适用），然后点击 **Add OS Definition**。

漏洞映射会已添加至 Pre-Defined OS Product Maps 列表。

步骤 6　点击 **Save**，以保存更改。

使用应用检测器

许可证：FireSIGHT

FireSIGHT 系统分析 IP 流量时，将使用检测器来识别网络上常用的应用。使用 Detectors 页面 (**Policies > Application Detectors**) 可以自定义 FireSIGHT 系统的检测功能。

该页面提供每个检测器的相关信息，包括：

- 检测器的名称
- 检测器检查的流量的协议 （TCP、 UDP 或二者）

- 检测器的类型是应用协议、客户端、网络应用还是内部检测器
- 对于基于端口的应用检测器，应用流量使用的端口
- 检测到的应用的相关详细信息，包括与检测器检测到的应用关联的名称、描述、任务、业务相关性、标记和类别
- 检测器的状态 （活动或非活动）

系统仅使用活动检测器来分析应用流量。

您可能会注意到，列出的检测器拥有不同的属性。例如，可查看部分检测器的设置，但是不能查看其他检测器的设置。类似地，可删除部分检测器，但是不能删除其他检测器。这是因为，思科提供有多种不同类型的检测器，如以下各节所述。

思科提供的内部检测器

*内部检测器*是仅随 FireSIGHT 系统更新提供的应用检测器。取决于检测器，内部检测器可以检测客户端、网络应用或应用协议流量，但它们被分类为内部检测器，而不是其他类型中的一种，因为它们是内置检测器，而且无法停用。

内部检测器始终处于开启状态；无法对其进行停用、删除或配置。内部检测器的示例包括：内置 Amazon 检测器和内置 AppleTalk 检测器。

思科提供的客户端检测器

思科提供的*客户端检测器*可检测客户端流量，通过 VDB 更新提供，也随 FireSIGHT 系统的更新提供。思科 Professional Services 也能以可导入检测器的形式提供这些检测器。

可根据贵组织的需求激活和停用客户端检测器。 VDB 更新也可激活或停用客户端检测器。仅当导入客户端检测器后，才可以将其导出。

客户端检测器的示例包括：Google Earth 和 Immunet 检测器。

思科提供的网络应用检测器

思科提供的*网络应用检测器*可检测 HTTP 流量负载中的网络应用，通过 VDB 更新提供，也随 FireSIGHT 系统更新提供。

可根据贵组织的需求激活和停用网络应用检测器。 VDB 更新可以激活或停用网络应用检测器。网络应用检测器的示例包括：Blackboard 和 LiveJournal 检测器。

思科提供的应用协议 （端口）检测器

*基于端口的应用协议检测器*由思科提供，基于对已知端口的网络流量检测。这些检测器通过 VDB 更新提供，也随 FireSIGHT 系统的更新提供，或由思科 Professional Services 以可导入检测器的形式提供。

可根据贵组织的需求激活和停用应用协议检测器。还可查看检测器定义，以便将其用作自定义检测器的基础。 VDB 更新可激活或停用应用协议检测器。

端口检测器的示例包括：chargen 和 finger 检测器。

思科提供的应用协议 (FireSIGHT) 检测器

FireSIGHT 的基于应用协议的检测器，由思科提供，使用 FireSIGHT 应用指纹，基于对网络流量的检测。这些检测器通过 VDB 更新提供，也随 FireSIGHT 系统的更新提供。

可根据贵组织的需求激活和停用应用协议检测器。 VDB 更新可以激活或停用思科提供的应用协议检测器。 FireSIGHT 的基于应用协议的检测器的示例包括：Jabber 和 Steam 检测器。

应用协议 （模式）检测器

*基于模式的应用检测器*基于对网络流量数据包中的模式的检测。这些检测器可以由思科 Professional Services 以可导入检测器的形式提供，也可自行创建。这样，就可通过新的基于模式的检测器增强系统的检测功能，而无需对 FireSIGHT 系统进行整体更新。

可根据贵组织的需求激活和停用应用协议检测器。

可完全控制导入和用户定义的检测器，可将其激活、停用、编辑、导入、导出和删除。基于模式的检测器的示例包括用户定义的检测器，该检测器使用数据包包头中的模式来检测自定义应用的流量。

切记，检测器列表可能会发生变化，具体取决于已安装的 FireSIGHT 系统和 VDB 的版本以及可能已导入或创建的任何个别检测器。应仔细阅读每个 FireSIGHT 系统更新的版本说明以及每次 VDB 更新的公告以便获得有关已更新检测器的信息。

有关详情，请参阅：

- 第 45-9 页上的了解应用检测
- 第 46-16 页上的创建用户定义的应用协议检测器
- 第 46-21 页上的管理检测器

创建用户定义的应用协议检测器

许可证：FireSIGHT

如果在网络上使用自定义应用，可以创建用户定义的应用协议检测器，这些检测器向系统提供识别这些应用所需的信息。可基于应用流量使用的端口、流量内的模式或者端口和模式二者进行应用协议检测。

例如，如果预期自定义应用协议的流量使用端口 1180，则可创建检测该端口上流量的应用协议检测器。另一个示例是，如果知道包含应用协议流量的任何数据包的包头中拥有字符串 `ApplicationName`，则可创建将 ASCII 字符串 `ApplicationName` 注册为需要匹配的模式的检测器。

只能为应用程序协议创建用户定义的应用检测器，**不能**为客户端或网络应用创建。有关其各自的说明，请参阅第 45-9 页上的了解应用检测。只有客户端会话包含来自服务器的响应器数据包，系统才能开始检测和识别服务器流量中的应用协议。请注意，对于 UDP 流量，系统将响应器数据包的来源指定为服务器。

注意事项 创建并激活新的应用检测器后，受管设备上的流量和处理可能暂停，这可能会导致一些数据包未经检查地通过。

用户定义的应用协议检测器必须使用端口或模式匹配；不能创建二者均不使用的检测器，即使基于现有检测器创建检测器。还可创建同时使用二个条件的检测器，这可提高正确识别该应用协议流量的可能性。

提示 如果已经在另一防御中心上创建了检测器，可将其导出后，再导入至此防御中心。然后，可根据自己的需求编辑已导入的检测器。可导入和导出用户定义的检测器以及思科 Professional Services 提供的检测器。然而，**不能**导出或导入思科提供的任何其他类型检测器。有关详细信息，请参阅第 A-1 页上的导入和导出配置。

要创建用户定义的应用协议检测器：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Application Detectors**。

系统将显示 Detectors 页面。

步骤 2　点击 **Create Detector**。

系统将显示 Create Detector 页面。

步骤 3　提供基本的检测器信息，如检测器名称和描述。

请参阅第 46-17 页上的提供基本的应用协议检测器信息。

步骤 4　或者，可以为检测器创建用户定义的应用。

请参阅第 46-18 页上的创建用户定义的应用。

步骤 5　提供检测条件，包括检测器应检查的流量的协议以及流量使用的端口。

请参阅第 46-19 页上的为应用协议检测器指定检测条件。

步骤 6　或者，配置检测器配置，使其在流量中检查该应用协议流量中出现的一个或多个模式的匹配项。

请参阅第 46-19 页上的向应用协议检测器添加检测模式。

步骤 7　或者，针对一个或多个 PCAP 文件的内容测试新检测器。

请参阅第 46-20 页上的针对数据包捕获测试应用协议检测器。

步骤 8　点击 **Save**。

系统将保存应用协议检测器。

注　必须先激活检测器，然后系统才能将其用于分析应用协议流量。有关详细信息，请参阅第 46-24 页上的激活和停用检测器。请注意，如将应用纳入访问控制规则中，则检测器将自动激活，而且在使用时不能停用。

提供基本的应用协议检测器信息

许可证：FireSIGHT

必须为每个用户定义的应用协议检测器提供名称，并确定想要检测的应用协议。或者，可提供检测器的简短描述。

除了您提供的信息，防御中心还指示检测器是处于活动状态还是非活动状态，以及检测器是端口检测器还是模式检测器。如果检测器通过端口和模式识别应用协议流量， FireSIGHT 系统会将其视为模式检测器。

如在编辑现有检测器，防御中心也会显示检测器的作者。如已创建用户定义的应用协议检测器，则您是作者。您也是自己导入或编辑与保存的任何检测器的作者。

要提供基本的应用协议检测器信息，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Detector 页面上的 **Please enter a name** 字段中，键入检测器名称。

在将检查的流量的协议内，检测器名称必须是唯一的。也就是说，可创建名称相同的 TCP 检测器和 UDP 检测器，但不能创建名称相同的两个 TCP 检测器。

步骤 2　识别想要检测的应用协议。您有以下选项：

- 如在为现有应用协议创建检测器（例如，如果想要检测非标准端口上的特定应用协议），请从 **Application Protocol** 下拉列表选择应用协议。继续执行第 46-19 页上的为应用协议检测器指定检测条件中的操作步骤。
- 如在为自定义应用创建检测器，请继续执行下一节创建用户定义的应用中的操作步骤。

创建用户定义的应用

许可证：FireSIGHT

可创建用户定义的应用以识别网络上的自定义应用。还可创建自定义的类别和自定义的标记来描述应用。此处创建的应用、类别和标记在访问控制规则以及在应用过滤对象管理器中均可用。

有关应用检测的详细信息，包括就用于对其进行描述的应用协议与类别、标记、风险级别以及业务相关性进行的讨论，请参阅第 45-9 页上的了解应用检测。

要创建用户定义的应用，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Detector 页面上，点击 **Add**。

系统将显示 Application Editor 弹出窗口。

步骤 2　为自定义应用键入 **Name**。

步骤 3　为自定义应用键入 **Description**。

步骤 4　选择 **Business Relevance**。

步骤 5　选择 **Risk**。

步骤 6　点击 Categories 旁的 **Add** 以添加类别，并键入新的类别名称，或者从 **Categories** 下拉列表选择现有类别。

步骤 7　或者，点击 Tags 旁的 **Add**，以添加标记，并键入新的标记名称，或者从 **Tags** 下拉列表选择现有标记。

点击 **OK**，以返回 Create Detector 页面。

步骤 8　继续执行下一节为应用协议检测器指定检测条件中的操作步骤。

为应用协议检测器指定检测条件

许可证：FireSIGHT

如果创建用户定义的应用协议检测器，必须指定检测器应检查的流量的协议（TCP、UDP 或二者）。或者，可指定流量使用的端口。

请注意，如未指定端口，则必须配置检测器，使其在流量中检查一个或多个模式的匹配项，如第 46-19 页上的向应用协议检测器添加检测模式中所述。

要指定应用协议检测器的检测条件，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Detector 页面上，从 **Protocol** 下拉列表，选择检测器应检查的流量的协议。

检测器可检查 TCP、UDP、或 TCP 和 UDP 流量。

步骤 2　或者，要根据其使用的端口识别应用协议流量，在 **Port(s)** 字段中键入从 1 至 65535 的端口。要使用多个端口，请用逗号分隔它们。

步骤 3　您有以下选项：

- 如果想要配置应用协议检测器，使其在流量中检查该应用协议流量中出现的一个或多个模式的匹配项，请继续执行下一节向应用协议检测器添加检测模式中的操作步骤。
- 如果想要针对一个或多个 PCAP 文件的内容测试新的检测器，跳至第 46-20 页上的针对数据包捕获测试应用协议检测器。
- 创建检测器完毕，点击 **Save**。

  系统将保存应用协议检测器。

请注意，必须先激活检测器，然后系统才能将其用于分析应用协议流量。有关详细信息，请参阅第 46-24 页上的激活和停用检测器。

向应用协议检测器添加检测模式

许可证：FireSIGHT

如果知道包含应用协议流量的任何数据包的包头包含特定模式的字符串，则可配置用户定义的应用协议检测器来搜索该模式。

应用协议检测器可使用任何偏移搜索 ASCII 或十六进制模式。也可配置检测器，使其搜索多个模式，在这种情况下，应用协议流量必须匹配所有模式，以便检测器主动识别应用协议。

请注意，如未指定模式，必须配置检测器，使其检查使用一个或多个端口的流量，如第 46-19 页上的为应用协议检测器指定检测条件中所述。

要向应用协议检测器添加检测模式，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Detector 页面上的 Detection Patterns 部分中，点击 **Add**。

系统将显示 Add Pattern 弹出窗口。

步骤 2　指定想要检测的模式类型：**Ascii** 或 **Hex**。

步骤 3　在 **Pattern String** 字段中，键入指定的类型的字符串。

步骤 4　或者，指定系统应在数据包中开始搜索模式的位置，该位置称为偏移。

在 **Offset** 字段中，键入偏移 （从数据包负载起始位置计算，以字节为单位）。

因为数据包负载从 0 字节开始，请按以下方法计算偏移：将想要从数据包负载起始位置前移的字节数减去 1。例如，要查找数据包的第 5 个位中的模式，在 `Offset` 字段中键入 **4**。

步骤 5　或者，请重复步骤 1 至步骤 4，添加其他模式。

提示　要删除模式，点击想要删除的模式旁的删除图标 ( )。

步骤 6　您有以下选项：

- 如果想要针对一个或多个 PCAP 文件的内容测试新检测器，继续执行下一节针对数据包捕获测试应用协议检测器中的步骤。
- 创建检测器完毕，点击 **Save**。

  系统将保存应用协议检测器。

注　必须先激活检测器，然后系统才能将其用于分析应用协议流量。有关详细信息，请参阅第 46-24 页上的激活和停用检测器。

针对数据包捕获测试应用协议检测器

许可证：FireSIGHT

如您拥有的数据包捕获 (PCAP) 文件包含的数据包带有要检测的应用协议的流量，则可针对该 PCAP 文件测试用户定义的应用协议检测器。请注意，PCAP 文件必须为 32KB 或更小，如果尝试针对较大的 PCAP 文件测试检测器，防御中心会自动将其截断。

要针对 PCAP 文件测试应用协议检测器，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Detector 页面上的 Packet Captures 部分中，点击 **Add**。

系统将显示一个弹出窗口。

步骤 2　浏览至 PCAP 文件，并点击 **OK**。

PCAP 文件在 Packet Captures 文件列表中显示。

步骤 3　要针对 PCAP 文件的内容测试检测器，点击 PCAP 文件旁的评估图标。

系统显示消息，指示测试是否成功。

步骤 4　或者，重复第 1至 3 步，针对额外的 PCAP 文件测试检测器。

提示　要删除 PCAP 文件，点击想要删除的文件旁的删除图标 ( )。

步骤 5　要保存检测器，点击 **Save**。

注　必须先激活检测器，然后系统才能将其用于分析应用协议流量。有关详细信息，请参阅第 46-24 页上的激活和停用检测器。

管理检测器

许可证：FireSIGHT

可查看和管理 Detectors 页面上的检测器。

从 Detectors 页面，您可以：

- 查看检测器识别的应用的相关详细信息
- 对检测器列表进行排序、过滤和浏览
- 查看思科提供的内部检测器的列表
- 查看思科提供的应用协议端口检测器的属性，或者，将副本另存为可修改的、新的、用户定义的新检测器
- 创建、修改、删除和导出用户定义的应用协议检测器
- 删除和导出个别导入的任何应用协议检测器
- 激活和停用用户定义的、导入的或思科提供的网络应用、客户端和应用协议检测器

请注意，无法修改或删除内部或思科提供的应用协议、客户端或网络应用检测器，而且无法停用内部检测器。

有关详情，请参阅：

- 第 46-22 页上的查看检测器详细信息
- 第 46-22 页上的对检测器列表进行排序
- 第 46-22 页上的过滤检测器列表
- 第 46-24 页上的导航至其他检测器页面
- 第 46-24 页上的激活和停用检测器
- 第 46-25 页上的修改应用检测器
- 第 46-26 页上的删除检测器

查看检测器详细信息

许可证：FireSIGHT

可查看关于应用检测器列表中的检测器的更多详细信息。

要查看应用检测器详细信息，请执行以下操作：

访问：管理员/发现管理员

步骤 1　点击 Details 列中的信息图标 ( )。

系统将显示检测器的信息弹出窗口。

有关风险、业务相关性、标记和类别的详细信息，请参阅第 45-9 页上的了解应用检测。

对检测器列表进行排序

许可证：FireSIGHT

默认情况下， Detectors 页面将按名称以字母顺序列出检测器。列标题旁的向上 (▲) 或向下箭头指示页面按该列以此方向排序。

要对检测器进行排序，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Detectors 页面上，点击适当的列标题。

检测器会以列标题上显示的箭头所指示的方向排序。要按相反方向排序，请再次点击标题。

过滤检测器列表

许可证：FireSIGHT

可通过一个条件或多个条件组合过滤 Detectors 页面上显示的检测器。构建的过滤器将显示在页面顶部。可单独或组合使用多个过滤器组，以过滤检测器列表。

字段名称

查找名称或描述包含您键入的字符串的检测器。字符串可能包含任何字母数字或特殊字符。

自定义过滤器

查找与对象管理页面上创建的自定义应用过滤器匹配的检测器。有关详细信息，请参阅第 3-13 页上的使用应用过滤器。

作者

按检测器的创建者查找检测器。可按以下内容过滤检测器：

- 创建或导入检测器的任何个别用户
- **思科**，代表所有思科提供的检测器，个别导入的附加检测器*除外*；您是自己导入的任何检测器的作者
- **Any User**，代表非思科提供的所有检测器

州

根据检测器的状态（即 **Active** 或 **nactive**）查找检测器。有关详细信息，请参阅第 46-24 页上的激活和停用检测器。

类型

根据检测器的类型查找检测器：**Application Protocol**、 **Web Application**、 **Client** 或 **Internal Detector**。

应用协议检测器有三种子类型可用于进一步过滤检测器：

- **Port** 应用协议检测器包含思科提供的已知端口检测器，以及任何基于端口的用户定义的应用检测器。
- **Pattern** 应用协议检测器包含基于模式或者基于端口与模式的用户定义的应用检测器。
- **FireSIGHT** 应用协议检测器是思科提供的应用协议指纹检测器，可以激活和停用。

有关检测器类型的详细信息，请参阅第 46-14 页上的使用应用检测器。

协议

根据检测器检查的流量协议查找检测器。检测器可检查 TCP、 UDP、或 TCP 和 UDP 流量。

类别

根据分配至所检测应用的类别查找检测器。

标记

根据分配至所检测应用的标记查找检测器。

风险

根据分配至所检测应用的风险查找检测器：**Very High**、 **High**、 **Medium**、 **Low** 和 **Very Low**。

业务相关性

根据分配至所检测应用的业务相关性查找检测器：**Very High**、 **High**、 **Medium**、 **Low** 和 **Very Low**。

要应用过滤器，请执行以下操作：

管理员/发现管理员

步骤 1　在 Detectors 页面上，展开想要用于过滤检测器的过滤器组。

步骤 2　选择想要使用的特定过滤器或键入其名称。要选择组中的所有过滤器，右键单击组名称，然后选择 **Check All**。

步骤 3　或者，如果正在使用的过滤器拥有子过滤器，选择子过滤器以进一步过滤检测器。

要移除过滤器，请执行以下操作：

访问：管理员/发现管理员

步骤 1　点击移除图标（ ✖ ）（位于 **Filters** 字段的过滤器名称中）或禁用过滤器列表中的过滤器。要移除组中的所有过滤器，右键单击组名称，然后选择 **Uncheck All**。

系统移除过滤器并更新结果。

要移除所有过滤器，请执行以下操作：

访问：管理员/发现管理员

步骤 1　点击已应用至检测器的过滤器列表旁的 **Clear all**。

导航至其他检测器页面

许可证：FireSIGHT

Detectors 页面一次显示 25 个检测器。下表解释了如何使用页面底部的导航链接查看其他的检测器页面。

访问：管理员/发现管理员

表 46-1　　导航检测器页面

要.....	您可以.....
查看下一页	点击右箭头图标 ( )。
查看上一页	点击左箭头图标 ( )。
查看其他页面	键入页码并按 Enter 键。
跳至最后一页	点击右端箭头图标 ( )。
跳至第一页	点击左端箭头图标 ( )。

激活和停用检测器

许可证：FireSIGHT

必须激活检测器，然后才能将其用于分析网络流量。默认情况下，思科提供的所有检测器均已激活。

可为每个端口激活多个应用检测器，以补充系统的检测能力。

在策略的访问控制规则中包含应用并应用策略时，如果该应用没有活动检测器，一个或多个检测器将会自动激活。类似地，在已应用策略中使用应用时，如果停用检测器会使该应用没有活动检测器，则不能停用检测器。

注意事项　激活或停用现有检测器后，受管设备上的流量和处理可能暂停，这可能会导致一些数据包未经检查地通过。

提示　为提高性能，请停用任何您不感兴趣的应用协议、客户端或网络应用检测器。

要激活或停用检测器，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Application Detectors**。

系统将显示 Detectors 页面。

步骤 2　找到想要激活或停用的检测器。

如果想要激活或停用的检测器不在第一页，对检测器列表进行翻页或应用一个或多个过滤器即可找到它。有关详细信息，请参阅第 46-21 页上的管理检测器。

步骤 3　您有以下选项：

- 要**激活**检测器，以使系统在分析网络流量时使用该检测器，请点击检测器旁的已停用滑块（  ）。
- 要**停用**检测器，以使系统在分析网络流量时不使用该检测器，请点击检测器旁的已激活滑块（  ）。

请注意，其他检测器可能需要部分应用检测器。如果停用其中一个这些检测器，系统将显示警告来指示依赖该检测器的检测器也被禁用。

修改应用检测器

许可证：FireSIGHT

使用以下步骤修改用户定义的应用检测器。

要修改应用检测器，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Applications**。

系统将显示 Detectors 页面。

步骤 2　找到想要修改的检测器。

如果想要修改的检测器不在第一页，对检测器列表进行翻页或应用一个或多个过滤器即可找到它。有关详细信息，请参阅第 46-21 页上的管理检测器。

步骤 3　要修改用户定义的检测器，请点击想要修改的检测器旁的 **Edit**。

系统将显示 Edit Application Detector 页面。

步骤 4　更改检测器。

有关可更改的各种配置的信息，请参阅第 46-16 页上的创建用户定义的应用协议检测器。

步骤 5　您有以下选项：

- 如果正在修改非活动的用户定义检测器，可点击 **Save** 以保存更改，也可点击 **Save as New** 以将检测器另存为新的、非活动的、用户定义检测器。
- 如果正在修改活动的用户定义检测器，可点击 **Save and Reactivate** 以保存更改并立即开始使用经过修改的检测器，也可点击 **Save as New** 以将检测器另存为新的、非活动的、用户定义检测器。

注　系统仅使用带有活动检测器的应用来分析应用流量。有关详细信息，请参阅第 46-24 页上的激活和停用检测器。

删除检测器

许可证：FireSIGHT

使用以下步骤来删除检测器。可删除用户定义的检测器以及个别导入的思科 Professional Services 提供的附加检测器。不能删除思科提供的任何其他检测器，尽管可以停用许多此类检测器。

注　如在已应用策略中使用检测器，则不能停用或删除该检测器。

要删除检测器，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Application Detectors**。

系统将显示 Detectors 页面。

步骤 2　选择想要删除的检测器旁的复选框，然后点击 **Delete**。

如果想要删除的检测器不在第一页，对检测器列表进行翻页或应用一个或多个过滤器即可找到它。有关详细信息，请参阅第 46-21 页上的管理检测器。

步骤 3　点击 **OK** 确认想要删除检测器。

系统删除检测器。

导入主机输入数据

许可证：FireSIGHT

如果贵组织能够编写脚本或创建命令行导入文件来导入来自第三方的网络映射数据，则可导入数据以扩充网络映射中的信息。还可使用主机输入功能，只需使用网络界面修改操作系统或应用标识，或删除应用协议、协议、主机属性或客户端。

系统可协调来自多个源的数据，以确定操作系统或应用的当前标识。有关系统如何执行此操作的详细信息，请参阅第 46-4 页上的了解当前标识。

请注意，从网络映射中移除受影响的主机后，除第三方漏洞之外的所有数据都将被丢弃。有关设置脚本或导入文件的详细信息，请参阅 《*FireSIGHT 系统主机输入 API 指南*》。

要将已导入数据纳入影响关联中，必须将数据映射至数据库中的操作系统和应用定义。有关详细信息，请参阅以下各节：

- 第 46-27 页上的启用第三方数据
- 第 46-27 页上的管理第三方产品映射
- 第 46-30 页上的映射第三方漏洞
- 第 46-30 页上的管理自定义产品映射

启用第三方数据

许可证：FireSIGHT

可从网络上的第三方系统导入网络映射数据。然而，要启用入侵和发现数据结合使用的功能，如 FireSIGHT 推荐、自适应配置文件或影响评估，应将其中的尽可能多的元素映射至相应的定义。考虑对使用第三方数据的以下要求：

- 如果拥有在您的网络资产上有特定数据的第三方系统，则可使用主机输入功能导入该数据。然而，因为第三方可能会以不同的方式命名产品，所以，必须将第三方供应商、产品和版本映射至相应的思科产品定义。映射产品后，必须在系统策略为影响评估启用漏洞映射，以便支持影响关联。对于无版本或无供应商的应用协议，需要在系统策略中为应用协议映射漏洞。有关详细信息，请参阅第 46-27 页上的映射第三方产品。
- 如果导入来自第三方的修补程序信息，并想要将修补程序修补的所有漏洞标记为无效，则必须将第三方修补程序的名称映射至数据库中的定义。修补程序针对的所有漏洞随后会从添加该修补程序所在的主机中移除。有关详细信息，请参阅第 46-29 页上的映射第三方产品修补程序。
- 如果导入来自第三方的操作系统和应用协议漏洞，并想将其用于影响关联，则必须将第三方漏洞标识字符串映射至数据库中的漏洞。请注意，尽管许多客户端拥有关联的漏洞，而且客户端用于影响评估，但不能导入和映射第三方客户端漏洞。漏洞映射后，必须在系统策略中为影响评估启用第三方漏洞映射。有关详细信息，请参阅第 46-30 页上的映射第三方漏洞。要使没有供应商或版本信息的应用协议映射至漏洞，管理用户还必须在系统策略中映射应用的漏洞。有关详细信息，请参阅第 63-27 页上的映射服务器的漏洞。
- 如果导入应用数据并想要将该数据用于影响关联，则必须将每个应用协议的供应商字符串映射至相应的思科应用协议定义。有关详细信息，请参阅第 46-30 页上的管理自定义产品映射。

管理第三方产品映射

许可证：FireSIGHT

如果通过用户输入功能将第三方数据添加至网络映射，则必须将第三方使用的供应商、产品和版本名称映射至思科产品定义。将产品映射至思科定义后，将根据这些定义分配漏洞。

类似地，如果正在导入第三方修补程序信息，如修补程序管理产品，则必须将修补程序的名称映射至适当供应商和产品以及数据库中的相应修补程序。

有关详细信息，请参阅以下各节：

- 第 46-27 页上的映射第三方产品
- 第 46-29 页上的映射第三方产品修补程序

映射第三方产品

许可证：FireSIGHT

如果导入第三方数据，则必须将思科产品映射至第三方名称，以分配漏洞并使用该数据执行影响关联。映射产品可以将思科漏洞信息与第三方产品名称关联，这样，系统就可使用该数据执行影响关联。

如果使用主机输入导入功能导入数据，还可以在导入过程中，使用 AddScanResult 函数将第三方产品映射至操作系统和应用漏洞。

例如，如果导入将 Apache Tomcat 列为应用的第三方的数据，而且知道该产品的版本为 6，则可添加第三方映射，其中 **Vendor Name** 设置为 `Apache`，**Product Name** 设置为 `Tomcat`，**Apache** 从 **Vendor** 下拉列表选择，**Tomcat** 从 **Product** 下拉列表选择，**6** 从 **Version** 下拉列表选择。该映射会使 Apache Tomcat 6 的任何漏洞分配至其应用列出了 Apache Tomcat 的主机。

请注意，对于无版本或无供应商的应用，必须在系统策略中为应用类型映射漏洞。有关详细信息，请参阅第 63-27 页上的映射服务器的漏洞。请注意，尽管许多客户端拥有关联的漏洞，而且客户端用于影响评估，但不能导入和映射第三方客户端漏洞。

提示 如已在另一防御中心上创建了第三方映射，则将其导出后可导入至此防御中心。然后，可根据自己的需求编辑已导入的映射 有关详细信息，请参阅第 A-1 页上的导入和导出配置。

要将第三方产品映射思科产品定义，请执行以下操作：

访问：管理

步骤 1 选择 **Policies > Application Detectors**，然后点击 **User Third-Party Mappings**。

系统将显示 User Third-Party Mappings 页面。

步骤 2 您有两种选择：

- 要编辑现有映射集，点击映射集旁的 **Edit**。
- 要创建新的映射集，点击 **Create Product Map Set**。

系统将显示 Edit Third-Party Product Mappings 页面。

步骤 3 在 **Mapping Set Name** 字段中，键入映射集的名称。

步骤 4 在 **Description** 字段中键入描述。

步骤 5 您有两种选择：

- 要映射第三方产品，点击 **Add Product Map**。
- 要编辑现有第三方产品映射，点击映射集合旁的 **Edit**。

系统将显示 Add Product Map 页面。

步骤 6 在 **Vendor String** 字段中，键入第三方产品使用的供应商字符串。

步骤 7 在 **Product String** 字段中，键入第三方产品使用的产品字符串。

步骤 8 在 **Version String** 字段中，键入第三方产品使用的版本字符串。

步骤 9 在 Product Mappings 部分中，从以下列表 （如适用）为漏洞映射选择想要使用的操作系统、产品和版本：

- **供应商**
- **产品**
- **Major Version**
- **Minor Version**
- **Revision Version**
- **构建**
- **配线板**
- **分机**

例如，如果想要运行名称包含第三方字符串的产品的主机使用 Red Hat Linux 9 的漏洞，选择 **Redhat, Inc.** 作为供应商， **Redhat Linux** 作为产品，以及 **9** 作为版本。

步骤 10 点击 **Save**。

映射第三方产品修补程序

许可证：FireSIGHT

如果将修补程序名称映射至数据库中的特定修补程序集，则可从第三方修补程序管理应用中导入数据，并将修补程序应用至主机集。修补程序名称导入至主机后，对于该主机，系统会将修补程序针对的所有漏洞标记为无效。

要将第三方修补程思科修补程序定义，请执行以下操作：

访问：管理员/

步骤 1　选择 **Policies > Application Detectors**，然后点击 **User Third-Party Mappings**。

系统将显示 User Third-Party Mappings 页面。

步骤 2　您有两种选择：

- 要编辑现有映射集，点击映射集旁的 **Edit**。
- 要创建新的映射集，点击 **Create Product Map Set**。

系统将显示 Edit Third-Party Product Mappings 页面。

步骤 3　在 **Mapping Set Name** 字段中，键入映射集的名称。

步骤 4　在 **Description** 字段中键入描述。

步骤 5　您有两种选择：

- 要映射第三方产品，点击 **Add Fix Map**。
- 要编辑现有第三方产品映射，点击映射旁的 **Edit**。

系统将显示 Add Fix Map 页面。

步骤 6　在 **Third-Party Fix Name** 字段中，键入想要映射的修补程序的名称。

步骤 7　在 Product Mappings 部分中，从以下列表 （如适用）为修补程序映射选择想要使用的操作系统、产品和版本：

- **供应商**
- **产品**
- **Major Version**
- **Minor Version**
- **Revision Version**
- **构建**
- **配线板**
- **分机**

例如，如果您想要您的映射分配来自 Red Hat Linux 9 的选定补丁至修补程序应用至的主机，选择 **Redhat, Inc.** 作为供应商， **Redhat Linux** 作为产品，以及 **9** 作为版本。

步骤 8　点击 **Save**，以保存修补程序映射。

映射第三方漏洞

许可证：FireSIGHT

要将第三方的漏洞信息添加至 VDB，必须将每个导入的漏洞的第三方标识字符串映射至任何现有的思科、 Bugtraq 或 Snort ID。为漏洞创建映射后，映射作用于导入至网络映射中主机的所有漏洞，并允许对这些漏洞进行影响关联。

请注意，只能为第三方漏洞启用影响关联，才能执行影响关联。有关详细信息，请参阅第 45-28 页上的启用漏洞影响评估映射。对于无版本或无供应商的应用，还必须在系统策略中为应用类型映射漏洞。有关详细信息，请参阅第 63-27 页上的映射服务器的漏洞。

另外，尽管许多客户端拥有关联的漏洞，而且客户端用于影响评估，但不能将第三方客户端漏洞用于影响评估。

提示 如已在另一防御中心上创建了第三方映射，则将其导出后可导入至此防御中心。然后，可根据自己的需求编辑已导入的映射 有关详细信息，请参阅第 A-1 页上的导入和导出配置。

要将第三方漏洞映射至现有漏洞，请执行以下操作：

访问：管理

步骤 1 选择 **Policies > Application Detectors**，然后点击 **User Third-Party Mappings**。

系统将显示 User Third-Party Mappings 页面。

步骤 2 您有两种选择：

- 要编辑现有漏洞集，点击漏洞集旁的 **Edit**。
- 要新建漏洞集，点击 **Create Vulnerability Map Set**。

系统将显示 Edit Third-Party Vulnerability Mappings 页面。

步骤 3 点击 **Add Vulnerability Map**。

系统将显示 Add Vulnerability Map 弹出窗口。

步骤 4 在 **Vulnerability ID** 字段中，键入第三方漏洞标识。

步骤 5 在 **Vulnerability Description** 字段中，键入描述。

步骤 6 或者，在 **Snort Vulnerability ID Mappings** 字段中，输入签名 ID。

步骤 7 或者，在**思科 Vulnerability ID Mappings** 字段中，输入思科漏洞 ID。

步骤 8 或者，在 **Bugtraq Vulnerability ID Mappings** 字段中，输入 Bugtraq 标识号。

步骤 9 点击**添加**。

管理自定义产品映射

许可证：FireSIGHT

可使用产品映射来确保第三方的多个输入与适当思科定义关联。定义和激活产品映射后，拥有已映射供应商字符串的网络映射中主机上的所有服务器或客户端均使用自定义产品映射。为此，您可能想要为网络中带有特定供应商字符串的服务器映射漏洞，而不是显式地为服务器设置供应商、产品和版本。

有关详情，请参阅：

- 第 46-31 页上的创建自定义产品映射
- 第 46-32 页上的编辑自定义产品映射列表
- 第 46-32 页上的管理自定义产品映射激活状态

创建自定义产品映射

许可证：FireSIGHT

如果系统无法将网络映射中的服务器映射至 VDB 中的供应商和产品，则可为系统手动创建映射以便在识别服务器时使用。激活自定义产品映射后，系统会将选定供应商和产品的漏洞映射至网络映射中的出现供应商字符串的所有服务器。

注　自定义产品映射将应用至应用协议的所有出现位置，而无论应用数据的源如何（如 Nmap、主机输入功能或 FireSIGHT 系统自身）。然而，如果使用主机输入功能导入的数据的第三方漏洞映射与通过自定义产品映射设置的映射发行冲突，则输入出现时，第三方漏洞映射将覆盖自定义产品映射并使用第三方漏洞映射设置。有关详细信息，请参阅第 46-30 页上的映射第三方漏洞。

可创建产品映射列表，然后通过激活或停用每份列表而一次性启用或禁用多个映射。选择将要映射至的供应商后，系统将更新产品列表，以仅纳入该供应商提供的产品。

创建自定义产品映射后，必须激活自定义产品映射列表。激活自定义产品映射列表后，系统将更新出现指定供应商字符串的所有服务器。对于通过主机输入功能导入的数据，漏洞将更新，除非已为此服务器显式设置产品映射。

例如，如果贵公司将您的 Apache Tomcat 网络服务器的横幅修改为 `Internal Web Server`，则可将供应商字符串 `Internal Web Server` 映射至供应商 **Apache** 和产品 **Tomcat**，然后激活包含该映射的列表，出现标有 `Internal Web Server` 的服务器的所有主机均拥有数据库中的 Apache Tomcat 漏洞。

提示　可使用此功能将漏洞映至至本地入侵规则，只需将规则的 SID 映射至另一漏洞。

要创建自定义产品映射，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Application Detectors**，然后点击 **Custom Product Mappings**。

系统将显示 Custom Product Mappings 页面。

步骤 2　点击 **Create Custom Product Mapping List**。

系统将显示 Edit Custom Product Mappings List 页面。

步骤 3　在 **Custom Product Mapping List Name** 字段中键入名称。

步骤 4　点击 **Add Vendor String**。

系统将显示 Add Vendor String 弹出窗口。

步骤 5　在 **Vendor String** 字段中，键入供应商字符串，该字符串标识应映射至选定供应商和产品值的应用。

步骤 6　从 **Vendor** 下拉列表，选择想要映射的供应商。

步骤 7　从 **Product** 下拉列表，选择想要映射的产品。

步骤 8　点击 **Add**，以将已映射的供应商字符串添加至列表。

步骤 9　或者，在必要时，重复第 4 至 8 步，将额外的供应商字符串映射添加至列表。

步骤 10　完成后，点击 **Save**。

系统将再次显示 Custom Product Mappings 页面，带有您添加的列表。

编辑自定义产品映射列表

许可证：FireSIGHT

可修改现有自定义产品映射列表，只需添加或移除供应商字符串或更改列表名称。

要编辑自定义产品映射，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Application Detectors**，然后点击 **Custom Product Mappings**。

系统将显示 Custom Product Mappings 页面。

步骤 2　点击想要编辑的产品映射列表旁的编辑图标 ( )。

系统将显示 Edit Custom Product Mappings List 页面。

步骤 3　必要时，更改列表。有关详细信息，请参阅第 46-31 页上的创建自定义产品映射。

步骤 4　完成后，点击 **Save**。

系统将显示 Custom Product Mappings 页面，带有您已更新的列表。

管理自定义产品映射激活状态

许可证：FireSIGHT

可一次性启用或禁用整个自定义产品映射列表。激活自定义产品映射列表后，该列表上的每个映射均应用至网络映射中主机上的所有带有指定供应商字符串的应用，无论是通过受管设备检测到的，还是通过主机输入功能导入的。

要激活或停用自定义产品映射列表，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Application Detectors**，然后点击 **Custom Product Mappings**。

系统将显示 Custom Product Mappings 页面。

步骤 2　修改自定义产品映射列表的状态：

- 要启用自定义产品映射列表，请点击 **Activate**。
- 要禁用自定义产品映射列表，请点击 **Deactivate**。

配置主动扫描

FireSIGHT 系统 通过对网络上的流量进行被动分析构建网络映射。然而，有时可能需要主动扫描主机，确定有关主机的信息。例如，如果主机有一台服务器在开放端口上运行但在系统监控网络期间未收发流量，则系统不向网络映射添加有关该服务器的信息。但是，如使用主动扫描仪直接扫描主机，则可检测到服务器的存在。

主动扫描主机时，可发送数据包，尝试获取有关此主机的信息。 FireSIGHT 系统可与 Nmap™ 6.01 相集成， Nmap™ 6.01 是一个开源主动扫描仪，可用于网络探索和安全审计，检测正在主机上运行的操作系统和服务器。通过 Nmap 扫描，可查找有关主机上运行的操作系统和服务器的详细信息，根据结果改进系统的漏洞报告。

注 有些扫描选项 （例如，端口扫描）会显著增加低带宽网络的负载。应始终安排此类扫描在网络使用量较低的时段运行。

有关详细信息，请参阅以下各节：

了解 Nmap 扫描

许可证：FireSIGHT

可使用 Nmap 主动扫描网络主机的端口，确定主机的操作系统和服务器数据，从而增强网络映射，微调已映射至已扫描主机的漏洞精确度。注意，只有网络映射中存在主机， Nmap 才能将其结果附加至主机配置文件。还可在结果文件中查看扫描结果。

使用 Nmap 扫描主机时，之前未检测到的开放端口上的服务器将添加至该主机配置文件中的服务器列表。主机配置文件在“扫描结果”部分列出在已过滤或关闭 TCP 端口或 UDP 端口上检测到的任何服务器。默认情况下， Nmap 扫描超过 1660 个 TCP 端口。

Nmap 将扫描结果与超过 1500 个已知操作系统指纹进行对比，确定操作系统，并为每个操作系统评分。分配给主机的操作系统是得分最高的操作系统指纹。

如果系统识别在 Nmap 扫描中已确定的服务器且有对应的服务器定义，则系统会将该服务器的漏洞映射至主机。系统将 Nmap 使用的服务器名称映射至对应的思科服务器定义，然后使用已映射至系统中每台服务器的漏洞。同样，系统会将 Nmap 操作系统名称映射至思科操作系统定义。当 Nmap 检测主机的操作系统时，系统会将漏洞从对应的思科操作系统定义分配给主机。

有关用于扫描的基础 Nmap 技术的详细信息，请参阅 http://insecure.org 上的 Nmap 文档。

有关思科设备上 Nmap 的详细信息，请参阅以下主题：

- 第 47-2 页上的了解 Nmap 补救
- 第 47-4 页上的创建 Nmap 扫描策略
- 第 47-5 页上的样本 Nmap 扫描配置文件

了解 Nmap 补救

许可证：FireSIGHT

可为 Nmap 扫描定义设置，只需创建 Nmap 补救。 Nmap 补救可用作关联策略中的响应，按需运行，或预定在特定时间运行。为了让 Nmap 扫描结果出现在网络映射中，已扫描的主机必须已存在于网络映射中。

请注意， Nmap 提供的服务器和操作系统数据将保持不变，直到您运行另一个 Nmap 扫描为止。如计划使用 Nmap 扫描主机以获取操作系统和服务器数据，则可能希望设置定期扫描，随时更新任何 Nmap 提供的操作系统和服务器数据。有关详细信息，请参阅第 62-5 页上的自动运行 Nmap 扫描。另请注意，如从网络映射中删除主机，则将丢弃该主机的任何 Nmap 扫描结果。

有关 Nmap 功能的详细信息，请参阅 http://insecure.org 上的 Nmap 文档。下表说明可在 FireSIGHT 系统上的 Nmap 补救中配置的选项。

表 47-1　　Nmap 补救选项

选项	说明	对应的 Nmap 选项
Scan Which Address(es) From Event?	将 Nmap 扫描用作对关联规则的响应时，选择一个选项以控制扫描事件中的哪个地址，源主机的地址、目标主机的地址或两者。	不适用
Scan Types	选择 Nmap 如何扫描端口： • **TCP Syn** 扫描可以快速连接到数千个端口，无需使用完整的 TCP 握手。此选项可用于在以下主机上以隐形模式快速扫描，可发起但不完成 TCP 连接：`admin` 帐户拥有原始数据包访问权限的主机，或未运行 IPv6 的主机。如果主机确认在 TCP Syn 扫描中发送的 Syn 数据包， Nmap 会重置连接。 • **TCP Connect** 扫描使用 `connect()` 系统调用，打开穿过主机操作系统的连接。如果防御中心或受管设备上的 `admin` 用户在主机上没有原始数据包权限，或正在扫描 IPv6 网络，则可使用 TCP Connect 扫描。换句话说，在无法使用 TCP Syn 扫描的情况下使用此选项。 • **TCP ACK** 扫描发送 ACK 数据包，检查端口是否已被过滤。 • **TCP Window** 扫描的工作方式与 TCP ACK 扫描相同，但也可确定端口已打开还是关闭。 • **TCP Maimon** 扫描使用 FIN/ACK 探针识别 BSD 派生系统。	**TCP Syn**: `-sS` **TCP Connect**: `-sT` **TCP ACK**: `-sA` **TCP Window**: `-sW` **TCP Maimon**: `-sM`
Scan for UDP ports	启用此选项，可扫描 UDP 端口以及 TCP 端口。请注意，扫描 UDP 端口可能比较耗时，因此，如果想快速扫描，请避免使用此选项。	`-sU`

表 47-1　Nmap 补救选项（续）

选项	说明	对应的 Nmap 选项
Use Port From Event	如果计划将补救用作关联政策中的响应，请启用此选项，使补救仅扫描在触发关联响应的事件中指定的端口。 **提示**　也可控制 Nmap 是否收集操作系统信息和服务器信息。启用 **Use Port From Event** 选项，可扫描与新服务器关联的端口。	不适用
Scan from reporting detection engine	启用此选项，可从报告主机的检测引擎所驻留的设备扫描主机。	不适用
Fast Port Scan	启用此选项，仅扫描 `nmap-services` 文件中所列的 TCP 端口，而忽略其他端口设置，该文件位于执行扫描设备上的 `/var/sf/nmap/share/nmap/nmap-servicesservices` 目录中。请注意，不能同时使用此选项与 **Port Ranges and Scan Order** 选项。	`-F`
Port Ranges and Scan Order	使用 Nmap 端口规范语法设置要扫描的特定端口及其扫描顺序。请注意，不能同时使用此选项与 **Fast Port Scan** 选项。	`-p`
Probe open ports for vendor and version information	启用此选项，可检测服务器厂商和版本信息。如探测开放端口以获取服务器厂商和版本信息， Nmap 将获取其用来识别服务器的服务器数据。然后，它将用思科服务器数据替换该服务器。	`-sV`
Service Version Intensity	选择适用于服务器版本的 Nmap 探针强度。服务强度越大，使用的探针越多，精确度也越高，而强度越低，探针速度越快，但获取的信息越少。	`--version-intensity <intensity>`
Detect Operating System	启用此选项，可检测主机的操作系统信息。 如果配置主机的操作系统检测， Nmap 将扫描主机，使用扫描结果创建每个操作系统的评级，反映操作系统在主机上运行的可能性。有关 Nmap 识别的身份数据何时及如何出现在网络映射中的详细信息，请参阅第 46-4 页上的了解当前标识。	`-o`
Treat All Hosts As Online	启用此选项，可跳过主机发现过程，在目标范围的每台主机上运行端口扫描。请注意，启用此选项时， Nmap 会忽略 **Host Discovery Method** 和 **Host Discovery Port List** 的设置。	`-PN`
Host Discovery Method	选择此选项，在 **Host Discovery Port List** 中列出的端口上，为目标范围中的所有主机执行主机发现，或者，如未列出端口，则在适用于主机发现方法的默认端口上执行。 然而，请注意，如也启用 **Treat All Hosts As Online**， **Host Discovery Method** 选项不起作用，不执行主机发现。 选择 Nmap 测试时要使用的方法，查看主机是否存在并可用： • 如果收到响应， **TCP SYN** 选项将发送设置了 SYN 标记的空 TCP 数据包，并认为主机可用。默认情况下， TCP SYN 扫描端口 80。请注意，TCP SYN 扫描不太可能被设有状态性防火墙规则的防火墙拦截。 • 如果收到响应， **TCP ACK** 选项将发送设置了 ACK 标志的空 TCP 数据包，并认为主机可用。默认情况下， TCP ACK 扫描端口 80。请注意，TCP ACK 扫描不太可能被设有无状态防火墙规则的防火墙拦截。 • 如果端口不可达响应来自已关闭端口， **UDP** 选项将发送 UDP 数据包，并假设主机可用性。默认情况下， UDP 扫描端口 40125。	**TCP SYN**: `-PS` **TCP ACK**: `-PA` **UDP**: `-PU`
Host Discovery Port List	指定在执行主机发现时要扫描的自定义端口列表，用逗号隔开。	主机发现方法端口列表
Default NSE Scripts	启用此选项，运行默认 Nmap 脚本集，执行主机发现以及服务器、操作系统和漏洞检测。有关默认脚本列表，请参阅 http://nmap.org/nsedoc/categories/default.html。	`-sC`

表 47-1　Nmap 补救选项 （续）

选项	说明	对应的 Nmap 选项
计时模板	选择扫描过程的时间；选择的数字越大，扫描越快、越不全面。	**0**: `T0` (paranoid) **1**: `T1` (sneaky) **2**: `T2` (polite) **3**: `T3` (normal) **4**: `T4` (aggressive) **5**: `T5` (insane)

创建 Nmap 扫描策略

许可证：FireSIGHT

尽管主动扫描可以获取宝贵信息，但过度使用 Nmap 等工具可能会使您的网络资源超载，甚至使重要的主机瘫痪。使用任何主动式扫描仪时，应创建扫描策略，确保仅扫描需要扫描的主机和端口。

有关详细信息，请参阅以下各节：

- 第 47-4 页上的选择适当的扫描目标
- 第 47-5 页上的选择适当端口进行扫描
- 第 47-5 页上的设置主机发现选项

选择适当的扫描目标

许可证：FireSIGHT

配置 Nmap 时，可创建扫描目标以识别要扫描的主机。扫描目标包括一个 IP 地址、 CIDR 块或八位字节 IP 地址范围、 IP 地址范围或要扫描的 IP 地址或范围列表，以及一台或多台主机上的端口。

可通过以下方式指定目标：

- 对于 IPv6 主机：
  - 精确的 IP 地址 （例如 `192.168.1.101`）
- 对于 IPv4 主机：
  - 精确的 IP 地址 （例如， `192.168.1.101`）或 IP 地址列表 （用逗号或空格隔开）
  - 使用 CIDR 表示法的 IP 地址块（例如，`192.168.1.0/24` 扫描 192.168.1.1 和 192.168.1.254 （含）之间的 254 台主机）

    有关在 FireSIGHT 系统中使用 CIDR 表示法的信息，请参阅第 1-16 页上的 IP 地址约定。
  - 使用八位字节范围寻址的 IP 地址范围 （例如， `192.168.0-255.1-254` 扫描 192.168.x.x 范围内的所有地址，但以 .0 和 .255 结尾的地址除外）
  - 使用连字符的 IP 地址范围 （例如， `192.168.1.1 - 192.168.1.5` 扫描在 192.168.1.1 和 192.168.1.5 （含）之间的六台主机）
  - 地址或范围列表，用逗号或空格隔开 （例如， `192.168.1.0/24, 194.168.1.0/24` 扫描 192.168.1.1 和 192.168.1.254（含）之间的 254 台主机，以及 194.168.1.1 和 194.168.1.254 （含）之间的 254 台主机）

Nmap 扫描的理想扫描目标包括有系统无法识别的操作系统的主机、有无法识别的服务器的主机，或者最近在网络上检测到的主机。谨记， Nmap 结果不能添加至不存在于网络映射中主机的网络映射。

注意事项 Nmap 提供的服务器和操作系统数据将保持不变，直到您运行另一个 Nmap 扫描为止。如果计划使用 Nmap 扫描主机，可能要设置定期扫描，随时更新 Nmap 提供的任何操作系统和服务器数据。有关详细信息，请参阅第 62-5 页上的自动运行 Nmap 扫描。另请注意，如从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。此外，请确保您有权限扫描您的目标。使用 Nmap 扫描不属于您或贵公司的主机可能违法。

选择适当端口进行扫描

许可证：FireSIGHT

可为已配置的每个扫描目标选择要扫描的端口。您可以指定各个端口号、端口范围或一系列端口号和端口范围，识别应当在每个目标上扫描的精确端口集。

默认情况下，Nmap 扫描 TCP 端口 1 至端口 1024。如果计划将补救用作关联政策中的响应，则可使补救仅扫描在触发关联响应的事件中指定的端口。如果按需运行补救或将补救作为预定任务加以运行，或者，如不使用来自事件的端口，则可使用其他端口选项确定哪些端口已扫描。可选择仅扫描在 `nmap-services` 文件中列出的 TCP 端口，忽略其他端口设置。除 TCP 端口外，还可扫描 UDP 端口。请注意，扫描 UDP 端口可能比较耗时，因此，如要快速扫描，请避免使用此选项。为选择要扫描的特定端口或端口范围，请使用 Nmap 端口规范语法识别端口。

设置主机发现选项

许可证：FireSIGHT

在开始主机的端口扫描之前，可决定是否执行主机发现，或者，可假设计划要扫描的所有主机均在线。如果选择不将所有主机视为在线，则可选择要使用的主机发现方法，如果需要，自定义在主机发现过程中扫描的端口列表。主机发现不能从已列出端口探测操作系统或服务器信息；它仅使用特殊端口上的响应确定主机是否活动且可用。如果执行主机发现且主机不可用， Nmap 则不扫描该主机上的端口。

样本 Nmap 扫描配置文件

许可证：FireSIGHT

下列情境通过示例说明如何在网络上使用 Nmap：

- 第 47-5 页上的示例：解析未知操作系统
- 第 47-6 页上的示例：响应新主机

示例：解析未知操作系统

许可证：FireSIGHT

如果系统无法确定网络上主机的操作系统，则可使用 Nmap 主动扫描主机。 Nmap 使用其通过扫描获取的信息对可能的操作系统进行评级。然后，它使用评级最高的操作系统作为主机操作系统标识。

如使用 Nmap 向新主机质询操作系统和服务器信息，则将停用系统为已扫描主机对该数据进行的监控。如果使用 Nmap 发现主机的主机操作系统和服务器操作系统，系统会标记为拥有未知操作系统，您可以识别相似的主机组。然后，可根据其中一个主机组创建自定义指纹，使系统能够根

据 Nmap 扫描，将指纹与已知在主机上运行的操作系统相关联。尽可能创建自定义指纹，而不是通过第三方来源 （例如， Nmap）输入静态数据，因为自定义指纹允许系统继续监控主机操作系统并按需更新。

要使用 Nmap 发现操作系统，请执行以下操作：

访问：管理员/发现管理员

步骤 1　为 Nmap 模块配置扫描实例。

有关详细信息，请参阅第 47-8 页上的创建 Nmap 扫描实例。

步骤 2　使用以下设置创建 Nmap 补救：

- 启用 **Use Port From Event**，可扫描与新服务器相关的端口。
- 启用 **Detect Operating System**，可检测主机的操作系统信息。
- 启用 **Probe open ports for vendor and version information**，可检测服务器厂商和版本信息。
- 启用 **Treat All Hosts as Online**，因为已知存在主机。

有关创建 Nmap 补救的信息，请参阅第 47-10 页上的创建 Nmap 补救。

步骤 3　创建在系统检测具有未知操作系统的主机时可触发的关联规则。

该规则应在**发生发现事件**并且**主机的操作系统信息已更改**且符合以下条件时触发：**操作系统名称未知**。

有关创建关联规则的信息，请参阅第 51-2 页上的创建关联策略规则。

步骤 4　创建包含关联规则的关联策略。

有关创建关联策略的更多信息，请参阅第 51-42 页上的创建关联策略。

步骤 5　在关联策略中，将在以前步骤中创建的 Nmap 补救作为响应添加至在第 3 步中创建的规则。

步骤 6　激活关联策略。

步骤 7　清除网络映射上的主机，强制网络发现重新启动，重建网络映射。

步骤 8　一两天后，搜索关联策略生成的事件。分析在主机上检测到的操作系统的 Nmap 结果，弄清网络上是否有系统无法识别的特殊主机配置。

有关分析 Nmap 结果的详细信息，请参阅第 47-19 页上的分析扫描结果。

步骤 9　如果发现未知操作系统的 Nmap 结果相同的主机，请为其中一台主机创建自定义指纹，并用它识别未来的类似主机。

有关详细信息，请参阅第 46-7 页上的设置客户端指纹。

示例：响应新主机

许可证：FireSIGHT

当系统在子网中检测到可能被入侵的新主机时，您可能想扫描该主机，确保获取该主机漏洞的准确信息。

要完成此操作，可创建和激活关联策略，当子网中出现新主机时进行检测，启动补救以对主机上执行 Nmap 扫描。

激活关联策略后，可定期查看补救状态视图 (**Policy & Response > Responses > Remediations > Status**)，查看补救启动时间。补救的动态扫描目标应当包括其因服务器检测而扫描的主机的 IP 地址。根据 Nmap 检测的操作系统和服务器，查看这些主机的主机配置文件，弄清主机上是否存在需要解决的漏洞。

注意事项 如有大型或动态网络，新主机检测可能太频繁，而无法使用扫描进行响应。为防止资源超载，请避免使用 Nmap 扫描响应频繁发生的事件。此外，请注意，如果使用 Nmap 向新主机质询操作系统和服务器信息思科，则将停用系统为已扫描主机对该数据进行的监控。

要为响应新主机的出现执行扫描，请执行以下操作：

访问：管理员/发现管理员

步骤 1 为 Nmap 模块配置扫描实例。

有关详细信息，请参阅第 47-8 页上的创建 Nmap 扫描实例。

步骤 2 使用以下设置创建 Nmap 补救：

- 启用 **Use Port From Event**，可扫描与新服务器相关的端口。
- 启用 **Detect Operating System**，可检测主机的操作系统信息。
- 启用 **Probe open ports for vendor and version information**，可检测服务器厂商和版本信息。
- 启用 **Treat All Hosts as Online**，因为已知存在主机。

有关创建 Nmap 补救的信息，请参阅第 47-10 页上的创建 Nmap 补救。

步骤 3 创建在系统检测特定子网中的新主机时可触发的关联规则。

此规则应在**发生发现事件**并**检测到新主机时**触发。

有关创建关联规则的信息，请参阅第 51-2 页上的创建关联策略规则。

步骤 4 创建包含关联规则的关联策略。

有关创建关联策略的更多信息，请参阅第 51-42 页上的创建关联策略。

步骤 5 在关联策略中，将在以前步骤中创建的 Nmap 补救作为响应添加至在第 3 步中创建的规则。

步骤 6 激活关联策略。

步骤 7 收到出现新主机的通知时，检查主机配置文件，查看 Nmap 扫描结果，解决任何适用于主机的漏洞。

设置 Nmap 扫描

许可证：FireSIGHT

要使用 Nmap 扫描，必须首先配置扫描实例和扫描补救。如果计划安排 Nmap 扫描，还必须界定扫描目标。

有关详细信息，请参阅以下各节：

创建 Nmap 扫描实例

许可证：FireSIGHT

可为要用于扫描网络漏洞的每个 Nmap 模块设置独立的扫描实例。可为防御中心上的本地 Nmap 模块以及想要用于远程运行扫描的任何设备设置扫描实例。每次扫描的结果始终存储在防御中心上，可在这里配置扫描，即使是从远程设备运行扫描。为防止意外或恶意扫描关键任务主机，可创建实例黑名单，指出不应通过实例扫描的主机。

请注意，不可添加与现有扫描实例名称相同的扫描实例。

要创建扫描实例，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Scanners**。

系统将显示 Scanners 页面。

步骤 2　点击 **Add Nmap Instance**。

系统将显示 Instance Detail 页面。

步骤 3　在 **Instance Name** 字段中，输入包括 1 至 63 个字母数字字符的名称，不得含有空格以及除下划线 (_) 和 连接号 (-) 的特殊字符。

步骤 4　在 **Description** 字段中，指定描述，其中包含 0 到 255 个字母数字字符，可以包含空格和特殊字符。

步骤 5　或者，在 **Black Listed Scan hosts** 字段中，使用以下语法指定 *不应*通过该扫描实例扫描的任何主机或网络：

- 对于 IPv6 主机，精确的 IP 地址 （例如， `2001:DB8:fedd:eeff`）
- 对于 IPv4 主机，精确的 IP 地址 （例如， `192.168.1.101`）或使用 CIDR 表示法的 IP 地址块（例如， `192.168.1.0/24` 扫描 `192.168.1.1` 与 `192.168.1.254` 之间的 254 台主机，包括二者）
- 请注意，不能使用感叹号 (!) 否定地址值。

如将已列入黑名单网络的主机指定为扫描目标，则该扫描将不运行。

步骤 6　或者，要从远程设备而非防御中心运行扫描，请在 **Remote Device Name** 字段中指定设备的 IP 地址或名称，因为它会显示在 防御中心网络界面中的设备 Information 页面中。

步骤 7　点击 **Create**。

扫描实例创建成功。

创建 Nmap 扫描目标

许可证：FireSIGHT

可创建和保存扫描目标以识别特定主机和端口。然后，在执行按需扫描或安排扫描时，可使用其中一个已保存的扫描目标。

如果扫描带 IPv4 地址的目标，可使用 IP 地址、IP 地址列表、CIDR 表示法或 Nmap 扫描八位字节选择要扫描的主机。也可使用连字符指定地址范围。使用逗号或空格分隔列表中的地址和范围。

如果扫描 IPv6 地址，请使用 IP 地址。不支持地址范围。

请注意， Nmap 提供的服务器和操作系统数据将保持不变，直至运行另一个 Nmap 扫描。如果计划使用 Nmap 扫描主机，可能要设置定期扫描，随时更新 Nmap 提供的任何操作系统和服务器数据。有关详细信息，请参阅第 62-5 页上的自动运行 Nmap 扫描。另请注意，如从网络映射中删除主机，则将丢弃该主机的任何 Nmap 扫描结果。

要创建扫描目标，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Scanners**。

系统将显示 Scanners 页面。

步骤 2　在工具栏上，点击 **Targets**。

系统将显示 Scan Target List 页面。

步骤 3　点击 **Create Scan Target**。

系统将显示 Scan Target 页面。

步骤 4　在 **Name** 字段中，键入要用于此扫描目标的名称。

步骤 5　在 **IP Range** 文本框中，使用以下语法指定要扫描的主机：

- 对于 IPv6 主机，精确的 IP 地址 （例如， `2001:DB8::fedd:eeff`）
- 对于 IPv4 主机，精确的 IP 地址 （例如， `192.168.1.101`）或逗号隔开的 IP 地址列表
- 对于 IPv4 主机，使用 CIDR 表示法的 IP 地址块（例如，`192.168.1.0/24` 扫描 192.168.1.1 和 192.168.1.254 （含）之间的 254 台主机）

  有关在 FireSIGHT 系统中使用 CIDR 表示法的信息，请参阅第 1-16 页上的 IP 地址约定。
- 对于 IPv4 主机，使用八位字节范围寻址的 IP 地址范围 （例如， `192.168.0-255.1-254` 扫描 `192.168.x.x` 范围内的所有地址，但以 .0 和 .255 结尾的地址除外）
- 对于 IPv4 主机，使用连字符的 IP 地址范围 （例如， `192.168.1.1 - 192.168.1.5` 扫描 192.168.1.1 和 192.168.1.5 （含）之间的 6 台主机）
- 对于 IPv4 主机，用逗号或空格隔开的地址或范围列表 （例如， `192.168.1.0/24`, `194.168.1.0/24` 扫描 192.168.1.1 和 192.168.1.254 （含）之间的 254 台主机，以及 194.168.1.1 和 194.168.1.254 （含）之间的 254 台主机）

注　**IP Range** 文本框最多可接受 255 个字符。此外，请注意，如在扫描目标中的 IP 地址或范围列表中使用逗号，则保存目标时，逗号将转换为空格。

步骤 6　在 **Ports** 字段中，指定要扫描的端口。

可使用从 1 到 65535 的值输入以下任意项：

- 端口号
- 用逗号分隔的端口列表
- 用连接号分隔的端口号范围
- 用连接号连接的端口号范围，用逗号分隔

步骤 7　点击 **Save**。

扫描目标创建成功。

创建 Nmap 补救

许可证：FireSIGHT

可为 Nmap 扫描定义设置，只需创建 Nmap 补救。 Nmap 补救可用作关联策略中的响应，按需运行，或预定在特定时间运行。为了让 Nmap 扫描结果出现在网络映射中，已扫描的主机必须已存在于网络映射中。

有关 Nmap 补救中特定设置的详细信息，请参阅第 47-2 页上的了解 Nmap 补救。

请注意， Nmap 提供的服务器和操作系统数据将保持不变，直至运行另一个 Nmap 扫描。如计划使用 Nmap 扫描主机以获取操作系统和服务器数据，则可能希望设置定期扫描，随时更新任何 Nmap 提供的操作系统和服务器数据。有关详细信息，请参阅第 62-5 页上的自动运行 Nmap 扫描。另请注意，如从网络映射中删除主机，则将丢弃该主机的任何 Nmap 扫描结果。

有关 Nmap 功能的一般信息，请参阅 http://insecure.org 上的 Nmap 文档。

要创建 Nmap 补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Scanners**。

系统将显示 Scanners 页面。

步骤 2　在要为其添加补救的扫描实例旁，点击 **Add Remediation**。

系统将显示 Edit Remediation 页面。

步骤 3　在 **Remediation Name** 字段中，键入补救名称，其中包含 1 到 63 个字母数字字符，没有空格以及除下划线 (_) 和连接号 (-) 以外的特殊字符。

步骤 4　在 **Description** 字段中，键入补救说明，其中包含 0 到 255 个字母数字字符，包括空格和特殊字符。

步骤 5　如果计划使用此补救响应在发生入侵事件、连接事件或用户事件时触发的关联规则，请配置 **Scan Which Address(es) From Event?** 选项：

- 选择 **Scan Source and Destination Addresses**，扫描事件中源 IP 地址和目标 IP 地址代表的主机。
- 选择 **Scan Source Address Only**，扫描事件源 IP 地址代表的主机。
- 选择 **Scan Destination Address Only**，扫描事件目标 IP 地址代表的主机。

如果计划使用此补救响应在发生发现事件或主机输入事件时触发的关联规则，默认情况下，补救将扫描事件涉及到的主机的 IP 地址；无需配置此选项。

注　不能将 Nmap 修复作为响应分配至在流量量变曲线变更上触发的关联规则。

步骤 6　配置 **Scan Type** 选项：

- 要在以下主机上以隐形模式快速扫描，可发起但不完成 TCP 连接：`admin` 帐户拥有原始数据包访问权限的主机，或未运行 IPv6 的主机，请选择 **TCP Syn Scan**。
- 要使用系统 `connect()` 调用 （可用于以下主机：防御中心上的 `admin` 帐户没有原始数据包访问权限的主机，或未运行 IPv6 的主机）进行扫描，请选择 **TCP Connect Scan**。
- 要发送 ACK 数据包检查端口是否过滤，请选择 **TCP ACK Scan**。
- 要发送 ACK 数据包以检查端口是否被过滤以及确定端口已打开还是关闭，请选择 **TCP Window Scan**。
- 要使用 FIN/ACK 探针识别 BSD 派生的系统，请选择 **TCP Maimon Scan**。

步骤 7　或者，除了 TCP 端口，如果还要扫描 UDP 端口，请针对 **Scan for UDP ports** 选项选择 **On**。

提示　UDP 端口扫描比 TCP 端口扫描需要更多时间。要加快扫描速度，请保持禁用该选项。

步骤 8　如计划使用此补救响应违反关联策略的情况，请配置 **Use Port From Event** 选项：

- 选择 **On** 可扫描关联事件中的端口，而不是第 11 步指定的端口。

  如果扫描关联事件中的端口，请注意补救扫描的是第 5 步指定的 IP 地址的端口。这些端口也将添加至补救的动态扫描目标。
- 选择 **Off** 可仅扫描第 11 步指定的端口。

步骤 9　如果计划使用此补救响应关联策略违反事件，并希望使用运行检测引擎来检测事件的设备运行扫描，请配置 **Scan from reporting detection engine** 选项：

- 要从运行报告检测引擎的设备进行扫描，请选择 **On**。
- 要从在补救中配置的设备进行扫描，请选择 **Off**。

步骤 10　配置 **Fast Port Scan** 选项：

- 要仅扫描 `nmap-services` 文件中列出的端口，而忽略其他端口设置，请选择 **On**，该文件可在扫描设置上的 `/var/sf/nmap/share/nmap/nmap-services` 目录中找到。
- 要扫描所有 TCP 端口，请选择 **Off**。

步骤 11　在 **Port Ranges and Scan Order** 字段中，键入要在默认情况下使用 Nmap 语法按自己想要的顺序扫描的端口。

指定值为 1 到 65535。端口间用逗号或空格分隔。还可使用连字符指明端口范围。扫描 TCP 和 UDP 端口时，以 T 作为要扫描的 TCP 端口列表的开端，以 U 作为 UDP 端口列表的开端。例如，要扫描 UDP 流量的端口 53 和 111，然后扫描 TCP 流量的端口 21-25，请输 入`U:53,111,T:21-25`。

请注意，启动补救以响应关联策略违反事件时，如第 8 步中所述，**Use Port From Event** 选项将覆盖此设置。

步骤 12　要探测开放端口以了解服务器厂商和版本信息，请配置 **Probe open ports for vendor and version information**：

- 选择 **On**，扫描主机上的开放端口以获取服务器信息，识别服务器厂商和版本。
- 选择 **Off**，继续使用主机的思科服务器信息。

步骤 13　如果选择探测开放端口，请从 **Service Version Intensity** 下拉列表中选择一个数字，设置使用的探针数量：

- 要使用更多探针进行更精确、更长久的扫描，请选择一个较大的数字。
- 要使用更少探针进行不太精确、更加快速的扫描，请选择一个较小的数字。

步骤 14　要扫描操作系统信息，请配置 **Detect Operating System** 设置：

- 选择 **On** 可扫描主机信息以确定操作系统。
- 选择 **Off**，继续使用主机的思科操作系统信息。

步骤 15　要确定主机发现是否发生，是否仅针对可用端口运行端口扫描，请配置 **Treat All Hosts As Online**：

- 要跳过主机发现过程并对目标范围内每个主机运行端口扫描，请选择 **On**。
- 要使用 **Host Discovery Method** 和 **Host Discovery Port List** 的设置执行主机发现，并跳过对所有不可用主机的端口扫描，选择 **Off**。

步骤 16 选择希望 Nmap 在测试主机可用性时使用的方法：

- 要发送设置了 SYN 标记的空 TCP 数据包，在已关闭端口上引发 RST 响应，或者在可用主机的开放端口上引发 SYN/ACK 响应，请选择 **TCP SYN**。

  请注意，此选项在默认情况下扫描端口 80，TCP SYN 扫描不太可能被设有状态性防火墙规则的防火墙拦截。

- 要发送设置了 ACK 标记的空 TCP 数据包，在可用主机上引发 RST 响应，请选择 **TCP ACK** 。

  请注意，该选项在默认情况下扫描端口 80， TCP ACK 扫描不太可能被防火墙通过状态性防火墙规则阻止。

- 要发送 UDP 数据包，从可用主机的关闭端口引发端口不可达响应，请选择 **UDP**。默认情况下，该选项扫描端口 40125。

步骤 17 如果要在主机发现过程中扫描自定义端口列表，请在 **Host Discovery Port List** 字段中键入适合已选择的主机发现方法的端口列表，用逗号隔开。

步骤 18 配置 **Default NSE Scripts** 选项，控制是否使用默认 Nmap 脚本集进行主机发现以及服务器、操作系统和漏洞发现：

- 要运行默认 Nmap 脚本集，请选择 **On**。
- 要跳过默认 Nmap 脚本集，请选择 **Off**。

有关默认脚本列表，请参阅 http://nmap.org/nsedoc/categories/default.html。

步骤 19 要为扫描过程设置定时，选择定时模板编号；如需进行更快、不太全面的扫描，选择较大的编号，如需进行更慢、更全面的扫描，选择较小的编号。

步骤 20 依次点击 **Save** 和 **Done**。

补救创建成功。

管理 Nmap 扫描

许可证：FireSIGHT

可按需修改或删除 Nmap 扫描实例和补救。还可运行按需 Nmap 扫描。还可查看或下载先前扫描的 Nmap 结果。有关详细信息，请参阅以下各节：

- 第 47-12 页上的管理 Nmap 扫描实例
- 第 47-14 页上的管理 Nmap 补救
- 第 47-15 页上的运行按需 Nmap 扫描

管理 Nmap 扫描实例

许可证：FireSIGHT

可编辑或删除 Nmap 扫描实例。有关详细信息，请参阅以下各节：

- 第 47-13 页上的编辑 Nmap 扫描实例
- 第 47-13 页上的删除 Nmap 扫描实例

编辑 Nmap 扫描实例

许可证：FireSIGHT

遵循以下步骤修改扫描实例。请注意，修改扫描实例时，可查看、添加和删除与该实例相关联的补救。

要编辑扫描实例，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Scanners**。

系统将显示 Scanners 页面。

步骤 2　在要编辑的实例旁，点击 **View**。

系统将显示 Instance Detail 页面。

步骤 3　或者，在要查看或编辑的补救旁，点击 **View**。

有关编辑补救的详细信息，请参阅第 47-14 页上的编辑 Nmap 补救。

步骤 4　或者，在要删除的补救旁，点击 **Delete**。

有关删除补救的详细信息，请参阅第 47-14 页上的删除 Nmap 补救。

步骤 5　或者，点击 **Add**，将新补救添加至此扫描实例。

有关创建新补救的详细信息，请参阅第 47-14 页上的管理 Nmap 补救。

步骤 6　或者，更改扫描实例设置，然后点击 **Save**。

步骤 7　点击 **Done**。

扫描实例修改成功。

删除 Nmap 扫描实例

许可证：FireSIGHT

不再想使用 Nmap 扫描实例中描述的 Nmap 模块时，请删除该 Nmap 扫描实例。请注意，如果删除扫描实例，也将删除使用该实例的任何补救。

要删除扫描实例，请执行以下操作：

访问：管理员/发现管理员

步骤 1　点击 **Policies > Actions > Scanners**。

系统将显示 Scanners 页面。

步骤 2　在要删除的扫描实例旁，点击 **Delete**。

实例删除成功。

管理 Nmap 补救

许可证：FireSIGHT

可编辑或删除 Nmap 补救。有关详细信息，请参阅以下各节：

编辑 Nmap 补救

许可证：FireSIGHT

对 Nmap 补救所做的更改不会影响正在进行的扫描。新设置将在下一次扫描开始时生效。

要编辑 Nmap 补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Scanners**。

系统将显示 Scanners 页面。

步骤 2　在要编辑的补救旁，点击 **View**。

系统将显示 Remediation Edit 页面。

步骤 3　按需进行修改。

有关可更改的设置的信息，请参阅第 47-10 页上的创建 Nmap 补救。

步骤 4　依次点击 **Save** 和 **Done**。

补救修改成功。

删除 Nmap 补救

许可证：FireSIGHT

删除不再需要的 Nmap 补救。

要删除 Nmap 补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Scanners**。

系统将显示 Scanners 页面。

步骤 2　在要删除的补救旁，点击 **Delete**。

步骤 3　确认要删除补救。

补救删除成功。

运行按需 Nmap 扫描

许可证：FireSIGHT

可在需要时启动按需 Namp 扫描。可指定按需扫描目标，只需输入要扫描的 IP 地址和端口，或者选择现有扫描目标。

请注意， Nmap 提供的服务器和操作系统数据将保持不变，直至运行另一个 Nmap 扫描。如果计划使用 Nmap 扫描主机，可能要设置定期扫描，随时更新 Nmap 提供的任何操作系统和服务器数据。有关详细信息，请参阅第 62-5 页上的自动运行 Nmap 扫描。另请注意，如从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。

要运行按需 Nmap 扫描，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Scanners**。

系统将显示 Scanners 页面。

步骤 2　在要用于执行扫描的 Nmap 补救旁，点击 **Scan**。

系统将显示 Nmap Scan Target 对话框。

步骤 3　或者，要使用已保存的扫描目标进行扫描，请从 **Saved Targets** 下拉列表中选择目标，点击 **Load**。

与扫描目标关联的 IP 地址和端口填充 **IP Range(s)** 和 **Ports** 字段。

提示　要创建扫描目标，请点击 **Edit/Add Targets**。有关详细信息，请参阅第 47-8 页上的创建 Nmap 扫描目标。

步骤 4　在 **IP Range(s)** 字段中，为要扫描的主机指定 IP 地址，或修改已加载的列表，最多不超过 255 个字符。

对于带 IPv4 地址的主机，可指定多个 IP 地址，用逗号隔开，或者使用 CIDR 表示法。也可在 IP 地址前面添加感叹号 (!)，否定 IP 地址。有关在 FireSIGHT 系统中使用 CIDR 表示法的信息，请参阅第 1-16 页上的 IP 地址约定。

对于带 IPv6 地址的主机，请使用精确的 IP 地址。不支持地址范围。

步骤 5　在 **Ports** 字段中，指定要扫描的端口或修改已加载的列表。

可输入一个端口号、用逗号隔开的端口列表或者用连接号隔开的端口号范围。有关输入端口的详细信息，请参阅第 60-7 页上的在搜索中指定端口。

步骤 6　点击 **Scan Now**。

Nmap 服务器执行扫描。

请注意，Nmap 将验证 IP 地址范围，如果 IP 地址范围无效，将显示一条错误消息。如果出现这种情况，请纠正 **IP Range(s)** 字段中的内容，指明有效的 IP 地址范围。

管理扫描目标

许可证：FireSIGHT

配置 Nmap 模块时，可创建和保存扫描目标，识别想在执行按需或预定扫描时作为扫描目标的主机和端口，从而避免每次构建新扫描目标。扫描目标包括一个或一组要扫描的 IP 地址，以及一台或多台主机上的端口。对于 Nmap 目标，也可使用 Nmap 八位字节范围寻址或 IP 地址范围。有关 Nmap 八位字节范围寻址的详细信息，请登录 http://insecure.org，参阅 Nmap 文档。

请注意，扫描包含大量主机的扫描目标可能需要较长的时间。作为一种解决方法，每次仅扫描几台主机。

创建扫描目标后，可以修改或删除它。

有关详细信息，请参阅以下各节：

- 第 47-8 页上的创建 Nmap 扫描目标
- 第 47-16 页上的编辑扫描目标
- 第 47-17 页上的删除扫描目标

编辑扫描目标

许可证：FireSIGHT

可修改已创建的扫描目标。

提示 如果不想使用补救扫描特定 IP 地址，但是该 IP 地址已添加至目标，则可能想编辑补救的动态扫描目标，因为主机参与了启动补救的关联策略违反事件。

要编辑现有扫描目标，请执行以下操作：

访问：管理员/发现管理员

步骤 1 选择 **Policies > Actions > Scanners**。

系统将显示 Scanners 页面。

步骤 2 在工具栏上，点击 **Targets**。

系统将显示 Scan Target List 页面。

步骤 3 在要编辑的扫描目标旁，点击 **Edit**。

系统将显示 Scan Target 页面。

步骤 4 根据需要进行修改并点击 **Save**。

扫描目标更新成功。

删除扫描目标

许可证：FireSIGHT

如果不再想扫描已在扫描目标中列出的主机，请删除扫描目标。

要删除扫描目标，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Scanners**。

系统将显示 Scanners 页面。

步骤 2　在工具栏上，点击 **Targets**。

系统将显示 Scan Target List 页面。

步骤 3　在要删除的扫描目标旁，点击 **Delete**。

扫描目标删除成功。

处理主动扫描结果

许可证：FireSIGHT

有关以下信息：如何监控正在进行的 Nmap 扫描，导入之前通过 FireSIGHT 系统执行的扫描的结果或在 FireSIGHT 系统外面执行的扫描的结果，以及查看和分析扫描结果的信息，请参阅：

- 第 47-17 页上的查看扫描结果
- 第 47-19 页上的了解扫描结果表
- 第 47-19 页上的分析扫描结果
- 第 47-19 页上的监控扫描
- 第 47-20 页上的导入扫描结果
- 第 47-21 页上的搜索扫描结果

查看扫描结果

许可证：FireSIGHT

可查看扫描结果表，然后根据正在查找的信息处理事件视图。

访问扫描结果时看到的页面因使用的工作流程而异。可使用预定义的工作流程，其中包括扫描结果表视图。

您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关创建自定义工作流程的信息，请参阅第 58-34 页上的创建自定义工作流程。

下表描述了一些可在扫描结果工作流程页面执行的特定操作。

表 47-2　扫描结果表功能

要.....	您可以.....
了解有关表中各列的更多信息	在第 47-19 页上的了解扫描结果表中获得详细信息。
修改扫描结果的时间和日期范围	点击时间范围链接。有关详细信息，请参阅第 58-19 页上的设置事件时间限制。
对扫描结果进行排序	点击列标题。再次点击列标题以反转排列顺序。
约束显示的列数	在要隐藏的列标题中点击关闭图标 (✖)。在显示的弹出窗口中，点击 **Apply**。 **提示**　要隐藏或显示其他列，选择或清除相应的复选框，然后点击 **Apply**。要将已禁用的列重新添加至视图， 点击展开箭头 ( )，展开搜索约束，然后点击 **Disabled Columns** 下的列名称。
向下钻取到工作流程中的下一页，限制特定值	可使用以下其中一种方法： • 在自定义工作流程中创建的向下展开页面上，点击某行内的一个值。请注意，点击表视图行中的值可限制表视图，且不会向下钻取到下一页。 • 要向下钻取到限制某些用户的下一个工作流程页面，在要在下一个工作流程页面上查看的用户旁，选择复选框，然后点击 **View**。 • 要向下钻取到保留当前限制的下一工作流程页面，请点击 **View All**。 **提示**　表视图的页面名称中始终包括“Table View”。 有关详细信息，请参阅第 58-26 页上的限制事件。
配置扫描实例和补救	点击工具栏中的 **Scanners**。 有关详细信息，请参阅第 47-7 页上的设置 Nmap 扫描。
在工作流程页面之内及在各工作流程页面之间导航	在第 58-16 页上的使用工作流程页面中获得详细信息。
导航至其他事件视图查看相关事件	想从 **Jump to** 下拉列表查看的事件视图的名称。有关详细信息，请参阅第 58-31 页上的在工作流程之间导航。
搜索扫描结果	点击 **Search**。有关详细信息，请参阅第 47-21 页上的搜索扫描结果。

要查看扫描结果，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Scanners**。

步骤 2　点击 **Scan Results**。

系统将显示默认扫描结果工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请按工作流程标题点击 **(switch workflows)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

了解扫描结果表

许可证：FireSIGHT

运行 Nmap 扫描时，防御中心 在数据库中收集扫描结果。下表描述了扫描结果表中的字段。

表 47-3　　扫描结果字段

字段	说明
开始时间	生成结果的扫描的开始日期和时间。
结束时间	生成结果的扫描的结束日期和时间。
Scan Target	生成结果的扫描的扫描目标的 IP 地址 （或主机名，如果 DNS 解析已启用）。
Scan Type	要么是 Nmap，要么是第三方扫描仪的名称，指明生成结果的扫描的类型。
Scan Mode	生成结果的扫描的模式： • On Demand - 来自按需扫描的结果。 • Imported - 来自不同系统上扫描的结果，已导入 防御中心。 • Scheduled - 来自作为预定任务运行的扫描的结果。

分析扫描结果

许可证：FireSIGHT

可查看作为弹出窗口中渲染页面的扫描结果 （使用本地 Nmap 模块创建）。也可下载原始 XML 格式的 Nmap 结果文件。

还可在主机配置文件和网络映射中查看由 Nmap 检测到的操作系统和服务器信息。如果主机扫描为已过滤或已关闭端口上的服务器生成服务器信息，或者如果扫描收集无法包含在操作系统信息或服务器部分中的信息，主机配置文件会将这些结果纳入 Nmap Scan Results 部分。有关详细信息，请参阅第 49-4 页上的查看主机配置文件。

监控扫描

许可证：FireSIGHT

可查看 Nmap 扫描的进度，以及取消当前正在进行的扫描作业。扫描结果提供每次扫描的开始时间和结束时间。此外，扫描完成后，也可查看作为弹出窗口中渲染页面的扫描结果。可在 http://insecure.org 上下载 Nmap 结果，并使用 Nmap 1.01 DTD 查看。还可清除扫描结果。

要监控扫描，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Scanners**。

步骤 2　点击 **Scan Results**。

系统将显示默认扫描结果工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请按工作流程标题点击 **(switch workflows)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

提示　如在使用的自定义工作流程不包括扫描结果表视图，请按工作流程标题点击 **(switch workflows)**，然后后选择 **Scan Results**。

步骤 3　可执行以下操作：

- 要查看作为弹出窗口中渲染页面的扫描结果，请在扫描作业旁点击 **View**。
- 要保存扫描结果文件的副本，以便在任何文本编辑器中查看原始 XML 代码，请在扫描作业旁点击 **Download**。

导入扫描结果

许可证：FireSIGHT

可导入在 FireSIGHT 系统外面执行的 Nmap 扫描创建的 XML 结果文件。也可导入之前从 FireSIGHT 系统下载的 XML 结果文件。要导入 Nmap 扫描结果，结果文件必须采用 XML 格式，且兼容于 Nmap 1.01 DTD。有关创建 Nmap 结果和 Nmap DTD 的更多信息，请登录 http://insecure.org，参阅 Nmap 文档。有关从 FireSIGHT 系统下载 XML 结果的信息，请参阅第 47-19 页上的监控扫描。

注意，只有网络映射中存在主机， Nmap 才能将其结果附加至主机配置文件。

要导入结果，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Scanners**。

系统将显示 Scan Instances 页面。

步骤 2　在工具栏上，点击 **Import Results**。

系统将显示 Import Results 页面。

步骤 3　点击 **Browse**，导航至结果文件。

步骤 4　返回 Import Results 页面后，点击 **Import**，导入结果。

结果文件导入成功。

搜索扫描结果

许可证：FireSIGHT

可搜索在 FireSIGHT 系统中设备或受管设备上运行的任何扫描的 Nmap 或第三方扫描结果。

表 47-4　　扫描结果搜索条件

字段	搜索条件规则
开始时间	键入生成结果的扫描的开始日期和时间。 有关时间输入语法，请参阅第 60-5 页上的在搜索中指定时间约束。
结束时间	键入生成结果的扫描的结束日期和时间。 有关时间输入语法，请参阅第 60-5 页上的在搜索中指定时间约束。
Scan Target	键入生成结果的扫描的扫描目标的 IP 地址 （或主机名，如果 DNS 解析已启用）。 使用特定 IP 地址或 CIDR 表示法指定 IP 地址范围。有关允许用于 IP 地址的语法的详细说明，请参阅第 60-6 页上的在搜索中指定 IP 地址。
Scan Type	键入 `Nmap` 或第三方扫描仪 ID，指明生成结果的扫描的类型。
Scan Mode	键入生成结果的扫描的模式： • 键入 `On Demand`，检索按需运行扫描的结果。 • 键入 `Imported`，检索在不同系统上运行并且已导入防御中心的扫描的结果。 • 键入 `Scheduled`，检索作为预定任务运行的扫描的结果。

有关搜索的详细信息，包括如何加载和删除已保存搜索，请参阅第 60-1 页上的搜索事件。

搜索扫描结果：

访问：管理员/发现管理员

步骤 1　选择 **Analysis > Search**，然后从表下拉列表选择 **Scan Results**。

系统将显示 Scan Results 搜索页面。

提示　要在数据库中搜索另一类型的事件，请从表下拉列表选择它。

步骤 2　在相应字段中输入搜索条件，如扫描结果搜索条件表中所述。

如果您为多个字段输入条件，搜索仅返回符合为所有字段指定的搜索条件的记录。

步骤 3　或者，但是，如果您计划保存搜索，可以选择 **Private** 复选框，将搜索保存为专用搜索，以便只有您可以访问该搜索。否则，请保持清除此复选框，为所有用户保存此搜索。

提示　如果要将搜索另存为对权限有限的自定义用户角色的约束，**必须**将其另存为私有搜索。

步骤 4　或者，您可以保存搜索以备将来使用。您有以下选项：

- 点击 **Save** 保存搜索条件。

  对于新的搜索，系统显示对话框，提示输入搜索名称；请输入一个唯一搜索名称并点击 **Save**。如果为先前存在的搜索保存新条件，则不会出现提示。已保存搜索（并且如果选择 **Private**，仅对您的帐户可见），以便以后运行。

- 点击 **Save as New** 保存新的搜索，或通过修改先前保存的搜索为已创建的搜索指定名称。

  系统显示对话框，提示输入搜索名称；请输入一个唯一搜索名称并点击 **Save**。已保存搜索（并且如果选择 **Private**，仅对您的帐户可见），以便以后运行。

步骤 5　点击 **Search** 开始搜索。

系统将显示搜索结果。

使用网络映射

FireSIGHT 系统被动收集通过网络传输的流量，解码数据，然后将其与既有的操作系统和指纹相比较。根据此信息，系统构建*网络映射*，它是网络的详细再现。

通过网络映射，可以使用防御中心从主机和网络设备 （网桥、路由器、 NAT 设备和负载均衡器）方面查看网络拓扑。它是用于快速全面了解网络的一种有用工具。通过网络映射，还可对关联的主机属性、应用、客户端、受损主机指示和漏洞进行向下钻取。换句话说，可以根据执行的分析选择不同的网络映射视图。

通过使用主机输入功能从第三方应用添加操作系统应用、客户端、协议或主机属性信息，可以扩增系统收集的信息。也可使用 Nmap 主动扫描网络映射中的主机，并将扫描结果添加至网络映射。

可以使用自定义拓扑功能帮助排列和识别网络映射视图中的子网。例如，如果贵公司中的每个部门使用不同的子网，则可使用自定义拓扑功能将熟悉的标签分配到这些子网。

有关详细信息，请参阅：

了解网络映射

许可证：FireSIGHT

网络映射的每个视图都有相同的格式：具有可扩展的类别和子类别的分层树。点击类别时，该类别展开显示其下方的子类别。可以根据执行的分析类型选择不同的网络映射视图。

防御中心从应用了发现策略的所有安全区域收集数据 （包括从支持 NetFlow 的设备处理数据的区域）。如果多台设备检测同一网络资产，防御中心会将信息合并成资产的合成再现。

虽然可以配置网络发现策略以添加由支持 NetFlow 的设备导出的数据，但是有关这些主机的可用信息有限。例如，这些主机没有可用的操作系统数据，除非您使用主机输入功能提供这些数据。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

从任何网络映射中，可查看任何主机的*主机配置文件*，此文件全面概括系统收集的有关该主机的所有信息。主机配置文件包含一般信息（如主机名，操作系统和所有关联的 IP 地址）以及更多特定信息（包括检测的协议、应用、危害表现和主机上运行的客户端）。主机配置文件还包括有关与主机及其检测的资产关联的漏洞的信息。有关主机配置文件的详细信息，请参阅第 49-1 页上的使用主机配置文件。

如果对于调查某项不再感兴趣，可以从网络映射中将其删除。可从网络映射中删除主机和应用；也可以删除或停用漏洞。如果系统检测到与已删除主机关联的活动，则会将该主机重新添加至网络映射。同样，如果系统检测到应用发生更改（例如，如果 Apache 网络服务器升级至最新版本），则会将已删除应用重新添加至应用网络映射。如果系统检测到使主机易受攻击的更改，则表明在特定主机上重新激活了漏洞。

也可使用网络映射在全网停用漏洞，意味着将系统判定为易受攻击的这些主机视为可安全防御该特定攻击或利用。

提示　如果要从网络映射永久排除主机或子网，请修改网络发现策略。您可能希望从监控中排除负载均衡器和 NAT 设备。它们可能会创建过量并有误导性的事件，从而填充数据库并使防御中心过载。有关详情，请参见第 45-2 页上的了解主机数据收集。

使用主机网络映射

许可证：FireSIGHT

使用主机网络映射查看网络上按分层树中子网排列的主机，以及向下钻取到特定主机的主机配置文件。此网络映射视图提供系统检测到的所有唯一主机的计数，无论主机有一个 IP 地址还是多个 IP 地址。

虽然可配置网络发现策略以根据由支持 NetFlow 的设备导出的数据将主机添加至网络映射，但是有关这些主机的可用信息有限。例如，除非使用主机输入功能提供操作系统数据，否则没有可用于使用 NetFlow 数据添加至网络映射的主机的操作系统数据。

通过为网络创建自定义拓扑，可向主机网络映射中显示的子网分配有意义的标签，例如，部门名称。

也可根据在自定义拓扑中指定的公司查看主机网络映射；请参阅第 48-8 页上的使用自定义网络拓扑。

可从主机网络映射中删除整个网络、子网或个别主机。例如，如果知道主机不再连接到网络，即可从网络映射中将其删除以简化分析。如果系统此后检测到与已删除主机关联的活动，则会将该主机重新添加至网络映射。如果要从网络映射永久排除主机或子网，请修改网络发现策略。有关详情，请参见第 45-19 页上的创建网络发现策略。

注　思科**强烈建议不要**从网络映射中删除网络设备，因为系统使用其位置确定网络拓扑（包括为受监控主机生成网络跃点和 TTL 值）。虽然无法从网络设备网络映射中删除网络设备，请确保勿从主机网络映射中将其删除。

要查看主机网络映射，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Network Map**，然后选择 **Hosts** 选项卡。

系统将显示主机网络映射，其中显示主机计数以及主机 IP 地址和 MAC 地址的列表。每个地址或部分地址都是一条指向下一级的链接。

步骤 2　向下钻取到要调查的主机的特定 IP 地址或 MAC 地址。

例如，要查看 IP 地址为 192.168.40.11 的主机，请依次点击 **192**、**192.168**、**192.168.40**、**192.168.40.11**。点击 **192.168.40.11** 时，系统将显示主机配置文件。有关主机配置文件的详细信息，请参阅第 49-1 页上的使用主机配置文件。

要按 IP 地址或 MAC 地址过滤，请在搜索字段中键入地址。要清除搜索，请点击清除图标 ( )。

步骤 3　或者，要删除子网、IP 地址或 MAC 地址，请点击要删除的元素旁边的删除图标 ( )，然后确认要删除主机还是子网。

主机删除成功。如果系统重新发现主机，则会将该主机添加至网络映射。

步骤 4　或者，在主机网络映射的主机视图和拓扑视图之间切换：

- 要切换至按自定义拓扑排列的主机网络映射的视图，在主机视图 （默认）上，请点击网络映射顶部的 **（拓扑）**。
- 要切换至按子网排列的主机网络映射的视图，在拓扑视图上，请点击网络映射顶部的 **（主机）**。

有关配置自定义拓扑的信息，请参阅第 48-8 页上的使用自定义网络拓扑。

使用网络设备网络映射

许可证：FireSIGHT

使用网络设备网络映射查看将一段网络连接到另一段网络的网络设备 （网桥、路由器、 NAT 设备和负载均衡器），以及向下钻取至这些网络设备的主机配置文件。网络设备网络映射分为两个部分：IP 和 MAC。 IP 部分列出通过 IP 地址识别的网络设备；Mac 部分列出通过 MAC 地址识别的网络设备。此网络映射视图也提供系统检测到的所有唯一设备的计数，无论设备有一个 IP 地址还是多个 IP 地址。

如果为网络创建自定义拓扑，则网络设备网络映射中会显示分配给子网的标签。

系统用于区分网络设备的方法包括：

- 分析思科发现协议 (CDP) 消息，可识别网络设备及其类型 （仅限思科设备）
- 检测生成树协议 (STP)，可识别作为交换机或网桥的设备
- 检测使用同一 MAC 地址的多台主机，可用于识别 MAC 地址为属于路由器
- 检测客户端 TTL 值的变化或变化频率高于典型启动时间的 TTL 值，可用于识别 NAT 设备和负载均衡器

如果网络设备使用 CDP 进行通信，则其可能有一个或多个 IP 地址。如果它使用 STP 进行通信，则它可能仅有 MAC 地址。

不能从网络映射中删除网络设备，因为系统使用其位置确定网络拓扑 （包括为受监控主机生成网络跃点和 TTL 值）。

网络设备的主机配置文件具有 System 部分而不是 Operating Systems 部分，其中包括反映网络设备后检测到的任何移动设备的硬件平台的 Hardware 列。如果 Systems 下列出硬件平台值，该系统是网络设备后检测出的一个或多个移动设备。请注意，移动设备可能有，也可能没有硬件平台信息，但不会检测到非移动设备系统的硬件平台信息。

要查看网络设备网络映射，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Network Map > Network Devices**。

系统将显示网络设备网络映射，其中显示唯一网络设备的计数以及网络设备 IP 地址和 MAC 地址的列表。每个地址或部分地址都是指向下一级地址或指向个别主机的主机配置文件的链接。

步骤 2　向下钻取至要调查的网络设备的特定 IP 地址或 MAC 地址。

系统将显示网络设备的主机配置文件。有关主机配置文件的详细信息，请参阅第 49-1 页上的使用主机配置文件。

步骤 3　或者，要按 IP 地址或 MAC 地址过滤，请在搜索字段中键入地址。要清除搜索，请点击清除图标 (✖)。

使用危害表现网络映射

许可证：FireSIGHT

使用危害表现 (IOC) 网络映射查看网络上按 IOC 类别排列的受损主机。受影响主机列在每个类别下方。

系统使用来自多个源的数据确定主机的受损状态，包括入侵事件、安全情报和 FireAMP。

从危害表现网络映射中，可查看通过特定方式确定为已受损的每个主机的主机配置文件。也可删除 （标记为已解析）任何 IOC 类别或任何特定主机，这会从相关主机中移除 IOC 标记。例如，如已确定问题得到解决且不可能复发，即可从网络映射中删除 IOC 类别。

标记从网络映射解析的主机或 IOC 类别不会将其从网络中移除。如果系统最近检测到触发该 IOC 的信息，则网络映射中会重新显示已解析的主机或 IOC 类别。

要查看危害表现网络映射，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Network Map > Indications of Compromise**。

系统将显示危害表现网络映射。

步骤 2　点击要调查的特定 IOC 类别。

例如，如要查看检测到恶意软件的主机，请点击 **Malware Detected**。

要按 IP 地址或 MAC 地址过滤，请在搜索字段中键入地址。要清除搜索，请点击清除图标 (✖)。

步骤 3　向下钻取至选定 IOC 类别下方的特定 IP 地址。每个地址或部分地址都是一条指向下一级的链接。

系统将显示受损主机的主机配置文件，其中危害表现部分已展开。有关主机配置文件的 IOC 部分的详细信息，请参阅第 49-7 页上的使用主机配置文件中的危害表现。

步骤 4　或者，要标记任何 IOC 类别、受损主机或已解析的受损主机组，请点击要解析的元素旁边的删除图标 ( )，然后确认要对其进行解析。

类别或主机解析成功 （IOC 标记已移除）。如果再次触发 IOC，则会将其重新添加至网络映射。

使用移动设备网络映射

许可证：FireSIGHT

使用移动设备网络映射查看连接至网络的移动设备，并且向下钻取至这些设备的主机配置文件。此网络映射视图也提供系统检测到的所有唯一移动设备的计数，无论设备有一个 IP 地址还是多个 IP 地址。

系统可用下列方法区分移动设备：

- 分析来自移动设备的移动浏览器的 HTTP 流量中的用户代理字符串
- 监控特定移动应用的 HTTP 流量

如为网络创建自定义拓扑，则移动设备网络映射中会显示分配给子网的标签。

要查看移动设备网络映射，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Network Map**，然后选择 **Mobile Devices** 选项卡。

系统将显示移动设备网络映射，其中显示唯一移动设备的计数和移动设备 IP 地址列表。每个地址或部分地址都是一条指向下一级的链接。

步骤 2　向下钻取至要调查的移动设备的特定 IP 地址。

例如，要查看 IP 地址为10.11.40.11 的设备，请依次点击 **10**、**10.11**、**10.11.40**、**10.11.40.11**。点击 **10.11.40.11** 时，系统将显示主机配置文件。有关主机配置文件的详细信息，请参阅第 49-1 页上的使用主机配置文件。

要按 IP 地址或 MAC 地址过滤，请在搜索字段中键入地址。要清除搜索，请点击清除图标 ( )。

步骤 3　或者，要删除子网、或 IP 地址，请点击要删除的元素旁边的删除图标 ( )，然后确认要删除设备或子网。

设备删除成功。如果系统重新发现设备，则会将该设备重新添加至网络映射。

使用应用网络映射

许可证：FireSIGHT

使用应用网络映射查看网络上在分层树中按应用名称、厂商、版本并最终按运行每个应用的主机排列的应用。

系统检测至的应用可能随系统软件和 VDB 更新而变化，并且在导入任何附加探测器的情况下也会变化。每个系统或 VDB 更新的版本说明或咨询文本均包含有关任何新的和已更新的探测器的信息。有关探测器的全面最新列表，请参阅以下支持站点之一：

- **Sourcefire：**(https://support.sourcefire.com/)
- **思科：**(http://www.cisco.com/cisco/web/support/index.html)

从应用网络映射，可查看运行特定应用的每个主机的主机配置文件，以及删除任何应用类别、在所有主机上运行的任何应用或在特定主机上运行的任何应用。例如，如果知道应用在主机上已禁用并要确保系统不使用它进行影响级别限定，即可从网络映射中删除该应用。

从网络映射中删除应用不会将其从网络中移除。如果系统检测到应用发生变化 （例如，如果 Apache 网络服务器升级到新版本），或者如果重新启动系统的发现功能，则网络映射中会重新显示已删除的应用。

视乎删除的内容，行为有所不同：

- 如果删除应用类别，则会将该应用类别从网络映射中移除。驻留在该类别下的所有应用都会从包含应用的任何主机配置文件中移除。

  例如，如果删除 **http**，则会从所有主机配置文件中移除标识为 **http** 的所有应用，并且网络映射的应用视图中不再显示 **http**。

- 如果删除特定应用、厂商或版本，则会从网络映射中以及从包含该网络映射的任何主机配置文件中移除受影响应用。

  例如，如果展开 **http** 类别并删除 **Apache**，则会从包含列为 Apache 的所有应用 （具有 Apache 下列出的任何版本）的任何主机配置文件中移除这些应用。同样，如果删除特定版本 （例如 **1.3.17**）而不是删除 **Apache**，则仅会将所选版本从受影响主机配置文件中删除。

- 如果删除特定 IP 地址，则会从应用列表中移除该 IP 地址，并从所选 IP 地址的主机配置文件中移除应用本身。

  例如，如果展开 **http**、 **Apache**、 **1.3.17 (Win32)**，然后删除 **172.16.1.50:80/tcp**，则会从 IP 地址 172.16.1.50 的主机配置文件中删除 Apache 1.3.17 (Win32) 应用。

要查看应用网络映射，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Network Map > Applications**。

系统将显示应用网络映射。

步骤 2　向下钻取至要调查的特定应用。

例如，要查看特定类型的 网络服务器 （如 Apache），请点击 **http**，再点击 **Apache**，然后点击要查看的 Apache 网络服务器的版本。

要按 IP 地址或 MAC 地址过滤，请在搜索字段中键入地址。要清除搜索，请点击清除图标 (✖)。

步骤 3　点击选定应用下方的特定 IP 地址。

系统将显示运行应用的主机的主机配置文件，其中应用部分已展开。有关主机配置文件的应用部分的详细信息，请参阅第 49-13 页上的使用主机配置文件中的服务器。

步骤 4　或者，要删除任何应用类别、在所有主机上运行的任何应用或在特定主机上运行的任何应用，请点击要删除的元素旁边的删除图标 ( )，然后确认要将其删除。

应用删除成功。如果系统重新发现应用程序，则会将其重新添加至网络映射。

使用漏洞网络映射

许可证：FireSIGHT

使用漏洞网络映射查看系统在网络上检测到的按旧版漏洞 ID (SVID)、 Bugtraq ID、 CVE ID 或 Snort ID 排列的漏洞。漏洞按标识号排列，并且每个漏洞下会列出受影响主机。

从漏洞网络映射中，可查看特定漏洞的详细信息；还可查看易受特定漏洞攻击的任何主机的主机配置文件。这有助于评估该漏洞对特定受影响主机造成的威胁。

如果认为特定漏洞不适用于网络上的主机（例如，已应用修补程序），则可停用漏洞。已停用的漏洞仍显示在网络映射中，但是其先前受影响主机的 IP 地址以灰色斜体显示。这些主机的主机配置文件将已停用的漏洞显示为无效，不过可以手动将其标记为对于个别主机有效；有关详细信息，请参阅第 49-26 页上的设置单个主机的漏洞。

如果主机上的应用或操作系统存在身份冲突，则系统会列出两种潜在身份的漏洞。解决身份冲突后，漏洞保持与当前身份关联。有关详细信息，请参阅第 46-4 页上的了解当前标识和第 46-5 页上的了解标识冲突。

默认情况下，仅当数据包包含应用的厂商和版本时，漏洞网络映射才会显示检测到的应用的漏洞。但是，可将系统配置列出缺少厂商和版本数据的应用的漏洞，只需在系统策略中为应用启用漏洞映射设置。有关为应用设置漏洞映射的信息，请参阅第 63-27 页上的映射服务器的漏洞。

漏洞 ID（或漏洞 ID 的范围）旁边的数字表示两个计数：

- 第一个数字是受漏洞影响的非唯一主机的计数。如果主机受多个漏洞影响，则会多次对其进行计数。因此，计数可能高于网络上的主机数。停用漏洞会按可能受该漏洞影响的主机数减小此计数。如果尚未面向漏洞或漏洞范围停用任何潜在受影响主机的任何漏洞，则不显示此计数。
- 第二个数字是系统已确定为*潜在*受漏洞影响的非唯一主机的总数的类似计数。

停用漏洞致使其仅对指定的主机处于非活动状态。可停用已判定为易受攻击的所有主机或指定的个别易受攻击主机的漏洞。如果系统随后在主机上检测到未尚未停用的漏洞（例如，在网络映射中的新主机上），则系统会激活该主机的漏洞。必须明确停用最近发现的漏洞。此外，如果系统检测到主机的操作系统或应用变化，则可能重新激活关联的已停用漏洞。

要查看漏洞网络映射，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Network Map > Vulnerabilities**。

系统将显示漏洞网络映射。

步骤 2　从 **Type** 下拉列表，选择要查看的漏洞的等级。默认情况下，漏洞按旧版漏洞 ID (SVID) 显示。

步骤 3　向下钻取至要调查的特定漏洞。

要按 IP 地址或 MAC 地址过滤，请在搜索字段中键入地址。要清除搜索，请点击清除图标 (✖)。

系统将显示漏洞详细信息。有关所提供的信息的详情，请参阅第 49-24 页上的查看漏洞细节。

此外，在网络映射中，防御中心显示受影响主机的 IP 地址。可以点击任何 IP 地址以显示该主机的主机配置文件。

步骤 4　或者，停用漏洞：

- 要停用受漏洞影响的所有主机的漏洞，请点击漏洞编号旁边的删除图标 ( )。
- 要停止个别主机的漏洞，请点击主机 IP 地址旁边的删除图标 ( )。

漏洞停用成功。适用的主机 IP 地址在网络映射中以灰色斜体显示。此外，这些主机的主机配置文件将已停用的漏洞显示为无效。

提示　有关重新激活漏洞的详细信息，请参阅第 49-26 页上的设置单个主机的漏洞。

处理主机属性网络映射

许可证：FireSIGHT

使用主机属性网络映射查看网络上按其主机属性排列的主机。选择要用于排列主机的主机属性时，防御中心列出该属性在网络映射中的可能值并根据主机的分配值将主机分组。还可查看为其分配了特定主机属性值的任何主机的主机配置文件。

主机属性网络映射可以根据用户定义的主机属性排列主机。对于任何这些属性，网络映射显示不将值作为 Unassigned 分配的主机。

有关详细信息，请参阅第 49-27 页上的使用用户定义的主机属性。

此外，主机属性网络映射可以根据对应于已创建的任何合规性白名单的主机属性排列主机。所创建的每个合规性白名单会创建与白名单具有相同名称的主机属性。

可能的白名单主机属性值为：

- `Compliant`，适用于符合白名单的主机
- `Non-Compliant`，适用于不符合白名单的主机
- `Not Evaluated`，适用于不是白名单的有效目标或因任何原因尚未评估的主机

有关合规性白名单的详细信息，请参阅第 52-1 页上的将 FireSIGHT 系统用作一个合规工具。

注　不能在主机属性网络映射中使用预定义主机属性 （如主机关键程度）排列主机。

要查看主机属性网络映射，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Network Map > Host Attributes**。

系统将显示主机属性网络映射。

步骤 2　从 **Attribute** 下拉列表，选择主机属性。

防御中心列出主机属性的值，并用括号指明已为其分配该值的主机的数量。

要按 IP 地址或 MAC 地址过滤，请在搜索字段中键入地址。要清除搜索，请点击清除图标 (✖)。

步骤 3　点击任何主机属性值以查看为其分配了值的主机。

步骤 4　点击主机 IP 地址以查看该主机的主机配置文件。

使用自定义网络拓扑

许可证：FireSIGHT

使用自定义拓扑功能帮助排列和识别主机及网络设备网络映射中的子网。

例如，如果贵公司中的每个部门使用不同的子网，则可使用自定义拓扑功能标示这些子网。然后，在查看主机或网络设备网络映射时，会显示分配给子网的标签，如下图中所示。

也可根据在自定义拓扑中指定的公司查看主机网络映射。

有关主机和网络设备网络映射的详细信息，请参阅第 48-2 页上的使用主机网络映射和第 48-3 页上的使用网络设备网络映射。

有关详细信息，请参阅：

- 第 48-9 页上的创建自定义拓扑
- 第 48-13 页上的管理自定义拓扑

创建自定义拓扑

许可证：FireSIGHT

要创建自定义拓扑，必须指定其网络。可使用任何或所有三种策略执行此操作：

- 通过导入思科发现的拓扑，这会使用根据系统检测到的主机和网络设备对网络部署方式的“最佳猜测”添加网络
- 通过从网络发现策略导入网络，这会添加将 FireSIGHT 系统配置为在网络发现策略中监控的网络
- 通过手动向拓扑中添加网络，前提是其他两种方法创建不准确或不完整的部署再现

必须先保存并激活拓扑，然后再将其与网络映射组合使用。

要创建自定义拓扑，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Network Discovery**，然后点击 **Custom Topology**。

系统将显示 Custom Topology 页面。

步骤 2　点击 **Create Topology**。

系统将显示 Create Topology 页面。

步骤 3　提供基本拓扑信息，如拓扑名称和描述。

请参阅第 48-10 页上的提供基本拓扑信息。

步骤 4　向拓扑添加网络。可使用以下任何或所有策略：

- 要通过导入思科发现的拓扑向拓扑添加网络，请遵循第 48-11 页上的导入发现的拓扑中所述的操作步骤。
- 要通过从网络发现策略导入网络向拓扑添加网络，请遵循第 48-11 页上的从网络发现策略导入网络中所述的操作步骤。
- 要手动向拓扑添加网络，请遵循第 48-12 页上的手动向自定义拓扑添加网络中所述的操作步骤。

步骤 5　优化拓扑：

- 要从自定义拓扑移除网络，点击要移除的网络旁边的 **Delete**。
- 要重命名网络，请点击网络旁边的 **Rename**。在显示的弹出窗口中，在 **Name** 字段中键入新名称并点击 **Rename**。此名称标示网络映射中的网络。

步骤 6　点击 **Save**。

拓扑保存成功。

注　必须先激活拓扑，然后才能在网络映射中对其进行使用。有关详细信息，请参阅第 48-13 页上的管理自定义拓扑。

提供基本拓扑信息

许可证：FireSIGHT

必须为每个自定义拓扑提供名称，并或者提供简短描述。

要提供基本拓扑信息，请执行以下操作：

访问：管理

步骤 1　在 Edit Topology 页面上的 **Name** 字段中，键入拓扑的名称。

步骤 2　或者，在 **Description** 字段中，键入拓扑的描述。

步骤 3　或者，视乎想要如何构建自定义拓扑，继续执行以下各节中的操作步骤：

- 第 48-11 页上的导入发现的拓扑
- 第 48-11 页上的从网络发现策略导入网络
- 第 48-12 页上的手动向自定义拓扑添加网络

导入发现的拓扑

许可证：FireSIGHT

可将网络添加至自定义拓扑的一种方法是导入 FireSIGHT 系统发现的拓扑。此发现的拓扑是系统根据其检测到的主机和网络设备对网络部署方式的“最佳猜测”。

要导入发现的拓扑，请执行以下操作：

访问：管理

步骤 1　在 Edit Topology 页面上，点击 **Import Discovered Topology**。

步骤 2　发现的网络填充该页面。

步骤 3　或者，视乎想要如何构建自定义拓扑，继续执行以下各节中的操作步骤：

- 第 48-11 页上的导入发现的拓扑
- 第 48-11 页上的从网络发现策略导入网络
- 第 48-12 页上的手动向自定义拓扑添加网络

从网络发现策略导入网络

许可证：FireSIGHT

可将网络添加至自定义拓扑的一种方法是导入将 FireSIGHT 系统配置为在网络发现策略中监控的网络；请参阅第 45-19 页上的创建网络发现策略。

要从网络发现策略导入网络，请执行以下操作：

访问：管理

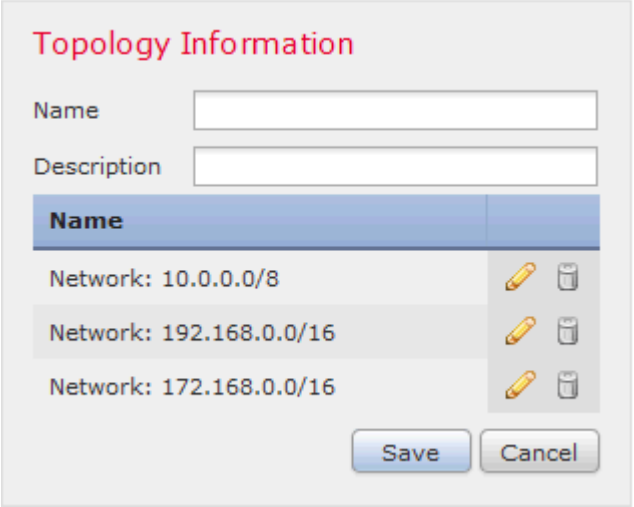
步骤 1　在 Edit Topology 页面上，点击 **Import Policy Networks**。

系统将显示一个弹出窗口。

步骤 2　从下拉列表，选择要使用的网络发现策略并点击 **Load**。

步骤 3　网络发现策略中的受监控网络填充该页面。

例如，如将网络发现策略配置为监控 10.0.0.0/8、 192.168.0.0/16 和 172.12.0.0/16 网络，则页面中会显示这些网络。



步骤 4　要从其他网络发现策略添加网络，请重复第 1 步和第 2 步。

步骤 5　或者，视乎想要如何构建自定义拓扑，遵循以下各节中的操作步骤：

- 第 48-11 页上的导入发现的拓扑
- 第 48-12 页上的手动向自定义拓扑添加网络

手动向自定义拓扑添加网络

许可证：FireSIGHT

如果导入思科发现的拓扑并从网络发现策略导入网络会创建不准确或不完整的网络部署再现，则可手动向自定义拓扑添加网络。

要向自定义拓扑手动添加网络，请执行以下操作：

访问：管理

步骤 1　在 Edit Topology 页面上，点击 **Add Network**。

系统将显示一个弹出窗口。

步骤 2　或者，通过在 **Name** 字段中键入名称来命名网络。

激活拓扑后，此名称标示主机和网络设备网络映射中的网络。

有关详细信息，请参阅第 48-2 页上的使用主机网络映射和第 48-3 页上的使用网络设备网络映射。

步骤 3　在 **IP Address** 和 **Netmask** 字段中，输入表示要添加至拓扑的网络的 IP 地址和网络掩码（使用 CIDR 表示法）。

有关在 FireSIGHT 系统中使用 CIDR 表示法的信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 4　点击 **Add**。

系统将网络添加至拓扑。

步骤 5　要向拓扑添加其他网络，请重复第 1 步到第 4 步。

提示　要从拓扑删除网络，在要删除的网络旁，点击 **Delete**，然后确认要删除网络以及指向网络的所有链接。

步骤 6　或者，视乎想要如何构建自定义拓扑，遵循以下各节中的操作步骤：

- 第 48-11 页上的导入发现的拓扑
- 第 48-11 页上的从网络发现策略导入网络

管理自定义拓扑

许可证：FireSIGHT

使用 Custom Topology 页面管理自定义拓扑。可创建、修改和删除拓扑。

系统将显示拓扑的状态及其名称。如果策略名称旁边的灯泡图标亮起，表明拓扑处于活动状态并影响网络映射。如果该图标熄灭，表明拓扑处于非活动状态。只有一个自定义拓扑可以随时处于活动状态。如已创建多个拓扑，则激活一个拓扑会自动停用当前活动的拓扑。

遵循以下操作步骤激活或停用自定义拓扑、修改拓扑或删除拓扑。

如果删除活动拓扑，则更改立即生效；即，网络映射不再显示自定义拓扑。

要激活或停用自定义拓扑，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Network Discovery > Custom Topology**。

系统将显示 Custom Topology 页面。

步骤 2　此时您有两种选择：

- 要**激活**拓扑，请点击策略旁边的 **Activate**。
- 要**停用**拓扑，请点击策略旁边的 **Deactivate**。

要修改自定义拓扑，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Network Discovery > Custom Topology**。

系统将显示 Custom Topology 页面。

步骤 2　点击要编辑的拓扑旁边的编辑图标 ( )。

系统将显示 Edit Topology 页面。有关可更改的各种配置的信息，请参阅第 48-9 页上的创建自定义拓扑。

步骤 3　根据需要做出更改，然后点击 **Save**。

拓扑更改成功。如果拓扑处于活动状态，则已做出的更改在网络映射中立即生效。

要删除自定义拓扑，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Network Discovery > Custom Topology**。

系统将显示 Custom Topology 页面。

步骤 2　点击要删除的拓扑旁边的 **Delete**。如果拓扑处于活动状态，请确认要将其删除。

拓扑删除成功。

使用主机配置文件

主机配置文件可完整展现系统搜集到的有关单台主机的全部信息。通过主机配置文件，可获得主机名和操作系统等主机的一般信息。例如，可通过主机配置文件，快速找到主机的 MAC 地址。

配置文件还包含*主机属性*信息。主机属性指可应用于主机的用户定义的说明。例如，可指定能表明主机所在建筑物的主机属性。通过主机简档，您可以查看相关主机应用的现有主机属性，也可以修改主机属性的值。再如，可利用*主机重要性*属性指定特定主机的业务重要性，并根据主机重要性定制关联策略和警报。

此外，主机配置文件还包含与服务器、客户端和在特定主机运行的主机协议相关的信息，包括它们是否符合合规性白名单。可从服务器列表上删除服务器并查看那些服务器的详情。此外，还可查看服务器的*连接事件*，以及检测到服务器流量的会话的日志信息。此外，还可查看客户端详情和连接事件，以及从主机配置文件中删除服务器、客户端或主机协议。

如果 FireSIGHT 系统部署包括 FireSIGHT 许可证，可在主机配置文件中查看*危害表现* (IOC)。这些指示关系到与主机相关的各种数据 （入侵事件、安全情报、连接事件、及文件事件或恶意软件事件），以确定监控网络上的主机是否可能遭受恶意侵害。可在主机配置文件中查看主机的 IOC 标记，查看与 IOC 有关的事件，将 IOC 标记标记为已解决、并编辑发现策略中的 IOC 规则状态。

如果部署包括保护许可证，可定制系统处理流量的方式，以便其更好地适应主机上的操作系统的类型，以及主机正在运行的服务器和客户端。有关详细信息，请参阅第 30-1 页上的调整被动部署中的预处理。

此外，如果已经配置系统对主机进行跟踪，还可查看主机的用户历史信息。然后，用户在过去二十四小时的活动以图形方式显示。

可修改主机配置文件中的主机漏洞列表。可使用该功能跟踪主机中哪些漏洞已经修补。此外，还可利用修复程序来修补漏洞，并把已经修补的漏洞自动标记为无效。

可利用思科系统生成的漏洞信息，以及利用主机输入功能导入到防御中心上的第三方扫描仪检测到的漏洞信息。

或者，进行 Nmap 扫描以增加主机配置文件中有关服务器和操作系统的信息。 Nmap 扫描仪主动扫描主机以获得在主机上运行的操作系统和服务器的有关信息。扫描结果会添加到主机操作系统和服务器标识列表。

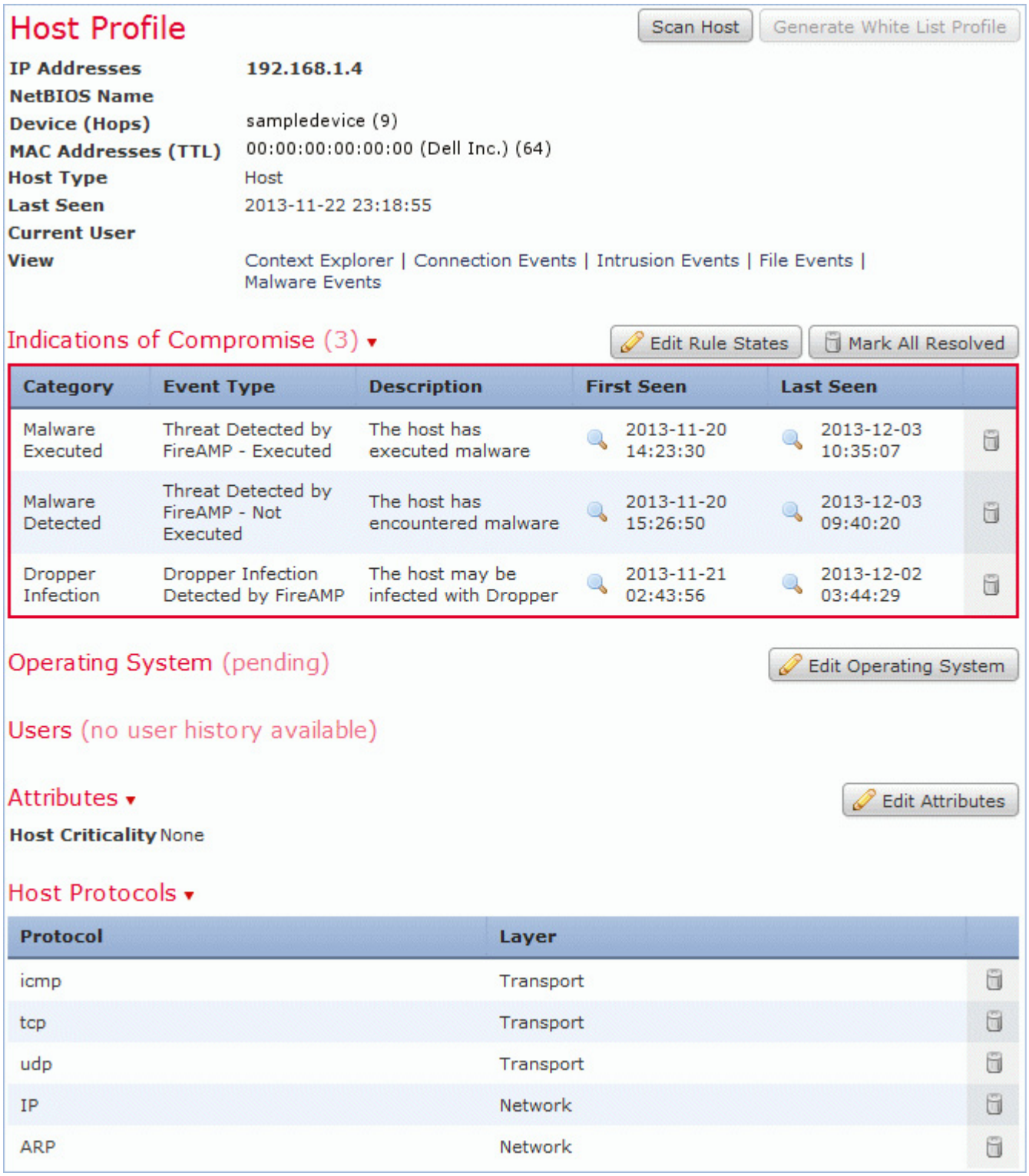
请注意，并非网络上的所有主机都可使用主机配置文件。可能的原因包括：

- 由于超时，主机已从网络映射删除
- 已达到 FireSIGHT 主机许可证限制
- 主机所在网段不受网络发现策略的监控

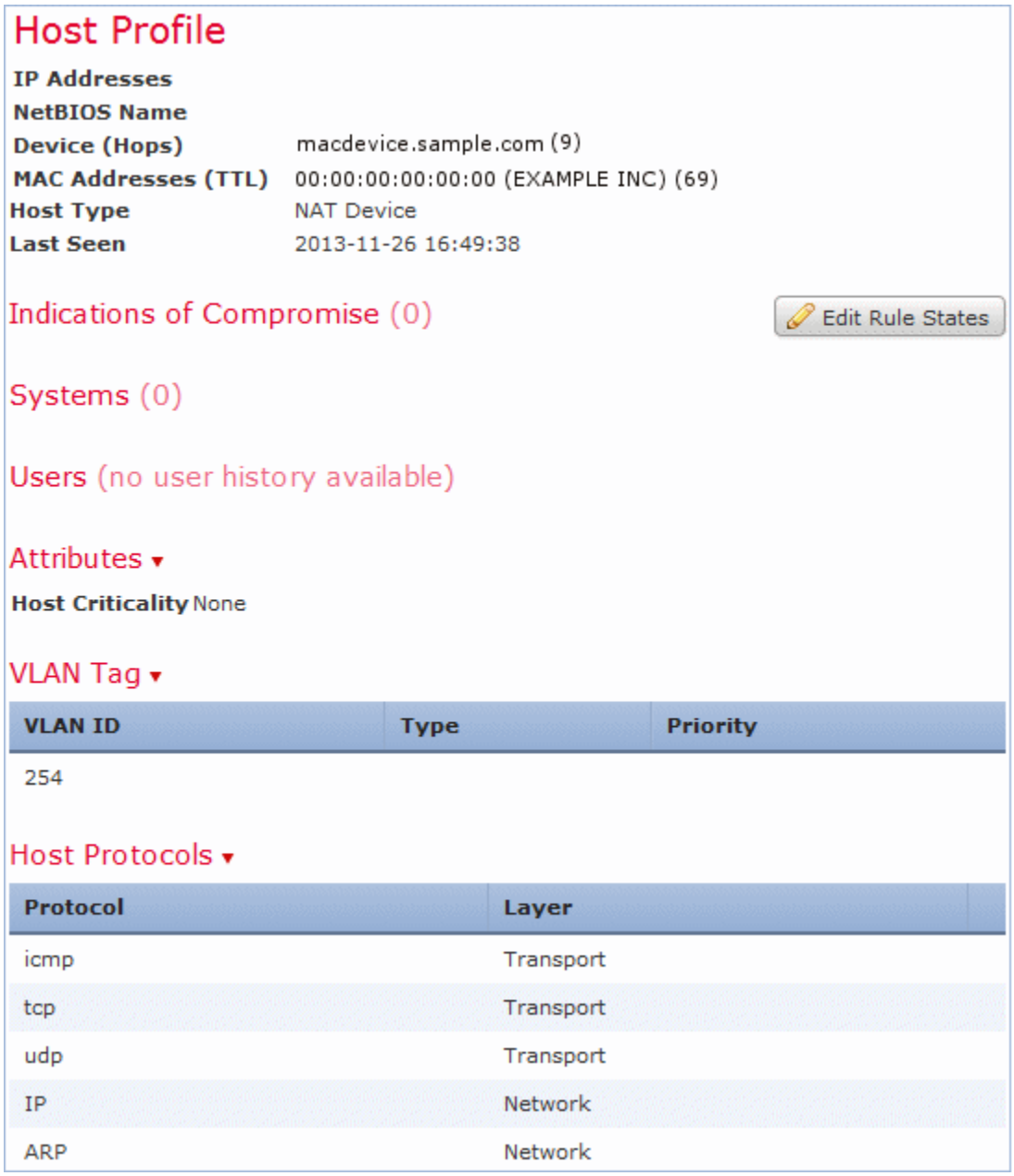
请注意，主机配置文件信息随主机类型和主机可用信息的不同而发生变化。例如，如果系统检测到使用非基于 IP 的协议 （比如 STP、 SNAP 或 IPX）的主机，系统会将主机作为 MAC 主机添加至网络映射，而且为主机提供的信息少于 IP 主机。

又如，尽管可根据由 NetFlow 驱动的装置导出的数据配置网络发现策略把主机、服务器和客户端添加至网络映射，但获得的有关这些主机、服务器和客户端的可用信息有限。例如，除非利用扫描仪或主机输入功能提供有关操作系统的数据，否则这些主机没有可用的操作系统数据。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

下图所示为主机配置文件的示例。



下图所示为 MAC 主机的主机配置文件的示例。



有关主机配置文件每个部分的详细信息，请参阅：

- 第 49-4 页上的查看主机配置文件说明如何访问主机配置文件。
- 第 49-5 页上的使用主机配置文件中的基本主机信息描述主机配置文件中 Host 部分的信息。
- 第 49-6 页上的使用主机配置文件中的 IP 地址描述主机配置文件中 IP Addresses 部分的信息。
- 第 49-7 页上的使用主机配置文件中的危害表现描述主机配置文件中 Indications of Compromise 部分的信息。
- 第 49-9 页上的使用主机配置文件中的操作系统描述主机配置文件中 Operating System 或 Operating System Conflicts 部分的信息并说明如何编辑操作系统或解决操作系统冲突。

- 第 49-13 页上的使用主机配置文件中的服务器描述主机配置文件中 Servers、 Server Detail 和 Server Banner 部分的信息。
- 第 49-17 页上的使用主机配置文件中的应用描述主机配置文件中 Clients 部分的信息。
- 第 49-19 页上的使用主机配置文件中的 VLAN 标签描述主机配置文件中 VLAN Tag 部分的信息。
- 第 49-19 页上的使用主机配置文件中的用户历史描述主机配置文件中 User History 部分的信息。
- 第 49-19 页上的使用主机配置文件中的主机属性描述主机配置文件中 Attributes 部分的信息。
- 第 49-27 页上的使用预先定义的主机属性说明如何设置主机重要性属性和如何添加主机配置文件注释。
- 第 49-27 页上的使用用户定义的主机属性提供创建和使用用户定义的主机属性的信息。
- 第 49-20 页上的使用主机配置文件中的主机协议描述主机配置文件中 Host Protocols 部分的信息。
- 第 49-21 页上的使用主机配置文件中的白名单违规描述主机配置文件中 White List Violations 部分的信息。
- 第 49-22 页上的使用主机配置文件中的恶意软件检测描述主机配置文件中 Most Recent Malware Detections 部分的信息。
- 第 49-23 页上的使用主机配置文件中的漏洞描述主机配置文件中 Vulnerabilities 和 Vulnerability Detail 部分的信息。

查看主机配置文件

许可证：FireSIGHT

可从任何包含监控网络上主机的 IP 地址的网络映射或事件视图访问主机配置文件。例如，在发现事件表视图的 IP Address 列中每个条目旁边，均包含一个至主机配置文件的链接。如果启动任何危害表现 (IOC) 规则，可能受到攻击的主机会显示不同的主机配置文件图标。

要从事件视图查看主机配置文件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在任何事件视图上，点击想要浏览的配置文件的主机 IP 地址旁边的主机配置文件图标 () 或受攻击的主机图标 ()。

主机配置文件在弹出窗口中显示。

要从网络映射查看主机配置文件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在任何网络映射上，钻取至想要浏览的配置文件的主机的 IP 地址。

系统将显示该主机配置文件。有关如何从网络映射访问主机配置文件的示例，请参阅第 48-2 页上的使用主机网络映射。

使用主机配置文件中的基本主机信息

许可证：FireSIGHT

主机配置文件包含有关检测到的主机或其他设备的基本信息。

主机配置文件中的每个基本字段的描述如下。

IP 地址

所有与主机相关的 IP 地址（IPv4 和 IPv6）。IPv6 主机通常至少有两个 IPv6 地址（仅本地和全局路由），也可能拥有 IPv4 地址。纯 IPv4 主机可拥有多个 IPv4 地址。如可用，路由主机 IP 地址还包含一个表明与地址相关的地理位置数据的旗帜图标和国家代码。有关该方面和其他地理位置功能的详细信息，请参阅第 58-17 页上的使用地理定位。

主机名

如果已知，为主机的完全限定域名。

NetBIOS Name

如可用，为主机的 NetBIOS 名称。为使用 NetBIOS 而配置的 Microsoft Windows 主机、以及 Macintosh、Linux 或其他平台都可以拥有一个 NetBIOS 名称。例如，配置为 Samba 服务器的 Linux 主机可拥有多个 NetBIOS 名称。

Device (Hops)

存在以下其中一种情况：

- 根据网络发现策略中的定义，主机所在网络的报告设备，或者
- 处理把主机添加至网络映射的 NetFlow 数据的设备
- 设备以及检测到主机的设备与设备名称后面括号里的主机之间的网络跳数。如果多台设备可看见主机，报告设备以粗体显示。
- 如果此字段为空，则以下两项任选一项：
- 按照网络发现策略中的规定，由未明确监控主机所在网络的设备将该主机添加到网络映射中，或
- 使用主机输入功能添加主机，并且未被 FireSIGHT 系统检测到

MAC Addresses (TTL)

主机被检测到的 MAC 地址或多个地址和相关 NIC 供应商，括号中为 NIC 硬件供应商和当前生存时间 (TTL) 值。如果 MAC 地址以粗体显示，则 MAC 地址是系统通过 ARP 和 DHCP 流量检测到的主机的实际 MAC 地址。如果有多台设备检测到主机，不管是哪台设备报告的地址，防御中心都会显示与主机相关的所有 MAC 地址和 TTL 值。

可点击 MAC 地址查看具有同样 MAC 地址的主机列表。通常，路由器主机配置文件在该列表中显示路经的网络分段中的主机 （IP 地址），以及频繁出现的监控路由器的 IP 地址 （针对监控工作站和服务器）。 MAC 地址的真实 IP 地址以粗体显示。

Host Type

系统检测到的设备类型：主机、移动设备、越狱的移动设备、路由器、网桥、 NAT 设备或负载均衡器。

系统用于区分网络设备的方法包括：

- 分析思科发现协议 (CDP) 消息，可识别网络设备及其类型 （仅限思科设备）
- 检测生成树协议 (STP)，可识别作为交换机或网桥的设备

- 检测使用同一 MAC 地址的多台主机，可用于识别 MAC 地址为属于路由器
- 检测客户端 TTL 值的变化或变化频率高于典型启动时间的 TTL 值，可用于识别 NAT 设备和负载均衡器
- 系统可用下列方法区分移动设备：
- 分析来自移动设备的移动浏览器的 HTTP 流量中的用户代理字符串
- 监控特定移动应用的 HTTP 流量

如果一种设备未被确定为网络设备或移动设备，该设备将归类为主机。

Last Seen

最后一次检测主机的 IP 地址的日期和时间。

Current User

最近一次登录该主机的用户。

请注意，只有当现有当前用户不是授权用户时，登录主机的非授权用户才注册为当前用户。有关详细信息，请参阅第 45-6 页上的用户数据库。

View

事件数据视图链接，使用该事件类型的默认工作流并仅限于显示与主机相关的事件；如果可能，这些事件包括与主机相关的所有 IP 地址。有关详细信息，请参阅：

- Content Explorer - 有关详细信息，请参阅第 56-1 页上的使用 Context Explorer。
- Connection Events - 有关详细信息，请参阅第 39-2 页上的了解连接和安全情报数据。
- Connection Events - 有关详细信息，请参阅第 50-1 页上的使用发现事件。
- Malware Events - 有关详细信息，请参阅第 40-14 页上的使用恶意软件事件。
- Intrusion Events by Source - 有关详细信息，请参阅第 41-1 页上的处理入侵事件。
- Intrusion Events by Destination - 有关详细信息，请参阅第 41-1 页上的处理入侵事件。

使用主机配置文件中的 IP 地址

许可证：FireSIGHT

系统检测与主机相关的 IP 地址，并且，如果支持的话，把同一主机使用的多个 IP 地址进行分组。 IPv6 主机通常拥有至少两个 IPv6 地址：仅本地和全局路由。 IPv6 主机还可有一个或多个分配的 IPv4 地址。纯 IPv4 主机可拥有多个 IPv4 地址。

主机配置文件列出所有检测到的与主机相关的 IP 地址。如果可用， IP 地址还有一个代表相关国家的小旗帜图标和 ISO 国家代码。有关地理位置的进一步详细信息，可点击旗帜图标或国家代码。有关详细信息，请参阅第 58-17 页上的使用地理定位。

请注意，默认情况下，仅显示前三个地址。点击 **show all** 显示主机的所有地址。

使用主机配置文件中的危害表现

许可证：FireSIGHT

FireSIGHT 系统可关联与主机相关的各种数据 （入侵事件、安全情报、连接事件和文件事件或恶意软件事件），以确定监控网络上的主机是否可能会受到恶意侵害。事件数据的某些组合和频率触发了受影响主机上的危害表现 (IOC) 标记。主机配置文件中 Indications of Compromise 部分显示了所有主机的 IOC 标记。在本节，可查看主机面临的威胁的详细情况，跳至可触发 IOC 标记的事件，编辑 IOC 规则状态、以及解决不再相关的 IOC 标记。

要使用 IOC 功能，您必须先激活该功能以及发现策略中的至少一条 IOC 规则。此外，还可在主机的配置文件页面上编辑该主机的 IOC 规则状态。每条 IOC 规则对应一种类型的 IOC 标记；根据公司需求，可激活任何一条或全部规则。有关发现策略中 IOC 的详细信息和整体信息，请参阅第 45-17 页上的了解危害表现。

除了主机配置文件中包含 IOC 数据外，还可以在事件查看器中对 IOC 数据进行分析。有关详细信息，请参阅第 50-28 页上的使用危害表现。

主机配置文件显示的 IOC 信息字段的说明如下。

IP地址

与触发 IOC 的主机关联的 IP 地址。

类别

所指示危害类型的简要说明，例如 `Malware Executed` 或 `Impact 1 Attack`。

事件类型

与特定危害表现 (IOC) 关联的标识符，指触发该标识的事件。

说明

说明可能受攻击的主机面临的威胁情况，比如 `This host may be under remote control` 或 `Malware has been executed on this host`。

First/Last Seen

触发主机 IOC 的事件的第一次出现 （或最近）日期和时间。

有关使用主机配置文件中的 IOC 数据的详细信息，请参阅以下各节：

- 第 49-7 页上的编辑单台主机的危害表现规则状态
- 第 49-8 页上的查看危害表现源事件
- 第 49-9 页上的解决危害表现

编辑单台主机的危害表现规则状态

许可证：FireSIGHT

为使系统能够检测和标记危害表现 (IOC)，首先必须激活发现策略中的 IOC 功能并且激活至少一条 IOC 规则 （适用于整个策略或单个主机）。从主机配置文件，设置适用于单个主机的 IOC 规则状态。有关配置发现策略中的 IOC 和设置适用于整个策略 IOC 规则状态的详细信息，请参阅第 45-29 页上的设置危害表现规则。

从主机配置文件，可访问并利用 Indications of Compromise 部分的 **Edit Rule States** 编辑 IOC 规则列表。可根据网络和组织需要启用任何或全部规则。例如，如果使用诸如 Microsoft Excel 等软件的主机从未出现在监控网络上，可决定不启用与基于 Excel 的威胁相关的 IOC 。

所有 IOC 规则都经思科事先定义；尽管可根据触发的 IOC 标记编写合规性规则，但不得创建原始规则。有关详细信息，请参阅第 51-1 页上的配置关联策略和规则。每条 IOC 规则仅由一种类型的事件 （比如恶意软件或入侵）触发并对应一种特定的 IOC 标记。为方便对应，规则和标记的类别、事件类型和说明数据相同；IOC 规则状态的编辑页面还显示每条规则的事件数据源，以方便用户了解触发规则所需要的系统功能。

要编辑主机的危害表现规则状态，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在主机配置文件中，点击 **Indications of Compromise** 部分的 **Edit Rule States**。

系统将在新窗口中显示 Edit Indication of Compromise Rule States 页面。

步骤 2　在规则的 **Enabled** 列中，点击滑块启用或禁用规则。

步骤 3　点击 **Save**。

已保存您的更改。

查看危害表现源事件

许可证：FireSIGHT

您可利用危害表现部分快速导航至在主机上触发 IOC 标记的事件。通过分析这些事件，可获得信息，以确定是否需要采取措施解决可能受到攻击的主机面临的威胁以及采取什么措施。

点击 IOC 标记时间戳旁边的查看图标 ( ) 可导航至相关事件类型的事件表视图，仅显示触发 IOC 标记的事件。

有关触发 IOC 标记的事件类型和功能的详细信息，请参阅下列内容：

- 第 39-1 页上的使用连接与安全情报数据
- 第 41-1 页上的处理入侵事件
- 第 37-2 页上的了解恶意软件防护和文件控制

要查看危害表现标记的源事件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在主机配置文件的 **Indications of Compromise** 部分，点击想要调查的 IOC 标记的 **First Seen** 或 **Last Seen** 列中的查看图标 ( )。

系统将显示触发 IOC 的适当事件的事件表视图，但仅限于显示触发事件。如果您在一个单独的窗口中查看主机配置文件，事件视图在主窗口中显示。

解决危害表现

许可证：FireSIGHT

在分析和处理完 IOC 标记显示的威胁后，或如果确定 IOC 标记代表误报，可将标记标记为已解决。将 IOC 标记标记为已经解决时，该标记会从主机配置文件中删除；当主机上的所有有源 IOC 标记都已解决，主机不再显示标有受攻击主机的图标 ()。请注意，对于已经解决的 IOC，仍然可查看 IOC 触发事件。

如果触发主机 IOC 标记的事件再次出现，重新设置该标记。您可解决主机上的单独 IOC 标记，或将主机上的所有标记标记为已解决。

要解决危害表现标记，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在主机配置文件的 **Indications of Compromise** 部分，您有两个选项：

- 要将单独的 IOC 标记标记为已解决，请点击要解决的标记右侧的解决图标 ( )。
- 要将主机上的所有 IOC 标记标记为已解决，请点击 **Mark All Resolved**。

系统保存更改，并删除所选的 IOC 标记。

使用主机配置文件中的操作系统

许可证：FireSIGHT

通过分析流量中主机生成的网络和应用堆栈或分析用户代理报告的主机数据，系统被动检测运行在主机上的操作系统的标识。此外，系统还将核对其他来源的操作系统信息，比如通过主机输入功能导入的 Nmap 扫描仪或应用数据。当确定将要使用的标识时，系统会考虑分配给每个标识源的优先级。默认情况下，用户输入的优先级最高，其次是应用或扫描仪源，最后是思科发现的标识。

有时候，系统会提供通用操作系统定义而非具体的定义，因为流量和其他标识源无法提供足够信息以确定更具针对性的标识。系统核对其他来源的信息，以尽可能利用最详细的定义。

主机配置文件中显示的操作系统信息字段说明如下。

Hardware

移动设备的硬件平台。

OS Vendor/Vendor

操作系统供应商。

OS Product/Product

根据从各种来源搜集到的标识数据确定的最可能运行在主机上的操作系统。

如果操作系统处于 `Pending` 状态，系统还未确定操作系统，没有其他可用的标识数据。如果操作系统处于 `unknown` 状态，系统无法确定操作系统，也没有可用的操作系统的其他标识数据。

如果主机的操作系统不是系统可以检测得到的系统，要使用下列任何一种策略：

- 根据第 46-6 页上的使用自定义指纹技术的描述，为主机创建自定义指纹
- 根据第 49-31 页上的扫描主机配置文件中的主机的描述，运行主机的 Nmap 扫描仪

- 按照《*FireSIGHT 系统主机输入 API 指南*》中的说明使用主机输入功能，将数据导入网络映射
- 根据第 49-9 页上的使用主机配置文件中的操作系统的描述，手动输入操作系统的信息

OS Version/Version

操作系统版本。如果主机属于越狱的移动设备，版本后面的圆括号里会标识 `Jailbroken`。

Source

选择以下值之一：

- 用户：*`user_name`*
- 应用：*`app_name`*
- 扫描仪：*`scanner_type`*（通过系统策略添加的 Nmap 或扫描仪）
- FireSIGHT

系统可能从多个源协调数据，以确定操作系统的标识；请参阅第 46-4 页上的了解当前标识。

因为主机漏洞列表以及以主机为目标的事件的事件影响相关性取决于操作系统，可能要手动提供更多具体的操作系统信息。此外，可标明已经应用到操作系统的修复，比如补丁包和更新，以及使修复已经解决的漏洞失效。

例如，如果系统确定主机的操作系统为 Microsoft Windows 2003，但主机实际上运行的是 Microsoft Windows XP Professional SP2，可相应地设置操作系统的标识。设置更具体的操作系统标识可以完善主机漏洞列表，以便该主机的影响相关性更具针对性、更准确。

如果系统检测到的主机操作系统信息与由活动源提供的现有操作系统标识相冲突，会发生标识冲突。当确实存在标识冲突时，系统同时使用漏洞标识和影响相关性。

尽管可根据启用了 NetFlow 的设备导出的数据配置网络发现策略，将主机添加至网络映射，但这些主机的操作系统数据仍然不可用，除非设置了操作系统标识。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

请注意，如果主机运行的操作系统违反了激活的网络发现策略中的合规性白名单，防御中心将为操作系统信息标记白名单违规图标 ( )。此外，如果越狱的移动设备违反有效的白名单，该图标会出现在该设备的操作系统旁边。

可以为主机的操作系统标识设置自定义显示字符串。上述自定义显示字符随后用于主机配置文件中。

注　请注意，改变主机的操作系统的信息可能会改变其符合合规性白名单的合规情况。

在网络设备的主机配置文件中，Operating Systems 一节的标签变为 Systems，并显示另外一个 Hardware 列。如果 Systems 下列出硬件平台值，该系统是网络设备后检测出的一个或多个移动设备。请注意，移动设备可能有，也可能没有硬件平台信息，但不会检测到非移动设备系统的硬件平台信息。

查看操作系统的标识

许可证：FireSIGHT

可查看发现的或添加的主机特定操作系统的标识。系统利用来源优先分级来确定主机当前的标识。在标识列表中，当前标识以粗体突出显示。

对于每个操作系统标识，主机配置文件可能包括第 49-9 页上的使用主机配置文件中的操作系统描述的信息。

请注意，只有当主机存在多个操作系统标识时， View 按钮才可用。

要查看主机的操作系统标识列表，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在主机配置文件的 **Operating System** 或 **Operating System Conflicts** 部分，点击 **View**。

系统将显示 Operating System Identity Information 弹出窗口。

提示　点击操作系统标识旁边的删除图标 ( )，从 Operating System Identity Information 弹出窗口中删除标识；如适用，更新主机配置文件中的操作系统的当前标识。请注意，由思科检测到的操作系统的标识不能删除。

编辑操作系统

许可证：FireSIGHT

可使用 FireSIGHT 系统的网络界面来设置主机当前操作系统的标识。在网络界面设置标识来覆盖所有其他标识源，以便把标识用于漏洞评估和影响相关性。但是，请注意，如果在编辑操作系统后，系统检测到主机存在相互冲突的操作系统标识，会发生操作系统冲突。

在解决冲突前，这两种操作系统都被视为当前操作系统。有关详细信息，请参阅第 49-12 页上的解决操作系统的标识冲突。

要更改操作系统标识，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在主机配置文件中，点击 **Operating System** 部分的 **Edit**。

此时将显示一个弹出窗口，您可以在该窗口中设置操作系统标识。

步骤 2　此时有多个选择：

- 选择 **OS Definition** 下拉列表中的 **Current Definition**，通过主机输入确认当前的操作系统标识，然后跳转至第 6 步。
- 从 **OS Definition** 下拉列表中选择当前操作系统的标识上的一个变体，然后跳转至第 6 步。
- 从 **OS Definition** 下拉列表选择 **User-Defined**，然后继续第 3 步。

步骤 3　或者，选择 **Use Custom Display String** 并修改要在 **Vendor String**、**Product String**、和 **Version String** 字段中要显示的自定义字符串。

步骤 4　或者，要更改为不同供应商提供的操作系统，请从 **Vendor** 和 **Product** 下拉列表选择供应商和其他操作系统详细信息。

步骤 5　或者，要配置操作系统的产品版本级别，请选择 **Major**、**Minor**、**Revision**、**Build**、**Patch** 和 **Extension** 下拉列表中的适用项目。

步骤 6　或者，如果要表示已经应用操作系统的修复程序，请点击 **Configure Fixes**。

显示可用修复程序包列表。

步骤 7　在下拉列表中选择适用的修复程序，并点击 **Add**。

步骤 8　或者，使用 **Patch** 和 **Extension** 下拉列表添加相关补丁和扩展。

步骤 9　点击 **Finish** 完成操作系统的标识配置。

解决操作系统的标识冲突

许可证：FireSIGHT

如果当前标识是由诸如扫描仪、应用或用户之类的活动源提供，当系统检测到的新标识与当前标识冲突时，会发生操作系统标识冲突。

冲突的操作系统标识列表在主机配置文件中以粗体显示。

可在系统网络界面解决标识冲突并设置主机当前的操作系统标识。在网络界面设置标识来覆盖所有其他标识源，以便把标识用于漏洞评估和影响相关性。

要使相互冲突的标识变为当前标识，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1 此时您有两种选择：

- 点击要设置为主机操作系统的操作系统标识旁边的 **Make Current**。
- 如果*不希望*作为当前标识的标识来自活动源，请删除不必要的标识。

要解决操作系统的标识冲突，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1 在主机配置文件中，点击 **Operating System Conflicts** 部分的 **Resolve**。

在可设置当前操作系统的标识处，系统将显示一个弹出窗口。

步骤 2 此时有多个选择：

- 选择 **OS Definition** 下拉列表中的 **Current Definition**，通过主机输入确认当前的操作系统标识，然后跳转至第 6 步。
- 从 **OS Definition** 下拉列表选择相互冲突的操作系统的标识上的一个变体，然后跳转至第 6 步。
- 从 **OS Definition** 下拉列表选择 **User-Defined**，然后继续第 3 步。

步骤 3 或者，选择 **Use Custom Display String** 并键入要在 **Vendor String**、**Product String**、和 **Version String** 字段中显示的自定义字符串。

步骤 4 或者，要更改为不同供应商的操作系统，请选择供应商和其他操作系统详细信息。

步骤 5 或者，要配置操作系统的产品版本级别，请选择 **Major**、**Minor**、**Revision**、**Build**、**Patch** 和 **Extension** 下拉列表中的适用项目。

步骤 6 或者，如果要表示已经应用操作系统的修复程序，请点击 **Configure Fixes**。

步骤 7 把已经应用的修复添加至修复列表。

步骤 8 点击 **Finish** 完成操作系统的标识配置并返回至主机配置文件。

使用主机配置文件中的服务器

许可证：FireSIGHT

如果系统检测到多个服务器在监控网络上的主机上运行或通过主机输入功能或扫描仪或其他活动源添加服务器，防御中心把这些服务器列入主机配置文件的服务器部分。

防御中心最多可为每台主机列出 100 台服务器。达到限制后，不管是源自活动源或被动源的新服务器信息都会被删除，直到您从主机上删除服务器或服务器超时。有关详细信息，请参阅第 45-11 页上的主机限制和发现事件日志记录。

如果使用 Nmap 扫描主机， Nmap 会把此前未检测到的在开放 TCP 端口运行的服务器的结果添加至服务器列表。如果在主机上进行 Nmap 扫描或导入 Nmap 结果，可展开的 Scan Results 部分内容也会出现在主机配置文件中，列出 Nmap 扫描工具在主机上检测到的服务器信息。有关详细信息，请参阅第 49-31 页上的使用主机配置文件的扫描结果和第 47-7 页上的设置 Nmap 扫描。此外，请注意，如果从网络映射中删掉主机，主机服务器的 Nmap 扫描结果会被丢弃。

注 尽管您可根据 NetFlow 启动的设备导出的数据配置网络发现策略，以把服务器和客户添加至网络映射，但有关这些应用的可用信息是有限的。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

使用主机配置文件中的服务器的流程取决于访问文件的方式：

- 如果通过服务器的网络映射访问主机配置文件，会出现该服务器的详细信息，粗体高亮该服务器的名称。如果要查看主机上的任何其他服务器的详细信息，请点击服务器名称旁边的查看图标 ( )。
- 如果以任何其他方式访问主机配置文件，展开服务器部分并点击要查看详细信息的服务器旁边的查看图标 ( )。

您也可以执行以下操作：

- 要分析与主机上特定服务器相关的连接事件，请点击该服务器旁边的事件图标。

  系统将显示连接事件首选工作流程的首页，该页面显示受服务器的端口和协议以及主机的 IP 地址限制的连接事件。如果连接事件没有首选工作流程，必须选择一个首选工作流程。有关连接数据的详细信息，请参阅第 39-1 页上的使用连接与安全情报数据。
- 要从主机配置文件中删除服务器，请点击服务器旁边的删除图标 ( )。

  服务器从主机配置文件删除，但是，如果系统再次检测到服务器的流量，服务器会再次出现。请注意，删除主机上的服务器可实现主机达到白名单的要求。
- 要解决服务器标识冲突，请点击服务器旁边的解决图标。

  可选择一个冲突的标识、选择这些标识中的一个的变体或设置一个新的用户定义的标识。
- 要编辑服务器标识，请点击服务器旁边的编辑图标 ( )。

  可选择当前的标识、选择该标识上的变体或设置一个新的用户定义的标识。

服务器列表中的列说明如下。

协议

服务器所用协议名称。

端口

运行服务器的端口。

Application Protocol

以下任一选项：

- 应用协议的名称
- `pending`，如果出于几种原因中的其中之一，系统无法准确地识别应用协议
- `unknown`，如果系统无法根据已知应用协议指纹识别应用协议或在没有添加相应服务器的情况下，通过主机输入功能添加具有端口信息的漏洞来添加服务器

将鼠标悬停在应用协议名称上，会显示标记。有关标记的信息，请参阅第 45-9 页上的了解应用检测：

Vendor and Version

由 FireSIGHT 系统、 Nmap、或其他活动源识别的或通过主机输入功能获得的供应商和版本。如果没有可用源提供任何识别信息，字段为空。

请注意，如果主机正在运行的是违反经激活的关联策略中的合规性白名单的服务器，防御中心利用白名单违规图标 () 来标记不符合规定的服务器。

有关详细信息，请参阅以下各节：

- 第 49-14 页上的服务器详细信息
- 第 49-16 页上的编辑服务器标识
- 第 49-16 页上的解决服务器标识冲突

服务器详细信息

许可证：FireSIGHT

防御中心列出的每个服务器的被动检测到的 （思科或 NetFlow 检测到的）标识最多可达 16。如果系统检测到多个供应商或服务器版本，该服务器可拥有多个被动标识。例如，如果网络服务器运行不同版本的服务器软件，受管设备和网络服务器场之间的负载均衡器会让系统识别多种 HTTP 被动标识。请注意，防御中心对源自活动源的服务器标识数量没有限制，例如，用户输入、扫描仪或其他应用。

防御中心以粗体显示当前的标识。系统可把服务器当前的标识用于各种用途，包括把漏洞分配给主机、影响评估、根据主机配置文件限制性条件和合规性白名单编写评估相关性规则等。

提示 有关修改服务器标识和解决服务器详细信息中的标识冲突的信息，请参阅读第 49-16 页上的编辑服务器标识和第 49-16 页上的解决服务器标识冲突。

服务器详细信息可显示与所选服务器相关的更新后的子服务器信息。最后，当您查看主机配置文件中的服务器时，服务器详细信息可在服务器详细信息下方显示服务器横幅。

服务器横幅提供服务器的额外信息，以帮助您识别服务器。当攻击者有意修改服务器横幅字符串时，系统无法识别或检测被错误识别的服务器。服务器横幅显示检测到的服务器的第一个数据包中的前 256 个字节。这类信息仅在系统第一次检测到服务器的时候收集，而且仅收集一次。横幅内容分两列列出，左侧以十六进制表示，右侧以相应的 ASCII 表示。

注 要查看服务器横幅，您必须启用网络发现策略中的 **Capture Banners** 复选框。默认情况下该选项处于禁用状态。

对服务器详细信息中的信息的说明如下。

协议

服务器所用协议名称。

端口

运行服务器的端口。

Hits

由思科受管设备或 Nmap 检测到的服务器的次数。请注意，除非系统检测到该服务器的流量，否则通过主机输入导入的服务器的命中次数为 0。

Last Used

最后一次检测到服务器的时间和日期。请注意，除非系统检测到该服务器有新的流量，否则主机输入数据的最后一次被使用的时间反映了初始数据导入时间。此外，还要注意，根据系统策略中的设置通过主机输入功能导入的扫描仪和应用数据会超时，但通过防御中心网络界面的用户输入不会超时。

Application Protocol

如果已知，服务器所用的应用协议的名称。

供应商

服务器供应商。如果供应商未知，不显示该字段。

版本

服务器版本。如果版本未知，不显示该字段。

信息来源

选择以下值之一：

- 用户：*user_name*
- 应用：*app_name*
- 扫描仪：*scanner_type*（通过系统策略添加的 Nmap 或扫描仪）
- 思科检测到的应用，FireSIGHT、FireSIGHT Port Match、或 FireSIGHTPattern Match
- 对于根据 NetFlow 数据添加至网络映射的服务器，为 NetFlow

系统可能从多个源协调数据，以确定服务器的标识；请参阅第 46-4 页上的了解当前标识。

要查看服务器的服务器详细信息，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击主机配置文件 **Servers** 中服务器旁边的查看图标 ( )。

系统将显示 Server Detail 弹出窗口。

编辑服务器标识

许可证：FireSIGHT

可手动更新主机上服务器的标识设置和配置已经应用到主机的任何修复，以删除经修复解决的漏洞。此外，还可以删除服务器标识。

请注意，删除标识不会删除服务器，即使该标识是唯一标识。删除标识会将标识从 Server Detail 弹出窗口移除，而且如果适用，更新主机配置文件中的服务器当前的标识。

不能编辑或删除由思科管理的设备添加的服务器标识。

要编辑服务器标识，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在主机配置文件的 **Servers** 部分，点击 **View**，打开 Server Detail 弹出窗口。

步骤 2　此时您有两种选择：

- 要删除服务器标识，请点击要移除的服务器标识旁边的删除图标 ( )。
- 要修改服务器标识，请点击服务器列表中的服务器旁边的编辑图标 ( )。

  系统将显示 Server Identity 弹出窗口。

步骤 3　此时您有两种选择：

- 从 **Select Server Type** 下拉列表中选择当前定义。
- 从 **Select Server Type** 下拉列表中选择服务器的类型。

步骤 4　或者，要只列出该类型服务器的供应商和产品，请选择 **Restrict by Server Type** 复选框。

步骤 5　或者，要自定义服务器的名称和版本，请选择 **Use Custom Display String** 并键入 **Vendor String** 和 **Version String**。

步骤 6　在 **Product Mappings** 中，选择要使用的操作系统、产品和版本。

例如，如果要把服务器映射至 Red Hat Linux 9，请选择 **Redhat, Inc.** 作为供应商，**Red Hat** Linux 作为产品，**9** 作为版本。

步骤 7　如果要表示已经应用操作系统的修复程序，请点击 **Configure Fixes**。否则，跳转至第 9 步。

系统将显示 Available Package Fixes 页面。

步骤 8　把想要应用到该服务器的补丁添加至修复列表。

步骤 9　点击 **Finish** 完成服务器的标识配置。

解决服务器标识冲突

许可证：FireSIGHT

当应用或扫描仪等活动源将服务器标识数据添加到主机上时，如果系统随后检测到该端口上出现表明冲突服务器标识的流量，则会出现服务器标识冲突。

要解决服务器标识冲突，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击 **Servers** 列表中的服务器旁边的解决图标。

系统将显示 Server Identity 弹出窗口。

步骤 2　从 **Select Server Type** 下拉列表中选择服务器的类型。

步骤 3　或者，要只列出该类型服务器的供应商和产品，请选择 **Restrict by Server Type** 复选框。

步骤 4　或者，要自定义服务器的名称和版本，请选择 **Use Custom Display String** 并键入 **Vendor String** 和 **Version String**。

步骤 5　在 **Product Mappings** 中，选择要使用的操作系统、产品和版本。

例如，如果要把服务器映射至 Red Hat Linux 9，请选择 **Redhat, Inc.** 作为供应商，**Red Hat** Linux 作为产品，**9** 作为版本。

步骤 6　如果要表示已经应用操作系统的修复程序，请点击 **Configure Fixes**。否则，跳转至第 9 步。

系统将显示 Available Package Fixes 页面。

步骤 7　把想要应用到该服务器的补丁添加至修复列表。

步骤 8　点击 **Finish** 完成服务器的标识配置并返回至主机配置文件。

使用主机配置文件中的应用

许可证：FireSIGHT

可在主机配置文件中查看在主机上运行的应用。如果想从主机配置文件中移除应用，您可删除该应用。

有关管理主机配置文件中的应用的详细信息，请参阅：

- 第 49-17 页上的查看主机配置文件中的应用
- 第 49-18 页上的删除主机配置文件上的应用

查看主机配置文件中的应用

许可证：FireSIGHT

系统可检测到在网络的主机上运行的各种客户端和网络应用。

注　请注意，为使系统可以检测监控网络中主机上的应用，您必须选择系统网络发现策略中的 NetFlow 设备的发现规则中的 **Applications** 复选框。默认情况下，该选项在 NetFlow 规则中启用，而且，对于受管设备发现所用的规则，该选项不能禁用。

主机配置文件包含在主机上检测到的应用的产品和版本、任何可用客户端或网络应用信息，以及上一次检测到使用应用的时间。

防御中心最多列出 16 个在主机上运行的客户端。在达到限制后，会丢弃来自主动或被动来源的新客户端信息，直到您从主机上删除客户端应用，或系统由于客户端闲置把客户端从主机配置文件中删除 （客户端超时）。

此外，对于每个检测到的网络浏览器，主机配置文件显示浏览器访问的前 100 个网络应用。在达到限制后，来自主动或被动源的与该浏览器相关的新的网络应用均会丢弃，直到出现下列任何一种情况：

- 网络浏览器客户端应用超时，或
- 从主机配置文件删除与网络应用相关的应用信息

在主机配置文件中显示的应用信息说明如下。

Application Protocol

显示应用 （HTTP 浏览器、 DNS 客户端等等）所使用的应用协议。

客户端

来源于负载的客户端信息，由 FireSIGHT 系统识别、或由 Nmap、或其他活动源捕获、或通过主机输入功能获得。如果没有可用源提供任何识别信息，字段为空。

版本

显示客户端版本。

Web 应用程序

对于网络浏览器，系统在 HTTP 流量中检测到的内容。网络应用信息表示由 FireSIGHT 系统识别、Nmap 或其他活动源捕获、或通过主机输入功能获得的特定类型的内容（例如，WMV 或 QuickTime）。如果没有可用源提供任何识别信息，字段为空。

请注意，如果主机正在运行违反了激活的关联策略中的合规性白名单的应用，防御中心利用白名单违规图标 ( ) 来标记不符合规定的应用。

要分析与主机上特定应用相关的连接事件，请点击该应用旁边的事件图标 ( )。系统将显示连接事件首选工作流程的首页，该页面显示受应用的类型、产品和版本，以及主机的 IP 地址限制的连接事件。如果连接事件没有首选工作流程，必须选择一个首选工作流程。有关连接数据的详细信息，请参阅第 39-1 页上的使用连接与安全情报数据。

删除主机配置文件上的应用

许可证：FireSIGHT

要移除已知的未在主机上运行的应用，您可从主机配置文件删除该应用。请注意，删除主机上的应用可让主机符合白名单。

注　如果系统再次检测到应用，系统会将该应用重新添加至网络映射和主机配置文件。

要从主机配置文件删除应用，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在主机配置文件的 **Applications** 部分，点击要删除的应用旁边的删除图标 ( )。

此时系统已删除该主机的应用。

使用主机配置文件中的 VLAN 标签

许可证：FireSIGHT

如果主机构成虚拟局域网 (VLAN) 的一部分，系统会显示主机配置文件的 VLAN Tag 部分。

物理网络设备通常使用 VLAN 从各种网络块创建逻辑网段。系统检测到 802.1q VLAN 标记并显示每个标记的下列信息：

- **VLAN ID** 标识主机所属的 VLAN。对于 802.1q VLAN，它可以是 0 至 4095 之间的任何一个整数。
- **Type** 标识包含 VLAN 标记的封装包，可以是以太网或令牌环。
- **Priority** 标识在 VLAN 标记中的优先级，可以是 0 至 7 之间的任何一个整数，其中 7 表示最高优先级。

如果 VLAN 标记嵌套在数据包中，系统进行处理，且防御中心显示最里面的 VLAN 标记。系统搜集其防御中心显示其通过 ARP 和 DHCP 流量确定的仅适于 MAC 地址的 VLAN 标记信息。

例如，在一个全部由打印机构成的 VLAN 中，并且系统在该 VLAN 中检测到 Microsoft Windows 2000 操作系统，VLAN 标记信息是有用的。此外，VLAN 信息帮助系统生成更准确的网络映射。

使用主机配置文件中的用户历史

许可证：FireSIGHT

主机配置文件中的用户历史部分图示了过去二十四个小时的用户活动。用户通常会在晚上注销，而且可能与其他用户分享主机资源。用正常的短条形表示定期登录请求，例如要查看邮件的登录请求。用户标识列表附带有条形图，表明检测到用户登录的时间。请注意，对于未授权的登录，条形图将灰显。

请注意，系统的确会将主机上未授权的用户登录与该主机的 IP 地址关联，因此，用户会显示在该主机的用户历史中。然而，如果检测到同一台主机的授权用户登录，则与授权用户登录相关的用户将沿用与主机 IP 地址的关联，而新的未授权用户登录不会破坏用户与主机 IP 地址的关联。有关用户类型的详细信息，请参阅第 45-6 页上的用户数据库。如果在网络发现策略中配置捕获失败的登录，列表包括登录主机失败的用户。

使用主机配置文件中的主机属性

许可证：FireSIGHT

可利用*主机属性*按照对网络环境而言重要的方式来对主机进行分门别类。主机属性值可以是正整数、字符串或 URL。此外，还可以创建字符串值列表并根据主机的 IP 地址自动分配字符串值。有关创建和管理用户定义的主机属性的详细信息，请参阅第 49-27 页上的使用用户定义的主机属性。

FireSIGHT 系统包含两个预先定义的主机属性：主机重要性和注释。有关使用这些预先定义的主机属性的详细信息，请参阅第 49-27 页上的使用预先定义的主机属性。

此外，创建的每个合规性白名单会自动创建与白名单名称相同的主机属性。可能的主机属性值包括 Compliant（用于符合白名单的主机）、Non-Compliant（用于违反白名单的主机）或 Not Evaluated（用于不是白名单有效目标或由于某种原因没有进行评估的主机）。**无法**手动更改白名单的主机属性值。有关白名单的详细信息，请参阅第 52-1 页上的将 FireSIGHT 系统用作一个合规工具。

分配主机的属性值

许可证：FireSIGHT

可将正整数、字符串或 URL 指定为现有主机属性值。

提示 可通过点击主机配置文件页面上的 **Attributes** 中的 **Edit** 链接快速为主机分配主机属性。将会弹出包含所有主机属性的字段的窗口。

要分配主机属性值，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1 打开主机配置文件。

步骤 2 在 **Attributes** 项下，点击要分配值的主机属性名称。

系统将显示一个弹出窗口。

步骤 3 输入属性值或从下拉列表中选择一个值。

步骤 4 点击 **Save**。

主机属性值保存成功。

使用主机配置文件中的主机协议

许可证：FireSIGHT

可通过主机配置文件查看在主机上运行的主机协议。如果必要，还可从主机配置文件中删除特定主机的主机协议。

每个主机配置文件都包含在网络流量中检测到的与主机关联的协议有关的信息。

协议和网络层信息说明如下。

Protocol

指主机使用的协议的名称。

层

指协议运行的网络层 （`Network` 或 `Transport`）。

请注意，如果主机正在运行的是违反已激活关联策略中的合规性白名单的协议，则防御中心用白名单违规图标 （防御中心）来标记不符协议。防御中心

要移除已知的未在主机上运行的协议，从主机配置文件中删除协议即可。请注意，从主机上删除协议可让主机符合合规性白名单。

注 如果系统再次检测到协议，系统会将该协议重新添加至网络映射和主机配置文件。

要从主机配置文件中删除协议，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在主机配置文件的 **Protocols** 部分，点击要删除的协议旁边的删除图标 ( )。

该主机上的协议删除成功。

使用主机配置文件中的白名单违规

许可证：FireSIGHT

合规性白名单（或*白名单*）指允许用户指定可在特定子网上运行的操作系统、应用协议、客户端、网络应用和协议的一系列标准。

如果在活动关联策略中添加白名单，系统检测到主机违反白名单时，防御中心会将白名单事件（一种特殊类型的关联活动）记入数据库。这些白名单事件中的任何一个事件都对应一种*白名单违规*，表明特定主机违反白名单的原因和方式。如果主机违反一个或多个白名单，可以两种方式查看其主机配置文件中的这些违规情况。

首先，主机配置文件列出与主机相关的单个白名单违规事项。

主机配置文件中的白名单违规信息的说明如下。

类型

违规类型，即违规是由于操作系统、应用、服务器还是协议不符合规定造成的。

原因

出现违规的具体原因。例如，如果白名单仅容许 Microsoft Windows 主机，主机配置文件会显示当前运行在主机上的操作系统（比如，`Linux Linux 2.4、2.6`）

White List

与违规关联的白名单的名称。

其次，在与操作系统、应用、协议和服务器有关的部分中，防御中心将为不合规元素标记白名单违规图标 ( )。例如，对于仅容许 Microsoft Windows 主机的白名单，主机配置文件会在该主机操作系统信息旁边显示白名单违规图标。

请注意，可利用主机的配置文件为合规性白名单创建共享主机配置文件。有关详细信息，请参阅下一节，从主机配置文件创建白名单主机配置文件。

从主机配置文件创建白名单主机配置文件

许可证：FireSIGHT

合规性白名单共享主机配置文件明确规定操作系统、应用协议、客户端、网络应用和允许在多个白名单的目标主机上运行的协议。也就是说，如果创建了多个白名单，但要使用相同的主机配置文件来评估运行白名单中规定的特定操作系统的主机，可使用共享主机配置文件。

可使用任何 IP 地址已知的主机的主机配置文件创建可供合规性白名单使用的共享主机配置文件。但是，请注意，如果系统还未确定主机的操作系统，不得根据单个主机的主机配置文件创建共享主机配置文件。

要根据主机配置文件为合规性白名单创建共享主机配置文件，请执行以下操作：

访问：管理

步骤 1　通过任何网络映射或活动视图访问主机配置文件。

有关详细信息，请参阅第 49-4 页上的查看主机配置文件。

步骤 2　点击 **Generate White List Profile**。

系统将显示 Edit Shared Profiles 页面。根据所访问的主机配置文件中的信息预先填充页面上的字段。

步骤 3　根据特定需要修改并保存共享主机配置文件。

有关为合规性白名单创建共享主机配置文件的详细信息，请参阅第 52-21 页上的使用共享主机配置文件。

使用主机配置文件中的恶意软件检测

许可证：FireSIGHT 和 恶意软件

Most Recent Malware Detections 部分列出主机发送或接收恶意软件文件的最新恶意软件事件，最多 100 个。主机配置文件包含基于网络和终端的恶意软件事件。

如果主机涉及文件事件，且文件在回溯时被确定为恶意软件，在识别恶意软件开始后，恶意软件检测列表会显示传输文件的原始事件。当确定为恶意软件的文件在回溯时被确定为非恶意软件时，该列表不会再显示与该文件相关的恶意软件事件。例如，如果文件性质为 `Malware`，并且该性质更改为 `Clean`，则从主机配置文件中的恶意软件检测列表中移除针对该文件的事件。有关恶意软件事件的详细信息，请参阅第 40-14 页上的使用恶意软件事件。

对主机配置文件中 Most Recent Malware Detection 部分中各列的描述如下。

时间

事件生成的日期和时间。

对于文件在回溯时被确定为恶意软件的事件，请注意，这是指原始事件的时间而非确定恶意软件的时间。

Host Role

主机在传输检测到的恶意软件中的角色，发送方或接收方。请注意，对于基于终端的恶意软件事件，主机扮演的角色始终是接收者。

Threat Name

被测恶意软件名称。

文件名

恶意软件文件名。

文件类型

文件类型；例如， `PDF` 或 `MSEXE`。

在主机配置文件中查看恶意软件检测情况时，可在事件查看器中查看该主机的恶意软件事件。要查看事件，请点击恶意软件图标 ()。

使用主机配置文件中的漏洞

许可证：FireSIGHT

主机配置文件 Vulnerabilities 部分显示影响该主机的漏洞。

Sourcefire Vulnerabilities 部分显示系统在主机上检测到的，基于操作系统、服务器和应用的漏洞。

如果主机操作系统标识或主机上的一种应用协议存在标识冲突，系统会在冲突解决前显示这两种标识的漏洞。

因为根据 NetFlow 数据添加至网络映射的主机没有可用的操作系统信息，所以防御中心无法确定影响这些主机的漏洞，除非使用主机输入功能手动设置主机的操作系统标识。

流量通常不包括有关服务器供应商和版本的信息。默认情况下，系统并不映射此类流量的发送和接收主机的关联漏洞。然而，可使用系统策略配置系统以映射没有供应商或版本信息的特定应用协议的漏洞。有关详细信息，请参阅第 63-27 页上的映射服务器的漏洞。

如果使用主机输入功能添加网络中主机的第三方漏洞信息，系统会额外显示 Vulnerabilities 部分。例如，如果导入从 QualysGuard 扫描仪获得的漏洞，系统上的主机配置文件将包含 QualysGuard Vulnerabilities 部分。

您可把第三方漏洞与操作系统和应用协议关联起来，但不得关联客户端。有关导入第三方漏洞的详细信息，请参阅《*FireSIGHT 系统主机输入 API 指南*》。

主机配置文件中 Vulnerabilities 部分中各列的说明如下。

字段名称

漏洞名称。

远程

表明漏洞是否可以远程利用。如果该列为空，漏洞定义不包含此信息。

组件

与漏洞有关的操作系统、应用协议或客户端的名称。

端口

端口号，如果漏洞与在特定端口运行的应用协议相关。

请谨记，对于第三方漏洞，主机配置文件中相应的 Vulnerabilities 部分包含的信息仅限于用户使用主机输入功能导入漏洞数据时提供的信息。

查看主机配置文件中的漏洞时，您可以：

- 点击列标题以对 **Vulnerabilities** 部分的列进行排序。要反向排序，请再次点击。
- 点击漏洞名称，可查看与漏洞有关的详细技术信息，包括已知的解决方案。有关详情，请参见第 49-24 页上的查看漏洞细节。请注意，您还可以通过漏洞视图或 Vulnerabilities 网络映射来了解漏洞详细信息。
- 避免使用漏洞对影响相关性进行评估。有关详情，请参见第 49-25 页上的设置漏洞影响限定。
- 下载修补程序以减少在网络中主机上发现的漏洞。有关详情，请参见第 49-26 页上的下载漏洞补丁。
- 如果确定主机已经修补，把主机标记为不易受漏洞攻击。有关详情，请参见第 49-26 页上的设置单个主机的漏洞。

查看漏洞细节

许可证：FireSIGHT

漏洞细节对漏洞和已知解决方案进行了技术说明。

要访问特定漏洞的漏洞细节，请选择 **Analysis > Vulnerabilities** 或 **Analysis > Third-Party Vulnerabilities**，然后点击 SVID 旁边的查看图标 ( )。此外，还可以从网络映射和主机配置文件访问漏洞细节。

Vulnerability Detail 页面上的字段说明如下。

思科 Vulnerability ID

指系统用来跟踪漏洞的标别号 (SVID)。

Snort ID

与 Snort ID (SID) 数据库中漏洞关联的标识号。也就是说，如果入侵规则能检测利用特殊漏洞的网络流量，则此漏洞与入侵规则的 SID 关联。

注意，一个漏洞可能与多个 SID （或根本不与 SID）关联。如果漏洞没有关联的 SID，该字段不会显示。

BugTraq ID

指与 Bugtraq 数据库 (http://www.securityfocus.com/bid) 中的漏洞相关的标识号。

CVE ID

与 MITRE 的常见漏洞和攻击 (CVE) 数据库 (http://www.cve.mitre.org/) 中漏洞关联的标识号。

职位

漏洞的标题。

Impact Qualification

使用下拉列表启用或禁用漏洞。防御中心忽略其影响相关性中的禁用漏洞。

此处指定的设置确定如何在整个系统范围内处理漏洞，而且该设置不限于选择该值的主机配置文件。有关使用该功能启用或禁用漏洞的详细信息，请参阅第 49-25 页上的设置漏洞影响限定。

Date Published

指漏洞的发布日期。

Vulnerability Impact

Bugtraq 数据库中按照 1 至 10 的标准为漏洞分配的严重性，其中， 10 代表严重性最高。漏洞的影响程度由 Bugtraq 条目编写人员在 SANS 关键漏洞分析 (CVA) 标准基础上根据自己的最佳判断来确定。

远程

表示漏洞是否可以远程利用。

Available Exploits

表示是否有已知漏洞利用。

说明

指漏洞概述。

Technical Description

指对漏洞的详细技术说明。

解决方案

有关修补漏洞的信息。

更多信息

点击箭头查看其他有关漏洞的信息（如果可用），例如已知使用和其可用性、使用情景和缓解策略。

Fixes

提供所选漏洞可用的可下载的补丁的链接。

提示 如果出现修复程序或补丁下载的直接链路，右击该链接并保存至本地计算机。

设置漏洞影响限定

许可证：FireSIGHT

如果系统报告不适用于网络的漏洞，可避免使用该漏洞对影响标记关联进行评估。请注意，如果停用主机配置文件中漏洞，网络中的所有主机都会停用该漏洞。然而，可随时启用该漏洞。

当主机操作系统或主机上的其中一个应用的标识出现冲突时，系统会在冲突解决前显示这两种相互冲突的标识的漏洞。有关详细信息，请参阅第 46-5 页上的了解标识冲突和第 49-12 页上的解决操作系统的标识冲突。

此外，请注意，系统不会根据使用影响限定功能禁用的漏洞而推荐入侵规则的规则状态。有关详细信息，请参阅第 33-1 页上的为您的网络资产定制入侵防御。

提示 此外，您还可以禁用网络映射和漏洞事件视图的漏洞。有关详细信息，请参阅第 48-6 页上的使用漏洞网络映射和第 50-46 页上的停用漏洞。

要更改漏洞在系统中的使用，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1 访问受要停用漏洞影响的主机的主机配置文件。

步骤 2 展开 **Vulnerabilities** 部分。

步骤 3 点击要启用或禁用的漏洞的名称。

弹出一个窗口，显示漏洞详细信息。有关详细信息，请参阅第 49-24 页上的查看漏洞细节。

步骤 4 选择 **Impact Qualification** 下拉列表中的 **Disabled** 或 **Enabled**，以指定如何使用漏洞。

步骤 5 确定要更改网络映射上的所有主机的影响限定。

漏洞启用或禁用成功。

步骤 6 点击 **Done** 关闭漏洞细节弹出窗口。

下载漏洞补丁

许可证：FireSIGHT

如果补丁可用，可下载补丁减少在网络中的主机上发现的漏洞。

要下载漏洞补丁，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　访问要下载补丁的主机的主机配置文件。

步骤 2　展开 **Vulnerabilities** 部分。

步骤 3　点击要修补漏洞的名称。

系统将显示 Vulnerability Detail 页面。

步骤 4　展开 **Fixes** 部分。

系统将显示该漏洞的可下载补丁列表。

步骤 5　点击要下载的补丁旁边的 **Download**。

系统将显示补丁供应商的下载页面。

步骤 6　下载补丁并应用到受影响的系统上。

设置单个主机的漏洞

许可证：FireSIGHT

可使用主机漏洞编辑器逐台激活或停用主机上的漏洞。当停用主机漏洞时，该主机的影响相关性依然在使用该漏洞，但其影响级别自动降低一个级别。

要激活或停用单台主机的漏洞，请执行以下操作：

访问：管理员/安全分析师

步骤 1　打开主机配置文件。

步骤 2　点击 **Vulnerabilities** 旁边的 **Edit**。

系统将显示 Host Vulnerabilities 编辑器页面。

提示　要查看漏洞详细信息，请选择漏洞并点击 **View**。有关详细信息，请参阅第 49-24 页上的查看漏洞细节。

步骤 3　此时您有两种选择：

- 要停用漏洞，请选择 **Valid Vulnerabilities** 列表中的漏洞，然后点击向下箭头。
- 要激活漏洞，请选择 **Invalid Vulnerabilities** 列表中的漏洞，然后点击向上箭头。

提示　要选择多个漏洞，可在点击的同时使用 Ctrl 或 Shift 键。可点击拖动选择多个相邻漏洞；还可双击漏洞在列表间移动漏洞。

步骤 4　点击 **Save**。

已保存您的更改。

使用预先定义的主机属性

许可证：FireSIGHT

可分配给每台主机的预定义主机属性有两个：主机重要性和主机特定注释。可利用主机重要性属性指定特定主机的业务重要性，并根据主机重要性修改关联策略和警报。例如，如果您认为公司的邮件服务器比一般用户工作站对业务更重要，可把 High 值分配给邮件服务器和其他业务关键设备，把 Medium 或 Low 值分配给其他主机。然后，根据受影响的主机重要性创建可发出不同警报的关联策略。

使用注释功能记录要其他分析师查看的主机的信息。例如，如果网络上有使用测试用旧版未打补丁操作系统的计算机，可使用注释功能注明此系统特意未打补丁。

要在主机配置文件设置预先定义的主机属性，请执行以下操作：

访问：管理员/安全分析师

步骤 1　打开要设置业务重要性的主机的主机配置文件。

步骤 2　点击 **Attributes** 旁边的铅笔图标 ( )。

系统将显示 Host Attributes 弹出窗口。

步骤 3　从 **Host Criticality** 下拉列表中选择要应用的值：**None**、 **Low**、 **Medium** 或 **High**。

步骤 4　点击 **Save**。

选择内容保存成功。

使用用户定义的主机属性

许可证：FireSIGHT

FireSIGHT 系统包含两种预先定义的可用来表明网络上的主机的业务重要性的主机属性：主机重要性和主机注释。如果用户有其他想用来识别主机的标准，可创建用户定义主机属性。

用户定义的主机属性显示在主机配置文件页面中，可在此页面为每台主机分配值。然后，可在关联策略和搜索中使用这些属性。此外，还可在事件的主机属性表视图中查看属性并据此生成报告。

注　主机属性是全局定义，而非基于策略的定义。在创建主机属性后，无论应用哪种策略，主机属性都可用。

用户定义的主机属性举例如下：

- 向主机分配物理位置标识符，比如设备代码、城市或房间号码。
- 分配表明特定主机的系统管理员的责任方标识符。然后，制定相关性规则和策略，当检测到与主机相关的问题时，把警报发送给适当的系统管理员。

主机属性可以是从预先定义的文本列表或数字范围选择的文本字符串或值。此外，还可根据主机的 IP 地址自动将预先定义的列表值分配给主机。当新主机第一次出现在网络上时，可使用该功能自动把值分配给新主机。

主机属性可以是下列类型之一：

文本

可手动向主机分配最多包含 255 个字符的文本字符串。

整数

允许用户指定一系列正整数中的第一个和最后一个数字，然后手动把这些数字中的一个数字分配给主机。

清单

允许用户创建字符串值列表，然后手动将这些值中的其中一个分配给主机。此外，还可根据主机的 IP 地址自动把值分配给主机。

注 如果根据具有多个 IP 地址的主机的一个 IP 地址自动分配值，那些值将应用到与该主机相关的所有地址。当查看 Host Attributes 表时，请记住此点。

URL

允许用户手动把 URL 值分配给主机。

请注意，创建的每个合规性白名单会自动创建与白名单名称相同的主机属性。可能的主机属性值包括 `Compliant`（用于符合白名单的主机）、`Non-Compliant`（用于违反白名单的主机）或 `Not Evaluated`（用于不是白名单有效目标或由于某种原因没有进行评估的主机）。**无法**手动更改白名单的主机属性值。有关白名单的详细信息，请参阅第 52-1 页上的将 FireSIGHT 系统用作一个合规工具。

有关详细信息，请参阅：

- 第 49-28 页上的创建用户定义的主机属性
- 第 49-30 页上的编辑用户定义的主机属性
- 第 49-31 页上的删除用户定义的主机属性

创建用户定义的主机属性

许可证：FireSIGHT

下列操作步骤说明如何创建用户定义的主机属性。

注 主机属性是全局定义，而非基于策略的定义。在创建主机属性后，无论应用哪种策略，主机属性都可用。

要创建新的主机属性，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Analysis > Hosts > Host Attributes**。

系统将显示 Host Attributes 页面。

步骤 2　点击 **Host Attribute Management**。

系统将显示 Host Attribute Management 页面。

步骤 3　点击 **Create Attribute**。

系统将显示 Create Attribute 页面。

步骤 4　在 **Name** 字段，使用字母数字字符和空格键入主机属性名称。

步骤 5　从 **Type** 下拉列表中选择要创建的属性的类型，如第 49-19 页上的使用主机配置文件中的主机属性所述：

- 如果正在创建 **Text** 或 **URL** 主机属性，请继续第 6 步。
- 如果正在创建 **Integer** 主机属性，请参阅第 49-29 页上的创建整数主机属性。
- 如果正在创建 **List** 主机属性，请参阅第 49-29 页上的创建列表主机属性。

步骤 6　点击 **Save**。

新的用户定义的主机属性保存成功。

创建整数主机属性

许可证：FireSIGHT

当定义基于整数的主机属性时，必须指定属性接受的数字范围。

要创建基于整数的主机属性，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 **Min** 字段，输入可分配给主机的最小整数值。

步骤 2　在 **Max** 字段，输入可分配给主机的最大整数值。

步骤 3　点击 **Save**。

新的基于整数的主机属性保存成功。

创建列表主机属性

许可证：FireSIGHT

当定义基于列表的主机属性时，必须为列表提供所有的值。这些值可包含字母数字字符、空格和符号。

当为主机属性创建值时，还可把值自动分配到 IP 地址块，从而可以在发现新主机时，自动为主机属性分配该值。

要创建基于列表的主机属性，请执行以下操作：

访问：管理员/发现管理员

步骤 1　要将值添加到列表，请点击 **Add Value**。

系统将展开 List Values 部分。

步骤 2　在 **Name** 字段，用数字字符、符号和空格输入要添加的第一个值。

步骤 3　或者，要自动分配刚刚添加至主机属性值，请点击 **Add Networks**。

系统将展开 Auto-Assign Networks 部分。

步骤 4　从 **Value** 下拉列表选择已添加的值。

步骤 5　在 **IP Address** 和 **Netmask** 字段，输入代表要自动分配该值的 IP 地址块的 IP 地址和网络掩码 （以 CIDR 表示）。

有关在 FireSIGHT 系统中使用 CIDR 表示法的信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 6　重复第 1 步至第 5 步，在列表中添加更多值，并自动将其分配给 IP 地址块中的新主机。

提示　如果不想将列表值自动分配给特定 IP 块内的主机，可以按照第 49-27 页上的使用预先定义的主机属性所述手动分配列表值。

编辑用户定义的主机属性

许可证：FireSIGHT

当修改现有用户定义的主机属性时，可更改值的定义，但不能更改属性类型 （文本、列表、整数和 URL）。此外，**无法**修改合规性白名单主机属性。

要编辑现有用户定义的主机属性，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Analysis > Hosts > Host Attributes**。

系统将显示 Host Attributes 页面。

步骤 2　点击 **Host Attribute Management**。

系统将显示 Host Attribute Management 页面。

步骤 3　点击要编辑的主机属性旁边的编辑图标 ( )。

系统将显示主机属性页面，并显示所选属性的设置。

步骤 4　修改任何您要修改的设置并点击 **Save**。

有关可编辑的属性类型和属性所含值的详细信息，请参阅第 49-28 页上的创建用户定义的主机属性。

删除用户定义的主机属性

许可证：FireSIGHT

删除用户定义的主机属性可将用户定义的主机属性从所有使用该主机属性的主机配置文件中删除。请注意**无法**删除合规性白名单主机属性。

要删除主机属性，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Analysis > Hosts > Host Attributes**。

系统将显示 Host Attributes 页面。

步骤 2　点击 **Host Attribute Management**。

系统将显示 Host Attribute Management 页面。

步骤 3　点击要删除的主机属性旁边的编辑图标 ( )。

所选的主机属性已从系统中删除。

使用主机配置文件的扫描结果

许可证：FireSIGHT

当您使用 Nmap 扫描主机时，或者导入 Nmap 的扫描结果时，这些结果出现在所有被扫描的主机的主机配置文件中。

直接把 Nmap 搜集到的有关主机操作系统和运行在开放式未经过滤的端口的服务器的信息分别添加到主机配置文件的 Operating System 和 Servers 部分。此外， Nmap 在 Scan Results 部分添加该主机的扫描结果列表。

结果代表的是信息源、扫描的端口的数量和类型、运行在端口的服务器的名称和任何 Nmap 检测到的其他信息，比如端口状态或服务器的供应商名称。如果扫描 UDP 端口，在这些端口上检测到的服务器仅出现在 Scan Results 部分。

请注意，可从主机配置文件运行 Nmap 扫描。有关详细信息，请参阅，扫描主机配置文件中的主机。

扫描主机配置文件中的主机

许可证：FireSIGHT

可对主机配置文件中的主机进行 Nmap 扫描。在扫描完后，更新主机配置文件中的该主机的服务器和操作系统信息。所有其他扫描结果可添加至主机配置文件中的 Scan Results 部分。

注意事项　在再一次运行 Nmap 扫描或用更高优先级的主机输入覆盖之前， Nmap 提供的服务器和操作系统数据保持不变。如果使用 Nmap 扫描主机，可设置定期计划扫描以随时更新由 Nmap 提供的操作系统和服务器的数据。有关详细信息，请参阅第 62-5 页上的自动运行 Nmap 扫描。

要扫描主机配置文件中的主机，请执行以下操作：

访问：管理

步骤 1　在主机配置文件中，点击 **Scan Host**。

系统将显示 Scan Host 弹出窗口。

步骤 2　点击要用来扫描主机的扫描更正旁边的 **Scan**。

扫描主机并把扫描结果添加至主机配置文件。

使用发现事件

发现事件提醒网络活动并提供正确响应所需的信息。这些事件是由受管设备在所监控网段检测到的变化触发的。*网络发现策略*规定了系统所采集数据、受监控网段以及系统用于监控流量的特定硬件接口的类型。有关网络发现的详细信息，请参阅第 45-1 页上的了解发现数据收集。

拥有访问员工连接到网络的会议室或备用工作空间是发现事件的简单例子。可在这些分段中发现定期生成的新主机事件，无需怀疑其恶意目的。但是，如果在锁定网段发现新主机事件，则可相应地升级响应。

用户发现事件提供登录到网络中的主机的用户信息。可查看网络上用户活动的事件目录并钻取查看特定用户的信息。例如，如果要查看与新主机关联的用户，可通过查看主机配置文件了解用主机流量监控过程中检测到的用户。

通过发现事件可更加深入地了解网络上的活动，其程度比简单示例所示程度更加细致。对于每个受监控主机，可通过配置系统检测相关应用协议、网络协议、客户端、用户和潜在漏洞。系统也可提供有关使用主机输入功能导入到防御中心上的第三方扫描仪所检测到的漏洞的信息。危害表现 (IOC) 使用入侵、恶意软件和其他数据识别安全可能受到威胁的主机。此外，可跟踪在主机重要性、主机属性或用户通过用户界面输入的漏洞设置的所有更改。

系统提供了用于分析系统生成的发现事件的一系列预定义工作流程。也可创建仅显示与特定需求匹配的自定义工作流程。

要采集和存储网络发现数据用于分析，确保配置网络发现策略，发现思科受管设备和 NetFlow 可用设备监控流量的网络和区域中的适当数据。要从发现的区域中排除受监控区域，请在网络发现策略中进行配置。注意在应用网络发现策略前必须在受管设备上应用访问控制策略。有关详细信息，请参阅第 45-19 页上的创建网络发现策略。

有关详情，请参阅：

查看发现事件统计数据

许可证：FireSIGHT

Discovery Statistics 页面显示系统检测到的主机、事件、协议、应用协议和操作系统的摘要：

- 统计摘要提供有关事件总量、应用协议、主机、网络设备的一般统计数据和主机上限使用情况的信息，请参阅第 50-2 页上的统计摘要。
- 事件明细提供有关系统中所发生事件类型的统计数据；请参阅第 50-3 页上的事件明细。
- 协议明细提供有关检测到的主机上所使用协议的统计数据。请参阅第 50-4 页上的协议明细。
- 应用协议明细提供有关网络所使用的应用协议的统计数据；请参阅第 50-4 页上的应用协议明细。
- 操作系统明细列出在网络上运行的操作系统以及每种操作系统有多少台主机使用；请参阅第 50-4 页上的 OS 明细。

此页面列出了最近一小时的统计数据和全部的累积统计数据。可选择特定设备或所有设备的统计数据。也可通过点击摘要内列出的事件、服务器、操作系统或操作系统供应商查看与此页面上条目匹配的事件。

要查看发现统计数据摘要，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Summary > Discovery Statistics**。

系统显示统计数据摘要页面。

步骤 2　从 **Select Device** 列表中选择要查看其统计数据的设备。选择 **All** 查看由 防御中心.管理的所有设备的统计数据。

统计摘要

许可证：FireSIGHT

统计摘要提供有关事件总量、应用协议、主机、网络设备的一般统计数据以及有关主机上限使用情况的信息。

以下对统计摘要部分的各行进行了说明。

Total Events

防御中心上存储的发现事件的总数。

Total Events Last Hour

最近一小时生成的发现事件的总数。

Total Events Last Day

最后一天生成的发现事件的总数。

Total Application Protocols

检测到的主机上运行的服务器所使用的应用协议总数。

Total IP Hosts

通过唯一 IP 地址识别的检测到的主机总数。

Total MAC Hosts

不是通过 IP 地址识别的检测到的主机总数。

注意无论用户是否查看所有设备或特定设备的发现统计数据，Total MAC Hosts 统计数据都保持不变。这是因为受管设备是根据其 IP 地址发现主机的。此统计数据提供通过其他方式识别的独立于给定受管设备的所有主机的总数。

Total Routers

检测到的识别为路由的节点总数。

Total Bridges

检测到的识别为网桥的节点总数。

Host Limit Usage

当前所使用主机上限的总百分比。主机上限应用是通过 FireSIGHT 许可证定义的。注意只有在查看所有受管设备的统计数据时才会显示主机上限的使用情况。有关主机使用监控的详细信息，请参阅第 68-15 页上的配置 FireSIGHT 主机使用情况监控。

注 如果达到主机上限且已删除一台主机，则此主机不会再出现在网络映射上，直到配置为执行发现的所有受管设备上的网络发现重新启用为止。

Last Event Received

最新发现事件发生的日期和时间。

Last Connection Received

最新连接完成的日期和时间。

事件明细

许可证：FireSIGHT

事件明细章部分列出了最近一小时内发生的各种网络发现和主机输入事件的计数，以及数据库中存储的每种事件类型的总数的计数。有关每种事件类型的完整说明，请参阅第 50-8 页上的了解发现事件类型和第 50-11 页上的了解主机输入事件类型。

也可通过事件明细部分查看发现和主机输入事件的详细信息。

通过键入以下内容查看网络发现和和主机输入事件：

访问：管理员/任何安全分析师

步骤 1　点击要查看的事件类型。

系统显示默认发现事件工作流程的第一页，这是由所选事件的类型限制的。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示任何事件，可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

有关使用发现事件的详细信息，请参阅第 50-7 页上的使用发现和主机输入事件。

协议明细

许可证：FireSIGHT

协议明细部分列出了检测到的主机当前所使用的协议。显示每个检测到的协议的名称、其在协议栈中的“协议层”和使用此协议进行通信的主机的总数。

应用协议明细

许可证：FireSIGHT

应用协议明细部分列了检测到的主机当前所使用的应用协议。列出了协议名称、最近一个小时内运行应用协议的主机的总数和检测到的随时运行协议的主机的总数。

也可通过应用协议明细部分查看使用所检测到协议的服务器的详细信息。

查看使用所列应用协议的服务器。

访问：管理员/任何安全分析师

步骤 1　点击要查看应用协议的名称。

系统显示默认服务器工作流程的第一页，这是由所选应用协议限制的。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

有关所使用服务器的详细信息，请参阅第 50-31 页上的使用服务器。

OS 明细

许可证：FireSIGHT

OS 明细列部分出了当前在受监控网络中运行的操作系统，及其供应商和运行每个操作系统的主机的总数。

操作系统名称或版本的 `unknown` 值是指操作系统或其版本与系统的任何指纹都不匹配。`pending` 值表明系统尚未采集到足够的信息用于识别操作系统或其版本。

可通过 OS 明细部分查看检测到的操作系统的详细信息。

通过操作系统或供应商查看主机：

访问：管理员/任何安全分析师

步骤 1　此时您有两种选择：

- 要查看运行特定操作系统的所有主机，请在 **OS Name** 下，点击操作系统名称。
- 要查看特定供应商提供的运行任何操作系统的所有主机，请在 **OS Vendor** 下点击供应商名称。

系统显示默认主机工作流程的第一页，这是由所选的操作系统或供应商限制的。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

有关所使用主机的详细信息，请参阅第 50-17 页上的使用主机。

查看发现性能 图表

许可证：FireSIGHT

可利用发现事件生成显示受管设备性能统计数据的图表。

注　新数据将进行累计，统计信息图表每五分钟更新一次。因此，如果快速重新加载图表，直到下一次五分钟更新间隔之前数据可能不会更改。

可用图表类型的说明如下。

Processed Events/Sec

显示表示数据相关器每秒钟所处理事件数量的图表

Processed Connections/Sec

显示表示数据相关器每秒钟所处理连接数量的图表

Generated Events/Sec

显示表示系统每秒钟所生成的事件数量的图表

兆位/秒

显示表示发现进程每秒钟所分析流量兆比数的图表

平均字节/数据包

显示表示发现进程所分析的每个数据包中所含平均兆比数的图表

K Packets/Sec

显示表示发现进程每秒钟所分析的数千个数据包数量的图表

生成发现性能图表：

访问：管理员/维护人员

步骤 1　选择 **Overview > Summary > Discovery Performance**。

系统显示发现性能页面。

步骤 2　从 **Select Device** 列表中选择防御中心或要包括的受管设备。

Select Graph(s) 列表根据所选设备调整显示可用图表。

步骤 3　从 **Select Graph(s)** 列表中，选择要创建的图表类型。

提示　可选择多个图表，只需在按住 Ctrl 和 Shift 键的同时点击图表类型。

步骤 4　从 **Select Time Range** 列表中，选择要用于图表的时间范围。可供选择的时间范围有：过去一小时、前一天、上一周和上个月。

步骤 5　点击 **Graph** 生成所选统计数据的图表。

显示所选图表。

了解发现事件工作流程

许可证：FireSIGHT

防御中心提供了一套可用于分析生成的网络发现事件的工作流程。工作流程与网络映射是关于网络资产的关键信息来源。这些工作流程包括填入了系统所生成发现数据的表。

从 **Analysis > Hosts** 菜单访问网络发现工作流程。防御中心提供了发现事件、检测到的主机以及其主机属性、服务器、应用、应用详情、漏洞、用户活动和用户的预定义工作流程。也可创建自定义工作流程。有关工作流程的详细信息，请参阅第 58-1 页上的了解和使用工作流程。

提示　选择 **Analysis > Custom > Custom Tables**，根据自定义表访问工作流程。

如果使用网络发现工作流程，无论任何事件类型，都可执行许多常见操作。常见发现事件操作表中对这些常见功能进行了说明。

表 50-1　　常见发现事件操作

要.....	您可以.....
查看 IP 地址的主机配置文件	点击主机配置文件图标 ( )，或者，对于带有效危害表现 (IOC) 标记的主机，点击 IP 地址旁边显示的危害主机图标 ( )。有关 IOC 的详细信息，请参阅第 50-28 页上的使用危害表现。
查看用户配置文件信息	点击用户标识旁边显示的用户图标 ( )。有关详细信息，请参阅第 50-55 页上的了解用户详细信息和主机历史记录。
对数据进行排序	点击列标题。再次点击列标题以反转排列顺序。

表 50-1　　常见发现事件操作 （续）

要.....	您可以.....
向下钻取到工作流程中的下一个页面	可使用以下其中一种方法： • 要向下钻取到限制某个特定值的下一个工作流程页面，请点击某一行中的一个值。请注意，此操作仅适用于向下钻取页面。在表视图中点击一行中的一个值仅限于表视图，不能钻取到下一页面。 • 要向下钻取到限制某些事件的下一个工作流程页面，请选择您想要在下一个工作流程页面上查看的事件旁的复选框，然后点击 **View**。 • 要向下钻取到保留当前限制的下一工作流程页面，请点击 **View All**。 **提示**　表视图的页面名称中始终包括“Table View”。 有关详细信息，请参阅第 58-26 页上的限制事件。
约束显示的列数	在要隐藏的列标题中点击关闭图标 (✖)。在显示的弹出窗口中，点击 **Apply**。 **提示**　要隐藏或显示其他列，选择或清除相应的复选框，然后点击 **Apply**。要将禁用列添加回视图中，请点击展开箭头展开搜索限制条件，然后点击 Disabled Columns 下的列名称。
在当前工作流程页面中导航	在第 58-30 页上的导航到工作流程中的其他页面中获得详细信息。
在当前工作流程中的页面之间导航，同时保留当前限制条件	点击工作流程页面左上角的相应页面链接。有关的详细信息，请参阅第 58-16 页上的使用工作流程页面。
从系统中删除项目，包括: • 从发现事件工作流程中删除发现和主机输入事件 • 从主机工作流程中删除主机和网络设备 • 从主机属性工作流程中删除主机属性 • 从服务器工作流程中删除服务器 • 从应用工作流程中删除应用 • 从第三方漏洞工作流程中删除第三方漏洞 • 从用户工作流程中删除用户	可使用以下其中一种方法： • 要删除某些项目，请选择要删除的项目旁边的复选框，然后点击 **Delete**。 • 要删除当前受限视图中的所有项目，请点击 **Delete All**，然后确认要删除所有项目。 这些项目保持删除状态，直到系统的发现功能重新启用时才可再次检测到这些项目。 **提示**　有关如何从数据库中删除所有发现事件的信息以及有关如何重新启用发现的详细信息，请参阅第 B-1 页上的从数据库清除发现数据。 注意**不能**删除思科 （与第三方对立的）漏洞；但是，可将其标记为已审查。有关详细信息，请参阅第 50-43 页上的使用漏洞。
导航至其他事件视图查看相关事件	在第 58-31 页上的在工作流程之间导航中获得详细信息。

使用发现和主机输入事件

许可证：FireSIGHT

系统生成变化详情在受监控网段中通信的发现事件。为新发现的网络功能生成*新的*事件，并为先前识别的网络资产的任何变化生成更改事件。

在初始网络发现阶段，系统为每台主机以及已发现在每台主机上运行的每个 TCP 或 UDP 服务器生成新的事件。或者，可配置系统，通过 NetFlow 可用设备使用导出数据生成这些新的主机和服务器事件。

此外，系统为每个网络、传送和在每台已发现主机上运行的应用协议生成新的事件。创建已配置的发现规则用于包括 NetFlow 可用设备时，可禁用应用协议检测。但是，不能在未使用已配置的 NetFlow 可用设备的发现规则中禁用应用检测。如果在非 NetFlow 发现规则中启用的主机或用户发现，系统自动发现应用。

初次网络映射完成后，系统通过生成更改事件持续记录网络变化。无论先前发现的资产配置何时发生改变，系统都会生成更改事件。

如果生成发现事件，表明已登录到数据库。可使用防御中心网络界面查看、搜索和删除发现事件。也可在关联规则中使用发现事件。根据生成的发现事件类型以及其他指定条件，用于关联策略时可生成关联规则，网络流量符合条件时可启动修复和系统记录、 SNMP和邮件警报响应。

可使用主机输入功能向网络映射中添加数据。可添加、修改或删除操作系统信息，这些操作会导致系统停止更新此主机的此信息。也可手动添加，修改或删除应用协议、客户端、服务器和主机属性或修改漏洞信息。执行此操作时，系统生成主机输入事件。

有关详细信息，请参阅：

- 第 50-8 页上的了解发现事件类型
- 第 50-11 页上的了解主机输入事件类型
- 第 50-13 页上的查看发现和主机输入事件
- 第 50-14 页上的了解发现事件表
- 第 50-15 页上的搜索发现事件

了解发现事件类型

许可证：FireSIGHT

发现事件有许多不同的类型。例如，在受监控网段检测到新主机时，系统生成并记录一个新的主机事件。查看发现事件表时， **Event** 列中列出事件类型。有关详细信息，请参阅第 50-13 页上的查看发现和主机输入事件。

对比系统检测到所监控网络中的变化 （例如检测到来自之前未检测到主机的流量）时生成的发现事件与用户执行特定操作 （例如手动添加主机）时生成的主机输入事件。有关主机输入事件的详细信息，请参阅第 50-11 页上的了解主机输入事件类型。

可配置系统通过修改网络发现策略记录的发现事件的类型。默认情况下，系统记录所有发现事件的类型。有关详细信息，请参阅第 63-14 页上的配置控制面板事件限制。

如果了解了不同类型发现事件事件所提供的信息，可以更有效地确定需记录和警报的事件以及如何在关联策略中使用这些警报。此外，了解事件类型的名称有助于更有效地进行事件搜索。不同类型的发现事件的说明如下。

Additional MAC Detected for Host

系统检测到先前所发现主机的新 MAC 地址时，生成此事件。

系统检测到主机经流量通过路由器时，经常生成此事件。虽然每台主机都有不同的 IP 地址，但它们似乎有与路由器关联的 MAC 地址。系统检测到与 IP 地址关联的实际 MAC 地址时，主机配置文件中 MAC 地址显示为粗体文本且在事件视图的事件说明中 MAC 地址显示为“检测到 ARP/DHCP”消息。

Client Timeout

系统从数据库中删除一个不活跃的客户端时，生成此事件。

Client Update

系统在 HTTP 流量中检测到负载 （即特定类型的内容，例如音频、视频或网页邮件）时，生成此事件。

DHCP: IP Address Changed

系统检测到主机 IP 地址因 DHCP 地址分配改变时，生成此事件。

DHCP: IP Address Reassigned

主机重新使用 IP 地址时，生成此事件；即主机因 DHCP IP 地址分配获得另一物理主机以前使用的 IP 地址时。

Hops Change

系统检测到主机与检测此主机的设备之间的网络跳数发生变化时，生成此事件。

设备通过通过不同路由器查看主机流量时可能发生此事件并能够更好地确定主机的位置。如果设备检测到来自该主机的 ARP 传输也可能发生此事件，这表明主机在本地网段。

Host Deleted: Host Limit Reached

在防御中心中超过主机上限时发生此事件且从防御中心网络映射删除一台受监控主机。

Host Dropped: Host Limit Reached

在防御中心中达到主机上限时发生此事件且并丢弃一台新主机。对比此事件与达到主机上限时旧主机从网络映射中被删除的先前事件

要在达到主机上限时丢弃新主机，请转至 **Policies > Network Discovery > Advanced** 并将 **When Host Limit Reached** 设置为 **Drop hosts**。有关详情，请参见第 45-30 页上的配置数据存储。

Host IOC Set

为主机设置 IOC （危害表现）时生成此事件并并生成警报。

Host Timeout

主机由于未在网络发现策略规定的区间内发生流量而从网络映射中丢失时生成此事件。注意个别主机 IP 地址和 MAC 地址会单独超时；主机不会从网络映射中消失除非其所有关联地址均已超时。有关配置主机超时值的信息，请参阅第 45-30 页上的配置数据存储。

如果更改了网络发现策略需监控的网络，可能需要从网络映射中手动删除旧主机，以免 FireSIGHT 许可证受到影响。有关详细信息，请参阅第 48-2 页上的使用主机网络映射。

Host Type Changed to Network Device

系统检测到的主机实际上是网络设备时生成此事件。

Identity Conflict

系统检测到新服务器或操作系统标识与服务器或操作系统的当前活跃标识相冲突时生成此事件。

如果要通过重新扫描主机获取更新的有效标识数据来解决标识冲突，可使用标识冲突事件触发 Nmap 修复。有关详细信息，请参阅第 54-10 页上的配置 Nmap 补救。

有关详细信息，请参阅第 46-5 页上的了解标识冲突和第 45-27 页上的配置身份冲突解决。有关手动解决冲突的详细信息，请参阅第 49-12 页上的解决操作系统的标识冲突和第 49-16 页上的解决服务器标识冲突。

Identity Conflict

通过有效源添加到网络映射中标识数据超时时，生成此事件。

如果要通过重新扫描主机获取更新的有效标识数据来刷新标识冲突，可使用标识冲突事件触发 Nmap 修复。有关详细信息，请参阅第 54-10 页上的配置 Nmap 补救。

有关详细信息，请参阅第 49-16 页上的解决服务器标识冲突。

MAC Information Change

系统检测到与特定 MAC 地址或 TTL 值关联的信息发生变化时，生成此事件。

系统检测到主机流量通过路由器时，经常生成此事件。虽然每台主机都有不同的 IP 地址，但它们似将都有与路由器关联的 MAC 地址。系统检测到与 IP 地址关联的实际 MAC 地址时，主机配置文件中 MAC 地址显示为粗体文本且在事件视图的事件说明中 MAC 地址显示为“检测到 ARP/DHCP”消息。 TTL 可能会因为流量可能通过不同的路由器或者系统检测到主机的实际 MAC 地址而发生改变。

NETBIOS Name Change

系统检测到主机的 NetBIOS 名称改变时，生成此事件。只有有主机使用 NetBIOS 协议时才会生成此事件。

New Client

系统检测到新的客户端时，生成此事件。

注 要采集和存储客户数据用于分析，请确保网络发现策略的发现规则中启用应用检测。有关详细信息，请参阅第 45-9 页上的了解应用检测。

New Host

系统检测到新主机在网络中运行时，生成此事件。

如果选择 **Discover** 选项并在选择了 NetFlow 设备的发现网络规则中选择 **Hosts**，设备在处理涉及新主机的 NetFlow 数据时，也会生成此事件。

New Network Protocol

系统检测到主机使用新的网络协议 （IP、 ARP 等）通信时，生成此事件。

New OS

系统检测到主机适用新的操作系统或者主机操作系统发生变化时，生成此事件。

New TCP Port

系统检测到主机上有活跃的新 TCP 服务器端口 （例如， SMTP 或网络服务使用的端口）时，生成此事件。注意此事件不用于识别应用协议或与其关联的服务器；此信息在 TCP 服务器信息更新事件中传输。

如果选择 **Discover** 选项并在 NetFlow 数据的网络发现规则中选择 **Applications**，设备在处理涉及网络映射中已不存在的受监控网络中服务器的 NetFlow 数据时，也会生成此事件。

New Transport Protocol

系统检测到主机使用新的传输协议，例如 TCP 或 UDP，通信时，生成此事件。

New UDP Port

系统检测到主机上有新的 UDP 服务器端口时，生成此事件。

如果选择 **Discover** 选项并在 NetFlow 数据的网络发现规则中选择 **Applications**，设备在处理涉及网络映射中已不存在的受监控网络中服务器的 NetFlow 数据时，也会生成此事件。

TCP Port Closed

系统检测到主机上的 TCP 端口关闭时，生成此事件。

TCP Port Timeout

系统在系统网络发现策略规定的区域内未检测到来自 TCP 端口的活动时，生成此事件。有关配置服务器超时值的信息第 45-30 页上的配置数据存储，请参阅。

TCP Server Information Update

系统检测到主机上运行的已发现 TCP 服务器发生变化时，生成此事件。

如果 TCP 服务器已升级，则生成此事件。

UDP Port Closed

系统检测到主机上 UDP 端口关闭时，生成此事件。

UDP Port Timeout

系统在网络发现策略规定的区域内未检测到来自 UDP 端口的活动时，生成此事件。有关配置服务器超时值的信息第 45-30 页上的配置数据存储，请参阅。

UDP Server Information Update

系统检测到主机上运行的已发现 UDP 服务器发生变化时，生成此事件。

如果 UDP 服务器已升级，则生成此事件。

VLAN Tag Information Update

系统检测到主机的 VLAN 标签发生改变时，生成此事件。有关 VLAN 标记的详细信息，请参阅第 49-19 页上的使用主机配置文件中的 VLAN 标签。

了解主机输入事件类型

许可证：FireSIGHT

许多类型的主机输入事件。例如，用户使用主机导入功能添加主机时，系统生成并记录添加主机事件。查看发现事件表时， **Event** 列中列出事件类型。有关详细信息，请参阅第 50-13 页上的查看发现和主机输入事件。

对比用户执行特定操作 （例如手动添加主机）时生成的主机输入事件与系统自身检测到受监控网络发生变化 （例如来自之前未检测到主机的流量）时生成的发现事件。有关主机输入事件的详细信息，请参阅第 50-8 页上的了解发现事件类型。

可通过修改网络发现策略配置主机输入事件的类型。默认情况下，系统记录所有类型的主机输入事件。有关详细信息，请参阅第 63-14 页上的配置控制面板事件限制。

如果了解了不同类型主机输入事件事件所提供的信息，可以更有效地确定需记录和警报的事件以及如何在关联策略中使用这些警报。此外，了解事件类型的名称有助于更有效地进行事件搜索。不同类型的主机输入事件的说明如下。

Add Client

用户添加客户端时，生成此事件。

Add Host

用户添加主机时，生成此事件。

Add Protocol

用户添加协议时，生成此事件。

Add Scan Result

系统成功将 Nmap 扫描的结果添加到主机时，生成此事件。

Add Port

用户添加服务器端口时，生成此事件。

Delete Client

用户从系统中删除客户端时，生成此事件。

Delete Host/Network

用户从系统中删除 IP 地址或子网时，生成此事件。

Delete Protocol

用户从系统中删除协议时，生成此事件。

Delete Port

用户从系统中删除服务器端口或服务器端口组时，生成此事件。

Host Attribute Add

用户创建新的主机属性时，生成此事件。

Host Attribute Delete

用户删除自定义主机属性时，生成此事件。

Host Attribute Delete Value

用户删除主机属性赋值值时，生成此事件。

Host Attribute Delete Value

用户设置为主机设置主机属性值时，生成此事件。

Host Attribute Update

用户改变自定义主机属性的定义时，生成此事件。

Set Host Criticality

用户设置或修改主机的主机重要性时，生成此事件。

Set Operating System Definition

用户设置主机的操作系统时，生成此事件。

Set Server Definition

用户设置服务器的供应商和版本定义时，生成此事件。

Set Vulnerability Impact Qualification

设置漏洞影响限制时，生成此事件。

在全球层面上禁止漏洞用于影响限制，或者在全球层面上禁用漏洞时，生成此事件。

Vulnerability Set Invalid

用户作废（或审查）一个漏洞或多个漏洞时，生成此事件。

Vulnerability Set Valid

用户作废之前标记为无效的漏洞时，生成此事件。

查看发现和主机输入事件

许可证：FireSIGHT

使用发现事件工作流程可查看发现事件和主机输入事件。发现事件基于设备配置的网络发现策略记录网络发现数据的检测结果。主机输入事件记录通过主机输入功能将主机数据输入到网络映射中的事件。有关详细信息，请参阅第 50-8 页上的了解发现事件类型和第 50-11 页上的了解主机输入事件类型。

可使用防御中心查看发现或主机输入事件表。然后，可根据要查找的信息操纵事件视图。

访问事件时所看到的页面因所使用的工作流程而异。可使用预定义工作流程，包括发现事件的表视图和终止主机视图页面。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关创建自定义工作流程的信息，请参阅第 58-34 页上的创建自定义工作流程。

以下发现事件操作表说明可在发现事件工作流程页面执行的一些特定操作。也可执行常见发现事件操作表中所描述的任务。

表 50-2　　发现事件操作

要.....	您可以.....
修改所显示事件的时间和日期范围	在第 58-19 页上的设置事件时间限制中获得详细信息。 请注意，如果按时间限制事件视图，则在设备配置的时间段外生成的事件（无论是全局或特定事件）可能显示在事件视图中。即使已经为设备配置一个滑动时间窗，这种情况仍然可能发生。
了解有关表中各列的更多信息	在第 50-14 页上的了解发现事件表中获得详细信息。

要查看发现事件。

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Discovery Events**。

系统显示默认发现事件工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示任何事件，可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

了解发现事件表

许可证：FireSIGHT

系统生成变化详情在受监控网段中通信的发现事件。为新发现的网络功能生成*新的*事件，并为先前识别的网络资产的任何变化生成更改事件。

在初始网络发现阶段，系统为每台主机以及在每台主机发现的任何 TCP 或 UDP 服务器生成新的事件。此外，系统为在每台已发现主机上运行的每个网络、传送或应用协议生成新的事件。对于 NetFlow 相关的流量，可在系统检测到主机上有应用协议运行时控制系统是否生成新的事件。初次网络映射完成后，系统通过生成更改事件持续记录网络变化。无论先前发现的主机、服务器或客户端配置何时发生改变，系统都会生成更改事件。

以下对发现事件表中的字段进行了说明。

时间

系统生成事件的时间。

活动

事件类型。有关每个可用事件的说明，请参阅第 50-8 页上的了解发现事件类型和第 50-11 页上的了解主机输入事件类型。

IP地址

与事件所涉及主机关联的 IP 地址。

用户

事件生成前登录到事件所涉及的主机的最后一名用户。如果授权用户登录后只有未授权用户登录，除非其他授权用户登录，否则此授权用户仍是主机的当前用户。

MAC 地址

触发发现事件的网络流量所使用 NIC 的 MAC 地址。MAC 地址可以是事件所涉及的主机的实际 MAC 地址或者是有流量通过的网络设备的 MAC 地址。

MAC Vendor

触发发现事件的网络流量所使用 NIC 的 MAC 硬件供应商。

端口

如适用，是指触发此事件的流量所使用的端口。

说明

事件的文字说明。

设备

生成事件的设备的名称。对于基于 NetFlow 数据的新主机和新服务器事件，此设备是处理 NetFlow 数据的设备。

搜索发现事件

许可证：FireSIGHT

可搜索特定发现事件。您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 对于某些字段，可以在字段中指定 `n/a` 或 `blank` 识别信息不可用的字段的事件；使用 `!n/a` 或 `!blank` 识别已填入字段的事件。
- 大多数字段不区分大小写。
- 可以使用 CIDR 表示法指定 IP 地址。
- 使用设备字段搜索特定设备以及组、堆栈或集群中的设备。有关 FireSIGHT 系统如何处理搜索中的设备字段的详细信息，请参阅第 60-6 页上的在搜索中指定设备。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

发现事件的特殊搜索语法

下表注明了特定发现事件字段的搜索信息。有关发现事件字段的详细信息，请参阅第 50-18 页上的了解主机表。

表 50-3　　发现事件条件注释

字段	搜索条件注释
活动	第 50-8 页上的了解发现事件类型和第 50-11 页上的了解主机输入事件类型中列出了事件名称的范围
MAC Vendor	要搜索虚拟 MAC 供应商，即搜索涉及虚拟机的事件，请键入 `virtual_mac_vendor`。 要搜索名称包含逗号的供应商，请用引号将整个搜索术语引住。否则，防御中心 会将此术语视为两个搜索，并返回与每个搜索术语都匹配的事件。

表 50-3　　发现事件条件注释 （续）

字段	搜索条件注释
端口	注意不可以： • 搜索其他类型事件时输入能够输入的端口/协议组合 • 指定端口数或范围时，使用空格。

要搜索发现事件：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Discovery Events**。

页面根据相应限制进行更新。

步骤 3　按照第 50-15 页上的通用搜索语法和第 50-15 页上的发现事件的特殊搜索语法的说明，在相应的字段中输入的搜索条件。

如果您输入多个字段的条件，则搜索仅返回符合为所有字段指定的搜索条件的记录。点击在搜索字段旁边显示的添加图标 (+)，使用对象作为搜索条件。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

默认发现事件工作流程中显示搜索结果，这是由当前时间范围限制的。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

使用主机

许可证：FireSIGHT

系统检测到主机并采集其有关信息用于生成主机配置文件时，生成此事件。可使用防御中心网络界面查看，搜索和删除主机。

查看主机时，可根据所选主机创建流量量变曲线和合规性白名单。也可赋予主机属性，包括主机对于主机重要性。然后可使用这些关键性值、白名单和关联规则和策略中的流量量变曲线。

虽然可将网络发现策略配置为根据 NetFlow 支持设备导入的数据向网络映射添加主机，但关于这些主机的可用信息是有限的。例如，这些主机没有可用的操作系统数据，除非您使用主机输入功能提供这些数据。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

有关详细信息，请参阅以下各节：

查看主机

许可证：FireSIGHT

可使用防御中心查看列出了系统检测到的主机的表。然后，可根据要查找的信息操作视图。

访问主机时所看到的页面因所使用工作流程的不同而不同。两个预定义工作流程结束于主机视图中，该视图包含符合限制条件的每台主机的配置文件。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关详细信息，请参阅第 58-34 页上的创建自定义工作流程。

以下主机操作表说明可在主机工作流程页面执行的一些特定操作。也可执行常见发现事件操作表中所描述的任务。

表 50-4　　主机操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 50-18 页上的了解主机表中获得详细信息。
为所选主机赋予主机属性	在第 50-26 页上的为所选主机设置主机属性中获得详细信息。
为所选主机创建流量量变曲线	在第 50-20 页上的为所选主机创建流量量变曲线中获得详细信息。
根据所选主机创建合规性白名单	在第 50-21 页上的在所选主机上创建合规性白名单中获得详细信息。

要查看主机：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Hosts**.

系统显示默认主机工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

提示　如在使用的自定义工作流程不包括主机的表视图，请点击 **(switch workflow)**, ，然后选择 **Hosts**。

了解主机表

许可证：FireSIGHT

系统发现主机时，会采集有关此主机的数据。该数据可能包括主机的 IP 地址、其运行的操作系统等等。可在主机表视图中查看部分该信息。有关系统采集的所检测到主机的数据的详细信息，请参阅第 49-1 页上的使用主机配置文件。

以下对主机表中的字段进行了说明。

虽然可将网络发现策略配置为根据 NetFlow 支持设备导入的数据向网络映射添加主机，但关于这些主机的可用信息是有限的。例如，这些主机没有可用的操作系统数据，除非您使用主机输入功能提供这些数据。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

Last Seen

系统最后检测到的任何主机 IP 地址的日期和时间。至少应按网络发现策略中配置的更新间隔更新 Last Seen 值，另外当系统为任何主机 IP 地址生成新的主机事件时，也要执行该更新。

对于使用主机输入功能更新操作系统数据的主机， Last Seen 值表示最初添加数据的日期和时间。

IP地址

与主机关联的 IP 地址。

MAC 地址

检测到的主机 NIC 的 MAC 地址。

MAC Address 字段显示在主机表视图中，该视图可在主机工作流程中找到。也可将 MAC Address 字段添加至：

- 包括来自主机表的字段的自定义表
- 基于主机表的自定义工作流程中的向下钻取页面

MAC Vendor

检测到的主机 NIC 的 MAC 硬件供应商。

MAC Vendor 字段显示在主机表视图中，该视图可在主机工作流程中找到。也可将 MAC Vendor 字段添加至：

- 包括来自主机表的字段的自定义表
- 基于主机表的自定义工作流程中的向下钻取页面

Current User

主机当前登录用户的用户标识（用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，未授权用户是主机当前用户时，该用户仍不能进行用户管理。

Host Criticality

分配给主机的用户指定的关键性值。请参阅第 50-25 页上的了解主机属性表中 Host Criticality 列的说明，了解有关此字段的详细信息。

NetBIOS Name

主机的 NetBIOS 名称。只有运行 NetBIOS 协议的主机才有 NetBIOS 名称。

VLAN ID

主机使用的 VLAN ID。有关 VLAN ID 的详细信息，请参阅第 49-19 页上的使用主机配置文件中的 VLAN 标签。

跃点数

逐一检测主机的设备的网络跳数。

Host Type

主机类型 （主机、移动设备、越狱移动设备、路由器、网桥、 NAT 设备或负载均衡器）。系统用于区分网络设备的方法包括：

- 分析思科发现协议 (CDP) 消息，可识别网络设备及其类型 （仅限思科设备）
- 检测生成树协议 (STP)，可识别作为交换机或网桥的设备
- 检测使用同一 MAC 地址的多台主机，可用于识别 MAC 地址为属于路由器
- 检测客户端 TTL 值的变化或变化频率高于典型启动时间的 TTL 值，可用于识别 NAT 设备和负载均衡器

如果设备未被识别为网络设备，则归类为主机。

硬件

移动设备的硬件平台。

操作系统

检测到的在主机上运行的 （名称、供应商和版本）或使用 Nmap 或主机输入功能更新的操作系统。从控制面板上 Custom Analysis 构件中调用主机事件视图时，此字段显示。它也是基于主机表的自定义表中的一个字段选项。

注意：如果系统检测到多个标识，这些标识将显示在逗号分隔列表中。

在此字段中， `unknown` 值是指不与任何已知指纹匹配的操作系统。 `pending` 值表明系统尚未采集到足够的信息用于识别操作系统。

OS Vendor

主机上检测到的或使用 Nmap 或主机输入功能升级的的操作系统的供应商。

注意：如果系统检测到多个供应商，这些供应商将显示在逗号分隔列表中。

在此字段中， `unknown` 值是指不与任何已知指纹匹配的操作系统。 `pending` 值表明系统尚未采集到足够的信息用于识别操作系统。

OS Name

检测到的在主机上运行的或使用 Nmap 或主机输入功能更新的操作系统。

注意：如果系统检测到多个名称，这些名称将显示在逗号分隔列表中。

在此字段中， `unknown` 值是指不与任何已知指纹匹配的操作系统。 `pending` 值表明系统尚未采集到足够的信息用于识别操作系统。

操作系统版本

主机上检测到的或使用 Nmap 或主机输入功能升级的的操作系统的版本。

注意：如果系统检测到多个版本，这些版本将显示在逗号分隔列表中。

在此字段中，`unknown` 值是指不与任何已知指纹匹配的操作系统。`pending` 值表明系统尚未采集到足够的信息用于识别操作系统。

Source Type

下列值之一用做主机操作系统标识源：

- 用户：*`user_name`*
- 应用：*`app_name`*
- 扫描仪：*`scanner_type`*（通过网络发现配置添加的 Nmap 或扫描仪）
- FireSIGHT，对于系统检测到的操作系统

系统可能从多个源协调数据，以确定操作系统的标识；请参阅第 46-4 页上的了解当前标识。

信心

以下任一选项：

- 对于系统检测到的主机，指系统对在主机上运行的操作系统的标识的置信百分比
- 对于通过活跃源识别的操作系统，则为 100%，例如主机输入功能或 Nmap 扫描仪
- 对于系统不能确定操作系统标识的主机和根据 NetFlow 数据已添加到网络映射的主机，则为 `unknown`。

备注

注释主机属性的自定义内容。

设备

检测流量的受管设备或处理 NetFlow 或将主机添加至网络映射的主机输入数据的设备。

如果此字段为空，则如网络发现策略中所定义，主机已由并非显式监控主机所在网络的设备添加到网络映射，或使用主机输入功能添加了主机并且系统也尚未检测到该主机。

计数

与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

为所选主机创建流量量变曲线

许可证：FireSIGHT

流量量变曲线是以指定的时间跨度内采集的连接数据为基础的网络流量的配置文件。创建流量量变曲线后，可通过对照配置文件评估新流量的方式检测异常网络流量，新流量应代表正常网络流量。

可使用主机页面创建指定主机组的流量量变曲线。流量量变曲线以检测到的连接为基础，其中所指定主机之一是启动连接的主机。使用排序和搜索功能隔离要为其创建配置文件的主机。

要为所选主机创建流量量变曲线：

访问：管理

步骤 1　在主机工作流程的表视图中，选择要为其创建流量量变曲线的主机旁边的复选框。

步骤 2　在页面底部，点击 **Create Traffic Profile**。

系统显示填入了指定为受监控主机的主机 IP 地址的创建配置文件页面。

步骤 3　根据特定需要修改并保存流量量变曲线。

有关创建流量量变曲线的详细信息，请参阅第 53-1 页上的创建流量量变曲线。

在所选主机上创建合规性白名单

许可证：FireSIGHT

使用合规性白名单可以指定网络允许的操作系统、客户端和网络、传送或应用协议。

可在主机页面上根据指定的主机组的主机配置文件创建合规性白名单。使用排序和搜索功能隔离要用于创建白名单的主机。

要根据所选主机创建合规性白名单：

访问：管理

步骤 1　在主机工作流程的表视图中，选择要为其创建白名单的主机旁边的复选框。

步骤 2　在页面底部，点击 **Create White List**。

系统显示创建白名单页面，该页面上填入了指定主机的主机配置文件中的信息。

步骤 3　根据特定需要修改并保存白名单。

有关创建合规性白名单的详细信息，请参阅第 52-7 页上的创建合规白名单。

搜索主机

许可证：FireSIGHT

可通过使用预定义搜索条件之一或使用自定义的搜索条件搜索特定主机。

搜索主机时，请谨记，虽然可将网络发现策略配置为根据 NetFlow 支持设备导入的数据向网络映射添加主机，但关于这些主机的可用信息是有限的。例如，这些主机没有可用的操作系统数据，除非您使用主机输入功能提供这些数据。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

可搜索特定发现事件。您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B` 或同时包含 `C`、`D` 和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 对于某些字段，可以在字段中指定 `n/a` 或 `blank` 识别信息不可用的字段的事件；使用 `!n/a` 或 `!blank` 识别已填入字段的事件。
- 大多数字段不区分大小写。
- 可以使用 CIDR 表示法指定 IP 地址。有关在 FireSIGHT 系统中输入 IP 地址的详细信息，请参阅第 1-16 页上的 IP 地址约定。

注 按 IP 地址搜索主机时，结果包括至少有一个 IP 地址与搜索条件匹配的所有主机，即搜索 IPv6 地址可能会返回原地址是 IPv4 的主机。

- 使用设备字段搜索特定设备以及组、堆栈或集群中的设备。有关 FireSIGHT 系统如何处理搜索中的设备字段的详细信息，请参阅第 60-6 页上的在搜索中指定设备。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

适用于主机的特定搜索语法

下表注明了特殊主机字段的特定搜索信息。有关主机字段的详细信息，请参阅第 50-18 页上的了解主机表。

表 50-5　　主机搜索条件

字段	搜索条件注释
Host Type	要搜索所有网络设备，请键入 `!host`。
MAC Vendor	要搜索虚拟 MAC 供应商，即搜索涉及虚拟机的事件，请键入 `virtual_mac_vendor`。 要搜索名称包含逗号的供应商，请用引号将整个搜索术语引住。否则，防御中心 会将此术语视为两个搜索，并返回与每个搜索术语都匹配的事件。
OS Vendor/Name/Version	键入 `unknown` 搜索操作系统未知的主机。键入 `n/a` 搜索操作系统尚未识别出的主机。

表 50-5　　主机搜索条件 （续）

字段	搜索条件注释
信心	可在置信前面加上大于 (>)、大于或等于 (>=)、小于 (<)、小于或等于 (<=) 或等于 (=) 运算符。 与 n/a 搜索匹配的项包括根据 NetFlow 数据添加至网络映射的主机。
OS Conflict	注意：搜索结果中不显示 OS 冲突列。要确定在查看的主机是否有操作系统冲突，请展开工作流程页面上搜索限制条件。有关解决操作系统冲突的详细信息，请参阅第 49-12 页上的解决操作系统的标识冲突。

有关搜索的详细信息，包括如何加载和删除已保存搜索，请参阅第 60-1 页上的搜索事件。

要搜索主机：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉菜单中选择 **Hosts**。

页面根据相应限制进行更新。

提示　要在数据库中搜索另一类型的事件，请从表下拉列表选择它。

步骤 3　在相应字段中输入搜索条件，如主机搜索条件表中所述。

如果您输入多个字段的条件，则防御中心仅返回符合为所有字段指定的搜索条件的记录。点击在搜索字段旁边显示的添加图标 (+)，使用对象作为搜索条件。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如果要将搜索另存为对权限有限的自定义用户角色的约束，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认主机工作流程中。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

使用主机属性

许可证：FireSIGHT

FireSIGHT 系统采集有关主机检测和使用其生成主机配置文件的信息。但是，可能会有要提供给分析师的有关网络上主机的附加信息。可在主机配置文件中添加注释，设置主机的业务关键性或提供您所选择的任何其他信息。每个信息都称为主机属性。

可在主机配置文件限制中使用主机属性，用于生成流量量变曲线时限制所采集的数据，也可限制用于触发关联规则的条件。也对应关联规则设置属性值。

有关详情，请参阅：

- 第 50-24 页上的查看主机属性
- 第 50-25 页上的了解主机属性表
- 第 50-26 页上的为所选主机设置主机属性
- 第 50-26 页上的搜索主机属性
- 第 54-14 页上的配置设定的属性补救

查看主机属性

许可证：FireSIGHT

可使用防御中心查看系统检测到的主机表，与他们的主机属性。然后，可根据要查找的信息操作视图。

访问主机属性时所看到的页面因所使用工作流程的不同而不同。可使用预定义工作流程，此流程包括列出了所有检测到的主机及其属性的主机属性表视图，并在主机视图页面结束，此页面包含符合限制条件的每台主机的主机配置文件。

您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关创建自定义工作流程的信息，请参阅第 58-34 页上的创建自定义工作流程。

下表主机属性操作说明可在主机属性工作流程页面进行的某些特定操作。也可执行常见发现事件操作表中所描述的任务。

表 50-6　　主机属性操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 50-25 页上的了解主机属性表中获得详细信息。
为所选主机赋予主机属性	在第 50-26 页上的为所选主机设置主机属性中查找详细信息。

要查看主机属性：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Host Attributes**。

系统显示默认主机属性工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

提示　如在使用的自定义工作流程不包括主机属性的表视图，请点击 **(switch workflow)**，然后选择 **Attributes**。

了解主机属性表

许可证：FireSIGHT

FireSIGHT 系统采集有关主机检测和使用其生成主机配置文件的信息。但是，可能会有要提供给分析师的有关网络上主机的附加信息。可为主机配置文件添加注释，设置业务关键性或提供所选择的任何其他信息。每个信息都称为主机属性。

可在主机配置文件限制中使用主机属性，用于生成流量量变曲线时限制所采集的数据，也可限制用于触发关联规则的条件。

注意主机属性表不显示仅通过 MAC 地址识别的主机。

有关主机属性的详细信息，请参阅第 49-27 页上的使用预先定义的主机属性和第 49-27 页上的使用用户定义的主机属性。

以下对主机属性表中的字段进行了说明。

IP地址

与主机关联的 IP 地址。

Current User

主机当前登录用户的用户标识 （用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，未授权用户是主机当前用户时，该用户仍不能进行用户管理。

Host Criticality

用户赋予主机对于您所在企业的重要性。可在关联规则和策略中使用主机重要性用于修改策略违规和对事件中所涉及主机重要性的响应。可封皮低级、中级、高级或零级主机重要性。

有关设置主机重要性的详细信息，请参阅第 49-27 页上的使用预先定义的主机属性和第 50-26 页上的为所选主机设置主机属性。

备注

有关希望其他分析师查看的主机的信息。有关如何添加注释的详细信息，请参阅第 49-27 页上的使用预先定义的主机属性。

所有自定义主机属性，包括适用于合规性白名单的属性。

自定义主机属性值。

主机属性表包括每个自定义主机属性的字段。有关详细信息，请参阅第 49-27 页上的使用用户定义的主机属性。

计数

与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

为所选主机设置主机属性

许可证：FireSIGHT

可分配给每台主机的预定义主机属性有两个：主机重要性和主机特定注释。

使用主机重要性标明给定主机的业务关键性。可根据主机重要性修改关联策略和警报。例如，对于业务来说，您所在组织的邮件服务器比典型用户工作站更为重要。可赋予邮件服务器和其他关键业务服务器高级主机重要性值，赋予其它主机中级或低级关键性值。然后可根据受影响主机的关键性创建发出不同警报的关联策略。

使用注释记录有关希望其他分析师查看的主机的信息。例如，如果网络上有使用测试用旧版未打补丁操作系统的计算机，可使用注释功能注明此系统特意未打补丁。

也可创建自定义主机属性。例如，可创建为主机分配物理位置标识的主机属性，例如设备代码、城市或房间号。有关创建自定义主机属性的详细信息，请参阅第 49-28 页上的创建用户定义的主机属性。

也可在主机工作流程中从主机配置文件内部设置所选主机的主机重要性，或通过修复设置。有关详细信息，请参阅第 49-27 页上的使用预先定义的主机属性或第 54-14 页上的配置设定的属性补救。

为所选主机设置主机属性：

访问：管理员/任何安全分析师

步骤 1　选择要添加主机属性的主机旁边的复选框。

提示　使用排序和搜索功能隔离要为其分配特定属性的主机。

步骤 2　在页面底部，点击 **Set Attributes**。

系统将显示 Host Attributes 弹出窗口。

步骤 3　或者，为所选主机设置主机重要性。

可选择 **None**、 **Low**、 **Medium** 或 **High**。

步骤 4　或者，向所选主机的主机配置文件添加注释，只需在文本框中输入最多 255 个字符，包括字母数字、特殊字符和空格。

步骤 5　或者，设置已配置的任何用户定义的主机属性。

步骤 6　点击 **Save**。

指定的主机属性已分配给所选主机。

搜索主机属性

许可证：FireSIGHT

可搜索具有特定主机属性的主机。例如，如果公司有多个区域办公室，可通过配置主机属性了解任何一台主机所在的城市。然后可搜索特定区域的主机。有关主机属性的详细信息，请参阅第 49-27 页上的使用用户定义的主机属性。

您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。有关主机属性字段的详细信息，请参阅第 50-25 页上的了解主机属性表。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B` 或同时包含 `C`、`D` 和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 对于某些字段，可以在字段中指定 `n/a` 或 `blank` 识别信息不可用的字段的事件；使用 `!n/a` 或 `!blank` 识别已填入字段的事件。
- 大多数字段不区分大小写。
- 可以使用 CIDR 表示法指定 IP 地址。有关在 FireSIGHT 系统中输入 IPv4 和 IPv6 地址的详细信息，请参阅第 1-16 页上的 IP 地址约定。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

要搜索主机属性：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Host Attributes**。

页面根据相应限制进行更新。

提示　要在数据库中搜索另一类型的事件，请从表下拉列表选择它。

步骤 3　按了解主机属性表中所述，在相应的字段中输入搜索条件。

如果您输入多个字段的条件，则搜索仅返回符合为所有字段指定的搜索条件的记录。点击在搜索字段旁边显示的添加图标 (✚)，使用对象作为搜索条件。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如果要将搜索另存为对权限有限的自定义用户角色的约束，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认主机属性工作流程中。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

使用危害表现

许可证：FireSIGHT

FireSIGHT 系统将与主机有关的各种类型的数据 （入侵事件、安全情报、连接事件和文件或恶意软件事件）关联起来，以确定受监控网络上的主机是否可能被恶意手段损害。事件数据的某些组合和频率触发了受影响主机上的危害表现 (IOC) 标记。有 IOC 标记的主机的 IP 地址显示在有特殊危害主机图标 ( ) 的事件视图中；也可写入对有 IOC 标记的主机进行说明的合规性规则。

要使用此功能，必须在网络发现策略中启用 IOC 规则。可启用任何或所有预定义规则，以触发危害主机上的 IOC 标记。有关详细信息，请参阅第 45-29 页上的设置危害表现规则。

有关危害表现的详细信息，请参阅：

- 第 50-28 页上的查看危害表现
- 第 50-29 页上的了解危害表现表
- 第 50-30 页上的搜索危害表现

查看危害表现

许可证：FireSIGHT

可使用防御中心查看已触发危害表现 (IOC) 表。然后，可根据要查找的信息操纵事件视图。

访问 IOC 时所看到的页面因所使用的工作流程的而异。两个预定义的 IOC 工作流程均在主机视图中终止，该主机视图包含符合限制条件的每台主机的主机配置文件。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关详细信息，请参阅第 58-34 页上的创建自定义工作流程。

下表说明了可在 IOC 工作流程页面上执行的一些特定操作。也可执行常见发现事件操作表中所描述的任务。

表 50-7　　危害表现操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 50-29 页上的了解危害表现表中获得详细信息。
查看受损主机的主机配置文件	在 **IP Address** 列中，点击危害主机图标 ( )。

表 50-7　危害表现操作 （续）

要.....	您可以.....
将所选 IOC 事件标记为已解决，这样他们就不会再出现在此列表中。	选择要编辑的 IOC 事件旁边的复选框，然后点击 **Mark Resolved**。有关详细信息，请参阅第 49-9 页上的解决危害表现。
查看触发 IOC 的事件的详细信息	在 **First Seen** 或 **Last Seen** 列中，点击视图图标 ( )。

要查看危害表现，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Indications of Compromise**。

系统显示默认危害表现 (IOC) 工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

提示　如在使用的自定义工作流程不包括 IOC 表视图，请点击 **(switch workflow)**，然后选择 **Indications of Compromise**。

了解危害表现表

许可证：FireSIGHT

FireSIGHT 系统 将与主机相关的各种类型的事件数据关联起来，以确定受监控网络上的主机是否可能被恶意手段损害。与主机关联的这些相关性显示为危害表现 (IOC)。可将主机 IOC 标记为已解决，这样可从主机清除此 IOC 标记。主机可触发多个 IOC 标记；可查看与主机配置文件的“危害表现”部分中的主机关联的所有 IOC 标记。有关主机配置文件中 IOC 数据的详细信息，请参阅第 49-7 页上的使用主机配置文件中的危害表现。

以下对 IOC 表中的字段进行了说明。

IP地址

与触发 IOC 的主机关联的 IP 地址。

类别

所指示危害类型的简要说明，例如 `Malware Executed` 或 `Impact 1 Attack`。

事件类型

与特定危害表现 (IOC) 关联的标识符，指触发该标识的事件。

说明

说明 IOC 对于潜在危害主机的意义，例如此主机可能受到远程控制或已针对此主机执行了恶意软件。

First/Last Seen

触发主机 IOC 的事件的第一次出现 （或最近）日期和时间。

搜索危害表现

许可证：FireSIGHT

可通过使用预定义搜索之一或使用自己的搜索条件搜索受监控主机上已触发的特定危害表现 (IOC) 标记。预定义搜索用作示例，可用于快速访问关于网络的重要信息。

您可能想要修改默认搜索中的特定字段，以根据网络环境对它们进行自定义，然后保存以便日后重复使用。第 50-29 页上的了解危害表现表 中对可用于检索数据的字段进行了说明。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 对于某些字段，可以在字段中指定 `n/a` 或 `blank` 识别信息不可用的字段的事件；使用 `!n/a` 或 `!blank` 识别已填入字段的事件。
- 大多数字段不区分大小写。
- 可以使用 CIDR 表示法指定 IP 地址。有关在 FireSIGHT 系统中输入 IPv4 和 IPv6 地址的详细信息，请参阅第 1-16 页上的 IP 地址约定。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

要搜索危害表现，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Indications of Compromise**。

页面根据相应限制进行更新。

提示　要在数据库中搜索另一类型的事件，请从表下拉列表选择它。

步骤 3　按第 50-29 页上的了解危害表现表中所述，在相应的字段中输入搜索条件。

如果您输入多个字段的条件，则搜索仅返回符合为所有字段指定的搜索条件的记录。点击在搜索字段旁边显示的添加图标 (✚)，使用对象作为搜索条件。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如果要将搜索另存为对权限有限的自定义用户角色的约束，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认 IOC 工作流程中。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

使用服务器

许可证：FireSIGHT

FireSIGHT 系统 采集有关在受监控网段主机上运行的所有服务器的信息。系统采集的信息包括服务器名称、服务器使用的应用和网络协议、服务器供应商和版本、与运行服务器的主机相关的 IP 地址以及服务器通信端口。

系统检测到服务器时，生成发现事件，除非关联的主机已达到其最大服务器数量。有关详细信息，请参阅第 45-11 页上的主机限制和发现事件日志记录。可使用防御中心网络界面查看、搜索和删除服务器事件。

关联规则也可基于服务器事件。例如，可在系统检测到其中一台主机上有聊天服务器运行时触发关联规则，例如 ircd。

虽然可将网络发现策略配置为根据 NetFlow 支持设备导入的应用数据向网络映射添加服务器，但关于这些服务器的可用信息是有限的。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

有关详细信息，请参阅以下各节：

- 第 50-32 页上的查看服务器
- 第 50-32 页上的了解服务器表
- 第 50-34 页上的搜索服务器
- 第 49-16 页上的编辑服务器标识

查看服务器

许可证：FireSIGHT

可使用防御中心查看检测到的服务器表。然后，可根据要查找的信息操纵事件视图。

访问服务器时所看到的页面因所使用的工作流程的而异。所有预定义的工作流程均在主机视图中终止，该主机视图包含符合限制条件的每台主机的主机配置文件。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关详细信息，请参阅第 58-34 页上的创建自定义工作流程。

以下服务器操作表对说明可在服务器工作流程页面执行的一些特定操作。也可执行常见发现事件操作表中所描述的任务。

表 50-8　　服务器操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 50-32 页上的了解服务器表中获得详细信息。
编辑服务器标识	选择要编辑的服务器事件旁边的复选框，然后点击 **Set Server Identity**。有关详细信息，请参阅第 49-16 页上的编辑服务器标识。

要查看服务器：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Hosts**。

系统显示默认服务器工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

提示　如在使用的自定义工作流程不包括服务器的表视图，请点击 **(switch workflow)**，然后选择 **Hosts**。

了解服务器表

许可证：FireSIGHT

FireSIGHT 系统 采集有关在受监控网段主机上运行的服务器的信息。

以下对服务器表中的字段进行了说明。

虽然可将网络发现策略配置为根据 NetFlow 支持设备导入的数据向网络映射添加服务器，但关于这些服务器的可用信息是有限的。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

Last Used

服务器在网络上最后一次使用的日期和时间或使用主机输入功能初始更新服务器的日期和时间。至少按网络发现策略中配置的更新间隔更新 Last Used 值，当系统检测到服务器信息更新时也更新该值。有关设置更新间隔的详细信息，请参阅第 45-30 页上的配置数据存储。

IP地址

与运行服务器的主机关联的 IP 地址。

端口

服务器运行所在端口。

协议

服务器使用的网络或传输协议。

Application Protocol

应用协议如下列其中一项所述：

- 服务器应用协议的名称。
- 如果系统由于几个原因之一无法积极地或消极地识别服务器，则为 `pending`。
- 如果系统无法根据已知服务器指纹识别服务器或者服务器是通过主机输入添加的且不包括应用协议，则为 `unknown`。

应用协议的类别、标记、风险或业务相关性。

已分配给应用协议的分类、标记、风险级别和业务相关性。这些过滤器可用于集中过滤特定数据集。有关详细信息，请参阅第 45-9 页上的表 45-2。

供应商

以下任一选项：

- 系统、 Nmap 或其他活跃源识别的服务器供应商或者使用主机输入功能指定的服务器供应商
- 如果系统无法根据已知服务器指纹识别其供应商或者服务器是使用 NetFlow 数据添加至网络映射的，则为 blank。

版本

以下任一选项：

- 系统、 Nmap 或其他活跃源识别的服务器版本或者使用主机输入功能指定的服务器版本
- 如果系统无法根据已知服务器指纹识别其版本或者服务器是使用 NetFlow 数据添加至网络映射的，则为 blank。

Web Application

基于系统在 http 流量中检测到的负载内容的网络应用。注意，如果系统检测到 `HTTP` 应用协议，但无法检测到特定网络应用，则系统提供通用网络浏览名称。

Category、 Tags、 Risk 或者 Business Relevance for Web Applications

分配给网络应用的分类、标记、风险级别和业务相关性。这些过滤器可用于集中过滤特定数据集。有关详细信息，请参阅第 45-9 页上的表 45-2。

Hits

服务器被访问的次数。对于使用主机输入功能添加的服务器，此值始终为 0。

Source Type

选择以下值之一：

- 用户：*`user_name`*
- 应用：*`app_name`*

– 扫描仪：*scanner_type*（通过网络发现配置添加的 Nmap 或扫描仪）
– 对于 FireSIGHT 系统检测到的服务器，应为 FireSIGHT、 FireSIGHT Port Match 或 FireSIGHT Pattern Match
– 对于根据 NetFlow 数据添加至网络映射的服务器，为 NetFlow

系统可能从多个源协调数据，以确定服务器的标识；请参阅第 46-4 页上的了解当前标识。

设备

检测到服务器或处理 NetFlow 或主机输入数据且将服务器添加至网络映射的设备的名称。

Current User

主机当前登录用户的用户标识（用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，未授权用户是主机当前用户时，该用户仍不能进行用户管理。

计数

与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

搜索服务器

许可证：FireSIGHT

可通过预定义搜索条件之一或使用自己的搜索条件搜索在受监控主机上运行的特定服务器。预定义搜索用作示例，可用于快速访问关于网络的重要信息。

您可能想要修改默认搜索中的特定字段，以根据网络环境对它们进行自定义，然后保存以便日后重复使用。第 50-32 页上的了解服务器表 中对可用于检索数据的字段进行了说明。

搜索服务器时，请谨记，虽然可将网络发现策略配置为根据 NetFlow 支持设备导入的数据向网络映射添加应用，包括服务器，但关于这些服务器的可用信息是有限的。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  – 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  – 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  – 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、 `D`和 `E`。

- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 对于某些字段，可以在字段中指定 `n/a` 或 `blank` 识别信息不可用的字段的事件；使用 `!n/a` 或 `!blank` 识别已填入字段的事件。
- 大多数字段不区分大小写。
- 可以使用 CIDR 表示法指定 IP 地址。有关在 FireSIGHT 系统中输入 IPv4 和 IPv6 地址的详细信息，请参阅第 1-16 页上的 IP 地址约定。
- 使用设备字段搜索特定设备以及组、堆栈或集群中的设备。有关 FireSIGHT 系统如何处理搜索中的设备字段的详细信息，请参阅第 60-6 页上的在搜索中指定设备。
- 点击搜索字段旁边的添加对象图标 (+)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

要搜索服务器：

访问：管理员/任何安全分析师

步骤 1 选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2 从表下拉列表中选择 **Servers**。

页面根据相应限制进行更新。

提示 要在数据库中搜索另一类型的事件，请从表下拉列表选择它。

步骤 3 在相应字段输入搜索条件。

如果您输入多个字段的条件，则搜索仅返回符合为所有字段指定的搜索条件的记录。点击在搜索字段旁边显示的添加图标 (+)，使用对象作为搜索条件。

步骤 4 如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示 如果要将搜索另存为对权限有限的自定义用户角色的约束，**必须**将其另存为私有搜索。

步骤 5 或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6 点击 **Search** 开始搜索。

搜索结果显示在默认服务器工作流程中。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

使用应用

许可证：FireSIGHT

当受监控主机连接到另一台主机时，在许多情况下，系统可以确定所使用的应用。 FireSIGHT 系统检测许多邮件、即时消息、对等设备、网络应用以及其他类型的应用的使用情况。

对于每个检测到的应用，系统均将记录使用该应用的 IP 地址、产品、版本和检测到的使用次数。可使用网络界面查看、搜索和删除应用事件。也可在主机上使用主机输入功能更新应用数据。

如果知道哪些应用在哪些主机上运行，则可使用此信息创建主机配置文件限制，以便在构建流量量变曲线时限制所采集的数据，也可限制用于触发关联规则的条件。关联规则也可基于应用检测。例如，如果希望员工使用特定邮件客户端，可在系统检测到一台主机上有不同的邮件客户端运行时触发关联规则。

应仔细阅读每个 FireSIGHT 系统更新的版本说明以及每次 VDB 更新的公告以便获得有关已更新检测器的信息。

要采集和存储应用数据用于分析，请确保在网络发现策略中启用应用检测。有关详细信息，请参阅第 45-1 页上的了解发现数据收集。

有关详细信息，请参阅：

- 第 50-40 页上的查看应用详情
- 第 50-40 页上的了解应用详情表
- 第 50-42 页上的搜索应用详情

查看应用

许可证：FireSIGHT

可使用防御中心查看检测到的应用表。然后，可根据要查找的信息操纵事件视图。

访问应用时所看到的页面因所使用的工作流程而异。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关详细信息，请参阅第 58-34 页上的创建自定义工作流程。

以下应用操作表说明可在应用工作流程页面执行的一些特定操作。也可执行常见发现事件操作表中所描述的任务。

表 50-9　　应用操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 50-37 页上的了解应用表中获得详细信息。
打开特定应用的应用详情视图	点击客户端、应用协议或网络应用旁边的应用详情视图图标 ( )。

要查看应用：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Application Details**。

系统显示默认应用详情工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

提示　如在使用的自定义工作流程不包括应用详情表视图，请点击 **(switch workflow)**，然后选择 **Clients**。

了解应用表

许可证：FireSIGHT

当受监控主机连接至另一台主机时，在许多情况下， FireSIGHT 系统可确定所使用是的什么应用。系统检测各种网络浏览器或服务器、邮件客户端或服务器、即时消息工具、 P2P 应用等。系统检测已知客户端流量、应用协议或网络应用时，会记录有关该应用及运行该应用的主机的信息。

FireSIGHT 系统将应用数据分为三类：客户端、网络应用和应用协议。应用表提供的列表组合了设备上已检测到的所有三种类型的应用。

以下对应用表中的字段进行了说明。

应用

检测到的应用的名称。

IP地址

与使用应用的主机关联的 IP 地址。

Category

说明应用的最基本功能的应用通用分类。每个应用都至少归属于一个类别。

Tag

有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。

Risk

应用被用于可能违反组织安全策略之目的的可能性。应用风险的取值范围为 `Very Low` 到 `Very High`。

在应用协议风险、客户端风险和网络应用风险中，如适用，则是触发入侵事件的流量中检测到的三个风险中级别最高的风险。

Business Relevance

应用被用于组织的企业运营中 （而不是被用于娱乐目的）的可能性。应用的业务相关性的取值范围为 `Very Low` 到 `Very High`。

在应用协议业务相关性、客户端业务相关性和网络应用业务相关性中，如适用，则是触发入侵事件的流量中检测到的三个业务关联性中关联性最低的一个。

Current User

主机当前登录用户的用户标识 （用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，未授权用户是主机当前用户时，该用户仍不能进行用户管理。

类型

应用类型：

- **Application Protocols** 代表主机之间的通信。
- **Client Applications** 代表在主机上运行的软件。
- **Web Applications** 代表 HTTP 流量的内容或请求 的 URL。

计数

与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

搜索应用

许可证：FireSIGHT

可搜索运行特定客户端、应用协议或网络应用的主机。您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、 `D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 对于某些字段，可以在字段中指定 `n/a` 或 `blank` 识别信息不可用的字段的事件；使用 `!n/a` 或 `!blank` 识别已填入字段的事件。
- 大多数字段不区分大小写。
- 可以使用 CIDR 表示法指定 IP 地址。有关在 FireSIGHT 系统中输入 IPv4 和 IPv6 地址的详细信息，请参阅第 1-16 页上的 IP 地址约定。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

要搜索应用：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Applications**。

页面根据相应限制进行更新。

步骤 3　在相应字段输入搜索条件。

如果您输入多个字段的条件，则搜索仅返回符合为所有字段指定的搜索条件的记录。点击在搜索字段旁边显示的添加图标 (+)，使用对象作为搜索条件。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如果要将搜索另存为对权限有限的自定义用户角色的约束，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认客户端工作流程中。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

使用应用详情

许可证：FireSIGHT

当受监控主机连接到另一台主机时，在许多情况下，系统可以确定所使用的应用。 FireSIGHT 系统检测许多邮件、即时消息、对等设备、网络应用以及其他类型的应用的使用情况。

对于每个检测到的应用，系统均将记录使用该应用的 IP 地址、产品、版本和检测到的使用次数。可使用网络界面查看、搜索和删除应用事件。也可在主机上使用主机输入功能更新应用数据。

如果知道哪些应用在哪些主机上运行，则可使用此信息创建主机配置文件限制，以便在构建流量量变曲线时限制所采集的数据，也可限制用于触发关联规则的条件。关联规则也可基于应用检测。例如，如果希望员工使用特定邮件客户端，可在系统检测到一台主机上有不同的邮件客户端运行时触发关联规则。

应仔细阅读每个 FireSIGHT 系统更新的版本说明以及每次 VDB 更新的公告以便获得有关已更新检测器的信息。

要采集和存储应用数据用于分析，请确保在网络发现策略中启用应用检测。有关详细信息，请参阅第 45-9 页上的了解应用检测。

有关详细信息，请参阅以下各节：

查看应用详情

许可证：FireSIGHT

可使用防御中心查看检测到的应用详情表。然后，可根据要查找的信息操纵事件视图。

访问应用详情时看到的页面因使用的工作流程而异。有两个预定义工作流程。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关详细信息，请参阅第 58-34 页上的创建自定义工作流程。

以下应用详情操作表说明可在应用详情工作流程页面执行的一些特定操作。也可执行常见发现事件操作表中所描述的任务。

表 50-10　　应用详情操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 50-40 页上的了解应用详情表中获得详细信息。
打开特定应用的应用详情视图	点击客户端旁边的应用详细视图图标 ( )。

要查看应用详情：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Hosts > Application Details**。

系统显示默认应用详情工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

提示　如在使用的自定义工作流程不包括应用详情表视图，请点击 **(switch workflow)**，然后选择 **Clients**。

了解应用详情表

许可证：FireSIGHT

当受监控主机连接至另一台主机时，在许多情况下， FireSIGHT 系统可确定所使用是的什么应用。系统检测各种网络浏览器、邮件客户端、即时消息工具、 P2P 应用等，。

系统检测已知客户端流量、应用协议或网络应用时，会记录有关该应用及运行该应用的主机的信息。以下对应用详情表中的字段进行了说明。

Last Used

最后一次检测到该应用的时间或使用主机输入功能更新该应用的数据的时间。至少按网络发现策略中配置的更新间隔更新 Last Used 值，当系统检测到应用信息更新时也更新该值。有关设置更新间隔的详细信息，请参阅第 45-30 页上的配置数据存储。

IP地址

与使用应用的主机关联的 IP 地址。

Client

应用的名称。注意：如果系统检测到应用协议但无法检测到特定客户端，则 `client` 会附加至应用协议名称以提供通用名。

版本

应用的版本。

Category、 Tags、 Risk 或 Business Relevance for Clients、 Application Protocols 和 Web Applications

分配给应用的分类、标记、风险级别和业务相关性。这些过滤器可用于集中过滤特定数据集。有关详细信息，请参阅第 45-9 页上的表 45-2。

Application Protocol

应用所使用的应用协议。注意：如果系统检测到应用协议但无法检测到特定客户端，则 `client` 会附加至应用协议名称以提供通用名。

Web Application

基于系统在 http 流量中检测到的负载内容或 URL 的网络应用。注意，如果系统检测到 `HTTP` 应用协议，但无法检测到特定网络应用，则系统在此提供通用网络浏览名称。

Hits

系统检测到在使用的应用的次数。对于使用主机输入功能添加的应用，此值始终为 `0`。

设备

生成发现事件的设备，包括应用详情。

Current User

主机当前登录用户的用户标识 （用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，未授权用户是主机当前用户时，该用户仍不能进行用户管理。

计数

与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

搜索应用详情

许可证：FireSIGHT

可搜索运行特定客户端、应用协议或网络应用的主机。您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 对于某些字段，可以在字段中指定 `n/a` 或 `blank` 识别信息不可用的字段的事件；使用 `!n/a` 或 `!blank` 识别已填入字段的事件。
- 大多数字段不区分大小写。
- 可以使用 CIDR 表示法指定 IP 地址。有关在 FireSIGHT 系统中输入 IPv4 和 IPv6 地址的详细信息，请参阅第 1-16 页上的 IP 地址约定。
- 使用设备字段搜索特定设备以及组、堆栈或集群中的设备。有关 FireSIGHT 系统如何处理搜索中的设备字段的详细信息，请参阅第 60-6 页上的在搜索中指定设备。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

要搜索应用详情：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Application Details**。

页面根据相应限制进行更新。

提示　要在数据库中搜索另一类型的事件，请从表下拉列表选择它。

步骤 3　在相应字段输入搜索条件。

如果您输入多个字段的条件，则搜索仅返回符合为所有字段指定的搜索条件的记录。点击在搜索字段旁边显示的添加图标 (＋)，使用对象作为搜索条件。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如果要将搜索另存为对权限有限的自定义用户角色的约束，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认应用详情工作流程中。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

使用漏洞

许可证：FireSIGHT

FireSIGHT 系统有自己的漏洞跟踪数据库，该数据库与系统的指纹识别功能相结合，以识别与网络中主机关联的漏洞。

主机上运行的操作系统、服务器和客户端有不同组关联漏洞。为主机安装修复程序后可停用其漏洞或者将其判断为漏洞免疫。可使用防御中心跟踪和审查每台主机的漏洞。

注意，除非系统策略中映射了服务器所使用的应用协议，否则不会映射无供应商和无版本服务器的漏洞。无法映射无供应商和无版本客户端的漏洞。有关详细信息，请参阅第 63-27 页上的映射服务器的漏洞。

有关详情，请参阅：

查看漏洞

许可证：FireSIGHT

可使用防御中心查看漏洞表。然后，可根据要查找的信息操纵事件视图。

访问漏洞时所看到的页面因所使用的工作流程而异。可使用包含漏洞表视图的预定义工作流程。数据库中的每个漏洞在表视图中都各占一行，无论任何检测到的主机是否显示这些漏洞。适用于网络中所检测到主机的每个漏洞 （未停用）在预定义工作流程的第二页都各占一行。预定义工作流程在漏洞详情视图中终止，该视图包含符合限制条件的每个漏洞的详细说明。

提示 如要查看适用于单台主机或一组主机的漏洞，应通过指定主机 IP 地址或 IP 地址范围的方式执行漏洞搜索。有关搜索漏洞的详细信息，请参阅第 50-46 页上的搜索漏洞。

您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关创建自定义工作流程的信息，请参阅第 58-34 页上的创建自定义工作流程。

下表说明了可在漏洞工作流程页面上执行的一些特定操作。也可执行常见发现事件操作表中所描述的任务。

表 50-11　　漏洞操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 50-45 页上的了解漏洞表中获得详细信息。
查看漏洞的漏洞详情	点击 SVID 列中的视图图标 ( )。或者，限制漏洞 ID 并向下钻取至漏洞详情页面。有关详细信息，请参阅第 49-24 页上的查看漏洞细节。
停用所选漏洞，以使这些漏洞不再用于当前有漏洞主机的入侵影响关联。	在第 50-46 页上的停用漏洞中获得详细信息。
查看漏洞标题的完整文本	右键点击标题并选择 **Show Full Text**。

要查看漏洞：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Vulnerabilities > Vulnerabilities**。

系统显示默认漏洞工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

提示 如在使用的自定义工作流程不包括漏洞的表视图，请点击 **(switch workflow)**，然后选择 **Vulnerabilities**。

了解漏洞表

许可证：FireSIGHT

FireSIGHT 系统有自己的漏洞跟踪数据库，该数据库与系统的指纹识别功能相结合，以识别与网络中主机关联的漏洞。

主机上运行的操作系统、服务器和客户端有不同组关联漏洞。为主机安装修复程序后可停用其漏洞或者将其判断为漏洞免疫。可使用防御中心跟踪和审查每台主机的漏洞。

有关漏洞的详细信息，请参阅第 48-6 页上的使用漏洞网络映射和第 49-23 页上的使用主机配置文件中的漏洞。

以下对漏洞表中的字段进行了说明。

SVID

系统用于跟踪漏洞的思科漏洞标识号。

点击视图图标 ( ) 访问 SVID 的漏洞详情。有关详情，请参见第 49-24 页上的查看漏洞细节。

Bugtraq ID

与 Bugtraq 数据库中漏洞关联的标识号。 (http://www.securityfocus.com/bid/)

Snort ID

与 Snort ID (SID) 数据库中漏洞关联的标识号。也就是说，如果入侵规则能检测利用特殊漏洞的网络流量，则此漏洞与入侵规则的 SID 关联。

注意，一个漏洞可能与多个 SID （或根本不与 SID）关联。如果一个漏洞与多个 SID 关联，则每个 SID 在漏洞表中各占一行。

职位

漏洞的标题。

IP地址

与受漏洞影响主机关联的 IP 地址。

Date Published

发布漏洞的日期。

Vulnerability Impact

显示分配给 Bugtraq 数据库中漏洞的严重性，等级从 0 级至 10 级，10 级最严重。漏洞影响是由 Bugtraq 条目编者根据其最佳判断并按照 SANS 重要漏洞分析 (CVA) 标准确定的。

远程

表示漏洞是否可以远程利用。

Available Exploits

表示是否有已知漏洞利用。

说明

漏洞的简要说明。

Technical Description

漏洞的详细技术说明。

解决方案

有关修补漏洞的信息。

计数

与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

停用漏洞

许可证：FireSIGHT

为网络中主机安装修复程序后停用漏洞或者将其判断为免疫漏洞。停用的漏洞不再用于入侵影响关联。注意，如果系统发现一台新主机受该漏洞影响，可视为该漏洞对此主机有效（不会自动停用）。

可**仅**在显示网络中特定主机漏洞的工作流程页面上的漏洞工作流程中停用漏洞，即：

- 默认漏洞工作流程的第二页 **Vulnerabilities on the Network**，该页仅显示仅显示应用于网络中主机的漏洞
- 在使用搜索根据 IP 地址 限制的自定义或预定义漏洞工作流程的任何页面上

停用不是根据 IP 地址 限制的漏洞工作流程中的漏洞会停用网络上检查到的*所有*主机的漏洞。要停用单台主机的漏洞，有三种选择：

- 使用网络映射。

  有关详细信息，请参阅第 48-6 页上的使用漏洞网络映射。
- 使用主机的主机配置文件。

  有关详细信息，请参阅第 49-26 页上的设置单个主机的漏洞。
- 根据要停用的主机的 IP 地址限制漏洞工作流程。对有多个关联 IP 地址的主机，此功能仅适用于该主机的单一选定 IP 地址。

要根据 IP 地址限制该视图，请执行漏洞搜索，只需为要停用漏洞的主机指定 IP 地址或 IP 地址范围。有关搜索漏洞的详细信息，请参阅第 50-46 页上的搜索漏洞。

要停用漏洞：

访问：管理员/任何安全分析师

步骤 1　在 Vulnerabilities on the Network 页面中，选中要停用漏洞旁边的复选框，然后点击 **Review**。

搜索漏洞

许可证：FireSIGHT

可搜索影响网络上主机的漏洞。您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 对于某些字段，可以在字段中指定 `n/a` 或 `blank` 识别信息不可用的字段的事件；使用 `!n/a` 或 `!blank` 识别已填入字段的事件。
- 大多数字段不区分大小写。
- 可以使用 CIDR 表示法指定 IP 地址。有关在 FireSIGHT 系统中输入 IPv4 和 IPv6 地址的详细信息，请参阅第 1-16 页上的 IP 地址约定。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

漏洞的特定搜索条件

注意，以下信息只适用于搜索漏洞：

- 在以下网址 http://www.securityfocus.com/bid 查找 Bugtraq ID 编号。
- 输入 `TRUE` 搜索被利用的漏洞，或者输入 `FALSE` 排除此类漏洞。

要搜索漏洞：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Vulnerabilities**。

页面根据相应限制进行更新。

步骤 3　在相应字段输入搜索条件。

如果您输入多个字段的条件，则搜索仅返回符合为所有字段指定的搜索条件的记录。点击在搜索字段旁边显示的添加图标 (✚)，使用对象作为搜索条件。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认漏洞工作流程中。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

使用第三方漏洞

许可证：FireSIGHT

FireSIGHT 系统有自己的漏洞跟踪数据库，该数据库与系统的指纹识别功能相结合，以识别与网络中主机关联的漏洞。

如果贵组织能够编写脚本或创建命令行导入文件以从第三方应用导入网络映射数据，则可导入第三方漏洞数据以扩增系统漏洞数据。有关详细信息，请参阅 《*FireSIGHT 系统 Host Input API Guide*》。

要将已导入数据纳入影响关联，必须将第三方漏洞信息映射至数据库中的操作系统和应用定义。不能将第三方漏洞信息映射至客户端定义。

有关详情，请参阅：

- 第 50-48 页上的查看第三方漏洞
- 第 50-49 页上的了解第三方漏洞表
- 第 50-50 页上的搜索第三方漏洞

查看第三方漏洞

许可证：FireSIGHT

使用主机输入功能导入第三方漏洞数据后，可使用防御中心查看第三方漏洞表。然后，可根据要查找的信息操纵事件视图。

访问第三方漏洞时所看到的页面因所使用的工作流程而异。有两个预定义工作流程。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关详细信息，请参阅第 58-34 页上的创建自定义工作流程。

下表介绍可在第三方漏洞工作流程页面执行的某些特定操作。也可执行常见发现事件操作表中所描述的任务。

表 50-12　第三方漏洞操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 50-49 页上的了解第三方漏洞表中获得详细信息。
查看第三方漏洞的漏洞详情	点击 SVID 列中的视图图标 ( )。或者，限制漏洞 ID 并向下钻取至漏洞详情页面。有关详细信息，请参阅第 49-24 页上的查看漏洞细节。

要查看第三方漏洞：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Vulnerabilities > Third-Party Vulnerabilities**。

系统显示默认第三方漏洞工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

提示　如在使用的自定义工作流程不包括第三方漏洞的表视图，请点击 **(switch workflow)**，然后选择 **Vulnerabilities by Source** 或 **Vulnerabilities by IP Address**。

了解第三方漏洞表

许可证：FireSIGHT

使用主机输入功能导入第三方漏洞信息时，系统会将该信息存储至其数据库。下表对第三方漏洞表中的字段进行了说明。

Vulnerability Source

第三方漏洞的来源，例如，QualysGuard 或 NeXpose。

Vulnerability ID

与其源漏洞关联的 ID 编码。

IP地址

与受漏洞影响主机关联的 IP 地址。

端口

如果漏洞与特定端口上运行的服务器关联，则为端口号。

Bugtraq ID

与 Bugtraq 数据库中漏洞关联的标识号。 (http://www.securityfocus.com/bid/)

CVE ID

与 MITRE 的常见漏洞和攻击 (CVE) 数据库 (http://www.cve.mitre.org/) 中漏洞关联的标识号。

SVID

系统用于跟踪漏洞的旧版漏洞标识号

点击视图图标 ( ) 访问 SVID 的漏洞详情。有关详情，请参见第 49-24 页上的查看漏洞细节。

Snort ID

与 Snort ID (SID) 数据库中漏洞关联的标识号。也就是说，如果入侵规则能检测利用特殊漏洞的网络流量，则此漏洞与入侵规则的 SID 关联。

注意，一个漏洞可能与多个 SID （或根本不与 SID）关联。如果一个漏洞与多个 SID 关联，则每个 SID 在漏洞表中各占一行。

职位

漏洞的标题。

说明

漏洞的简要说明。

计数

与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

搜索第三方漏洞

许可证：FireSIGHT

可搜索影响网络上主机的第三方漏洞。您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (`!`)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、 `D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (`*`) 作为通配符。
- 对于某些字段，可以在字段中指定 `n/a` 或 `blank` 识别信息不可用的字段的事件；使用 `!n/a` 或 `!blank` 识别已填入字段的事件。
- 大多数字段不区分大小写。

- 可以使用 CIDR 表示法指定 IP 地址。有关在 FireSIGHT 系统中输入 IPv4 和 IPv6 地址的详细信息，请参阅第 1-16 页上的 IP 地址约定。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

漏洞的特定搜索条件

注意，以下信息只适用于搜索漏洞：

- 在以下网址 http://www.securityfocus.com/bid 查找 Bugtraq ID 编号。
- 输入 TRUE 搜索被利用的漏洞，或者输入 FALSE 排除此类漏洞。

要搜索第三方漏洞：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Third-Party Vulnerabilities**。

页面根据相应限制进行更新。

步骤 3　在相应字段输入搜索条件。

如果您输入多个字段的条件，则搜索仅返回符合为所有字段指定的搜索条件的记录。点击在搜索字段旁边显示的添加图标 (✚)，使用对象作为搜索条件。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。
- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认第三方漏洞工作流程中。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

使用用户

许可证：FireSIGHT

如果 Active Directory Agent 或受管设备检测到非数据库中用户的登录，则将该用户添加至数据库，除非您明确限制该登录类型 （请参阅第 45-25 页上的限制用户日志记录）。

注 虽然系统检测到 SMTP 登录，但系统不会记录它们，除非数据库中已有匹配邮件地址的用户；将不根据 SMTP 登录将用户添加至数据库。

系统检测到的登录类型决定新用户的哪些信息会被存储，下表对此进行了说明。

表 50-13　登录类型和存储的用户数据

登录类型	存储的用户数据
LDAP AIM Oracle SIP HTTP FTP MDNS	• username • 当前 IP 地址 • 登录类型 （`aim`、`ldap`、`Oracle`、`SIP`、`http`、`ftp` 或者 `mdns`）
POP3 IMAP	• username • 当前 IP 地址 • email address • 登录类型 （`pop3` 或 `imap`）

如已配置防御中心 LDAP 服务器连接，则防御中心会每五分钟查询一次 LDAP 服务器并获取用户数据库中新用户的数据。同时，防御中心也会从 LDAP 服务器中查询防御中心数据库中记录超过 12 小时的用户的更新信息。系统检测到新用户登录后，防御中心数据库可能需要五到十分钟的时间来使用用户元数据更新。防御中心从 LDAP 服务器获取每个用户的以下信息和元数据：

- LDAP 用户名
- 名和姓
- email address
- department
- 电话号码

防御中心可在其数据库中存储的用户数取决于您的FireSIGHT许可证。注意，AIM、Oracle 和 SIP 登录会创建重复用户记录，因为它们不与系统从 LDAP 服务器中获得的任何用户元数据关联。为了防止由于这些协议的重复用户记录而导致过度使用用户计数，请在网络发现策略中禁用协议登录。有关详细信息，请参阅第 45-25 页上的限制用户日志记录。

可从数据库中搜索、查看和删除用户；也可从数据库中清除所有用户。有关详细信息，请参阅以下各节：

- 第 50-53 页上的查看用户
- 第 50-53 页上的了解用户表
- 第 50-55 页上的了解用户详细信息和主机历史记录
- 第 50-55 页上的搜索用户

查看用户

许可证：FireSIGHT

可查看用户表，然后根据所查找的信息操纵事件视图。

访问用户时所看到的页面因所使用的工作流程而异。可使用预定义工作流程并在用户详情页面终止，此工作流程包括列出了所有已检测到用户的用户表视图。用户详情页面提供有关符合限制条件的所有用户的信息。

您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关创建自定义工作流程的信息，请参阅第 58-34 页上的创建自定义工作流程。

有关表中列内容的详细信息，请参阅第 50-53 页上的了解用户表。下表对可在用户工作流程页面执行的一些特定操作进行了说明。也可在常见发现事件操作表中执行这些操作。

要查看用户：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Users > Users**。

系统显示默认用户工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

提示　如在使用的自定义工作流程不包括用户的表视图，请点击 **(switch workflow)**, ，然后选择 **Users**。

了解用户表

许可证：FireSIGHT

如果系统发现用户，会采集有关此用户的数据并将其存储在数据库中。以下对用户表中的字段进行了说明。

用户

以下任一选项：

- 通过选配防御中心 LDAP 服务器连接采集到的用户的名字、姓氏和用户名
- 如果尚未配置防御中心 LDAP 服务器连接，或对防御中心无法将其 LDAP 记录关联的用户，仅指用户名

防御中心也显示用于检测用户的协议。

注意，由于记录了失败的 AIM 登录尝试，防御中心可存储无效 AIM 用户 （例如，用户名拼写错误的用户）。

Current IP

与用户登录的主机关联的 IP 地址。如果该用户登录后另一授权用户登录具有相同 IP 地址的主机，则此字段为空，除非该用户为授权用户且新用户为未授权用户。（系统将 IP 地址与登录到该主机的最后一名授权用户关联。）有关授权与 未授权用户的详细信息，请参阅第 45-6 页上的用户数据库。

名字

通过选配防御中心 LDAP 服务器连接获取的用户的名字。如果符合以下条件，则此字段为空：

- 尚未配置防御中心 LDAP 服务器连接
- 防御中心无法将防御中心数据库中的用户与 LDAP 记录关联 （例如，对于通过 AIM、Oracle 或 SIP 登录添加至数据库的用户）
- 没有与 LDAP 服务器上用户关联的名字

姓氏

通过选配防御中心 LDAP 服务器连接获取的用户的姓氏。如果符合以下条件，则此字段为空：

- 尚未配置防御中心 LDAP 服务器连接
- 防御中心无法将防御中心数据库中的用户与 LDAP 记录关联 （例如，对于通过 AIM、Oracle 或 SIP 登录添加至数据库的用户）
- 没有与 LDAP 服务器上用户关联的姓氏

电邮

用户的邮件地址。如果符合以下条件，则此字段为空：

- 用户已通过 AIM 登录添加至数据库
- 用户已通过 LDAP 登录添加至数据库且没有与 LDAP 服务器用户关联的邮件地址

部门

通过选配防御中心 LDAP 服务器连接获取的用户所在的部门。如果没有明确地与 LDAP 服务器上用户关联的部门，则该部门列为服务器分配的任何默认组。例如，在 Active Directory 中，这是 `Users (ad)`。如果符合以下条件，则此字段为空：

- 尚未配置防御中心 LDAP 服务器连接
- 防御中心无法将防御中心数据库中的用户与 LDAP 记录关联 （例如，对于通过 AIM、Oracle 或 SIP 登录添加至数据库的用户）

电话

通过选配防御中心 LDAP 服务器连接获取的用户的电话号码。如果符合以下条件，则此字段为空：

- 尚未配置防御中心 LDAP 服务器连接
- 防御中心无法将防御中心数据库中的用户与 LDAP 记录关联 （例如，对于通过 AIM、Oracle 或 SIP 登录添加至数据库的用户）
- 没有与 LDAP 服务器上用户关联的电话号码

用户类型

用于检测用户的协议。例如，对于检测到 POP3 登录时添加至数据库的用户，用户类型是 `pop3`。

计数

与每行中所显示的信息匹配的用户数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

了解用户详细信息和主机历史记录

许可证：FireSIGHT

从将用户标识数据与其他类型事件关联的任何事件视图以及用户表视图中，可以显示 User Identity 弹出窗口以了解有关特定用户的详细信息。用户信息也可在用户工作流程终止页面上显示。

所看到的用户数据与在用户表视图中所看到的数据相同；有关详细信息，请参阅第 50-53 页上的了解用户表。

主机历史记录以图表再现了最后二十四个小时的用户活动。用户所登录和所注销主机的 IP 地址的列表以条形图大约显示登录和注销次数。典型用户在一天中可能登录和注销多台主机。例如，如果定期自动登录邮件服务器，则将显示多个短期会话，而如果长时间登录（例如在工作时间），则将显示长时间会话。

注意，如果检测到未授权用户登录主机，则将该登录记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，检测至一个授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，未授权用户是主机当前用户时，该用户仍不能进行用户管理。如果在网络发现策略中配置了捕获失败登录，则主机历史记录也包括用户登录失败的主机。

用于生成主机历史记录的数据存储在用户历史记录数据库中，默认情况下可存储 10 百万次用户登录事件。如果在主机历史记录中未看到特殊用户的任何数据，则该用户为非活动用户，或者可能需要增加数据库限制。有关详细信息，请参阅第 63-14 页上的配置控制面板事件限制。

要查看用户详细信息和主机历史记录：

访问：管理员/任何安全分析师

步骤 1　此时您有两种选择：

- 在列出了用户的任何事件视图中，点击用户标识旁边显示的用户图标 ()。
- 在任何用户工作流程中，点击 Users terminating 页面。

系统显示用户详细信息。

搜索用户

许可证：FireSIGHT

可搜索特定用户。您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。

  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、 `D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 对于某些字段，可以在字段中指定 `n/a` 或 `blank` 识别信息不可用的字段的事件；使用 `!n/a` 或 `!blank` 识别已填入字段的事件。
- 大多数字段不区分大小写。
- 可以使用 CIDR 表示法指定 IP 地址。有关在 FireSIGHT 系统中输入 IPv4 和 IPv6 地址的详细信息，请参阅第 1-16 页上的IP 地址约定。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

特定用户搜索条件

对于**用户类型**，有效的搜索条件为 `ldap`、`pop3`、`imap`、`oracle`、`sip`、`http`、`ftp`、`mdsn` 和 `aim`；因为未根据 SMTP 登录将用户添加至数据库，所以，输入 `smtp` 将不返回任何结果。

要搜索用户：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Users**。

系统将显示 Users 搜索页面。

提示　要在数据库中搜索另一类型的事件，请从表下拉列表选择它。

步骤 3　在相应字段输入搜索条件。

如果您输入多个字段的条件，则搜索仅返回符合为所有字段指定的搜索条件的记录。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请保持清除此复选框，将搜索保存为适用于所有用户

提示　如果要将搜索另存为对权限有限的自定义用户角色的约束，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。
- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认用户工作流程中。要使用不同的工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

使用用户活动

许可证：FireSIGHT

FireSIGHT 系统生成在网络上传达用户活动详情的事件。以下对四种类型的用户活动进行了说明。

New User Identity

系统检测到非数据库中用户登录时，生成此事件。

用户登录

出现以下任一情况时，生成此事件：

- Active Directory 服务器上安装的 Active Directory Agent 检测到 LDAP 登录
- 受管设备检测到 LDAP、POP3、IMAP、SMTP、AIM、Oracle、FTP、HTTP、MDNS 或 SIP 登录
- 有关用户登录事件需要谨记以下几点：
- 系统将不记录 SMTP 登录，除非数据库中已有匹配邮件地址的用户。
- 失败登录仅限 LDAP、 IMAP、 FTP 和 POP3，且仅限在流量中被检测到时。系统不因失败登录而将用户添加至检测到的用户数据库，但是，可选择根据网络发现策略中的用户登录配置在用户活动数据库中记录此活动。
- 如果明确限制了登录类型，则不会记录用户登录；请参阅第 45-25 页上的限制用户日志记录。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，未授权用户是主机当前用户时，该用户仍不能进行用户管理。

Delete User Identity

手动删除数据库中用户时，生成此事件。

User Identity Dropped: User Limit Reached

系统检测到非数据库中用户时生成此事件，但是，无法添加用户，因为数据库中用户数已经达到 FireSIGHT 许可证规定的最大数量。

防御中心可存储的检测用户的总数取决于 FireSIGHT 许可证。如果达到许可的限制，多数情况下，系统会停止向数据库添加新用户。要添加新用户，必须手动从数据库中删除旧的或非活动用户，或者清除数据库中的所有用户。

但是，系统支持授权用户。如果已达到极限且系统检测到先前未检测到的授权用户登录，则系统会删除保持非活动状态时间最长的未授权用户，并用新授权用户替换该用户。

系统检测用户活动时，会将该操作记录到数据库中。可查看、搜索和删除用户活动；也可从数据库中清除所有用户活动。

FireSIGHT 系统会尽可能地将用户活动与其他类型的事件关联。例如，入侵事件可以指出在事件发生时登录源主机和目标主机的用户。这样，可以了解哪个用户拥有作为攻击目标的主机，或者了解内部攻击或端口扫描的发起者。

也可在关联规则中使用用户活动。根据用户活动的类型和指定的其他条件，用于关联策略时可构建关联规则，网络流量符合条件时可启动补救和警报响应。有关用户活动的详细信息，请参阅第 45-3 页上的了解用户数据收集。

有关详细信息，请参阅：

- 第 50-58 页上的查看用户活动事件
- 第 50-58 页上的了解用户活动表
- 第 50-59 页上的搜索用户活动

查看用户活动事件

许可证：FireSIGHT

可查看用户活动表，然后根据所需查找的信息操纵事件视图。

访问用户活动时看到的页面因所使用的工作流程而异。可使用预定义工作流程（该工作流程包括用户活动表视图）并在用户详细信息页面（该页面包括符合限制条件的每个用户的详细信息）中终止。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关创建自定义工作流程的信息，请参阅第 58-34 页上的创建自定义工作流程。

有关表中列内容的详细信息，请参阅第 50-58 页上的了解用户活动表。下表对可在用户活动工作流程页面执行的一些特定操作进行了说明。也可在常见发现事件操作表中执行这些操作。

要查看用户活动：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Users > User Activity**。

系统显示默认用户活动工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示任何事件，可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

提示　如在使用的自定义工作流程不包括用户活动的表视图，请点击 **(switch workflow)**，然后选择 **User Activity**。

了解用户活动表

许可证：FireSIGHT

系统检测用户活动时，会将该操作记录到数据库中。以下对用户表中的字段进行了说明。

时间

系统检测到用户活动的时间。

活动

用户活动类型。有关详细信息，请参阅第 50-57 页上的使用用户活动。

用户

与活动关联的用户。至少，此字段应包含用户名和用于检测用户的协议。如有关于用户的 LDAP 元数据，则此字段也应包含用户的名字和姓氏。

用户类型

用于检测用户的协议。例如，对于系统检测到 POP3 登录时添加至数据库的用户，用户类型为 `pop3`。

IP地址

对于用户登录活动、登录中所涉的 IP 地址，可能是用户主机 （对于 LDAP、 POP3、 IMAP、 FTP、 HTTP、 MDNS 和 AIM 登录）、服务器 （对于 SMTP 和 Oracle 登录）或会话发起者（对于 SIP 登录）的 IP 地址。

注意，关联的 IP 地址并不意味着用户是该 IP 地址的当前用户；未授权用户登录一台主机时，用户历史记录和主机历史记录中会记录此次登录。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。

对于其他类型的用户活动，此字段留空。

说明

对于 Delete User Identity 和 User Identity Dropped activity 活动，指从数据库中删除的或未能添加至数据库的用户的用户名。对于网络资源的登录，显示 `network login`。对于其他类型的用户活动，此字段留空。

设备

对于受管设备检测到的用户活动，指该设备的名称。对于其他用户活动类型，是管理防御中心。

计数

与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

搜索用户活动

许可证：FireSIGHT

可搜索特定用户活动。您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。

通用搜索语法

系统在每个搜索字段旁边显示有效语法示例。输入搜索条件时，请记住以下几点：

- 所有字段都接受求反 (`!`)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。

  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 对于某些字段，可以在字段中指定 `n/a` 或 `blank` 识别信息不可用的字段的事件；使用 `!n/a` 或 `!blank` 识别已填入字段的事件。
- 大多数字段不区分大小写。
- 可以使用 CIDR 表示法指定 IP 地址。有关在 FireSIGHT 系统中输入 IPv4 和 IPv6 地址的详细信息，请参阅第 1-16 页上的 IP 地址约定。
- 使用设备字段搜索特定设备以及组、堆栈或集群中的设备。有关 FireSIGHT 系统如何处理搜索中的设备字段的详细信息，请参阅第 60-6 页上的在搜索中指定设备。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法的详细信息，包括在搜索中使用对象，请参阅第 60-1 页上的搜索事件。

要搜索用户活动：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉菜单中选择 **User Activity**。

系统将显示 User Activity 搜索页面。

提示　要在数据库中搜索另一类型的事件，请从表下拉列表选择它。

步骤 3　在相应字段输入搜索条件。

如果您输入多个字段的条件，则搜索仅返回符合为所有字段指定的搜索条件的记录。点击在搜索字段旁边显示的添加图标 (✚)，使用对象作为搜索条件。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如果要将搜索另存为对权限有限的自定义用户角色的约束，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。
- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认用户活动工作流程中，受当前时间范围限制。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

配置关联策略和规则

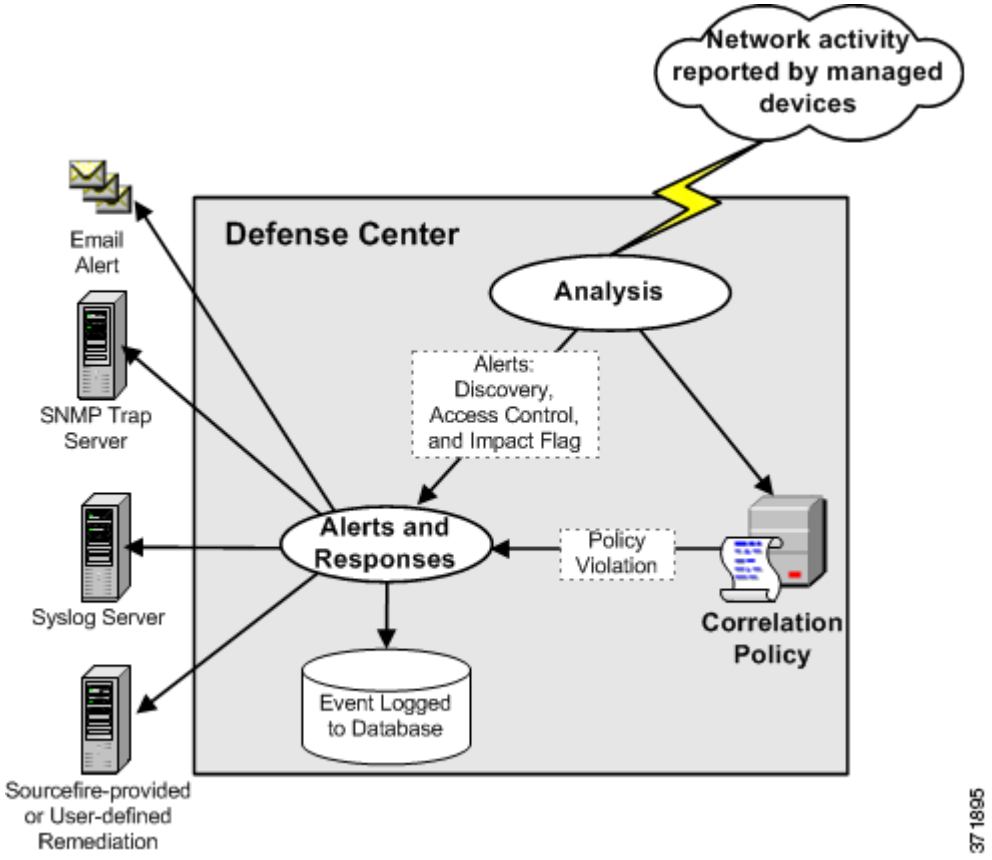
您可使用 FireSIGHT 系统的*关联*功能构建由*关联规则*和*合规性白名单*填充的*关联策略*，以帮助用户实时响应网络威胁。当用户网络活动触发关联规则或白名单时，会导致关联策略*违规*的发生。

当由 FireSIGHT 系统生成的特定事件达到指定标准或网络流量偏离在现有流量量变曲线中展示特征的正常网络通讯模式时，会触发关联规则。

另一方面，当系统确定网络上的主机正在运行被禁止的操作系统、客户端应用软件 （或客户端）、应用协议或协议时，会触发合规性白名单。

可以配置 FireSIGHT 系统以便响应违反策略情况。响应包括简单的警报以及各种修复 （例如扫描主机）。可将响应分门别类，以便系统对每种违反策略的情况作出多种响应。

下图图示说明事件通知和关联过程：



本章重点介绍如何创建关联规则、如何使用策略中的那些规则、如何将那些规则与响应和响应组关联起来，以及如何分析关联事件。有关详情，请参阅：

有关创建合规性白名单和关联响应 （警报和修复）的详细信息，请参阅：

创建关联策略规则

许可证：FireSIGHT、保护、 URL 过滤或者 恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

在创建关联策略之前，应先创建填充关联策略的关联规则或合规性白名单 （或两者兼有）。

注　本节介绍如何创建关联规则。有关创建合规性白名单的详细信息，请参阅第 52-7 页上的创建合规白名单。

当网络流量达到指定标准时，会触发关联规则 （并生成关联事件）。当创建关联规则时，可使用简单的条件或通过合并和嵌套条件和限制条件创建较复杂的结构。

可以下列方式进一步增加关联规则：

- 添加*主机配置文件限定条件*以使用涉及触发事件的主机的主机配置文件中的信息限制该规则。
- 将*连接跟踪器*添加至关联规则，以便在满足规则的初始条件后，系统开始跟踪某些连接。然后，只有在跟踪的连接满足其他标准时，才可生成关联事件。
- 将*用户资格*添加至关联规则以跟踪某些用户或用户群。例如，可限制关联规则，以便只有在源用户或或目标用户的标识是特定用户时，抑或是营销部门的特定用户时才会触发关联规则。
- 添加*暂停周期*和*非活动周期*。当触发一次关联规则时，在暂停周期，在一定时段内，规则不会再次触发，即使是在该时段内，再次出现违反规则的情况。在暂停时间过后，规则会再次触发 （并开始进入新的暂停周期）。在非活动周期，关联规则不会触发。

注意事项　评估触发常见事件的复杂关联规则可降低防御中心的性能。例如，防御中心必须根据系统记录的每个连接评估的多条件规则可能会导致资源超载。

下表对构建有效的关联规则必须拥有的许可证进行说明。如果没有适当的许可证，则不会触发使用 FireSIGHT 系统未经许可的许可证的关联规则。有关特定许可证的详细信息，请参阅第 65-2 页上的许可证类型和限制。

表 51-1　　构建关联规则的许可证要求

要.....	您需要该许可证.....
在入侵事件或安全情报事件上触发关联规则	保护
在发现事件、主机输入事件、地理定位数据或用户活动上触发关联规则，或将主机配置文件或用户资格添加至关联规则	FireSIGHT
在连接事件或基于终端的恶意软件事件上触发关联规则，或将连接跟踪器添加至规则	任何环境
在具有 URL 数据的连接事件上触发关联规则，或利用 URL 数据建立连接跟踪器 请注意， 2 系列设备和 DC500 防御中心都不会按类别或信誉支持 URL 过滤，而且 2 系列设备不会按照文字 URL 或 URL 组支持 URL 过滤。	URL 过滤
根据基于网络的恶意软件数据或回顾性的基于网络的恶意软件数据在恶意软件事件上触发关联规则 请注意， 2 系列和用于 Blue Coat X-系列的思科 NGIPS设备以及 DC500 防御中心均不支持基于网络的恶意软件防护。	恶意软件

当创建关联规则触发标准、主机配置文件限定条件、用户资格或连接跟踪器时，语法发生变化但结构保持不变。有关详细信息，请参阅第 51-31 页上的了解规则构建细节。

要创建关联规则，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**，然后选择 **Rule Management** 选项卡。

系统将显示 Rule Management 页面。

步骤 2　点击 **Create Rule**。

系统将显示 Create Rule 页面。

步骤 3　提供基本规则信息，例如规则名称、说明和组。

请参阅第 51-4 页上的提供基本规则信息。

步骤 4　指定要据此触发规则的基本标准。

请参阅第 51-4 页上的指定关联规则触发标准。

步骤 5　或者，将主机配置文件限定条件添加至规则。

请参阅第 51-17 页上的添加主机配置文件限定条件。

步骤 6　或者，将连接跟踪器添加至规则。

请参阅第 51-19 页上的使用超时连接数据限制关联规则。

步骤 7　或者，将用户资格添加至规则。

请参阅第 51-29 页上的添加用户资格。

步骤 8　或者，将非活动周期或暂停周期 （或两者）添加至规则。

请参阅第 51-30 页上的添加暂停和非活动周期。

步骤 9　点击 **Save Rule**。

系统保存规则。现在，可以使用关联规则或在同一事件类型上触发的其他关联规则中的规则。

提供基本规则信息

许可证：任何环境

您必须为每个关联规则提供一个名称，或者提供一段简短的说明。还可以将规则置于规则组中。

要提供基本规则信息，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**，然后选择 **Rule Management** 选项卡。

系统将显示 Rule Management 页面。

步骤 2　点击 **Create Rule**。

系统将显示 Create Rule 页面。

步骤 3　在 Create Rule 页面的 **Rule Name** 字段中，键入规则的名称。

步骤 4　在 **Rule Description** 字段中，键入规则的说明内容。

步骤 5　或者，从 **Rule Group** 下拉列表中选择规则的分组。

有关规则组的详细信息，请参阅第 51-38 页上的管理关联策略的规则。

步骤 6　继续执行下一节指定关联规则触发标准中的操作步骤。

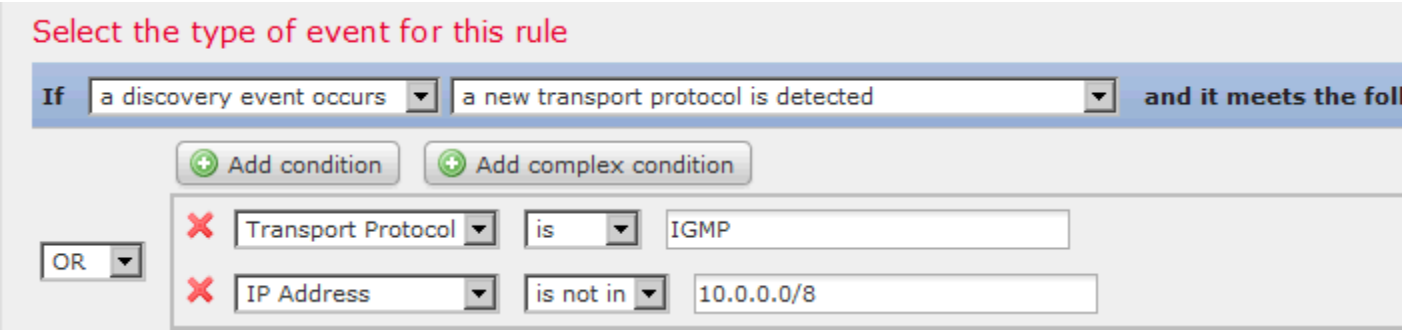
指定关联规则触发标准

许可证：因功能而异

受支持的设备：因功能而异

受支持的防御中心：因功能而异

简单的关联规则仅要求发生特定类型的事件；您不需要提供更具体的条件。例如，基于流量量变曲线变更的关联规则根本不需要任何条件。相反，关联规则可能比较复杂，有多个嵌套条件。例如，下图所示规则包括如果发送 IGMP 消息的 IP 地址不是在 10.x.x.x 子网中而引导规则触发的标准。



注　当根据事件构建条件时，只有在设备可收集条件所需信息而且防御中心可以管理该信息时，才可以添加关联规则触发标准。例如，由于 2 系列设备和 DC500 防御中心都不支持 SSL 检查、按类别或信誉的 URL 过滤或安全情报，因此，您无法根据这些功能在这些设备上配置事件条件。有关详细信息，请参阅第 51-2 页上的创建关联策略规则。

要指定关联规则触发标准，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择规则以之为基础的事件类型。

在构建关联规则时，首先必须选择规则以之为基础的事件类型。 **Select the type of event for this rule** 下有几个选项：

- 在出现特定入侵事件时选择 **an intrusion event occurs**。
- 在特定恶意软件事件出现时请选择 **a Malware event occurs** 触发该规则。
- 在特定发现事件出现时请选择 **a discovery event occurs** 触发该规则。在发现事件上触发关联规则时，还必须选择要使用的事件类型。可从第 50-8 页上的了解发现事件类型介绍的发现事件 子集中选择；例如，无法在跃点变更上触发关联规则。然而，当任何类型的发现事件发生时，可选择 **there is any type of event** 来触发该规则。
- 当检测到新用户或用户登录到主机时选择 **user activity is detected** 以触发该规则。
- 当特定主机输入事件发生时，选择 **a host input event occurs** 以触发该规则。在主机输入事件上触发关联规则时，还必须选择要使用的事件类型。可从第 50-11 页上的了解主机输入事件类型介绍的事件的子集中选择。
- 当连接数据满足特定标准时，选择 **a connection event occurs** 以触发该规则。在连接事件上触发关联规则时，还必须选择是否使用代表连接开始或结束的连接事件，或二者中的任何一种。
- 当网络流量偏离在现有流量量变曲线中展示特征的正常网络通讯模式时，选择 **a traffic profile changes** 以触发该关联规则。

步骤 2　指定规则条件。

在关联规则中使用以触发标准条件的语法会根据您在第 1 步中选择的基础事件而变化，但是机制相同。有关详细信息，请参阅第 51-31 页上的了解规则构建细节。

以下各节介绍可用来构建条件的语法：

- 第 51-6 页上的入侵事件语法
- 第 51-8 页上的恶意软件事件的语法
- 第 51-9 页上的发现事件的语法
- 第 51-11 页上的用户活动事件的语法
- 第 51-12 页上的主机输入事件的语法
- 第 51-13 页上的连接事件的语法
- 第 51-15 页上的流量量变曲线更改的语法

提示　可以嵌套分享您在第 1 步中指定的基础事件类型的规则。例如，如果您基于开放的 TCP 端口的检测创建新规则，则新规则的触发标准可包括 **rule “MyDoom Worm” is true** 和 **rule “Kazaa (TCP) P2P” is true**。

步骤 3　或者，继续执行以下各节中的操作步骤：

- 第 51-17 页上的添加主机配置文件限定条件
- 第 51-19 页上的使用超时连接数据限制关联规则
- 第 51-29 页上的添加用户资格
- 第 51-30 页上的添加暂停和非活动周期

如果已构建完关联规则，继续执行第 51-2 页上的创建关联策略规则中操作步骤的第 9 步以保存规则。

入侵事件语法

许可证：保护

下表介绍将入侵事件选定为基础事件时如何构建关联规则条件。

在构建规则条件时，应确保网络流量可触发规则。任何单个入侵事件的可用信息取决于多种因素，包括检测方法和记录方法。有关详细信息，请参阅第 41-8 页上的了解入侵事件。

表 51-2　　入侵事件的语法

如果指定.....	选择一个运算符，然后.....
访问控制策略	选择使用生成入侵事件的入侵策略的一个或多个访问控制策略。
Access Control Rule Name	键入使用生成入侵事件的入侵策略的访问控制规则的全部或部分名称。
Application Protocol	选择一个或多个与入侵事件相关的应用协议。
Application Protocol Category	选择一个或多个应用协议类别。
分类	选择一个或多个分类。
客户端	选择一个或多个与入侵事件相关的客户端。
Client Category	选择一个或多个客户端类别。
Destination Country 或 Source Country	选择一个或多个与入侵事件中的源或目标 IP 地址相关的国家/地区。
Destination IP、 Source IP 或 Source/Destination IP	指定单个 IP 地址或地址块。有关在 FireSIGHT 系统中使用 IP 地址表示法和前缀长度的详细信息，请参阅第 1-16 页上的 IP 地址约定。
Destination Port/ICMP Code 或 Source Port/ICMP Type	键入源流量的端口号或 ICMP 类型或目标流量的端口号或 ICMP 类型。
设备	选择一个或多个可能生成事件的设备。
Egress Interface 或 Ingress Interface	选择一个或多个接口。
Egress Security Zone 或 Ingress Security Zone	选择一个或多个安全区域。
Generator ID	选择一个或多个预处理器。有关可用的预处理器的详细信息，请参阅第 26-5 页上的在网络分析策略中配置预处理器。

表 51-2　　入侵事件的语法 （续）

如果指定.....	选择一个运算符，然后.....
Impact Flag	选择分配给入侵事件的影响级别。与指定 `is`、`is not`、`is greater than` 等运算符一起，选择以下任何一项： • 0 - 灰色 (Unknown) • 1 - 红色 (Vulnerable) • 2 - 橙色 (Potentially Vulnerable) • 3 - 黄色 (Currently Not Vulnerable) • 4 - 蓝色 (Unknown Target) **注**　因为没有可用于基于 NetFlow 数据添加至网络映射的主机的操作系统信息，所以防御中心无法为涉及那些主机的入侵事件分配 Vulnerable （级别：1，红色）影响级别，除非您使用主机输入功能手动设置主机的操作系统标识。 有关详细信息，请参阅第 41-32 页上的使用影响级别评估事件。
Inline Result	选择以下选项中的一种： • **dropped**，用来指定是否已经在内联、交换的或路由的部署中丢弃数据包 • **would have dropped**，用来指定如果已经设置入侵策略以在内联、交换的或路由的部署中丢弃数据包，则是否将丢弃该数据包 请注意，不管规则状态或入侵策略的丢弃行为如何 （包括当内联集处于分路模式下），系统都无法在被动部署情况下丢失数据包。
Intrusion Policy	选择一个或多个生成入侵事件的入侵策略。
IOC Tag	选择将 IOC 标记 `is` 还是 `is not` 设置为入侵事件的结果。
优先级	选择规则优先级：**low**、 **medium** 或 **high**。 对于基于规则的入侵事件，优先级对应于 `priority` 关键字的值或 `classtype` 关键字的值。对于其他入侵事件，优先级由解码器或预处理器决定。
协议	键入下列网址所列的传输协议的名称或编号： http://www.iana.org/assignments/protocol-numbers。
Rule Message	键入全部或部分规则消息。
Rule SID	键入由逗号分隔的单个 Snort ID 号 (SID) 或多个 SID。 **注**　如果将 **is in** 或 **is not in** 选定为运算符，则无法使用具有多项选择的弹出窗口。必须键入由逗号分隔的 SID 列表。
规则类型	指定规则是否是或不是本地的。本地规则包括自定义的标准文本入侵规则、已经修改的标准文本规则和在保存具有已修改的报头信息时创建的任何共享对象规则的新实例。有关详细信息，请参阅第 36-95 页上的修改现有规则。
SSL Actual Action	选择指示系统如何处理加密连接的 SSL 规则操作。
SSL Certificate Fingerprint	键入用来加密流量的证书的指纹或选择与指纹相关的对象通用名称。
SSL Certificate Subject Common Name (CN)	键入用于加密会话的证书的全部或部分对象通用名称。
SSL Certificate Subject Country (C)	选择一个或多个用于加密会话的证书的对象国家/地区代码。
SSL Certificate Subject Organization (O)	键入用于加密会话的证书的全部或部分对象组织名称。

表 51-2　　入侵事件的语法 （续）

如果指定.....	选择一个运算符，然后.....
SSL Certificate Subject Organizational Unit (OU)	键入用于加密会话的证书的全部或部分对象组织的单位名称。
SSL Flow Status	基于系统尝试解密流量的结果选择一种或多种状态。
用户名	键入登录入侵事件中的源主机的用户的用户名。
VLAN ID	键入与触发入侵事件的数据包相关的最内部的 VLAN ID
Web 应用程序	选择与入侵事件相关的一个或多个网络应用。
Web Application Category	选择一种或多种网络应用类别。

恶意软件事件的语法

许可证：任意或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

基于恶意软件事件的关联规则条件的语法取决于是否由基于终端的恶意软件代理报告事件、由受管设备检测事件，或者由受管设备检测到并回顾性地识别为恶意软件的事件。

请注意，因为 2 系列和用于 Blue Coat X-系列的思科 NGIPS设备以及 DC500 防御中心都不支持基于网络的恶意软件防护，所以，这些设备不支持根据基于网络的恶意软件数据或基于网络的回顾性恶意软件数据在恶意软件事件上触发关联规则。

在构建规则条件时，应确保网络流量可触发规则。单个连接或连接摘要事件的可用信息取决于几个因素，包括检测方法、日志记录方法和事件类型。有关详细信息，请参阅第 40-17 页上的了解恶意软件事件表。

下表介绍将恶意软件事件选定为基础事件时如何构建关联规则条件。

表 51-3　　恶意软件事件的语法

如果指定.....	选择一个运算符，然后.....
Application Protocol	选择一个或多个与恶意软件事件相关的应用协议。
Application Protocol Category	选择一个或多个应用协议类别。
客户端	选择一个或多个与恶意软件事件相关的客户端。
Client Category	选择一个或多个客户端类别。
Destination Country 或 Source Country	选择一个或多个与恶意软件事件中的源或目标 IP 地址相关的国家/地区。
Destination IP, Host IP, or Source IP	指定单个 IP 地址或地址块。有关在 FireSIGHT 系统中使用 IP 地址表示法的详细信息，请参阅第 1-16 页上的 IP 地址约定。
Destination Port/ICMP Code	键入目标流量的端口号或 ICMP 代码。
布置	选择 `Malware` 或 `Custom Detection` 或选择两者。
事件类型	选择与恶意软件事件相关的一个或多个基于终端的事件类型。有关详细信息，请参阅第 40-21 页上的恶意软件事件类型。
文件名	键入文件的名称。

表 51-3　　恶意软件事件的语法 （续）

如果指定.....	选择一个运算符，然后.....
文件类型	选择文件的类型，例如 PDF 或 MSEXE。
File Type Category	选择一个或多个文件类型类别，例如 Office Documents 或 Executables。
IOC Tag	选择将 IOC 标记 is 还是 is not 设置为恶意软件事件的结果。
SHA-256	键入或粘贴文件的 SHA-256 哈希值。
SSL Actual Action	选择指示系统如何处理加密连接的 SSL 规则操作。
SSL Certificate Fingerprint	键入用来加密流量的证书的指纹或选择与指纹相关的对象通用名称。
SSL Certificate Subject Common Name (CN)	键入用于加密会话的证书的全部或部分对象通用名称。
SSL Certificate Subject Country (C)	选择一个或多个用于加密会话的证书的对象国家/地区代码。
SSL Certificate Subject Organization (O)	键入用于加密会话的证书的全部或部分对象组织名称。
SSL Certificate Subject Organizational Unit (OU)	键入用于加密会话的证书的全部或部分对象组织的单位名称。
SSL Flow Status	基于系统尝试解密流量的结果选择一种或多种状态。
Source Port/ICMP Type	键入源流量的端口号或 ICMP 类型。
Web 应用程序	选择与恶意软件事件相关的一个或多个网络应用。
Web Application Category	选择一种或多种网络应用类别。

发现事件的语法

许可证：FireSIGHT

如果将关联规则以发现事件为基础，则首先必须从下拉列表中选择要使用的事件的类型。下表列出可从下拉列表中选定为触发标准的事件，与其相应的事件类型相互参照。有关发现事件类型的详细说明，请参阅第 50-8 页上的了解发现事件类型。

表 51-4　　关联规则触发标准与 发现事件类型

选择此选项…	要在该事件类型上触发规则.....
a client has changed	Client Update
a client timed out	Client Timeout
a host IP address is reused	DHCP: IP Address Reassigned
a host is deleted because the host limit was reached	Host Deleted: Host Limit Reached
a host is identified as a network device	Host Type Changed to Network Device
a host timed out	Host Timeout
a host’s IP address has changed	DHCP: IP Address Changed
a NETBIOS name change is detected	NETBIOS Name Change
a new client is detected	New Client
a new IP host is detected	New Host
a new MAC address is detected	Additional MAC Detected for Host

表 51-4　　关联规则触发标准与 发现事件类型 （续）

选择此选项…	要在该事件类型上触发规则.....
a new MAC host is detected	New Host
a new network protocol is detected	New Network Protocol
a new transport protocol is detected	New Transport Protocol
a TCP port closed	TCP Port Closed
a TCP port timed out	TCP Port Timeout
a UDP port closed	UDP Port Closed
a UDP port timed out	UDP Port Timeout
a VLAN tag was updated	VLAN Tag Information Update
an IOC was set	Indication of Compromise
an open TCP port is detected	New TCP Port
an open UDP port is detected	New UDP Port
the OS information for a host has changed	New OS
the OS or server identity for a host has a conflict	Identity Conflict
the OS or server identity for a host has timed out	Identity Timeout
there is any kind of event	任何事件类型
there is new information about a MAC address	MAC Information Change
there is new information about a TCP server	TCP Server Information Update
there is new information about a UDP server	UDP Server Information Update

请注意，在跃点变更上或由于达到许可主机限制而使系统丢弃新的主机时，不能触发关联规则。然而，当任何类型的发现事件发生时，可选择 **there is any type of event** 来触发该规则。

在选择发现事件类型后，可以构建关联规则条件，如下表所述。根据选择的事件类型，可以使用下表中的标准子集构建条件。例如，如果在检测到新的客户端时触发关联规则，则可基于主机的 IP 地址或 MAC 地址、客户端名称、类型或版本，以及检测到事件的设备来构建条件。

表 51-5　　发现事件的语法

如果指定.....	选择一个运算符，然后.....
Application Protocol	选择一个或多个应用协议。
Application Protocol Category	选择一个或多个应用协议类别。
Application Port	键入应用协议端口号。
Client	选择一个或多个客户端。
Client Category	选择一个或多个客户端类别。
Client Version	键入客户端的版本号。
设备	选择一个或多个可能生成发现事件的设备。
硬件	键入移动设备的硬件型号。例如，要与所有 Apple iPhone 匹配，键入 `iPhone`。
Host Type	从下拉列表中选择一个或多个主机类型。可以在一个主机或多种网络设备中的一种之间选择。

表 51-5　　发现事件的语法 （续）

如果指定.....	选择一个运算符，然后.....
IP Address 或 New IP Address	键入单个 IP 地址或地址块。有关在 FireSIGHT 系统中使用 IP 地址表示法的详细信息，请参阅第 1-16 页上的 IP 地址约定。
Jailbroken	选择 **Yes** 表示事件中的的主机属于越狱移动设备，选择 **No** 表示事件中的主机不是越狱移动设备。
MAC 地址	键入主机的全部或部分 MAC 地址。 例如，如果知道特定硬件制造商的设备拥有的 MAC Addresses 以 0A:12:34 开始，则可选择 **begins with** 作为运算符，然后键入 `0A:12:34` 作为值。
MAC Type	选择 MAC 地址是否是 **ARP/DHCP Detected**。 例如，选择系统是否将 MAC 地址明确识别为属于主机 (**is ARP/DHCP Detected**)，或者因为，打个比方，受管设备和主机之间有路由器，所以系统是否可以看见具有该 MAC 地址的许多主机 (**is not ARP/DHCP Detected**)。
MAC Vendor	键入触发发现事件的网络流量使用的 NIC 的 MAC 硬件供应商的全部或部分名称。
移动	选择 **Yes** 表示事件中的的主机属于移动设备，选择 **No** 表示事件中的主机不是移动设备。
NETBIOS Name	键入主机的 NetBIOS 名称。
网络协议	键入 http://www.iana.org/assignments/ethernet-numbers 列出的网络协议号。
OS Name	选择一个或多个操作系统名称。
OS Vendor	选择一个或多个操作系统供应商。
操作系统版本	选择一个或多个操作系统版本。
Protocol 或 Transport Protocol	键入下列网址所列的传输协议的名称或编号： http://www.iana.org/assignments/protocol-numbers。
信息来源	选择主机输入数据的来源 （用于操作系统和服务器标识更改和超时）。
Source Type	选择主机输入数据的来源的类型 （用于操作系统和服务器标识更改和超时）。
VLAN ID	键入涉及事件的主机的 VLAN ID。
Web Application	选择一个网络应用。

用户活动事件的语法

许可证：FireSIGHT

如果将关联规则以用户活动为基础，则首先必须要从下拉列表中选择要使用的用户活动的类型，两者中的任何一个即可：

- 登录主机的用户或
- 检测到的新用户标识

在选择用户活动类型后，可以构建关联规则条件，如下表所述。根据所选用户活动类型，可以使用下表中的标准子集构建条件；对于在新的用户标识上触发的关联规则，不能指定 IP 地址。

表 51-6　用户活动的语法

如果指定.....	选择一个运算符，然后.....
设备	选择已经检测到用户活动的一个或多个设备。
IP地址	键入单个 IP 地址或地址块。有关在 FireSIGHT 系统中使用 IP 地址表示法的详细信息，请参阅第 1-16 页上的 IP 地址约定。
用户名	键入用户名。

主机输入事件的语法

许可证：FireSIGHT

如果将关联规则以主机输入事件为基础，则首先必须要从下拉列表中选择要使用的主机输入事件的类型。下表列出可从下拉列表中选定为触发标准的事件，与其相应的主机输入事件类型相互参照。有关主机输入事件类型的详细说明，请参阅第 50-11 页上的了解主机输入事件类型。

表 51-7　关联规则触发标准与主机输入事件类型

选择此选项…	要在该事件类型上触发规则.....
a client is added	Add Client
a client is deleted	Delete Client
a host is added	Add Host
a protocol is added	Add Protocol
a protocol is deleted	Delete Protocol
a scan result is added	Add Scan Result
a server definition is set	Set Server Definition
a server is added	Add Port
a server is deleted	Delete Port
a vulnerability is marked invalid	Vulnerability Set Invalid
a vulnerability is marked valid	Vulnerability Set Valid
an address is deleted	Delete Host/Network
an attribute value is deleted	Host Attribute Delete Value
an attribute value is set	Host Attribute Set Value
an OS definition is set	Set Operating System Definition
host criticality is set	Set Host Criticality

当添加、删除或更改用户定义的主机属性的定义，或设置漏洞影响限定条件时，不能触发关联规则。

在选择主机输入事件后，可以构建关联规则条件，如下表说述。根据选择的主机输入事件类型，您可以使用下表中的标准子集构建条件。例如，如果在客户端已删除时触发关联规则，则可以基于事件涉及的主机的 IP 地址、删除源类型 （手动、第三方应用或扫描仪）以及源本身 （具体的扫描仪类型或用户）来构建条件。

表 51-8　主机输入事件的语法

如果指定.....	选择一个运算符，然后.....
IP地址	键入单个 IP 地址或地址块。有关在 FireSIGHT 系统中使用 IP 地址表示法的详细信息，请参阅第 1-16 页上的 IP 地址约定。
信息来源	选择主机输入数据的来源。
Source Type	选择主机输入数据的来源的类型。

连接事件的语法

许可证：任何环境

如果将关联规则以连接事件为基础，则首先必须选择是否要评估代表连接开始或结束的事件，或者选择开始或者选择结束。在选择连接事件类型后，可以构建关联规则条件，如连接事件的语法表中所述。

在构建规则条件时，应确保网络流量可触发规则。单个连接或连接摘要事件的可用信息取决于几个因素，包括检测方法、日志记录方法和事件类型。有关详细信息，请参阅第 39-9 页上的连接和安全情报事件中的可用信息。

表 51-9　连接事件的语法

如果指定.....	选择一个运算符，然后.....
访问控制策略	选择记录连接的一个或多个访问控制策略。
Access Control Rule Action	选择与记录连接的访问控制规则相关的一个或多个操作。 **注**　当网络流量与任何监控规则的条件匹配时，不管随后处理连接的规则或默认操作如何，都选择 **Monitor** 以触发关联事件。
Access Control Rule Name	键入记录连接的访问控制规则的全部或部分名称。 **注**　不管随后处理连接的规则或默认操作如何，您都可以键入其条件与连接匹配的任何监控规则的名称。
Application Protocol	选择一个或多个与连接相关的应用协议。
Application Protocol Category	选择一个或多个应用协议类别。
Client	选择一个或多个客户端。
Client Category	选择一个或多个客户端类别。
Client Version	键入客户端的版本号。
Connection Duration	键入连接事件的持续时间，单位为秒。
连接类型	选择是否要基于思科受管设备 (**FireSIGHT**) 检测到的连接或已启用 NetFlow 的设备 (**NetFlow**) 导出的连接来触发关联规则。
Destination Country 或 Source Country	选择一个或多个与连接事件中的源或目标 IP 地址相关的国家/地区。
设备	选择一个或多个检测到连接或处理连接 （对于已启用 NetFlow 的设备导出的连接数据）的设备。

表 51-9　连接事件的语法 （续）

如果指定.....	选择一个运算符，然后.....
Egress Interface 或 Ingress Interface	选择一个或多个接口。
Egress Security Zone 或 Ingress Security Zone	选择一个或多个安全区域。
Initiator Bytes、 Responder Bytes 或 Total Bytes	键入以下内容之一： • 发送的字节数 (**Initiator Bytes**)。 • 接收的字节数 (**Responder Bytes**)。 • 发送和接收的字节数 (**Total Bytes**)。
Initiator IP、 Responder IP 或 Initiator/Responder IP	指定单个 IP 地址或地址块。有关在 FireSIGHT 系统中使用 IP 地址表示法和前缀长度的详细信息，请参阅第 1-16 页上的 IP 地址约定。
Initiator Packets、 Responder Packets 或 Total Packets	键入以下内容之一： • 发送的数据包数量 (**Initiator Packets**)。 • 接收的数据包数量 (**Responder Packets**)。 • 发送和接收的数据包数量 (**Total Packets**)。
Initiator Port/ICMP Type 或 Responder Port/ICMP Code	键入发起方流量的端口号或 ICMP 类型或者接收方流量的端口号或 ICMP 类型。
IOC Tag	选择将 IOC 标记 `is` 还是 `is not` 设置为连接事件的结果。
NETBIOS Name	键入连接中受监控主机的 NetBIOS 名称。
NetFlow Device	选择导出可用来触发关联规则的连接数据的已启用 NetFlow 的设备的 IP 地址。如果没有将任何已启用 NetFlow 的设备添加至部署，则 NetFlow Device 下拉列表为空。
原因	选择与连接事件相关的一个或多个原因。
Security Intelligence Category	选择与连接事件相关的一个或多个安全情报类别。 **注**　要将安全情报类别用作连接结束事件的条件，必须在访问控制策略的安全情报部分将该条件设置到 **Monitor** 而非 **Block** 中。有关详细信息，请参阅第 13-3 页上的建立安全情报白名单和黑名单。
SSL Actual Action	选择指示系统如何处理加密连接的 SSL 规则操作。
SSL Certificate Fingerprint	键入用来加密流量的证书的指纹或选择与指纹相关的对象通用名称。
SSL 证书状态	选择与用来加密会话的证书相关的一个或多个状态。
SSL Certificate Subject Common Name (CN)	键入用于加密会话的证书的全部或部分对象通用名称。
SSL Certificate Subject Country (C)	选择一个或多个用于加密会话的证书的对象国家/地区代码。
SSL Certificate Subject Organization (O)	键入用于加密会话的证书的全部或部分对象组织名称。
SSL Certificate Subject Organizational Unit (OU)	键入用于加密会话的证书的全部或部分对象组织的单位名称。
SSL Cipher Suite	选择用于加密会话的一个或多个加密套件。
SSL Encrypted Session	选择 **Successfully Decrypted**。

表 51-9　　连接事件的语法 （续）

如果指定.....	选择一个运算符，然后.....
SSL Flow Status	基于系统尝试解密流量的结果选择一种或多种状态。
SSL Policy	选择记录加密连接的一个或多个 SSL 策略。
SSL Rule Name	键入记录加密连接的 SSL 规则的全部或部分名称。
SSL Server Name	键入客户端用来建立加密连接的服务器的全部或部分名称。
SSL URL Category	选择在加密连接中受访的 URL 的一个或多个 URL 类别。
SSL Version	选择用来加密会话的一个或多个 SSL 或 TLS 版本。
TCP Flags	选择为了触发关联规则，连接事件必须包含的 TCP 标志。 **注**　仅由已启用 NetFlow 的设备导出的连接数据才含有 TCP 标志。
Transport Protocol	键入连接使用的传输协议：`TCP` 或 `UDP`。
URL	键入在连接中受访的全部或部分 URL。
URL 类别	选择在连接中受访的 URL 的一个或多个 URL 类别。
URL Reputation	选择在连接中受访的 URL 的一个或多个 URL 信誉值。
用户名	键入登录连接中的一个主机的用户的用户名。
Web Application	选择与连接相关的一个或多个网络应用。
Web Application Category	选择一种或多种网络应用类别。

流量量变曲线更改的语法

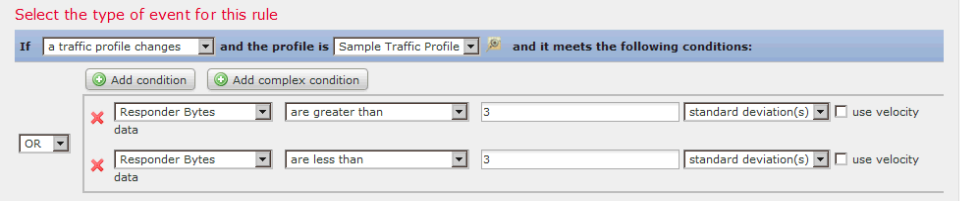
许可证：任何环境

如果将关联规则以流量量变曲线更改为基础，则当网络流量偏离在现有流量量变曲线中展示特征的正常网络通讯模式时，规则会触发。有关如何构建流量量变曲线的详细信息，请参阅第 53-1 页上的创建流量量变曲线。

可以基于原始数据或从计算数据得出的统计结果触发该规则。例如，您可以编写如果通过网络的数据量 （单位：字节）突然达到高峰时触发的规则，该高峰可能是由于攻击或其他安全策略违规造成的。如果出现下列两种情况中的一种，可以指定规则触发：

- 通过网络的字节数激增，超过流量平均值上下的一定数量的标准偏差

  请注意，要创建在通过网络的字节数超出一定数量的标准偏差 （高于或低于）时触发的规则，必须指定上下限，如下图所示。



  要创建在通过网络的字节数超过一定数量的**高于**平均值的标准偏差时触发的规则，请仅使用图中所示的第一个条件。

  要创建在通过网络的字节数超过一定数量的**低于**平均值的标准偏差时触发的规则，请仅使用第二个条件。

- 通过网络的字节数量激增，超过一定数量的字节

可以选择 **use velocity data** 复选框（请参阅第 39-14 页上的更改图形类型），以基于数据点之间的变化率触发关联规则。如果要使用上例中的速度数据，则可以指定在出现下列任何一种情况时触发规则：

- 通过网络的字节数量变化幅度非常大，高于或低于一定数量的高于平均变化率的标准偏差
- 通过网络的字节数激增，高于一定数量的字节

下表介绍在将流量量变曲线变更选定为基础事件时如何构建关联规则中的条件。如果流量量变曲线使用由已启用 NetFlow 的设备导出的连接数据，则请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异了解检测方法如何影响用于创建流量量变曲线的数据。

表 51-10　　流量量变曲线更改的语法

如果指定.....	选择一个运算符，然后键入.....	然后选择以下任一选项.....
连接数	检测到的连接总数 **或** 高于或低于平均值的标准偏差的数量，检测到的连接数量必须在此范围内以触发该规则	connections standard deviation(s)
Total Bytes、Initiator Bytes 或 Responder Bytes	以下任一选项： • 发送的总字节数 (**Total Bytes**) • 发送的字节数 (**Initiator Bytes**) • 接收的字节数 (**Responder Bytes**) **或** 高于或低于平均值的标准偏差的数量，上述标准之一必须在此范围内以触发该规则	字节 standard deviation(s)
Total Packets, Initiator Packets 或 Responder Packets	以下任一选项： • 发送的数据包总数 (**Total Packets**) • 发送的数据包数量 (**Initiator Packets**) • 接收的数据包数量 (**Responder Packets**) **或** 高于或低于为平均值的标准偏差的数量，上述标准之一必须在此范围内以触发该规则	数据包 standard deviation(s)
Unique Initiators	发起会话的独立主机的数量 **或** 高于或低于平均值的标准偏差的数量，检测到的独立发起方的数量必须为该平均值以触发该规则	initiators standard deviation(s)
Unique Responders	响应会话的独立主机的数量 **或** 高于或低于平均值的标准偏差的数量，检测到的独立响应方的数量必须为该平均值以触发该规则	responders standard deviation(s)

添加主机配置文件限定条件

许可证：FireSIGHT

如果使用连接事件、入侵事件、发现事件、用户活动或主机输入事件触发关联规则，则可以基于涉及事件的主机的主机配置文件限制该规则。此类限制被称为*主机配置文件限定条件*。

注　您**无法**将主机配置文件限定条件添加至在恶意软件事件、流量量变曲线更改或新的 IP 主机的检测上触发的关联规则。

例如，您可以限制关联规则，以便仅当 Microsoft Windows 主机为冲突流量的目标时触发该规则，因为只有 Microsoft Windows 计算机易受写入该规则的漏洞的影响。再比如，您还可限制关联规则，以便仅当主机违反白名单时触发该规则。

要匹配*隐含*或一般客户端，请根据响应客户端的服务器所用的应用协议创建主机配置文件限定条件。当作为连接发起方或源的主机上的客户端列表包含**客户端**遵循的应用协议名称时，该客户端可能实际上就是一种隐含客户端。换句话说，系统会根据使用该客户端的应用协议的服务器响应流量，而非检测到的客户端流量来报告该客户端。

例如，如果系统将 **HTTPS client** 作为主机上的一个客户端进行报告，请为 **Responder Host** 或 **Destination Host** 创建主机配置文件限定条件，其中 **Application Protocol** 被设置为 **HTTPS**，因为 **HTTPS client** 会根据响应方或目标主机发送的 HTTPS 服务器响应流量被报告为一种一般客户端。

请注意，要使用主机配置文件限定条件，主机必须存在于网络映射上，且要用作限定条件文件的主机配置文件属性必须已经包含在主机配置文件中。例如，如果配置关联规则以触发何时为运行 Windows 的主机生成入侵事件，则该规则仅会在生成入侵事件时主机已经被识别为 Windows 时触发。

要添加主机配置文件限定条件，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**，然后选择 **Rule Management** 选项卡。

系统将显示 Rule Management 页面。

步骤 2　点击 **Create Rule**。

系统将显示 Create Rule 页面。

步骤 3　在 Create Rule 页面上，点击 **Add Host Profile Qualification**。

系统将显示 Host Profile Qualification 部分。

提示　要移除主机配置文件限定条件，请点击 **Remove Host Profile Qualification**。

步骤 4　构建主机配置文件限定条件的条件。

可以创建一个简单的条件，或者通过结合和嵌套条件来创建较复杂的结构。有关如何使用网络界面构建条件的信息，请参阅第 51-31 页上的了解规则构建细节。

第 51-18 页上的用于主机配置文件限定条件的语法中介绍可以用来构建条件的语法。

步骤 5　或者，继续执行以下各节中的操作步骤：

- 第 51-19 页上的使用超时连接数据限制关联规则
- 第 51-29 页上的添加用户资格
- 第 51-30 页上的添加暂停和非活动周期

如果已构建完关联规则，继续执行第 51-2 页上的创建关联策略规则中操作步骤的第 9 步以保存规则。

用于主机配置文件限定条件的语法

许可证：FireSIGHT

当构建主机配置文件限定条件时，必须首先选择要用于限制关联规则的主机。可选择的主机取决于要用来触发规则的事件的类型，如下说述：

- 如果您正在使用连接事件，则选择 **Responder Host** 或 **Initiator Host**。
- 如果您正在使用入侵事件，则选择 **Destination Host** 或 **Source Host**。
- 如果您正在使用发现事件、主机输入事件或用户活动，则选择 **Host**。

在选择主机类型之后，请继续构建主机配置文件限定条件，如下表所述。

请注意，虽然您可以根据已启用 NetFlow 的设备导出的数据配置网络发现策略以将主机添加到网络映射中，但有关这些主机的可用信息是有限的。例如，这些主机没有可用的操作系统数据，除非您使用主机输入功能提供这些数据。此外，如果使用由已启用 NetFlow 的设备导出的连接数据，请记住， NetFlow 记录中不包含哪个主机是发起方以及哪个主机是响应方的信息。当系统处理 NetFlow 记录时，它会根据各主机正在使用的端口以及此类端口是否为公认端口来使用一种算法确定该信息。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

表 51-11　　主机配置文件限定条件的语法

如果指定.....	选择一个运算符，然后.....
Host Type	选择一个或多个主机类型。可以在一个主机或多种网络设备中的一种之间选择。
NETBIOS Name	键入主机的 NetBIOS 名称。
Operating System > OS Name	选择一个或多个操作系统名称。
Operating System > OS Vendor	选择一个或多个操作系统供应商名称。
Operating System > OS Version	选择一个或多个操作系统版本。
硬件	键入移动设备的硬件型号。例如，要与所有 Apple iPhone 匹配，键入 `iPhone`。
IOC Tag	选择一个或多个 IOC 标记。有关 IOC 标记类型的详细信息，请参阅第 45-17 页上的了解危害表现类型。
Jailbroken	选择 **Yes** 表示事件中的的主机属于越狱移动设备，选择 **No** 表示事件中的主机不是越狱移动设备。
移动	选择 **Yes** 表示事件中的的主机属于移动设备，选择 **No** 表示事件中的主机不是移动设备。
网络协议	键入 http://www.iana.org/assignments/ethernet-numbers 列出的网络协议号。
Transport Protocol	键入 http://www.iana.org/assignments/protocol-numbers 列出的传输协议的名称或编号。
Host Criticality	选择主机重要性：**None**、**Low**、**Medium** 或 **High**。有关主机重要性的详细信息，请参阅第 49-27 页上的使用预先定义的主机属性。
VLAN ID	键入与主机相关的 VLAN ID 。
Application Protocol > Application Protocol	选择一个或多个应用协议。
Application Protocol > Application Port	键入应用协议端口号。 如果您正在使用入侵事件触发关联规则，则根据您为主机配置文件限定条件选定的主机，本字段中预填充事件中的端口：`dst_port`（适用于 **Destination Host**）或 `src_port`（适用于 **Source Host**）。

表 51-11　主机配置文件限定条件的语法 （续）

如果指定.....	选择一个运算符，然后.....
Application Protocol > 协议	选择一个或多个协议。
Application Protocol Category	选择一个类别。
Client > Client	选择一个或多个客户端。
Client > Client Version	键入客户端版本。
Client Category	选择一个类别。
Web 应用程序	选择一个网络应用。
Web Application Category	选择一个类别。
MAC Address > MAC Address	键入主机的全部或部分 MAC 地址。 例如，如果知道特定硬件的设备拥有的 MAC Addresses 以 0A:12:34 开始，则可选择 **begins with** 作为运算符，然后键入 `0A:12:34` 作为值。
MAC Address > MAC Type	选择 MAC 类型是否为 **ARP/DHCP Detected**。 也就是说，选择系统是否将 MAC 地址明确识别为属于主机 (**is ARP/DHCP Detected**)，系统是否认为许多主机带有该 MAC 地址，例如，因为在受管设备和主机之间有一个路由器 (**is not ARP/DHCP Detected**)，或者 MAC 类型是否无关 （**is any**）。
MAC Vendor > MAC Vendor	键入主机的 MAC 硬件供应商的全部或部分名称。
任何可用的主机属性，包括默认合规性白名单主机属性	指定适当的值，这取决于选择的主机属性类型： • 如果主机属性类型为 `Integer`，请在针对该属性确定的范围中输入整数值。 • 如果主机属性类型为 `Text`，请输入文本值。 • 如果主机属性类型为 `List`，请选择有效的列表字符串。 • 如果主机属性类型为 `URL`，请输入 URL 值。 有关主机属性的详细信息，请参阅第 49-27 页上的使用用户定义的主机属性。

请注意，当构建主机配置文件限定条件时，可经常使用事件数据。例如，当系统检测到受控主机之一使用 Internet Explorer 时，假设触发关联规则。进一步假设，当检测该用法时，如果浏览器版本不是最新版本，则可以生成事件 （对于本示例，假设最新版本是 9.0）。

可将主机配置文件资格添加至该关联规则，以便只有在 **Client** 是 **Event Client** （例如， Internet Explorer）的情况下才会触发规则，但是， **Client Version** 版本不是 `9.0`。

使用超时连接数据限制关联规则

许可证：FireSIGHT

*连接跟踪器*限制关联规则，以便在满足规则的初始标准后 （包括主机配置文件和用户资格），系统开始跟踪某些连接。如果跟踪到的连接满足指定的时间内搜集到的其他标准，则防御中心会生成关联事件。

如果您正在使用连接事件、入侵事件、发现事件、用户活动或主机输入事件来触发关联规则，则您可以将连接跟踪器添加至规则。不能将连接跟踪器添加至在恶意软件事件或流量量变曲线更改上触发的规则。

提示 通常，连接跟踪器监控非常具体的流量，而且当被触发时，仅运行指定的一段时间。将连接跟踪器与流量量变曲线进行对比，发现后者一般监控的网络流量范围比较广并且持续运行；请参阅第 53-1 页上的创建流量量变曲线。

取决于您如何构建连接跟踪器，该跟踪器生成事件的方式有两种：

满足条件时，立即触发的连接跟踪器

可以配置连接跟踪器，以便在网络流量满足跟踪器的条件时，立即触发关联规则。如果出现这种情况，即使还没有超过超时周期，系统也为该连接跟踪器实例停止跟踪连接。如果此前触发关联规则的相同类型的策略违规再次发生，则系统可创建新的连接跟踪器。

另一方面，如果在网络流量满足连接跟踪器的条件前时间过期，则防御中心不会生成关联事件，而且还会停止跟踪该规则实例的连接。

例如，只有在特定类型的连接发生的次数超过一定时间周期内的具体次数时，连接跟踪器才可以通过生成关联事件作为一种事件阈值。或者，只有在初始连接之后，系统检测到其他数据传输时，才可以生成关联事件。

在超时期末触发的连接跟踪器

可以配置连接跟踪器，以便连接跟踪器可依靠在整个超时周期内搜集到的数据，因此在超时期末前，您不能触发连接跟踪器。

例如，如果将连接跟踪器配置为在检测到的字节数少于在一定时间周期内传输的一定数量的字节数时即触发，则系统在那段时间周期终止前处于等待状态，然后在网络流量满足该条件时生成事件。

有关详细信息，请参阅以下各节：

- 第 51-20 页上的添加连接跟踪器
- 第 51-21 页上的连接跟踪器的语法
- 第 51-23 页上的连接跟踪器事件的语法
- 第 51-24 页上的示例：来自外部主机的其他连接
- 第 51-26 页上的示例：其他 BitTorrent 数据传输

添加连接跟踪器

许可证：FireSIGHT

连接跟踪器限制关联规则，以便在满足初始标准 （包括主机配置文件和用户资格）后，系统开始跟踪某些连接。如果跟踪到的连接满足指定的时间内搜集到的其他标准，则防御中心会生成关联事件。

在配置连接跟踪器时，必须指定：

- 要跟踪哪些连接
- 您正在跟踪的连接必须满足以使防御中心生成关联事件的条件
- 连接跟踪器的最长持续时间，即，必须满足指定的条件以生成关联事件的时间

提示 可以将连接跟踪器添加至仅要求任何连接事件、入侵事件、发现事件、用户标识或主机输入事件发生的简单的关联规则。

要添加连接跟踪器，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Rule 页面上，点击 **Add Connection Tracker**。

系统将显示 Connection Tracker 部分。

提示　要移除连接跟踪器，请点击 **Remove Connection Tracker**。

步骤 2　通过设置连接跟踪器的标准指定要跟踪哪些连接。

可以通过创建一个简单的条件来设置连接跟踪器标准，或者通过结合和嵌套条件来创建更较复杂的结构。

有关如何使用网络界面构建条件的信息，请参阅第 51-31 页上的了解规则构建细节。第 51-21 页上的连接跟踪器的语法中介绍可用来构建连接跟踪器条件的语法。

步骤 3　根据在第 2 步中确定要跟踪的连接，确定要生成关联事件的时间。

可以创建一个简单的说明要生成事件时间的条件，或通过结合和嵌套条件来创建较复杂的结构。

此外，还必须指定在此期间满足指定的条件以生成关联事件的时间间隔 （单位：秒、分或小时）。

有关如何使用网络界面构建条件的信息，请参阅第 51-31 页上的了解规则构建细节。第 51-23 页上的连接跟踪器事件的语法中介绍可用来构建连接跟踪器条件的语法。

步骤 4　或者，继续执行以下各节中的操作步骤：

- 第 51-29 页上的添加用户资格
- 第 51-30 页上的添加暂停和非活动周期

如果已构建完关联规则，继续执行第 51-2 页上的创建关联策略规则中操作步骤的第 9 步以保存规则。

连接跟踪器的语法

许可证：任何环境

下表介绍如何构建指定要跟踪的连接种类的连接跟踪器条件。

您应记住，思科受管设备检测到的连接和由已启用 NetFlow 的设备导出的连接数据包含不同的信息。例如，受管设备检测到的连接不包含 TCP 标记信息。因此，如果要指定连接事件具有特定 TCP 标记以触发关联规则，则受管设备检测到的连接都不会触发该规则。

再比如， NetFlow 记录不包含连接中哪个主机是发起方、哪个主机是响应方的信息。当系统处理 NetFlow 记录时，它会根据各主机正在使用的端口以及此类端口是否为公认端口来使用一种算法确定该信息。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

表 51-12　连接跟踪器的语法

如果指定.....	选择一个运算符，然后.....
访问控制策略	选择记录要跟踪的连接的一个或多个访问控制策略。
Access Control Rule Action	选择与记录要跟踪的连接的访问控制规则相关的一个或多个访问控制规则操作。 **注**　不管随后处理连接的规则或默认操作如何，请选择 **Monitor** 以跟踪与任何监控规则的条件匹配的连接。

表 51-12　连接跟踪器的语法 （续）

如果指定.....	选择一个运算符，然后.....
Access Control Rule Name	键入记录要跟踪的连接的访问控制规则的全部或部分名称。 **注**　要跟踪匹配监控规则的连接，请键入监控规则的名称。不管随后处理连接的规则或默认操作如何，系统都对连接进行跟踪。
Application Protocol	选择一个或多个应用协议。
Application Protocol Category	选择一个或多个应用协议类别。
客户端	选择一个或多个客户端。
Client Category	选择一个或多个客户端类别。
Client Version	键入客户端的版本。
Connection Duration	键入连接持续时间，以秒为单位。
连接类型	选择是否要基于连接检测方式跟踪连接：由思科受管设备 (**FireSIGHT**) 检测或由已启用 NetFlow 的设备 (**NetFlow**) 导出。
Destination Country 或 Source Country	选择一个或多个国家/地区。
设备	选择要跟踪其已检测连接的一个或多个设备。如果要跟踪 NetFlow 连接，选择处理由已启用 NetFlow 的设备导出的连接数据的设备。
Ingress Interface 或 Egress Interface	选择一个或多个接口。
Ingress Security Zone 或 Egress Security Zone	选择一个或多个安全区域。
Initiator IP、Responder IP 或 Initiator/Responder IP	键入单个 IP 地址或地址块。有关在 FireSIGHT 系统中使用 IP 地址表示法的详细信息，请参阅第 1-16 页上的 IP 地址约定。
Initiator Bytes、Responder Bytes 或 Total Bytes	键入以下内容之一： • 发送的字节数 (**Initiator Bytes**) • 接收的字节数 (**Responder Bytes**) • 发送和接收的字节数 (**Total Bytes**)
Initiator Packets、Responder Packets 或 Total Packets	键入以下内容之一： • 发送的数据包数量 (**Initiator Packets**) • 接收的数据包数量 (**Responder Packets**) • 发送和接收的数据包数量 (**Total Packets**)。
Initiator Port/ICMP Type 或 Responder Port/ICMP Code	键入发起方流量的端口号或 ICMP 类型或者接收方流量的端口号或 ICMP 类型。
IOC Tag	选择 IOC 标记 `is` 或 `is not` 设置。
NETBIOS Name	键入连接中受监控主机的 NetBIOS 名称。
NetFlow Device	选择导出要跟踪的连接的已启用 NetFlow 的设备的 IP 地址。如果没有将任何已启用 NetFlow 的设备添加至部署，则 NetFlow Device 下拉列表为空。
原因	选择与要跟踪的连接有关的一个或多个原因。
Security Intelligence Category	选择与要跟踪的连接有关的一个或多个安全情报类别。

表 51-12　连接跟踪器的语法 （续）

如果指定.....	选择一个运算符，然后.....
TCP Flags	选择为了跟踪连接在连接中必须包含的 TCP 标记。 **注**　只有已启用 NetFlow 的设备导出的连接才包含 TCP 标记数据。
Transport Protocol	键入连接使用的传输协议：TCP 或 UDP。
URL	键入要跟踪的连接中受访的全部或部分 URL。
URL 类别	选择要跟踪的连接中受访的 URL 的一个或多个 URL 类别。
URL Reputation	选择要跟踪的连接中受访的 URL 的一个或多个 URL 信誉值。
用户名	键入登录要跟踪的连接中的一个主机的用户的用户名。
Web Application	选择一个或多个网络应用。
Web Application Category	选择一个或多个网络应用类别。

请注意，当构建连接跟踪器时，可以经常使用事件数据。例如，假设当系统在一个受控主机上检测到新的客户端时触发关联规则；即，当生成其基础事件类型是 **a new client is detected** 的系统事件时触发规则。

进一步假设，当检测到该新客户端时，要跟踪涉及主机上的新客户端的连接。因为系统知道主机的 IP 地址和客户端名称，所以可以构建跟踪那些连接的简单的连接跟踪器。

实际上，当将连接跟踪器添加至该类型的关联规则时，连接跟踪器用那些默认约束条件进行填充；即，将 **Initiator/Responder IP** 设置为 **Event IP Address** 并将 **Client** 设置为 **Event Client**。

提示　要指定连接跟踪器跟踪具体 IP 地址或 IP 地址块的连接，请点击 **switch to manual entry** 手动指定 IP。点击 **switch to event fields** 返回以使用事件中的 IP 地址。

连接跟踪器事件的语法

许可证：任何环境

下表介绍如何构建指定何时基于正在跟踪的连接生成关联事件的连接跟踪器条件。

表 51-13　连接跟踪器事件的语法

如果指定.....	选择一个运算符，然后.....
连接数	键入检测到的连接总数。
Number of SSL Encrypted Sessions	键入检测到的 SSL 或 TLS 加密的会话的总数。
Total Bytes、Initiator Bytes 或 Responder Bytes	键入以下内容之一： • 发送的总字节数 (**Total Bytes**) • 发送的字节数 (**Initiator Bytes**) • 接收的字节数 (**Responder Bytes**)

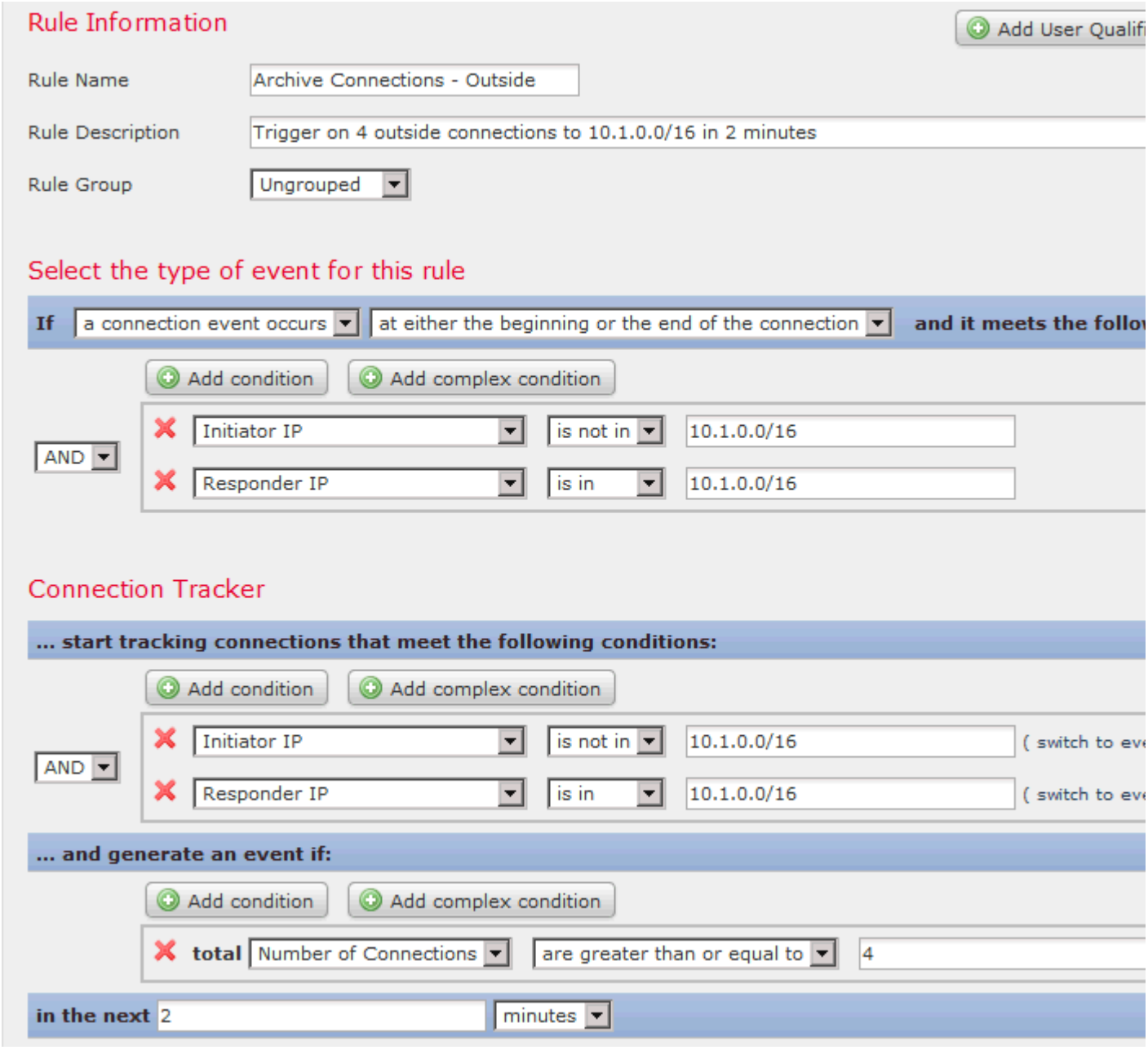
表 51-13　连接跟踪器事件的语法 （续）

如果指定.....	选择一个运算符，然后.....
Total Packets， Initiator Packets 或 Responder Packets	键入以下内容之一： • 发送的数据包总数 (**Total Packets**) • 发送的数据包数量 (**Initiator Packets**) • 接收的数据包数量 (**Responder Packets**)
Unique Initiators 或 Unique Responders	键入以下内容之一： • 检测到的发起会话的独立主机的数量 (**Unique Initiators**) • 响应检测到的连接的独立主机的数量 (**Unique Responders**)

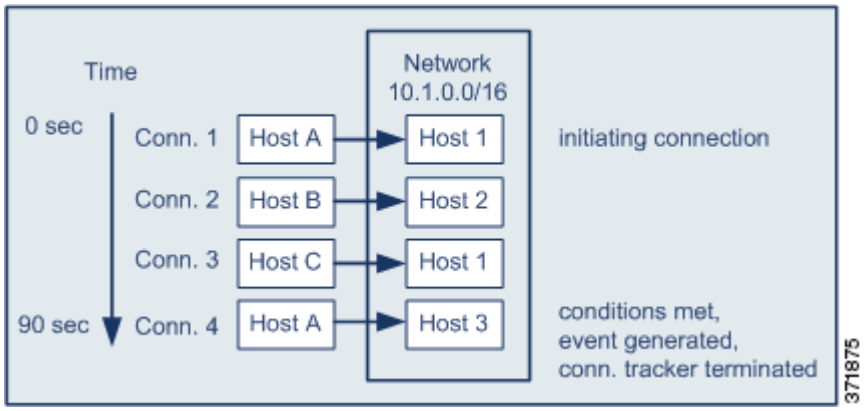
示例：来自外部主机的其他连接

考虑这样一个场景：您将敏感文件存档到网络 10.1.0.0/16 上，而且该网络外的主机通常不向网络内的主机发起连接。网络外的主机偶尔会发起连接，但当您确定在两分钟内发起四次或更多次的连接时，则说明有令人担心的问题。

下图所示规则规定 10.1.0.0/16 网络外的主机向网络内的主机发起连接的时间，系统开始跟踪符合该标准的连接。然后，即使系统在两分钟内检测到符合该特征的四次连接 （包括原始连接），防御中心也生成关联事件。


Rule Information
Add User Qualifi
Rule Name
Archive Connections - Outside
Rule Description
Trigger on 4 outside connections to 10.1.0.0/16 in 2 minutes
Rule Group
Ungrouped
Select the type of event for this rule
If
a connection event occurs
at either the beginning or the end of the connection
and it meets the follo
Add condition
Add complex condition
AND
Initiator IP
is not in
10.1.0.0/16
Responder IP
is in
10.1.0.0/16
Connection Tracker
... start tracking connections that meet the following conditions:
Add condition
Add complex condition
AND
Initiator IP
is not in
10.1.0.0/16
(switch to eve
Responder IP
is in
10.1.0.0/16
(switch to eve
... and generate an event if:
Add condition
Add complex condition
total
Number of Connections
are greater than or equal to
4
in the next
2
minutes

下图显示网络流量如何触发上述关联规则。



在本示例中，系统检测到满足关联规则的基本条件的连接，即，系统检测到从 10.1.0.0/16 网络外的主机向该网络内的主机及进行的连接。这样创建连接跟踪器。

处理连接跟踪器的阶段如下：

步骤 1　当系统检测到从网络外的 Host A 向网络内的 Host 1 进行的连接时，系统开始跟踪连接。

步骤 2　系统检测到符合连接跟踪器特征的两次以上的连接：Host B 至 Host 2 和 Host C 至 Host 1。

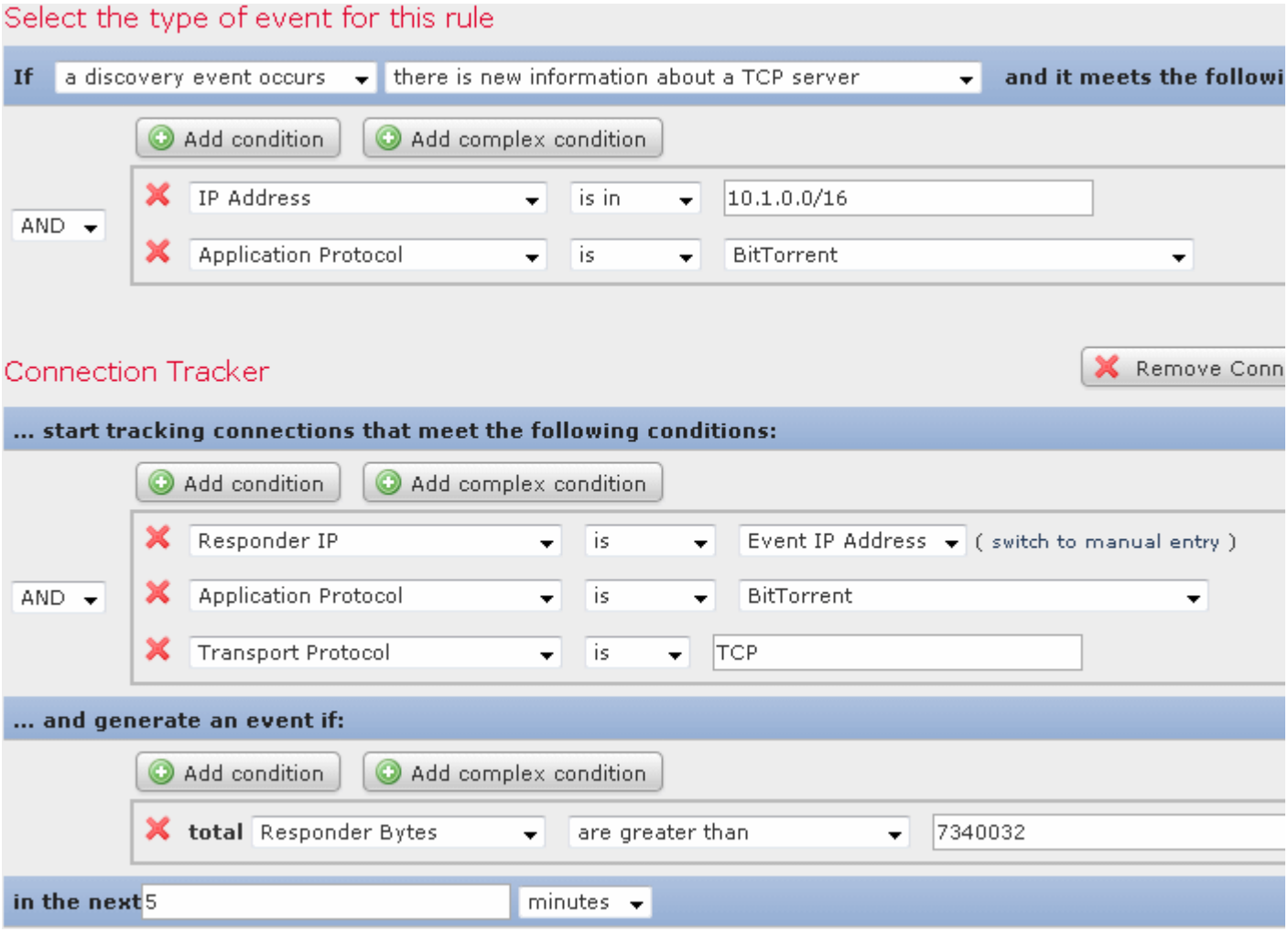
步骤 3　当在两分钟的时间限制内 Host A 连接到 Host 3 时，系统检测到第四次符合特征的连接。满足规则条件。

步骤 4　防御中心生成关联事件，系统停止跟踪连接。

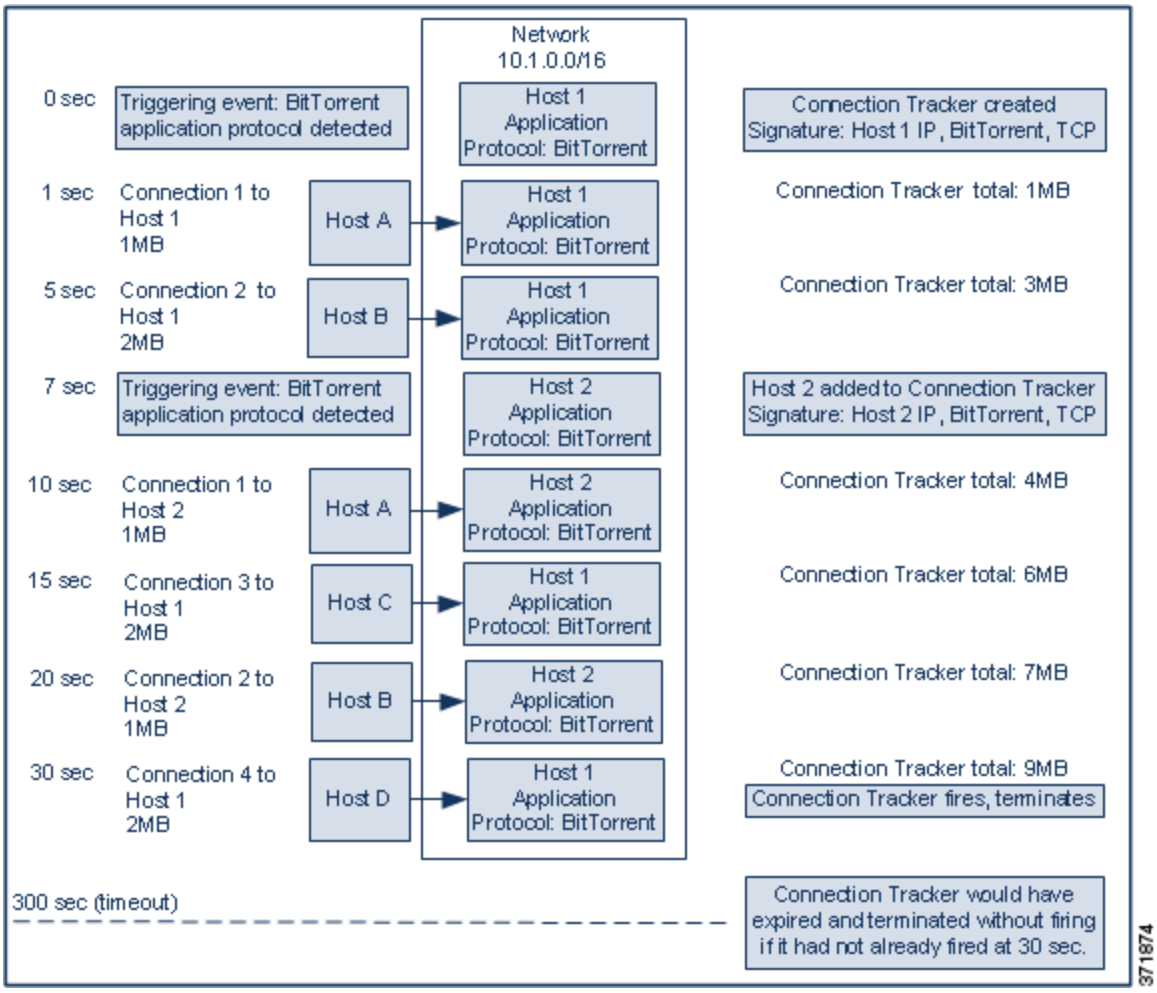
示例：其他 BitTorrent 数据传输

考虑这样一个场景：要生成关联事件，即使系统检测到在初始连接后其他 BitTorrent 数据传输到受控网络上的任何一台主机。

下图显示当系统检测到受控网络上的 BitTorrent 应用协议时触发的关联规则。该规则具有限制规则的连接跟踪器，以便仅当受控网络 （在本例中，受控网络为 10.1.0.0/16）上的主机在出现初始策略违规后的五分钟内通过 BitTorrent 传输的数据共超过 7 MB （7340032 字节）时触发该规则。


Select the type of event for this rule
If
a discovery event occurs
there is new information about a TCP server
and it meets the followi
Add condition
Add complex condition
AND
IP Address
is in
10.1.0.0/16
Application Protocol
is
BitTorrent
Connection Tracker
Remove Conn
... start tracking connections that meet the following conditions:
Add condition
Add complex condition
AND
Responder IP
is
Event IP Address
(switch to manual entry)
Application Protocol
is
BitTorrent
Transport Protocol
is
TCP
... and generate an event if:
Add condition
Add complex condition
total
Responder Bytes
are greater than
7340032
in the next
5
minutes

下图显示网络流量如何触发上述关联规则。



在本示例中，系统在两个不同的主机上检测到 BitTorrent TCP 应用协议：Host 1 和 Host 2。这两台主机通过 BitTorrent 将数据传输到其他四台主机：Host A、 Host B、 Host C 和 Host D。

处理该连接跟踪器的阶段如下：

步骤 1　当系统检测到 Host 1 上的 BitTorrent 应用协议时，系统开始跟踪 0 秒标记处的连接。

请注意，如果系统无法检测到接下来的 5 分钟（按 300 秒标记）内传输的 7 MB 的 BitTorrent TCP 数据，则连接跟踪器将过期。

步骤 2　5 秒钟时， Host 1 已经传输符合特征的 3 MB 数据：

- 在 1 秒标记处时，从 Host 1 传输至 Host A 的 1 MB 的数据量 （实现连接跟踪器时计算的 1 MB 的 BitTorrent 总流量）
- 在 5 秒标记处时，从 Host 1 传输至 Host B 的 2 MB 的数据量 （总共 3 MB）

步骤 3　在 7 秒种时，系统检测 Host 2 上的 BitTorrent 应用协议，同时也开始跟踪该主机的 BitTorrent 连接。

步骤 4　在 20 秒种时，系统已经检测到从 Host 1 和 Host 2 传输的符合特征的其他数据：

- 在 10 秒标记处时，从 Host 2 传输至 Host A 的 1 MB 的数据量 （总共 4 MB）

- 在 15 秒标记处时，从 Host 1 传输至 Host C 的 2 MB 的数据量 （总共 6 MB）
- 在 20 秒标记处时，从 Host 2 传输至 Host B 的 1 MB 的数据量 （总共 7 MB）

尽管 Host 1 和 Host 2 目前已经传输 7 MB 的 BitTorrent 综合数据，但因为传输字节总数必须**超过** 7 MB，所以规则不会触发 (**Responder Bytes are greater than 7340032**)。

此时，如果系统在跟踪器超时期间余下的 280 秒内没有检测到其他 BitTorrent 数据传输，则跟踪器过期、防御中心不会生成关联事件。

步骤 5　但是，在 30 秒钟时，系统检测到其他 BitTorrent 传输：

- 在 30 秒标记处时， 2 MB 数据从 Host 1 传输至 Host D （总共 9 MB）

满足规则条件。

步骤 6　防御中心生成关联事件。

此外，尽管 5 分钟的周期尚未过期，但是在该连接跟踪器示例中，防御中心也停止跟踪连接。如果此时系统检测到使用 BitTorrent TCP 应用协议的新连接，则系统会创建新的连接跟踪器。

请注意，在 Host 1 向 Host D 传输总计 2 MB 的数据*后*，防御中心生成关联事件，因为其在会话终止后才会计算连接数据。

添加用户资格

许可证：FireSIGHT

如果您使用连接事件、入侵事件、发现事件或主机输入事件触发关联规则，则您可以基于涉及事件的用户的标识限制该规则。此限制称为*用户资格*。您**无法**将用户资格添加至在流量量变曲线变更或用户活动检测上触发的关联规则。

例如，您可以限制关联规则，以便仅当源用户或目标用户源自销售部门时才会触发关联规则。

要添加用户标识资格，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Rule 页面上，点击 **Add User Qualification**。

系统将显示 User Identity Qualification 部分。

提示　要移除用户资格，请点击 **Remove User Qualification**。

步骤 2　构建用户资格条件。

可以创建一个简单的条件，或者通过结合和嵌套条件来创建较复杂的结构。有关如何使用网络界面构建条件的信息，请参阅第 51-31 页上的了解规则构建细节。

第 51-30 页上的用户资格的语法中介绍可以用来构建条件的语法。

步骤 3　或者，继续执行第 51-30 页上的添加暂停和非活动周期中的步骤。

如果已构建完关联规则，继续执行第 51-2 页上的创建关联策略规则中操作步骤的第 9 步以保存规则。

用户资格的语法

许可证：FireSIGHT

当构建用户资格条件时，必须首先选择要用来限制关联规则的标识。可选择的标识取决于要用来触发规则的事件的类型，如下说述：

- 如果您正在使用连接事件，则选择 **Identity on Initiator** 或 **Identity on Responder**。
- 如果您正在使用入侵事件，则选择 **Identity on Destination** 或 **Identity on Source**。
- 如果您正在使用发现事件，则选择 **Identity on Host**。
- 如果您正在使用主机输入事件，则选择 **Identity on Host**。

在选择用户类型之后，请继续构建用户资格条件，如下表所述。

防御中心从可选防御中心 LDAP 服务器连接获得某些用户信息，其中包括姓名、部门、电话号码和邮件地址；请参阅第 17-9 页上的使用用户代理报告 Active Directory 登录情况。该信息不能提供给数据库中的所有用户。

表 51-14　　用户资格的语法

如果指定.....	选择一个运算符，然后.....
用户名	键入要用来限制关联规则的用户的用户名。
Authentication Protocol	选择验证协议 （或用户类型）协议。该协议用于检测用户。
名字	键入要用来限制关联规则的用户的名字。
姓氏	键入要用来限制关联规则的用户的姓氏。
部门	键入要用来限制关联规则的用户所在的部门。
电话	键入要用来限制关联规则的用户的电话号码。
电子邮件	键入要用来限制关联规则的用户的邮件地址。

添加暂停和非活动周期

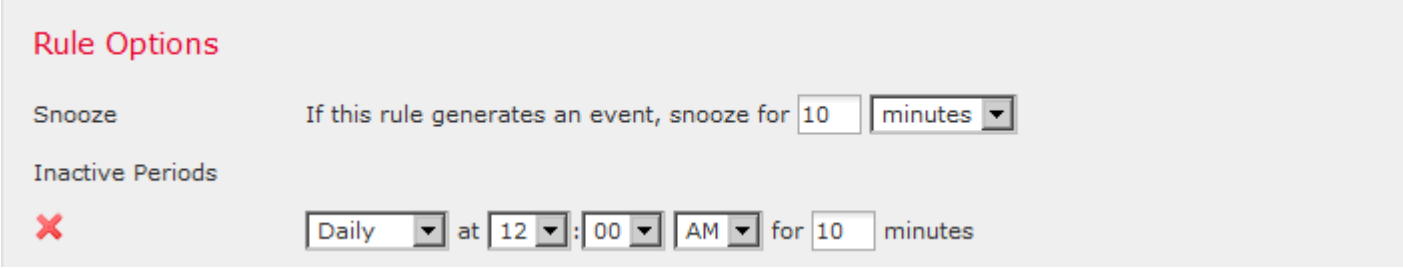
许可证：任何环境

您可以在关联规则中配置*暂停周期*。当关联规则触发时，即使是在指定的间隔周期内再次违反该规则，暂停周期也指示防御中心在该时间间隔内停止触发该规则。在暂停周期过后，规则可以再次触发 （并开始进入新的暂停周期）。

例如，可以将网络上的一个主机设置为永远不产生流量。取决于主机上的网络流量，每当系统检测到涉及该主机的连接时都会触发的简单关联规则可在短时间内创建多个关联事件。要限制披露策略违规的关联事件数量，可以添加暂停周期，以便防御中心仅为系统检测到的涉及主机的第一个连接 （在指定的时间周期内）生成关联事件。

此外，还可以在关联规则中设置非活动周期。在非活动周期，关联规则将不会触发。可以将非活动周期设置为每日、每周或每月。例如，可以在内部网络中在夜间扫描 Nmap，以寻找主机操作系统的变化情况。在这种情况下，可以在扫描周期在受影响的关联规则上设置每天的非活动周期，以便那些规则不会错误地触发。

下图显示配置有暂停和非活动周期的部分关联规则。



要添加暂停周期，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Profile 页面的 **Rule Options** 下，指定在规则触发后防御中心应等待再次触发规则的时间间隔。

提示　要移除暂停周期，请将时间间隔指定为 0（秒、分钟或小时）。

要添加非活动周期，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Profile 页面的 **Rule Options** 下，点击 **Add Inactive Period**。

步骤 2　使用下拉列表和文本框指定您希望防御中心停止根据关联规则评估网络流量的时间和频率。

提示　要删除非活动周期，请点击要删除的非活动周期旁边的删除图标 (✖)。

完成添加暂停和非活动周期后，继续执行第 51-2 页上的创建关联策略规则中的操作步骤中的第 9 步以保存该规则。

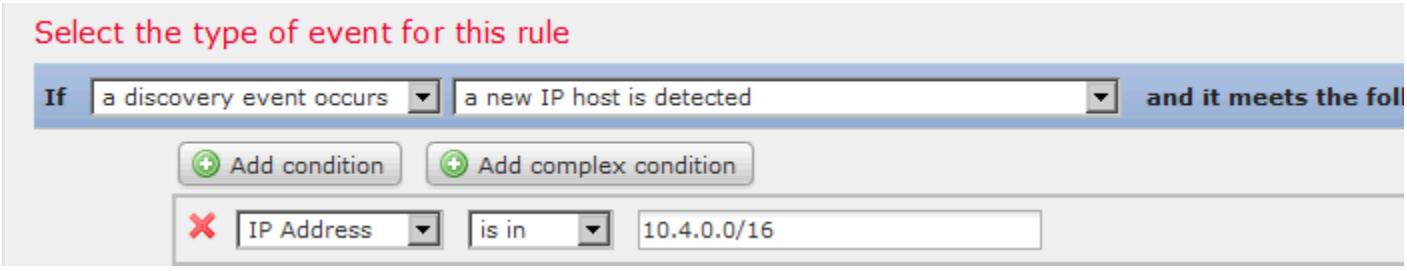
了解规则构建细节

许可证：任何环境

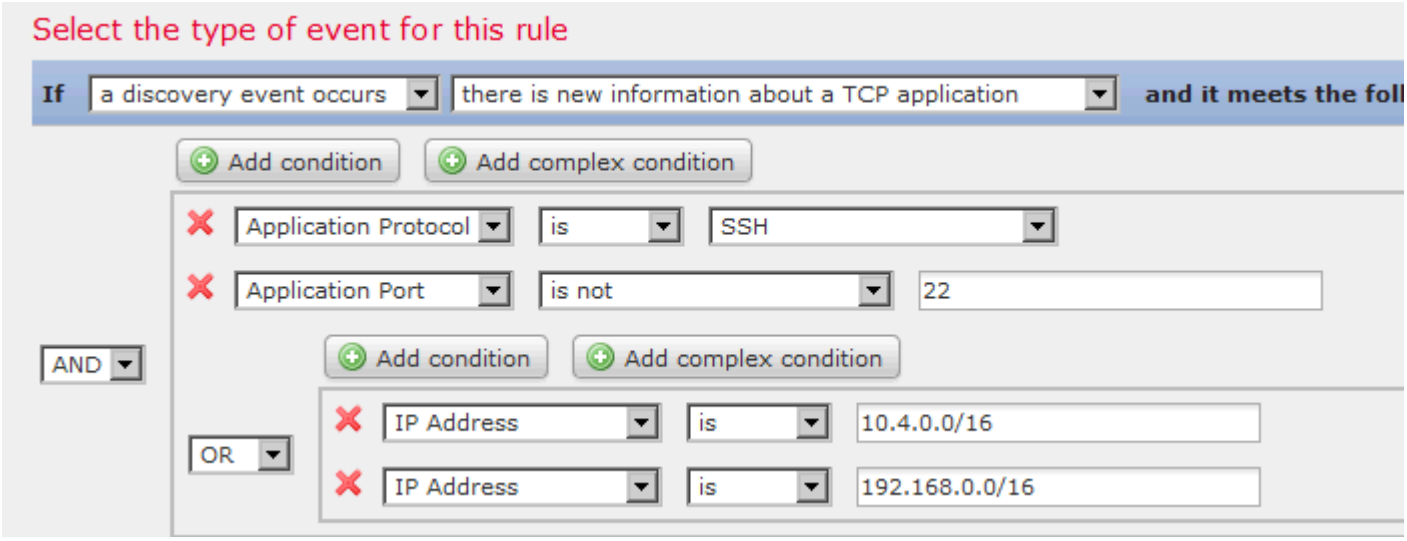
您通过指定其触发条件来构建关联规则、连接跟踪器、用户资格和主机配置文件限定条件。您可以创建简单的条件，或者通过结合和嵌套条件来创建较复杂的结构。

例如，如果要在每次检测到新主机时都生成关联事件，则可以创建非常简单的规则，不使用任何条件，如下图所示。

如果要在仅当 10.4.x.x 网络中检测到该新的主机时进一步限制规则并生成事件，则可以添加简单的条件，如下图所示。



但检测 10.4.x.x 网络和 192.168.x.x 网络上的非标准端口的 SSH 活动的以下规则具有四个条件，底部的两个的条件较复杂。



可以在条件中使用的语法会根据您正在创建的元素而变化，但是机制相同。

注意事项　评估触发常见事件的复杂关联规则可降低防御中心的性能。例如，防御中心必须根据系统记录的每个连接评估的多条件规则可能会导致资源超载。

有关条件构建的详细信息，请参阅：

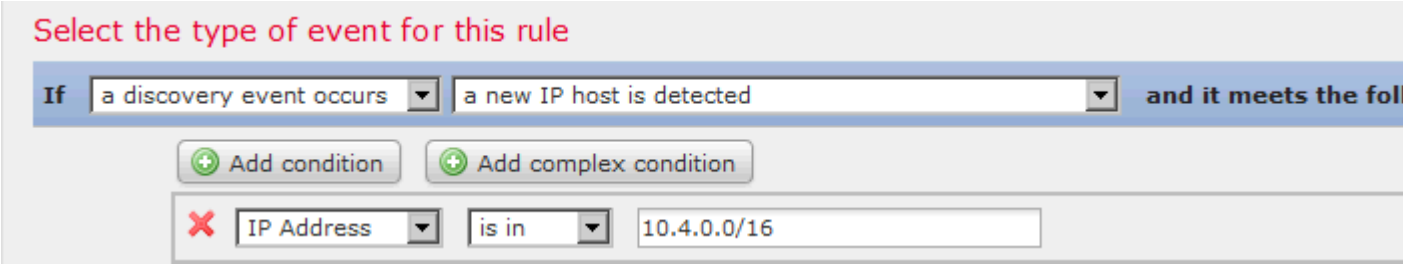
- 第 51-33 页上的构建一个条件
- 第 51-35 页上的添加和连接条件
- 第 51-38 页上的在一个条件中使用多个值

构建一个条件

许可证：任何环境

大部分条件由三部分构成：*类别*、*运算符*和*值*；有些条件更为复杂，并且包含若干类别，每个条件都有各自的运算符和值。

例如，如果在 10.4.x.x 网络上检测到新的主机，则会触发以下关联规则。条件的类别是 **IP Address**，运算符是 **is in**，值是 `10.4.0.0/16`。



要在以上示例中构建关联规则触发标准，请执行以下操作：

访问：管理员/发现管理员

步骤 1　开始构建关联规则。

有关详细信息，请参阅第 51-2 页上的创建关联策略规则。

步骤 2　在 Create Rule 页面的 **Select the type of event for this rule** 下面，选择 **a discovery event occurs**，然后从下拉列表中选择 **a new IP host is detected**。

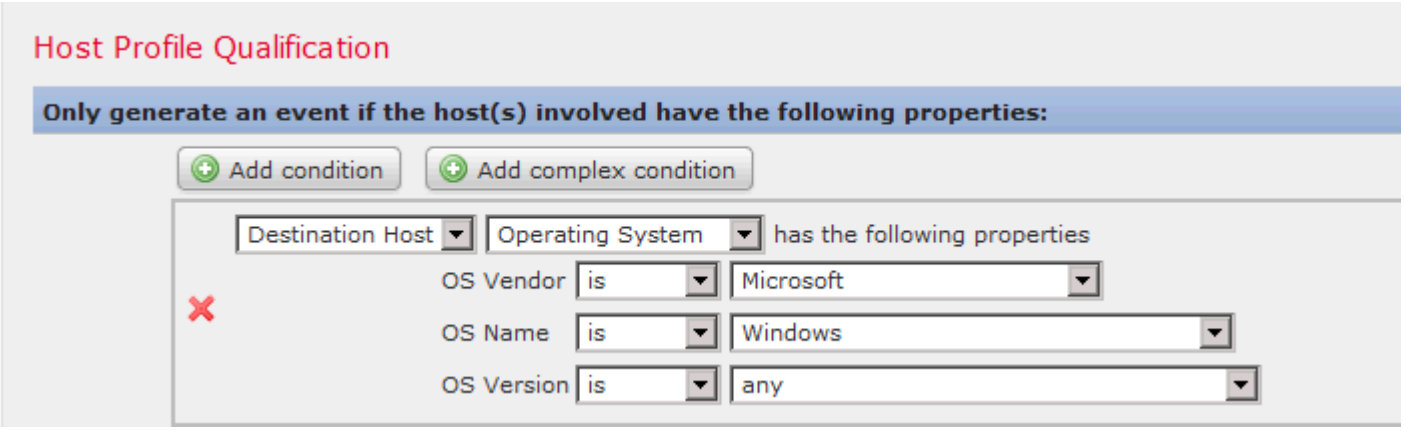
步骤 3　从第一个（或*类别*）下拉列表中选择 **IP Address**，以开始构建规则的单个条件。

步骤 4　从显示的运算符下拉列表中选择 **is in**。

提示　当类别为 IP address 时，选择 **is in** 或 **is not in** 作为运算符使您可以指定 IP 地址*是*还是*不是*在 IP 地址块中，如特殊表示法（例如 CIDR）所述。有关在 FireSIGHT 系统中使用 IP 地址表示法的详细信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 5　在文本字段中键入 `10.4.0.0/16`。

相反，下列主机配置文件限定条件更复杂；它限制关联规则，以便该规则仅在涉及作为其基础的发现事件的主机运行一个 Microsoft Windows 版本时才触发。



要在以上示例中构建主机配置文件限定条件，请执行以下操作：

访问：管理员/发现管理员

步骤 1　构建在发现事件上触发的关联规则。

有关详细信息，请参阅第 51-2 页上的创建关联策略规则。

步骤 2　在 Create Rule 页面上，点击 **Add Host Profile Qualification**。

系统将显示 Host Profile Qualification 部分。

步骤 3　在 **Host Profile Qualification** 下，在第一个条件中，指定要用其主机配置文件限制关联规则的主机。

因为该主机配置文件限定条件是基于发现事件的关联规则的一部分，所以唯一可用的类别是 **Host**。

步骤 4　通过选择 **Operating System** 类别，开始指定主机的操作系统的详细信息。

系统显示三个子类别：**OS Vendor**、 **OS Name** 和 **OS Version**。

步骤 5　要指定主机可运行任何版本的 Microsoft Windows，请对所有这三个子类别使用相同的运算符：**is**。

步骤 6　最后，指定子类别的值。

将 **Microsoft** 选定为 **OS Vendor** 的值、 **Windows** 选定为 **OS Name** 的值，将 **any** 保留为 **OS Version** 的值。

请注意，可选择的类别取决于您是在构建关联规则触发器、主机配置文件限定条件、连接跟踪器还是用户资格。在关联规则触发器中，类别的划分进一步取决于关联规则的基础事件类型。

此外，条件的可用运算符取决于选择的类别。最后，可用于指定条件值的语法取决于类别和运算符。有时候，必须在文本字段中键入值。有时候，可以从下拉列表中选择值。

注　如果条件语法允许您从下拉列表中选择值，通常可使用多个列表中的值。有关详细信息，请参阅第 51-38 页上的在一个条件中使用多个值。

有关构建关联规则触发标准的语法的详细信息，请参阅：

- 第 51-6 页上的入侵事件语法
- 第 51-8 页上的恶意软件事件的语法
- 第 51-9 页上的发现事件的语法

- 第 51-11 页上的用户活动事件的语法
- 第 51-12 页上的主机输入事件的语法
- 第 51-13 页上的连接事件的语法
- 第 51-15 页上的流量量变曲线更改的语法

有关构建主机配置文件限定条件、用户资格和连接跟踪器的语法的详细信息，请参阅：

- 第 51-18 页上的用于主机配置文件限定条件的语法
- 第 51-21 页上的连接跟踪器的语法
- 第 51-23 页上的连接跟踪器事件的语法
- 第 51-30 页上的用户资格的语法

添加和连接条件

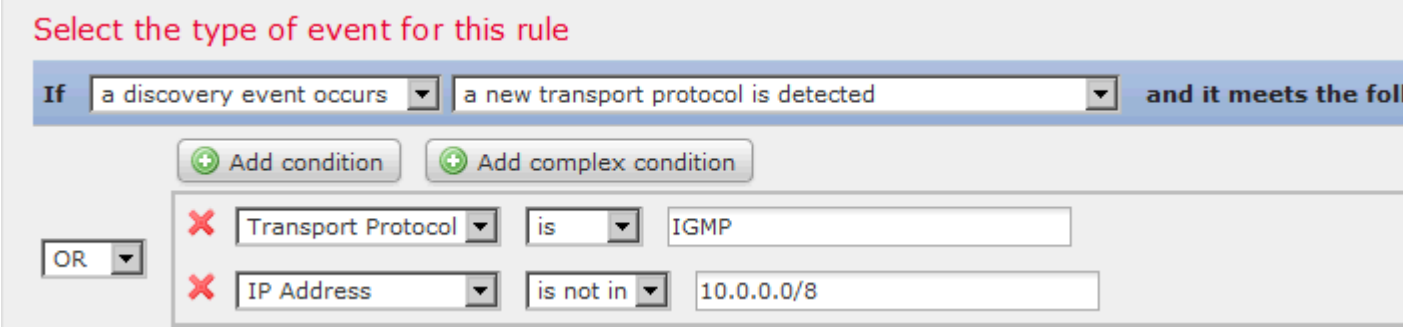
许可证：任何环境

您可以创建简单的关联规则触发器、连接跟踪器、主机配置文件限定条件和用户资格，或通过结合和嵌套条件来创建较复杂的结构。

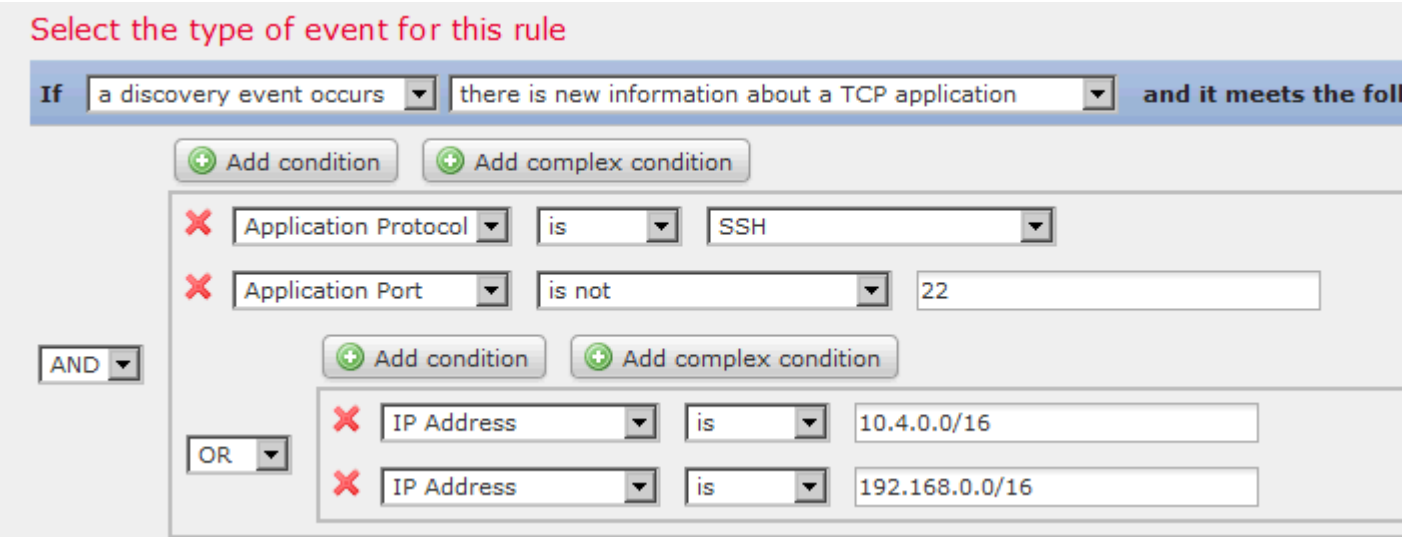
当构建的结构不止一个条件时，必须将这些条件用 **AND** 与 **OR** 运算符结合起来。相同级别的条件会被放在一起评估：

- **AND** 操作符要求必须满足其控制的级别上的所有条件。
- **OR** 运算符要求必须满足其控制的级别上的至少一个条件。

例如，以下关联规则触发标准包含两个条件，它们由 **OR** 连接。这意味着，如果任何一个条件真实，即，如果具有 IP 地址的主机不是在 10.x.x.x 子集中，或主机传输 IGMP 消息，则规则触发。



相反，以下检测 10.4.x.x 网络和 192.168.x.x 网络上的非标准端口的 SSH 活动的规则具有四个条件，底部的两个的条件较复杂。



如果在非标准端口上检测到 SSH，前两个条件要求应用协议名称为 SSH 并且端口不是 22，则该规则触发。规则进一步要求，涉及事件的主机的 IP 地址不属于 10.4.x.x 网络，便属于 192.168.x.x 网络。

从逻辑上讲，该规则被评估如下：

```
(A and B and (C or D))
```

表 51-15　　规则评估

其中.....	为陈述以下情况的条件.....
A	Application Protocol 是 SSH
B	Application Port 不是 22
C	IP Address 为 10.4.0.0/8
D	IP Address 为 196.168.0.0/16

要添加一个条件，请执行以下操作：

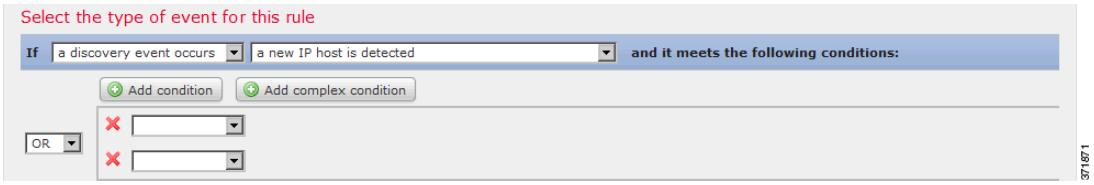
访问：管理员/发现管理员

步骤 1　要添加一个条件，请点击当前条件上方的 **Add condition**。

在与当前条件集相同的级别上，在当前条件集下，添加新的条件。默认情况下，使用 **OR** 运算符将其与同一级别上的条件连接，尽管还可以将运算符改为 **AND**。

例如，如果将简单条件添加至以下规则：

结果为：



要添加一个复杂的条件，请执行以下操作：

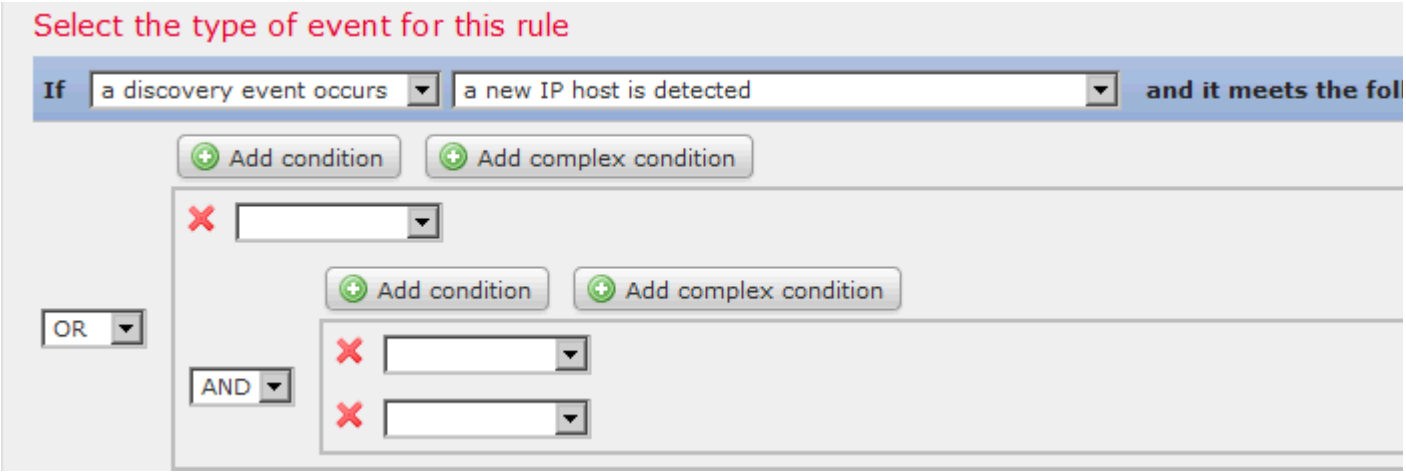
访问：管理员/发现管理员

步骤 1　点击当前条件上方的 **Add complex condition**。

复杂条件会被添加到当前条件集的下方。复杂条件包括两个子条件，这两个子条件会用相反的运算符从用于连接上一级别的条件相互连接。

例如，如果将复杂条件添加至以下规则：

结果为：



要连接条件，请执行以下操作：

访问：管理员/发现管理员

步骤 1　使用条件集左侧的下拉列表。选择:

- **AND** 运算符要求满足其控制的级别上的所有条件
- **OR** 运算符要求只满足其控制的级别上的一个条件

在一个条件中使用多个值

许可证：任何环境

在构建条件，且条件语法允许您从下拉列表中选择值时，通常可以从列表中选择多个值。例如，如果要将主机配置文件限定条件添加至需要主机运行 UNIX 的规则，而非构建使用 OR 运算符连接的多个条件，请使用以下操作步骤。

要在一个条件中包含多个值，请执行以下操作：

访问：管理员/发现管理员

步骤 1　构建一个条件，选择 **is in** 或 **is not in** 作为运算符。

下拉列表更改至文本字段。

步骤 2　点击文本字段或 **Edit** 链接的任意位置。

系统将显示一个弹出窗口。

步骤 3　在 **Available** 下，点击的同时使用 Ctrl 或 Shift 选择多个值。也可以点击并拖动以选择多个相邻值。

步骤 4　点击右箭头 (**>**) 以将选定条目移至 **Selected**。

步骤 5　点击 **OK**。

系统再次显示 Create Rule 页面。条件值字段中显示选择的结果。

管理关联策略的规则

许可证：任何环境

使用 Rule Management 页面管理在关联策略中使用的关联规则。可以创建、修改和删除规则。还可以创建规则组以便组织关联规则。有关修改规则规则、删除规则和创建规则组的详细信息，请参阅：

- 第 51-39 页上的修改规则
- 第 51-39 页上的删除规则
- 第 51-39 页上的创建规则组

有关创建规则的详细信息，请参阅第 51-2 页上的创建关联策略规则。

修改规则

许可证：任何环境

使用以下操作步骤来修改现有的关联规则。

要修改现有规则，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**，然后选择 **Rule Management** 选项卡。

系统将显示 Rule Management 页面。

步骤 2　如果规则在规则组中，则点击规则组名称展开该组。

步骤 3　点击要修改的规则旁边的编辑图标 ( )。

系统将显示 Create Rule 页面。

步骤 4　根据需要进行修改并点击 **Save**。

规则更新成功。

删除规则

许可证：任何环境

您不能删除在一个或多个关联策略中使用的关联规则；您必须首先从包含该规则的所有策略中删除该规则。有关从策略中删除规则的详细信息，请参阅第 51-47 页上的编辑关联策略。

要删除现有规则，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**，然后选择 **Rule Management** 选项卡。

系统将显示 Rule Management 页面。

步骤 2　如果规则在规则组中，则点击规则组名称展开该组。

步骤 3　点击要删除的规则旁边的删除图标 ( )。

步骤 4　确认要删除的规则。

规则删除成功。

创建规则组

许可证：任何环境

创建规则组以便组织关联规则。 FireSIGHT 系统附带许多根据功能分组的默认规则。例如，Worms 规则组包括检测一般蠕虫活动的规则。请注意，规则组之所以存在仅为了便于组织关联规则；不能将规则组分配至关联策略。相反，可以单独添加规则。

当创建规则时，可以将该规则添加至现有规则组。此外，还可以修改现有规则以将其添加至规则组。有关详细信息，请参阅：

- 第 51-2 页上的创建关联策略规则
- 第 51-39 页上的修改规则

提示 要删除规则组，请点击要删除的组旁边的删除图标 ( )。当删除规则组时，并**未**删除该规则组中的规则。更确切地说，它们仅是未分组而已。

要创建规则组，请执行以下操作：

访问：管理员/发现管理员

步骤 1 选择 **Policies > Correlation**，然后选择 **Rule Management** 选项卡。

系统将显示 Rule Management 页面。

步骤 2 点击 **Create Group**。

系统将显示 Create Group 页面。

步骤 3 在 **Group Name** 字段中键入组的名称。

步骤 4 点击 **Add Group**。

该组添加成功。

对关联响应进行分组

许可证：任何环境

在创建警报响应和修复后 （请参阅第 43-2 页上的使用警报响应和第 54-1 页上的创建补救），可将它们进行分组以便策略违规触发组中所有的响应。在将响应组分配至关联规则前，必须在 Groups 页面上创建组。

组旁边的滑动图标表示该组是否处于活动状态。要将响应组分配至关联策略中的规则，必须激活该响应组。使用 **Sort by** 下拉列表按状态 （活动和非活动）或按字母顺序排列的名称对响应组进行分类。

有关详细信息，请参阅：

- 第 51-40 页上的创建响应组
- 第 51-41 页上的修改响应组
- 第 51-41 页上的删除响应组
- 第 51-42 页上的激活和停用响应组

创建响应组

许可证：任何环境

可将单个警报和修复置于响应组中，然后可将响应组分配至关联策略中的规则，以便违反策略时发起一组警报和修复。将组分配至活动策略中的规则后，系统自动将组的变化和组中的警报和修复的变化应用到活动策略中。

要创建响应组，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Correlation**，然后点击 **Groups**。

系统将显示 Groups 页面。

步骤 2　点击 **Create Group**。

系统将显示 Response Group 页面。

步骤 3　在 **Name** 字段中键入新响应组的名称。

步骤 4　选择 **Active** 激活该响应组，以便可以使用该组响应关联策略违规。

步骤 5　从 **Available Responses** 列表中选择要包含在响应组中的警报和修复。

提示　点击时按住 Ctrl 键，以选择多个响应。

步骤 6　点击 **>** 将警报和修复移至响应组。

相反地，可以从 **Responses in Group** 列表选择警报和修复，然后点击 **<** 从响应组中移出警报。

步骤 7　点击 **Save**。

组创建成功。

修改响应组

许可证：任何环境

使用以下操作步骤修改响应组。

要修改响应组，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Correlation**，然后点击 **Groups**。

系统将显示 Groups 页面。

步骤 2　点击要修改的组旁边的编辑图标 ( )。

系统将显示 Response Group 页面。

步骤 3　根据需要做出更改，然后点击 **Save**。

如果响应组处于活动和使用状态，所作更改立即生效。

删除响应组

许可证：任何环境

如果关联策略中没有使用响应组，可以删除该组。删除响应组**不会**删除响应组中的响应，仅删除相互之间的联系。

要删除响应组，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Correlation**，然后点击 **Groups**。

系统将显示 Groups 页面。

步骤 2　点击要删除的响应组旁边的删除图标 ( )。

步骤 3　确认要删除的响应组。

响应组删除成功。

激活和停用响应组

许可证：任何环境

您可以在不删除响应组的情况下，暂时停用响应组。这样可以在系统中保留响应组，但当违反响应组所分配到的策略时不会发起响应组。请注意，如果停用响应组时关联策略中使用该响应组，则依然认为响应组处于使用状态，尽管该响应组被停用；不能删除正在使用中的响应组。

要激活或停用响应组，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Correlation**，然后点击 **Groups**。

系统将显示 Groups 页面。

步骤 2　点击要激活或停用的响应组旁边的滑动图标。

如果响应组被激活，则已将其停用。如果其被停用，则已将其激活。

创建关联策略

许可证：任何环境

在创建关联规则或白名单 （或两者），或者警报响应和修复之后，可以使用它们来构建关联策略。

当网络流量满足关联规则或有效策略中的白名单规定的标准时，防御中心生成关联事件或白名单事件。其还可以发起分配至规则或白名单的任何响应。可以将规则或白名单映射至单个响应或一组响应。如果网络流量触发多个规则或白名单，则防御中心发起与每个规则和白名单相关的所有响应。

有关创建关联规则、合规性白名单和可用于构建关联策略的响应的详细信息，请参阅：

- 第 51-2 页上的创建关联策略规则
- 第 52-7 页上的创建合规白名单
- 第 43-1 页上的配置外部警报
- 第 54-1 页上的配置补救

提示　或者，创建基本策略，然后对基本策略进行修改以添加规则和响应。

要创建关联策略，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**。

系统将显示 Policy Management 页面。

步骤 2　点击 **Create Policy**。

系统将显示 Create Policy 页面。

步骤 3　提供基本策略信息，例如名称和说明。

请参阅第 51-43 页上的提供基本策略信息。

步骤 4　将一个或多个规则或白名单添加至关联策略。

请参阅第 51-44 页上的将规则和白名单添加至关联策略。

步骤 5　或者，设置规则和白名单优先级。

请参阅第 51-44 页上的设置规则和白名单优先级。

步骤 6　或者，将响应添加至以已添加的规则或白名单。

请参阅第 51-45 页上的将响应添加至规则和白名单。

步骤 7　点击 **Save**。

该策略保存成功。

注　在策略可以生成关联事件和白名单事件并向策略违规发起响应前，必须先激活该策略。有关详细信息，请参阅第 51-46 页上的管理关联策略。

提供基本策略信息

许可证：任何环境

您必须为每个策略提供一个识别名称。或者，将简要说明添加至策略。

此外，还可以将用户定义的优先级分配给策略。如果已经违反关联策略，则产生的关联事件显示分配给该策略的优先级 （除非已经触发的规则已经拥有自己的优先级）。

注　规则和白名单优先级覆盖策略优先级。有关详细信息，请参阅第 51-44 页上的将规则和白名单添加至关联策略。

要提供基本的策略信息，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Policy 页面上，在 **Policy Name** 字段中，键入策略名称。

步骤 2　在 **Policy Description** 字段中，输入策略的说明内容。

步骤 3　从 **Default Priority** 下拉列表中选择策略的优先级。

可以从 1 至 5 中选一个优先级值，其中 1 表示优先级最高， 5 表示优先级最低。或者，可以选择 **None** 以仅使用分配给特定规则的优先级。

步骤 4　继续执行下一节第 51-44 页上的将规则和白名单添加至关联策略中的操作步骤。

将规则和白名单添加至关联策略

许可证：任何环境

关联策略包含一个或多个规则或白名单。如果违反策略中的任何规则或白名单，则系统将事件记录到数据库中。如果将一个或多个响应分配给规则或白名单，则发起这些响应。

下图显示由合规性白名单和一组配置有各种响应的关联规则所组成的关联策略。

要将规则或白名单添加至关联策略中，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Policy 页面上，点击 **Add Rules**。

系统将显示一个 Available Rules 弹出窗口。

步骤 2　点击适当的文件夹名称将其展开。

步骤 3　选择策略中要使用的规则和白名单，然后点击 **Add**。

系统再次显示 Create Policy 页面。所选规则和白名单填充该策略。

步骤 4　继续执行下一节第 51-44 页上的设置规则和白名单优先级中的操作步骤。

设置规则和白名单优先级

许可证：任何环境

您可以将用户定义的优先级分配给关联策略中的每个关联规则或合规性白名单。如果触发规则或白名单，则产生的事件显示分配给规则或白名单的优先级。另一方面，如果没有分配优先级值且触发规则或白名单，产生的事件显示策略的优先级值。

例如，可以考虑这样一个策略：策略本身的优先级为 1，其规则或白名单设置有默认的优先级，但异常情况是一个规则的优先级设为 3。如果触发优先级为 3 的规则，则产生的关联事件显示 3 作为其优先级值。如果触发策略中的其他规则或白名单，则产生的事件显示 1 作为其从策略优先级中保留的优先级值。

要设置规则或白名单优先级，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Policy 页面上，从每个规则或白名单的 **Priority** 列表中选择默认优先级。可以选择：

- 从 1 至 5 中选一个优先级值，其中 1 表示优先级最高， 5 表示优先级最低。
- **无**
- **Default**，以使用策略的默认优先级

步骤 2　继续执行下一节第 51-45 页上的将响应添加至规则和白名单中的操作步骤。

将响应添加至规则和白名单

许可证：任何环境

在关联策略中，您可以将每个规则或白名单映射至单个响应或一组响应。当违反策略中的任何一个规则或白名单时，系统将关联事件记录到数据库中并发起分配至该规则或白名单的响应。如果触发策略中的多个规则或白名单，防御中心发起与每个规则或白名单相关的响应。

有关创建响应和响应组的详细信息，请参阅：

- 第 43-1 页上的配置外部警报
- 第 54-1 页上的配置补救
- 第 51-40 页上的对关联响应进行分组

注　**不能**将 Nmap 修复作为响应分配至在流量量变曲线变更上触发的关联规则。系统不会发起修复。

下图显示由合规性白名单和一组配置有各种响应的关联规则所组成的关联策略。

Policy Rules

Rule	Responses
Bugbear Worm Detects the Bugbear HTTP server backdoor	Sample Email Alert Response (Email
Default White List	Sample SNMP Alert Response (SNMP
Lovgate Worm Detects activity by the Lovgate worm backdoor component	Sample Syslog Alert Response (Sysl
MyDoom Worm Detects activity by the backdoor component of MyDoom	Sample Syslog Alert Response (Sysl Sample SNMP Alert Response (SNMP Sample Email Alert Response (Email
NetSky.S Detects the backdoor component of the NetSky.S worm.	This rule does not have any respons

要将响应添加至规则和白名单，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Policy 页面上，点击要添加响应的规则或白名单旁边的响应图标 ()。

系统将显示一个弹出窗口。

步骤 2　在 **Unassigned Responses** 下，选择当触发规则或白名单时要发起的响应、多种响应或响应组，并点击向上箭头。

提示　点击时按住 Ctrl 键，以选择多个响应。

步骤 3　点击**更新**。

系统再次显示 Create Policy 页面。将指定的响应添加至规则或白名单。

管理关联策略

许可证：任何环境

您可以在 Policy Management 页面上管理关联策略。可以创建、修改、分类、激活、停用和删除策略。

策略旁边的滑动图标表示该组是否处于活动状态。如果要通过策略生成关联事件和白名单事件，必须激活该策略。使用 **Sort by** 下拉列表按状态 （活动和非活动）或按字母顺序排列的名称对策略进行分类。

如果活动的关联策略包含合规性白名单，下列操作**无法**删除与白名单相关的主机属性，也不会改变主机属性值：

- 停用策略
- 修改策略以移除白名单
- 删除策略

例如，执行操作时兼容的主机在主机属性网络映射上仍旧显示为兼容等。要删除主机属性，必须删除相应的白名单。

要更新网络上的主机的白名单合规性，必须重新激活关联策略 （如果其被停用）或将白名单添加至另一个活动的关联策略 （如果从关联策略中删除白名单或删除策略本身）。请注意，在执行此操作时会重新评估白名单，这**不**会生成白名单事件，因此也不会触发任何与白名单有关的任何响应。有关合规性白名单的详细信息，请参阅第 52-1 页上的将 FireSIGHT 系统用作一个合规工具。

有关管理关联策略的详细信息，请参阅：

- 第 51-47 页上的激活和停用关联策略
- 第 51-47 页上的编辑关联策略
- 第 51-47 页上的删除关联策略

有关创建新策略的详细信息，请参阅第 51-42 页上的创建关联策略。

激活和停用关联策略

许可证：任何环境

使用以下操作步骤激活或停用关联策略。

要激活或停用策略，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**。

系统将显示 Policy Management 页面。

步骤 2　点击要激活或停用的策略旁边的滑动图标。

如果策略处于活动状态，则已将其停用。如果其被停用，则已将其激活。

编辑关联策略

许可证：任何环境

使用以下操作步骤修改关联策略。

要编辑策略，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**。

系统将显示 Policy Management 页面。

步骤 2　点击策略旁边的编辑图标 ( )。

系统将显示 Create Policy 页面。有关可更改的各种配置的信息，请参阅第 51-42 页上的创建关联策略。要从关联策略中移除规则或白名单，请在 Create Policy 页面上点击要移除的规则或白名单旁边的删除图标 ( )。

步骤 3　根据需要做出更改，然后点击 **Save**。

该策略更改成功。如果该策略处于活动状态，则所作更改立即生效。

删除关联策略

许可证：任何环境

使用以下操作步骤删除关联策略。

要删除策略，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**。

系统将显示 Policy Management 页面。

步骤 2　点击要删除的策略旁边的删除图标 ( )。

该策略删除成功。

使用关联事件

许可证：任何环境

当活动的关联策略中的关联规则触发时，防御中心生成关联事件并将其记录至数据库。有关配置保存在数据库中的关联事件数量的详细信息，请参阅第 63-14 页上的配置控制面板事件限制。

注　当活动的关联策略中的合规性白名单触发时，防御中心生成白名单事件。有关详细信息，请参阅第 52-26 页上的处理白名单事件。

有关详细信息，请参阅：

- 第 51-48 页上的查看关联事件
- 第 51-50 页上的了解关联事件表
- 第 51-51 页上的搜索关联事件

查看关联事件

许可证：任何环境

您可以查看关联事件表，然后根据查找的信息操作事件视图。

访问关联事件时看到的页面随使用的工作流程而变化。可以使用预定义的工作流程，其中包括关联事件表视图。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关创建自定义工作流程的信息，请参阅第 58-34 页上的创建自定义工作流程。

下表介绍在关联事件工作流程页面上可进行的某些特定操作。

表 51-16　关联事件操作

要.....	您可以.....
查看 IP 地址的主机配置文件	点击 IP 地址旁边显示的主机配置文件图标。
查看用户配置文件信息	点击用户标识旁边显示的用户图标 ( )。有关详细信息，请参阅第 50-55 页上的了解用户详细信息和主机历史记录。
对当前工作流程页面上的事件进行排序和限制	在第 58-29 页上的对向下钻取工作流程页面进行排序中获得详细信息。
在当前工作流程页面中导航	在第 58-30 页上的导航到工作流程中的其他页面中获得详细信息。
在当前工作流程中的页面之间导航，同时保留当前限制条件	点击工作流程页面左上角的相应页面链接。有关详细信息，请参阅第 58-16 页上的使用工作流程页面。
了解有关显示的列的详细信息	在第 51-50 页上的了解关联事件表中获得详细信息。

表 51-16　关联事件操作 （续）

要.....	您可以.....
修改所显示事件的时间和日期范围	在第 58-19 页上的设置事件时间限制中查找详细信息。 请注意，如果按时间限制事件视图，则在设备配置的时间段外生成的事件 （无论是全局或特定事件）可能显示在事件视图中。即使已经为设备配置一个滑动时间窗，这种情况仍然可能发生。
向下钻取到工作流程中的下一页，限制特定值	可使用以下其中一种方法： • 在自定义工作流程中创建的向下展开页面上，点击某行内的一个值。请注意，点击表视图行中的值可限制表视图，且不会向下钻取到下一页。 • 要向下钻取到限制某些用户的下一个工作流程页面，在要在下一个工作流程页面上查看的用户旁，选择复选框，然后点击 **View**。 • 要向下钻取到保留当前限制的下一工作流程页面，请点击 **View All**。 **提示**　表视图的页面名称中始终包括“Table View”。 有关详细信息，请参阅第 58-26 页上的限制事件。
从系统中删除关联事件	可使用以下其中一种方法： • 要删除某些事件，请选择要删除的事件旁边的复选框，然后点击 **Delete**。 • 要删除当前已限制视图中的所有事件，点击 **Delete All**，然后确认要删除所有事件。
导航至其他事件视图查看相关事件	在第 58-31 页上的在工作流程之间导航中获得详细信息。

要查看关联事件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Correlation > Correlation Events**。

系统显示默认关联事件工作流程的首页。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示任何事件，可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

提示　如果正在使用不包括关联事件表视图的自定义工作流程，请点击 (**switch workflow**)，然后选择 **Correlation Events**。

了解关联事件表

许可证：任何环境

当关联规则触发时，防御中心生成关联事件。下表介绍关联事件表中的字段。

表 51-17　　关联事件字段

字段	说明
时间	生成关联事件的日期和时间。
影响	基于入侵数据、发现数据和漏洞信息之间的关联分配给关联事件的影响级别。有关详细信息，请参阅第 41-32 页上的使用影响级别评估事件。
Inline Result	以下任一选项： • 一个黑色向下箭头，表示系统丢弃触发入侵规则的数据包 • 一个灰色向下箭头，表示如果启用 **Drop when Inline** 入侵策略选项，则系统已经丢弃内联中的数据包、交换或路由部署 • 空白，表示触发的入侵规则未设置为 Drop and Generate Events 请注意，不管规则状态或入侵策略的丢弃行为如何 （包括当内联集处于分路模式下），系统都无法在被动部署情况下丢失数据包。
Source IP 或 目标 IP：	触发策略违规的事件中的源主机或目标主机的 IP 地址。
Source Country 或 Destination Country	与触发策略违规的事件中的 源 IP 地址或目标 IP 地址相关的国家/地区。
Security Intelligence Category	代表或包含触发策略违规的事件中的列入黑名单的 IP 地址的被列入黑名单的对象的名称。
Source User 或 Destination User	登录触发策略违规的事件中的源主机或目标主机的用户的姓名。
Source Port/ICMP Type 或 Destination Port/ICMP Code	与触发策略违规的事件有关的源流量的源端口或 ICMP 类型或者目标流量的目标端口或 ICMP 代码。
说明	关联事件的说明。说明中的信息取决于规则触发方式。 例如，如果操作系统的信息更新事件触发规则，则系统显示新的操作系统名称和可信度。
策略	违反的策略的名称。
Rule	触发策略违规的规则的名称。
优先级	触发策略违规的策略或规则指定的优先级。
Source Host Criticality 或 Destination Host Criticality	涉及关联事件的源主机或目标主机的用户分配的主机重要性：`None`、`Low`、`Medium` 或 `High`。 请注意，只有基于发现事件、主机输入事件或连接事件按规则生成的关联事件才包含源主机重要性。有关主机重要性的详细信息，请参阅第 49-27 页上的使用预先定义的主机属性。
Ingress Security Zone 或 Egress Security Zone	触发策略违规的入侵或连接事件的入口或出口安全区域。
设备	生成触发策略违规的事件的设备的名称。

表 51-17　关联事件字段 （续）

字段	说明
Ingress Interface 或 Egress Interface	触发策略违规的入侵或连接事件的入口或出口界面。
计数	与每行中所显示的信息匹配的事件数。注意，**Count** 字段仅在应用了创建两个或多个相同行的约束后才显示。

有关显示关联事件表的详细信息，请参阅：

- 第 51-48 页上的查看关联事件
- 第 51-51 页上的搜索关联事件

搜索关联事件

许可证：任何环境

您可以搜索特定的关联事件。您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。下表列出了可以使用的搜索条件。

表 51-18　关联事件搜索条件

字段	搜索条件规则
策略	键入要搜索的关联策略的名称。
Rule	键入要搜索的关联规则的名称。
说明	键入全部或部分关联事件说明。说明中的信息取决于触发规则的事件。
优先级	指定关联事件的优先级，其根据触发的规则或违反的关联策略的优先级确定。输入 `none`，表示没有优先级。有关设置关联规则和策略优先级的详细信息，请参阅第 51-43 页上的提供基本策略信息和第 51-44 页上的设置规则和白名单优先级。
Source Country Destination Country 或 Source/Destination Country	指定与触发策略违规的事件中的源、目标、或者源或目标主机 IP 地址相关的国家/地区。
Source Continent、 Destination Continent 或 Source/Destination Continent	指定与触发策略违规的事件中的源、目标、或者源或目标主机 IP 地址相关的洲。
Security Intelligence Category	指定与触发策略违规的关联事件相关的安全情报类别。安全情报类别可能是安全情报对象的名称、全局黑名单、自定义安全情报列表或源，或者情报源中的其中一个类别。有关详细信息，请参阅第 13-1 页上的使用安全情报 IP 地址信誉实施黑名单。
Source IP、 Destination IP 或 Source/Destination IP	指定触发策略违规的事件中的源、目标或者源或目标主机的 IP 地址。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。也可使用求反。有关详情，请参见第 60-6 页上的在搜索中指定 IP 地址。
Source User 或 Destination User	指定登录触发策略违规的事件中的源主机或目标主机的用户。
Source Port/ICMP Type 或 Destination Port/ICMP Code	指定与触发策略违规的事件有关的源流量的源端口或 ICMP 类型或者目标流量的目标端口或 ICMP 代码。

表 51-18　关联事件搜索条件 （续）

字段	搜索条件规则
影响	指定分配给关联事件的影响。有效值（不区分大小写）包括 `Impact 0`、`Impact Level 0`、`Impact 1`、`Impact Level 1`、`Impact 2`、`Impact Level 2`、`Impact 3`、`Impact Level 3`、`Impact 4` 和 `Impact Level 4`。请勿使用影响图标颜色或部分字符串（例如，请勿使用 `blue`、`level 1` 或 `0`）。有关详细信息，请参阅第 41-32 页上的使用影响级别评估事件。
Inline Result	对于入侵事件触发的策略违规，键入： • `dropped`，用来指定是否已经在内联、交换的或路由的部署中丢弃数据包 • `would have dropped`，用来指定如果已经设置入侵策略以在内联、交换的或路由的部署中丢弃数据包，则是否将丢弃该数据包 请注意，不管规则状态或入侵策略的丢弃行为如何（包括当内联集处于分路模式下），系统都无法在被动部署情况下丢失数据包。
Source Host Criticality 或 Destination Host Criticality	指定涉及策略违规的源主机或目标主机的的主机重要性：`None`、`Low`、`Medium` 或 `High`。请注意，只有基于发现事件、主机输入事件或连接事件按规则生成的关联事件才包含源主机重要性。有关主机重要性的详细信息，请参阅第 49-27 页上的使用预先定义的主机属性。
Ingress Security Zone、Egress Security Zone 或 Ingress/Egress Security Zone	指定触发策略违规的入侵事件或连接事件中的入口、出口或者入口或出口安全区域。
设备	键入设备名称或 IP 地址或设备组、堆栈或集群名称，将搜索限制于已生成触发策略违规的事件的特定设备。有关 FireSIGHT 系统如何处理搜索中的设备字段的详细信息，请参阅第 60-6 页上的在搜索中指定设备。
Ingress Interface 或 Egress Interface	指定触发策略违规的入侵或连接事件的入口或出口界面。

要搜索关联事件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Correlation Events**。

页面根据相应限制进行更新。

步骤 3　在相应字段中输入搜索条件，如关联事件搜索条件表所述：

- 所有字段都接受求反 (`!`)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。

  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 在任一字段指定 `n/a` 以便识别信息不适用于该字段的事件；使用 `!n/a` 识别字段填充事件。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法 （包括在搜索中使用对象）的详细信息，请参阅第 60-1 页上的搜索事件。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。
- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认关联事件工作流程中，受到当前的时间范围的限制。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

第 52 章

将 FireSIGHT 系统用作一个合规工具

合规白名单（或*白名单*）是允许用户指定可在特定子网上运行的操作系统、应用及和协议的一系列标准，并且如果该子网上的主机违反了白名单，则会自动生成事件。例如，安全策略可声明，当允许网络服务器运行 HTTP 时，该网络上的其他主机均不得运行 HTTP。可以创建一份白名单，评估整个网络 （不包括网络场），以确定哪些主机正在运行 HTTP。

请注意，可以创建一条执行此功能的关联规则，对该 规则进行配置，使其在下列情况下触发：

- 系统发现了有关应用协议的新信息
- 应用协议的名称为 HTTP
- 该事件中涉及的主机的 IP 地址不在相关网络场之中

关联规则能够以更灵活的方式发送警报，并对网络上的违规行为作出反应，但是，其配置和维护过程比白名单更复杂。关联规则的范围也更广，当其中一种类型的事件符合指定的任何条件时，可以生成关联事件。另一方面，白名单专门用于评估网络上运行的操作系统、应用协议、客户端、网络应用及通信协议是否违反了组织的策略。

可以创建符合特定需求的自定义白名单，也可以使用由思科漏洞研究团队 (VRT) 创建的默认白名单。该白名单包含适用于所允许的操作系统、应用协议、客户端、网络应用及通信协议的建议设置。您可能还想根据网络环境来自定义默认的白名单。

如果在活动关联策略中添加白名单，系统检测到主机违反白名单时，会将白名单事件 （一种特殊类型的关联活动）记入数据库。此外，还可以配置系统，使系统在检测到白名单被违反时自动触发响应 （补救措施和警报）。

注 虽然可以配置网络发现策略，根据支持 NetFlow 的设备所导出的数据，在网络映射中添加主机和应用协议，但是，有关这些主机和应用协议的可用信息受到限制。例如，这些主机没有可用的操作系统数据，除非您使用主机输入功能提供这些数据。这样可能会影响创建合规白名单的方式。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

系统会创建每台主机的属性，以表明该主机是否符合所创建白名单的条件，因此提供了网络合规性的一览汇总。只需几秒钟，便可以确定组织内的哪些主机违反了策略正在运行 HTTP，并采取相应的行动。

然后，使用关联功能配置系统，使系统在网络场之外的主机开始运行 HTTP 时发出警报。

此外，系统允许使用主机配置文件，来确定是否有单个主机违反了所配置的任何白名单以及违反白名单的方式。 FireSIGHT 系统还提供工作流程，可用于查看违反白名单的各违规行为以及每台主机的违规次数。

最后，可以使用控制面板监控系统范围内最近的合规活动，包括白名单事件以及网络整体合规性的汇总视图。

有关创建和管理合规白名单以及解释白名单事件和违规行为的详细信息，请参阅以下各节：

- 第 52-2 页上的了解合规白名单
- 第 52-7 页上的创建合规白名单
- 第 52-20 页上的管理合规白名单
- 第 52-21 页上的使用共享主机配置文件
- 第 52-26 页上的处理白名单事件
- 第 52-30 页上的处理白名单的违规事件

此外，有关详细信息，请参阅以下章节：

- 第 51-42 页上的创建关联策略介绍如何创建并配置包括合规白名单在内的关联策略，并说明如何向白名单分配响应活动和优先级。
- 第 49-1 页上的使用主机配置文件介绍如何使用主机的配置文件确定是否违反任何白名单。
- 第 55-1 页上的使用控制面板介绍如何获取当前系统状态（包括白名单合规活动）的一览视图。

了解合规白名单

许可证：FireSIGHT

*合规白名单*指允许用户指定可在网络上运行的操作系统、客户端、应用协议、网络应用和通信协议的一系列标准。可以创建符合特定需求的自定义白名单，也可以使用由 VRT 创建的包含建议设置的默认白名单。

自定义白名单的条件可以简单；可以指定只允许运行某个特定操作系统的主机。条件也可以复杂；可以指定当允许运行所有操作系统时，只允许运行某个特定操作系统的主机在特定端口上运行某个特定的应用协议。

白名单由两个主要部分组成：*目标*和*主机配置文件*。目标指白名单评估的特定主机，而主机配置文件则指定了允许在目标上运行的操作系统、客户端、应用协议、网络应用及通信协议。

创建了一个白名单并将其添加到活动的关联策略后，系统会根据主机配置文件来评估白名单的目标，以确定这些目标是否符合白名单的条件。完成初始评估后，当系统检测到某个有效目标违反了白名单时，会生成*白名单事件*。

有关详细信息，请参阅：

- 第 52-3 页上的了解白名单的目标介绍白名单如何只以指定的主机为目标。
- 第 52-3 页上的了解白名单主机配置文件介绍不同类型的配置文件，这些配置文件描述了允许在网络上运行的客户端、应用协议、网络应用及通信协议。
- 第 52-5 页上的了解白名单评估介绍系统如何根据白名单来评估网络上的主机，以及如何区分哪些主机是合规的，而哪些主机是违规的。
- 第 52-5 页上的了解白名单违规介绍系统如何检测并通知白名单的违规行为。

了解白名单的目标

许可证：FireSIGHT

创建一份白名单时，首先应指定适用的网络部分。可以使用白名单来评估受监控网络上的所有主机，也可以对白名单进行限制，只评估特定的网段甚至是个别主机。还可以进一步限制白名单，只评估具备特定主机属性或者属于某个特定的 VLAN 的主机。符合白名单评估条件的主机被称为*有效目标*（或*目标*）。有效目标：

- 必须在指定的 IP 地址块中。还可以将 IP 地址块排除在外。
- 必须具备至少一个指定的主机属性。

  例如，可以将白名单配置为只评估主机重要性较高的主机。有关主机属性（包括主机重要性）的信息，请参阅第 49-27 页上的使用用户定义的主机属性和第 49-27 页上的使用预先定义的主机属性。
- 必须属于某个指定的 VLAN。

如果主机不满足所有这些条件，系统便不会根据白名单对其进行评估，无论主机配置文件是否违反了白名单。

如果白名单包含多个目标，则主机必须符合其中一个目标的指定条件，才被视为有效。例如，如果创建了一个包括 10.10.x.x 网络的目标和一个不包括 10.10.x.x 网络的目标，该网络中的主机会被视为有效目标。请注意，如果白名单不包含任何目标，则系统不会根据该白名单对网络上的任何主机进行评估。

白名单的目标网络在 Create White List 页面的左侧列出。请注意，默认白名单使用目标 0.0.0.0/0 和 ::/0，表示整个受监控网络。如果选择使用此白名单，则可以让目标网络保留原样，或根据网络环境对其进行修改。

有关创建白名单目标的详细信息，请参阅第 52-9 页上的配置合规白名单的目标。

了解白名单主机配置文件

许可证：FireSIGHT

指定了白名单的评估对象之后，下一步便是配置*主机配置文件*。白名单中的主机配置文件指定了允许在目标主机上运行的操作系统、客户端、应用协议、网络应用及通信协议。

在白名单中可以配置三种类型的主机配置文件，分别是：全局主机配置文件、特定操作系统的主机配置文件以及共享主机配置文件。创建白名单时，每一种主机配置文件有不同的显示方式。

下表说明了如何识别和访问不同类型的主机配置文件。

表 52-1　　访问合规白名单主机配置文件

要查看.....	在允许的主机配置文件下，点击.....
白名单的全局主机配置文件	**任何操作系统**
特定操作系统的主机配置文件	以纯文本形式而不是斜体格式列出的主机配置文件的名称
白名单使用的共享主机配置文件	以斜体格式列出的主机配置文件的名称

有关详细信息，请参阅：

- 第 52-4 页上的了解全局主机配置文件
- 第 52-4 页上的了解特定操作系统的主机配置文件
- 第 52-4 页上的了解共享主机配置文件

了解全局主机配置文件

许可证：FireSIGHT

所有白名单均包含一个全局主机配置文件，该文件指定了允许在目标主机上运行的应用协议、客户端、网络应用及通信协议，无论该主机使用的是什么操作系统。

例如，无需编辑多个 Microsoft Windows 和 Linux 主机配置文件以允许 Internet Explorer，可以将全局主机配置文件配置为允许 Internet Explorer，无论检测到该主机使用的是什么操作系统。请注意，始终允许在每台主机上运行 ARP、 IP、 TCP 和 UDP 通信协议；这些通信协议无法被禁用。有关详细信息，请参阅第 52-12 页上的配置全局主机配置文件。

了解特定操作系统的主机配置文件

许可证：FireSIGHT

必须为允许在网络上运行的各个操作系统创建一个主机配置文件。要禁止网络上的某个操作系统，则不要创建该操作系统的主机配置文件。例如，为了确保网络上的所有主机均运行 Microsoft Windows，请将白名单配置为只包含该操作系统的主机配置文件。

创建某个操作系统的主机配置文件时，可以要求该操作系统具有特殊版本。例如，可以要求主机运行 Windows 7 或 Server 2008 R2。

为某个特定的操作系统创建主机配置文件后，可以指定允许在使用该操作系统的目标主机上运行的应用协议、客户端、网络应用及通信协议。例如，可以允许 SSH 于端口 22 在 Linux 主机上运行。还可以将特殊供应商和版本限定为 OpenSSH 4.2。

请注意，主机在被识别之前，一直处于符合所有白名单条件的状态。但是，可以为未知主机创建一份白名单主机配置文件。

注　未识别的主机不同于未知主机。*未识别的*主机是指系统尚未收集足够的信息识别其操作系统的主机。*未知*主机是指系统对其流量进行过分析，但其操作系统与任何已知指纹均不匹配的主机。

有关详细信息，请参阅第 52-12 页上的创建特定操作系统的主机配置文件。

了解共享主机配置文件

许可证：FireSIGHT

共享主机配置文件与特定的操作系统绑定，但是每个共享主机配置文件可以在多个白名单中使用。也就是说，如果创建了多个白名单，但要使用相同的主机配置文件来评估运行白名单中规定的特定操作系统的主机，可使用共享主机配置文件。

例如，如果想要为世界范围内多个办公地点创建单独的白名单，但对运行 Apple Mac OS X 的所有主机使用同一个配置文件，则可以为该操作系统创建共享配置文件，并在所有白名单中使用该配置文件。

默认白名单提供了为允许运行的操作系统、客户端、应用协议、网络应用和通信协议建议的“最佳实践”设置。此白名单使用共享主机配置文件的一个特殊类别，即*内置主机配置文件*。请注意，内置主机配置文件标有内置主机配置文件的图标 ( )。

内置主机配置文件使用内置应用协议、通信协议和客户端。您可以在默认白名单以及创建的任何自定义白名单中按原样使用这些元素，或根据需要对这些元素进行修改。在内置主机配置文件以及使用这些元素的任何其他主机配置文件中，这些元素以斜体显示。

请记住，与所有共享主机配置文件相同，如果对某个内置主机配置文件进行修改，则会影响到使用该配置文件的所有白名单。同样，如果对某个内置应用协议、通信协议或客户端进行修改，则会影响到使用它的所有白名单。

有关共享主机配置文件的详细信息，请参阅第 52-21 页上的使用共享主机配置文件。

了解白名单评估

许可证：FireSIGHT

创建白名单主机配置文件并保存该白名单后，可以将白名单添加至关联策略，如同添加一个关联规则。有关详细信息，请参阅第 51-1 页上的配置关联策略和规则。

启用该关联策略后，系统会根据白名单的条件来评估其目标。然后，您可以使用主机属性网络映射，获取网络上符合条白名单件的主机的整体视图。

分配给网络上每台主机的主机属性与白名单上的名称相同。此主机属性值可以为以下当中的一种：

- **合规**，适用于符合白名单条件的有效目标
- **违规**，适用于违反白名单的有效目标
- **未评估**，适用于出于任何原因尚未评估的无效目标和主机

请注意，如果网络规模庞大，并且系统正在根据白名单评估网络映射中的所有有效目标，则尚未被评估的目标将被标记为*未评估*。系统完成处理后，更多的主机属性将从*未评估*更改为*合规*或*违规*。系统每秒可以评估约 100 台主机。

此外，如果系统没有足够的信息来确定主机是否合规，则该主机可能会被标记为*未评估*。例如，如果系统检测到一台新主机但尚未收集到在该主机上运行的操作系统、客户端、应用协议、网络应用或通信协议的相关信息，就可能出现这种情况。

注　如果您从一台主机更改或删除主机属性，则执行更改或删除操作后，该主机将不再是有效的目标，主机属性从*合规*或*违规*更改为*未评估*。

有关主机属性的详细信息，请参阅第 48-8 页上的处理主机属性网络映射。

了解白名单违规

许可证：FireSIGHT

完成白名单的初始评估后，当系统检测到某个有效目标违反了白名单时，会生成*白名单事件*。白名单事件是特殊类型的关联事件，会被记录到防御中心关联事件数据库中。您可以查看某个工作流程中的白名单事件，或搜索特定的白名单事件。有关详细信息，请参阅第 52-26 页上的处理白名单事件。

当系统生成一个表示主机违规的事件时，产生白名单违规行为。同样地，发现事件可能表明之前违规的主机现在的属性为合规，即使发生该事件时系统并**未**生成白名单。

下列事件会改变主机的合规性：

- 系统检测到主机的操作系统发生变化
- 系统检测到主机的操作系统或主机上的应用协议存在身份冲突
- 系统检测到主机上有新的 TCP 服务器端口（例如， SMTP 或网络服务器使用的端口）处于活动状态，或主机上有新的 UDP 服务器正在运行
- 系统检测到主机上运行的 TCP 或 UDP 服务器发生变化，例如由于升级导致版本发生变化

- 系统检测到主机上有新的客户端正在运行
- 系统从数据库中删除了某个不活动的客户端
- 系统检测到主机上有新的网络应用正在运行
- 系统从主机配置文件中删除了某个不活动的网络应用
- 系统检测到主机正在与新的网络协议（例如 Novell Netware 或 IPv6）或新的传输协议（例如 ICMP 或 EGP）进行通信
- 系统检测到一台越狱的新移动设备
- 系统检测到主机上的某个 TCP 或 UDP 端口已关闭或超时

此外，您还可以使用主机输入功能或主机配置文件执行以下操作来触发主机合规性的改变：

- 向主机添加客户端、协议或服务器
- 从主机中删除客户端、协议或服务器
- 设置主机的操作系统定义
- 更改主机的主机属性，这样该主机便不再是一个有效目标

例如，如果白名单指定只允许在网络上运行 Microsoft Windows 主机，但系统检测到该主机当前正在运行 Mac OS X，则系统会生成一个白名单事件。此外，该主机与白名单关联的主机属性的值从合规更改为违规。

要将本示例中主机的合规属性恢复为合规，必须发生下列任一情况：

- 您编辑白名单，以允许 Mac OS X 操作系统的运行
- 您手动将主机的操作系统定义更改为 Microsoft Windows
- 系统检测到操作系统已更改回 Microsoft Windows

此外，与白名单关联的主机属性的值从违规更改为合规。

又例如，如果合规白名单禁止使用 FTP，并且您从应用协议网络映射或事件视图中删除了 FTP，则运行 FTP 的主机的属性变为合规。但如果系统再次检测到该应用协议，则会生成白名单事件，且该主机的属性变为违规。

请注意，如果系统生成的事件所包含的白名单信息不足，则不会触发白名单。例如，白名单指定端口 21 上只允许传输 TCP FTP 流量。然后，系统检测到使用 TCP 协议的端口 21 已在白名单的其中一个目标上激活，但系统无法该流量是否来自 FTP。在这种情况下，不会触发白名单，除非系统将该数据流识别为是除 FTP 流量以外的流量，或者您使用主机输入功能将该流量指定为非 FTP 流量。

注 在白名单的初始评估期间，系统**不会**对违规主机生成白名单事件。如果想要对所有违规目标的生成白名单事件，则必须清除防御中心数据库。这样，系统会重新发现网络上的主机以及与其关联的客户端、应用协议、网络应用与通信协议，从而触发白名单事件。有关详细信息，请参阅第 B-1 页上的从数据库清除发现数据。

此外，还可以将系统配置为检测到白名单违规行为时自动触发响应。响应包括补救措施 （例如运行 Nmap 扫描）、警报 （邮件、 SNMP 和系统日志警报），或警报与补救措施的组合。有关详细信息，请参阅第 51-45 页上的将响应添加至规则和白名单。

创建合规白名单

许可证：FireSIGHT

创建白名单时，您可以调查整个网络或某个特定网段。调查网络后，使用适用于系统在该网段上检测到的各操作系统的一个配置文件来填充白名单。默认情况下，这些主机配置文件允许系统在适用的操作系统上检测到的所有客户端、应用协议、网络应用和通信协议。

然后，您必须指定白名单的目标。您可以将白名单配置为评估受监控网络上的所有主机，也可以将白名单限制为只评估特定的网段甚至是个别主机。还可以进一步限制白名单，只评估具备特定主机属性或者属于某个特定的 VLAN 的主机。如果已对网络进行了调查，默认情况下，您已调查的网段即表示白名单目标。您可以编辑或删除已调查的网络，也可以添加新的目标。

接下来，创建表示合规主机的主机配置文件。白名单中的主机配置文件指定了允许在目标主机上运行的操作系统、客户端、应用协议、网络应用及通信协议。您可以配置全局主机配置文件，编辑任一网络调查创建的主机配置文件，添加新的主机配置文件，以及添加和编辑共享主机配置文件。

最后，保存该白名单并将其添加至活动的关联策略。系统开始评估目标主机是否合规，在主机违反白名单时生成白名单事件，并触发针对白名单违规行为配置的任何响应。有关合规白名单的更详细的说明，请参阅第 52-2 页上的了解合规白名单。

提示　也可以从主机的表视图中创建一份白名单。有关详细信息，请参阅第 50-21 页上的在所选主机上创建合规性白名单。

要创建一份合规白名单，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Correlation**，然后点击 **White List**。

系统将显示 White List 页面。

步骤 2　点击 **New White List**。

系统将显示 Survey Network 页面。

步骤 3　或者，调查网络：

- 要调查网络，请参阅第 52-8 页上的调查网络。
- 要在不调查网络的情况下创建白名单，请点击 **Skip** 并继续执行下一步。

系统将显示 Create White List 页面。

步骤 4　在 **Name** 字段中，输入新的白名单的名称。

步骤 5　在 **Description** 字段中，输入白名单的简短描述。

步骤 6　要在网络中允许越狱的移动设备，请启用 **Allow Jailbroken Mobile Devices**。要让白名单评估的所有越狱设备生成一个白名单违规事件，请禁用该选项。

步骤 7　指定白名单的目标。您可以编辑或删除网络调查创建的目标并添加新的目标。或者，根据主机属性或 VLAN ID 进一步限制目标。有关详细信息，请参阅第 52-9 页上的配置合规白名单的目标。

步骤 8　创建表示合规主机的主机配置文件。您可以配置全局主机配置文件，编辑网络调查创建的主机配置文件，添加新的主机配置文件，以及添加和编辑共享主机配置文件。有关详细信息，请参阅第 52-11 页上的配置合规白名单的主机配置文件。

步骤 9　点击 **Save White List** 保存白名单。

白名单已保存。现在，可以将该白名单添加至活动的关联策略，开始评估目标主机的合规性，在主机违反白名单时生成白名单事件，或者触发针对白名单违规的响应。有关详细信息，请参阅第 51-42 页上的创建关联策略。

调查网络

许可证：FireSIGHT

开始创建合规白名单时，可以调查整个网络或某个特定网段。

调查网络时，系统从数据库收集在检测到的不同操作系统上运行的应用协议、客户端、网络应用及通信协议的相关数据。然后，系统会在白名单内为检测到的各操作系统创建一个主机配置文件。默认情况下，这些主机配置文件允许系统在适用的操作系统上检测到的所有客户端、应用协议、网络应用和通信协议。

这样，系统可以创建一个基准白名单，您就无需手动创建和配置多个主机配置文件。调查网络之后，您可以编辑或删除调查根据需求而创建的主机配置文件；还可以添加您可能需要的任何其他主机配置文件。

请注意，在创建白名单的过程中，您可以随时调查网络。这样，便可以向已有的主机配置文件添加其他允许的客户端、应用协议、网络应用及通信协议，并且如果调查检测到有主机正在运行初始调查时未检测到的操作系统，则会创建其他主机配置文件。如果重新调查活动的关联策略下所使用白名单中的网络，则该调查会更改目标或主机配置文件，当您保存该名单时系统重新评估目标主机。尽管此次重新评估可能将某些主机的属性改为合规，但它不会生成任何白名单事件。

要通过网络调查开始创建合规白名单，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Correlation**，然后点击 **White List**。

系统将显示 White List 页面。

步骤 2　点击 **New White List**。

系统将显示 Survey Network 页面。

步骤 3　是否要调查网络？

- 如果选择 **yes**，请继续执行下一步。
- 如果选择 **no**，请点击 **Skip**。

  系统将显示 Create White List 页面，并显示一个空白的白名单。继续执行下一节提供白名单的基本信息中的操作步骤。

步骤 4　在 **IP Address** 和 **Netmask** 字段中，输入表示要调查的主机的 IP 地址和网络掩码（使用特殊表示法，例如 CIDR）。

请确保在网络发现策略中指定系统监控的网络。有关在 FireSIGHT 系统中使用 IP 地址表示法的详细信息，请参阅第 1-16 页上的 IP 地址约定。

提示　要调查整个受监控网络，请使用默认值 `0.0.0.0/0` 和 `::/0`。

步骤 5　点击 **OK**。

系统将显示 Create White List 页面。

白名单已预填充；其目标为被调查网络中的主机，允许的主机配置文件为这些目标的主机配置文件。

步骤 6　要调查其他网络，请点击 **Target Network**，并对要调查的其他每个网络重复执行第 4 步和第 5 步。

通过调查其他网络，可以向已有的主机配置文件添加其他允许的客户端、应用协议、网络应用及通信协议，并且如果调查检测到有主机正在运行初始调查时未检测到的操作系统，则会创建其他主机配置文件。通过调查其他网络，还可以在白名单中添加目标，此目标表示所调查网段中的主机。您可以编辑或删除此目标。

步骤 7　进入下一节提供白名单的基本信息。

提供白名单的基本信息

许可证：FireSIGHT

必须为每个白名单提供名称，或者简短描述。此外，您可以选择越狱的移动设备是否会导致白名单违规。

要提供白名单的基本信息，请执行以下操作：

访问：管理

步骤 1　在 **Name** 字段中，输入新的白名单的名称。

步骤 2　在 **Description** 字段中，输入白名单的简短描述。

步骤 3　要在网络中允许越狱的移动设备，请启用 **Allow Jailbroken Mobile Devices**。要让白名单评估的所有越狱设备生成一个白名单违规事件，请禁用该选项。

步骤 4　进入下一节配置合规白名单的目标。

配置合规白名单的目标

许可证：FireSIGHT

在创建一个合规白名单时，必须指定适用的网络部分。可以使用白名单来评估受监控网络上的所有主机，也可以对白名单进行限制，只评估特定的网段甚至是个别主机。还可以进一步限制白名单，只评估具备特定主机属性或者属于某个特定的 VLAN 的主机。符合白名单评估条件的主机被称为*目标*。有关白名单目标的更详细的说明，请参阅第 52-3 页上的了解白名单的目标。

完成合规白名单目标的创建后，继续第 52-11 页上的配置合规白名单的主机配置文件。

注　如果您从一台主机更改或删除主机属性，执行修改操作后该主机不再是一个有效目标，则白名单不会再评估该主机，且该主机不会被视为合规或违规。

有关如何修改和删除目标的详细信息，请参阅：

- 第 52-11 页上的修改现有目标
- 第 52-11 页上的删除现有目标

创建合规白名单的目标时，须指定主机要接受白名单评估所必须达到的条件。有效目标：

- 必须在指定的 IP 地址块中。还可以将 IP 地址块排除在外。
- 必须具备至少一个指定的主机属性。
- 必须属于某个指定的 VLAN。

请注意，如果您在一个活动的关联策略所使用的白名单中添加目标并保存该白名单后，系统会评估新的目标主机是否合规。但此评估不会生成白名单事件。

要创建合规白名单的目标，请执行以下操作：

访问：管理

步骤 1 在 Create White List 页面上，点击 **Target Networks** 旁的添加图标 ( )。

系统将显示新目标的设置。

提示 您还可以通过调查网段创建一个新目标。在 Create White List 页面上，点击 **Target Network**，然后执行第 52-8 页上的调查网络中的第 4 至 5 步。系统会根据您指定的 IP 地址创建新的目标并为其命名。点击刚刚创建的目标，然后继续执行剩余的步骤重命名该目标，添加或排除其他网络，以及添加主机属性或 VLAN 限制。

步骤 2 在 **Name** 字段中，输入新目标的名称。

步骤 3 点击 **Targeted Networks** 旁的添加图标 ( )，将一组特定的 IP 地址作为目标。

步骤 4 在 **IP Address** 和 **Netmask** 字段中，输入表示要作为目标或从目标中排除的主机的 IP 地址和网络掩码（使用特殊表示法，例如 CIDR）。

请确保在网络发现策略中指定系统监控的网络。有关在 FireSIGHT 系统中使用 IP 地址表示法的详细信息，请参阅第 1-16 页上的 IP 地址约定。

提示 要以整个受监控网络为目标，请使用 `0.0.0.0/0` 和 `::/0`。

步骤 5 如果要将该网络从监控目标中排除，请选择 **Exclude**。

步骤 6 要添加其他网络，请重复第 4 步和第 5 步。

步骤 7 点击 **Targeted Host Attributes** 旁的 **Add**，将具有特定主机属性的主机作为目标。

步骤 8 在 **Attribute** 和 **Value** 下拉列表中，指定该主机属性。

步骤 9 要添加其他主机属性，请重复第 7 步和第 8 步。

主机必须具备您所指定的根据白名单进行评估的至少一个主机属性。

步骤 10 点击 **Targeted Host Attributes** 旁的 **Add**，定向属于特定 VLAN 的主机。

步骤 11 在 **VLAN ID** 字段中，指定要根据白名单进行评估的主机的 VLAN ID。对于 802.1q VLAN， VLAN ID 可以是介于 0 和 4095 之间的任何整数。

步骤 12 要添加其他 VLAN ID，请重复第 10 步和第 11 步。

主机必须是您指定根据白名单进行评估的其中一个 VLAN 的成员。

提示 要移除某个网络、主机属性限制或 VLAN 限制，请点击要删除的元素旁的删除图标 ( )。

修改现有目标

许可证：FireSIGHT

修改某个目标后，必须保存该白名单以使更改生效。请注意，如果对一个活动的关联策略所使用的白名单中的某个目标进行修改，则保存该白名单后，系统会评估新的目标主机是否合规。但此评估不会生成白名单事件。此外，系统将之前有效的目标的白名单主机属性更改为未评估。

要修改现有目标，请执行以下操作：

访问：管理

步骤 1　在 Create White List 页面上的 **Targets** 下，点击要修改的目标。

系统将显示该目标的设置。

步骤 2　根据需要进行更改。

您可以重命名该目标，添加或排除其他网络，以及添加主机属性或 VLAN 限制。有关详细信息，请参阅第 52-9 页上的配置合规白名单的目标。

删除现有目标

许可证：FireSIGHT

删除某个目标后，必须保存该白名单以使更改生效。请注意，如果从一个活动的关联策略所使用的白名单中删除某个目标，则系统会将之前有效的目标的白名单主机属性更改为未评估。

要删除白名单目标，请执行以下操作：

访问：管理

步骤 1　在要删除的目标旁，点击删除图标 ( )。

步骤 2　系统提示时，确认您要删除该目标。

目标已删除。

配置合规白名单的主机配置文件

许可证：FireSIGHT

合规白名单中的主机配置文件指定了允许在目标主机上运行的操作系统、客户端、应用协议、网络应用及通信协议。可以在白名单中配置三种类型的主机配置文件，分别是：

- 全局主机配置文件，该配置文件指定了允许在目标主机上运行的应用协议、客户端、网络应用及通信协议，无论该主机使用的是什么操作系统
- 特定操作系统的主机配置文件，该配置文件不仅指定了允许在网络上运行的操作系统，还指定了允许在这些操作系统上运行的应用协议、客户端、网络应用及通信协议
- 共享主机配置文件，其作用类似于特定操作系统的主机配置文件，只不过它们没有与单个白名单绑定；您可以在多个白名单上使用这些配置文件

有关合规白名单的主机配置文件更详细的说明，请参阅第 52-3 页上的了解白名单主机配置文件。

完成合规白名单的主机配置文件的创建后，您可以在一个活动的关联策略中添加该白名单，开始评估目标主机是否合规，在主机违反白名单时生成白名单事件，或者针对白名单违规行为触发响应。

有关如何创建、修改和删除合规白名单主机配置文件的信息，请参阅：

- 第 52-12 页上的配置全局主机配置文件
- 第 52-12 页上的创建特定操作系统的主机配置文件
- 第 52-17 页上的添加共享主机配置文件至合规白名单
- 第 52-17 页上的修改现有的主机配置文件
- 第 52-20 页上的删除现有的主机配置文件

配置全局主机配置文件

许可证：FireSIGHT

所有白名单均包含一个全局主机配置文件，该文件指定了允许在目标主机上运行的应用协议、客户端、网络应用及通信协议，无论该主机使用的是什么操作系统。有关全局主机配置文件更详细的说明，请参阅第 52-4 页上的了解全局主机配置文件。

要配置全局主机配置文件，请执行以下操作：

访问：管理

步骤 1　在 Create White List 的 **Allowed Host Profiles** 下方，点击 **Any Operating System**。

系统将显示全局主机配置文件的设置。

步骤 2　要指定允许的应用协议，请按照第 52-13 页上的添加应用协议至主机配置文件中的描述操作。

步骤 3　要指定允许的客户端，请按照第 52-14 页上的添加客户端至主机配置文件中的描述操作。

步骤 4　要指定允许的网络应用，请按照第 52-15 页上的添加网络应用至主机配置文件中的描述操作。

步骤 5　要指定允许的通信协议，请按照第 52-16 页上的添加通信协议至主机配置文件中的描述操作。

请注意，始终允许 ARP、 IP、 TCP 和 UDP 通信协议。

创建特定操作系统的主机配置文件

许可证：FireSIGHT

特定操作系统的主机配置文件不仅指定了允许在网络上运行的操作系统，还指定了允许在这些操作系统上运行的应用协议、客户端、网络应用及通信协议。有关更详细的说明，请参阅第 52-4 页上的了解特定操作系统的主机配置文件。

要为某个特定的操作系统新建一个合规白名单主机配置文件，请执行以下操作：

访问：管理

步骤 1　在 **Allowed Host Profiles** 旁，点击添加图标 ( )。

系统将显示新的主机配置文件的设置。

步骤 2　在 **Name** 字段中，输入该主机配置文件的描述性名称。

步骤 3　在 **OS Vendor**、 **OS Name** 和 **Version** 下拉列表中，选择您要创建的主机配置文件的操作系统和版本。

步骤 4　指定允许的应用协议。您会看到三个选项：

- 要允许所有应用协议，请将 **Allow all Application Protocols** 复选框保持选中状态。
- 要允许所有应用协议，请清除 **Allow all Application Protocols** 复选框。
- 要允许特定的应用协议，请按照第 52-13 页上的添加应用协议至主机配置文件中的描述操作。

步骤 5　指定允许的客户端。您会看到三个选项：

- 要允许所有客户端，请将 **Allow all Clients** 复选框保持选中状态。
- 要禁止所有客户端，请清除 **Allow all Clients** 复选框。
- 要允许特定的客户端，请按照第 52-14 页上的添加客户端至主机配置文件中的描述操作。

步骤 6　指定允许的网络应用。您会看到三个选项：

- 要允许所有网络应用，请将 **Allow all Web Applications** 复选框保持选中状态。
- 要允许所有网络应用，请清除 **Allow all Web Applications** 复选框。
- 要允许特定的网络应用，请按照第 52-15 页上的添加网络应用至主机配置文件中的描述操作。

步骤 7　指定允许的通信协议。

要添加一个通信协议，在 **Allowed Protocols** 旁，按照第 52-16 页上的添加通信协议至主机配置文件中的描述操作。请注意，始终允许 ARP、 IP、 TCP 和 UDP 通信协议。

添加应用协议至主机配置文件

许可证：FireSIGHT

您可以使用共享主机配置文件或属于单个白名单的主机配置文件，将合规白名单配置为允许某些应用协议在特定的操作系统上运行。还可以将白名单配置为允许某些应用协议在任何有效的目标上运行；这些应用协议被称为全局允许的应用协议。

对于任何允许的应用协议，您可以指定允许的应用协议的类型 （例如 FTP 和 SSH），也可以通过指定应用协议的类型为*任何*以允许自定义应用协议。还必须指定允许的应用协议所使用的通信协议 （TCP 或 UDP）。您可以允许该应用协议在任何端口上运行，或者仅限在指定的端口上运行。

或者，要求该应用协议服务器具有特定的供应商或版本。例如，可以允许 SSH 于端口 22 在 Linux 主机上运行。还可以将特殊供应商和版本限定为 OpenSSH 4.2。

要在合规白名单主机配置文件中添加应用协议，请执行以下操作：

访问：管理

步骤 1　创建或修改白名单主机配置文件时，点击 **Allowed Application Protocols** 旁的添加图标 () （或者，如果修改适用任何操作系统的主机配置文件，则点击 **Globally Allowed Application Protocols** 旁的添加图标）。

系统将显示一个弹出窗口。列出以下应用协议：

- 在白名单中创建的应用协议
- 在第 52-8 页上的调查网络中所述调查网络时，已存在于网络映射中的应用协议
- 白名单中的其他主机配置文件使用的应用协议，包括 VRT 创建的用于默认白名单的内置应用协议

步骤 2　此时您有两种选择：

- 要添加列表中已有的应用协议，请选择此应用协议并点击 **OK**。点击的同时使用 Ctrl 或 Shift 选择多个应用协议。您也可以点击并拖动鼠标，以选择多个相邻的应用协议。

  该应用协议已添加。请注意，如果添加的是内置应用协议，则其名称以斜体显示。您可以跳过剩余步骤，或者更改该应用协议的任何值 （例如端口或通信协议），点击刚刚添加的应用协议即可显示应用协议编辑器。

- 要添加新的应用协议，请选择 **<New Application Protocol>** 并点击 **OK**。

  系统将显示应用协议编辑器。

步骤 3　从 **Type** 下拉列表中，选择应用协议的类型。对于自定义应用协议，请选择 **any**。

步骤 4　指定应用协议端口。此时您有两种选择：

- 要允许应用协议在任何端口上运行，请选择 **Any port** 复选框。
- 要只允许应用协议在某个特定端口上运行，请在 **port** 字段中输入端口号。

步骤 5　从 **Protocol** 下拉列表中，选择通信协议：**TCP** 或 **UDP**。

步骤 6　或者，在 **Vendor** 和 **Version** 字段中，指定应用协议的供应商和版本。

如果不指定供应商或版本，则只要类型与协议匹配，白名单便允许所有供应商和版本。请注意，如果您限制供应商和版本，就必须指定供应商和版本，确保它们与将显示在事件视图或应用协议网络映射中的供应商和版本完全相同。

步骤 7　点击 **OK**。

该应用协议已添加。请注意，白名单保存后，更改才会生效。

如果在一个活动的关联策略所使用的白名单中添加了应用协议，则保存该白名单后，系统会重新评估目标主机。尽管此次重新评估可能将某些主机的属性改为合规，但它不会生成任何白名单事件。

添加客户端至主机配置文件

许可证：FireSIGHT

您可以使用共享主机配置文件或属于单个白名单的主机配置文件，将合规白名单配置为允许某些客户端在特定的操作系统上运行。还可以将白名单配置为允许某些客户端在任何有效的目标上运行；这些客户端被称为全局允许的客户端。

或者，要求客户端的特定版本。例如，可以只允许 Microsoft Internet Explorer 8.0 在 Microsoft Windows 主机上运行。

要添加客户端至合规白名单主机配置文件，请执行以下操作：

访问：管理

步骤 1　创建或修改白名单主机配置文件时，点击 **Allowed Clients** 旁的添加图标 () （或者，如果修改适合任何操作系统的主机配置文件，则点击 **Globally Allowed Clients** 旁的添加图标）。

系统将显示一个弹出窗口。列出以下客户端：

- 在白名单中创建的客户端
- 在第 52-8 页上的调查网络中所述调查网络时，已在网络映射中的主机上运行的客户端
- 白名单中的其他主机配置文件使用的客户端，包括 VRT 创建的用于默认白名单的内置客户端

步骤 2　此时您有两种选择：

- 要添加列表中已有的客户端，请选择此客户端并点击 **OK**。点击的同时使用 Ctrl 或 Shift 选择多个客户端。您也可以点击并拖动鼠标，以选择多个相邻的客户端。

  客户端已添加。请注意，如果添加的是内置客户端，则其名称以斜体显示。您可以跳过剩余步骤，或者更改该客户端的任何值 （例如版本），点击刚刚添加的客户端即可显示客户端编辑器。

- 要添加新的客户端，请选择 **<New Client>** 并点击 **OK**。

  系统将显示客户端编辑器。

步骤 3　从 **Client** 下拉列表中，选择该客户端。

步骤 4　或者，在 **Version** 字段中，指定该客户端的版本。

如果不指定版本，则只要名称匹配，白列表便允许所有版本。请注意，如果您限制版本，就必须将版本指定为与将显示在客户端表视图中的版本完全相同。

步骤 5　点击 **OK**。

客户端已添加。请注意，白名单保存后，更改才会生效。

如果在一个活动的关联策略所使用的白名单中添加了客户端，则保存该白名单后，系统会重新评估目标主机。尽管此次重新评估可能将某些主机的属性改为合规，但它不会生成任何白名单事件。

添加网络应用至主机配置文件

许可证：FireSIGHT

您可以使用共享主机配置文件或属于单个白名单的主机配置文件，将合规白名单配置为允许某些网络协议在特定的操作系统上运行。还可以将白名单配置为允许某些网络应用在任何有效的目标上运行；这些网络应用被称为全局允许的网络应用。

要添加网络应用至合规白名单主机配置文件，请执行以下操作：

访问：管理

步骤 1　创建或修改白名单主机配置文件时，点击 **Allowed Web Applications** 旁的添加图标 ( )（或者，如果修改适合任何操作系统的主机配置文件，则点击 **Globally Allowed Web Applications** 旁的添加图标）。

系统将显示弹出窗口，列出系统检测到的所有网络应用。

步骤 2　选择某个网络应用并点击 **OK**。点击的同时使用 Ctrl 或 Shift 选择多个网络应用。您也可以点击并拖动鼠标，以选择多个相邻的网络应用。

该网络应用已添加。请注意，白名单保存后，更改才会生效。

如果在一个活动的关联策略所使用的白名单中添加了网络应用，则保存该白名单后，系统会重新评估目标主机。尽管此次重新评估可能将某些主机的属性改为合规，但它不会生成任何白名单事件。

添加通信协议至主机配置文件

许可证：FireSIGHT

您可以使用共享主机配置文件或属于单个白名单的主机配置文件，将合规白名单配置为允许某些通信协议在特定的操作系统上运行。还可以将白名单配置为允许某些通信协议在任何有效的目标上运行；这些通信协议被称为全局允许的通信协议。请注意，始终允许在任何主机上运行 ARP、IP、 TCP 和 UDP 通信协议；这些通信协议无法被禁用。

对于任何允许的通信协议，必须指定其类型 （网络或传输）和编号。

要添加通信协议至合规白名单主机配置文件，请执行以下操作：

访问：管理

步骤 1　创建或修改白名单主机配置文件时，点击 **Allowed Protocols** 旁的添加图标 ( ) （或者，如果修改适合任何操作系统的主机配置文件，则点击 **Globally Allowed Protocols** 旁的添加图标）。

系统将显示一个弹出窗口。列出以下通信协议：

- 在白名单中创建的通信协议
- 在第 52-8 页上的调查网络中所述调查网络时，已在网络映射中的主机上运行的通信协议
- 白名单中的其他主机配置文件使用的通信协议，包括 VRT 创建的用于默认白名单的内置通信协议

步骤 2　此时您有两种选择：

- 要添加列表中已有的通信协议，请选择此通信协议并点击 **OK**。点击的同时使用 Ctrl 或 Shift 选择多个通信协议。您也可以点击并拖动鼠标，以选择多个相邻的通信协议。

  该通信协议已添加。请注意，如果添加的是内置通信协议，则其名称以斜体显示。您可以跳过剩余步骤，或者更改该通信协议的任何值 （例如类型或编号），点击刚刚添加的通信协议即可显示通信协议编辑器。

- 要添加新的通信协议，请选择 **<New Protocol>** 并点击 **OK**。

  系统将显示通信协议编辑器。

步骤 3　从 **Type** 下拉列表中，选择通信协议的类型：**Network** 或 **Transport**。

步骤 4　指定通信协议。此时您有两种选择：

- 从下拉列表中选择一个通信协议。
- 选择 **Other (manual entry)** 以指定不在列表中的通信协议。对于网络协议，请键入 http://www.iana.org/assignments/ethernet-numbers/ 中列出的相应编号。对于传输协议，请键入 http://www.iana.org/assignments/protocol-numbers/ 中列出的相应编号。

步骤 5　点击 **OK**。

该通信协议已添加。请注意，白名单保存后，更改才会生效。

如果在一个活动的关联策略所使用的白名单中添加了通信协议，则保存该白名单后，系统会重新评估目标主机。尽管此次重新评估可能将某些主机的属性改为合规，但它不会生成任何白名单事件。

添加共享主机配置文件至合规白名单

许可证：FireSIGHT

共享主机配置文件虽与特定的操作系统绑定，但您可以在多个白名单上使用这些共享主机配置文件。也就是说，如果创建了多个白名单，但要使用相同的主机配置文件来评估运行白名单中规定的特定操作系统的主机，可使用共享主机配置文件。

您可以将任何内置或新创建的共享主机配置文件添加至合规白名单。有关详细信息，请参阅第 52-4 页上的了解共享主机配置文件和第 52-22 页上的创建共享主机配置文件。

要添加共享主机配置文件至合规白名单，请执行以下操作：

访问：管理

步骤 1　在 Create White List 页面上，点击 **Add Shared Host Profile**。

系统将显示 Add Shared Host Profile 页面。

步骤 2　从 **Name** 下拉列表中，选择要添加至白名单的共享主机配置文件，然后点击 **OK**。

共享主机配置文件已添加至白名单。系统再次显示 Create White List 页面。共享主机配置文件的名称在 Allowed Host Profiles 下方以斜体显示。

提示　您可以在 Allowed Host Profiles 下点击某个共享主机配置文件的名称，从使用此配置文件的白名单中编辑配置文件。有关详细信息，请参阅第 52-17 页上的修改现有的主机配置文件。

修改现有的主机配置文件

许可证：FireSIGHT

对合规白名单中的某个主机配置文件进行修改后，必须保存该白名单，以使更改生效。

如果您修改的主机配置文件属于在某个活动的关联策略中所使用的白名单，则修改操作可能会将主机的属性变为合规或违规，但**不会**生成白名单事件。此外，对共享主机配置文件进行修改会影响使用此配置文件的所有白名单。此操作可能会将主机的属性在当前处理的白名单及其他名单中变为合规或违规。

提示　对于其他共享主机配置文件，可以编辑默认白名单使用的内置主机配置文件。您还可以将共享主机文件重置为出厂默认设置。有关详细信息，请参阅第 52-25 页上的将内置主机配置文件重置为出厂默认设置。

要修改某个现有的主机配置文件，请执行以下操作：

访问：管理

步骤 1　在 Create White List 页面上，点击要修改的主机配置文件的名称。

系统将显示该主机配置文件的设置。请注意，如果编辑的是一个共享主机配置文件，则该主机配置文件的名称旁会显示 **Edit** 链接。如果编辑的是一个内置主机配置文件，则系统也会显示内置主机配置文件的图标 ( )。

步骤 2　此时您有两种选择：

- 如果修改的是一个共享主机配置文件，请点击 **Edit**。

  系统将显示一个弹出窗口。根据下表按需要进行更改。点击 **Save All Profiles** 保存该配置文件，然后点击 **Done** 关闭弹出窗口。

  有关编辑共享主机配置文件的详细信息，请参阅第 52-23 页上的修改共享主机配置文件。
- 如果修改的是白名单的全局主机配置文件或特定操作系统的主机配置文件，请执行以下步骤中所述的操作之一。

要重命名主机配置文件，请执行以下操作：

访问：管理

步骤 1　在 **Name** 字段中输入新的名称。

要更改主机配置文件的操作系统，请执行以下操作：

访问：管理

步骤 1　从 **OS Vendor**、 **OS Name** 和 **Version** 下拉列表中选择新的操作系统和版本。

更改这些值后，您可能还想重命名该主机配置文件。请注意，白名单的全局主机配置文件没有与之关联的操作系统，因此无法对其进行更改。

要添加一个应用协议，请执行以下操作：

访问：管理

步骤 1　按照第 52-13 页上的添加应用协议至主机配置文件中的描述操作。

要添加客户端，请执行以下操作：

访问：管理

步骤 1　按照第 52-14 页上的添加客户端至主机配置文件中的描述操作。

要添加网络应用，请执行以下操作：

访问：管理

步骤 1　按照第 52-15 页上的添加网络应用至主机配置文件中的描述操作。

要添加通信协议，请执行以下操作：

访问：管理

步骤 1　按照第 52-16 页上的添加通信协议至主机配置文件中的描述操作。

要允许所有应用协议，请执行以下操作：

访问：管理

步骤 1　在 **Allowed Application Protocols** 下，选择 **Allow all Application Protocols** 复选框。

请注意，只有在您删除之前允许的应用协议后，系统才会显示该复选框。

要允许所有客户端，请执行以下操作：

访问：管理

步骤 1　在 **Allowed Clients** 下，选择 **Allow all Clients** 复选框。

请注意，只有在您删除之前允许的客户端后，系统才会显示复选框。

要允许所有网络应用，请执行以下操作：

访问：管理

步骤 1　在 **Allowed Web Applications** 下，选择 **Allow all Web Applications** 复选框。

请注意，只有在您删除之前允许的网络应用后，系统才会显示该复选框。

要修改一个应用协议、客户端、网络应用或通信协议，请执行以下操作：

访问：管理

步骤 1　点击要修改的元素。

有关可更改的属性的详细信息，请参阅：

- 第 52-13 页上的添加应用协议至主机配置文件
- 第 52-14 页上的添加客户端至主机配置文件
- 第 52-16 页上的添加通信协议至主机配置文件

注　对应用协议、客户端、网络应用或通信协议进行的更改反映在使用该元素的所有主机配置文件中。

要删除一个应用协议、客户端、网络应用或通信协议，请执行以下操作：

访问：管理

步骤 1　在要删除的元素旁，点击删除图标 ( )。

要调查网络，请执行以下操作：

访问：管理

步骤 1　点击 **Survey Network**。通过调查网络，可以向已有的主机配置文件添加其他允许的客户端、应用协议及通信协议，并且如果调查检测到有主机正在运行初始调查时未检测到的操作系统，则会创建其他主机配置文件。有关详细信息，请参阅第 52-8 页上的调查网络。

删除现有的主机配置文件

许可证：FireSIGHT

删除合规白名单中的某个主机配置文件后，必须保存该白名单以使更改生效。请注意，删除某个共享主机配置文件只是从白名单中移除该配置文件，并不是删除该配置文件本身，也不会从使用它的任何其他白名单中移除。您无法删除白名单的全局主机配置文件。

如果删除的主机配置文件属于活动的关联策略中使用的一个或多个白名单，则删除该配置文件会导致主机违规，但**不会**生成白名单事件。

要删除合规白名单的主机配置文件，请执行以下操作：

访问：管理

步骤 1　在 Create White List 页面上要删除的主机配置文件旁，点击删除图标 ( )。

步骤 2　系统提示时，请确认是否要删除该主机配置文件。

该主机配置文件已删除。

管理合规白名单

许可证：FireSIGHT

使用 White List 页面管理合规白名单。您可以创建、修改和删除白名单，包括默认的白名单。还可以编辑所创建的或内置的共享主机配置文件，并添加新的共享主机配置文件。有关详情，请参阅：

- 第 52-7 页上的创建合规白名单
- 第 52-21 页上的修改合规白名单
- 第 52-21 页上的删除合规白名单
- 第 52-21 页上的使用共享主机配置文件

修改合规白名单

许可证：FireSIGHT

对活动的关联策略中包含的合规白名单进行修改时，系统会重新评估目标主机。请注意，在重新评估期间，系统**不会**成白名单事件，因此也不会触发与该白名单关联的任何响应，即使该白名单包含在某活动的关联策略中，并且之前合规的主机会随着白名单的更新变为违规属性。

要修改现有的合规白名单，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Correlation**，然后点击 **White List**。

系统将显示 White List 页面。

步骤 2　在要修改的白名单旁，点击编辑图标 ( )。

系统将显示 Create White List 页面。

步骤 3　根据需要进行修改，并点击 **Save White List**。

该白名单已更新。

删除合规白名单

许可证：FireSIGHT

您无法删除一个或多个关联策略正在使用的合规白名单；删除前，应首先将该白名单从其被使用的所有策略中删除。有关删除策略中某白名单的详细信息，请参阅第 51-47 页上的编辑关联策略。

如果某个白名单被删除，系统会从网络上所有主机中删除与该白名单关联的主机属性。

要删除某个现有的合规白名单，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Correlation**，然后点击 **White List**。

系统将显示 White List 页面。

步骤 2　在要删除的白名单旁，点击删除图标 ( )。

该白名单已删除。

使用共享主机配置文件

许可证：FireSIGHT

共享主机配置文件指定了允许在多个白名单的目标主机上运行的操作系统、客户端、应用协议、网络应用及通信协议。也就是说，如果创建了多个白名单，但要使用相同的主机配置文件来评估运行白名单中规定的特定操作系统的主机，可使用共享主机配置文件。请注意，默认白名单使用共享主机配置文件的一个特殊类别，即*内置主机配置文件*。

有关共享主机配置文件更详细的说明，请参阅第 52-4 页上的了解共享主机配置文件。

您可以创建、修改和删除某个共享主机配置文件。此外，如果修改或删除了任何内置共享主机配置文件，或者修改或删除了任何内置应用协议、通信协议或客户端，您可以将其重置为出厂默认设置。有关详情，请参阅：

- 第 52-22 页上的创建共享主机配置文件
- 第 52-23 页上的修改共享主机配置文件
- 第 52-25 页上的删除某个共享主机配置文件
- 第 52-25 页上的将内置主机配置文件重置为出厂默认设置

创建完一个共享主机配置文件后，您可以将其添加至多个白名单。有关详细信息，请参阅第 52-17 页上的添加共享主机配置文件至合规白名单。

创建共享主机配置文件

许可证：FireSIGHT

如果要使用同一个主机配置文件评估多个白名单上运行某个特定操作系统的主机，则需要创建一个共享主机配置文件。

提示 还可以使用某特定主机的主机配置文件为合规白名单创建一个共享主机配置文件。有关详细信息，请参阅第 49-21 页上的从主机配置文件创建白名单主机配置文件。

要创建一个共享主机配置文件，请执行以下操作：

访问：管理

步骤 1 选择 **Policies > Correlation**，然后点击 **White List**。

系统将显示 White List 页面。

步骤 2 点击 **Edit Shared Profiles**。

系统将显示 Edit Shared Profiles 页面。

步骤 3 或者，调查网络。

调查网络可以根据系统收集的网络数据创建多个基准共享白名单。这样，您就无需手动创建和配置多个共享主机配置文件。此时您有两种选择：

- 要调查网络，请点击 **Survey Network**。有关详细信息，请参阅第 52-8 页上的调查网络。

  系统将创建一个或多个基准共享主机配置文件。您可以按第 52-23 页上的修改共享主机配置文件和第 52-25 页上的删除某个共享主机配置文件中所述，编辑或删除这个或这些共享主机配置文件。要添加所需的任何其他共享主机配置文件，请继续执行下一步。
- 要跳过网络调查，请继续执行下一步。

步骤 4 在 **Shared Host Profiles** 旁，点击添加图标 ( )。

系统将显示新的共享主机配置文件的设置。

步骤 5 在 **Name** 字段中，输入该共享主机配置文件的描述性名称。

步骤 6 在 **OS Vendor**、**OS Name** 和 **Version** 下拉列表中，选择您要创建的共享主机配置文件的操作系统和版本。

步骤 7 指定允许的应用协议。您会看到三个选项：

- 要允许所有应用协议，请选择 **Allow all Application Protocols** 复选框。

- 要禁止所有应用协议，请将 **Allow all Application Protocols** 复选框保持未选中状态。
- 要允许特定的应用协议，请在 **Allowed Application Protocols** 旁，按照第 52-13 页上的添加应用协议至主机配置文件中的描述操作。

步骤 8　指定允许的客户端。您会看到三个选项：

- 要允许所有客户端，请选择 **Allow all Clients** 复选框。
- 要禁止所有客户端，请将 **Allow all Clients** 复选框保持未选中状态。
- 要允许特定的客户端，请按照第 52-14 页上的添加客户端至主机配置文件中的描述操作。

步骤 9　指定允许的网络应用。您会看到三个选项：

- 要允许所有网络应用，请选择 **Allow all Web Applications** 复选框。
- 要禁止所有网络应用，请将 **Allow all Web Applications** 复选框保持未选中状态。
- 要允许特定的网络应用，请按照第 52-15 页上的添加网络应用至主机配置文件中的描述操作。

步骤 10　指定允许的通信协议。

要添加一个通信协议，在 **Allowed Protocols** 旁，按照第 52-16 页上的添加通信协议至主机配置文件中的描述操作。请注意，始终允许 ARP、 IP、 TCP 和 UDP 通信协议。

步骤 11　点击 **Save all Profiles** 保存更改。

共享主机配置文件已创建。现在，您可以将共享主机配置文件添加至任何合规白名单。

修改共享主机配置文件

许可证：FireSIGHT

如果某个共享主机配置文件被修改，则系统会在包含它的所有白名单中更改该配置文件。对于使用共享主机配置文件同时被用于某活动关联策略中的白名单，修改共享主机配置文件会将主机的属性变为合规或违规，但**不会**生成白名单事件。

下表列出了修改共享主机配置文件可以采取的操作。

表 52-2　　对共享主机配置文件的操作

要.....	您可以.....
重命名主机配置文件	在 **Name** 字段中输入新的名称。
更改操作系统	从 **OS Vendor**、**OS Name** 和 **Version** 下拉列表中选择新的操作系统和版本。更改这些值后，您可能还想重命名该主机配置文件。
添加应用协议	按照第 52-13 页上的添加应用协议至主机配置文件中的描述操作。
添加客户端	按照第 52-14 页上的添加客户端至主机配置文件中的描述操作。
添加网络应用	按照第 52-15 页上的添加网络应用至主机配置文件中的描述操作。
添加通信协议	按照第 52-16 页上的添加通信协议至主机配置文件中的描述操作。
允许所有应用协议	在 **Allowed Application Protocols** 下，选择 **Allow all Application Protocols** 复选框。请注意，只有在您删除之前允许的应用协议后，系统才会显示该复选框。
允许所有的客户端	在 **Allowed Clients** 下，选择 **Allow all Clients** 复选框。请注意，只有在您删除之前允许的客户端后，系统才会显示复选框。

表 52-2　对共享主机配置文件的操作 （续）

要.....	您可以.....
允许所有的网络应用	在 **Allowed Web Applications** 下，选择 **Allow all Web Applications** 复选框。请注意，只有在您删除之前允许的客户端后，系统才会显示复选框。
修改某个应用协议、客户端、网络应用或通信协议	点击要修改的元素。有关可更改的属性的详细信息，请参阅： • 第 52-13 页上的添加应用协议至主机配置文件 • 第 52-14 页上的添加客户端至主机配置文件 • 第 52-15 页上的添加网络应用至主机配置文件 • 第 52-16 页上的添加通信协议至主机配置文件 **注**　对应用协议、客户端或通信协议进行的更改反映在使用该元素的所有主机配置文件中。
删除某个应用协议、客户端、网络应用或通信协议	在要删除的元素旁，点击删除图标 ( )。
调查网络	点击 **Survey Network**。通过调查网络，可以向已有的主机配置文件添加其他允许的客户端、应用协议、网络应用及通信协议，并且如果调查检测到有主机正在运行初始调查时未检测到的操作系统，则会创建其他主机配置文件。有关详细信息，请参阅第 52-8 页上的调查网络。

要修改某个共享主机配置文件，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Correlation**，然后点击 **White List**。

系统将显示 White List 页面。

步骤 2　点击 **Edit Shared Profiles**。

系统将显示 Edit Shared Profiles 页面。

步骤 3　您是否要编辑其中某个内置共享主机配置文件？

- 如果是，请展开 **Built-in Host Profiles** 以显示这些内置主机配置文件。
- 如果不是，请继续执行下一步。

步骤 4　点击要修改的共享主机配置文件的名称。

系统将显示该主机配置文件。

步骤 5　执行第 52-23 页上的表 52-2中描述的任何操作。

步骤 6　点击 **Save all Profiles** 保存更改。

该共享主机配置文件已保存。

删除某个共享主机配置文件

许可证：FireSIGHT

如果删除的共享主机配置文件属于某个活动的关联策略中使用的一个或多个白名单，则删除该配置文件会导致主机违规，但**不会**生成白名单事件。

提示 如果删除了默认白名单使用的内置共享主机配置文件，则可以通过将内置配置文件重置为出厂默认设置来进行还原。有关详细信息，请参阅第 52-25 页上的将内置主机配置文件重置为出厂默认设置。

要删除某个共享主机配置文件，请执行以下操作：

访问：管理

步骤 1 选择 **Policies > Correlation**，然后点击 **White List**。

系统将显示 White List 页面。

步骤 2 点击 **Edit Shared Profiles**。

系统将显示 Edit Shared Profiles 页面。

步骤 3 您是否要删除其中某个内置共享主机配置文件？

- 如果是，请展开 **Built-in Host Profiles** 以显示这些内置主机配置文件。
- 如果不是，请继续执行下一步。

步骤 4 在要删除的共享主机配置文件旁，点击删除图标 ( )。

请确认是否要删除该共享主机配置文件。

步骤 5 点击 **Save all Profiles** 保存更改。

该共享主机配置文件已删除，并且已从使用此配置文件的所有合规白名单中移除。

将内置主机配置文件重置为出厂默认设置

许可证：FireSIGHT

默认白名单使用共享主机配置文件的一个特殊类别，即*内置主机配置文件*。内置主机配置文件使用内置应用协议、通信协议和客户端。您可以在默认白名单以及创建的任何自定义白名单中按原样使用这些元素，或者根据需要对它们进行修改。有关详细信息，请参阅了解共享主机配置文件。

如果需要撤消对内置配置文件、应用协议、通信协议、网络应用或客户端进行的修改，则可以重置为出厂默认设置。重置为出厂默认设置时，会发生下列情况：

- **所有**已修改的内置主机配置文件、应用协议、通信协议和客户端都被重置为其出厂默认设置。
- **所有**已删除的内置主机配置文件、应用协议、通信协议和客户端都将还原。
- **所有**被活动关联策略使用及使用任何重置的内置主机配置文件、应用协议、通信协议或客户端的白名单（包括默认白名单）都将被重新评估。尽管此次重新评估可能将更改某些主机的合规属性，但它不会生成任何白名单事件。

要重置内置主机配置文件、应用协议、通信协议和客户端，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Correlation**，然后点击 **White List**。

系统将显示 White List 页面。

步骤 2　点击 **Edit Shared Profiles**。

系统将显示 Edit Shared Profiles 页面。

步骤 3　点击 **Built-in Host Profiles**。

系统将显示 Built-in Host Profiles 页面。

步骤 4　点击 **Reset to Factory Defaults**。

步骤 5　点击 **OK**，确认要重置为出厂默认设置。

所有内置主机配置文件、应用协议、通信协议和客户端都将重置为出厂默认设置。系统会重新评估活动关联策略所使用的任何白名单，以及使用任何重置的内置主机配置文件、应用协议、通信协议或客户端的任何白名单。

处理白名单事件

许可证：FireSIGHT

当系统生成了一个发现事件，而此事件表明主机不符合活动的关联策略中所包含的白名单的条件时，会生成一个白名单事件。白名单事件是特殊类型的关联事件，会被记录到关联事件数据库中。您可以搜索、查看和删除白名单事件。

提示　有关配置数据库中保存的事件数量的信息，请参阅第 63-14 页上的配置控制面板事件限制。请注意，白名单事件存储在关联事件数据库中。

有关详细信息，请参阅：

- 第 52-26 页上的查看白名单事件
- 第 52-28 页上的了解白名单事件表
- 第 52-29 页上的搜索合规白名单事件

查看白名单事件

许可证：FireSIGHT

您可以使用防御中心查看合规白名单事件表。然后，可根据要查找的信息操纵事件视图。

访问白名单事件时系统显示的页面取决于您使用的工作流程。您可以使用预定义工作流程，此工作流程包括白名单事件的表视图。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关创建自定义工作流程的信息，请参阅第 58-34 页上的创建自定义工作流程。

下表描述了在白名单事件工作流程页面上可以执行的某些特定操作。

表 52-3　　合规白名单事件的操作

要.....	您可以.....
查看某台主机的主机配置文件	点击 IP 地址旁显示的主机配置文件图标 ()。
查看用户配置文件信息	点击用户身份旁显示的用户图标 () 有关详细信息，请参阅第 50-55 页上的了解用户详细信息和主机历史记录。
对当前工作流程页面上的事件进行排序和限制	在第 58-29 页上的对向下钻取工作流程页面进行排序中获得详细信息。
在当前工作流程页面中导航	在第 58-30 页上的导航到工作流程中的其他页面中获得详细信息。
在当前工作流程中的页面之间导航，同时保留当前限制条件	点击工作流程页面左上角的相应页面链接。有关详细信息，请参阅第 58-16 页上的使用工作流程页面。
了解有关显示的列的详细信息	在第 52-28 页上的了解白名单事件表中获得详细信息。
修改所显示事件的时间和日期范围	在第 58-19 页上的设置事件时间限制中查找详细信息。
向下钻取到工作流程中的下一页，限制特定值	可使用以下其中一种方法： • 在自定义工作流程中创建的向下展开页面上，点击某行内的一个值。请注意，点击表视图行中的值可限制表视图，且不会向下钻取到下一页。 • 要向下钻取到限制某些用户的下一个工作流程页面，在要在下一个工作流程页面上查看的用户旁，选择复选框，然后点击 **View**。 • 要向下钻取到保留当前限制的下一工作流程页面，请点击 **View All**。 **提示**　表视图的页面名称中始终包括“Table View”。 有关详细信息，请参阅第 58-26 页上的限制事件。
删除系统中的白名单事件	可使用以下其中一种方法： • 要删除某些事件，请选择要删除的事件旁边的复选框，然后点击 **Delete**。 • 要删除当前已限制视图中的所有事件，点击 **Delete All**，然后确认要删除所有事件。
导航至其他事件视图查看相关事件	在第 58-31 页上的在工作流程之间导航中获得详细信息。

要查看合规白名单事件，请执行以下操作：

访问：管理员/任何安全分析师/发现管理员

步骤 1　选择 **Analysis > Correlation > White List Events**。

系统将显示默认白名单事件工作流程的第一个页面。要使用另一个工作流程，包括自定义工作流程，请按工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示任何事件，可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

了解白名单事件表

许可证：FireSIGHT

您可以使用关联策略功能，构建让系统实时响应网络威胁的*关联策略*。关联策略描述构成违规（包括违反合规白名单）的活动类型。有关关联策略的详细信息，请参阅第 51-1 页上的配置关联策略和规则。

出现合规白名单的违规时，系统生成一个白名单事件。下表列出了白名单事件表中的字段。

表 52-4　　合规白名单事件字段

字段	说明
时间	白名单事件生成时的日期和时间。
IP地址	违规主机的 IP 地址。
用户	登录违规主机的任何已知用户的身份。
端口	与触发应用协议白名单违规 （违规应用协议造成的违规）的事件关联的端口 （如有）。对于其他类型的白名单违规活动，该字段为空白。

说明	描述白名单是如何被违反的。例如：
	`Client "AOL Instant Messenger" is not allowed.`
	涉及应用协议的违规指明应用协议的名称和版本，以及所使用的端口和协议 （TCP 或 UDP）。如果限制禁止某个特定的操作系统，描述中会包含操作系统的名称。例如：
	`Server "ssh / 22 TCP ( OpenSSH 3.6.1p2 )" is not allowed on Operating System "Linux Linux 2.4 or 2.6".`

策略	被违反的关联策略的名称，即包含该白名单的关联策略。
White List	白名单的名称。
优先级	策略或触发策略违规的白名单所指定的优先级。有关设置关联规则和策略优先级的详细信息，请参阅第 51-43 页上的提供基本策略信息和第 51-44 页上的设置规则和白名单优先级。
Host Criticality	用户向不符合白名单规定的主机所分配的主机重要性：`None`、`Low`、`Medium` 或 `High`。有关主机重要性的详细信息，请参阅第 49-27 页上的使用预先定义的主机属性。
设备	检测到白名单违规行为的受管设备的名称。
计数	与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

搜索合规白名单事件

许可证：FireSIGHT

您可以搜索特定的合规白名单事件。您可能想要创建适合您网络环境的自定义搜索，然后进行保存，以便后续使用。下表列出了可以使用的搜索条件。

表 52-5　　合规白名单事件的条件

字段	搜索条件规则
策略	输入关联策略的名称，返回由于违反该策略所包含的白名单而导致的所有事件。
White List	输入白名单的名称，返回由于违反该白名单而导致的所有事件。
说明	输入白名单事件的描述。
优先级	根据关联策略中白名单的优先级或关联策略自身的优先级，指定白名单事件的优先级。请注意，白名单的优先级优先于策略的优先级。输入 `none`，表示没有优先级。 有关设置关联规则和策略优先级的详细信息，请参阅第 51-43 页上的提供基本策略信息和第 51-44 页上的设置规则和白名单优先级。
IP地址	指定不符合白名单规定的主机的 IP 地址。
用户	指定登录不符合白名单规定的主机的用户身份。
端口	指定与触发应用协议白名单违规 （违规应用协议造成的违规）的发现事件关联的端口 （如有）。
Host Criticality	指定白名单事件中涉及的源主机的重要性：`None`、`Low`、`Medium` 或 `High`。有关主机重要性的详细信息，请参阅第 49-27 页上的使用预先定义的主机属性。
设备	键入设备名称或 IP 地址或设备组、堆栈或集群名称，将搜索限制于已检测到白名单违规的特定设备。有关 FireSIGHT 系统如何处理搜索中的设备字段的详细信息，请参阅第 60-6 页上的在搜索中指定设备。

要搜索合规白名单事件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **White List Events**。

系统将用相应限制更新页面。

步骤 3　按照第 52-29 页上的表 52-5 中所述，在相应字段输入搜索条件，同时记住以下附加要点：

- 所有字段都接受求反 (`!`)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含用引号引住的指定精确字符串的指定字段的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含用引号引住的逗号分隔列表中所有值的记录与该搜索条件匹配。

  - 对于可能同时包含多个值的字段，搜索条件可以包括单个值以及用引号引住的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含其中一个或多个这些字母，则匹配记录的指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件均匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 在任一字段指定 `n/a` 以便识别信息不适用于该字段的事件；使用 `!n/a` 识别字段填充事件。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法 （包括在搜索中使用对象）的详细信息，请参阅第 60-1 页上的搜索事件。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索另存为私有，这样只有您才能访问它。否则，请清除此复选框，为所有用户保存搜索。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），以便您稍后运行此搜索。
- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），以便您稍后运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果将显示在默认白名单事件的工作流程中，受当前时间范围的限制。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

处理白名单的违规事件

许可证：FireSIGHT

系统跟踪网络上主机违反活动关联策略中的合规白名单的方式。您可以搜索并查看这些记录。

有关详细信息，请参阅：

- 第 52-31 页上的查看白名单违规事件
- 第 52-32 页上的了解白名单违规事件表
- 第 52-33 页上的搜索白名单的违规事件

查看白名单违规事件

许可证：FireSIGHT

您可以使用防御中心查看白名单违规事件表。然后，可根据要查找的信息操纵事件视图。访问白名单违规事件时显示的页面取决于您使用的工作流程。有两个预定义的工作流程：

- 主机违规计数工作流程提供一系列页面，列出了违反至少一个白名单的所有主机。第一页根据每台主机的违规次数对主机进行排序，违规次数最多的主机排在列表顶部。如果主机违反了多个白名单，则每个违反的白名单都会在单独的一行里列出来。工作流程还包含白名单违规事件的表视图，该视图列出了所有违规事件，最近检测到的违规事件排在列表顶部。该表中的每一行都包含一个检测到的违规事件。
- 白名单违规工作流程包含白名单违规事件的表视图，该视图列出了所有违规事件，最近检测到的违规事件排在列表顶部。该表中的每一行都包含一个检测到的违规事件。

两个预定义工作流程结束于主机视图中，该视图包含符合限制条件的每台主机的配置文件。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关详细信息，请参阅第 58-34 页上的创建自定义工作流程。

下表列出了在白名单违规事件工作流程页面上可以执行的某些特定操作。

表 52-6　　对合规白名单违规事件的操作

要.....	您可以.....
查看某台主机的主机配置文件	点击 IP 地址旁显示的主机配置文件图标 ()。
对当前工作流程页面上的事件进行排序和限制	在第 58-29 页上的对向下钻取工作流程页面进行排序中获得详细信息。
在当前工作流程页面中导航	在第 58-30 页上的导航到工作流程中的其他页面中获得详细信息。
在当前工作流程中的页面之间导航，同时保留当前限制条件	点击工作流程页面左上角的相应页面链接。有关详细信息，请参阅第 58-16 页上的使用工作流程页面。
了解有关显示的列的详细信息	在第 52-32 页上的了解白名单违规事件表中获得详细信息。
向下钻取到工作流程中的下一个页面	可使用以下其中一种方法： • 要向下钻取到限制某个特定值的下一个工作流程页面，请点击某一行中的一个值。请注意，此操作仅适用于向下钻取页面。请注意，在表视图中点击某一行中的一个值时，会限制该表视图，且**不会**向下钻取到下一个页面。 • 要向下钻取到限制某些事件的下一个工作流程页面，请选择您想要在下一个工作流程页面上查看的事件旁的复选框，然后点击 **View**。 • 要向下钻取到保留当前限制的下一工作流程页面，请点击 **View All**。 **提示**　表视图的页面名称中始终包括“Table View”。 有关详细信息，请参阅第 58-26 页上的限制事件。
导航至其他事件视图查看相关事件	在第 58-31 页上的在工作流程之间导航中获得详细信息。

要查看合规白名单的违规事件，请执行以下操作：

访问：管理员/任何安全分析师/发现管理员

步骤 1　选择 **Analysis > Correlation > White List Violations**。

系统将显示默认白名单违规事件工作流程的第一个页面。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

了解白名单违规事件表

许可证：FireSIGHT

您可以使用关联策略功能，构建让系统实时响应网络威胁的*关联策略*。关联策略描述构成违规（包括违反合规白名单）的活动类型。有关关联策略的详细信息，请参阅第 51-1 页上的配置关联策略和规则。

当合规白名单被违反时，系统记录该违规事件。请注意，您无法在表视图中设置事件时间限制，这是因为表视图仅显示网络上当前的主机违规事件。下表列出了白名单违规事件表中的字段。

表 52-7　　合规白名单的违规事件的字段

字段	说明
时间	该白名单违规事件被检测到的日期和时间。
IP地址	违规主机的相关 IP 地址。
类型	白名单违规事件的类型，即，该违规事件是否由于下列内容不合规而导致的： • 操作系统 (**os**) • 应用协议 (**server**) • 客户端 (**client**) • 通信协议 (**protocol**) • 网络应用 (**web**)
信息	与该白名单违规事件相关的任何可用的供应商、产品或版本信息。 例如，如果白名单只允许运行 Microsoft Windows 主机，则 Information 字段描述的是不运行 Microsoft Windows 的主机的操作系统。 对于违反白名单的通信协议， Information 字段表示违规是由网络协议还是传输协议造成的。
端口	与触发应用协议白名单违规 （违规应用协议造成的违规）的事件关联的端口（如有）。对于其他类型的白名单违规活动，该字段为空白。
协议	与触发应用协议白名单违规 （违规应用协议造成的违规）的事件关联的通信协议 （如有）。对于其他类型的白名单违规活动，该字段为空白。
White List	被违反的白名单的名称。
计数	与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

搜索白名单的违规事件

许可证：FireSIGHT

您可以搜索特定的合规白名单的违规事件。您可能想要创建适合您网络环境的自定义搜索，然后进行保存，以便后续使用。下表列出了可以使用的搜索条件。

表 52-8　　合规白名单的违规事件的搜索条件

字段	搜索条件规则
时间	指定白名单被违反时的日期和时间。
IP地址	指定不符合白名单规定的主机的 IP 地址。
White List	输入白名单的名称，返回该白名单中的所有违规事件。
类型	输入白名单违规的类型： • 输入 `os` （或 `operating system`）搜索基于操作系统的违规事件 • 输入 `server` 搜索基于应用协议的违规事件 • 输入 `client` 搜索基于客户端的违规事件 • 输入 `protocol` 搜索基于通信协议的违规事件 • 输入 `web application` 搜索基于网络应用的违规事件
信息	输入白名单违规信息。
端口	指定与触发应用协议白名单违规 （违规应用协议造成的违规）的发现事件关联的端口 （如有）。
协议	指定与触发应用协议白名单违规 （违规应用协议造成的违规）的发现事件关联的信讯协议 （如有）。

要搜索合规白名单的违规事件，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **White List Violations**。

系统将用相应限制更新页面。

步骤 3　按照合规白名单事件的条件表中所述，在相应的字段中输入搜索条件，并谨记以下几个要点：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含用引号引住的指定精确字符串的指定字段的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含用引号引住的逗号分隔列表中所有值的记录与该搜索条件匹配。

  - 对于可能同时包含多个值的字段，搜索条件可以包括单个值以及用引号引住的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含其中一个或多个这些字母，则匹配记录的指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件均匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 在任一字段指定 `n/a` 以便识别信息不适用于该字段的事件；使用 `!n/a` 识别字段填充事件。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

有关搜索语法 （包括在搜索中使用对象）的详细信息，请参阅第 60-1 页上的搜索事件。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索另存为私有，这样只有您才能访问它。否则，请清除此复选框，为所有用户保存搜索。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），以便您稍后运行此搜索。
- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），以便您稍后运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果将显示在默认白名单的违规工作流程中。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

创建流量量变曲线

流量量变曲线仅指根据您指定的一段时间跨度内所收集的连接数据确定的网络流量的量变曲线。您可以使用设备所收集的连接数据、任何或所有启用了 NetFlow 的设备导出的连接数据，或同时包含这两项数据。

创建流量量变曲线后，可通过对照配置文件评估新流量的方式检测异常网络流量，新流量应代表正常网络流量。

请记住， FireSIGHT 系统根据流量量变曲线更改使用连接数据来创建流量量变曲线并触发关联性规则。您不能包含未记录到流量量变曲线中防御中心数据库的连接。系统仅使用连接结束数据来填入连接摘要 （请参阅第 39-2 页上的了解连接摘要），然后系统会使用它来创建连接图和流量量变曲线。因此，如果您要创建和使用流量量变曲线，请确保在连接结束时记录连接事件。

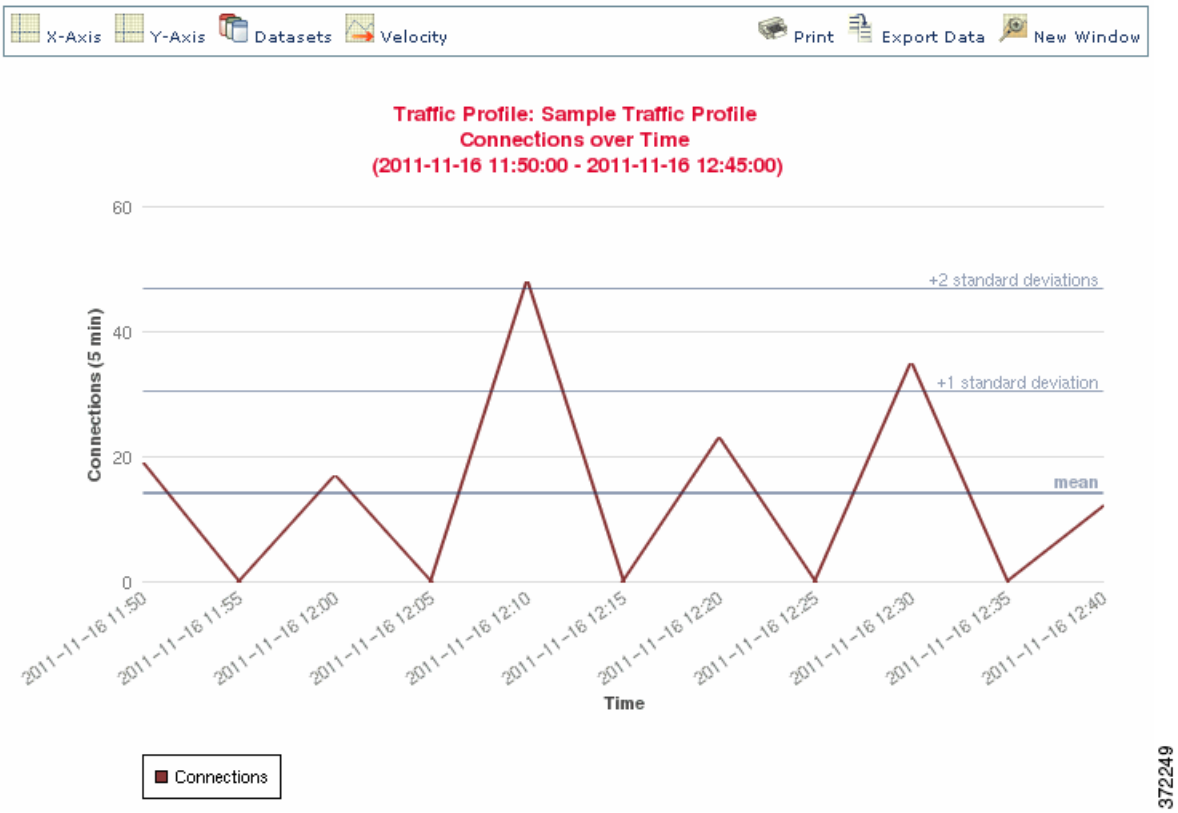
用于收集数据以构建流量量变曲线的时间跨度被称为量变曲线时间段 (PTW)。PTW 是一个滑动窗口；也就是说，如果 PTW 是一周 （默认值），流量量变曲线将包括上一周内收集的连接数据。您可以将 PTW 更改为短至 1 小时或长至几周。

当您首次激活流量量变曲线时，它会根据您设置的条件收集并评估在一段等同于 PTW 的学习期内的连接数据。直至学习期结束，防御中心不会评估您已经针对流量量变曲线写入的规则。

您可以使用监控网段的所有流量来创建量变曲线，或者使用基于连接事件中的数据的标准来创建更有针对性的量变曲线。例如，您可以设置量变曲线条件，使得流量量变曲线仅收集所检测的会话使用特定端口、协议或应用的数据。或者，您也可以将主机量变曲线限定条件添加到流量量变曲线中，以仅为显示出**高**主机重要性的主机收集数据。

最后，当您创建流量量变曲线时，可以指定不活跃周期，其中连接数据应不影响量变曲线统计数据并且不会触发为量变曲线写入的规则。您也可以更改流量量变曲线聚合的频率，并根据所收集的连接数据计算统计数据。

下图显示了 PTW 为一天及采样率为五分钟的流量量变曲线。



在创建并激活流量量变曲线且其学习期结束后，您可以创建在您检测到异常流量时触发的关联规则。例如，您可写入当通过网络的数据量 （单位为数据包、 KB 或连接数）突然达到平均流量以上三个标准差的峰值时触发的规则，这可能表示出现攻击或其他安全策略违规。然后，您可以包括关联策略中的规则以警告您流量达到峰值或执行补救措施作为响应措施。有关使用流量量变曲线检测网络异常流量的信息，请参阅第 51-2 页上的创建关联策略规则。

您可以在 Traffic Profiles 页面上创建流量量变曲线。每个量变曲线旁边的滑动图标表示量变曲线是否处于活动状态。如果您想要在关联规则的基础上实现流量量变曲线更改，则必须激活量变曲线。如果滑动图标显示为蓝色且带复选标记，则量变曲线处于活动状态。如果是灰色并带有一个 X 标记，则量变曲线处于不活动状态。有关详细信息，请参阅第 53-8 页上的激活和禁用流量量变曲线。

进度条可显示流量量变曲线学习期的状态。当进度条达 100% 时，将触发为量变曲线写入的关联规则。

提示　您可以使用 **Sort by** 下拉列表按状态 （活动还是不活动）或按字母顺序对流量量变曲线进行排序。

有关详情，请参阅：

- 第 53-3 页上的提供基本量变曲线信息
- 第 53-3 页上的指定流量量变曲线条件
- 第 53-5 页上的添加主机配置文件限定条件
- 第 53-7 页上的设置量变曲线选项
- 第 53-7 页上的保存流量量变曲线

提供基本量变曲线信息

许可证：FireSIGHT

当您创建流量量变曲线时，必须为其命名，并且或者作简要说明。

要开始创建流量量变曲线，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**，然后点击 **Traffic Profiles**。

系统将显示 Traffic Profiles 页面。

步骤 2　点击 **New Profile**。

系统将显示 Create Profile 页面。

步骤 3　在 **Profile Name** 字段中，键入至多 255 个字符的新流量量变曲线名称。

步骤 4　在 **Profile Description** 字段中，为新创建的流量量变曲线键入简短描述，最多 255 个字符。

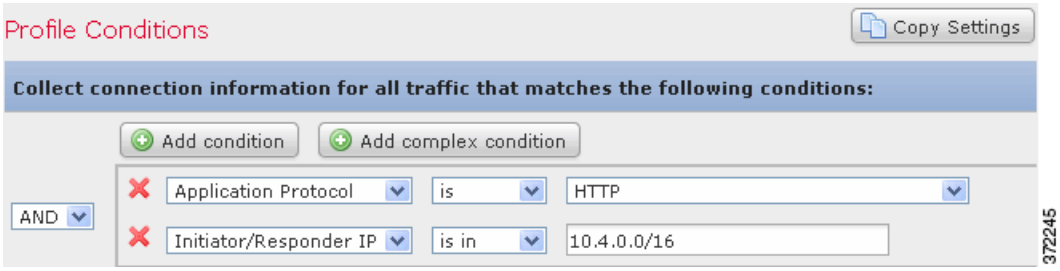
步骤 5　进入下一节指定流量量变曲线条件。

指定流量量变曲线条件

许可证：FireSIGHT

量变曲线条件限制您希望流量量变曲线跟踪的连接数据类型。简要介绍监控网段上的所有流量的简单流量量变曲线没有条件。相反，流量量变曲线可能非常复杂，并含有多个嵌套条件。

例如，下图中的流量量变曲线条件收集了 10.4.x.x 子网上的 HTTP 连接。



您可在 Create Profile 页面的 **Profile Conditions** 部分构建流量量变曲线条件。有关构建条件的信息，请参阅第 53-9 页上的了解条件构建机制。此外，您可以用来构建条件的完整语法描述在第 53-4 页上的流量量变曲线条件的语法进行了介绍。

提示　如果您想要使用来自某个现有流量量变曲线的设置，在弹出窗口中点击 **Copy Settings**，选择您想要使用的流量量变曲线并点击 **Load**。

流量量变曲线条件的语法

许可证：FireSIGHT

下表介绍了如何构建流量量变曲线条件。

请记住， NetFlow 记录不包含有关连接的主机是发起方、而其自身为响应方的信息。当系统处理 NetFlow 记录时，它会根据各主机正在使用的端口以及此类端口是否为公认端口来使用一种算法确定该信息。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

流量量变曲线的可用信息取决于多种因素，包括检测方法、日志记录方法和事件类型。有关详细信息，请参阅第 39-9 页上的连接和安全情报事件中的可用信息。

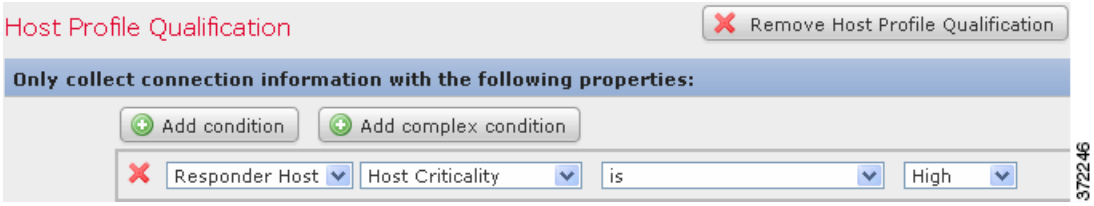
表 53-1　　量变曲线条件的语法

如果指定.....	选择一个运算符，然后.....
应用协议	从可用协议下拉列表中选择一个应用协议名称。
Application Protocol Category	从可用类别下拉列表中选择一个应用协议类别名称。
Client	从可用客户端下拉列表中选择一个客户端名称。
Client Category	从可用类别下拉列表中选择一个客户端类别名称。
连接类型	在流量量变曲线中指定您是想要使用思科设备还是启用了 NetFlow 的设备收集的连接数据。如果您不指定连接类型，则流量量变曲线会同时包括两者。
Destination Country 或 Source Country	从可用国家/地区下拉列表中选择一个国家/地区。这表示与网络流量中识别的源或目标 IP 地址相关联的国家/地区。
Initiator IP、Responder IP 或 Initiator/Responder IP	使用特定 IP 地址或 CIDR 表示法指定 IP 地址范围。 有关 IP 地址允许的语法的说明，请参阅第 60-6 页上的在搜索中指定 IP 地址。但请注意，**不能**使用 `local` 或 `remote` 关键字来指定在或不在您正在监控的网络中的 IP 地址。
NetFlow Device	选择您想要创建流量量变曲线时用其数据的启用了 NetFlow 的设备。如果您没有将任何启用了 NetFlow 的设备添加到部署中 （使用本地配置）， NetFlow Device 下拉列表将为空。
Responder Port/ICMP Code	键入端口号或 ICMP 代码。
Security Intelligence Category	从可用类别下拉列表中选择一个 Security Intelligence 类别名称。要将 Security Intelligence 类别用于流量量变曲线条件，该类别必须在访问控制策略的 Security Intelligence 部分被设置为 **Monitor** 而不是 **Block**。有关详细信息，请参阅第 13-3 页上的建立安全情报白名单和黑名单。
SSL Encrypted Session	选择 **Successfully Decrypted**。
Transport Protocol	键入 `TCP` 或 `UDP` 作为传输协议。
Web Application	从可用的网络应用下拉列表中选择一个网络应用名称。
Web Application Category	从可用类别下拉列表中选择一个网络应用类别名称。

添加主机配置文件限定条件

许可证：FireSIGHT

您可以使用来自被追踪主机的主机量变曲线的信息限制任何流量量变曲线。此类限制被称为*主机配置文件限定条件*。例如，如下图所示，您可以为仅被分配了**高**主机重要性的主机收集连接数据。



要使用主机配置条件限定条件，主机必须存在于数据库中，且您想要用作限定条件文件的主机配置文件属性必须已经包含在主机配置文件中。例如，如果您配置了关联策略规则以触发何时在运行 Windows 的主机上生成入侵事件，则该规则仅会在生成入侵事件时主机已经被识别为 Windows 时触发。

要添加主机配置文件限定条件，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在 Create Profile 页面上，点击 **Add Host Profile Qualification**。

系统将显示 Host Profile Qualification 部分。

步骤 2　构建主机配置文件限定条件的条件。

可以创建一个简单的条件，或者通过结合和嵌套条件来创建较复杂的结构。有关构建条件的信息，请参阅第 53-9 页上的了解条件构建机制。

第 53-5 页上的用于主机配置文件限定条件的语法中介绍可以用来构建条件的语法。

提示　要移除主机配置文件限定条件，请点击 **Remove Host Profile Qualification**。

用于主机配置文件限定条件的语法

许可证：FireSIGHT

当您构建主机配置文件限定条件时，必须首先选择要用于限制流量量变曲线的主机。您可以选择 **Responder Host** 或 **Initiator Host**。在选择主机角色之后，请继续构建主机配置文件限定条件，如主机配置文件限定条件的语法表中所述。

虽然可将网络发现策略配置为根据 NetFlow 支持设备导入的数据向网络映射添加主机，但关于这些主机的可用信息是有限的。例如，这些主机没有可用的操作系统数据，除非您使用主机输入功能提供这些数据。此外，如果流量量变曲线使用已启用 NetFlow 的设备导出的连接数据，请记住 NetFlow 记录不包含有关连接中的哪台主机是发起方、哪台是响应方的信息。当系统处理 NetFlow 记录时，它会根据各主机正在使用的端口以及此类端口是否为公认端口来使用一种算法确定该信息。有关详细信息，请参阅第 45-14 页上的 NetFlow 与 FireSIGHT 数据之间的差异。

要匹配*隐含*或一般客户端，请根据响应客户端的服务器所用的应用协议创建主机配置文件限定条件。当作为连接发起方或源的主机上的客户端列表包含**客户端**遵循的应用协议名称时，该客户端可能实际上就是一种隐含客户端。换句话说，系统会根据使用该客户端的应用协议的服务器响应流量，而非检测到的客户端流量来报告该客户端。

例如，如果系统将 **HTTPS 客户端**作为主机上的一个客户端进行报告，请为 **Responder Host** 创建主机配置限定条件，其中 **Application Protocol** 被设置为 **HTTPS**，因为 HTTPS 客户端会根据响应方或目标主机发送的 HTTPS 服务器响应流量被报告为一种一般客户端。

表 53-2　　主机配置文件限定条件的语法

如果指定.....	选择一个运算符，然后.....
Host Type	从下拉列表中选择一个或多个主机类型。您可以在一个常规主机或多种网络设备中的一种之间选择。
NETBIOS Name	键入主机的 NetBIOS 名称。
Operating System > OS Vendor	从下拉列表中选择一个或多个操作系统供应商名称。
Operating System > OS Name	从下拉列表中选择一个或多个操作系统名称。
Operating System > OS Version	从下拉列表中选择一个或多个操作系统版本名称。
网络协议	键入 http://www.iana.org/assignments/ethernet-numbers 列出的网络协议号。
Transport Protocol	键入 http://www.iana.org/assignments/protocol-numbers 列出的传输协议的名称或编号。
Host Criticality	从显示的列表中选择主机重要性。可选择 **None**、**Low**、**Medium** 或 **High**。有关主机重要性的详细信息，请参阅第 49-27 页上的使用预先定义的主机属性。
VLAN ID	键入主机的 VLAN ID 号。
Application Protocol> Application Protocol	从下拉列表中选择一个应用协议。
Application Protocol > Application Port	键入应用协议端口号。
Application Protocol > 协议	从下拉列表中选择协议。
Client > Client	从下拉列表中选择一个客户端。
Client > Client Version	键入客户端版本。
Web 应用程序	从下拉列表中选择一个客户端。
MAC Address > MAC Address	键入主机的全部或部分 MAC 地址。
MAC Address > MAC Type	选择 MAC 类型是否为 **ARP/DHCP Detected**。 也就是说，选择系统是否将 MAC 地址积极识别为属于主机 (**is ARP/DHCP Detected**)，系统是否认为许多主机带有该 MAC 地址，例如，因为在设备和主机之间有一个路由器 (**is not ARP/DHCP Detected**)，或者 MAC 类型是否无关 (**is any**)。
MAC Vendor	键入主机使用的硬件的全部或部分 MAC 供应商名称。
任何可用的主机属性，包括默认合规性白名单主机属性	指定适当的值，这取决于选择的主机属性类型： • 如果主机属性类型为 Integer，请在针对该属性确定的范围中输入一个整数值。 • 如果主机属性类型是 Text，请输入文本值。 • 如果主机属性类型是 List，请从下拉列表中选择一个有效的列表字符串。 • 如果主机属性类型是 URL，请输入 URL 值。 有关主机属性的详细信息，请参阅第 49-27 页上的使用用户定义的主机属性。

设置量变曲线选项

许可证：FireSIGHT

量变曲线时间段 (PTW) 是滑动时间窗，长度等于FireSIGHT 系统用于计算流量量变曲线统计数据的学习期长度。默认 PTW 是一周，但是，您可以将其更改为短至 1 小时或长至几周。

此外，流量量变曲线基于聚合的连接数据。默认情况下，流量量变曲线会生成系统在五分钟时间区间内生成的连接事件的统计数据。但是，您可以在默认的五分钟和一小时之间随意设置采样率。

请记住，您应设置 PTW 和采样率，以便流量量变曲线包含足够的数据以具备统计意义。例如，采样率为一小时的一天的 PTW 可能只包含 24 个数据点，可能不足以准确地分析网络流量模式。

提示　PTW 应至少包含 100 个数据点。

您也可以在流量量变曲线中设置非活动周期。例如，可以考虑所有工作站均在每晚午夜时备份的网络基础设施。备份大约需要 30 分钟，并将使网络流量达到峰值。在这种情况下，您可能希望为流量量变曲线设置一个经常性的非活动周期，以与定期备份相符。在非活动周期，流量量变曲线会收集数据 （因此，您可在流量量变曲线图上看到流量），但是，在计算量变曲线统计数据时不会使用收集到的数据。可以将非活动周期设置为每日、每周或每月。非活动周期可以短至五分钟或长至一小时。一段时间内划分的流量量变曲线图可显示非活动周期为阴影区域。

要设置量变曲线件选项，请执行以下操作：

访问：管理员/发现管理员

表 53-3　　量变曲线选项

如果要...	您可以.....
更改量变曲线时间段	在 **Profiling Time Window** 字段中，键入小时数、天数或周数。然后从下拉列表中选择 **hour(s)**、 **day(s)**、或 **week(s)**。
更改采样率	从 **Sampling Rate** 下拉列表中选择速率。
添加非活动周期	点击 **Add Inactive Period**。然后，使用下拉列表指定您希望流量量变曲线避免收集数据的时间和频率。
删除非活动周期	点击您要删除的非活动周期旁边的 **Delete**。

保存流量量变曲线

许可证：FireSIGHT

使用以下步骤保存流量量变曲线。

要保存流量量变曲线，请执行以下操作：

访问：管理员/发现管理员

步骤 1　此时您有两种选择：

- 要保存量变曲线而不激活它，请点击 **Save**。
- 要保存量变曲线并立即开始收集数据，请点击 **Save & Activate**。

激活和禁用流量量变曲线

许可证：FireSIGHT

当您想要在监控网段上开始配置流量时，则必须激活流量量变曲线。

当您要停止收集和评估连接数据时，请禁用量变曲线。对禁用的流量量变曲线写入的规则不会触发。此外，禁用流量量变曲线会删除变了曲线所收集和汇聚的所有数据。如果以后要重新激活已禁用的流量量变曲线，您必须等待 PTW 时常，对其写入的规则才会触发。

要激活或禁用流量量变曲线，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**，然后点击 **Traffic Profiles**。

系统将显示 Traffic Profiles 页面。

步骤 2　此时您有两种选择：

- 要激活非活动的流量量变曲线，请点击量变曲线旁边的 **Activate**。
- 要禁用活动的流量量变曲线，请点击量变曲线旁边的 **Deactivate**。点击 **OK** 确认要禁用量变曲线。

编辑流量量变曲线

许可证：FireSIGHT

您不能完全编辑活动的流量量变曲线；如果流量量变曲线处于活动状态，只能更改其名称和说明。要编辑流量量变曲线的条件选项，必须先禁用它。请注意，禁用流量量变曲线会删除其所收集的所有数据。

有关激活和禁用流量量变曲线的详细信息，请参阅第 53-8 页上的激活和禁用流量量变曲线。

要编辑流量量变曲线，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**，然后点击 **Traffic Profiles**。

系统将显示 Traffic Profiles 页面。

步骤 2　点击要编辑的流量量变曲线旁边的 **Edit**。

系统将显示 Create Profile 页面。

步骤 3　对量变曲线进行更改，然后点击 **Save**。

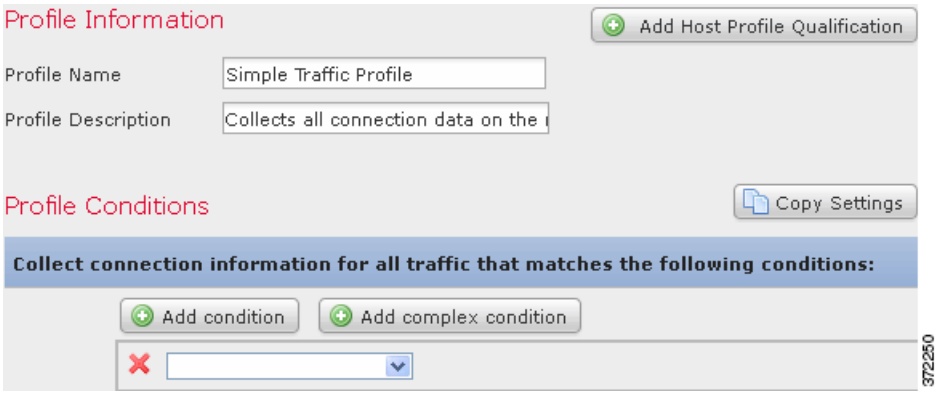
量变曲线更新成功。

了解条件构建机制

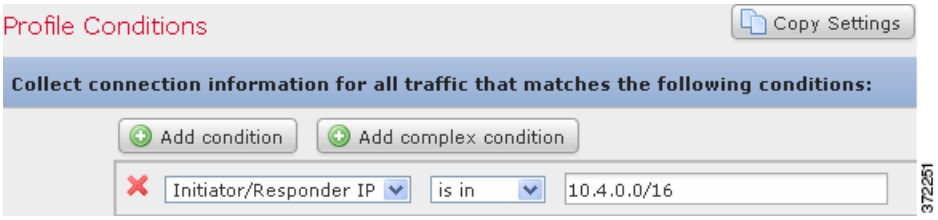
许可证：FireSIGHT

您可通过指定流量量变曲线用于收集数据的条件来构建流量量变曲线。您可以使用嵌套条件来创建简单的条件或较复杂的结构。

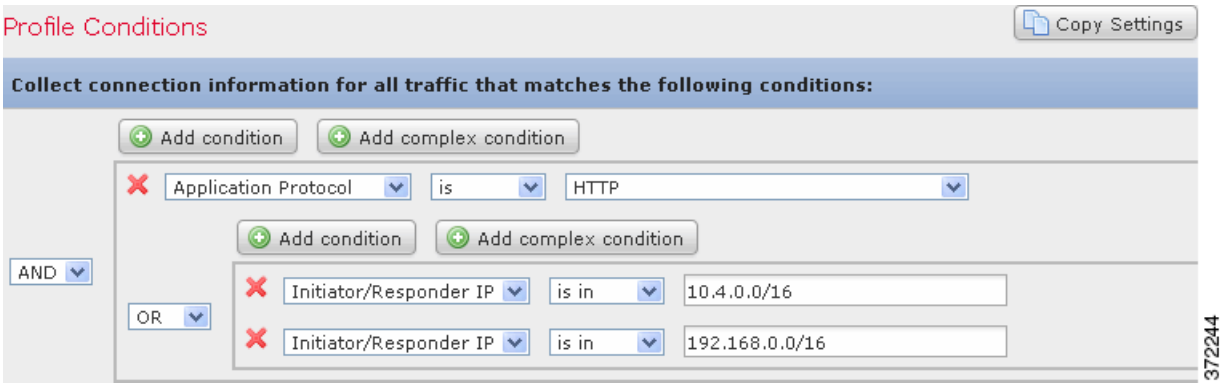
例如，如果想要创建为整个监控网段收集数据的流量量变曲线，您可以创建一个非常简单的不带条件的流量量变曲线，如下图所示。



如果想要仅为 10.4.x.x 网络限制流量量变曲线和收集数据，您可以添加单个条件，如下图所示。



但是，在 10.4.x.x 网络和 192.168.x.x 网络上收集 HTTP 活动的以下流量量变曲线有三个条件，最后一个构成复杂条件。



可以在条件中使用的语法会根据您正在创建的元素而变化，但是机制相同。有关详情，请参阅：

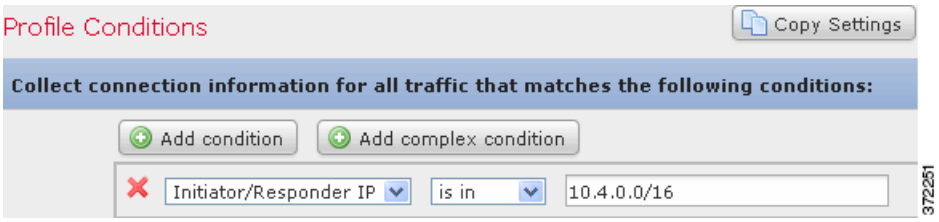
- 第 53-10 页上的构建一个条件
- 第 53-11 页上的添加和连接条件
- 第 53-14 页上的在一个条件中使用多个值

构建一个条件

许可证：FireSIGHT

大多数条件有三部分：类别、操作符和值。某些条件较为复杂，包含多个类别，每个类别都可能有自己的操作符和值。

例如，以下流量量变曲线可收集有关 10.4.x.x 网络的信息。条件的类别是 **Initiator/Responder IP**，操作符是 **is in**，值为 `10.4.0.0/16`。



以下步骤说明了如何构建该流量量变曲线条件。

要构建一个条件，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**，然后点击 **Traffic Profiles**。

系统将显示 Traffic Profiles 页面。

步骤 2　点击 **New Profile**。

系统将显示 Create Profile 页面。

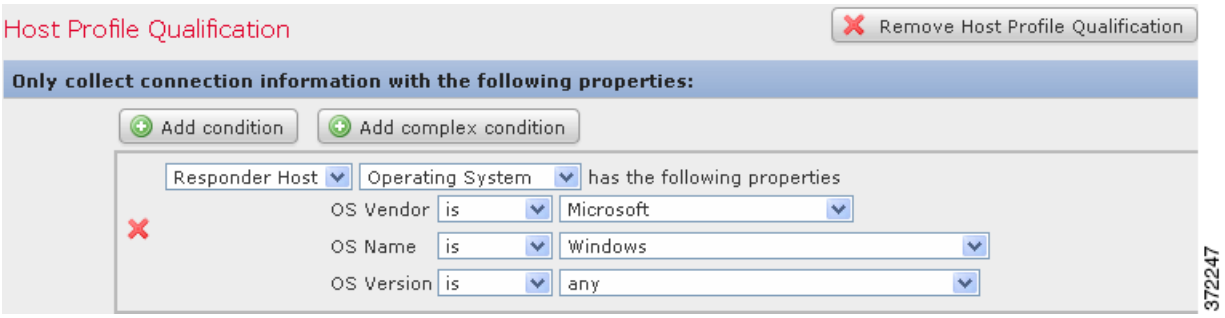
步骤 3　在 **Profile Conditions** 下，从第一个 （类别）下拉列表中选择 **Initiator/Responder IP** 可以开始构建流量曲线的一个条件。

步骤 4　从第二个 （操作符）下拉列表中选择 **is in**。

提示　当类别为某个 IP 地址时，选择 **is in** 或 **is not in** 作为操作符使您可以指定 IP 地址*是*还是*不是*在某个 IP 地址范围中，如 CIDR 表示法所示。有关在 FireSIGHT 系统中使用 CIDR 表示法的信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 5　在文本字段中键入 `10.4.0.0/16`。

相反，以下主机配置文件限定条件则较为复杂；它限制了流量量变曲线以便其只在检测到的连接中的响应主机运行 Microsoft Windows 版本时才会收集连接数据。



以下步骤说明了如何构建该主机配置文件限定条件。

要构建该主机配置文件限定条件，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**，然后点击 **Traffic Profiles**。

系统将显示 Traffic Profiles 页面。

步骤 2　点击 **New Profile**。

系统将显示 Create Profile 页面。

步骤 3　点击 **Add Host Profile Qualification**。

步骤 4　在第一个条件的 **Host Profile Qualification** 下，指定您想要收集其信息的主机。

在本示例中，选择 **Responder Host**，因为我们只想了解有关连接中应答主机的信息。

步骤 5　通过选择 **Operating System** 类别，开始指定主机的操作系统的详细信息。

系统显示三个子类别：**OS Vendor**、 **OS Name** 和 **OS Version**。

步骤 6　要指定主机可运行任何版本的 Microsoft Windows，请对所有这三个子类别使用相同的运算符：**is**。

步骤 7　最后，指定子类别的值。

将 **Microsoft** 选定为 **OS Vendor** 的值、 **Windows** 选定为 **OS Name** 的值，将 **any** 保留为 **OS Version** 的值。

请注意，您能从中选择的类别取决于您是构建流量量变曲线条件还是主机配置文件限定条件。此外，条件的可用运算符取决于选择的类别。最后，可用于指定条件值的语法取决于类别和运算符。有时候，必须在文本字段中键入值。有时候，可以从下拉列表中选择值。

注　如果条件语法允许您从下拉列表中选择值，通常可使用多个列表中的值。有关详细信息，请参阅第 53-14 页上的在一个条件中使用多个值。

有关构建流量量变曲线条件和主机配置文件限定条件的语法的详细信息，请参阅：

- 第 53-4 页上的流量量变曲线条件的语法
- 第 53-5 页上的用于主机配置文件限定条件的语法

添加和连接条件

许可证：FireSIGHT

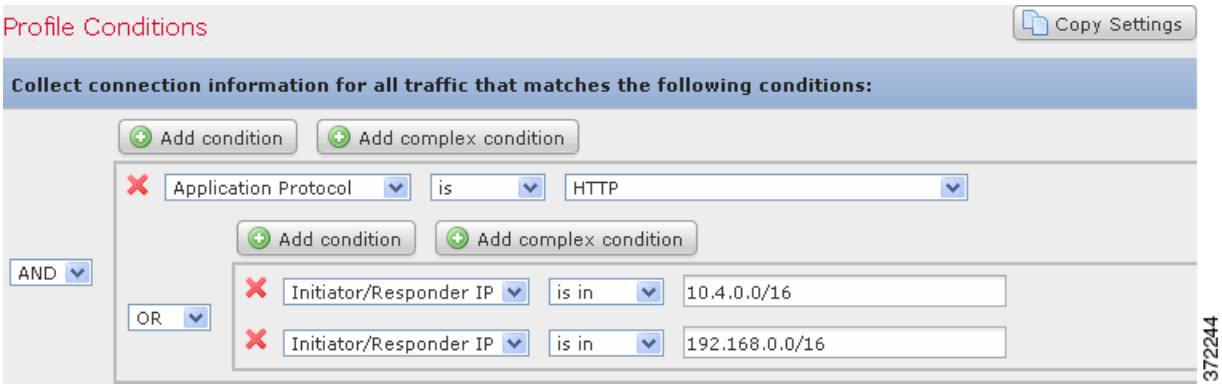
您可以创建简单的流量量变曲线条件和主机配置文件限定条件，也可以通过结合和嵌套条件创建较复杂的结构。

当构建的结构不止一个条件时，必须将这些条件用 **AND** 与 **OR** 运算符结合起来。相同级别的条件会被放在一起评估：

- **AND** 操作符要求必须满足其控制的级别上的所有条件。
- **OR** 运算符要求必须满足其控制的级别上的至少一个条件。

例如，以下流量量变曲线包含以 **AND** 连接的两个条件。这意味着流量量变曲线仅会在两种条件均为真时收集连接数据。在本示例中，它会收集所有 IP 地址在 10.4.x.x 子网中的主机的 HTTP 连接。

相反，在 10.4.x.x 网络或 192.168.x.x 网络中收集 HTTP 活动连接数据的以下流量量变曲线有三个条件，最后一个构成复杂条件。



从逻辑上讲，上述流量量变曲线应如下进行评估：

```
(A and (B or C))
```

其中.....	为陈述以下情况的条件.....
A	应用协议名称是 HTTP
B	IP 地址为 10.4.0.0/16
C	IP 地址为 192.168.0.0/16

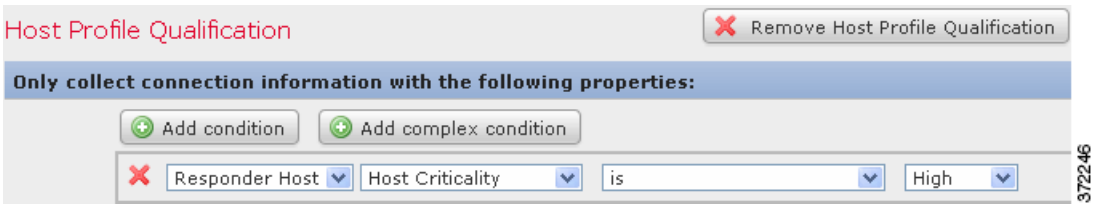
要添加一个条件，请执行以下操作：

访问：管理员/发现管理员

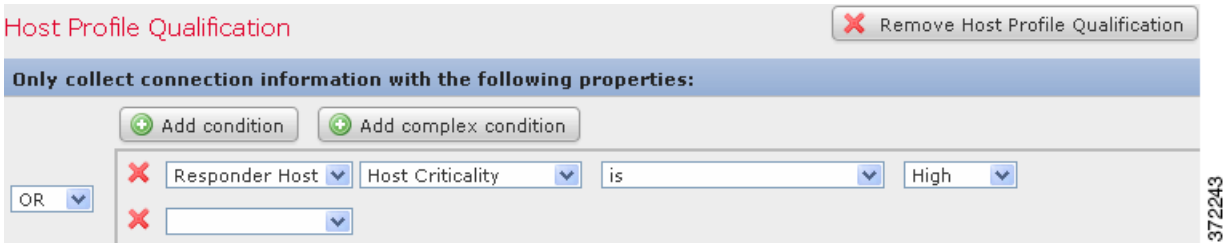
步骤 1　要添加一个条件，请点击当前条件上方的 **Add condition**。

新的条件会作为当前的条机集添加到相同逻辑级别。默认情况下，它会以 **OR** 操作符连接至其级别上的条件中，但您可以将操作符更改为 **AND**。

例如，如果您将简单条件添加到以下主机配置文件限定条件中：



结果为：



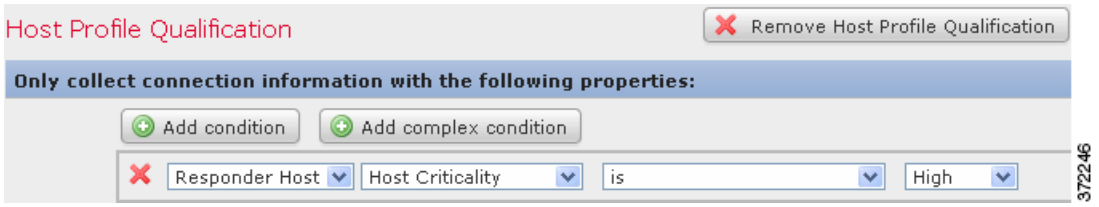
要添加一个复杂的条件，请执行以下操作：

访问：管理员/发现管理员

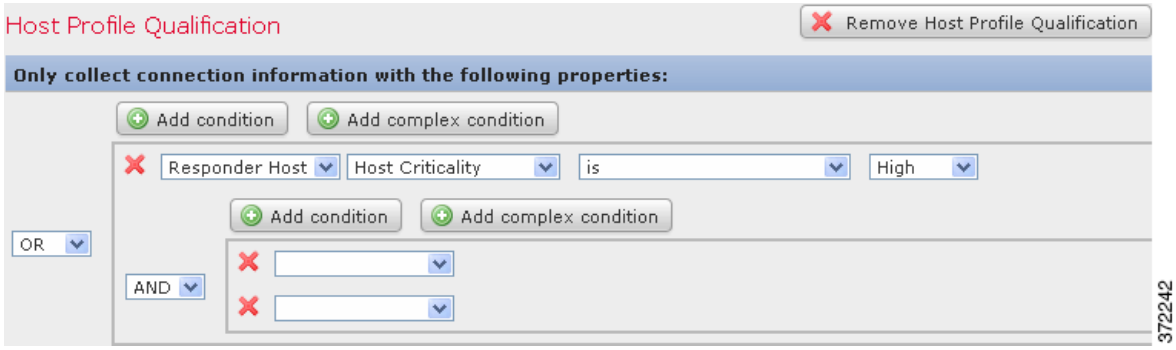
步骤 1　点击当前条件上方的 **Add complex condition**。

复杂条件会被添加到当前条件集的下方。复杂条件包括两个子条件，这两个子条件会用相反的运算符从用于连接上一级别的条件相互连接。

例如，如果添加复杂条件添加到以下主机配置文件限定条件中：



结果为：



要连接条件，请执行以下操作：

访问：管理员/发现管理员

步骤 1　使用条件集左侧的下拉列表：

- 如果需要所有条件都位于满足操作符控制的级别上，选择 **AND**。
- 如果需要只有一个条件位于满足操作符控制的级别上，选择 **OR**。

在一个条件中使用多个值

许可证：FireSIGHT

在构建条件，且条件语法允许您从下拉列表中选择值时，通常可以从列表中选择多个值。例如，如果想要将主机配置文件限定条件添加到需要主机运行 UNIX 的流量量变曲线，而非构建使用 OR 操作符连接的多个条件，请使用以下步骤。

要在一个条件中包含多个值，请执行以下操作：

访问：管理员/发现管理员

步骤 1　构建一个条件，选择 **is in** 或 **is not in** 作为运算符。

下拉列表更改至文本字段。

步骤 2　点击文本字段或 **Edit** 链接的任意位置。

系统将显示一个弹出窗口。

步骤 3　在 **Available** 下，点击的同时使用 Ctrl 或 Shift 选择多个值。也可以点击并拖动以选择多个相邻值。

步骤 4　点击右箭头 (**>**) 以将选定条目移至 **Selected**。

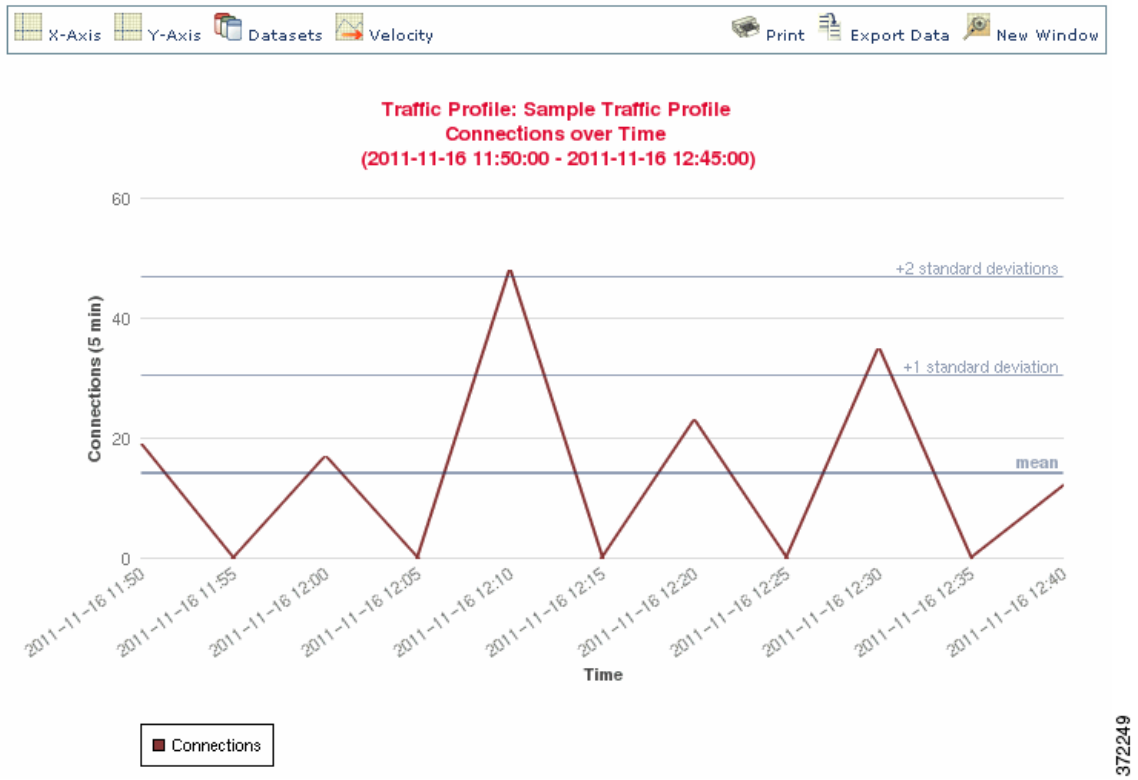
步骤 5　点击**确定**。

Create Profile 页面的条件值字段中显示您的选择。

查看流量量变曲线

许可证：FireSIGHT

由于流量量变曲线基于连接数据，因此您可以查看流量量变曲线图。下图显示了 PTW 为一周、采样率为五分钟，以及不活动周期为每天从午夜到上午 12:30 之间的半小时时间的流量量变曲线。



您可以在连接数据图上执行可在连接配置图上执行的几乎所有相同操作。但是，因为流量量变曲线基于聚合数据（连接摘要），您无法检查作为图形基础的单个连接事件。换句话说，您不能从流量量变曲线图中向下钻取至连接数据表视图。有关详情，请参见第 39-12 页上的查看连接和安全情报数据。此外，流量量变曲线会显示为孤立的图形。有关详细信息，请参阅第 39-23 页上的分离连接图。

此外，一段时间内的流量量变曲线图会显示平均（平均值）y 轴值为一条水平粗线。假设网络流量正常分布的话，一段时间内的图形还会在平均值上下标绘出前四个标准差。默认情况下，这些统计数据会采用 PTW 计算，但是，如果您修改图形的时间设置，防御中心会重新计算统计数据。但是，对流量配置统计数据写入的规则始终会根据 PTW 的统计数据进行评估。

要查看流量量变曲线的流量量变曲线图，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Correlation**，然后点击 **Traffic Profiles**。

系统将显示 Traffic Profiles 页面。

步骤 2　点击要查看的图形的流量量变曲线旁边的图形图标 ( )。

流量量变曲线图将显示在单独的浏览器窗口中。

配置补救

出现违反关联策略的情况时，可将 FireSIGHT 系统 配置为发起一个或多个响应，包括补救 （例如，运行 Nmap 扫描）和各种警报。

可发起的最基本响应类型就是警报。警报通过邮件、 SNMP 陷阱服务器或系统日志向您通知违反策略的情况。有关创建警报的信息，请参阅第 43-1 页上的配置外部警报。

可发起的另一种响应是补救。补救是一种程序，网络流量违反关联策略时，防御中心就会运行该程序。 FireSIGHT 系统附带了预定义的补救，可执行如下操作：违反策略时在防火墙或路由器位置阻止主机，或者扫描主机。

当防御中心发起补救时，会生成补救状态事件。与对任何其他事件一样，可搜索、查看和删除补救状态事件。

FireSIGHT 系统还提供灵活 API，可用于创建自定义补救模块，以响应违反关联策略的情况。例如，如在运行基于 Linux 的防火墙，则可在 Linux 服务器上编写并上传能够动态更新 `iptables` 文件的补救模块，以便阻止违反关联策略的流量。有关编写您自己补救模块的详细信息，请参阅《*思科补救 API 指南*》。

注 必须借助防御中心配置和使用补救。

有关详情，请参阅：

- 第 54-1 页上的创建补救
- 第 54-15 页上的处理补救状态事件

创建补救

许可证：FireSIGHT

警报是一种通知违反关联策略的简单响应形式，除此警报，还可配置名为*补救*的响应。补救是在违反关联策略时防御中心运行的程序。这些程序使用触发违反时提供的信息，执行特定操作。

FireSIGHT 系统附带几个预定义的补救模块：

- Cisco IOS Null Route 模块，如在运行 Cisco IOS® 12.0 或更高版本的思科路由器，该模块可用于动态阻止发送至 IP 地址或违反关联策略的网络的流量。

  有关详细信息，请参阅第 54-3 页上的为 Cisco IOS 路由器配置补救。

- Cisco PIX Shun 模块，如在运行 Cisco PIX® 6.0 或更高版本的防火墙，该模块可用于动态阻止从违反关联策略的 IP 地址发送的流量。

  有关详细信息，请参阅第 54-7 页上的配置 Cisco PIX 防火墙补救。

- Nmap 扫描模块，可用于主动扫描特定目标，以确定在这些主机上运行的操作系统和服务器。

  有关详细信息，请参阅第 54-10 页上的配置 Nmap 补救。

- Set Attribute Value 模块，可用于在发生关联事件的主机上设置主机属性。

  请参阅第 54-14 页上的配置设定的属性补救。

可为每个补救模块创建多个实例，每个实例代表一个与特定设备的连接。例如，如果要向四个 Cisco IOS 路由器发送补救，则应配置 Cisco IOS 补救模块的四个实例。

创建实例时，请指定 防御中心与设备建立连接所需的配置信息。然后，为每个已配置实例添加补救，这些补救介绍了违反策略时想要设备执行的操作。

配置完成后，可向响应组添加补救，或将补救专门分配至关联策略中的规则。系统执行这些补救时，将生成补救状态事件，包括详细信息，如补救名称、触发补救的策略和规则及退出状态消息。有关这些事件的详细信息，请参阅第 54-15 页上的处理补救状态事件。

除思科提供的默认模块外，还可编写自定义补救模块，在触发策略违反时执行其他特定任务。请参阅《*补救 API 指南*》，了解有关编写您自己的补救模块和在 防御中心 上进行安装的详细信息。如果安装自定义模块，可使用 Modules 页面来安装、查看和删除新模块。

要在防御中心安装新模块，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Modules**。

系统将显示 Modules 页面。

步骤 2　点击 **Browse**，导航至包含自定义补救模块的文件的保存位置（有关详细信息，请参阅《*补救 API 指南*》）。

步骤 3　点击 **Install**。

自定义补救模块自行安装。

要从防御中心查看或删除模块，请执行以下操作发：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Modules**。

系统将显示 Modules 页面。

步骤 2　执行下列操作之一：

- 点击 **View**，查看模块。

  系统将显示 Module Detail 页面。

- 在要删除的模块旁，点击 **Delete**。**不能**删除思科提供的默认模块。

  补救模块删除成功。

为 Cisco IOS 路由器配置补救

许可证：FireSIGHT

思科提供一个 Cisco IOS Null Route 补救模块，可用于在违反关联策略时借助思科的“null route”命令阻止单个 IP 地址或整个地址块。这会将发送至违反关联策略事件中列为源或目标主机的主机或网络的所有流量转发至路由器的 NULL 接口，从而丢弃该流量（请注意，这将不阻止从违反主机或网络发送的流量）。

Cisco IOS Null Route 补救模块支持运行 Cisco IOS 12.0 和更高版本的思科路由器。只有对路由器拥有 15 级管理访问权限才能执行 Cisco IOS 补救。

注　基于目标的补救仅在以下情况下起作用：将其配置为当基于连接事件或入侵事件的关联规则触发时启动。发现事件仅传输源主机。

注意事项　Cisco IOS 补救激活后，就不再有超时期限。要从路由器删除已阻止的 IP 地址或网络，必须从路由器本身清除路由变化。

要为运行 Cisco IOS 的路由器创建补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　在思科路由器上启用 Telnet。

请参阅思科路由器或 IOS 软件附带的文档，了解有关如何启用 Telnet 的详细信息。

步骤 2　在防御中心中，为计划借助防御中心使用的每个 Cisco IOS 路由器添加 Cisco IOS Null Route 实例。

请参阅第 54-3 页上的添加 Cisco IOS 实例了解相关步骤。

步骤 3　违反关联策略时，可按照要在路由器上引发响应的类型，为每个实例创建特定补救。

以下各节介绍了每种可用补救类型：

- 第 54-4 页上的 Cisco IOS Block Destination 补救
- 第 54-5 页上的 Cisco IOS Block Destination Network 补救
- 第 54-6 页上的 Cisco IOS Block Source 补救
- 第 54-6 页上的 Cisco IOS Block Source Network 补救

步骤 4　开始将 Cisco IOS 补救分配至特定关联策略规则。

添加 Cisco IOS 实例

许可证：FireSIGHT

在 Cisco IOS 路由器上配置 Telnet 访问权限后（请参阅思科路由器或 IOS 软件附带的文档，了解有关启用 Telnet 访问权限的详细信息），可将实例添加至 防御中心。如果要向多个路由器发送补救，必须为每个路由器单独创建实例。

要添加 Cisco IOS 实例，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Instances**。

系统将显示 Instances 页面。

步骤 2　从 **Add a New Instance** 列表，选择 **Cisco IOS Null Route (v1.0)** 并点击 **Add**。

系统将显示 Edit Instance 页面。

步骤 3　在 **Instance Name** 字段中，输入实例名称。

所选名称不得包含空格或特殊字符，且应为描述性名称。例如，如果打算连接多个 Cisco IOS 路由器，将拥有多个实例，因此，可能想要选择诸如 `IOS_01` 和 `IOS_02` 之类的名称。

步骤 4　在 **Router IP** 字段中，输入要用于补救的 Cisco IOS 路由器的 IP 地址。

步骤 5　在 **Username** 字段中，输入路由器的 Telnet 用户名。该用户必须对路由器拥有 15 级管理访问权限。

步骤 6　在 **Connection Password** 字段中，输入 Telnet 用户的用户密码。两个字段中输入的密码必须匹配。

步骤 7　在 **Enable Password** 字段中，输入 Telnet 用户的启用密码。该密码用于进入路由器的特权模式。两个字段中输入的密码必须匹配。

步骤 8　在 **White List** 字段中，输入要从补救中免除的 IP 地址，每行一条。还可使用 CIDR 表示法或特定 IP 地址。例如，系统将接受以下白名单：

```
10.1.1.152
172.16.1.0/24
```

请注意，该白名单与已创建的任何合规性白名单均不关联。有关在 FireSIGHT 系统中使用 CIDR 表示法的信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 9　点击 **Create**。

实例创建成功，补救显示在页面的 Configured Remediations 部分。必须为这些实例添加特定补救，以供关联策略使用。有关详细信息，请参阅：

- 第 54-4 页上的 Cisco IOS Block Destination 补救
- 第 54-5 页上的 Cisco IOS Block Destination Network 补救
- 第 54-6 页上的 Cisco IOS Block Source 补救
- 第 54-6 页上的 Cisco IOS Block Source Network 补救

Cisco IOS Block Destination 补救

许可证：FireSIGHT

Cisco IOS Block Destination 补救可用于阻止从路由器发送至关联事件中目标主机的流量。

注　请**勿**将该补救用作响应基于发现事件的关联规则；发现事件仅传输源主机，不传输目标主机。可用该补救响应基于连接事件或入侵事件的关联规则。

要添加补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Instances**。

系统将显示 Instances 页面。

步骤 2　在要向其添加补救的实例旁，点击视图图标 （  ）。

如果尚未添加实例，请参阅第 54-3 页上的添加 Cisco IOS 实例。

系统将显示 Edit Instance 页面。

步骤 3　在 **Configured Remediations** 部分，选择 **Block Destination**，然后点击 **Add**。

系统将显示 Edit Remediation 页面。

步骤 4　在 **Remediation Name** 字段中，输入补救名称。

选择的名称不得包含空格或特殊字符，且应为描述性名称。例如，如有多个 Cisco IOS 路由器实例，且每个实例有多个补救，则可能想要指定一个诸如 `IOS_01_BlockDest` 之类的名称。

步骤 5　或者，在 **Description** 字段中，输入补救的说明。

步骤 6　依次点击 **Create** 和 **Done**。

补救添加成功。

Cisco IOS Block Destination Network 补救

许可证：FireSIGHT

Cisco IOS Block Destination Network 补救可用于阻止从路由器发送至关联事件中目标网络的任何流量。

注　请**勿**将该补救用作响应基于发现事件的关联规则；发现事件仅传输源主机，不传输目标主机。可用该补救响应基于连接事件或入侵事件的关联规则。

要添加补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Instances**。

系统将显示 Instances 页面。

步骤 2　在要向其添加补救的实例旁，点击 **View**。

如果尚未添加实例，请参阅第 54-3 页上的添加 Cisco IOS 实例。

系统将显示 Edit Instance 页面。

步骤 3　在 **Configured Remediations** 部分，选择 **Block Destination Network**，然后点击 **Add**。

系统将显示 Edit Remediation 页面。

步骤 4　在 **Remediation Name** 字段中，输入补救名称。

选择的名称不得包含空格或特殊字符，且应为描述性名称。例如，如有多个 Cisco IOS 路由器实例，且每个实例有多个补救，则可能想要指定一个诸如 `IOS_01_BlockDestNet` 之类的名称。

步骤 5　或者，在 **Description** 字段中，输入补救的说明。

步骤 6　在 **Netmask** 字段中，输入子网掩码或使用 CIDR 表示法说明要阻止流量进入的网络。

例如，要在单个主机触发规则时阻止流量进入整个 Class C 网络 （不推荐），请使用 `255.255.255.0` 或 `24` 作为子网掩码。

又例如，要阻止流量进入包括触发 IP 地址的 30 条地址，请指定 `255.255.255.224` 或 `27` 作为子网掩码。在这种情况下，如果 IP 地址 `10.1.1.15` 触发补救，则将阻止 `10.1.1.1` 与 `10.1.1.30` 之间的所有 IP 地址。要阻止触发 IP 地址，请将该字段留空，输入 `32` 或 `255.255.255.255`。

步骤 7　依次点击 **Create** 和 **Done**。

补救添加成功。

Cisco IOS Block Source 补救

许可证：FireSIGHT

Cisco IOS Block Source 补救可用于阻止从路由器发送至违反关联策略的关联事件中源主机的任何流量。源主机是连接事件或入侵事件中的源 IP 地址 （这些事件均基于关联规则），或者是发现事件中的主机 IP 地址。

要添加补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Instances**。

系统将显示 Instances 页面。

步骤 2　在要向其添加补救的实例旁，点击 **View**。

如果尚未添加实例，请参阅第 54-3 页上的添加 Cisco IOS 实例。

系统将显示 Edit Instance 页面。

步骤 3　在 **Configured Remediations** 部分，选择 **Block Source**，然后点击 **Add**。

系统将显示 Edit Remediation 页面。

步骤 4　在 **Remediation Name** 字段中，输入补救名称。

选择的名称不得包含空格或特殊字符，且应为描述性名称。例如，如有多个 Cisco IOS 路由器实例，且每个实例有多个补救，则可能想要指定一个诸如 `IOS_01_BlockSrc` 之类的名称。

步骤 5　或者，在 **Description** 字段中，输入补救的说明。

步骤 6　依次点击 **Create** 和 **Done**。

补救添加成功。

Cisco IOS Block Source Network 补救

许可证：FireSIGHT

Cisco IOS Block Source Network 补救可用于阻止从路由器发送至关联事件中源主机网络的任何流量。源主机是连接事件或入侵事件中的源 IP 地址 （这些事件均基于关联规则），或者是发现事件中的主机 IP 地址。

要添加补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Instances**。

系统将显示 Instances 页面。

步骤 2　在要向其添加补救的实例旁，点击 **View**。

如果尚未添加实例，请参阅第 54-3 页上的添加 Cisco IOS 实例。

系统将显示 Edit Instance 页面。

步骤 3　在 **Configured Remediations** 部分，选择 **Block Source Network**，然后点击 **Add**。

系统将显示 Edit Remediation 页面。

步骤 4　在 **Remediation Name** 字段中，输入补救名称。

所选名称不得包含空格或特殊字符，且应为描述性名称。例如，如有多个 Cisco IOS 路由器实例，且每个实例有多个补救，则可能想要指定一个诸如 `IOS_01_BlockSourceNet` 之类的名称。

步骤 5　或者，在 **Description** 字段中，输入补救的说明。

步骤 6　在 **Netmask** 字段中，输入子网掩码或描述要阻止流量进入的网络 CIDR 表示法。

例如，要在单个主机触发规则时阻止流量进入整个 Class C 网络 （不推荐），请使用 `255.255.255.0` 或 `24` 作为子网掩码。

又例如，要阻止流量进入包括触发 IP 地址的 30 条地址，请指定 `255.255.255.224` 或 `27` 作为子网掩码。在这种情况下，如果 IP 地址 `10.1.1.15` 触发补救，则将阻止 `10.1.1.1` 与 `10.1.1.30` 之间的所有 IP 地址。要阻止触发 IP 地址，请将该字段留空，输入 `32` 或 `255.255.255.255`。

步骤 7　依次点击 **Create** 和 **Done**。

补救添加成功。

配置 Cisco PIX 防火墙补救

许可证：FireSIGHT

思科 提供 Cisco PIX Shun 补救模块，该模块可用于通过思科的“shun”命令阻止 IP 地址或网络。该模块阻止从违反关联策略的源或目标主机发送的所有流量，并关闭当前所有连接 （请注意，该模块不会阻止通过防火墙发送*至*主机的流量）。

Cisco PIX Shun 补救模块支持 Cisco PIX 防火墙 6.0 和更高版本。必须拥有 15 级或更高的管理访问权限才能启动 Cisco PIX 补救。

注　基于目标的补救仅在以下情况下起作用：将其配置为当基于连接事件或入侵事件的关联规则触发时启动。发现事件仅传输源主机。

注意事项　Cisco PIX 补救激活后，不再使用超时期限。要解除阻止 IP 地址或网络，必须手动从防火墙移除规则。

要创建 Cisco PIX 防火墙补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　启用防火墙的 Telnet 或 SSH （思科推荐 SSH）。

请参阅 Cisco PIX 防火墙附带的文档，解有关如何启用 SSH 或 Telnet 的详细信息。

步骤 2　在 防御中心 中，为打算通过 防御中心 使用的每个 Cisco PIX 防火墙添加 Cisco PIX Shun 实例。

请参阅第 54-8 页上的添加 Cisco PIX 实例了解相关步骤。

步骤 3　违反关联策略时，可按照要在防火墙上引发响应的类型，为每个实例创建特定补救。

以下各节介绍了可用的补救类型：

- 第 54-9 页上的 Cisco PIX Block Destination 补救
- 第 54-10 页上的 Cisco PIX Block Source 补救

步骤 4　开始将 Cisco PIX 补救分配至特定关联策略规则。

添加 Cisco PIX 实例

许可证：FireSIGHT

在 Cisco PIX 防火墙配置 SSH 或 Telnet 后，可将实例添加至防御中心。如果要向多个防火墙发送补救，则必须为每个防火墙单独创建实例。

注　思科 建议使用 SSH 连接而不是 Telnet 连接。使用 SSH 传输的数据已加密，比用 Telnet 传输安全得多。

要添加 Cisco PIX 实例，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Instances**。

系统将显示 Instances 页面。

步骤 2　从 **Add a New Instance** 列表，选择 **Cisco PIX Shun**，然后点击 **Add**。

系统将显示 Edit Instance 页面。

步骤 3　在 **Instance Name** 字段中，键入实例名称。

选择的名称不得包含空格或特殊字符，且应为描述性名称。例如，如果打算连接多个思科防火墙，则将拥有多个实例，因此，可能想要选择诸如 `PIX_01` 和 `PIX_02` 之类的名称。

步骤 4　或者，在 **Description** 字段键入实例的说明。

步骤 5　在 **PIX IP** 字段中，输入要用于补救的 Cisco PIX 防火墙 IP 地址。

步骤 6　除默认 (`PIX`) 外，如果需要特定用户名，请在 **Username** 字段中键入。

步骤 7　在 **Connection Password** 字段中，输入通过 SSH 或 Telnet 连接防火墙所需的密码。两个字段中输入的密码必须匹配。

步骤 8　在 **Enable Password** 字段中，输入 SSH 或 Telnet 启用密码。该密码用于进入防火墙的特权模式。两个字段中输入的密码必须匹配。

步骤 9　在 **White List** 字段中，输入要从补救中免除的 IP 地址，每行一条。还可使用 CIDR 表示法或特定 IP 地址。例如，系统将接受以下白名单：

```
10.1.1.152
172.16.1.0/24
```

请注意，该白名单与已创建的任何合规性白名单均不关联。有关在 FireSIGHT 系统中使用 CIDR 表示法的信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 10　从 **Protocol** 列表，选择要用于连接防火墙的方法。

步骤 11　点击 **Create**。

实例创建成功，补救显示在页面的 Configured Remediations 部分。必须为这些实例添加特定补救，以用于关联策略中。有关详细信息，请参阅以下各节：

- 第 54-9 页上的 Cisco PIX Block Destination 补救
- 第 54-10 页上的 Cisco PIX Block Source 补救

Cisco PIX Block Destination 补救

许可证：FireSIGHT

Cisco PIX Block Destination 补救可用于阻止从关联事件中目标主机发送的流量。

注　请**勿**将该补救用作响应基于发现事件的关联规则；发现事件仅传输源主机，不传输目标主机。可用该补救响应基于连接事件或入侵事件的关联规则。

要添加补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Instances**。

系统将显示 Instances 页面。

步骤 2　在要向其添加补救的实例旁，点击 **View**。

如果尚未添加实例，请参阅第 54-8 页上的添加 Cisco PIX 实例。

系统将显示 Edit Instance 页面。

步骤 3　在 **Configured Remediations** 部分，选择 **Block Destination**，然后点击 **Add**。

系统将显示 Edit Remediation 页面。

步骤 4　在 **Remediation Name** 字段中，输入补救名称。

选择的名称不得包含空格或特殊字符，且应为描述性名称。例如，如有多个 Cisco PIX 防火墙实例，且每个实例有多个补救，则可能想要指定一个诸如 `PIX_01_BlockDest` 之类的名称。

步骤 5　或者，在 **Description** 字段中，输入补救的说明。

步骤 6　依次点击 **Create** 和 **Done**。

补救添加成功。

Cisco PIX Block Source 补救

许可证：FireSIGHT

Cisco PIX Block Source 补救可用于阻止从违反关联策略的事件所包含源主机发送的任何流量。源主机是连接事件或入侵事件中的源 IP 地址（这些事件均基于关联规则），或者是发现事件中的主机 IP 地址。

要添加补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Instances**。

系统将显示 Instances 页面。

步骤 2　在要向其添加补救的实例旁，点击 **View**。

如果尚未添加实例，请参阅第 54-8 页上的添加 Cisco PIX 实例。

系统将显示 Edit Instance 页面。

步骤 3　在 **Configured Remediations** 部分，选择 **Block Source**，然后点击 **Add**。

系统将显示 Edit Remediation 页面。

步骤 4　在 **Remediation Name** 字段中，输入补救名称。

选择的名称不得包含空格或特殊字符，且应为描述性名称。例如，如有多个 Cisco PIX 防火墙实例，且每个实例有多个补救，则可能想要指定一个诸如 `PIX_01_BlockSrc` 之类的名称。

步骤 5　或者，在 **Description** 字段中，输入补救的说明。

补救添加成功。

配置 Nmap 补救

许可证：FireSIGHT

可响应关联事件，只需扫描触发事件发生的主机。可选择仅扫描触发关联事件的事件端口。

要设置响应关联事件的 Nmap 扫描，必须先创建 Nmap 扫描实例，然后添加 Nmap 扫描补救。然后，可配置 Nmap 扫描，以响应违反策略中规则的情况。

请参阅以下各节：

- 第 54-10 页上的添加 Nmap 扫描实例
- 第 54-11 页上的 Nmap 扫描补救

添加 Nmap 扫描实例

许可证：FireSIGHT

可为要用于扫描网络主机的每个 Nmap 模块设置单独的扫描实例，以查看操作系统和服务器信息。可为 防御中心 中的本地 Nmap 模块和用于远程运行扫描的任何受管设备设置扫描实例。每次扫描结果均始终存储在配置扫描所在的防御中心，即使是从远程受管设备运行扫描。为防止意外或恶意扫描关键任务主机，可创建实例黑名单，指出不应通过实例扫描的主机。

请注意，不可添加与现有扫描实例名称相同的扫描实例。

要创建扫描实例，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Instances**。

系统将显示 Instances 页面。

步骤 2　从 **Add a module type** 下拉列表，选择 **Nmap Remediation (v1.0)**，然后点击 **Add**。

系统将显示 Edit Instance 页面。

步骤 3　在 **Instance Name** 字段中，输入包括 1 至 63 个字母数字字符的名称，不得含有空格以及除下划线 (_) 和 连接号 (-) 的特殊字符。

步骤 4　在 **Description** 字段中，指定包括 0 至 255 个字母数字字符的说明，包括空格和特殊字符。

步骤 5　或者，在 **Black Listed Scan hosts** 字段中，使用以下语法指定 *不应*通过该扫描实例扫描的任何主机或网络：

- 对于 IPv6 主机，精确的 IP 地址 （例如， `2001:DB8:fedd:eeff`）
- 对于 IPv4 主机，精确的 IP 地址 （例如， `192.168.1.101`）或使用 CIDR 表示法的 IP 地址块（例如， `192.168.1.0/24` 扫描 `192.168.1.1` 与 `192.168.1.254` 之间的 254 台主机，包括二者）

如将已列入黑名单网络的主机指定为扫描目标，则该扫描将不运行。有关在 FireSIGHT 系统中使用 CIDR 表示法的信息，请参阅第 1-16 页上的 IP 地址约定。

步骤 6　或者，要从远程受管设备而非防御中心运行扫描，请在 **Remote Device Name** 字段中指定受管设备的名称或 IP 地址。

步骤 7　点击 **Create**。

扫描实例创建成功。

Nmap 扫描补救

许可证：FireSIGHT

可为 Nmap 扫描定义设置，只需创建 Nmap 补救。 Nmap 补救可用作关联策略中的响应，按需运行，或预定在特定时间运行。为了让 Nmap 扫描结果出现在网络映射中，已扫描的主机必须已存在于网络映射中。请注意， NetFlow、主机输入功能和系统本身可以添加主机至网络映射。

有关 Nmap 补救中特定设置的详细信息，请参阅第 47-2 页上的了解 Nmap 补救。

请注意， Nmap 提供的服务器和操作系统数据将保持不变，直至运行另一个 Nmap 扫描。如计划使用 Nmap 扫描主机以获取操作系统和服务器数据，则可能希望设置定期扫描，随时更新任何 Nmap 提供的操作系统和服务器数据。有关详细信息，请参阅第 62-5 页上的自动运行 Nmap 扫描。另请注意，如从网络映射中删除主机，则将丢弃该主机的任何 Nmap 扫描结果。

有关 Nmap 功能的一般信息，请参阅 http://insecure.org 上的 Nmap 文档。

要创建 Nmap 补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Scanners**。

系统将显示 Scanners 页面。

步骤 2　在要为其添加补救的扫描实例旁，点击 **Add Remediation**。

系统将显示 Edit Remediation 页面。

步骤 3　在 **Remediation Name** 字段中，键入补救名称，其中包含 1 到 63 个字母数字字符，没有空格以及除下划线 (_) 和连接号 (-) 以外的特殊字符。

步骤 4　在 **Description** 字段中，键入补救说明，其中包含 0 到 255 个字母数字字符，包括空格和特殊字符。

步骤 5　如果计划使用此补救响应在发生入侵事件、连接事件或用户事件时触发的关联规则，请配置 **Scan Which Address(es) From Event?** 选项。

- 选择 **Scan Source and Destination Addresses**，扫描事件中源 IP 地址和目标 IP 地址代表的主机。
- 选择 **Scan Source Address Only**，扫描事件源 IP 地址代表的主机。
- 选择 **Scan Destination Address Only**，扫描事件目标 IP 地址代表的主机。

如果计划使用此补救响应在发生发现事件或主机输入事件时触发的关联规则，默认情况下，补救将扫描事件涉及到的主机的 IP 地址；无需配置此选项。

注　请**不要**分配 Nmap 补救，以响应触发流量配置文件变化的关联规则。

步骤 6　配置 **Scan Type** 选项：

- 要在以下主机上以隐形模式快速扫描，可发起但不完成 TCP 连接：`admin` 帐户拥有原始数据包访问权限的主机，或未运行 IPv6 的主机，请选择 **TCP Syn Scan**。
- 要使用系统 `connect()` 调用 （可用于以下主机：防御中心上的 `admin` 帐户没有原始数据包访问权限的主机，或未运行 IPv6 的主机）进行扫描，请选择 **TCP Connect Scan**。
- 要发送 ACK 数据包检查端口是否过滤，请选择 **TCP ACK Scan**。
- 要发送 ACK 数据包检查端口是否过滤，并确定端口是否否打开，请选择 **TCP Window Scan**。
- 要使用 FIN/ACK 探针识别 BSD 派生的系统，请选择 **TCP Maimon Scan**。

步骤 7　或者，除了 TCP 端口，如果还要扫描 UDP 端口，请针对 **Scan for UDP ports** 选项选择 **On**。

提示　UDP 端口扫描比 TCP 端口扫描需要更多时间。要加快扫描速度，请保持禁用该选项。

步骤 8　如计划使用此补救响应违反关联策略的情况，请配置 **Use Port From Event** 选项：

- 选择 **On** 可扫描关联事件中的端口，而不是第 12 步指定的端口。

  如果扫描关联事件中的端口，请注意补救扫描的是第 8 步指定的 IP 地址的端口。这些端口也将添加至补救的动态扫描目标。
- 选择 **Off** 可仅扫描第 12 步指定的端口。

步骤 9　如果计划使用此补救响应关联策略违反事件，并希望使用运行检测引擎来检测事件的设备运行扫描，请配置 **Scan from reporting detection engine** 选项：

- 要从运行报告检测引擎的设备进行扫描，请选择 **On**。
- 要从在补救中配置的设备进行扫描，请选择 **Off**。

步骤 10　配置 **Fast Port Scan** 选项：

- 要仅扫描 `nmap-services` 文件中列出的端口，而忽略其他端口设置，请选择 **On**，该文件可在执行设置的受管设备上的 `/var/sf/nmap/share/nmap/nmap-services` 目录中找到。
- 要扫描所有 TCP 端口，请选择 **Off**。

步骤 11　在 **Port Ranges and Scan Order** 字段中，键入要在默认情况下使用 Nmap 语法按自己想要的顺序扫描的端口。

指定值为 1 到 65535。端口间用逗号或空格分隔。还可使用连字符指明端口范围。扫描 TCP 和 UDP 端口时，以 T 作为要扫描的 TCP 端口列表的开端，以 U 作为 UDP 端口列表的开端。例如，要扫描 UDP 流量的端口 53 和 111，然后扫描 TCP 流量的端口 21-25，请输 入`U:53,111,T:21-25`。

请注意，启动补救以响应关联策略违反事件时，如第 8 步中所述，**Use Port From Event** 选项将覆盖此设置。

步骤 12　要探测开放端口以了解服务器厂商和版本信息，请配置 **Probe open ports for vendor and version information**：

- 选择 **On**，扫描主机上的开放端口以获取服务器信息，识别服务器厂商和版本。
- 选择 **Off**，继续使用主机的服务器信息。

步骤 13　如果选择探测开放端口，请从 **Service Version Intensity** 下拉列表中选择一个数字，设置使用的探针数量：

- 要使用更多探针进行更精确、更长久的扫描，请选择一个较大的数字。
- 要使用更少探针进行不太精确、更加快速的扫描，请选择一个较小的数字。

步骤 14　要扫描操作系统信息，请配置 **Detect Operating System** 设置：

- 选择 **On** 可扫描主机信息以确定操作系统。
- 选择 **Off** 可继续使用主机的操作系统信息。

步骤 15　要确定是否发生主机发现以及是否仅针对可用主机运行端口扫描，请配置 **Treat All Hosts As Online**：

- 要跳过主机发现过程并对目标范围内每个主机运行端口扫描，请选择 **On**。
- 要使用 **Host Discovery Method** 和 **Host Discovery Port List** 的设置执行主机发现，并跳过对所有不可用主机的端口扫描，选择 **Off**。

步骤 16　选择 Nmap 测试时要使用的方法，查看主机是否存在并可用：

- 要发送设置了 SYN 标记的空 TCP 数据包，在已关闭端口上引发 RST 响应，或者在可用主机的开放端口上引发 SYN/ACK 响应，请选择 **TCP SYN**。

  请注意，此选项在默认情况下扫描端口 80，TCP SYN 扫描不太可能被设有状态性防火墙规则的防火墙拦截。

- 要发送设置了 ACK 标记的空 TCP 数据包，在可用主机上引发 RST 响应，请选择 **TCP ACK** 。

  请注意，该选项在默认情况下扫描端口 80， TCP ACK 扫描不太可能被防火墙通过状态性防火墙规则阻止。

- 要发送 UDP 数据包，从可用主机的关闭端口引发端口不可达响应，请选择 **UDP**。默认情况下，该选项扫描端口 40125。

步骤 17　如果要在主机发现过程中扫描自定义端口列表，请在 **Host Discovery Port List** 字段中键入适合已选择的主机发现方法的端口列表，用逗号隔开。

步骤 18　配置 **Default NSE Scripts** 选项，控制是否使用默认 Nmap 脚本集进行主机发现以及服务器、操作系统和漏洞发现：

- 要运行默认 Nmap 脚本集，请选择 **On**。
- 要跳过默认 Nmap 脚本集，请选择 **Off**。

有关默认脚本列表，请参阅 http://nmap.org/nsedoc/categories/default.html。

步骤 19　要为扫描过程设置定时，选择定时模板编号；如需进行更快、不太全面的扫描，选择较大的编号，如需进行更慢、更全面的扫描，选择较小的编号。

步骤 20　依次点击 **Save** 和 **Done**。

补救创建成功。

配置设定的属性补救

许可证：FireSIGHT

可响应关联事件，只需在触发事件发生的主机上设定主机属性值。对于文本主机属性，可选择使用事件说明作为属性值。有关主机属性的详细信息，请参阅第 49-27 页上的使用预先定义的主机属性和第 49-27 页上的使用用户定义的主机属性。

要配置设定的属性值设置以响应关联事件，必须先创建设定的属性实例，然后添加设定的属性补救。然后配置属性值更新，以响应策略内规则违反。

有关详细信息，请参阅以下各节：

- 第 54-14 页上的添加设定的属性值实例：
- 第 54-14 页上的设定的属性值补救

添加设定的属性值实例：

许可证：FireSIGHT

可为设定的属性值创建实例，响应违反关联规则的情况。

要创建设定的属性实例，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Instances**。

系统将显示 Instances 页面。

步骤 2　从 **Add a module type** 下拉列表中选择 **Set Attribute Value (v1.0)**，然后点击 **Add**。

系统将显示 Edit Instance 页面。

步骤 3　在 **Instance Name** 字段中，输入包括 1 至 63 个字母数字字符的名称，不得含有空格以及除下划线 (_) 和 连接号 (-) 的特殊字符。

步骤 4　在 **Description** 字段中，指定包括 0 至 255 个字母数字字符的说明，包括空格和特殊字符。

步骤 5　点击 **Create**。

实例创建成功。

设定的属性值补救

许可证：FireSIGHT

可为响应关联规则违反情况而要设置的每个属性值创建设定的属性值补救。如要设置的属性是文本属性，则可将补救设定为使用事件说明作为属性值。

要创建设定的属性值补救，请执行以下操作：

访问：管理员/发现管理员

步骤 1　选择 **Policies > Actions > Instances**。

系统将显示 Instances 页面。

步骤 2　在要向其添加补救的扫描实例旁，点击 **View**。

系统将显示 Edit Instance 页面。

步骤 3　从 **Add a new remediation of type** 下拉列表，选择 **Set Attribute Value**。

系统将显示 Edit Remediation 页面。

步骤 4　在 **Remediation Name** 字段中，键入补救名称，其中包含 1 到 63 个字母数字字符，没有空格以及除下划线 (_) 和连接号 (-) 以外的特殊字符。

步骤 5　在 **Description** 字段中，键入补救说明，其中包含 0 到 255 个字母数字字符，包括空格和特殊字符。

步骤 6　如果计划使用此补救响应在发生入侵事件、用户事件或连接事件时触发的关联规则，请配置 **Update Which Host(s) From Event** 选项。

- 选择 **Update Source and Destination Hosts**，可更新由事件中源 IP 地址和目标 IP 地址代表的主机上的属性值。
- 选择 **Update Source Host Only**，可更新由事件中源 IP 地址代表的主机上的属性值。
- 选择 **Update Destination Host Only**，可更新由事件中目标 IP 地址代表的主机上的属性值。

如果计划使用此补救响应在发生发现事件或主机输入事件时触发的关联规则，默认情况下，补救将扫描事件涉及到的主机的 IP 地址；无需配置此选项。

步骤 7　配置 **Use Description From Event For Attribute Value (text attributes only)** 选项：

- 要使用事件说明作为属性值，请选择 **On**。
- 要使用补救的 Attribute Value 设置作为属性值，请选择 **Off**。

步骤 8　如不计划使用事件说明，请在 **Attribute Value** 字段中键入要设置的属性值。

步骤 9　依次点击 **Save** 和 **Done**。

补救创建成功。

处理补救状态事件

许可证：FireSIGHT

触发补救之后，将生成补救状态事件。这些事件记录在数据库中，可在 Remediation Status 页面中查看。可搜索、查看和删除补救状态事件。

有关详情，请参阅：

- 第 58-19 页上的设置事件时间限制
- 第 54-18 页上的搜索补救状态事件

查看补救状态事件

许可证：FireSIGHT

视乎在使用的工作流程，访问补救状态事件时看到的页面有所不同。可使用预定义工作流程，包括补救的表视图。在表视图中，每个补救状态事件占一行。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关创建自定义工作流程的信息，请参阅第 58-34 页上的创建自定义工作流程。

下表介绍可在补救状态事件工作流程页面执行的某些特定操作。

表 54-1　　用于查看补救状态事件的选项

要.....	您可以.....
了解有关显示的列的详细信息	在第 54-17 页上的了解补救状态表中获得详细信息。
修改所显示事件的时间和日期范围	请参阅第 58-19 页上的设置事件时间限制。 请注意，如果按时间限制事件视图，则在设备配置的时间段外生成的事件（无论是全局或特定事件）可能显示在事件视图中。即使为该设备已配置滚动时窗，也会发生此情况。
对事件进行排序和限制	请参阅第 58-26 页上的限制事件和第 58-29 页上的对向下钻取工作流程页面进行排序。
暂时使用不同的工作流程	按照工作流程标题点击 **(switch workflow)**。有关详细信息，请参阅第 58-14 页上的选择工作流程。
导航至关联事件视图，查看关联事件	点击 **Correlation Events**。有关详细信息，请参阅第 58-31 页上的在工作流程之间导航。
为当前页面添加书签以便快速返回到该页面	点击 **Bookmark This Page**。有关详细信息，请参阅第 58-32 页上的使用书签。
导航到书签管理页面	点击 **View Bookmarks**。有关详细信息，请参阅第 58-32 页上的使用书签。
根据表视图中的数据生成报告	点击 **Report Designer**。有关详细信息，请参阅第 57-8 页上的从事件视图创建报告模板。
向下钻取到工作流程中的下一页，限制特定值	可使用以下其中一种方法： • 在自定义工作流程中创建的向下展开页面上，点击某行内的一个值。请注意，点击表视图行中的值可限制表视图，且不会向下钻取到下一页。 • 要向下钻取到限制某些用户的下一个工作流程页面，在要在下一个工作流程页面上查看的用户旁，选择复选框，然后点击 **View**。 • 要向下钻取到保留当前限制的下一工作流程页面，请点击 **View All**。 **提示**　表视图的页面名称中始终包括“Table View”。 有关详细信息，请参阅第 58-26 页上的限制事件。
从系统删除补救状态事件	可使用以下其中一种方法： • 要删除某些事件，选择要删除事件旁边的复选框，然后点击 **Delete**。 • 要删除当前已限制视图中的所有事件，点击 **Delete All**，然后确认要删除所有事件。
搜索补救状态事件	点击 **Search**。有关详细信息，请参阅第 54-18 页上的搜索补救状态事件。

要查看补救状态事件，请执行以下操作：

访问：管理

步骤 1　选择 **Analysis > Correlation > Status**。

系统将显示默认补救工作流程的第一个页面。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示任何事件，可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

提示　如在使用不含补救表视图的自定义工作流程，按工作流程标题点击 **(switch workflow)** 菜单，然后选择 **Remediation Status**。

处理补救状态事件

许可证：FireSIGHT

您可以更改事件视图的布局或按字段值限制视图中的事件。

禁用列时，该列在会话持续时间内处于禁用状态 （除非稍后重新添加该列）。请注意，禁用第一列时，会添加 Count 列。

请注意，在表视图中点击某一行中的一个值时，会限制该表视图，且不会向下钻取到下一个页面。

提示　表视图的页面名称中始终包括“Table View”。

有关详细信息，请参阅：

- 第 58-26 页上的限制事件.
- 第 58-28 页上的使用复合限制.
- 第 58-29 页上的对向下钻取工作流程页面进行排序.
- 第 54-17 页上的了解补救状态表

了解补救状态表

许可证：FireSIGHT

可将防御中心配置为向策略违反和发现事件发出各种响应。这些响应包括补救，如违反策略时在防火墙或路由器位置阻止主机。补救触发后，会生成补救状态事件并记录到数据库中。有关补救的详细信息，请参阅第 54-1 页上的配置补救。

下表介绍补救状态表中的字段。

表 54-2　　补救状态字段

字段	说明
策略	已违反并触发补救的关联策略的名称。
Remediation Name	已发起的补救的名称。

表 54-2　　补救状态字段 （续）

字段	说明
Result Message	描述在发起补救后所发生情况的消息。状态消息包括： • 成功完成补救 • 提供给补救模块的输入出错 • 补救模块配置出错 • 登录远程设备或服务器出错 • 无法在远程设备或服务器上获得所需权限 • 登录远程设备或服务器超时 • 执行远程命令或服务器超时 • 远程设备或服务器不可达 • 尝试补救失败 • 未能执行补救程序 • 未知/意外错误 **注**　如已安装自定义补救模块，则可能出现自定义模块实现的其他状态消息。
Rule	触发补救的规则的名称。
时间	防御中心发起补救的日期和时间。
计数	与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

要显示补救状态事件的表视图，请执行以下操作：

访问：管理

步骤 1　选择 **Analysis > Correlation > Status**。

系统显示表视图。有关处理补救状态事件的信息，请参阅第 54-15 页上的处理补救状态事件。

提示　如在使用的自定义工作流程不包括补救状态事件的表视图，按工作流程标题点击 **(switch workflow)**，然后点击 **Remediation Status**。

搜索补救状态事件

许可证：FireSIGHT

可搜索补救状态事件，以确定何时及是否发起特殊补救。您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。下表介绍可用的搜索条件。

表 54-3　补救状态搜索条件

搜索字段	说明
Result Message	输入要匹配的结果消息的**精确**名称 （描述发起补救后所发生情况的消息）。有效状态消息如下： • 成功完成补救 • 提供给补救模块的输入出错 • 补救模块配置出错 • 登录远程设备或服务器出错 • 无法在远程设备或服务器上获得所需权限 • 登录远程设备或服务器超时 • 执行远程命令或服务器超时 • 远程设备或服务器不可达 • 尝试补救失败 • 未能执行补救程序 • 未知/意外错误 **注**　如已安装自定义补救模块，则可输入自定义模块实现的其他状态消息。
时间	指定防御中心发起补救的日期和时间。有关时间输入语法，请参阅第 60-5 页上的在搜索中指定时间约束。
Remediation Name	输入已发起补救的精确名称。这是创建补救时指定的名称。
策略	输入触发补救的关联策略的名称。
Rule	输入触发补救的关联规则的名称。

有关搜索的详细信息，包括如何加载和删除已保存搜索，请参阅第 60-1 页上的搜索事件。

要搜索补救状态事件，请执行以下操作：

访问：管理

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉菜单中，选择 **Remediation Status**。

提示　要在数据库中搜索另一类型的事件，请从表下拉列表选择它。

步骤 3　在相应字段中输入搜索条件，如补救状态搜索条件表中所述。

如果您为多个字段输入条件，搜索仅返回符合为所有字段指定的搜索条件的记录。

步骤 4　或者，但是，如果您计划保存搜索，可以选择 **Private** 复选框，将搜索保存为专用搜索，以便只有您可以访问该搜索。否则，请保持清除此复选框，为所有用户保存此搜索。

提示　如要将搜索另存为对已受约事件分析师用户的限制，则**必须**将其另存为专用搜索。

步骤 5　或者，您可以保存搜索以备将来使用。您有以下选项：

- 点击 **Save** 保存搜索条件。

  对于新的搜索，系统显示对话框，提示输入搜索名称；请输入一个唯一搜索名称并点击 **Save**。如果为先前存在的搜索保存新条件，则不会出现提示。已保存搜索（并且如果选择 **Private**，仅对您的帐户可见），以便以后运行。

- 点击 **Save as New** 保存新的搜索，或通过修改先前保存的搜索为已创建的搜索指定名称。

  系统显示对话框，提示输入搜索名称；请输入一个唯一搜索名称并点击 **Save**。已保存搜索（并且如果选择 **Private**，仅对您的帐户可见），以便以后运行。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认补救状态工作流程中，受当前时间范围限制。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

使用控制面板

FireSIGHT 系统控制面板可显示当前的系统状态概况信息，包括有关系统收集和生成的事件的数据。您还可以使用控制面板了解部署中的设备状态和整体运行状况的信息。仅有某些用户角色（管理员、维护人员、安全分析师、安全分析师 [只读] 和自定义的具有控制面板权限的角色）可使用控制面板。其他角色可以看到与其角色相关的默认起始页面；例如，发现管理员可以查看 Network Discovery 页面。

控制面板有一个或多个选项卡，每个选项卡都会以三列布局显示一个或多个构件。构件是了解 FireSIGHT 系统的各个方面的独立组件。 FireSIGHT 系统配置了数个预定义构件。例如，Appliance Information 构件提供有关设备名称、型号、远程管理器，以及当前运行的 FireSIGHT 系统软件版本的信息。

控制面板上有限制其构件的时间范围。您可以更改时间范围，以反映短至前一小时，或长至前一年的时间段里的信息。

控制面板是一种复杂且高度可定制的监控功能。Context Explorer 是查看各种系统数据的另一种途径，它使用一组预定义视觉环境中的入侵、连接和发现数据来展示信息，而您仅仅是临时使用过滤器更改预定义视觉环境以增加粒度。与 FireSIGHT 系统控制面板的全部可用数据相比，Context Explorer 可提供有关监控网络的活动的全面而简洁的彩色照片。有关 Context Explorer 的详细信息，请参阅第 56-1 页上的使用 Context Explorer。

每种设备均有自带的默认控制面板，即 Summary Dashboard。该控制面板可为临时用户提供有关 FireSIGHT 系统部署的常规 FireSIGHT、入侵、威胁检测、地理定位和系统状态信息。请注意，由于一些构件只对特定类型的设备有用，因此， Summary Dashboard 因您是在使用防御中心虚拟防御中心还是受管设备而异。

注 虚拟受管设备没有网络界面，且不支持控制面板功能。

默认情况下，设备的主页会显示 Summary Dashboard，但您仍可以配置设备以显示不同的默认主页。

提示 如果您更改了主页，您可选择 **Overview > Dashboards** 来访问控制面板。有关详细信息，请参阅第 55-33 页上的查看控制面板。

请注意，显示的数据取决于您如何许可和部署受管设备、您是否配置了提供数据的功能，以及，如果是 2 系列设备和用于 Blue Coat X-系列的思科 NGIPS，设备是否支持提供数据的功能等因素。例如，因为 DC500 防御中心和 2 系列设备都不支持按类别和信誉进行 URL 过滤，所以，DC500 防御中心不能显示该功能的数据，且 2 系列设备也无法检测到该数据。

除 Summary Dashboard 外，防御中心还配置了下列预定义控制面板：

- Application Statistics 可提供有关监控的网络上的应用活动和入侵事件的详细信息。您可以使用该控制面板跟踪哪些应用产生了最多的流量、许可及拒绝的连接、入侵事件，以及正在使用的单独应用的数量和此类应用的预计风险及业务相关性。
- Connection Summary 控制面板使用连接数据来创建监控网络上的活动的表格和图表。您可以使用该控制面板来追踪与网络上的连接和流量相关的端口、应用和发起方及响应方 IP、连接量和流量总量、以及地理定位信息。您必须记录该控制面板的连接以生成数据；请参阅第 39-2 页上的了解连接和安全情报数据。请注意，该构件的输出取决于连接记录配置。

提示 该控制面板中的构件列出以千字节 (KB) 为单位的总流量。以 KB 为单位的总流量等于以 KB/s 为单位的流量乘以所选时间段的总秒数。

- Detailed Dashboard 为高级用户提供与 FireSIGHT 系统部署相关的详细信息，它包含多个构件。这些构件可汇总收集的入侵事件、网络发现、合规性、相关性、流量和系统状态数据的信息，并提供思科新闻和产品更新的信息。您可以立即使用此控制面板监控极为广泛的网络信息。
- Files Dashboard 可提供有关受管设备在网络上检测到的文件 （包括恶意软件文件），捕获到的存储于设备上并为动态分析而提交的文件，以及使用基于订用的 FireAMP 策略检测到的恶意软件的详细信息。请注意，您必须拥有恶意软件许可证并启用恶意软件检测，该控制面板才会包括基于网络的恶意软件数据。此外， DC500 和 2 系列设备或用于 Blue Coat X-系列的思科 NGIPS均不支持高级恶意软件防护，因此， DC500 无法显示这些数据，而且 2 系列设备和用于 Blue Coat X-系列的思科 NGIPS也检测不到这些数据。有关详细信息，请参阅第 37-2 页上的了解恶意软件防护和文件控制。
- URL Statistics 控制面板可提供有关从监控网络到外部 URL 的许可及拒绝流量 （按照 URL 类别和信誉划分）的详细信息。请注意，您必须持有 URL 过滤许可证并启用 URL 过滤，该控制面板才会包括 URL 类别和信誉数据。此外，请注意，DC500 和 2 系列设备均不支持按信誉和类别进行 URL 过滤，因此， DC500 无法显示该数据， 2 系列设备也无法检测到它。请参阅第 16-8 页上的执行基于信誉的 URL 阻止。
- Access Controlled User Statistics 控制面板提供了与受监控网络上的用户活动和入侵事件相关的详细信息。您可以使用该控制面板跟踪与您网络中的用户相关的被允许和拒绝的连接、流量和入侵事件，以及网络中的单独用户数量。由于该控制面板取决于用户感知数据，要让该控制面板显示有意义的统计数据，您必须至少配置一个用户代理和一个防御中心 - Active Directory LDAP 服务器连接；请参阅第 17-9 页上的使用用户代理报告 Active Directory 登录情况。

您可以使用预定义控制面板、修改预定义控制面板或创建一个自定义控制面板以满足需求。您可以与某台设备的所有用户共享自定义控制面板，也可以创建一个仅供自己使用的自定义控制面板。您还可以设置一个自定义控制面板作为默认控制面板。

某些事件的深入查看页面和表视图包含一个 **Dashboard** 工具栏链接，您可以点击查看相关的预定义控制面板。下表列出了事件视图与预定义控制面板的对应关系。请注意，如果您删除了某个预定义控制面板或选项卡，相关的控制面板链接将失效。

表 55-1　　事件表控制面板链接

表	控制面板链接
Connection Events (**Analysis > Connections > Events**)	Connection Summary
Security Intelligence Events (**Analysis > Connections > Security Intelligence**)	Connection Summary

表 55-1　事件表控制面板链接 （续）

表	控制面板链接
Intrusion Events (**Analysis > Intrusions > Events**)	摘要 （Intrusion Events 选项卡）
Malware Events (**Analysis > Files > Malware Events**)	文件 （Malware 选项卡）
File Events (**Analysis > Files > File Events**)	文件 （Files 选项卡）
Captured Files (**Analysis > Files > Captured Files**)	文件 （File Storage 选项卡）
应用 (**Analysis > Hosts > Applications**)	Application Statistics
Application Details (**Analysis > Hosts > Application Details**)	Application Statistics
危害表现 (**Analysis > Hosts > Indications of Compromise**)	摘要 （Threats 选项卡）
用户 (**Analysis > Users > Users**)	访问受控用户统计信息
用户活动 (**Analysis > Users > User Activity**)	访问受控用户统计信息
Correlation Events (**Analysis > Correlation > Correlation Events**)	详情 （Correlation 选项卡）
White List Events (**Analysis > Correlation > White List Events**)	详情 （Correlation 选项卡）

有关控制面板及其内容的详细信息，请参阅：

- 第 55-3 页上的了解控制面板构件
- 第 55-6 页上的了解预定义构件
- 第 55-31 页上的使用控制面板

了解控制面板构件

许可证：任何环境

控制面板有一个或多个选项卡，每个选项卡都会以三列布局显示一个或多个构件。 FireSIGHT 系统配置有许多预定义控制面板构件，每个构件都可以帮助了解 FireSIGHT 系统的不同方面。构件分为三类：

- *分析和报告构件*：显示有关 FireSIGHT 系统收集和生成的事件的数据。
- *其他构件*：不显示事件数据和运营数据。目前，该类别中仅有的一个构件显示 RSS 源。
- *运营构件*：显示有关 FireSIGHT 系统的状态和整体运行状况的信息。

可查看的控制面板小组件取决于正在使用的设备类型和用户角色。此外，每个控制面板都有一组可确定其行为的首选项。您可以将构件最小化和最大化，向选项卡添加和从选项卡移除构件，以及在选项卡上重新排列构件。

注　对于显示某个时间范围内的事件数的构件而言，事件的总数可能无法反映可在事件查看器中查看其详细数据的事件数量。因为系统有时会删掉较旧的事件详情以管理磁盘空间使用情况，所以会发生这种情况。要将事件详情删除的情况降到最少，您可以微调事件日志记录，以只记录对部署最重要的事件。有关详细信息，请参阅第 38-1 页上的记录网络流量中的连接。

有关详情，请参阅：

- 第 55-4 页上的了解构件可用性
- 第 55-6 页上的了解构件首选项
- 第 55-6 页上的了解预定义构件
- 第 55-31 页上的使用控制面板

了解构件可用性

许可证：任何环境

FireSIGHT 系统配置了数个预定义控制面板构件。可以查看的控制面板构件取决于正在使用的设备类型和用户角色。

- *无效*构件指由于您在使用错误的设备类型而导致无法查看的构件。
- *未授权*构件指由于您没有必需的帐户权限而导致无法查看的构件。

例如，所有设备均有 Current Sessions 构件，但是，只有具备管理员帐户权限的用户才可查看，而 Appliance Status 构件则仅在防御中心上对具有管理员、维护人员、安全分析师或安全分析师（只读）帐户权限的用户开放。

虽然您无法向控制面板添加未授权或无效构件，但如果您向控制面板导入了在不同类型的设备上创建的控制面板或由具备不同访问权限的用户创建的控制面板，则该控制面板可能包含未授权或无效的构件。这些构件均会被禁用，并显示错误消息，说明您无法查看它们的原因。

此外，请注意，此类构件不能显示设备不可访问的数据。例如，受管设备无法访问关联事件、入侵事件，发现事件，等等。如果将某个控制面板导入某个包含一个用于显示以上某一种数据的 Custom Analysis 构件的受管设备上，则该构件会显示错误消息。当此类构件超时或出现其他问题时，各个构件也会显示错误消息。

构件的内容会随正在使用的设备类型不同而不同。例如，在防御中心上的 Custom Analysis 构件可能显示发现信息，但是，当您在受管设备上配置 Custom Analysis 构件时，该功能不可用。请注意，您可以点击表格列标题来对以表格格式生成的所有内容进行分类。

您可以删除或最小化未授权和无效的构件，以及不显示数据的构件。请注意，在共享控制面板中对某个构件的修改会对该设备的所有用户适用。有关详细信息，请参阅第 55-38 页上的最小化和最大化构件和第 55-38 页上的删除构件。

下表列出了每台设备能够显示的有效构件。

表 55-2　FirePOWER 设备和控制面板构件可用性

构件	防御中心	任何受管设备
设备信息	是	是
设备状态	是	否
Correlation Events	是	否
Current Interface Status	是	是
Current Sessions	是	是
Custom Analysis	是	否
磁盘使用情况	是	是
Interface Traffic	是	是
Intrusion Events	是	否
Network Compliance	是	否
Product Licensing	是	否
Product Updates	是	是
RSS 源	是	是
系统负载	是	是
系统时间	是	是
White List Events	是	否

下表列出了查看各个构件所需的用户帐户权限。只有具备管理员、维护人员、安全分析师或安全分析师 （只读）权限的用户帐户才能使用控制面板。

自定义角色的用户可能访问构件的任何组合，也可能完全不能，具体取决于其用户角色是否许可。

表 55-3　用户角色和控制面板构件可用性

构件	管理员	Maintenance User	安全分析师	Security Analyst (RO)
设备信息	是	是	是	是
设备状态	是	是	是	否
Correlation Events	是	否	是	是
Current Interface Status	是	是	是	是
Current Sessions	是	否	否	否
Custom Analysis	是	否	是	是
磁盘使用情况	是	是	是	是
Interface Traffic	是	是	是	是
Intrusion Events	是	否	是	是
Network Compliance	是	否	是	是
Product Licensing	是	是	否	否
Product Updates	是	是	否	否

表 55-3　用户角色和控制面板构件可用性 （续）

构件	管理员	Maintenance User	安全分析师	Security Analyst (RO)
RSS 源	是	是	是	是
系统负载	是	是	是	是
系统时间	是	是	是	是
White List Events	是	否	是	是

了解构件首选项

许可证：任何环境

每个构件都有一组可确定其行为的首选项。

构件首选项可以很简单。例如，下图中显示了 Current Interface Status 构件的首选项，该构件显示内部网络中所有已启用接口的当前状态。您只能配置此构件的更新频率。

构件首选项也可以较为复杂。例如，下图显示了 Custom Analysis 构件的首选项，该构件是一个高度可定制的构件，可显示 FireSIGHT 系统所收集及生成的事件的详细信息。

要修改构件的首选项，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　在您想要更改首选项的构件标题栏上，点击显示首选项图标 ( )。

系统将显示该构件的首选项部分。

步骤 2　根据需要进行更改。

更改会立即生效。有关可为各个构件指定的首选项的详细信息，请参阅第 55-6 页上的了解预定义构件。

步骤 3　在构件标题栏上，点击隐藏首选项图标 ( ) 隐藏首选项部分。

了解预定义构件

许可证：任何环境

FireSIGHT 系统配置了多个预定义构件，当用于控制面板时，这些构件可显示当前系统状态的概览，其中包括有关系统收集和生成的事件的数据，以及有关部署中的设备的状态和整体运行状况的信息。

有关 FireSIGHT 系统配置的构件的详细信息，请参阅以下各节：

- 第 55-7 页上的了解 Appliance Information 构件
- 第 55-8 页上的了解 Appliance Status 构件
- 第 55-8 页上的了解 Correlation Events 构件
- 第 55-9 页上的了解 Current interface Status 构件
- 第 55-10 页上的了解 Current Sessions 构件
- 第 55-10 页上的了解 Custom Analysis 构件

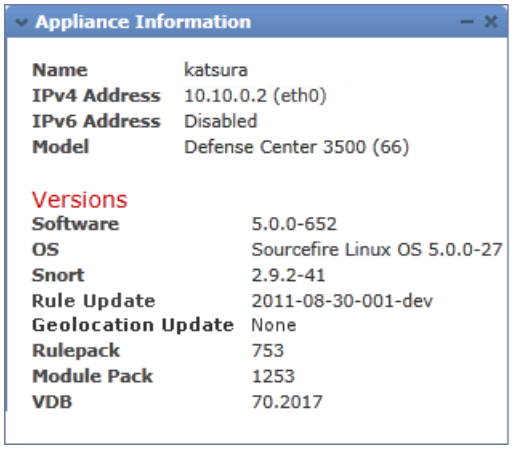
- 第 55-22 页上的了解 Disk Usage 构件
- 第 55-23 页上的了解 Interface Traffic 构件
- 第 55-24 页上的了解 Intrusion Events 构件
- 第 55-26 页上的了解 Network Compliance 构件
- 第 55-27 页上的了解 Product Licensing 构件
- 第 55-28 页上的了解 Product Updates 构件
- 第 55-29 页上的了解 RSS Feed 构件
- 第 55-29 页上的了解 System Load 构件
- 第 55-30 页上的了解 System Time 构件
- 第 55-30 页上的了解 White List Events 构件

注　可以查看的控制面板构件取决于正在使用的设备类型和用户角色。有关详细信息，请参阅第 55-4 页上的了解构件可用性。

了解 Appliance Information 构件

许可证：任何环境

Appliance Information 构件可提供设备的快照。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。



该构件提供：

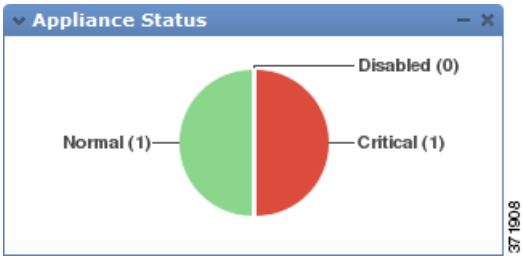
- 设备名称、 IPv4 地址、 IPv6 地址和型号
- 在某个带控制面板的设备上安装的 FireSIGHT 系统软件、操作系统、 Snort、规则更新、规则包、模块包、漏洞数据库 (VDB) 和地理定位更新的版本信息，虚拟防御中心除外。
- 受管设备与管理设备的通信链路的名称和状态
- 高可用性对中的防御中心的名称、型号和防御中心的 FireSIGHT 系统软件和操作系统版本，以及防御中心最近进行联系的信息

通过修改构件首选项以显示简单或高级视图，您可以配置构件显示更多或更少信息；首选项还可控制构件的更新频率。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

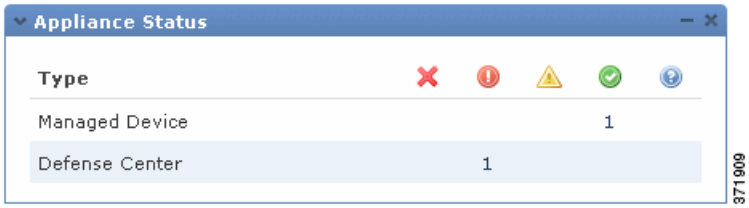
了解 Appliance Status 构件

许可证：任何环境

Appliance Status 构件指示设备及其所管理的任何设备的运行状况。请注意，由于防御中心不会自动将运行状况策略应用于受管设备，您必须将运行状况策略手动应用于设备上，否则设备状态会显示为禁用。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。



通过修改构件首选项，您可以配置构件以饼形图或表格形式显示设备状态。



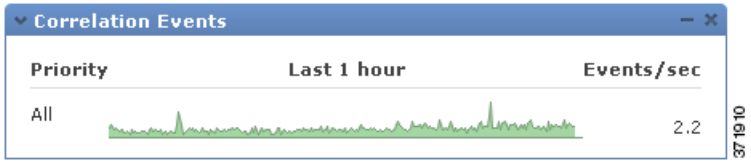
首选项还可控制构件的更新频率。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

您可以点击饼形图上的某个部分或设备状态表的一个数字转到 Health Monitor 页面，并查看设备及其所管理的任何设备的编译后的运行状况状态。有关详细信息，请参阅第 68-37 页上的使用运行状况监视器。

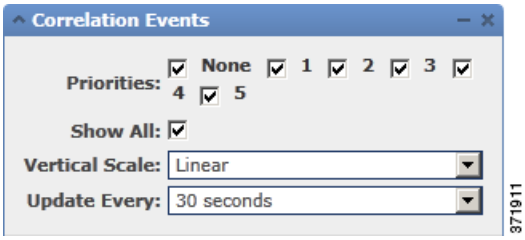
了解 Correlation Events 构件

许可证：FireSIGHT

Correlation Events 构件按照优先级显示控制面板时间范围内每秒发生关联事件的平均次数。默认情况下，该构件在 Detailed Dashboard 的 Correlation 选项卡中显示。



通过修改构件首选项，您可以配置构件以显示不同优先级的关联事件，并选择线性（增量）或对数（十倍）比例。



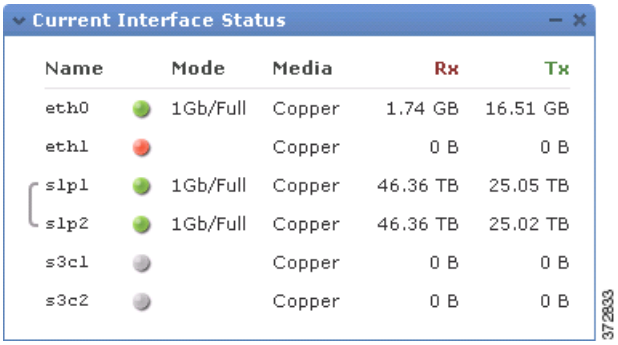
选择一个或多个 **Priorities** 复选框，以分别显示特定优先级事件的图形，包括不具有优先级的事件。选择 **Show All** 以显示所有关联事件的图形，无论其优先级如何。首选项还可控制构件的更新频率。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

您可以点击某个图形查看特定优先级的关联事件，或者点击 **All** 图形查看所有关联事件。在任何一种情况下，事件均受到控制面板时间范围的限制；通过控制面板访问关联事件可更改设备的事件 （或全球）时间段。有关关联事件的详细信息，请参阅第 51-48 页上的查看关联事件。

了解 Current interface Status 构件

许可证：任何环境

Current Interface Status 构件显示设备上已启用或未使用的所有接口的状态。在防御中心上，您可以显示管理 （`eth0`、`eth1`等等）接口。在受管设备上，可以选择仅显示感知 （`s1p1` 等）接口或同时显示管理和感知接口。接口按类型分组：管理、内联、被动、已交换、已路由、已堆栈和未使用。



对于每个接口，该构件都会提供：

- 接口的名称
- 接口的链路状态
- 接口的链路模式 （例如， 100Mb 全双工或 10Mb 半双工）
- 接口类型，例如，铜或光纤
- 接口接收 (Rx) 和发送 (Tx) 的数据量

代表链路状态的球的颜色表示当前状态，如下所示：

- 绿色：链路正在全速运行
- 黄色：链路正在运行，但未达到全速
- 红色：链路未运行

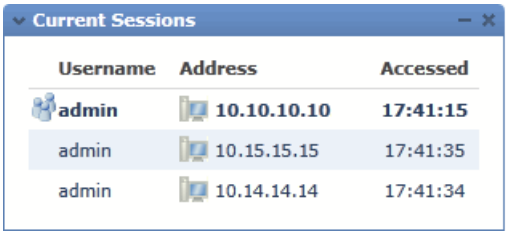
- 灰色：链路被系统管理禁用
- 蓝色：链路状态信息不可用 （例如 ASA）

构件首选项可控制构件的更新频率。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

了解 Current Sessions 构件

许可证：任何环境

Current Sessions 构件显示哪些用户目前已经登录设备、与发起会话的机器相关的 IP 地址，以及各用户最近一次访问设备页面的时间 （基于设备的本地时间）。代表用户，也就是说，当前查看构件的用户，会以用户图标 ( ) 标记并渲染为粗体。在注销或变成不活动状态后一小时内，会话会从构件数据中删除。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。



在 Current Sessions 构件上，您可以：

- 点击任何用户名以管理 User Management 页面上的用户帐户；请参阅第 61-40 页上的管理用户帐户
- 点击任何 IP 地址旁边的主机图标 ( ) 或受影响的主机图标 ( ) 以查看关联机器的主机配置文件；参阅第 49-1 页上的使用主机配置文件 （仅带网络发现的防御中心）
- 点击任何 IP 地址或访问时间以查看该 IP 地址和与该 IP 地址相关的用户登录网路界面的时间所限制的审核日志；参阅第 69-2 页上的查看审计记录

构件首选项可控制构件的更新频率。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

了解 Custom Analysis 构件

许可证：任何环境

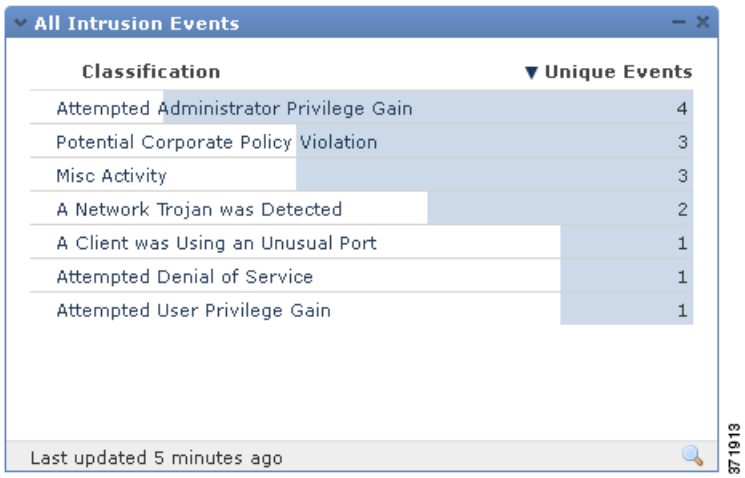
Custom Analysis 构件是一款高度可定制的构件，可用于显示 FireSIGHT 系统收集和生成的事件的详细信息。

Custom Analysis 构件配置多个构件预设，是思科预定义配置组。预设仅为示例，可提供有关部署的快速访问信息。您可以使用这些预设或创建自定义配置。

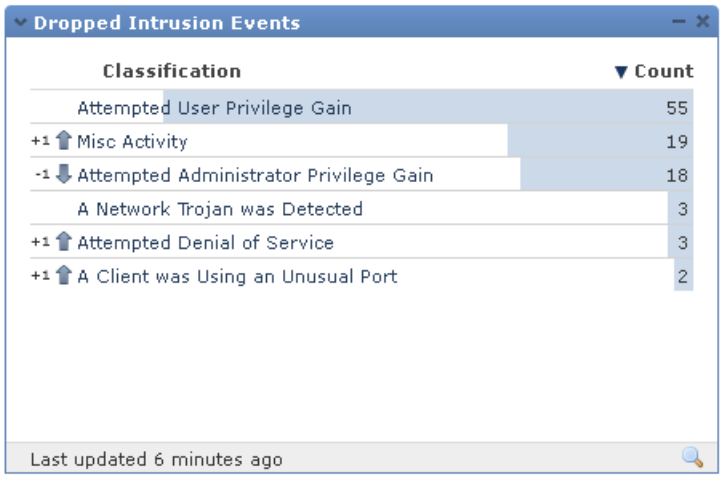
当您配置构件首选项时，您必须选择想要显示的表格和单个字段，以及配置构件对显示数据进行分组的聚合方法。

例如，通过配置构件显示来自**入侵事件**表的数据，您可以配置 Custom Analysis 构件显示最近入侵事件的列表。选择 **Classification** 字段并通过 **Count** 来合计该数据，可以告诉您生成的每种类型的事件的个数。请注意，计数包括经审核的入侵事件；如果您在事件查看器中查看计数，它不会包含经审核的事件。

另外，通过 **Unique Event** 合计可以了解每种类型有多少个入侵事件已经发生 （例如，检测到多少网络木马、可能违反公司政策的情况、试图拒绝服务攻击，等等）。



或者，您还可以使用已保存的搜索 （无论是设备预定义搜索之一还是您创建的自定义搜索）来进一步限制构件。例如，使用 **Dropped Events** 搜索限制第一个示例 （使用 **Classification**，通过 **Count** 合计的入侵事件）可帮助您了解每一种类型中有多少个入侵事件已丢弃。



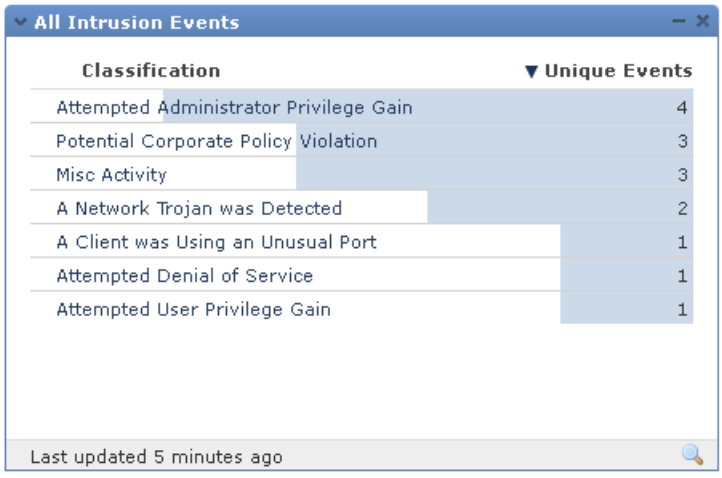
构件背景中的彩色条可显示每个事件发生的次数；您应该从右到左阅读彩色条。您可以更改构件显示的彩色条的颜色和行数。您还可以配置构件显示经常发生的事件或最少发生的事件。

方向图标 (▼) 指示和控制显示的排序顺序。向下指向的图标表示降序；向上的图标表示升序。要更改排序顺序，请点击图标。

在每个事件旁边，构件可以显示三个图标中的其中一个，以显示最近结果中的任何更改：

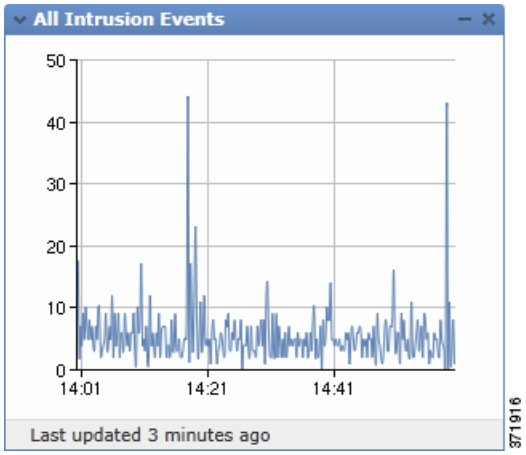
- 新的事件图标 ( ) 表示该事件对结果而言是第一次发生。
- 向上箭头图标 ( ) 表示该事件自上次构件更新以来已经上移。指示事件上移了多少个位置的数字在图标旁边显示。
- 向下箭头图标 ( ) 表示该事件自上次构件更新以来已经下移。指示事件下移了多少个位置的数字在图标旁边显示。

该构件基于设备本地时间显示其最近更新的时间。构件的更新频率取决于控制面板的时间范围。例如，如果您将控制面板时间范围设置为 1 小时，则构件每五分钟更新一次。另一方面，如果将控制面板时间范围设置为一年，则构件每周更新一次。要确定控制面板何时进行下次更新，请将光标停留在构件左下角 **Last updated** 通知处。



注　如果您使用已保存的搜索限制 Custom Analysis 构件，该构件在下一次更新之前不会反映更改。

如果您想了解时间范围内的事件或其他所收集数据的信息，您可以配置 Custom Analysis 构件显示一个线形图，例如显示时间范围内配置中所生成的入侵事件总数的线形图。对于一段时间内的图形而言，您可以选择构件使用的时区和线条的颜色。



最后，您可以选择构件的自定义标题。

在 Custom Analysis 构件中，您可以调用提供构件显示事件的相关详情的事件视图 （即，工作流程）。要做到这一点，请点击要详细了解的事件。

您还可以右击 Custom Analysis 中的任何 IP 地址以显示可让您获得更多有关相关主机上的信息的右键菜单，并将其添加到全球黑名单和白名单上以进行 Security Intelligence 过滤。

注　根据您配置它们的方式，Custom Analysis 构件可能将设备上的资源耗尽；红色的 Custom Analysis 构件表示其使用正在危害系统性能。如果构件继续保持红色，应移除该构件。

有关详细信息，请参阅：

- 第 55-13 页上的配置 Custom Analysis 构件
- 第 55-21 页上的从 Custom Analysis 构件查看关联事件
- 第 55-22 页上的 Custom Analysis 构件限制
- 第 2-4 页上的使用上下文菜单

配置 Custom Analysis 构件

许可证：任何环境

与所有构件一样， Custom Analysis 构件也有可确定其行为的首选项。要配置 Custom Analysis 构件，请按照第 55-6 页上的了解构件首选项所述显示首选项。

根据您是配置构件显示事件的相对发生 （即，条形图），还是配置构件显示一段时间内的图形（即，线形图），所显示的首选项组不同。

要配置构件显示条形图，请从 **Field** 下拉列表选择除 **Time** 之外的所有值。

要配置构件显示线形图，请从 **Field** 下拉列表选择 **Time**。

下表介绍了您可以在 Custom Analysis 构件中设置的不同首选项。

表 55-4　Custom Analysis 构件首选项

使用此首选项…	以控制…
职位	构件的标题。 如果不指定标题，设备会使用已配置的事件类型作为构件标题。
预设	构件的预设。 Custom Analysis 构件配置许多预设，是思科预定义构件配置。预设仅为示例，可提供有关部署的快速访问信息。您可以使用这些预设或创建自定义配置。 有关预设的详细列表，请参阅 Custom Analysis 构件预设表。
表	包含构件显示的事件数据的事件表。
字段	要显示事件类型的特定字段。 **提示**　要显示一段时间内的图形，请选择 **Time**。
聚合	构件的汇聚方法。 汇聚方法配置构件对显示数据的分组方法。对于大多数事件类型而言，默认聚合标准是 **Count**。
过滤	用户定义的应用过滤器，用来进一步限制构件显示的数据。 如果显示来自应用统计数据表或按应用统计的入侵事件统计表的数据，则只能使用过滤器。有关应用过滤器的详细信息，请参阅第 3-13 页上的使用应用过滤器。
搜索	想要用于进一步限制构件显示的数据的已保存搜索。 您必须指定搜索，不过，有些预设使用预定义搜索。 如果您创建了一个使用不带星号 (*) 的字段中的数据的已保存连接事件搜索，则构件会显示不正确的数据。只有限制连接概要的字段可以基于连接事件限制 Custom Analysis 控制面板构件。无效的搜索会呈灰色，且无法选择。
显示	是否要显示最常见事件 （**顶部**）或最不常见的事件 （**底部**）。
成果	想要显示的结果行数。 您可以显示 10 至 25 个结果行，增量为五。
Show Movers	是否要显示表示对最近结果的更改的图标。
时区	想要用来显示结果的时区。 时区会在您选择基于时间的字段时显示。
颜色	显示每个结果的相对数量的构件背景中的彩色条的颜色。

下表介绍了 Custom Analysis 构件可用的预设。它还指出了哪个防御中心预定义控制面板 （如果有）使用了预设。请注意：

- 受管设备上的预定义控制面板不包含 Custom Analysis 构件。
- DC500 防御中心不显示，且2 系列设备和用于 Blue Coat X-系列的思科 NGIPS无法检测其不支持的功能的数据。

有关特定的许可类型的详细信息，请参阅第 65-2 页上的许可证类型和限制。

表 55-5　Custom Analysis 构件预设

预设	说明	预定义控制面板	许可证
所有入侵事件	显示监控网络上控制面板一定时间范围内入侵事件总数的图片。	Detailed Dashboard Summary Dashboard	保护
所有入侵事件 （未丢弃）	按照分类显示最常见的入侵事件类型，其中数据包未作为事件的一部分丢弃。	Detailed Dashboard	保护
按应用划分的允许连接	显示按应用分组的、监控网络上允许的应用连接。	Application Statistics	FireSIGHT
按应用风险划分的允许连接	显示按应用风险级别分组的、监控网络上允许的应用连接。	Application Statistics	FireSIGHT
按业务相关性划分的允许连接	显示按业务活动的预计相关性分组的、监控网络上允许的应用连接。	Application Statistics	FireSIGHT
按 URL 类别划分的允许连接	显示按 URL 类别分组的、监控网络上允许的应用连接。	URL Statistics	URL 过滤
按 URL 信誉划分的允许连接	显示按 URL 信誉分组的、监控网络上允许的应用连接。	URL Statistics	URL 过滤
按用户划分的允许连接	显示按连接用户分组的、监控网络上允许的应用连接。	访问受控用户统计信息	FireSIGHT
引入恶意软件的应用协议	显示按用于传输文件的应用协议分组的、网络上传输的恶意软件文件数。	Files Dashboard	恶意软件
传输文件的应用协议	显示按用于传输文件的应用协议分组的、网络上传输的文件数。	Files Dashboard	保护
引入恶意软件的客户端应用	显示访问或创建了 FireAMP 连接器所检测到的恶意软件的应用，或父文件。	Files Dashboard	FireAMP 订用
传输文件的客户端应用	显示通过网络传输文件的应用，或父文件。	Files Dashboard	保护
客户端	显示按类型划分的监控网络上的客户端。	Detailed Dashboard	FireSIGHT
按应用划分的连接	根据所检测到的连接数量显示监控网络上的应用。	Connection Summary	FireSIGHT
按目标大陆划分的连接	根据连接数显示从监控网络上发送连接的大陆。	Connection Summary	FireSIGHT
按目标国家划分的连接	根据连接数显示从监控网络上发送连接的大陆。	Connection Summary	FireSIGHT
按发起方 IP 划分的连接	根据主机上的 IP 地址发起会话的连接数量显示监控网络上的主机 IP 地址。	Connection Summary	FireSIGHT
按端口划分的连接	根据检测到的连接数量显示监控网络上的端口。	Connection Summary	FireSIGHT
按响应方 IP 划分的连接	根据会话响应方为主机的 IP 地址的连接数量显示监控网络上的主机 IP 地址。该构件的输出根据连接日志配置不同而不同改变。	Connection Summary	FireSIGHT
按安全情报类别划分的连接	显示按安全情报类别分组的、监控网络上的安全情报监控或阻止的所有连接。	Summary Dashboard	保护
按照来源大陆划分的连接	根据每个大陆发起连接的数量显示与监控网络通信的连接。	Connection Summary	FireSIGHT

表 55-5　Custom Analysis 构件预设 （续）

预设	说明	预定义控制面板	许可证
按来源国家划分的连接	根据每个国家发起连接的数量显示与监控网络通信的连接。	Connection Summary	FireSIGHT
按 URL 类别划分的连接	显示按 URL 类别分组的、监控网络上允许的应用连接。	Summary Dashboard	URL 过滤
按 URL 信誉划分的连接	显示按 URL 信誉分组的、监控网络上允许的应用连接。	Summary Dashboard	URL 过滤
随时连接	显示监控网络上控制面板一定时间范围内连接总数的图片。	Connection Summary	FireSIGHT
按应用划分的拒绝连接	显示按应用划分的监控网络上的拒绝应用连接。	Application Statistics	FireSIGHT
按 URL 类别划分的拒绝连接	显示按 URL 类别划分的监控网络上的拒绝连接。	URL Statistics	URL 过滤
按 URL 信誉划分的拒绝连接	显示按 URL 信誉划分的监控网络上的拒绝连接。	URL Statistics	URL 过滤
按用户划分的拒绝连接	显示按连接用户划分的监控网络上的拒绝连接。	访问受控用户统计信息	FireSIGHT
按应用划分的已丢弃事件	显示按应用分组的已丢弃入侵事件	Application Statistics	保护 + FireSIGHT
按用户划分的已丢弃入侵事件	显示按用户分组的已丢弃入侵事件	访问受控用户统计信息	保护 + FireSIGHT
已丢弃入侵事件	显示按分类划分的、数据包已丢弃的入侵事件的数目。	Detailed Dashboard Summary Dashboard	保护
按设备划分的动态分析流量	根据提交给综合安全智能云分析的文件数据的大小显示最活跃的设备。	Files Dashboard	恶意软件
一段时间内流量的动态分析	显示控制面板时间范围内捕获的提交给云端分析的文件数据。	Files Dashboard	恶意软件
文件操作	显示按用于处理文件的文件规则行为分组的网络上传输的文件数。	Files Dashboard	保护或恶意软件
文件类别	显示按文件类别分组的网络上传输的文件数。	Files Dashboard	保护
文件性质	显示按恶意软件性质分组的、 Malware Cloud Lookup 文件规则所导致的网络流量检测到的文件数。	Files Dashboard	恶意软件
文件名	显示按文件名分组的网络上传输的文件数。	Files Dashboard	保护
按设备划分的文件存储	显示存储最多文件数据的设备。	Files Dashboard	恶意软件
按性质划分的文件存储	根据文件性质显示存储于设备上的文件数据大小 （千字节）。	Files Dashboard	恶意软件
按类型划分的文件存储	根据文件类型显示存储于设备上的文件数据大小 （千字节）。	Files Dashboard	恶意软件
一段时间内的文件存储	显示在控制面板时间范围内存储于受管设备上的文件数据 （千字节）图形。	Files Dashboard	恶意软件

表 55-5　Custom Analysis 构件预设 （续）

预设	说明	预定义控制面板	许可证
一段时间内的文件传输	显示控制面板时间范围内系统在网络流量中检测到的文件传输总数图形。	Files Dashboard	保护
文件类型	显示按文件类型分组的网络上传输的文件数。	Files Dashboard	保护
被恶意软件感染的文件类型	显示按文件类型分组的，由系统或 FireAMP 连接器检测到的网络流量中的恶意软件数。	Files Dashboard	恶意软件
为一段时间内的动态分析发送的文件	显示控制面板时间范围内为动态分析提交的文件总数图。	Files Dashboard	恶意软件
一段时间内的存储文件	显示控制面板时间范围内存储于受管设备上的文件总数图。	Files Dashboard	恶意软件
接收文件的主机	显示按 IP 地址分组的网络上的主机 IP 地址收到 （下载）的文件数量。	Files Dashboard	保护
接收恶意软件的主机	显示按 IP 地址分组的网络上的主机 IP 地址收到的恶意软件数量。	Files Dashboard	恶意软件许可证或 FireAMP 订用
发送文件的主机	显示按 IP 地址划分的网络上的主机 IP 地址发送 （上传）的文件数量。	Files Dashboard	保护
发送恶意软件的主机	显示按 IP 地址划分的网络上的主机 IP 地址发送的文件数量。	Files Dashboard	恶意软件
按应用划分的影响 x 事件	显示按应用划分的预计影响级别 x （其中 x 为 0 - 4）的事件数	Application Statistics	保护 + FireSIGHT
按应用协议划分的影响级别 x 事件	显示按应用协议分组的预计影响级别 x （其中 x 为 1 - 2）的事件数	Summary Dashboard	保护 + FireSIGHT
按用户划分的影响级别 x 事件	显示按用户分组的预计影响级别 x （其中 x 为 0 - 4）的事件数	访问受控用户统计信息	保护 + FireSIGHT
按主机划分的危害表现	显示按关联的主机 IP 地址分组的已触发危害表现数。	Summary Dashboard	FireSIGHT
要求分析的入侵事件	根据事件分类显示要求分析的入侵事件数。	Detailed Dashboard	保护 + FireSIGHT
按目标大陆划分的入侵事件	根据与每个大陆相关的事件数量显示入侵事件针对的大陆。	Summary Dashboard	FireSIGHT
按目标国家划分的入侵事件	根据与每个国家相关的事件数量显示入侵事件针对的国家。	Summary Dashboard	FireSIGHT
按来源大陆划分的入侵事件	根据于各个大陆发起的事件数显示入侵事件产生的大陆。	Summary Dashboard	FireSIGHT
按来源国家划分的入侵事件	根据于各个国家发起的事件数显示入侵事件产生的国家。	Summary Dashboard	FireSIGHT
对高重要性主机的入侵事件	根据发生在高重要性主机的入侵事件数显示入侵事件。	Detailed Dashboard	保护 + FireSIGHT
恶意软件入侵	根据发生于传输恶意软件的连接中入侵事件数显示入侵事件。	Files Dashboard	恶意软件

表 55-5　Custom Analysis 构件预设 （续）

预设	说明	预定义控制面板	许可证
恶意软件威胁数	显示按威胁类型分组的，由系统或 FireAMP 连接器检测到的网络流量中的恶意软件数。	Files Dashboard	恶意软件许可证或 FireAMP 订用
一段时间内的新危害表现	显示控制面板时间范围内检测到的新危害表现图形。	Summary Dashboard	FireSIGHT
操作系统	根据网络中运行每个操作系统的主机数量显示操作系统。	Detailed Dashboard	FireSIGHT
可能的零日恶意软件	根据文件被发现的次数显示捕获的最可能是零日恶意软件，并具备未知的文件性质，以及高或极高威胁评分的文件。	Files Dashboard	恶意软件
引入恶意软件的进程	显示访问或创建了 FireAMP 连接器所检测到的恶意软件的系统进程。	Files Dashboard	恶意软件许可证或 FireAMP 订用
低业务相关性的风险应用	显示监控网络中应用风险级别高而预计业务相关性低的所有应用连接。	Summary Dashboard	FireSIGHT
服务器	显示按工具数量划分的服务器。	Detailed Dashboard	FireSIGHT
SSL 行为	根据频率显示加密流量上采取的 SSL 规则行为数。	Connection Summary	任何环境
SSL 证书状态	根据频率显示系统在 SSL 加密会话中检测到的证书状态数。	Connection Summary	任何环境
SSL 解密失败原因	根据频率显示不正确解密 SSL 加密会话的系统原因数。	Connection Summary	任何环境
随着时间推移而解密的 SSL 会话	显示控制面板时间范围内系统解密的 SSL 加密会话数量图形。	Connection Summary	任何环境
未随着时间推移而解密的 SSL 会话	显示控制面板时间范围内系统未解密的 SSL 加密会话数量图形。	Connection Summary	任何环境
随着时间的推移而发生错误的 SSL 会话	显示控制面板时间范围内系统检测到的包含内部错误的 SSL 加密会话数量图形。	Connection Summary	任何环境
随着时间推移而发生的威胁检测	显示控制面板时间范围内系统或 FireAMP 连接器在网络流量中检测到的恶意软件威胁总数图形。	Files Dashboard	恶意软件许可证或 FireAMP 订用
主要攻击者	根据所列出的 IP 地址为与导致入侵事件相关的攻击者的入侵事件数显示监控网络上的攻击主机 IP 地址。	Summary Dashboard	保护
发现的主要客户端应用	根据客户端应用传输的数据总千字节数显示监控网络上的客户端应用。	Summary Dashboard	FireSIGHT
发现的主要操作系统	根据带该操作系统的网络主机数显示监控网络上的操作系统。	Summary Dashboard	FireSIGHT
发现的主要服务器应用	根据运行服务的主机数量显示监控网络上的服务器应用。	Summary Dashboard	FireSIGHT
主要目标	根据地址被定位为与导致入侵事件相关的入侵事件数显示监控网络上的主机 IP 地址。	Summary Dashboard	保护

表 55-5　Custom Analysis 构件预设 （续）

预设	说明	预定义控制面板	许可证
主要威胁	根据所存储的威胁评分相同的文件数显示威胁评分分布。	Files Dashboard	恶意软件
发现的主要网络应用	根据客户端应用传输的数据总千字节数显示监控网络上的网络应用。	Summary Dashboard	FireSIGHT
按应用划分的总事件	根据应用所产生的入侵事件数显示监控网络上的应用。	Application Statistics	保护 + FireSIGHT
按应用协议划分的总事件	根据与应用协议相关的入侵事件数显示监控网络上的应用协议。	Summary Dashboard	保护 + FireSIGHT
按用户划分的总事件	根据各用户活动所产生的入侵事件数显示监控网络上的用户。	Summary Dashboard 访问受控用户统计信息	保护 + FireSIGHT
按应用划分的流量	根据控制面板时间范围内应用在监控网络上传输的数据总千字节数显示监控网络上的应用。	Application Statistics Connection Summary Detailed Dashboard	FireSIGHT
按应用类别划分的流量	根据控制面板时间范围内各类别应用在监控网络上传输的数据总千字节数显示监控网络上的应用类别。	Application Statistics Summary Dashboard	FireSIGHT
按应用风险划分的流量	根据控制面板时间范围内各级别应用在监控网络上传输的数据总千字节数显示监控网络上的预计应用风险级别。	Summary Dashboard	FireSIGHT
按业务相关性划分的流量	根据控制面板时间范围内各级别应用在监控网络上传输的数据总千字节数显示监控网络上的预计应用业务相关性。	Summary Dashboard	FireSIGHT
按目标大陆划分的流量	根据控制面板时间范围内各大陆在监控网络上传输的数据总千字节数显示从监控网络上联系的大陆。	Connection Summary	FireSIGHT
按目标国家划分的流量	根据控制面板时间范围内各国家在监控网络上传输的数据总千字节数显示从监控网络上联系的国家。	Connection Summary	FireSIGHT
按发起方 IP 划分的流量	根据控制面板时间范围内监控网络上从某个 IP 地址传输的数据总千字节数显示监控网络上的主机 IP 地址。	Connection Summary Detailed Dashboard	FireSIGHT
按发起方用户划分的流量	根据用户登录的主机接收的数据总千字节数显示监控网络上的用户。	Detailed Dashboard Summary Dashboard	FireSIGHT
按端口划分的流量	根据控制面板时间范围内各端口在监控网络上传输的数据总千字节数显示监控网络上的响应方端口。该构件的输出根据连接日志配置不同而不同改变。	Connection Summary	FireSIGHT
按响应方 IP 划分的流量	根据控制面板时间范围内 （主机上的） IP 地址收到的数据总千字节数显示监控网络上的 IP 地址。该构件的输出根据连接日志配置不同而不同改变。	Connection Summary Detailed Dashboard	FireSIGHT

表 55-5　　Custom Analysis 构件预设 （续）

预设	说明	预定义控制面板	许可证
按安全情报类别划分的流量	根据控制面板时间范围内各类连接上传输的数据总千字节数显示监控网络上的安全情报类别。	Summary Dashboard	保护
按来源大陆划分的流量	根据控制面板时间范围内各大陆在监控网络上传输的数据总千字节数显示向监控网络传输数据的大陆。	Connection Summary	FireSIGHT
按来源国家划分的流量	根据控制面板时间范围内各国家在监控网络上传输的数据总千字节数显示向监控网络传输数据的国家。	Connection Summary	FireSIGHT
按 URL 类别划分的流量	根据控制面板时间范围内与各类 URL 交换的数据总千字节数显示监控网络上的应用 URL 类别。	URL Statistics	URL 过滤
按 URL 信誉划分的流量	根据控制面板时间范围内与各种信誉的 URL 交换的数据总千字节数显示监控网络上的应用 URL 信誉类型。	URL Statistics	URL 过滤
按用户划分的流量	根据控制面板时间范围内各用户交换的数据总千字节数显示监控网络上的用户。	无	FireSIGHT
一段时间内的流量	显示控制面板一定时间范围内在监控网络上传输的数据总千字节数的图片。	Connection Summary Detailed Dashboard	FireSIGHT
一段时间内的单独应用	显示控制面板一定时间范围内在监控网络上检测到的总单独应用的图片。	Application Statistics Summary Dashboard	FireSIGHT
一段时间内的单独用户	显示控制面板一定时间范围内在监控网络上检测到的总单独用户的图片。	访问受控用户统计信息	FireSIGHT
受恶意软件影响的用户	显示按用户分组的，由系统或 FireAMP 连接器检测到的网络流量中的威胁数。	Files Dashboard	恶意软件+ FireSIGHT或 FireAMP 订用
传输文件的用户	显示按发送者划分的网络上所传输的文件数。	Files Dashboard	恶意软件 + FireSIGHT
引入恶意软件的网络应用	显示访问或创建 FireAMP 连接器检测到的恶意软件的监控网络上的网络应用。	Files Dashboard	恶意软件许可证或 FireAMP 订用
传输文件的网络应用	显示按用于传输文件的网络应用划分的网络上所传输的文件数。	Files Dashboard	恶意软件许可证或 FireAMP 订用
White List Violations	显示按违规数划分的存在白名单违规的主机。	Detailed Dashboard	FireSIGHT

从 Custom Analysis 构件查看关联事件

许可证：任何环境

根据 Custom Analysis 构件配置显示的数据类型，您可以调用提供构件中显示的事件相关的详细信息的事件视图 （即，工作流程）。

在调用控制面板中的事件视图时，事件会在该事件类型的默认工作流程中显示，并受到控制面板时间范围的限制。这还会改变设备的适当时间段，具体取决于配置的时间段的数量和想要查看的事件的类型。

例如，如果您在防御中心上配置了多个时间段，然后从 Custom Analysis 构件上访问运行状况事件，那么事件即会在默认运行状况事件工作流程中显示，且运行状况监控时间段会变为控制面板时间范围。

又例如，如果您配置一个时间窗后访问 Custom Analysis 构件的任意类型的事件，该事件会在该事件类型的默认工作流程显示，且全球时间段会变为控制面板时间范围。

有关时间段的详细信息，请参阅第 71-5 页上的默认时间段和第 60-5 页上的在搜索中指定时间约束。

要查看 Custom Analysis 构件的关联事件，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　您有两个选项，具体取决于您配置构件的方法：

- 在配置用于显示事件的相对发生 （即，条形图）的构件上，点击任何事件以查看构件首选项以及该事件所限制的相关事件。您也可以点击构件右下角的查看所有图标 ( ) 查看所有相关事件 （受到构件首选项限制）。
- 在配置用于显示一段时间内连接数据的构件上，点击构件右下角的查看所有图标查看所有相关事件 （受到构件首选项限制）。

有关使用特定事件类型的详细信息，请参阅：

- 第 3-4 页上的使用安全情报列表和源
- 第 69-2 页上的查看审计记录
- 第 41-7 页上的查看入侵事件
- 第 50-13 页上的查看发现和主机输入事件
- 第 40-7 页上的查看文件事件
- 第 40-16 页上的查看恶意软件事件
- 第 40-26 页上的查看捕获的文件
- 第 50-17 页上的查看主机
- 第 50-24 页上的查看主机属性
- 第 50-28 页上的查看危害表现
- 第 50-32 页上的查看服务器
- 第 50-40 页上的查看应用详情
- 第 50-44 页上的查看漏洞
- 第 50-48 页上的查看第三方漏洞
- 第 39-12 页上的查看连接和安全情报数据
- 第 50-53 页上的查看用户
- 第 50-58 页上的查看用户活动事件

- 第 51-48 页上的查看关联事件
- 第 52-26 页上的查看白名单事件
- 第 52-31 页上的查看白名单违规事件
- 第 68-44 页上的查看运行状况事件
- 第 66-19 页上的查看规则更新日志
- 第 47-17 页上的处理主动扫描结果
- 第 58-17 页上的使用地理定位
- 第 59-1 页上的了解自定义表

Custom Analysis 构件限制

许可证：任何环境

当使用 Custom Analysis 构件时，需要记住几个要点。

如果您在共享控制面板中配置构件，请记住并非所有用户都可以查看所有事件类型的数据，具体取决于用户帐户权限。例如，维护人员无法查看发现事件。

同样，如果您使用从另一设备导入的控制面板，请记住并非所有设备都有权访问所有事件类型的数据。例如，受管设备不能存储相关性数据。如果控制面板包括某个显示您看不到的数据的 Custom Analysis 构件，表明您无权查看该数据。但是，请注意，您 （以及共享控制面板的任何其他用户）可以修改构件的首选项以显示您可以看到的数据，或者甚至是删除构件。如果您希望确保不发生这种情况，请将控制面板另存为专用控制面板。

切记只有您才能访问另存为专用的搜索。如果您在共享控制面板上配置构件，并限制其事件显示专用搜索，则构件会重置为当其他用户登录时不使用搜索。这也会影响构件视图。如果您希望确保不发生这种情况，请将控制面板另存为专用控制面板。

您可在系统策略的 Dashboard 设置中启用或禁用 Custom Analysis 构件。有关详细信息，请参阅第 63-13 页上的配置控制面板设置。

了解 Disk Usage 构件

许可证：任何环境

根据磁盘使用类别， Disk Usage 构件显示硬盘驱动器的空间使用比例。它还会显示设备硬盘驱动器上的空间使用比例及其每个分区的容量。 Disk Usage 构件如果被安装在设备中，或者如果防御中心管理某个包含恶意软件包的设备，则其会显示相同的恶意软件存储包信息。默认情况下，该构件在 Default Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

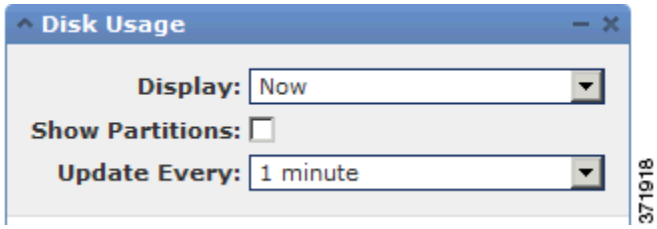
By Category 堆积条形图显示每个磁盘使用情况类别在使用的总可用磁盘空间中的比例。下表列出了可用的类别。

表 55-6　　磁盘使用情况类别

磁盘使用情况类别	说明
活动	系统记录的所有事件
文件	系统存储的所有文件
备用	所有备份文件
更新	与更新相关的所有文件，例如规则更新和系统更新
其他	系统故障排除文件和其他文件
免费	设备上剩余的可用空间

您可以将指针悬停在 By Category 堆积条形图中的磁盘使用情况类别上，以查看该类别使用的可用磁盘空间的比例、磁盘上的实际存储空间，以及该类别的总可用磁盘空间。请注意，如果您安装了一个恶意软件存储包，Files 类别的总可用磁盘空间为恶意软件包上的可用磁盘空间。有关详细信息，请参阅第 40-3 页上的了解捕获文件存储。

如果您安装了恶意软件存储包，您可以通过修改构件首选项配置构件仅显示 By Category 堆积条形图和管理员 (`/`)、`/Volume`、`/boot`分区使用情况，以及`/var/storage`分区。



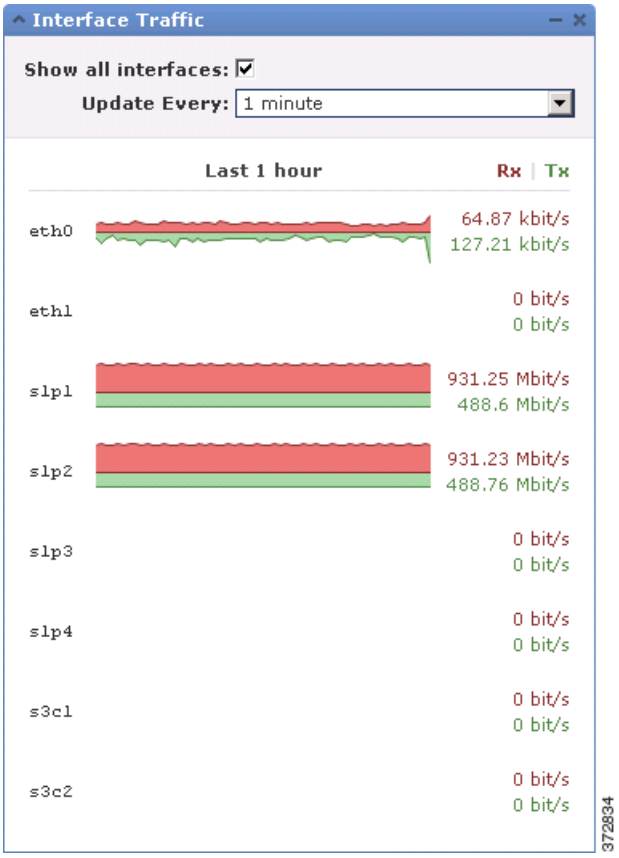
构件首选项还可以控制构件的更新频率，及其显示的是当前磁盘使用情况还是控制面板时间范围内收集的磁盘使用情况统计数据。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

了解 Interface Traffic 构件

许可证：任何环境

Interface Traffic 构件显示在控制面板时间范围内设备的管理 （`eth0` 等）和感知 （`s1p1` 等）接口上接收 (Rx) 和传输 (Tx) 的流量的速率。默认情况下，该构件不会在任何预定义控制面板上显示。

出站 （已传输）流量包括流量控制数据包。因此，您的设备上的被动接口可能显示已传输流量并生成事件；这是预期行为。另请注意，启用了恶意软件许可证的设备会定期尝试连接到思科云，即使未配置动态分析亦如此。因此，这些设备会显示已传输流量；这也是预期行为。

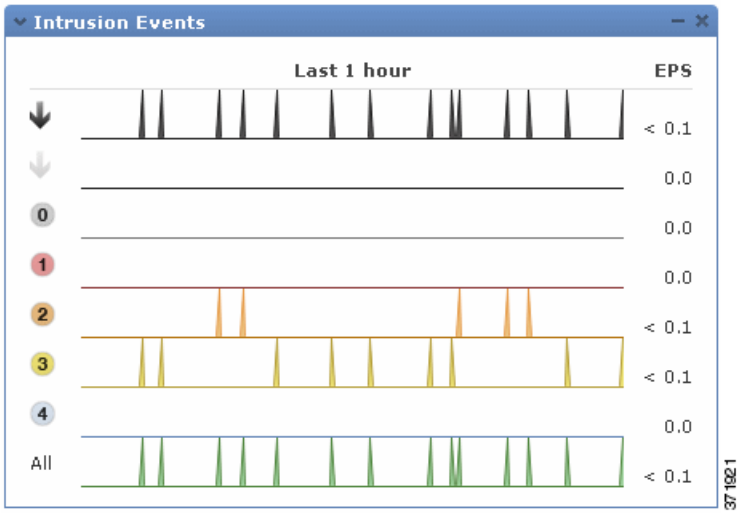


构件首选项可控制构件的更新频率。在受管设备上，首选项还可控制构件是否显示未使用的接口上的流量速率 （默认情况下，该构件只会显示活动接口的流量速率）。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

了解 Intrusion Events 构件

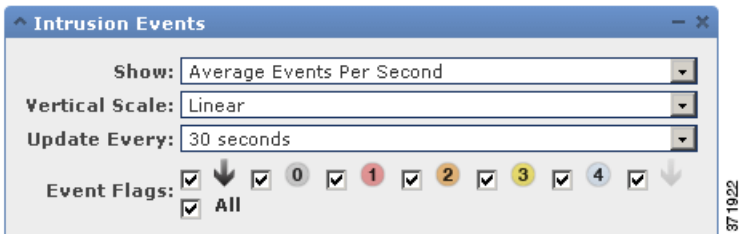
许可证：保护

Intrusion Events 构件可显示发生在控制面板时间范围内的入侵事件 （按优先级组织）。这包括有丢弃数据包和不同影响的入侵事件的统计数据。默认情况下，该构件在 Summary Dashboard 的 Intrusion Events 选项卡中显示。



在受管设备上，该构件可以显示丢弃（或者，在被动部署的设备上，则为已丢弃）入侵事件、所有入侵事件或两者皆显示。请注意，您必须启用本地事件存储，否则构件不会显示任何数据。还请注意，**All** 代表的总速率不包括已丢弃的事件速率。

在防御中心上，而非受管设备上，您可以修改构件首选项配置构件显示了已丢弃的入侵事件/可能已经丢弃的数据包以及不同影响。您可以在防御中心和设备上显示已丢弃和可能已丢弃的事件。下图显示了构件首选项的防御中心版本。



在构件首选项中，您可以：

- 在防御中心，选择一个或多个 **Event Flags** 复选框以显示已丢弃数据包、可能已丢弃数据包，或特定影响的独立图表；无论是影响还是规则状态，请选择 **All** 显示所有入侵事件的其他图形；有关详细信息，请参阅第 41-32 页上的使用影响级别评估事件。
- 选择 **Show** 显示 **Average Events Per Second** 或 **Total Events**
- 选择 **Vertical Scale** 以选择 **Linear**（增量）或 **Logarithmic**（十倍）比例

首选项还可控制构件的更新频率。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

在 Intrusion Events 构件上，您可以：

- 在防御中心 上，点击与已丢弃数据包、可能已丢弃数据包或特定影响相对应的图形以查看该类型的入侵事件
- 点击对应于已丢弃事件的图形查看已丢弃事件
- 点击与可能已丢弃事件相对应的图形以查看可能已丢弃事件
- 点击 **All** 图形查看所有入侵事件

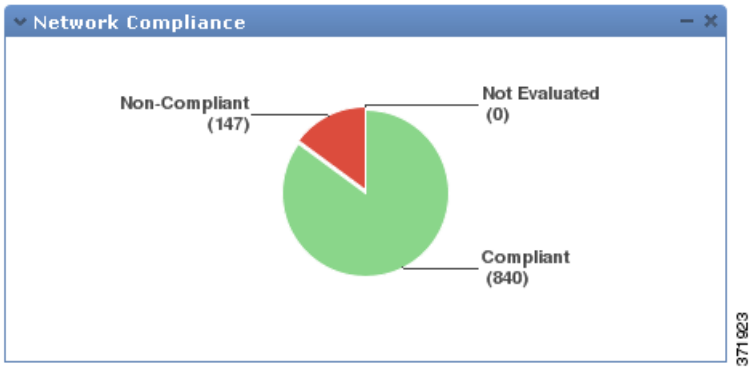
请注意，所发生的事件视图受到控制面板时间范围的限制；通过控制面板访问入侵事件可能更改设备的事件（或全球）时间段。有关入侵事件的详细信息，请参阅第 41-7 页上的查看入侵事件。

另请注意，被动部署的数据包不会丢弃，无论规则状态或入侵策略的串接丢包行为如何。

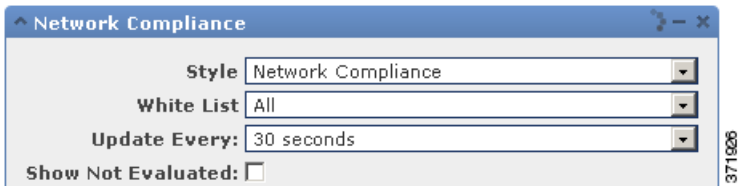
了解 Network Compliance 构件

许可证：FireSIGHT

Network Compliance 构件总结主机符合您配置的白名单的情况 （请参阅第 52-1 页上的将 FireSIGHT 系统用作一个合规工具）。默认情况下，该构件会显示有关活跃关联策略中的所有合规白名单列出的合规、不合规，以及未评估的主机数量的饼形图。默认情况下，该构件在 Detailed Dashboard 的 Correlation 选项卡中显示。



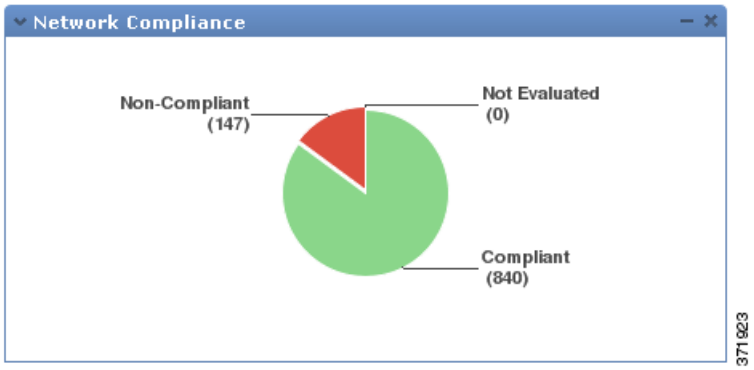
您可以通过修改构件首选项配置构件显示所有白名单或具体白名单的合规性。



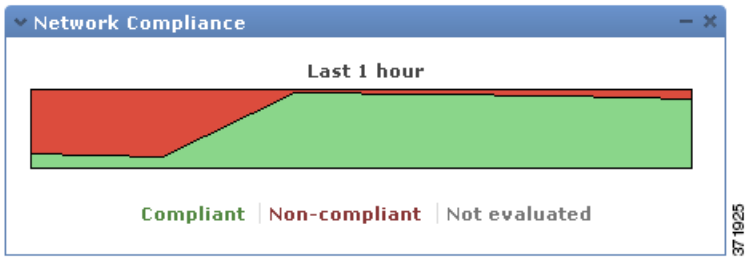
如果您选择显示所有白名单的网络合规性，而一旦其不符合某个有效的关联策略中的任何白名单，则构件会将主机视为不合规。

您还可以使用构件首选项以指定您想使用三种不同风格中的哪一种来显示网络合规性。

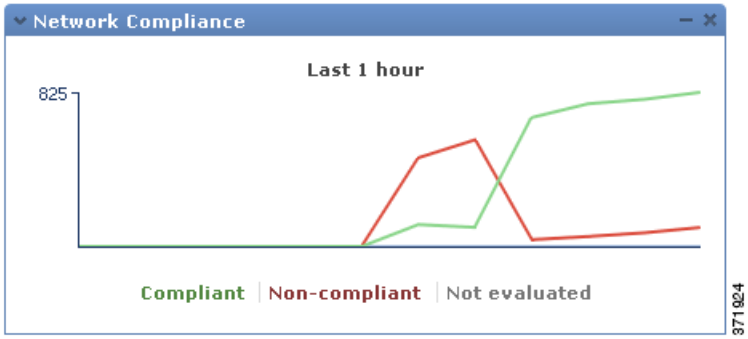
Network Compliance 风格 （默认）显示有关合规、不合规及尚未评估的主机数量的饼形图。您可以点击该饼形图以查看主机违规数，它会列出至少违反一个白名单的主机。有关详细信息，请参阅第 52-31 页上的查看白名单违规事件。



Network Compliance over Time (%) 风格会显示有关控制面板时间范围内合规，不合规，未评估的主机相对比例的堆积区域图。



Network Compliance over Time 风格会显示有关控制面板时间范围内合规，不合规，未评估的主机数量的线形图。

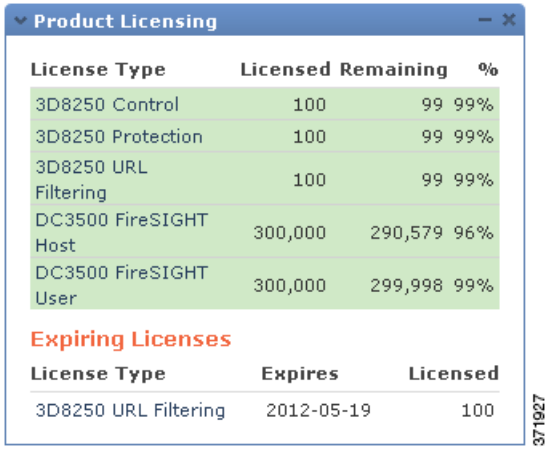


首选项可控制构件的更新频率。您可以选中 **Show Not Evaluated** 框以隐藏未评估的活动。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

了解 Product Licensing 构件

许可证：任何环境

Product Licensing 构件可显示当前安装于防御中心上的设备和功能许可证。它还可显示获得许可证的项目 （例如，主机或用户）数量及允许保留许可证的项目数量。默认情况下，该构件不会在任何预定义控制面板上显示。



构件的顶部显示在防御中心上安装的所有设备和功能许可证，包括临时许可证，而 Expiring Licenses 部分则显示临时及已到期许可证。例如，如果您有两张 FireSIGHT 功能许可证，其中一张是永久许可证，支持 750 台主机，另一张为临时许可证，支持另外 750 台主机，则构件的顶部可显示带 1500 台许可主机的 FireSIGHT 主机功能许可证，而 Expiring Licenses 部分则显示带 750 台主机的 FireSIGHT 主机功能许可证。

构件背景中的长条显示正在使用的各种许可证的比例；您应该从右到左阅读这些长条。已到期许可证标标记有一条删除线。

您可以通过修改构件首选项配置构件显示所有当前许可的功能，或者您可许可的所有功能。首选项还可控制构件的更新频率。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

您可以点击任何一种许可证类型发往本地配置的 License 页面并添加或删除功能许可证。有关详细信息，请参阅第 65-1 页上的许可 FireSIGHT 系统。

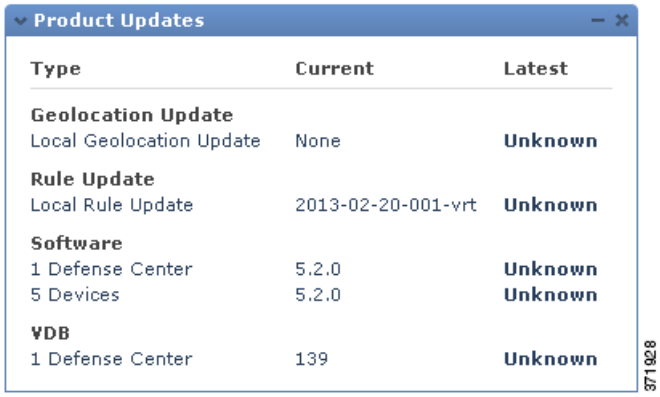
了解 Product Updates 构件

许可证：任何环境

Product Updates 构件为您提供当前安装在设备上的软件 （FireSIGHT 系统软件和规则更新）和您已经下载但未安装的可用更新的信息摘要。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

请注意，除非您已经配置定期下载、推送或安装软件更新的任务，否则构件会在软件最新版本一项显示 `Unknown`；该构件会使用定期任务确定最新版本。有关详细信息，请参阅第 62-1 页上的安排任务。

该构件还可使您了解您可以更新软件的网页链接；防御中心版本的构件会为您提供类似的链路，这样您就可以在受管设备上更新软件。



通过修改构件首选项，您可以配置构件以隐藏最新版本。首选项还可控制构件的更新频率。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

在 Product Updates 构件，您可以：

- 点击 FireSIGHT 系统软件的当前版本、规则更新、地理定位更新或 VDB 手动更新设备：
- 要更新系统软件、地理定位数据库或 VDB，请参阅第 66-1 页上的更新系统软件。
- 要导入最新的规则更新，请参阅第 66-13 页上的导入规则更新和本地规则文件。
- 点击最新版本或 Latest 列中的 **Unknown** 链接，创建一个预定任务，以下载 FireSIGHT 系统软件的最新版本、规则更新或 VDB；请参阅第 62-1 页上的安排任务。

了解 RSS Feed 构件

许可证：任何环境

RSS Feed 构件可向控制面板添加一个 RSS 源。默认情况下，该构件可显示思科安全新闻的信息源。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

您还可以配置构件显示公司新闻的预配置摘要、Snort.org 博客，或漏洞研究团队 (VRT) 博客，或者您也可以指定其在构件首选项的 URL 以创建任何其他 RSS 源的自定义连接。

信息源每 24 小时 （但您可以手动更新摘要）更新一次，而且，构件会根据设备的本地时间显示最近一次更新信息源的时间。请记住，设备必须访问 （两个预配置摘要的）网站或您配置的任何自定义信息源。

当您配置构件时，您还可以选择您想要在构件中显示多少个案例，以及是否想要在标题下显示案例说明；记住，并非所有的 RSS 源都会使用说明。

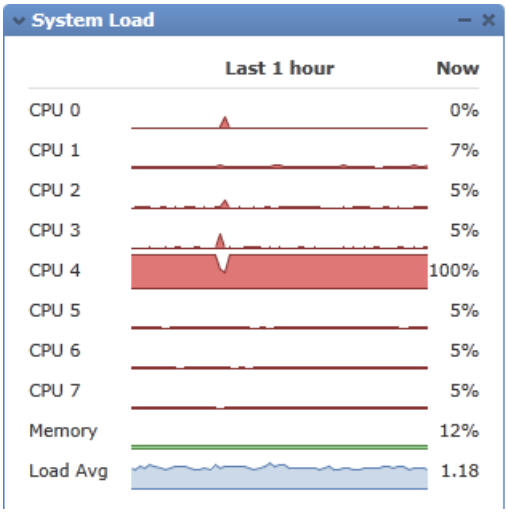
在 RSS Feed 构件中，您可以：

- 点击信息源中的某个案例查看案例
- 点击 **more** 链接转到信息源的网站
- 点击更新图标 ( ) 手动更新信息源

了解 System Load 构件

许可证：任何环境

System Load 构件可显示设备当前及控制面板时间范围内的 （每个 CPU） CPU 使用率、内存 (RAM) 使用情况和系统负载 （又称为平均负载，通过等待运行的进程数量衡量）。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

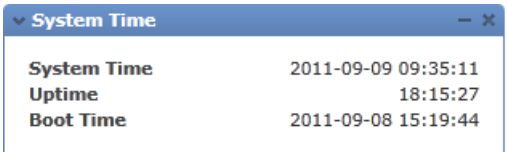


您可以通过修改构件首选项以配置构件显示或隐藏平均负载。首选项还可控制构件的更新频率。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

了解 System Time 构件

许可证：任何环境

System Time 构件可显示本地系统时间、正常运行时间和设备启动时间。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

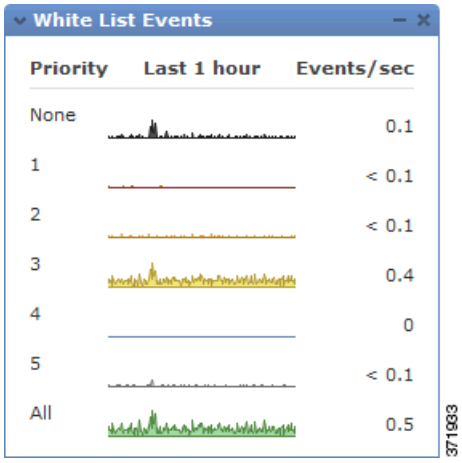


通过修改构件首选项，您可以配置构件以隐藏启动时间。首选项还会控制构件与设备的时钟同步的频率。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

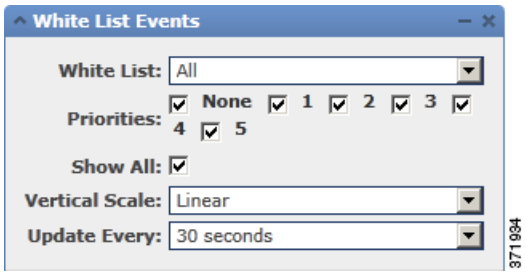
了解 White List Events 构件

许可证：FireSIGHT

White List Events 构件按照优先级显示控制面板时间范围内每秒内事件发生的平均次数。默认情况下，该构件在 Default Dashboard 的 Correlation 选项卡中显示。



通过修改构件首选项，您可以配置构件以显示不同优先级的白名单事件。



在构件首选项中，您可以：

- 选择一个或多个 **Priorities** 复选框显示特定优先级事件的图形，包括不具备优先级的事件。
- 选择 **Show All** 以显示所有白名单事件的其他图形，无论其优先级如何。
- 选择 **Vertical Scale** 以选择 **Linear** （增量）或 **Logarithmic** （十倍）比例

首选项还可控制构件的更新频率。有关详细信息，请参阅第 55-6 页上的了解构件首选项。

您可以点击某个图形查看特定优先级的白名单事件，或者点击 **All** 图形查看所有白名单事件。在任何一种情况下，事件均受到控制面板时间范围的限制；通过控制面板访问关联事件可更改防御中心的事件 （或全球）时间段。有关白名单事件的详细信息，请参阅第 52-26 页上的查看白名单事件。

使用控制面板

许可证：任何环境

您可以查看和修改显示在控制面板中的构件。

您可在 Dashboard Management 页面管理控制面板 （请参阅第 55-33 页上的查看控制面板）。您可以创建、查看、修改、导出和删除控制面板。

对于每个控制面板而言，页面都会显示所有者 （即，创建它的用户）以及该控制面板是否为专用控制面板。请注意，除非您拥有管理员权限，否则您将只能看到自己的专用控制面板；您将无法查看或修改其他用户创建的专用控制面板。

最后，页面会指示哪个控制面板为默认控制面板。您可在用户首选项中指定默认控制面板；有关详细信息，请参阅第 71-7 页上的指定默认控制面板。

有关使用控制面板的详细信息，请参阅：

- 第 55-32 页上的创建自定义控制面板
- 第 55-33 页上的查看控制面板
- 第 55-35 页上的修改控制面板
- 第 55-39 页上的删除控制面板
- 第 A-1 页上的导出配置

创建自定义控制面板

许可证：任何环境

当您创建新的控制面板时，您可以选择是否以任何现有控制面板作为基础，是由用户创建还是由思科预先确定。这可以复制预先存在的控制面板；您可以修改此复件以满足您自身的需求。或者，您也可以选择不以任何预先存在的控制面板作为基础来创建一个空白的新控制面板。

您还必须指定 （或禁用）选项卡更改和页面刷新时间间隔。这些设置可通过选项卡确定控制面板循环的频率，以及整个控制面板页面刷新的频率。

刷新整个控制面板可以让您查看自上一次控制面板更新以来，其他用户对共享控制面板所作的，或者您对另一台计算机上的专用控制面板所作的任何首选项或布局更改。这可能非常有用，例如，在控制面板始终显示的网络运营中心 (NOC) 中。如果想要对控制面板作出更改，您可以在本地计算机进行更改。然后，NOC 中的控制面板会自动刷新您指定和显示您更改的时间间隔，而无需您手动刷新 NOC 中的控制面板。请注意，您不需要更新整个控制面板以查看数据更新；各个构件会根据其首选项进行更新。

最后，您还可以通过将新的控制面板保存为专用控制面板来将新的控制面板与用户帐户相关联。如果您选择不保存控制面板为专用控制面板，则设备的所有其他用户都可以查看它。

请记住，因为并非所有用户角色都有权访问所有控制面板构件，查看权限较高的用户创建的控制面板的权限较低的用户可能无法使用控制面板上的所有构件。尽管未授权的构件仍将在控制面板上显示，但它们会被禁用。

您还应该记住，任何具有控制面板访问权限的用户，无论角色如何，都可以修改共享控制面板。如果您希望确保只有您可以修改特定控制面板，请将其保存为专用控制面板。

提示　您无需创建新的控制面板，而是可以从其他设备中导出，然后将其导入到设备中。随后，您将可以编辑所导入的控制面板以满足自身需求。请注意，您可以查看的控制面板构件取决于使用的设备类型和用户角色；例如，在防御中心上创建并导入至受管设备的控制面板可能显示一些无效、已禁用的构件。有关详细信息，请参阅第 A-1 页上的导入和导出配置。

要创建新的控制面板，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　选择 **Overview > Dashboards > Management**。

系统将显示 Dashboard Management 页面。

步骤 2　点击 **Create Dashboard**。

系统将显示 Create Dashboard 页面。

步骤 3　使用 **Copy Dashboard** 下拉列表选择要作为新控制面板的基础的控制面板。

您可以选择任何预定义或用户定义的控制面板。或者，选择 **None** （默认）创建一个空白控制面板。

步骤 4　键入控制面板的名称以及可选说明。

步骤 5　在 **Change Tabs Every** 字段，指定控制面板应更改选项卡的频率 （单位：分钟）。

除非您暂停控制面板或控制面板上只有一个选项卡，否则该设置会在您指定的时间间隔将视图转至下一个选项卡。要禁用选项卡循环，请输入 0 到 **Change Tabs Every** 字段中。

步骤 6　在 **Refresh Page Every** 字段中，指定当前的控制面板选项卡应该使用新数据刷新的频率 （单位：分钟）。该值必须高于 **Change Tabs Every** 设置。

除非您暂停控制面板，否则该设置将在您指定的时间间隔刷新整个控制面板。要禁用定期页面刷新，请输入 0 到 **Refresh Page Every** 字段中。

请注意，该设置独立于许多个别构件的可用更新时间间隔；虽然刷新控制面板页面会重置单个构件的更新时间间隔，但构件会根据其各自的首选项进行更新，即便是您禁用了 **Refresh Page Every**设 置。

步骤 7　或者，选择 **Save As Private** 复选框以将控制面板与您的用户帐户相关联，并防止其他用户查看和修改控制面板。

步骤 8　点击**保存 (Save)**。

控制面板在网络界面创建和显示。您现在可以通过添加选项卡和构件对其进行自定义以满足自身需求 （如果您在某个预先存在的控制面板上以其为基础，可通过重新排列和删除构件进行自定义）。有关详细信息，请参阅第 55-35 页上的修改控制面板。

查看控制面板

许可证：任何环境

默认情况下，设备的主页会显示默认控制面板。如果您没有确定默认控制面板，主页会显示 Dashboard Management 页面，您可以在此选择控制面板视图。在任何时候，要查看您已为设备配置的默认控制面板，您都可以选择 **Overview > Dashboards**；要查看所有可用控制面板的详情，请选择 **Overview > Dashboards > Management**。

提示　您可以配置设备显示不同的默认主页，包括不是控制面板页的页面。您还可以更改默认控制面板。有关详细信息，请参阅第 71-2 页上的指定主页和第 71-7 页上的指定默认控制面板。

每个控制面板上有限制其构件的时间范围。您可以更改时间范围以反映短至前一小时 （默认），或长至前一年的时间周期信息。当您更改时间范围时，可按时间限制构件自动更新以反映新的时间范围。

请注意，并非所有的构件都可受时间限制。例如，控制面板时间范围对 Appliance Information 构件无影响，该构件可提供包括设备名称、型号和 FireSIGHT 系统当前版本的信息。

请记住，对于 FireSIGHT 系统的企业部署而言，更改时间范围至长周期可能对 Custom Analysis 之类的构件无效，取决于新事件取代旧事件的频率。

您还可以暂停控制面板，这可以让您检查构件提供的数据，而无需更改和中断您的分析的显示。暂停控制面板具有以下影响：

- 各个构件停止更新，任何 **Update Every** 构件均如此。
- 控制面板选项卡停止循环，无论控制面板属性中的 **Cycle Tabs Every** 设置如何。
- 控制面板页面停止刷新，无论控制面板属性中的 **Refresh Page Every** 设置如何。
- 更改时间范围无效。

当您完成分析时，您可以取消控制面板暂停。恢复控制面板运行会使得页面上的所有相应的构件更新以反映当前时间范围。此外，控制面板选项卡会恢复循环，控制面板页面会根据您在控制面板属性中指定的设置进行刷新。

如果出现中断控制面板系统信息流的连接问题或其他问题，控制面板会自动暂停，并显示错误通知，直至问题解决为止。

注　您的会话一般会在 1 小时 （或其他配置的时间间隔）的非活动期后注销，无论控制面板是否暂停。如果您计划长时间被动监控控制面板，您可考虑使某些用户免于会话超时，或更改系统超时设置。有关详细信息，请参阅第 61-44 页上的管理用户登录设置和第 63-26 页上的配置用户界面设置。

要查看控制面板，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　选择 **Overview > Dashboards**。您有两个选项，具体取决于您是否定义了默认控制面板：

- 如果您已定义默认控制面板，系统将显示该控制面板。要查看不同的控制面板，请使用 **Overview > Dashboards** 菜单。
- 如果您没有定义默认控制面板，系统将显示 Dashboard Management 页面。点击您要查看的控制面板旁边的 **View**。

系统将显示您选择的控制面板。

要更改控制面板时间范围，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　从 **Show the Last** 下拉列表中，选择控制面板时间范围。

除非控制面板暂停，页面上的所有适当构件都会更新，以反映新的时间范围。

要暂停控制面板，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　在时间范围控件上，点击暂停图标 (❚❚)。

控制面板会暂停，直至您取消暂停。

要取消控制面板暂停，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　在暂停控制面板的时间范围控制面板上，点击播放图标 (▶)。

控制面板会取消暂停。

修改控制面板

许可证：任何环境

一个控制面板有一个或多个选项卡。您可以添加、删除和重命名选项卡。请注意，您不能更改控制面板选项卡的顺序。

每个选项卡都可以三列布局显示一个或多个构件。您可以将构件最小化和最大化，向选项卡添加和从选项卡移除构件，以及在选项卡上重新排列构件。

您也可以更改基本控制面板属性，包括其名称和说明、选项卡周期和页面刷新间隔，以及是否希望与其他用户共享控制面板。

请注意，有控制面板访问权限的任何用户，无论角色如何，都可以修改共享控制面板。如果您希望确保只有您可以修改特定控制面板，请确保在控制面板属性中将其设置为专用控制面板。

在所有思科预定义控制面板中的 Custom Analysis 配置都与该构件的预设相对应。如果您更改或删除了其中一个构件，您可以通过根据适当的预设创建一个新的 Custom Analysis 来恢复它。有关详细信息，请参阅：

提示 在所有思科预定义控制面板中的 Custom Analysis 配置都与该构件的系统预设相对应。如果您更改或删除了其中一个构件，您可以通过根据适当的预设创建一个新的 Custom Analysis 来恢复它。有关详细信息，请参阅第 55-13 页上的配置 Custom Analysis 构件。

有关详细信息，请参阅：

- 第 55-35 页上的更改控制面板属性
- 第 55-36 页上的添加选项卡
- 第 55-36 页上的删除选项卡
- 第 55-37 页上的重命名选项卡
- 第 55-37 页上的添加构件
- 第 55-38 页上的重新排列构件
- 第 55-38 页上的最小化和最大化构件
- 第 55-38 页上的删除构件

更改控制面板属性

许可证：任何环境

执行下列操作步骤以更改基本控制面板属性，包括其名称和说明、选项卡周期和页面刷新间隔，以及是否希望与其他用户共享控制面板。

要更改控制面板的属性，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1 选择 **Overview > Dashboards > Management**。

系统将显示 Dashboard Management 页面。

步骤 2 点击您想要改变的控制面板旁边的编辑图标 ( )。

系统将显示 Edit Dashboard 页面。有关可更改的各种配置的信息，请参阅第 55-32 页上的创建自定义控制面板。

步骤 3　根据需要做出更改，然后点击 **Save**。

控制面板更改成功。

添加选项卡

许可证：任何环境

执行下列操作步骤以添加选项卡到控制面板。

要添加选项卡到控制面板中，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　查看您想要添加选项卡的控制面板。

有关详细信息，请参阅第 55-33 页上的查看控制面板。

步骤 2　在现有选项卡右侧，点击添加选项卡图标 (+)。

系统将显示一个弹出窗口，提示您命名选项卡。

步骤 3　键入一个选项卡名称（最多 25 个字符）并点击 **OK**，或直接点击 **OK** 接受默认名称。请注意，您可随时重命名选项卡；请参阅第 55-37 页上的重命名选项卡。

新的选项卡会被添加。您现在可以添加构件到新的选项卡中。有关详细信息，请参阅第 55-37 页上的添加构件。

删除选项卡

许可证：任何环境

执行下列操作步骤以删除控制面板选项卡及其所有构件。您无法从控制面板中删除最后一个选项卡；每个控制面板必须至少有一个选项卡。

要从控制面板中删除一个选项卡，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　查看您想要删除选项卡的控制面板。

有关详细信息，请参阅第 55-33 页上的查看控制面板。

步骤 2　选中要删除的选项卡，点击删除图标 (×)。

步骤 3　确认要删除选项卡。

选项卡会被删除。

重命名选项卡

许可证：任何环境

执行下列操作步骤以重命名控制面板选项卡。

要重命名选项卡，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1 查看您想要重命名选项卡的控制面板。

有关详细信息，请参阅第 55-33 页上的查看控制面板。

步骤 2 点击要重命名的选项卡。

步骤 3 点击选项卡标题。

系统将显示一个弹出窗口，提示您重命名选项卡。

步骤 4 键入一个选项卡名称 （最多 25 个字符），并点击 **OK**。

选项卡会被重命名。

添加构件

许可证：任何环境

要添加一个构件到控制面板中，您必须首先确定要添加构件到哪个选项卡中。当您将一个构件添加到选项卡后，设备会自动将其添加到构件最少的一列。如果所有列的构件数量均相同，新的构件会被添加到最左边的一列。您最多可以添加 15 个构件到控制面板选项卡中。

提示 在添加构件后，您可以将其移到选项卡的任何位置。但是，您不能在选项卡之间移动构件。有关详细信息，请参阅第 55-38 页上的重新排列构件。

要添加构件到控制面板中，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1 查看您想要添加构件的控制面板。

有关详细信息，请参阅第 55-33 页上的查看控制面板。

步骤 2 选择要添加构件的选项卡。

步骤 3 点击 **Add Widgets**。

系统将显示 Add Widgets 页面。

可以查看的构件取决于正在使用的设备类型和用户角色。构件根据其功能分为：分析和报告、其他和操作性构件。您可以点击类别名称查看每个类别的构件，或点击 **All Categories** 查看所有构件。

步骤 4 点击您想要添加的构件旁边的 **Add**。

提示 要添加多个相同类型的构件 （例如，您可能希望添加多个 RSS Feed 构件，或多个 Custom Analysis 构件），可再次点击 **Add**。

构件会被立即添加到控制面板中。 Add Widgets 页面会显示每种类型有多少个构件在选项卡上，包括您刚刚添加的构件。

步骤 5　或者，当您完成添加构件时，点击 **Done** 返回控制面板。

系统将再次显示您已添加构件的选项卡，以反映您所作的改变。

重新排列构件

许可证：任何环境

您可以更改任何构件在选项卡上的位置。但请注意，您不能在选项卡之间移动构件。如果您想要构件显示在不同的选项卡上，您必须将其从现有选项卡中删除，并将其添加到新的选项卡上。

要移动构件，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　点击您想要移动的标题栏，然后将其拖到新位置。

最小化和最大化构件

许可证：任何环境

您可以将构件最小化以简化视图，然后在想再次看到时将其最大化。

要最小化构件，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　在构件标题栏上点击最小化图标 (−)。

要最大化构件，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　在最小化后的构件标题栏上点击最大化图标 (□)。

删除构件

许可证：任何环境

如果您不想再在选项卡上看到某个构件，可将其删除。

要删除构件，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　在构件的标题栏上点击关闭图标 (✖)。

步骤 2　确认要删除构件。

构件会从选项卡上删除。

删除控制面板

许可证：任何环境

如果不再需要使用某个控制面板，可将其删除。

如果您删除了默认控制面板，您必须定义一个新的默认控制面板，否则设备会在您每次查看控制面板时要求您选择一个控制面板。有关详细信息，请参阅第 71-7 页上的指定默认控制面板。

要删除控制面板，请执行以下操作：

访问：管理员/任何安全分析师/维护人员

步骤 1　选择 **Overview > Dashboards > Management**。

系统将显示 Dashboard Management 页面。

步骤 2　点击要删除的控制面板旁边的删除图标 ( )。

步骤 3　确认要删除控制面板。

控制面板会被删除。

第 56 章

使用 Context Explorer

FireSIGHT 系统Context Explorer 在上下文中显示有关受监控网络状态的详细、交互图形信息，包括有关应用、应用统计、连接、地理定位、危害表现、入侵事件、主机、服务器、安全情报、用户、文件 （包括恶意软件文件）和相关 URL 的数据。不同部分以生动的曲线图、条形图、饼状图和环状图方式显示这些数据，附有详细列表。

可轻松创建和应用自定义过滤器以微调分析，此外，还可更详细地查看各数据部分，只需点击图形区域或将光标悬停在图形区域上方。还可配置资源管理器的时间范围，以反映短至前一小时或长至上一年的时间段。只有具备管理员、安全分析师或安全分析师 （只读）用户角色的用户才能访问 Context Explorer。

FireSIGHT 系统 控制面板可自定义、分区且可实时更新。相反，Context Explorer 需手动更新，以便为其数据提供更广泛的上下文，而且拥有单一且一致的布局，以供活跃用户浏览。

可根据自己的特定需求使用控制面板监控网络上的实时活动和设备。相反，可用 Context Explorer 在特别详细和清晰的上下文中调查预定义的一组最新 FireSIGHT 数据：例如，如果注意到网络中只有 15% 的主机在使用 Linux，但却占据了几乎所有的 YouTube 流量，则可快速应用过滤器查看仅适合 Linux 主机的数据和/或 YouTube 关联的应用数据。与紧凑、狭小的控制面板构件不同， Context Explorer 部分旨在以对 FireSIGHT 系统专家和普通用户均有效的格式醒目再现的系统活动。

请注意，显示的数据取决于多个因素，例如，如何许可和部署受管设备，是否配置提供数据的功能，以及在使用 2 系列设备和 用于 Blue Coat X-系列的思科 NGIPS的情况下设备是否支持数据提供功能。例如， DC500 防御中心和 2 系列设备或用于 Blue Coat X-系列的思科 NGIPS均不支持高级恶意软件防护，因此， DC500 防御中心无法显示这些数据，而且 2 系列设备和用于 Blue Coat X-系列的思科 NGIPS也检测不到这些数据。

下表概述了控制面板与 Context Explorer 之间的一些主要差异。

表 56-1 对比：控制面板与 Context Explorer

特性	控制面板	情景管理器
可显示数据	FireSIGHT 系统的所有监控对象	应用、应用统计、地理定位、危害表现、入侵事件、文件 （包括恶意软件文件）、主机、安全情报事件、服务器、用户和 URL
可自定义性	• 控制面板构件的选择可自定义 • 可按不同程度自定义各个构件	• 不能改变基本布局 • 应用的过滤器显示在资源管理器 URL 中且可标上书签供以后使用
数据更新频率	自动 （默认）；用户配置的	手动
数据过滤	可用于某些构件 （必须编辑构件首选项）	可用于资源管理器的所有部分，可支持多个过滤器

表 56-1　对比：控制面板与 Context Explorer （续）

特性	控制面板	情景管理器
图形上下文	某些构件 （特别是 Custom Analysis）可以图形方式显示数据	所有数据的广泛图形上下文，包括特别详细的环状图
链接到相关网络界面页面	在某些构件中	在每个部分
已显示数据的时间范围	用户配置	用户配置

有关 FireSIGHT 系统控制面板的详细信息，请参阅第 55-1 页上的使用控制面板。

了解 Context Explorer

许可证：FireSIGHT

Context Explorer 包括多个不同的部分，它们共同完整概述有关受监控网络的 FireSIGHT 数据。第一部分是随着时间推移的流量和事件计数曲线图，提供网络活动的最新趋势一览图。

其他部分是交互图形和列表集合，提供有关危害表现、网络、应用、安全情报、入侵、文件、地理定位和 URL 数据的更详细信息。除了流量和事件时间图形，可查看或隐藏任何部分。也可用过滤器限制所有部分中显示的数据；有关详细信息，请参阅第 56-39 页上的使用 Context Explorer 中的过滤器。

有关 Context Explorer 各部分中内容和功能的详细信息，请参阅：

- 第 56-3 页上的了解“流量和入侵事件计数时间”图形
- 第 56-3 页上的了解“危害表现”部分
- 第 56-5 页上的了解“网络信息”部分
- 第 56-11 页上的了解“应用信息”部分
- 第 56-15 页上的了解“安全情报”部分
- 第 56-17 页上的了解“入侵信息”部分
- 第 56-24 页上的了解“文件信息”部分
- 第 56-30 页上的了解“地理定位信息”部分
- 第 56-33 页上的了解“URL 信息”部分

有关如何整体配置 Context Explorer 的信息，请参阅：

- 第 56-36 页上的刷新 Context Explorer
- 第 56-37 页上的设置 Context Explorer 的时间范围
- 第 56-37 页上的 Context Explorer 部分最小化和最大化
- 第 56-38 页上的向下钻取 Context Explorer 数据

有关配置和使用 Context Explorer 过滤器的信息，请参阅：

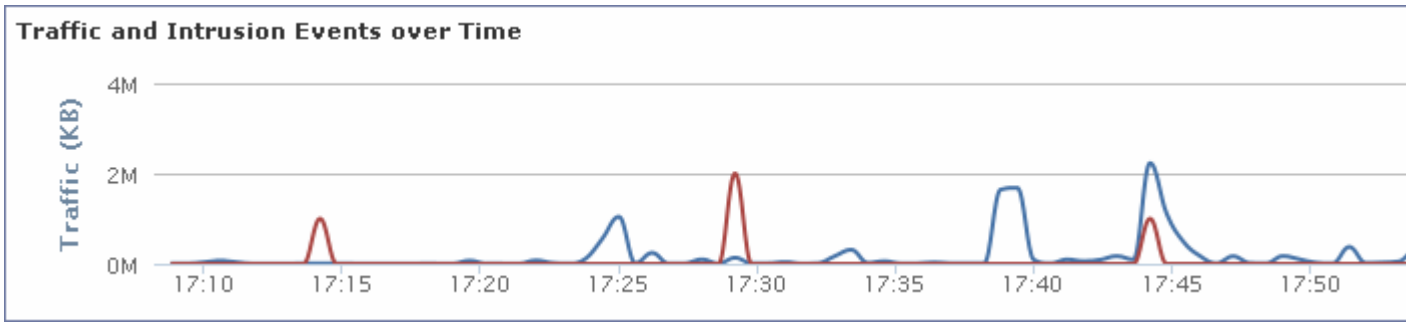
- 第 56-39 页上的使用 Context Explorer 中的过滤器
- 第 56-39 页上的添加和应用过滤器
- 第 56-42 页上的用上下文菜单创建过滤器
- 第 56-43 页上的用书签标示过滤器

了解“流量和入侵事件计数时间”图形

许可证：FireSIGHT

Context Explorer 顶部有一个随时间推移的流量和入侵事件曲线图。X 轴标绘时间间隔（从五分钟到一个月不等，取决于选定的时窗）。 Y 轴以千字节标绘流量 （蓝线）和入侵事件计数 （红线）。

请注意，最小的 X 轴间隔为五分钟。为满足此要求，系统将在选定的时间范围内将起点和终点四舍五入至最近的五分钟间隔。



在默认情况下，此部分显示选定时间范围内的所有网络流量和所有生成的入侵事件。如果应用过滤器，该图表会转而仅显示与过滤器中指定条件相关联的流量和入侵事件。例如，过滤 `Windows` 的 **OS Name** 导致时间图形仅显示与使用 Windows 操作系统的主机相关联的流量和事件。

如用 Context Explorer 过滤入侵事件数据 （例如高**优先级**），蓝色流量曲线将隐藏，以便单独突出入侵事件。

将鼠标指针悬停在图形线条的任何点上方，即可查看有关流量和事件计数的确切信息。将鼠标指针悬停在其中一个彩色线条上方，也可将该线条拖至图形前沿，提供更清晰的上下文。

此部分主要从“入侵事件”和“连接事件”表提取数据。

了解“危害表现”部分

许可证：FireSIGHT

Context Explorer 的“危害表现 (IOC)”部分包含两个交互部分，提供受监控网络上可能受损主机的全局视图：已触发最常用 IOC 类型的比例视图，以及按已触发指示数量显示的主机视图。

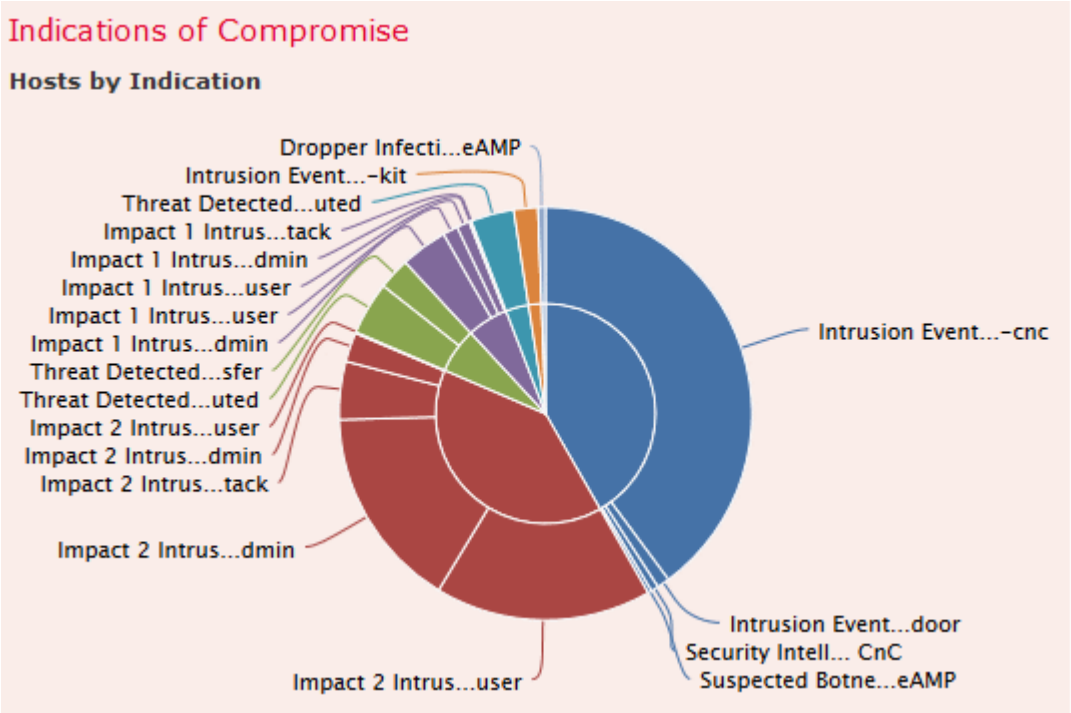
有关“危害表现”部分中图形的详细信息，请参阅：

- 第 56-4 页上的查看“按指示划分的主机”图形
- 第 56-4 页上的查看“按主机划分的指示”图形

查看“按指示划分的主机”图形

许可证：FireSIGHT

“按指示划分的主机”图形以环状图形式显示受监控网络中主机触发的危害表现 (IOC) 的比例视图。内环按 IOC 类别划分的（例如，`CnC Connected` 或 `Malware Detected`），同时，外环进一步按特定事件类型划分数据（例如，`Impact 2 Intrusion Event - attempted-admin` 或 `Threat Detected in File Transfer`）。



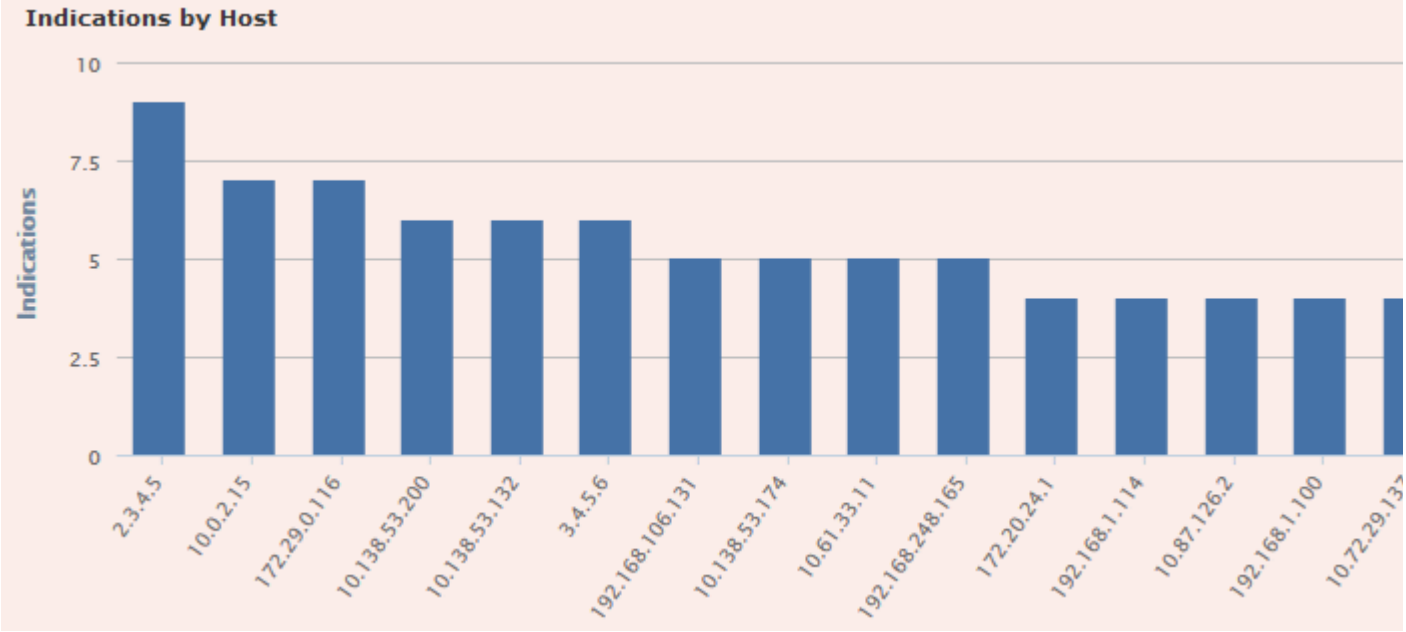
将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

此图形主要从“主机”和“危害表现”表提取数据。

查看“按主机划分的指示”图形

许可证：FireSIGHT

“按主机划分的指示”图形以条形图形式显示受监控网络中 15 个 IOC 最活跃的主机触发的独特危害表现 (IOC) 的计数。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

此图形主要从“主机”和“危害表现”表提取数据。

了解“网络信息”部分

许可证：FireSIGHT

Context Explorer 的 Network Information 部分包含六个交互图形，这六个交互图显示受监控网络中连接流量的全局视图：源、目标、用户、与流量关联的安全区域、网络主机使用的操作系统故障细分，以及 FireSIGHT 系统 对网络流量执行的访问控制措施的比例视图。

有关 Network Information 部分中图形的详细信息，请参阅：

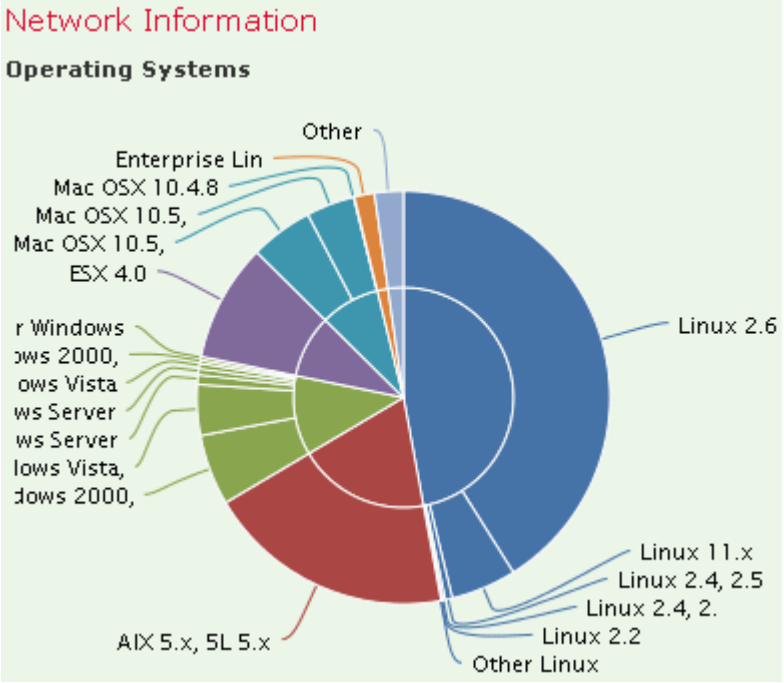
- 第 56-5 页上的查看“操作系统”图形
- 第 56-7 页上的查看“按源 IP 划分的流量”图形
- 第 56-8 页上的查看“按源用户划分的流量”图形
- 第 56-9 页上的 查看“按访问控制措施划分的连接”图形
- 第 56-10 页上的查看“按目标 IP 划分的流量”图形
- 第 56-10 页上的查看“按入口/出口安全区域划分的流量”图形

查看“操作系统”图形

许可证：FireSIGHT

“操作系统”图形以环状图形式显示在受监控网络中主机上检测到的操作系统的比例再现。内环按 OS 名称划分 （例如， `Windows` 或 `Linux`），而外环按特定操作系统版本进一步划分该数据 （例如，`Windows Server 2008` 或 `Linux 11.x`）。一些密切相关的操作系统（例如，Windows 2000、Windows XP 和 Windows Server 2003）组合在一起。非常罕见或无法识别的操作系统在 **Other** 下分组。

请注意，无论日期和时间限制如何，此图形均反映所有可用数据。如果更改资源管理器的时间范围，图形不变。



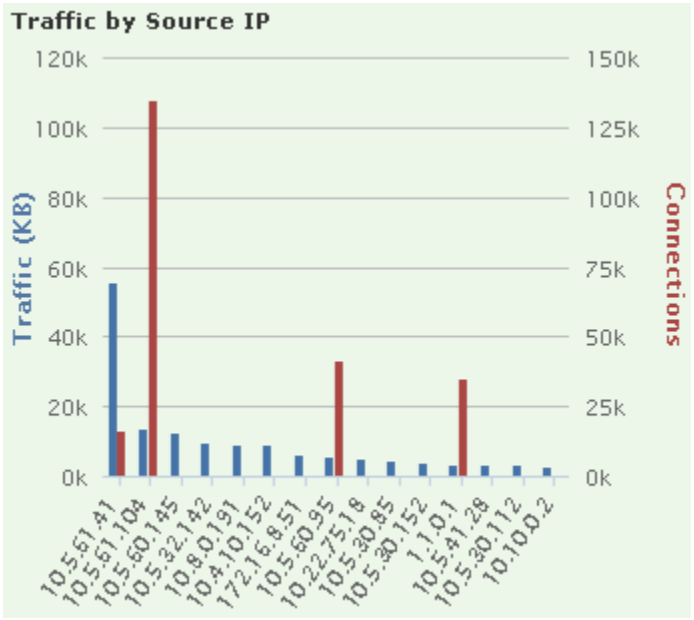
将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

此图形主要从“主机”表提取数据。

查看“按源 IP 划分的流量”图形

许可证：FireSIGHT

“按源 IP 划分的流量”图形以条形图形式显示受监控网络中前 15 个最活跃源 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个源 IP 地址，蓝条代表流量数据，红条代表连接数据。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

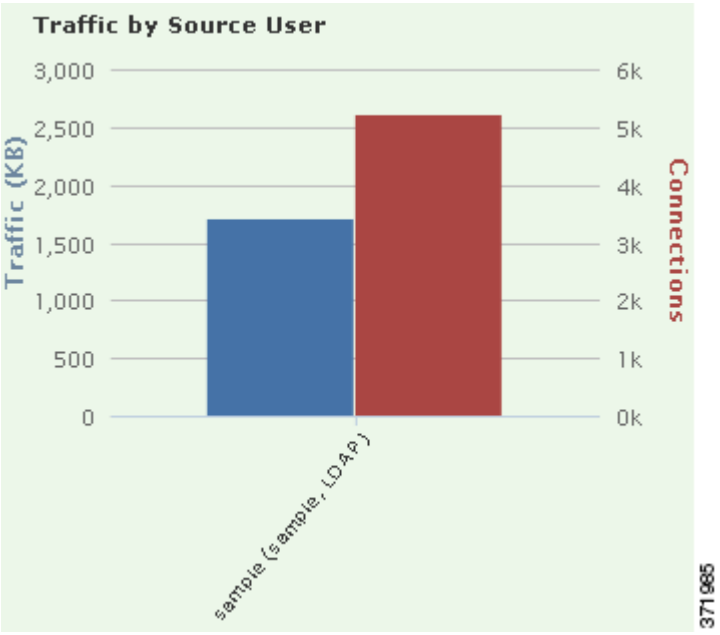
注　如果过滤入侵事件信息，“按源 IP 划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

查看“按源用户划分的流量”图形

许可证：FireSIGHT

“按源用户划分的流量”图形以条形图形式显示受监控网络中前 15 个最活跃源用户的网络流量（千字节每秒）和独特连接的计数。对于列出的每个源 IP 地址，蓝条代表流量数据，红条代表连接数据。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

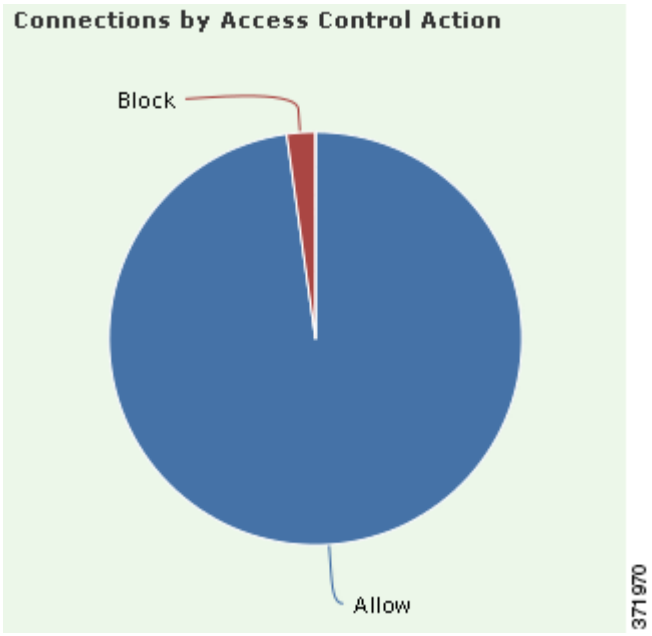
注　如果过滤入侵事件信息，“按源用户划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。请注意，此图形仅显示 User Agent 报告的用户。

查看“按访问控制措施划分的连接”图形

许可证：FireSIGHT

“按访问控制措施划分的连接”图形以饼状图形式显示 FireSIGHT 系统部署已对受监控流量采取的访问控制措施 （例如， `Block` 或 `Allow`）的比例视图。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

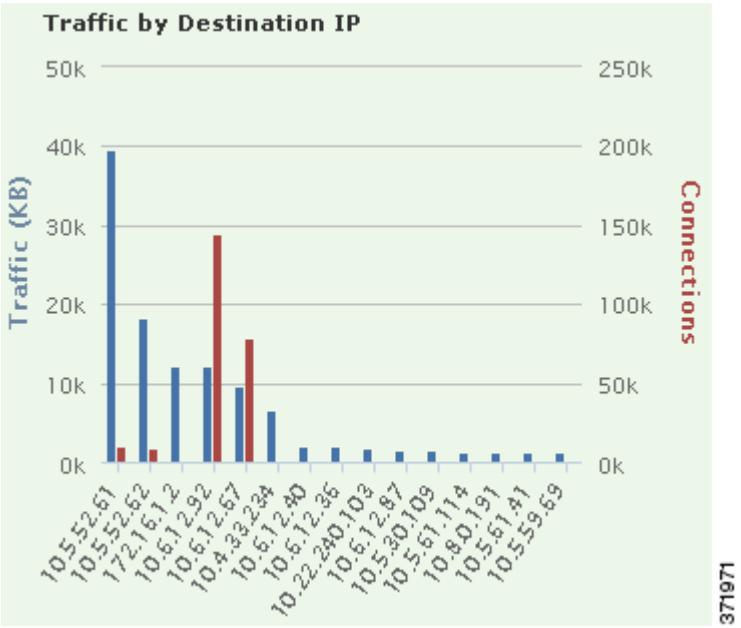
注　如果过滤入侵事件信息，“按源用户划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

查看“按目标 IP 划分的流量”图形

许可证：FireSIGHT

“按目标 IP 划分的流量”图形以条形图形式显示受监控网络中前 15 个最活跃目标 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个目标 IP 地址，蓝条代表流量数据，红条代表连接数据。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

注　如果过滤入侵事件信息，“按目标 IP 划分的流量”图形将隐藏。

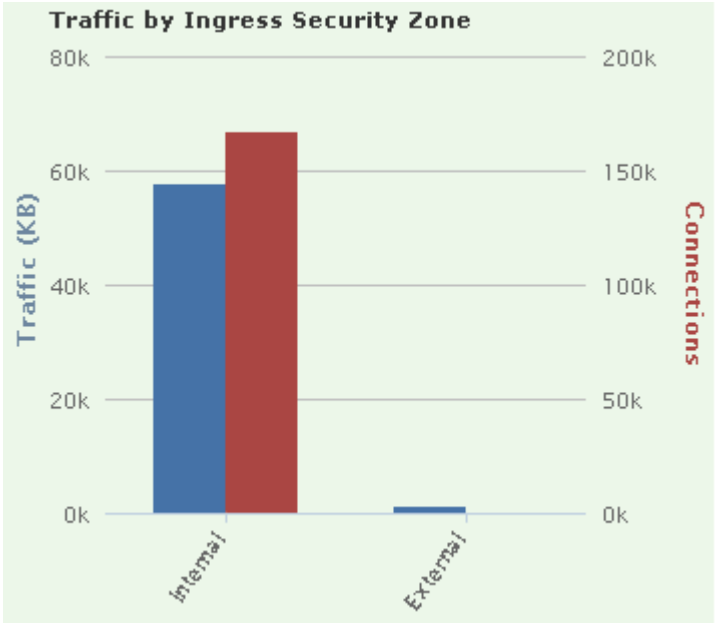
此图形主要从“连接事件”表提取数据。

查看“按入口/出口安全区域划分的流量”图形

许可证：FireSIGHT

“按入口/出口安全区域划分的流量”图形以条形图形式显示受监控网络上配置的每个安全区域的传入或传出网络流量（千字节每秒）和独特连接的计数。可配置此图形，根据自己的需求显示入口（默认）或出口安全区域的信息。

对于列出的每个安全区域，蓝条代表流量数据，红条代表连接数据。有关安全区域的信息，请参阅第 3-34 页上的使用安全区域。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

提示　要限制此图形，使其仅按出口安全区域显示流量，将鼠标指针悬停在图形上方，然后在显示的切换按钮上点击 **Egress**。点击 **Ingress** 返回默认视图。请注意，离开 Context Explorer 也会使图形返回默认 Ingress 视图。

注　如果过滤入侵事件信息，“按入口/出口安全区域划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

了解“应用信息”部分

许可证：FireSIGHT

Context Explorer 的 Application Information 部分包含三个交互图形和一个表格式列表，它们显示受监控网络中应用活动的全局视图：流量、入侵事件以及与应用相关联且进一步按分配给每个应用的预估风险或业务相关性排列的主机。“应用详情”列表列出了每个应用及其风险、业务相关性、类别和主机计数的交互列表。

对于此部分的所有“应用”实例，“应用信息”图形集默认对应用协议（例如 DNS 或 SSH）进行具体检查。还可配置 Application Information 部分，具体检查客户端应用（例如 PuTTY 或 Firefox）或 网络应用（例如 Facebook 或 Pandora）。

有关 Application Information 部分中图形和列表的详细信息，请参阅：

- 第 56-12 页上的查看“按风险/业务相关性和应用划分的流量”图形
- 第 56-13 页上的查看“按风险/业务相关性和应用划分的入侵事件”图形
- 第 56-14 页上的查看“按风险/业务相关性和应用划分的主机”图形
- 第 56-14 页上的查看“应用详细信息”列表

要配置 Application Information 部分，重点在于：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Context Explorer**。

系统将显示 Context Explorer。

步骤 2　将鼠标指针悬停在 **Application Protocol Information** 部分的上方。（请注意，如果之前在同一个 Context Explorer 会话中更改了此设置，该部分标题可能改为显示 **Client Application Information** 或 **Web Application Information**。）

此部分的选项按钮显示在右上角。

步骤 3　点击 **Application Protocol**、**Client Application** 或 **Web Application**。

Application Information 部分将根据所选选项刷新。

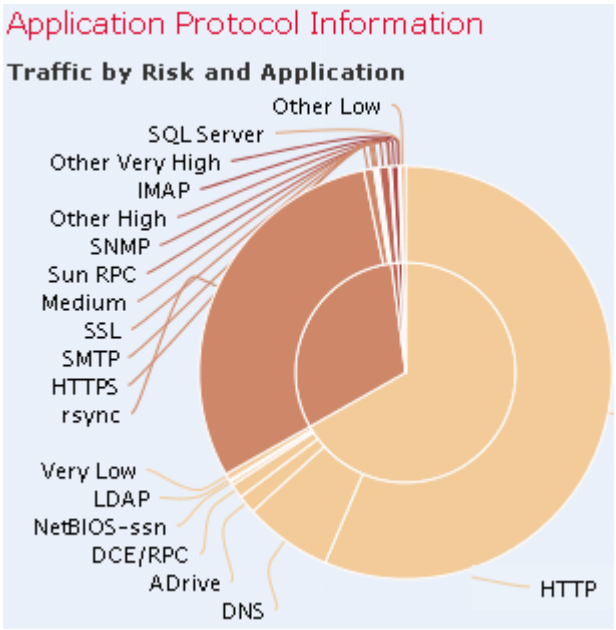
注　如果离开 Context Explorer，此部分恢复为其默认状态 （应用协议）。

查看“按风险/业务相关性和应用划分的流量”图形

许可证：FireSIGHT

“按风险/业务相关性和应用划分的流量”图形以环状图形式显示在受监控网络上检测到的应用流量的比例再现，这些受监控网络按应用的预估风险 （默认值）或预估业务相关性进行排列。内环按预估的风险/业务相关性水平 （例如，`Medium` 或 `High`）划分，而外环按特定应用对数据进行进一步的划分 （例如，`SSH` 或 `NetBIOS`）。很少检测到的应用在 **Other** 下分组。

请注意，无论日期和时间限制如何，此图形均反映所有可用数据。如果更改资源管理器的时间范围，图形不变。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其按业务相关性和应用显示流量，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击 **Business Relevance**。点击 **Risk** 返回默认视图。请注意，离开 Context Explorer 也会此图形返回默认 Risk 视图。

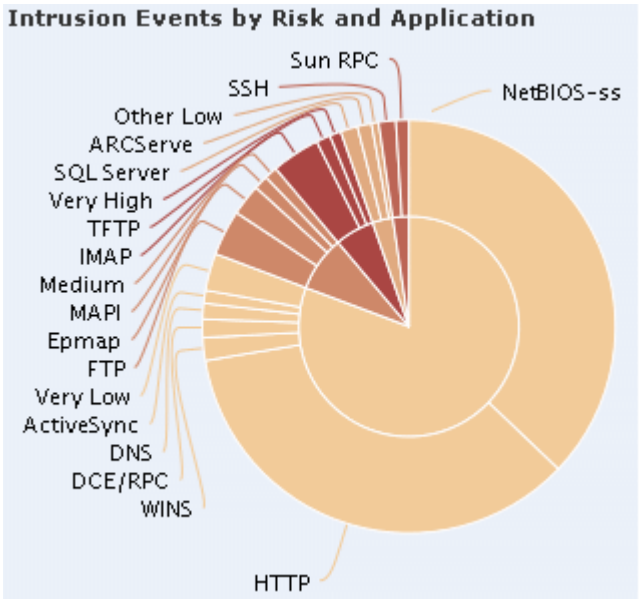
注 如果过滤入侵事件信息，“按风险/业务和应用划分的流量”图形将隐藏。

此图形主要从“连接事件”和“应用统计数据”表提取数据。

查看“按风险/业务相关性和应用划分的入侵事件”图形

许可证：FireSIGHT

“按风险/业务相关性和应用划分的入侵事件”图形以环状图形式显示受监控网络上检测到的入侵事件以及与这些入侵事件相关联的应用的比例再现，这些事件按应用的预估风险 （默认值）或预估业务相关性进行排列。内环按预估的风险/业务相关性水平 （例如， `Medium` 或 `High`）划分，而外环按特定应用对数据进行进一步的划分 （例如， `SSH` 或 `NetBIOS`）。很少检测到的应用在 **Other** 下分组。



将鼠标指针悬停在环状图形任何部分的上方，即可查看详细信息。点击图形中的任何部分，可过滤或向下展开该信息或 （如适用）查看应用信息。

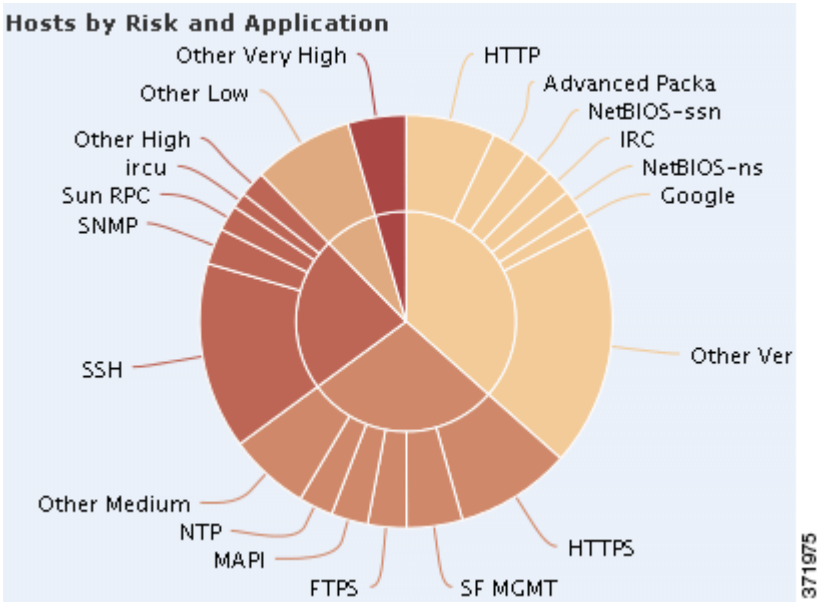
提示 要限制此图形，使其按业务相关性和应用显示入侵事件，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击 **Business Relevance**。点击 **Risk** 返回默认视图。请注意，离开 Context Explorer 也会此图形返回默认 Risk 视图。

此图形主要从“入侵事件”和“应用统计数据”表提取数据。

查看“按风险/业务相关性和应用划分的主机”图形

许可证：FireSIGHT

“按风险/业务相关性和应用划分的主机”图形以环状图形式显示受监控网络上检测到的主机以及与这些主机相关联的应用的比例化再现，这些主机按应用的预估风险（默认值）或预估业务相关性进行排列。内环按预估的风险/业务相关性水平（例如，`Medium` 或 `High`）划分，而外环按特定应用对数据进行进一步的划分（例如，`SSH` 或 `NetBIOS`）。非常罕见的应用在 **Other** 下分组。



将鼠标指针悬停在环状图形任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

提示　要限制此图形，使其按业务相关性和应用显示主机，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击 **Business Relevance**。点击 **Risk** 返回默认视图。请注意，离开 Context Explorer 也会此图形返回默认 Risk 视图。

此图形主要从“应用”表提取数据。

查看“应用详细信息”列表

许可证：FireSIGHT

Application Information 部分底端为“应用详细信息”列表，该表格提供受监控网络上检测到的每个应用的预估风险、预估业务相关性、类别和主机计数信息。应用按关联主机计数的降序列出。

“应用详细信息”列表不能排序，但是，可以点击任何表条目过滤或向下展开该信息或（如适用）查看应用信息。此表主要从“应用”表提取数据。

请注意，无论日期和时间限制如何，此列表均反映所有可用数据。如果更改资源管理器的时间范围，列表保持不变。

了解“安全情报”部分

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

Context Explorer 的 Security Intelligence 部分包含三个交互条形图，这些图显示被安全情报拉入黑名单或监控的受监控网络上流量的全局视图。这些图形按类别、源 IP 地址和目标 IP 地址分别对此类流量进行排序；流量数量（以千字节每秒）和适用的连接数均将显示。

有关 Security Intelligence 部分中图形的详细信息，请参阅：

- 第 56-15 页上的查看“按类别划分的安全情报流量”图形
- 第 56-16 页上的查看“按源 IP 划分的安全情报流量”图形
- 第 56-17 页上的查看“按目标 IP 划分的安全情报流量”图形

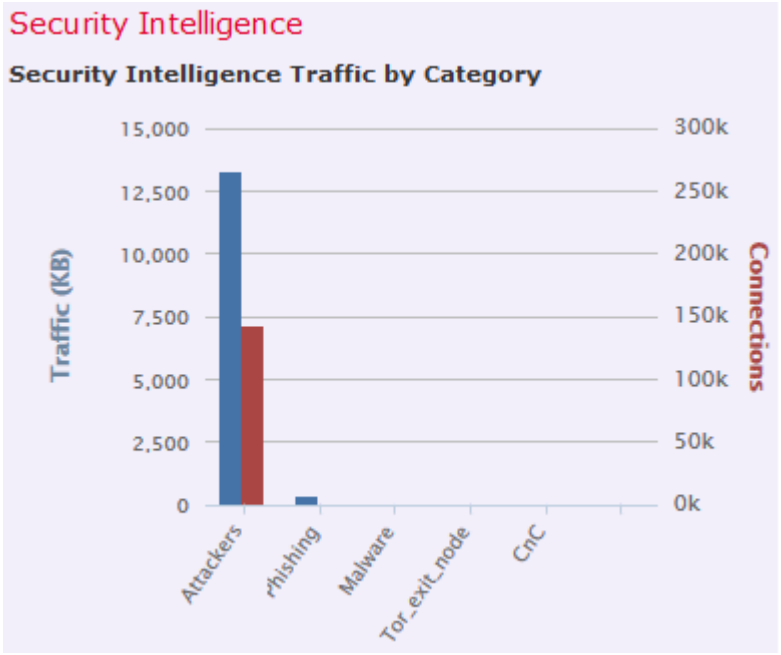
查看“按类别划分的安全情报流量”图形

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

“按类别划分的安全情报流量”图形以条形图形式显示受监控网络上的网络流量（千字节每秒）和顶级安全情报类别流量的独特连接的计数。对于列出的每个类别，蓝条代表流量数据，红条代表连接数据。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注　如果过滤入侵事件信息，“按类别划分的安全情报流量”图形将隐藏。

此图形主要从“安全情报事件”表提取数据。

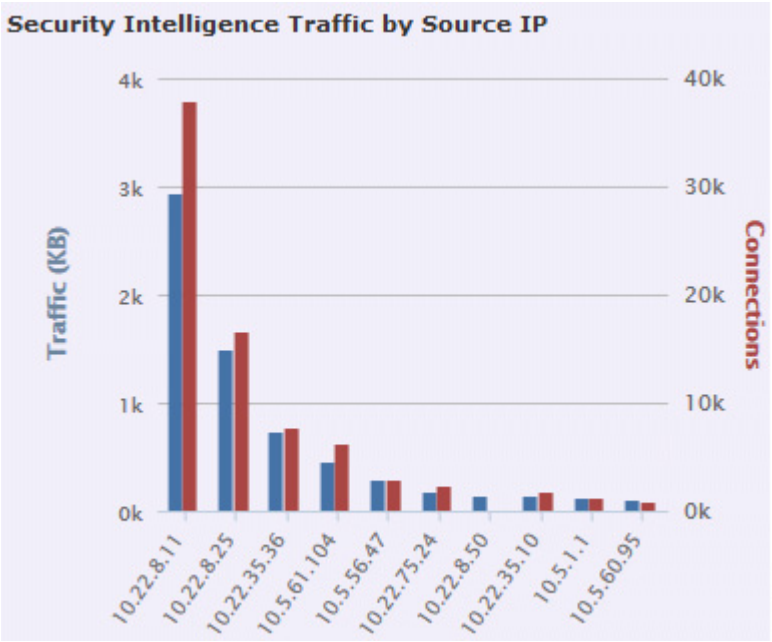
查看“按源 IP 划分的安全情报流量”图形

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

“按源 IP 划分的安全情报流量”视图以条形图形式显示受监控网络中安全情报监控流量的顶级源 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个类别，蓝条代表流量数据，红条代表连接数据。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注　如果过滤入侵事件信息，“按源 IP 划分的安全情报流量”图形将隐藏。

此图形主要从“安全情报事件”表提取数据。

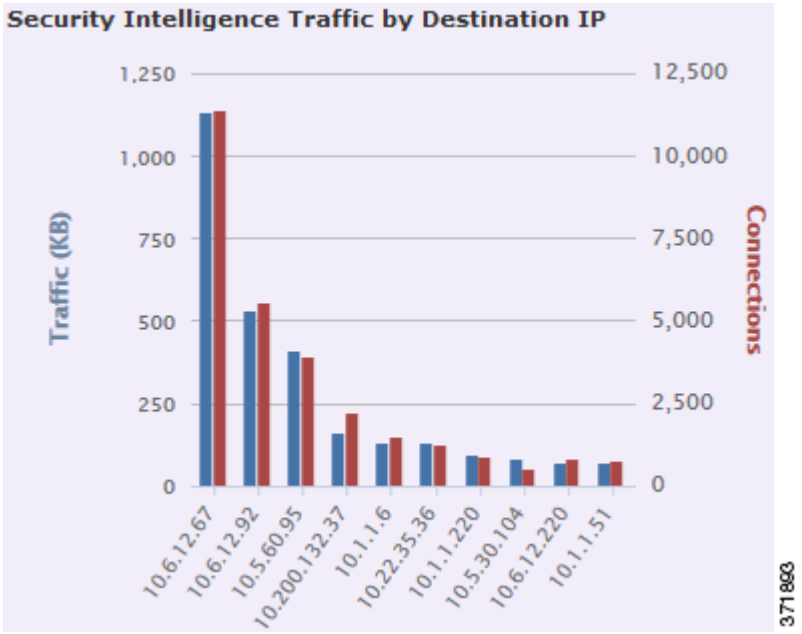
查看“按目标 IP 划分的安全情报流量”图形

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

“按目标 IP 划分的安全情报流量”视图以条形图形式显示受监控网络中安全情报监控流量的顶级源 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个类别，蓝条代表流量数据，红条代表连接数据。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注　如果过滤入侵事件信息，“按目标 IP 划分的安全情报流量”图形将隐藏。

此图形主要从“安全情报事件”表提取数据。

了解“入侵信息”部分

许可证：保护

Context Explorer 的 Intrusion Information 部分包含六个交互图形和一个表格式列表，它们显示受监控网络中入侵事件的全局视图：影响级别、攻击源、目标、用户、优先级、与入侵事件关联的安全区域，以及入侵事件分类、优先级和计数的详细列表。

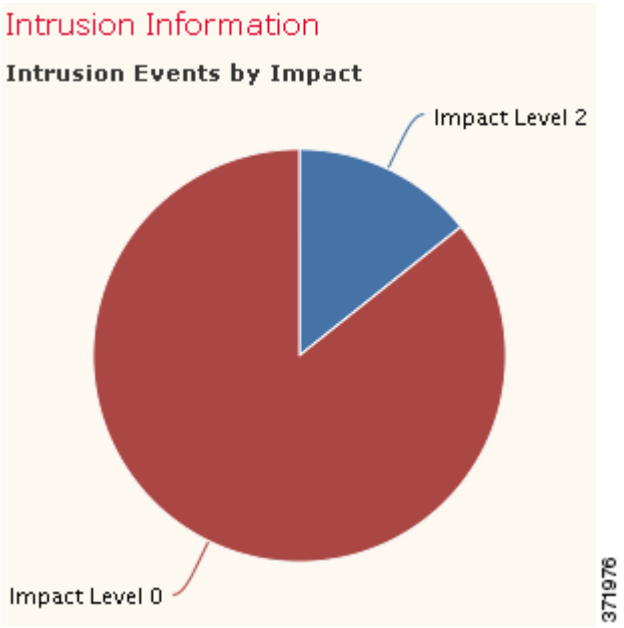
有关 Network Information 部分中图形和列表的详细信息，请参阅：

- 第 56-18 页上的查看“按影响划分的入侵事件”图形
- 第 56-19 页上的查看“主要攻击者”图形
- 第 56-20 页上的查看“主要用户”图形

查看“按影响划分的入侵事件”图形

许可证：保护

“按影响划分的入侵事件”图形以饼状图形式显示受监控网络上入侵事件的比例视图，按预估的影响级别 （从 0 - 4）分组。



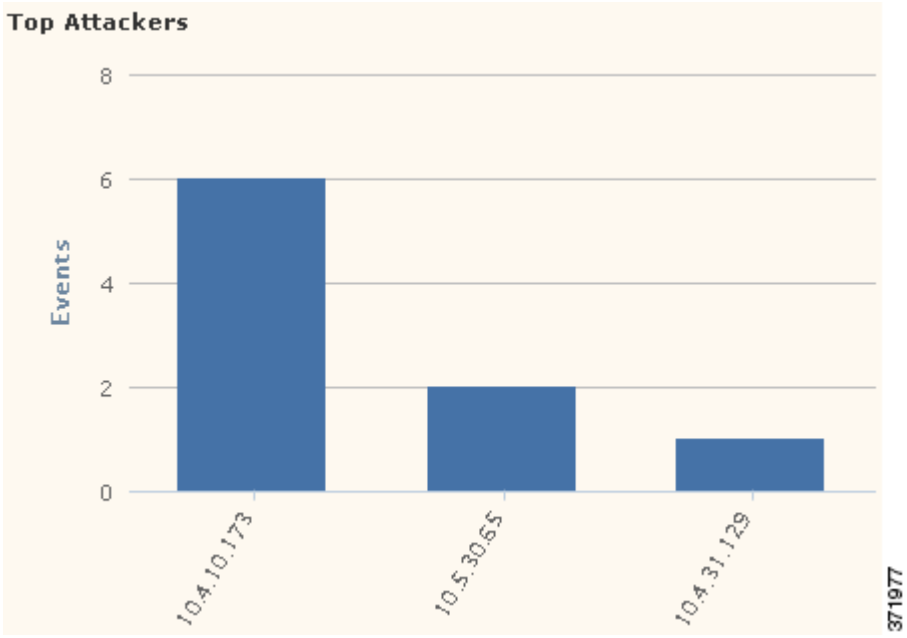
将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

此图形主要从“IDS 统计数据”和“入侵事件”表提取数据。

查看“主要攻击者”图形

许可证：保护

“主要攻击者”图形以条形图形式显示受监控网络中主要攻击性主机 IP 地址 （导致这些事件的地址）的入侵事件的计数。



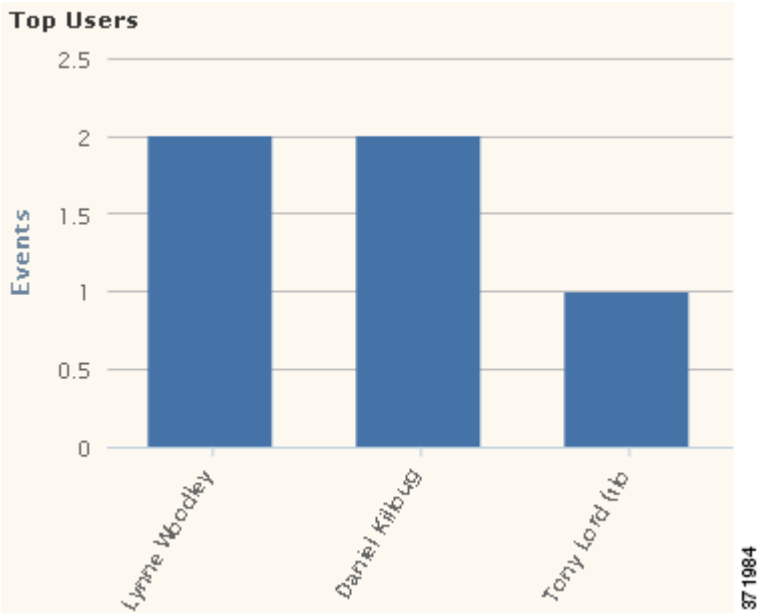
将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵事件”表提取数据。

查看“主要用户”图形

许可证：保护

“主要用户”图形以条形图形式按事件计数显示与最高入侵事件计数关联的受监控网络上的用户。



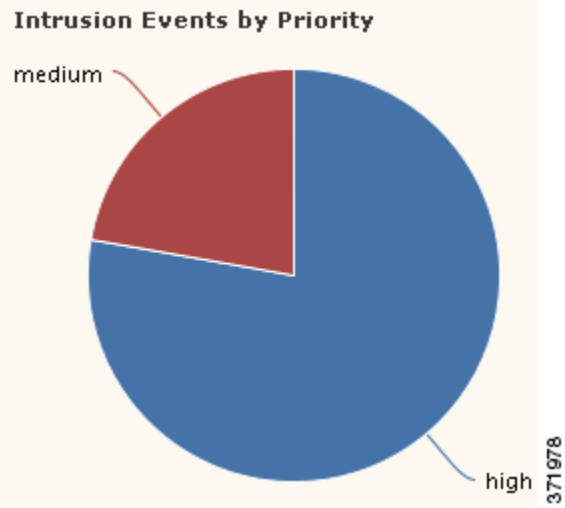
将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

此图形主要从“IDS 用户统计数据”和“入侵事件”表提取数据。请注意，此图形仅显示 User Agent 报告的用户。

查看“按优先级划分的入侵事件”图形

许可证：保护

“按优先级划分的入侵事件”图形以饼状图形式显示受监控网络中入侵事件的比例视图，按预估的优先级（例如，`High`、`Medium` 或 `Low`）分组。



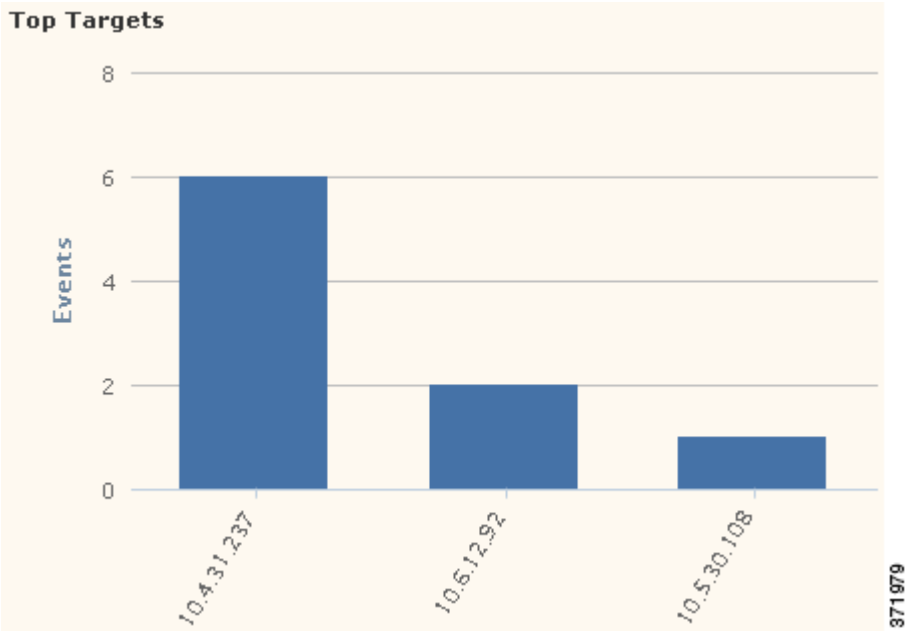
将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵事件”表提取数据。

查看“主要目标”图形

许可证：保护

“主要目标”图形以条形图形式显示受监控网络中主要目标主机 IP 地址 （导致这些事件的连接中的目标）的入侵事件计数。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵事件”表提取数据。

查看“主要入口/出口安全区域”图形

许可证：保护

“主要入口/出口安全区域”图形以条形图形式显示与受监控网络上配置的每个安全区域（入口或出口，取决于图形设置）关联的入侵事件计数。有关安全区域的信息，请参阅第 3-34 页上的使用安全区域。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

提示　要限制此图形，使其仅按出口安全区域显示流量，将鼠标指针悬停在图形上方，然后在显示的切换按钮上点击 **Egress**。点击 **Ingress** 返回默认视图。请注意，离开 Context Explorer 也会使图形返回默认 Ingress 视图。

此图形主要从“入侵事件”表提取数据。

可配置此图形，根据自己的需求显示入口（默认）或出口安全区域的信息。

查看“入侵事件详细信息”列表

许可证：保护

Intrusion Information 部分的底端为“入侵事件详细信息”列表，该表格提供了受监控网络上检测到的每个入侵事件的分类、预估优先级和事件计数信息。这些事件按事件计数的降序列出。

“入侵事件详细信息”列表不能排序，但是，可点击任何表条目过滤或向下展开该信息。此表主要从“入侵事件”表提取数据。

了解“文件信息”部分

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

Context Explorer 的 Files Information 部分包含六个交互图形，它们显示受监控网络上的文件和恶意事件的全局视图。五个图形显示网络流量中检测到的文件的文件类型、文件名和恶意软件性质，以及发送（上传）和接收（下载）这些文件的主机。最终图形显示网络上检测的恶意软件威胁，如已订用 FireAMP，也显示用户安装 FireAMP 连接器所在终点上检测到的恶意软件威胁。

注　如果过滤入侵信息，整个 Files Information 部分将隐藏。

请注意，您必须拥有恶意软件许可证并对 Files Information 图形启用恶意软件检测，以纳入基于网络的恶意软件数据。另请注意 DC500 防御中心和 2 系列设备以及用于 Blue Coat X-系列的思科 NGIPS不支持高级恶意软件防护，因此 DC500 防御中心无法显示这些数据，并且2 系列设备和用于 Blue Coat X-系列的思科 NGIPS检测不到这些数据。请参阅第 37-2 页上的了解恶意软件防护和文件控制。

有关 Files Information 部分的详细信息，请参阅：

- 第 56-25 页上的查看“主要文件类型”图形
- 第 56-26 页上的查看“主要文件名”图形
- 第 56-26 页上的查看“按性质划分的文件”图形
- 第 56-28 页上的查看“发送文件的主要主机”图形
- 第 56-29 页上的查看“接收文件的主要主机”图形
- 第 56-30 页上的查看“主要恶意软件检测”图形

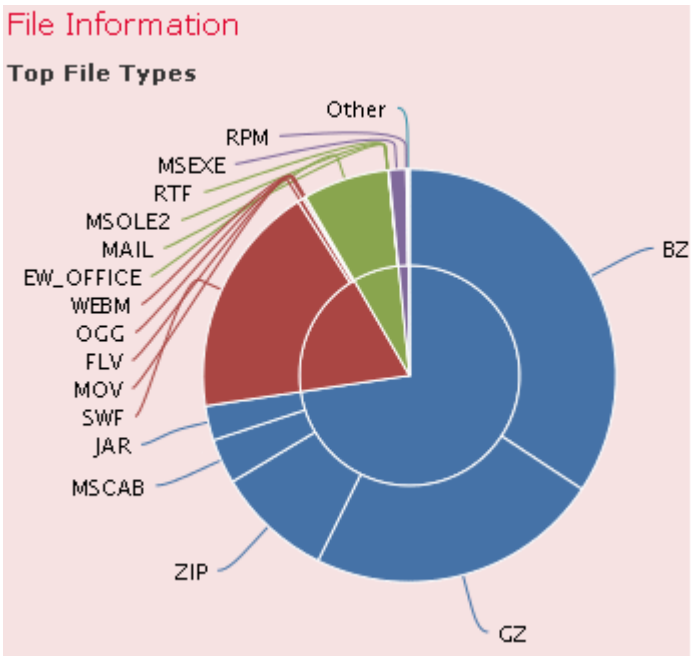
查看“主要文件类型”图形

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

“主要文件类型”图形以饼状图形式显示网络流量中检测到的文件类型的比例视图 （外环），按文件类别 （内环）分组。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

请注意，您必须拥有恶意软件许可证并对此图形启用恶意软件检测，以纳入基于网络的恶意软件数据。另请注意 DC500 防御中心和 2 系列设备以及用于 Blue Coat X-系列的思科 NGIPS不支持高级恶意软件防护，因此 DC500 防御中心无法显示这些数据，并且2 系列设备和用于 Blue Coat X-系列的思科 NGIPS检测不到这些数据。请参阅第 37-2 页上的了解恶意软件防护和文件控制。

此图形主要从“文件事件”表提取数据。

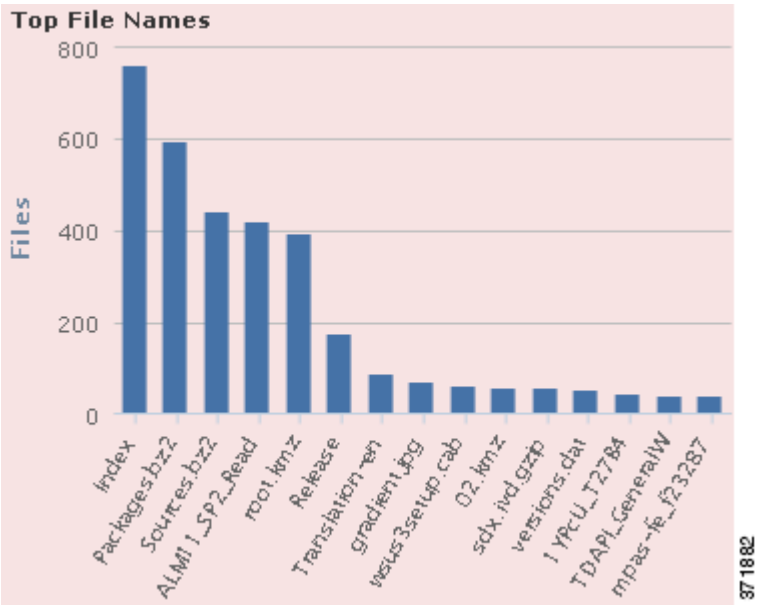
查看“主要文件名”图形

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

“主要文件名”图形以条形图形式显示网络流量中检测到的主要独特文件名的计数。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

请注意，您必须拥有恶意软件许可证并对此图形启用恶意软件检测，以纳入基于网络的恶意软件数据。另请注意 DC500 防御中心和 2 系列设备以及用于 Blue Coat X-系列的思科 NGIPS不支持高级恶意软件防护，因此 DC500 防御中心无法显示这些数据，并且2 系列设备和用于 Blue Coat X-系列的思科 NGIPS检测不到这些数据。请参阅第 37-2 页上的了解恶意软件防护和文件控制。

此图形主要从“文件事件”表提取数据。

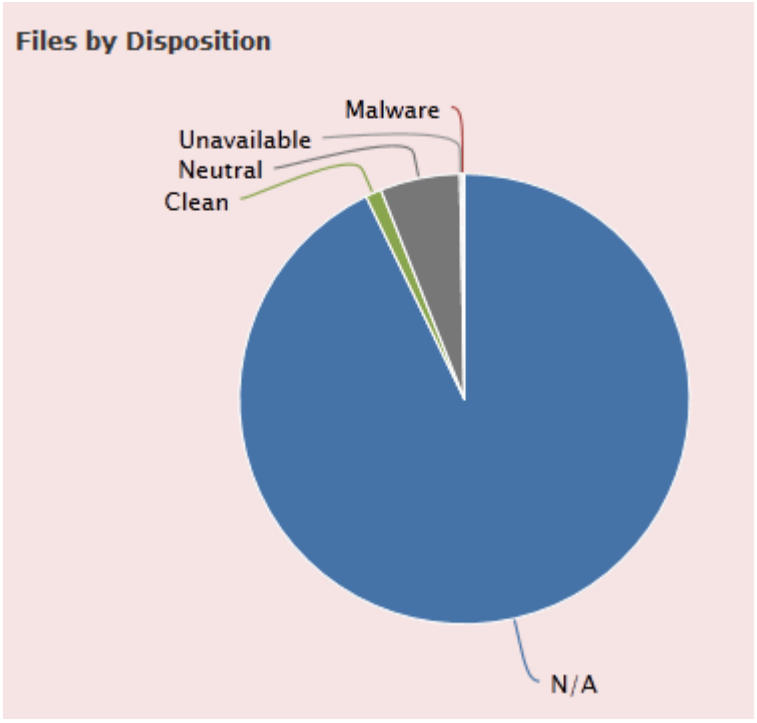
查看“按性质划分的文件”图形

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

“主要文件类型”图形以饼状图形式显示网络流量中检测到的恶意软件性质的比例视图。请注意，只有防御中心为其执行综合安全智能云查找 （需要恶意软件许可证）的文件才具有性质。未触发云查找的文件性质为 `N/A`。`Unavailable` 性质表示防御中心无法执行恶意软件云查找。请参阅第 37-2 页上的了解恶意软件防护和文件控制，了解其他性质的说明。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

请注意，您必须拥有恶意软件许可证并对此图形启用恶意软件检测，以纳入基于网络的恶意软件数据。另请注意 DC500 防御中心和 2 系列设备以及用于 Blue Coat X-系列的思科 NGIPS不支持高级恶意软件防护，因此 DC500 防御中心无法显示这些数据，并且 2 系列设备和用于 Blue Coat X-系列的思科 NGIPS检测不到这些数据。请参阅第 37-2 页上的了解恶意软件防护和文件控制。

此图形主要从“文件事件”表提取数据。

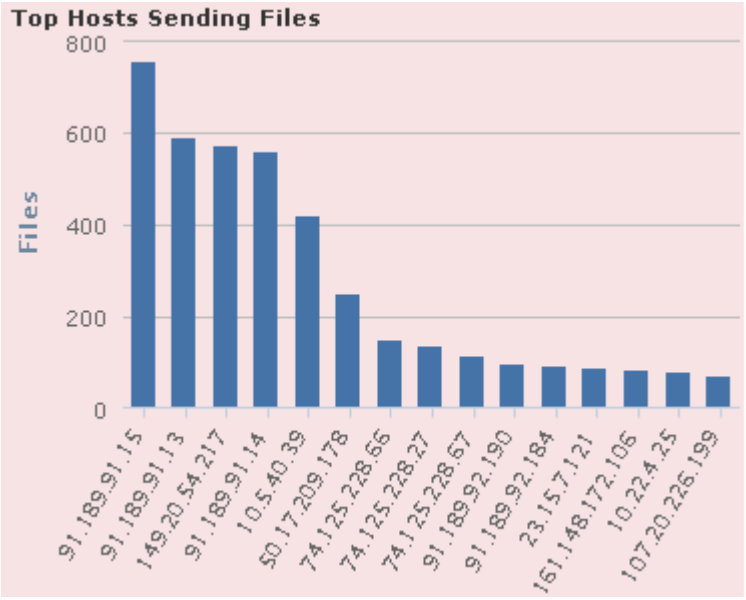
查看“发送文件的主要主机”图形

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

“发送文件的主要主机”图形以条形图形式显示网络流量中检测到的主要文件发送主机 IP 地址的文件数量计数。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

提示　要限制此图形，使其仅显示发送恶意软件的主机，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击 **Malware**。点击 **Files** 以返回默认文件视图。请注意，离开 Context Explorer 也会此图形返回默认文件视图。

请注意，您必须拥有恶意软件许可证并对此图形启用恶意软件检测，以纳入基于网络的恶意软件数据。另请注意 DC500 防御中心和2 系列设备以及用于 Blue Coat X-系列的思科 NGIPS不支持高级恶意软件防护，因此 DC500 防御中心无法显示这些数据，并且 2 系列设备和用于 Blue Coat X-系列的思科 NGIPS检测不到这些数据。请参阅第 37-2 页上的了解恶意软件防护和文件控制。

此图形主要从“文件事件”表提取数据。

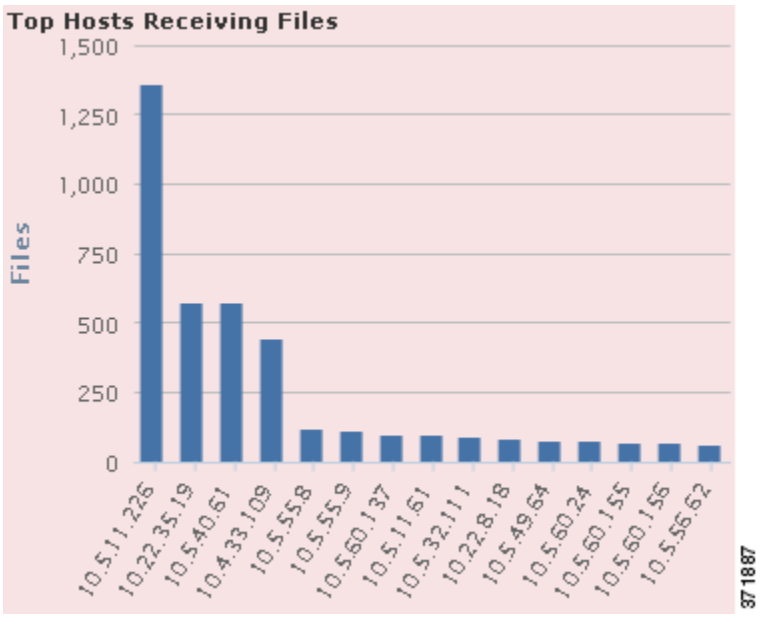
查看“接收文件的主要主机”图形

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

“接收文件的主要主机”图形以条形图形式显示网络流量中检测到的主要文件接收主机 IP 地址的文件数量。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

提示　要限制此图形，使其仅显示接收恶意软件的主机，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击 **Malware**。点击 **Files** 以返回默认文件视图。请注意，离开 Context Explorer 也会此图形返回默认文件视图。

请注意，您必须拥有恶意软件许可证并对此图形启用恶意软件检测，以纳入基于网络的恶意软件数据。另请注意 DC500 防御中心和 2 系列设备以及用于 Blue Coat X-系列的思科 NGIPS不支持高级恶意软件防护，因此 DC500 防御中心无法显示这些数据，并且 2 系列设备和用于 Blue Coat X-系列的思科 NGIPS检测不到这些数据。请参阅第 37-2 页上的了解恶意软件防护和文件控制。

此图形主要从“文件事件”表提取数据。

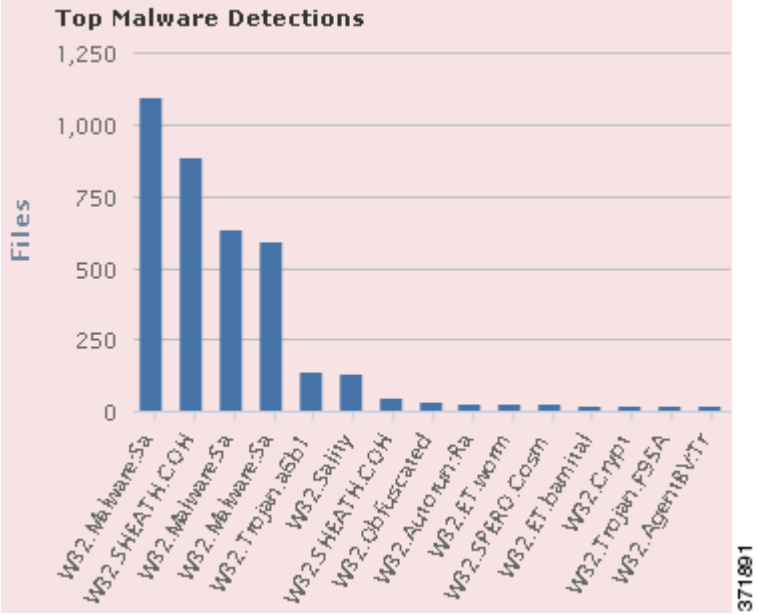
查看“主要恶意软件检测”图形

许可证：保护或恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

“恶意软件检测”图形以条形图形式显示网络上检测到的主要恶意软件威胁的计数，如已订用 FireAMP，也显示用户安装 FireAMP 连接器所在终点上检测到的主要恶意软件威胁的计数。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

请注意，您必须拥有恶意软件许可证并对此图形启用恶意软件检测，以纳入基于网络的恶意软件数据。另请注意 DC500 防御中心和 2 系列设备以及用于 Blue Coat X-系列的思科 NGIPS不支持高级恶意软件防护，因此 DC500 防御中心无法显示这些数据，并且 2 系列设备和用于 Blue Coat X-系列的思科 NGIPS检测不到这些数据。请参阅第 37-2 页上的了解恶意软件防护和文件控制。

此图形主要从“文件事件”和“恶意软件事件”表提取数据。

了解“地理定位信息”部分

许可证：FireSIGHT

受支持的防御中心：除 DC500 外的所有型号

Context Explorer 的 Geolocation Information 部分包含三个交互环状图形，它们显示与受监控网络上主机交换数据的国家/地区的全局视图：发起方或响应方国家/地区的独特连接、按源或目标国家/地区划分的入侵事件以及按发送或接收国家/地区划分的文件事件。

有关 Geolocation Information 部分的详细信息，请参阅：

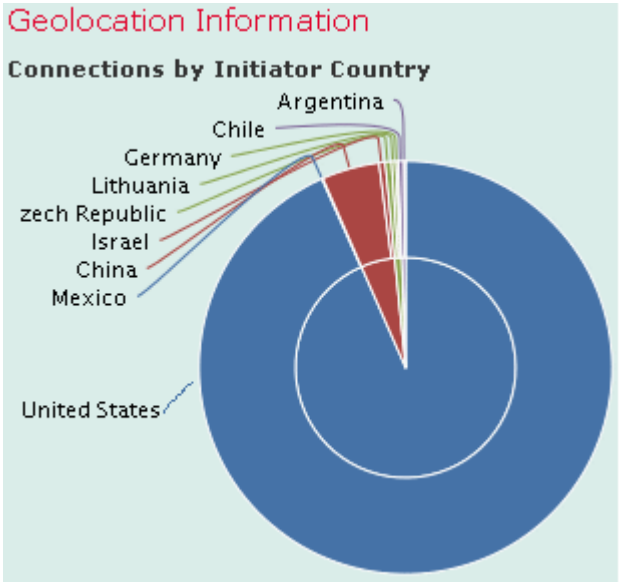
- 第 56-31 页上的查看“按发起方/响应方国家/地区划分的连接”图形
- 第 56-32 页上的查看“按源/目标地国家/地区划分的入侵事件”图形
- 第 56-33 页上的查看“按发送/接收国家/地区划分的文件事件”图形

查看“按发起方/响应方国家/地区划分的连接”图形

许可证：FireSIGHT

受支持的防御中心：除 DC500 外的所有型号

“按发起方/响应方国家/地区划分的连接”图形以环状图形式显示作为发起方（默认值）或响应方的网络连接涉及国家/地区的比例视图。内环将这些国家/地区按大陆分组。有关地理定位的信息，请参阅第 58-17 页上的使用地理定位。有关连接数据的信息，请参阅第 39-1 页上的使用连接与安全情报数据。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

提示　要限制此图形，使其仅显示作为连接响应方的国家/地区，将鼠标指针悬停在图形上方，然后在显示的切换按钮上，点击 **Responder**。点击 **Initiator** 返回默认视图。请注意，离开 Context Explorer 也会使此图形返回默认 Initiator 视图。

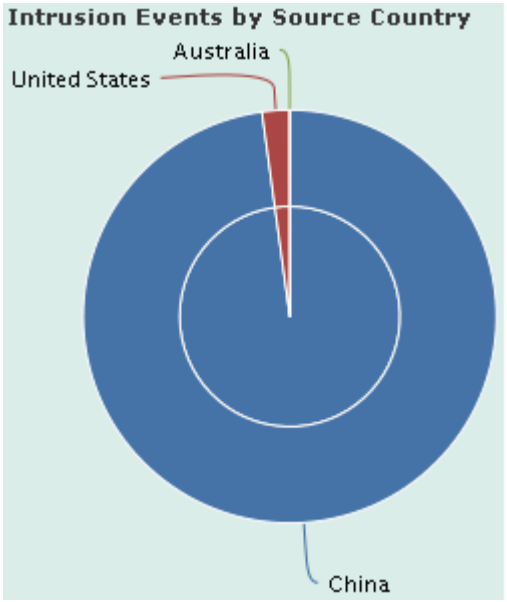
此图形主要从“连接摘要数据”表提取数据。

查看“按源/目标地国家/地区划分的入侵事件”图形

许可证：FireSIGHT

受支持的防御中心：除 DC500 外的所有型号

“按源/目标地国家/地区划分的入侵事件”图形以环状图形式显示作为事件（默认值）或目标来源的网络上入侵事件涉及的国家/地区的比例视图。内环将这些国家/地区按大陆分组。有关地理定位的信息，请参阅第 58-17 页上的使用地理定位。有关入侵事件数据的信息，请参阅第 41-1 页上的处理入侵事件。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示作为入侵事件目标的国家/地区，将鼠标指针悬停在图形上方，然后在显示的切换按钮上，点击 **Destination**。点击 **Source** 以返回默认视图。请注意，离开 Context Explorer 也会使此图形返回默认 Source 视图。

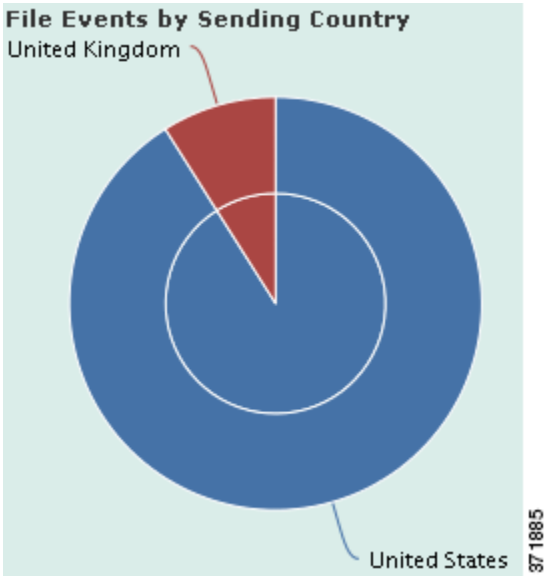
此图形主要从“入侵事件”表提取数据。

查看“按发送/接收国家/地区划分的文件事件”图形

许可证：FireSIGHT

受支持的防御中心：除 DC500 外的所有型号

“按发送/接收国家/地区划分的文件事件”图形以环状图形式显示网络上文件事件中检测到作为发送（默认值）或接收文件的国家/地区的比例视图。内环将这些国家/地区按大陆分组。有关地理定位的信息，请参阅第 58-17 页上的使用地理定位。有关文件事件数据的信息，请参阅第 40-6 页上的使用文件事件。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示接收文件的国家/地区，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击 **Receiver**。点击 **Sender** 返回默认视图。请注意，离开 Context Explorer 也会使此图形返回默认 Sender 视图。

此图形主要从“文件事件”表提取数据。

了解“URL 信息”部分

许可证：FireSIGHT或URL 过滤

受支持的设备：因功能而异

受支持的防御中心：因功能而异

Context Explorer 的 URL Information 部分包含三个交互条形图形，它们显示与受监控网络上主机交换数据的 URL 的全局视图：与 URL 相关联、按单个 URL、URL 类别和 URL 声誉排序的流量和独特连接。不能过滤 URL 信息。

注 如果过滤入侵事件信息，整个 RL Information 部分将隐藏。

请注意，您必须拥有 URL 过滤许可证并为 URL 过滤图形启用 URL 过滤，包括 URL 类别和声誉数据。另请注意，DC500 防御中心和 2 系列设备均不支持按声誉和类别执行 URL 过滤，因此，DC500 防御中心无法显示这些数据，而 2 系列设备也检测不到这些数据。请参阅第 16-7 页上的阻止 URL。

有关 URL Information 部分的详细信息，请参阅：

- 第 56-34 页上的查看“按 URL 划分的流量”图形
- 第 56-35 页上的查看“按 URL 类别划分的流量”图形
- 第 56-36 页上的查看“按 URL 声誉划分的流量”图形

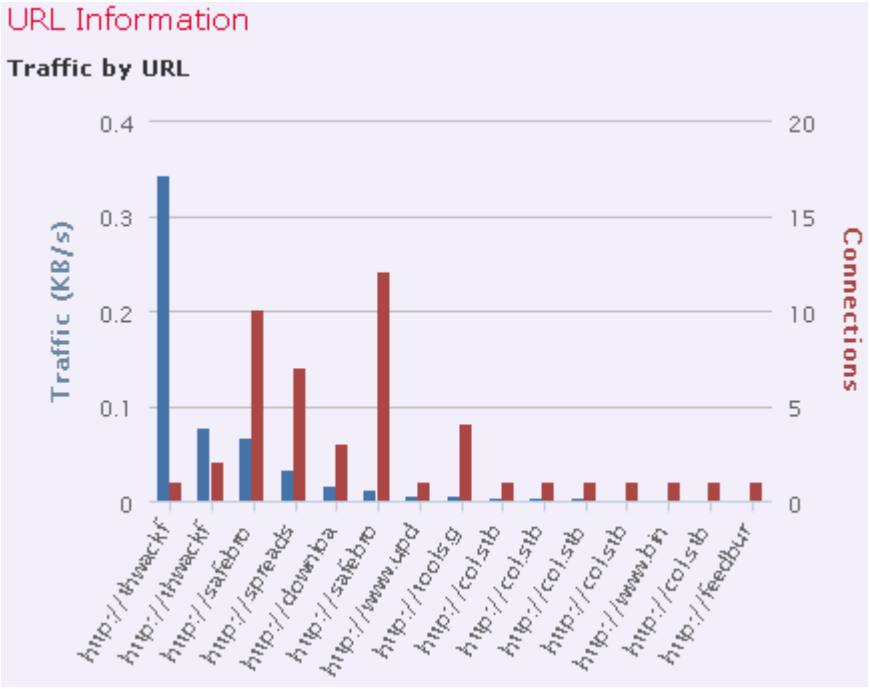
查看“按 URL 划分的流量”图形

许可证：FireSIGHT或URL 过滤

受支持的设备：因功能而异

受支持的防御中心：因功能而异

“按 URL 划分的流量”图形以条形图形式显示受监控网络中请求最频繁的 15 个 URL 的网络流量（千字节每秒）和独特连接的计数。对于列出的每个 URL，蓝条代表流量数据，红条代表连接数据。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注　如果过滤入侵事件信息，“按 URL 划分的流量”图形将隐藏。

请注意，您必须拥有 URL 过滤许可证并为 URL 过滤图形启用 URL 过滤，包括 URL 类别和声誉数据。另请注意，DC500 防御中心和 2 系列设备均不支持按声誉和类别执行 URL 过滤，因此，DC500 防御中心无法显示这些数据，而 2 系列设备也检测不到这些数据。请参阅第 64-25 页上的启用云通信。

此图形主要从“连接事件”表提取数据。

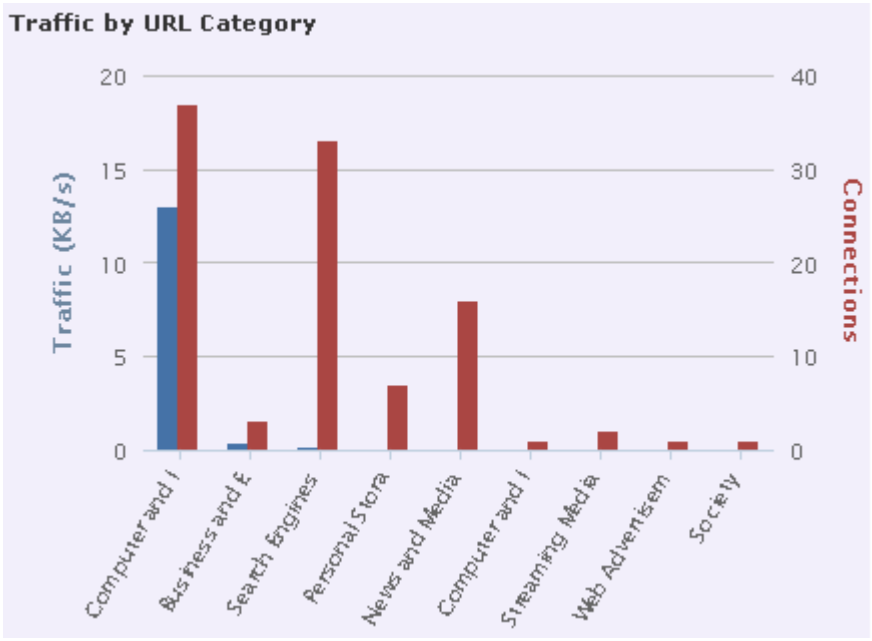
查看“按 URL 类别划分的流量”图形

许可证：URL 过滤

受支持的设备：因功能而异

受支持的防御中心：因功能而异

“按 URL 类别划分的流量”图形以条形图形式显示受监控网络中请求最频繁的 URL 类别 （例如， `Search Engines` 和 `Streaming Media`）的网络流量 （千字节每秒）和独特连接的计数。对于列出的每个 URL 类别，蓝条代表流量数据，红条代表连接数据。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注　如果过滤入侵事件信息，“按 URL 类别划分的流量”图形将隐藏。

请注意，您必须拥有 URL 过滤许可证并为 URL 过滤图形启用 URL 过滤，包括 URL 类别和声誉数据。另请注意， DC500 防御中心和 2 系列设备均不支持按声誉和类别执行 URL 过滤，因此，DC500 防御中心无法显示这些数据，而 2 系列设备也检测不到这些数据。请参阅第 16-8 页上的执行基于信誉的 URL 阻止。

此图形主要从“URL 统计数据”和“连接事件”表提取数据。

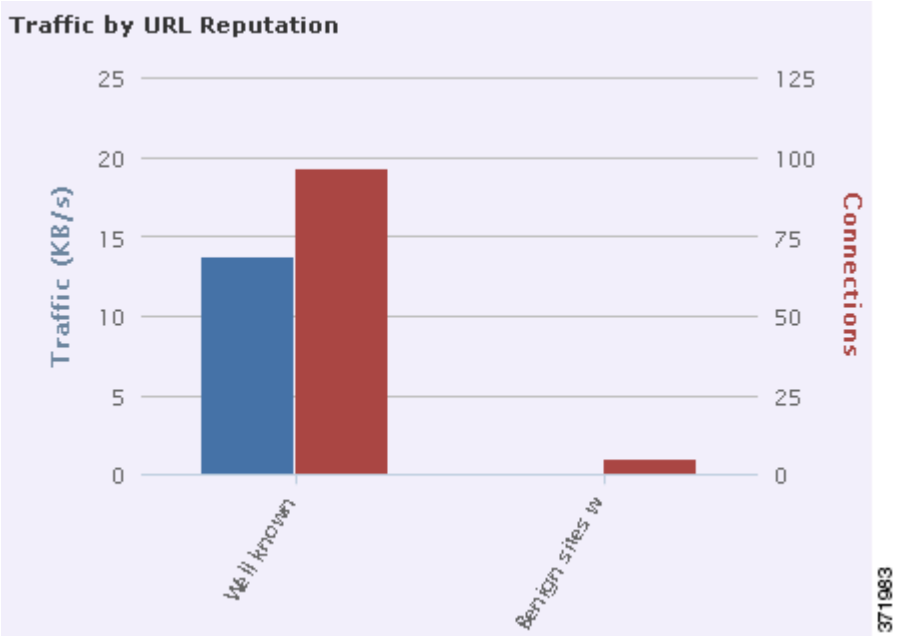
查看“按 URL 声誉划分的流量”图形

许可证：URL 过滤

受支持的设备：因功能而异

受支持的防御中心：因功能而异

“按 URL 声誉划分的流量”图形以条形图形式显示受监控网络中请求最频繁的 URL 声誉组 （例如，`Well known` 或 `Benign sites with security risks`）的网络流量 （千字节每秒）和独特连接的计数。对于列出的每个 URL 声誉组，蓝条代表流量数据，红条代表连接数据。



将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注　如果过滤入侵事件信息，“按 URL 声誉划分的流量”图形将隐藏。

请注意，您必须拥有 URL 过滤许可证并为 URL 过滤图形启用 URL 过滤，包括 URL 类别和声誉数据。另请注意， DC500 防御中心和 2 系列设备均不支持按声誉和类别执行 URL 过滤，因此，DC500 防御中心无法显示这些数据，而 2 系列设备也检测不到这些数据。请参阅第 16-8 页上的执行基于信誉的 URL 阻止。

此图形主要从“URL 统计数据”和“连接事件”表提取数据。

刷新 Context Explorer

许可证：FireSIGHT

Context Explorer 不会自动更新显示的信息。要更新数据，必须手动刷新资源管理器。

请注意，虽然重新加载 Context Explorer （通过刷新资源管理器程序或离开，然后返回 Context Explorer）可刷新所有显示的信息，但此操作不会保留对部分配置做出的任何更改 （例如“入口/出口”图形和 Application Information 部分）且可能导致加载延迟。

要刷新 Context Explorer，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在 Context Explorer 上，点击右上方的 **Reload**。

资源管理器更新，显示选定时间范围内的最新信息。请注意，在刷新完成之前， **Reload** 按钮灰显。

设置 Context Explorer 的时间范围

许可证：FireSIGHT

可配置 Context Explorer 的时间范围，以反映短至前一小时或长至上一年的时间段。请注意，如果更改时间范围， Context Explorer 无法自动更新反映所做的更改。要应用新的时间范围，必须手动刷新资源管理器。

即使离开 Context Explorer 或终止登录会话，对时间范围所做的更改也会持续。

要更改 Context Explorer 的时间范围，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　从 **Show the last** 下拉列表，选择时间范围。

步骤 2　或者，要从新时间范围查看数据，请点击 **Reload**。

Context Explorer 的所有部分均将更新，反映新的时间范围。

提示　点击 **Apply Filters** 也可应用任何时间范围更新。

Context Explorer 部分最小化和最大化

许可证：FireSIGHT

可最小化和隐藏 Context Explorer 的一个或多个部分。如要仅重点关注某些部分，或如果想要更简单的视图，此操作很有用。不能最小化“流量和入侵事件计数时间”图形。

请注意，即使刷新页面或注销设备， Context Explorer 部分仍会保留配置的最小化或最大化状态。

要最小化 Context Explorer 部分，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击一个部分标题栏中的最小化图标 (−)。

要最大化 Context Explorer 部分，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击已最小化部分标题栏中的最大化图标 (□)。

向下钻取 Context Explorer 数据

许可证：因功能而异

如果想要超出 Context Explorer 允许的范围，更详细地检查图形和列表数据，可向下展开相关数据的表视图。（请注意，不能向下展开“随时间推移的流量和入侵事件”图形。）例如，在“按源 IP 划分的流量”图形中向下展开一个 IP 地址可显示 Connection Events 表的 Connections with Application Details 视图，仅包括与所选源 IP 地址关联的数据。

视乎要检查的数据类型，上下文菜单中会显示其他选项。与特定 IP 地址相关联的数据点提供的选项可用于查看所选 IP 地址上的主机或域名信息。与特定应用相关联的数据点提供的选项可用于查看所选应用中的应用信息。与特定用户相关联的数据点提供的选项可用于查看用户的用户配置文件页。与入侵事件消息相关联的数据点提供的选项可用于查看规则文档，了解该事件的关联入侵规则，而与特定 IP 地址相关联的数据点提供的选项可用于将该地址列为黑名单和白名单。

用于向下展开数据的上下文菜单还包含用于过滤该数据的选项。有关过滤的详细信息，请参阅第 56-39 页上的使用 Context Explorer 中的过滤器。

要向下钻取 Context Explorer 中的数据，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Context Explorer**。

系统将显示 Context Explorer。

步骤 2　在除“随时间推移的流量和入侵事件”以外的任何部分，请点击要调查的数据点。

系统在附近显示上下文菜单弹出窗口。

步骤 3　视乎所选数据点，系统提供多个选项：

- 要在表视图中查看此数据的更多详细信息，请选择 **Drill into Analysis**。

  系统打开一个新窗口，显示所选数据的详细表视图。

- 如果选定一个与特定 IP 地址相关联的数据点并想要查看关联主机的更多信息，选择 **View Host Information**。

  系统打开一个新窗口，显示所选 IP 地址的主机配置文件页面。有关主机属性和主机配置文件的详细信息，请参阅第 49-1 页上的使用主机配置文件。

- 如果选定一个带有特定 IP 地址的数据点并想要搜索该地址的域名，请选择 **Whois**。

  系统打开一个新窗口，显示所选 IP 地址的域名查询结果。

- 如果选定一个与特定应用相关联的数据点并想要查看该应用的更多信息，选择 **View Application Information**。

  系统打开一个新窗口，显示所选应用的信息。有关应用属性的详细信息，请参阅第 45-9 页上的了解应用检测。

- 如果选定一个与特定用户相关联的数据点并想要查看该用户的更多信息，选择 **View User Information**。

系统打开一个新窗口，显示所选用户的用户配置文件页面。有关用户详情的详细信息，请参阅第 50-55 页上的了解用户详细信息和主机历史记录。

- 如果选定与特定入侵事件消息相关联的数据点并想要查看关联入侵规则的详细信息，请选择 **View Rule Documentation**。

  系统打开一个新窗口，显示与所选事件有关的规则详细信息页面。有关入侵规则详情的详细信息，请参阅第 32-4 页上的查看规则详细信息。

- 如果选定与特定 IP 地址相关联的数据点并想要将该 IP 地址添加至安全情报全局黑名单和白名单，请选择适当的选项：**Blacklist Now** 或 **Whitelist Now**。在显示的弹出窗口中确认选择。

  此时， IP 地址被拉入黑名单或白名单。有关详细信息，请参阅第 3-6 页上的使用全局白名单和黑名单。

  不支持安全情报数据的 DC500 防御中心未列出这些选项。

使用 Context Explorer 中的过滤器

许可证：FireSIGHT

除了 Context Explorer 初始显示的基本、广泛数据外，可选择为网络中活动的更精细的上下文照片过滤该数据。过滤器包含除 URL 信息外的所有类型 FireSIGHT 数据，支持排除和纳入，点击 Context Explorer 图形数据点即可快速应用，并影响整个资源管理器。一次最多可应用 20 个过滤器，创建符合网络和公司需求的非常具体的肖像。 Context Explorer URL 会反映应用的过滤器，因此，可用书签标记浏览器程序中的有用过滤器集供以后使用。

有关如何使用 Context Explorer 中过滤器的信息，请参阅：

- 第 56-39 页上的添加和应用过滤器
- 第 56-42 页上的用上下文菜单创建过滤器
- 第 56-43 页上的用书签标示过滤器

添加和应用过滤器

许可证：因功能而异

受支持的设备：因功能而异

受支持的防御中心：因功能而异

过滤器可以通过多种方式添加至 Context Explorer 数据：

- 从 Add Filter 窗口
- 在资源管理器中选择一个数据点时，从上下文菜单弹出窗口
- 从 Context Explorer 图标 ( ) 或特定详细信息视图页面 （Application Detail、 Host Profile、 Rule Detail 和 User Profile）显示的文本链接。点击这些链接，根据详细信息视图页面的相关数据自动打开并过滤 Context Explorer。例如，点击一个用户详细信息页面上的 Context Explorer 以便用户 `jenkins` 限制资源管理器仅显示与该用户相关的数据。

本小节重点介绍用 Add Filter 窗口从头创建过滤器。有关使用上下文菜单从 Context Explorer 图形和列表数据创建快速过滤器的信息，请参阅第 56-42 页上的用上下文菜单创建过滤器。

点击 Context Explorer 左上方的 **Filters** 下方的加号图标 (+) 即可访问的 Add Filter 窗口，该窗口仅包含两个字段：**Data Type** 和 **Filter**。

Data Type 下拉列表中包含可用于限制 Context Explorer 的许多不同类型的 FireSIGHT 系统数据。选择一个数据类型后，在 **Filter** 字段为该类型输入一个特定的值 （例如，为类型 **Continent** 输入一个值 `Asia`）。为了便于操作， Filter 字段将所选数据类型提供多个灰显示例值。（在该字段中输入数据时，这些示例值将被擦除。）

下表用列出可用作过滤器的数据类型，每种类型附有示例和简要定义。请注意， DC500 防御中心不显示数据，而且 2 系列设备和用于 Blue Coat X-系列的思科 NGIPS不为其不支持的功能检测数据。请参阅按设备型号支持的访问控制功能表，了解 2 系列设备和用于 Blue Coat X-系列的思科 NGIPS功能的摘要。

表 56-2　　过滤器数据类型

类型	示例值	定义
Access Control Action	`Allow`, `Block`	访问控制策略为允许或阻止流量而采取的措施
Application Category	`web browser`, `email`	应用的最基本功能的通用分类
应用名称	`Facebook`, `HTTP`	应用的名称
Application Risk	`Very High`, `Medium`	应用的预估安全风险
Application Tag	`encrypts communications`, `sends mail`	有关应用的其他信息；应用可以具备任意数量的标记，包括无
应用程序类型	`Client`, `Web Application`	应用的类型：应用协议、客户端或网络应用
业务相关性	`Very Low`, `High`	应用与业务活动 （与娱乐相对）的预估相关性
Continent	`North America`, `Asia`	与受监控网络中检测到的可路由 IP 地址相关联的大陆
国家/地区	`Canada`, `Japan`	与受监控网络中检测到的可路由 IP 地址相关联的国家/地区
设备	`device1.example.com`, `192.168.1.3`	受监控网络中设备的名称或 IP 地址。
Event Classification	`Potential Corporate Policy Violation`, `Attempted Denial of Service`	入侵事件的简要说明，取决于触发该事件的规则、解码器或预处理程序的分类
Event Message	`dns response`, `P2P`	事件生成的消息，取决于触发该事件的规则、解码器或预处理程序
File Disposition	`Malware`, `Clean`	由云确定的文件性质，对于该文件，防御中心已执行恶意软件云查找
文件名	`Packages.bz2`	网络流量中检测到的文件的名称
File SHA256	任何 32 位字符串	文件的 SHA-256 哈希值，对于该文件，防御中心已执行恶意软件云查找
文件类型	`GZ`, `SWF`, `MOV`	网络流量中检测到的文件类型
File Type Category	`Archive`, `Multimedia`, `Executables`	网络流量中检测到的文件类型的一般类别
IP地址	`192.168.1.3`, `2001:0db8:85a3::0000/24`	IPv4 或 IPv6 地址、地址范围或地址块 请注意，搜索 IP 地址时可返回事件，其中，该地址为事件源或目标
影响级别	`Impact Level 1`, `Impact Level 2`	受监控网络上事件的预估影响
Inline Result	`dropped`, `would have dropped`	流量是否已丢弃，可能已丢弃或未被系统操作
IOC Category	`High Impact Attack`, `Malware Detected`	已触发危害表现 (IOC) 事件的类别

表 56-2　过滤器数据类型（续）

类型	示例值	定义
IOC Event Type	`exploit-kit, malware-backdoor`	与特定危害表现 (IOC) 相关联的标识符，指触发该标识符的事件
Malware Threat Name	`W32.Trojan.a6b1`	恶意软件威胁的名称
OS Name	`Windows, Linux`	操作系统的名称
操作系统版本	`XP, 2.6`	操作系统的特定版本
优先级	`high, low`	事件的预估紧急程度
Security Intelligence Category	`Malware, Spam`	危险流量的类别，取决于安全情报
Security Zone	`My Security Zone,Security Zone X`	一组接口，流量通过该接口进行分析并在内联部署中传递
SSL	`yes, no`	SSL 或 TLS 加密流量
用户	`wsmith, mtwain`	登录至受监控网络中主机的用户的身份

在 Filter 字段中，可以输入特殊搜索参数，例如，* 和 ! 作为事件搜索的重要参数。可创建排斥过滤器，只需将 ! 符号作为过滤器参数的前缀。有关 FireSIGHT 系统通常支持的搜索限制的详细信息，请参阅第 60-5 页上的在搜索中使用通配符和符号。

当多个过滤器活跃时，同一种数据类型的值被视为 OR 搜索条件：将出现至少与其中一个值相匹配的所有数据。不同数据类型的值被视为 AND 搜索条件：显示至少与每种过滤数据类型相匹配的数据。例如，为 `Application: 2channel`、`Application: Reddit` 和 `User: edickinson` 的过滤器集显示的数据必须与用户 `edickinson` **和** 应用`2channel` **或**应用 `Reddit` 相关联。

确认过滤器的数据类型和值后，过滤器构件出现在页面的左上角，显示新过滤器的数据类型和值。

由于可能想要先配置多个过滤器，然后再应用它们，并且，Context Explorer 可能需要时间完全重新加载所有部分，添加的过滤器将不自动应用。要应用过滤器，必须点击 **Apply Filters**。已配置但尚未应用的过滤器会逐渐消失。一次性最多可配置 20 个过滤器，此外，点击过滤器构件上的删除图标 (✖) 即可删除单个过滤器。如果要一次性删除所有过滤器，可点击 **Clear** 按钮。

请注意某些过滤器类型与其他类型不兼容：例如，与入侵事件相关的过滤器（例如，**Device** 和 **Inline Result**）无法与连接事件相关的过滤器（例如，**Access Control Action**）同时应用，因为系统无法按入侵事件数据对连接事件数据进行排序。系统将自动阻止同时应用不兼容过滤器；只要存在不兼容性，当一个过滤器类型最近被激活时，不兼容的过滤器会被隐藏。

请注意，显示的数据取决于您如何许可和部署受管设备、您是否配置了提供数据的功能，以及，如果是 2 系列设备，该设备是否支持提供数据的功能等因素。例如，因为 DC500 防御中心和 2 系列设备都不支持按类别和信誉进行 URL 过滤，所以，DC500 防御中心不能显示该功能的数据，且 2 系列设备也无法检测到该数据。

要从 Add Filter 窗口新建过滤器，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Context Explorer**。

系统将显示 Context Explorer。

步骤 2　在右上角的 **Filters** 项下方，点击加号图标 (✚)。

系统将显示 Add Filter 弹出窗口。

步骤 3　从 **Data Type** 下拉列表，选择要过滤的数据类型。

系统用该数据类型的示例值填充 Filter 字段。

步骤 4　在 **Filter** 字段中，键入要过滤的数据类型值。

步骤 5　点击 **OK**。

过滤器添加成功。系统重新显示 Context Explorer 以及相应的过滤器构件。

步骤 6　或者，请重复以上步骤添加更多的过滤器，直至添加完所需的过滤器集。请注意，由于 Context Explorer 不自动刷新，添加过滤器时，过滤器未应用。

步骤 7　点击 **Apply Filters**。

系统应用过滤器， Context Explorer 刷新以反映已过滤数据。

要删除过滤器，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击任何过滤器窗口构件上的删除图标 (✖)。

过滤器删除成功。

要清除所有过滤器，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击过滤器构件右侧的 **Clear** 按钮。

所有过滤器清除成功。

请注意，如果尚未创建过滤器，该按钮不显示。

用上下文菜单创建过滤器

许可证：FireSIGHT

浏览 Context Explorer 图形和列表数据时，可点击数据点，然后使用上下文菜单根据该数据快速创建一个过滤器 （包容性或排除性）。如用上下文菜单过滤“应用”、“用户”或“入侵事件消息”数据类型的信息，或任何单个主机，则过滤器构件包括一个构件信息图标，该图标链接至该数据类型 （例如应用数据的“应用详细信息”）的相关详细信息页面。请注意，不能过滤 URL 数据。

上下文菜单还可用于更详细地调查特定图形或列表数据。有关信息，请参阅第 56-38 页上的向下钻取 Context Explorer 数据。

要从上下文菜单创建一个过滤器，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Context Explorer**。

系统将显示 Context Explorer。

步骤 2　在资源管理器的任何部分（“随时间推移的流量和入侵事件”部分或包含 URL 数据的部分除外），点击要过滤的数据点。

系统在附近显示上下文菜单弹出窗口。

步骤 3　此时您有两种选择：

- 要为该数据添加一个过滤器，请点击 **Add Filter**。

  添加过滤器后，其构件显示在左上角。

- 要为该数据添加一个排除过滤器，请点击 **Add Exclude Filter**。应用的过滤器显示与排除值不关联的所有数据。

  添加过滤器后，其构件显示在左上角。排除过滤器的过滤器值之前显示一个感叹号。

要查看过滤器的详细信息，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在任何符合条件的过滤器构件上，点击信息图标 ( )。

系统打开一个新窗口，显示与该过滤器数据类型有关的详细信息页面。

用书签标示过滤器

许可证：FireSIGHT

过滤器用作一种简单、灵活的工具，可在任何指定时间获取准确的 FireSIGHT 数据上下文。过滤器不用作永久性配置设置，在离开 Context Explorer 或结束会话时会消失。但是，贵公司可能经常使用某些 Filter 组合。要保留过滤器设置供以后使用，可用已应用的首选过滤器创建 Context Explorer 的浏览器书签。由于已应用的过滤器已纳入 Context Explorer 页面 URL，加载该页面的书签也会加载相应的过滤器。

使用报告

FireSIGHT 系统提供一个灵活的报告系统，能够利用防御中心上显示的事件视图或控制面板快速而轻松地生成多部分报告。还可以从头设计自定义报告。只有在防御中心上可以生成报告。

报告是一种采用 PDF、 HTML 或 CSV 格式的文档文件，其包含要传达的内容。报告模板为报告及其各章节指定了数据搜索和格式。 FireSIGHT 系统内有一个功能强大的报告设计器，用于自动化报告模板的设计。可以复制网络界面中显示的任何活动视图表或控制面板图形的内容。

可以根据需要的数量创建报告模板。每个报告模板分别定义报告中的各个部分并指定创建报告内容的数据库搜索，以及演示文稿格式 （表、图表，详细视图等等）和时间范围。模板还指定文档属性，例如封面和目录以及文档页面是否有页眉和页脚 （仅适用于 PDF 格式的报告）。可以将报告模板导出到单个的配置包文件中，然后再导入，以便在其他防御中心上重复使用。

在模板中可以加入输入参数，以扩展其实用性。使用输入参数，可以对同一报告生成定制的变量。当使用输入参数生成报告时，生成过程会提示输入每个输入参数的值。键入的值仅限报告内容一次。例如，在生成入侵事件报告的搜索的目标 IP 字段中可以放入一个输入参数；当系统提示输入目标 IP 地址时，可以指定部门的网段。生成的报告随后只包含该特定部门的相关信息。

有关报告和报告模板的详细信息，请参阅：

了解报告模板

许可证：任何环境

利用 FireSIGHT 系统的报告功能，可以从防御中心中快速获取任何事件视图、控制面板或工作流程的内容，并以报告格式展现。使用报告模板定义报告的每个部分中的数据内容和格式，以及报告文件的文档属性 （封面、目录及页眉和页脚）。在生成报告之后，模板仍可重复使用，直到将其删除为止。

报告包含一个或多个信息部分。为每个部分分别选择格式 （文本、表或图表）。为部分选择的格式可能限制可包含的数据。例如，使用饼图格式，无法显示某些表中基于时间的信息。可以随时更改部分的数据条件或格式，以获得最佳演示效果。

可以在预定义的事件视图基础上完成报告的初始设计，也可以通过从任何定义的控制面板、工作流程或摘要导入内容开始设计。还可以从空的模板外壳开始添加部分并逐一定义其属性。

报告中的所有部分都有一个标题栏和控制部分内容和外观的各种属性字段。有关详情，请参阅：

- 报告部分标题栏元素表
- 报告部分字段表

下表说明每个模板部分的标题栏上的控件。

表 57-1　报告部分标题栏元素

属性	定义
部分标题	包含部分显示在报告中的名称。点击该名称并键入新名称可更改名称。为避免显示问题，在 Report Sections 页面上查看时，系统会截断长部分标题名称。
部分标题图标	点击复制图标 (+) 可将部分添加到报告模板。 点击最小化图标 (−) 可使部分最小化。 点击删除图标 (×) 可在确认后删除部分。

下表说明报告模板每个部分中的字段。

表 57-2　报告部分字段

字段名称	定义
表	显示一个下拉菜单，用于选择提取部分数据的表。
预设	显示预定义搜索的下拉菜单。在定义新的搜索时，可以选择合适的预设初始化搜索条件。
格式	提供用于选择部分数据格式的图标。选项包括： 柱形图：比较选定变量的数量。 折线图：显示选定变量随着时间变化的趋势/变化。仅适用于基于时间的表。 饼图：显示每个所选变量占总体的百分比。数量为零的变量不在图表中显示。极少的数量归到标记为 **Other** 的类别。 表视图：显示每个记录的属性值。不适用于摘要或统计数据。 详细视图：显示与特定事件相关联的复杂对象数据，例如数据包 （用于入侵事件）和主机配置文件 （用于主机事件）。格式仅适用于涉及此类对象的事件类型。如果请求的数量很大，输出可能会降低性能。
Search 或 Filter	显示搜索或应用过滤器的下拉菜单。 对于大多数表，可使用预定义的或保存的 **Search** 限制报告。还可以通过点击编辑图标 ( ) 来创建新搜索；请参阅第 57-16 页上的使用报告模板部分中的搜索。 对于 Application Statistics 表，使用用户定义的应用 **Filter** 限制报告；有关创建过滤器的信息，请参阅第 3-13 页上的使用应用过滤器。
X-Axis	为所选图表的 X 轴显示其可用数据列的下拉菜单。只有选择图表格式时才会显示。对于折线图，X 轴值始终是 **Time**。对于条形图和饼图，则不能选择 **Time** 为 X 轴值。
Y-Axis	为所选图表的 Y 轴显示其可用数据列的下拉菜单。
Section Description	定义在部分中的搜索数据前面的描述性文本。输入文本和输入参数组合。新部分的默认值是以下两个输入参数的集合：`$<Time Window>` 和 `$<Constraints>`。 有关输入参数的详细信息，请参阅第 57-16 页上的使用输入参数。

表 57-2　报告部分字段 （续）

字段名称	定义
Time Window	为部分中显示的数据定义时间段。如果部分搜索基于时间的表，可以选择复选框以继承报告的全局时间段。或者，可以为部分设置特定时间段。有关设置时间段的信息，请参阅第 57-11 页上的编辑报告模板的各部分。
成果	选择 **Top** 或 **Bottom** 并输入要在部分中包括的最大记录数量。
颜色	定义部分中图形数据的颜色。根据需要选择一个或多个颜色。

创建和编辑报告模板

许可证：任何环境

可以使用以下任一方法构建新的报告模板：

- 第 57-3 页上的新建报告模板
- 第 57-5 页上的根据现有模板创建报告模板
- 第 57-8 页上的从事件视图创建报告模板
- 第 57-9 页上的通过导入控制面板或工作流程创建报告模板

要修改和自定义报告模板，请参阅：

- 第 57-11 页上的编辑报告模板的各部分
- 第 57-16 页上的使用报告模板部分中的搜索
- 第 57-16 页上的使用输入参数
- 第 57-20 页上的编辑报告模板中的文档属性
- 第 57-21 页上的自定义封面
- 第 57-22 页上的管理徽标

新建报告模板

许可证：任何环境

如果不想复制现有报告模板，可以创建一个全新模板。首先，创建一个默认模板外壳。然后，按照希望的顺序设计各个模板部分并设置报告文档的属性。有关这些步骤的信息，请参阅：

- 第 57-3 页上的创建模板外壳
- 第 57-4 页上的配置模板部分的内容
- 第 57-5 页上的设置 PDF 和 HTML 报告文档属性

创建模板外壳

许可证：任何环境

报告模板是各部分的框架，每个部分通过自己的数据库查询独立构建。创建模板的第一步是生成用于添加部分并设置其格式的框架外壳。

要创建模板外壳，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　点击 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　点击 **Create Report Template**。

Report Sections 页面显示，在 **Report Title** 字段中显示默认模板名称 `New Report`。

步骤 4　或者，在 **Report Title** 字段中输入新模板的名称，然后点击 **Save**。报告标题可以包含字母数字字符和空格的任意组合。

在 Report Templates 页面列表上显示使用新模板名称的条目。

步骤 5　报告标题也可以包含输入参数。要添加输入参数，请将光标置于标题中应显示参数值的位置，然后点击插入输入参数图标 ( )。

添加的输入参数显示在 **Report Title** 字段中。有关输入参数的信息，请参阅第 57-16 页上的使用输入参数。

步骤 6　根据需要，使用 Report Sections 标题栏下的一组添加图标来插入部分框架。有关部分格式设置的信息，请参阅报告部分字段表。

每个已添加部分显示在模板的底部。将其拖放到正确的位置。

步骤 7　单击部分标题栏上的部分标题并键入部分名称 （最多使用 120 个字符）。

步骤 8　点击 **Save** 以保存模板。

模板保存完毕。

配置模板部分的内容

许可证：任何环境

每个模板部分均包括由搜索或过滤器生成的数据集，且具有确定展现方式的格式规格 （表，饼图等）。通过选择要在输出中包含的数据记录中的字段，以及要显示的时间范围和记录数量，进一步确定部分内容。

要配置报告模板部分，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　按照第 57-11 页上的编辑报告模板的各部分中的说明编辑部分属性。

步骤 2　或者，点击部分窗口底部的 **Preview**，查看所选择的列布局或图形格式

注　使用部分预览实用程序检查列选择和饼图颜色等输出特性。这并不能可靠地表明配置的搜索是正确的。

设置 PDF 和 HTML 报告文档属性

许可证：任何环境

从模板生成的报告具有多个覆盖所有部分和控制功能的文档属性，例如封面、页眉和页脚、页码等。

要设置报告文档的属性，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　点击 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　针对要用于生成报告的报告模板点击 **Edit**。

系统将显示模板的 Report Sections 页面。

步骤 4　点击 **Advanced**。

系统将显示 Advanced Settings 弹出窗口。

步骤 5　对于 PDF 或 HTML 格式的文档，请执行第 57-20 页上的编辑报告模板中的文档属性中说明的任务。

如果选择 CSV 作为文档格式，则不需要设置文档属性。

根据现有模板创建报告模板

许可证：任何环境

如果在现有模板中找到理想模型，则可以复制模板并编辑其属性以创建新报告模板。思科还提供了一组预定义的报告模板，显示在 **Reports Tab** 上的模板列表中。有关这些模板的属性的说明，请参阅第 57-6 页上的使用预定义报告模板。

要从现有模板创建报告模板，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　点击 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。有关思科提供的报告模板的信息，请参阅第 57-6 页上的使用预定义报告模板。

步骤 3　点击要作为模型复制的报告模板旁边的复制图标 ()。

复制的模板显示为新报告模板。

步骤 4　在 **Report Title** 字段中，输入用于新报告模板的名称。

步骤 5　点击 **Save**。

系统保存报告模板，然后在 Report Templates 页面上显示新报告模板的一个条目。

步骤 6　根据需要对模板进行更改。

有关定义模板各部分和文档属性的信息，请参阅：

- 第 57-11 页上的编辑报告模板的各部分
- 第 57-20 页上的编辑报告模板中的文档属性

使用预定义报告模板

许可证：任何环境

可以按原样使用以下预定义报告模板，编辑它们，也可以将这些模板作为基础创建自己的模板。

- Host Report: $<Host>
- User Report: $<User>
- Attack Report: Attack $<Attack SID>
- Malware Report
- FireSIGHT Report: $<Customer Name>
- Files Report

Host Report: $<Host>

Host Report: $<Host> 报告模板提供网络上特定主机的相关信息。此报告模板包含以下部分：

- 服务器应用
- 客户端应用
- 源自该主机的入侵事件
- 目标指向该主机的入侵事件
- 源自该主机的连接
- 目标指向该主机的连接
- 该主机的用户
- 该主机的白名单违规

User Report: $<User>

User Report: $<User> 报告模板提供网络上特定用户的相关信息。此报告模板包含以下部分：

- 此用户使用的客户端应用
- 此用户使用的网络应用
- 此用户使用的应用协议
- 此用户使用的应用的完整列表
- 源自此用户设备的入侵事件
- 目标指向此用户设备的入侵事件
- 源自此用户设备的连接
- 目标指向此用户设备的连接
- 此用户的主机

Attack Report: Attack $<Attack SID>

Attack Report: Attack $<Attack SID> 报告模板提供网络上特定攻击的相关信息。此报告模板包含以下部分：

- 有关此攻击的常规信息
- 攻击次数
- 发起攻击的设备数量
- 受到攻击的设备数量
- 此攻击的来源
- 此攻击的目标
- 此攻击的流量模式

Malware Report

Malware Report 报告模板提供网络和基于终端的恶意软件事件的相关信息。此报告模板包含以下部分：

- 恶意软件威胁数
- 随着时间推移而发生的威胁检测
- 传输恶意软件的应用协议
- 接收恶意软件的主机
- 发送恶意软件的主机
- 受恶意软件影响的用户
- 恶意软件入侵
- 被恶意软件感染的文件类型
- 引入恶意软件的应用
- 恶意软件事件的表视图

请注意，2 系列设备和 DC500 防御中心都不支持基于网络的恶意软件防护，这会影响检测后显示的数据。例如，仅管理 2 系列设备的 3 系列防御中心只能显示基于终端的恶意软件事件。

FireSIGHT Report: $<Customer Name>

FireSIGHT Report: $<Customer Name> 报告模板提供公司网络的总体信息。此报告模板包含以下部分：

- 按风险分类的应用流量摘要
- 低业务相关性的风险应用
- 风险应用的用户
- 匿名访问者和代理
- 典型高带宽应用
- 按总带宽分类的应用
- 访问敏感网络的主机
- 访问敏感网络的用户
- 敏感网络上的应用
- 与敏感网络相关的端口和协议
- 访问恶意 URL 的主机

- 访问恶意 URL 的用户
- 精细应用使用情况
- Web 应用
- 客户端应用
- 应用协议
- 网络浏览器版本
- 操作系统版本
- 整体用户活动
- 按影响分类的入侵事件
- 按影响分类的入侵事件 （拦截之后）
- 按应用分类的入侵事件
- 首要入侵事件
- 综合应用列表

Files Report

Files Report 报告模板提供受管设备按网络流量检测的文件的相关信息。此报告模板包含以下部分：

- 一段时间内的文件传输
- 文件传输使用的应用协议
- 文件性质
- 文件操作
- 接收文件的主机
- 发送文件的主机
- 传输文件的用户
- 文件类别
- 文件类型
- 文件名
- 文件事件的表视图

从事件视图创建报告模板

许可证：任何环境

在生成报告前，报告系统创建一个报告模板，您可以根据需要进行修改。可以添加更多部分、修改自动包含的部分和删除各部分。

要从事件视图创建报告模板，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在一个事件视图中填入想要在报告中显示的事件。为此，有多种方法可以实现：

- 使用事件搜索定义要查看的事件。有关使用事件搜索的详细信息，请参阅第 60-1 页上的搜索事件。

- 深入查找工作流程，直到在事件视图中获得相应的事件。有关工作流程的详细信息以及如何限制工作流程中的事件，请参阅第 58-1 页上的了解和使用工作流程。

步骤 2　从事件视图页面中，点击 **Report Designer**。

系统将显示 Report Sections 页面，提供已捕获工作流程中各视图的相应部分。

步骤 3　或者，在 **Report Title** 字段中键入新名称并点击 **Save**。

步骤 4　或者，点击部分标题栏中的删除图标 (✖) 删除要从报告中排除的任何模板部分，然后确认删除。

已删除的部分不再显示。

注　有些工作流程中，报告的最后部分包含显示数据包、主机配置文件或漏洞的详细视图，具体视工作流程而定。生成报告时使用这些详细视图检索大量事件，可能会影响防御中心的性能。

步骤 5　或者，在报告部分中调整字段的设置。

有关配置报告部分中的字段的详细信息，请参阅第 57-11 页上的编辑报告模板的各部分。

提示　要查看某一部分的当前列布局或图表格式，请点击该部分的 **Preview** 链接。

步骤 6　或者，点击标题栏中任一部分的标题以更改该部分的标题。

系统将显示 Set Section Title 弹出窗口。键入部分标题并点击 **OK**。

步骤 7　或者，添加分页符。点击添加分页符图标 ()。

新分页符对象将显示在模板的底部。将其拖动到应开始新页面的部分的前面。有关使用分页符的信息，请参阅第 57-11 页上的编辑报告模板的各部分。

步骤 8　或者，添加文本部分。点击添加文本部分图标 ()。

新的文本部分将显示在模板的底部。将其拖动到应在报告模板中显示的位置。有关编辑文本部分的信息，请参阅第 57-11 页上的编辑报告模板的各部分。

提示　文本部分支持富文本 （粗体、斜体，可变字号等）以及导入的图像，非常适用于报告或报告部分的介绍。

步骤 9　或者，点击 **Advanced Settings** 以添加封面、目录、开始页码或页眉和页脚文本。有关详细信息，请参阅第 57-20 页上的编辑报告模板中的文档属性。

步骤 10　报告模板正确时，点击 **Save**。

系统保存报告模板，然后在 Report Templates 页面上显示报告模板的一个条目。

通过导入控制面板或工作流程创建报告模板

许可证：任何环境

通过导入控制面板、工作流程和统计摘要，可以快速创建新的报告。导入为控制面板中的每个构件图形以及工作流程中的每个事件视图创建一个部分。为重点显示最重要的信息，可以删除任何不必要的部分。下表说明导入选项。

表 57-3　导入报告部分窗口上的数据源选项

选择此选项…	导入…
Import Dashboard	所选控制面板上的任何自定义分析构件。
Import Workflow	任何预定义或自定义的工作流。 **提示**　选项具有以下格式： 表 - 工作流程名称 例如，`Connection Events - Traffic by Port` 导入从 Connection Events 表生成的 Traffic by Port 工作流程中的视图。
Import Summary Sections	以下任意一种通用摘要： • 入侵详细摘要 • 入侵简要摘要 • 发现详细摘要 • 发现简要摘要

要从控制面板、工作流程或统计摘要创建报告模板，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　确定要在报告中复制的控制面板、工作流程或摘要。

步骤 2　选择 **Overview > Reporting**。

步骤 3　点击 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 4　点击 **Create Report Template**。

系统将显示 Report Sections 页面。

步骤 5　在 **Report Title** 字段中键入新报告模板的名称。

步骤 6　点击 **Save** 使用新名称保存报告模板。

系统保存报告模板，然后在 Report Templates 页面上显示报告模板的一个条目。

步骤 7　点击控制面板、摘要和工作流程图标 () 中的导入部分。

系统将显示 Import Report Sections 弹出窗口。可以选择在导入报告部分窗口上的数据源选项表中说明的任何数据源。

步骤 8　从下拉菜单中选择控制面板、工作流程或摘要。

步骤 9　对要添加的数据源，点击 **Import**。

模板的 Report Sections 页面再次显示，提供所选数据源的各元素的相应部分。对于控制面板，每个构件图形都有自己的部分；对于工作流，每个事件视图都有自己的部分。

步骤 10　根据需要更改部分的内容。

有关编辑报告模板的信息，请参阅第 57-11 页上的编辑报告模板的各部分。

注　有些工作流程中，报告的最后部分包含显示数据包、主机配置文件或漏洞的详细视图，具体视工作流程而定。生成报告时使用这些详细视图检索大量事件，可能会影响防御中心的性能。

步骤 11　报告模板正确时，点击 **Save**。

系统保存报告模板，然后在 Report Templates 页面上显示报告模板的一个条目。

编辑报告模板的各部分

许可证：任何环境

可以通过修改各种报告部分属性调整部分的内容及其数据展示。有关信息，请参阅：

- 第 57-11 页上的设置模板部分的表和数据格式。
- 第 57-12 页上的为模板部分指定搜索或过滤器。
- 第 57-13 页上的设置表格式部分中显示的搜索字段
- 第 57-13 页上的向报告模板添加文本部分
- 第 57-13 页上的向报告模板添加分页符
- 第 57-14 页上的设置模板及其部分的时间段
- 第 57-15 页上的重命名模板部分
- 第 57-15 页上的预览模板部分

注　安全分析人员仅可以编辑由其创建的报告模板。

设置模板部分的表和数据格式。

许可证：任何环境

报告模板中的各部分通过查询数据库表生成该部分的内容。更改部分的数据格式使用相同的数据查询，但会根据格式类型的分析用途修改部分中显示的字段。例如，入侵事件的表视图在部分中填入每个事件记录的大量数据字段，而饼图部分则显示各个选定属性代表的所有匹配记录的比例，不显示单个事件的详细信息。条形图部分比较具有特定属性的匹配记录总数。折线图就单个属性总结匹配记录随时间推移的变化。折线图仅适用于基于时间的数据，不适用于有关主机、用户和第三方漏洞等信息。

有关不同可用格式的信息，请参阅报告部分字段表。

要选择模板部分的表和输出格式，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　使用 **Table** 下拉菜单选择要在此部分中查询的表。

适用于所选表的每个输出格式的图标显示在 **Format** 字段中。

步骤 2　选择用于部分的输出格式图标。有关这些格式的信息，请参阅报告部分标题栏元素表。

系统将显示输出中包括的字段。

步骤 3　要更改搜索限制，请点击 **Search** 或 **Filter** 字段旁边的编辑图标 ( )。

Search Editor 弹出窗口显示，提供用于限制搜索的选项。有关使用此窗口的信息，请参阅第 57-16 页上的使用报告模板部分中的搜索。

步骤 4　对于图形输出格式（饼图、条形图等），请使用下拉菜单调整 **X-Axis** 和 **Y-Axis** 参数。

当为 X 轴选择值时，只有相对应的值才显示在 Y 轴下拉菜单中，反之亦然。

步骤 5　对于表输出，请在输出中选择列、显示顺序和排序顺序。有关详细信息，请参阅第 57-13 页上的设置表格式部分中显示的搜索字段。

步骤 6　点击 **Save** 以保存模板。

模板保存完毕。

为模板部分指定搜索或过滤器。

许可证：任何环境

报告部分中的搜索或过滤器指定部分内容所基于的数据库查询。对于大多数表，可以使用预定义或保存的搜索来限定报告，也可以随时创建新的搜索：

- 预定义的搜索作为示例用于搜索特定事件表，并可以对可能想要在报告中包含的重要网络信息提供快速访问。
- 保存的事件搜索包括您或他人已创建的全部公共事件搜索，以及所有保存的私密事件搜索。有关定义、命名和使用保存事件搜索的信息，请参阅第 60-1 页上的搜索事件。
- 只有在报告模板本身中才能实现当前报告模板的保存搜索。保存的报告模板搜索的搜索名称以字符串“Custom Search”结尾。用户在设计报告时创建这些搜索。

对于 Application Statistics 表，使用用户定义的应用过滤器限制报告；有关创建过滤器的信息，请参阅第 3-13 页上的使用应用过滤器。

要为模板部分指定搜索或过滤器，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　从 **Table** 下拉菜单中选择要查询的数据库表：

- 对于大多数表，显示 **Search** 下拉列表。
- 对于 Application Statistics 表，显示 **Filter** 下拉列表。

步骤 2　选择要用于限制报告的搜索或过滤器。

点击编辑图标 () 可查看搜索条件或创建新的搜索。有关详细信息，请参阅第 57-16 页上的使用报告模板部分中的搜索。

设置表格式部分中显示的搜索字段

许可证：任何环境

如果在部分中包括表数据，则可以选择要显示数据记录中的哪些字段。表中所有字段都可以包括或排除。选择实现报告用途的字段，然后进行相应的排列和排序。

要添加和删除表格式部分中的字段，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　对于表格式部分，请点击 **Fields** 字段参数旁边的编辑图标 ( )。

系统将显示 Table Field Selector 窗口。

步骤 2　或者，添加和删除字段，然后将字段图标拖放到所需的列顺序中。

步骤 3　或者，更改所有列的排序顺序。使用每个字段图标上的下拉列表设置排序顺序和优先级。

步骤 4　当字段按正确顺序排列且具有所需的排序特征时，点击 **OK**。

系统将显示 Report Sections 页面。

向报告模板添加文本部分

许可证：任何环境

可以向模板添加文本部分以提供自定义文本，例如，整个报告或各部分的简介。文本部分可包含使用多种字体大小和样式 （如粗体、斜体等）的富文本，以及输入参数和导入的图像。有关输入参数的信息，请参阅第 57-16 页上的使用输入参数。

要向报告模板添加文本部分，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击添加文本部分图标 ( )。

文本部分显示在模板的底部。

步骤 2　将新文本部分拖放到其在报告模板的指定位置。

步骤 3　或者，在文本部分前后添加分页符。有关分页符的信息，请参阅第 57-13 页上的向报告模板添加分页符。

步骤 4　或者，点击标题栏中文本部分的通用名，键入新名称。

步骤 5　在文本部分的正文中添加带格式的文本和图像。可以包括在生成报告时动态更新的输入参数。

步骤 6　完成时点击 **Save**。

模板保存完毕。

向报告模板添加分页符

许可证：任何环境

在模板中，可以在任何部分的前面或后面添加分页符。此功能尤其适用于多部分报告，其具有介绍各个部分的文本页面。

要添加分页符，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击添加分页符图标 ( )。

分页符显示在模板的底部。

步骤 2　将分页符拖放到部分前面或后面的指定位置。

步骤 3　为添加到模板的所有分页符重复操作上述过程。

设置模板及其部分的时间段

许可证：任何环境

报告模板的时间段定义模板的报告周期。包含基于时间的数据的报告模板 （例如，入侵或发现事件）具有全局时间段，默认情况下，模板中基于时间的部分创建时会继承该时间段。更改全局时间段会更改配置为继承全局时间段的部分的本地时间段。可以通过清除 **Inherit Time Window** 复选框来禁用单个部分的时间段继承。然后可以编辑本地时间段。

注　全局时间段继承仅适用于具有基于时间的表数据的报告部分，例如入侵事件和发现事件。对于报告网络资产 （主机和设备）和相关信息 （如漏洞）的部分，必须分别设置每个时间段。

要更改报告模板的全局时间段，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在 Report Templates 页面上，点击要编辑的报告模板旁边的编辑图标 ( )。

系统将显示 Report Sections 页面。

步骤 2　点击 **Generate**。

系统将显示 Generate Report 弹出窗口。

步骤 3　要修改全局时间段，请点击时间段图标 ( )。

系统将在新窗口中显示 Events Time Window 页面。有关使用此页面的信息，请参阅第 58-19 页上的设置事件时间限制。

步骤 4　完成后，点击 Events Time Window 上的 **Apply**。

系统将再次显示 Generate Report 弹出窗口，提供新的时间段。

步骤 5　点击 **Cancel** 返回到 Report Sections 页面，或点击 **OK** 生成报告。

报告的每个部分可以有不同的时间范围。例如，第一部分可能是一个月度摘要，而剩余部分则可深入提供周级别的详细信息。在这些情况下，单独设置部分级别的时间段。

要配置部分的本地时间段，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在模板的 Report Sections 页面上，清除部分的 **Inherit Time Window** 复选框 （若有）。

系统将显示本地部分时间段图标。

步骤 2　要更改部分的本地时间段，请点击时间段图标 ()。

系统将显示 Events Time Window 页面。有关使用此页面的信息，请参阅第 58-19 页上的设置事件时间限制。

注　包含统计表的数据的部分只能有滑动时间窗。

步骤 3　设置完新本地时间段时，点击 Events Time Window 上的 **Apply**。

步骤 4　点击 **Save**。

系统将显示 Report Sections 页面，以便进行进一步编辑。

重命名模板部分

许可证：任何环境

创建新模板时，添加的部分接收通用的部分名称，并且为指明其内容应对其重命名。

要重命名模板部分，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　点击部分页眉中的当前部分名称。

系统将显示 Set Section Title 弹出窗口。

步骤 2　为部分键入新名词 （最多使用 120 个字符）并点击 **OK**。

部分标题栏中的名称更改完毕。

预览模板部分

许可证：任何环境

预览功能显示表视图的字段布局和排序顺序以及图形的重要易读特征，如饼图颜色。

要预览模板部分，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　在编辑部分的任何时候，点击 **Preview** 即可预览部分。

系统将显示 Preview 弹出窗口。

步骤 2　点击窗口底部的 **OK** 关闭预览。

系统将显示 Report Sections 页面。

使用报告模板部分中的搜索

许可证：任何环境

生成成功报告的关键在于定义填入报告部分的搜索。 FireSIGHT 系统提供搜索编辑器，可查看报告模板中可用的搜索以及定义新的自定义搜索。

提示 在报告模板中创建的自定义搜索专用于创建其所在的模板。在事件查看器中可以创建在所有报告模板中可重用的搜索。在事件查看器中保存自定义搜索时，自定义搜索将在所有报告模板的 **Search** 下拉菜单中显示。有关使用事件查看器创建和保存自定义搜索的详细信息，请参阅第 60-1 页上的搜索事件。

要创建自定义搜索，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1 在报告模板的相关部分中，点击 **Search** 字段旁边的编辑图标 ( )。

Search Editor 页面显示，提供所选的要搜索的表。

步骤 2 或者，从 **Saved Searches** 下拉菜单中选择预定义的搜索。

下拉列表显示此表的所有可用预定义搜索，包括系统别和报告专属的预定义搜索。

步骤 3 在相应的字段中编辑搜索条件。对于某些字段，限制可以包含与事件搜索相同的运算符 （<、 <> 等）。有关搜索条件的语法，请参阅第 60-1 页上的搜索事件。

如果输入多个条件，搜索仅返回符合所有条件的记录。

步骤 4 或者，在显示输入参数图标 ( ) 的位置，可以从下拉菜单中插入输入参数，以代替键入限制值。有关在报告设计中使用输入参数的信息，请参阅第 57-16 页上的使用输入参数。

对于某些搜索字段，下拉菜单可能包含用户定义的受管对象而不是输入参数，或者同时包含两者。受管对象根据其类型具有不同图标，是可作为值在限制搜索中使用的系统配置变量。但是，它们不为随输入参数而出现的用户输入创建生成时间查询。有关受管对象的信息，请参阅第 3-1 页上的管理可重用对象。

注 在编辑报告搜索的限制时，系统根据以下名称保存已编辑的搜索：*section* `custom search`，其中 *section* 是部分标题栏中的名称，后跟字符串 `custom search`。要使保存的自定义搜索具有有意义的名称，请确保更改部分名称后再保存已编辑搜索。无法重命名已保存的报告搜索。

步骤 5 在搜索编辑器中完成字段修改时，请点击 **OK**。

Report Sections 页面再次显示，并且在部分的 **Search** 下拉菜单中显示新的预定义搜索。

使用输入参数

许可证：任何环境

在报告模板中可以使用输入参数，使报告可以在生成时自动更新。输入参数图标 ( ) 指示可处理其的字段。有两种输入参数：

- 预定义的 - 请参阅预定义的输入参数表
- 用户定义的 - 请参阅用户定义的输入参数类型表

预定义的输入参数

许可证：任何环境

预定义的输入参数由内部系统功能或配置信息解析。例如，在生成报告时，系统用当前日期和时间替换 $<Time> 参数。下表定义可供使用的参数。例如，在计划程序控制下自动生成的月度摘要报告的标题中加入 $<Month>。报告标题随后自动更新为正确的月份。

表 57-4　　预定义的输入参数

插入此参数…	…在模板中包括此信息：
$<Logo>	所选的上传徽标
$<Report Title>	报告标题
$<Time>	运行报告的日期和时间，粒度为一秒
$<Month>	当前月份
$<Year>	当前年份
$<System Name>	防御中心的名称
$<Model Number>	防御中心的型号
$<Time Window>	当前应用于报告部分的时间段
$<Constraints>	当前应用于报告部分的搜索限制

下表列出在 Report Templates 页面内可用于不同区域的有效输入参数。

表 57-5　　预定义的输入参数使用情况

参数	报告模板封面	报告模板报告标题	报告模板部分说明	报告模板文本部分	生成报告文件名	生成报告邮件主题、正文
$<Logo>	是	否	否	否	否	否
$<Report Title>	是	否	是	是	是	是
$<Time>	是	是	是	是	是	是
$<Month>	是	是	是	是	是	是
$<Year>	是	是	是	是	是	是
$<System Name>	是	是	是	是	是	是
$<Model Number>	是	是	是	是	是	是
$<Time Window>	否	否	是	否	否	否
$<Constraints>	否	否	是	否	否	否

用户定义的输入参数

许可证：任何环境

可以创建自己的输入参数，以便在部分搜索中作为限制使用。使用输入参数限制搜索，会指示系统在生成时从请求报告的人员那里收集值。这样，可以在生成时动态地定制报告显示特定数据子集，而无需更改模板。例如，可以为报告部分搜索的 **Destination IP** 字段提供输入参数。然后，当生成报告时，可以输入特定部门的 IP 网段，以仅获得该部门的数据。

提示　还可以在输入参数字段中输入 *，从而忽略限制。

还可以定义字符串类型输入参数，在报告的以下特定区域中添加动态文本，例如，邮件 （主题或正文）、报告文件名和文本部分。可以为不同部门个性化设置报告，具有自定义的报告文件名、邮件地址和邮件消息，使同一模板适用一切。

定义的每个输入参数均具有名称和类型。下表说明参数类型。

表 57-6　　用户定义的输入参数类型

将此参数类型…...	用于包含此数据的字段…...
Network/IP	CIDR 格式的任何 IP 地址或网段
应用	应用协议、客户端应用或网络应用的名称
Event Message	任何事件视图消息
设备	3D 设备 （防御中心或 FireSIGHT 系统受管设备）
用户名	用户身份，比如发起者用户和响应者用户
Number (VLAN ID, Snort ID, Vuln ID)	任何 VLAN ID、 Snort ID 或漏洞 ID
字符串	文本字段 （如应用或操作系统版本、注释或说明）

输入参数的类型确定可以使用其的搜索字段。按照用户定义的输入参数类型表中所述，只有在相应的字段中可以给定的类型。例如，定义为字符串类型的用户参数可插入文本字段，但不可插入接受 IP 地址的字段。

要为报告模板创建用户定义的输入参数，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　点击要编辑的模板的编辑图标 ( )。

系统将显示 Report Sections 页面。

步骤 4　点击 **Advanced**。

系统将显示 Advanced Settings 弹出窗口。

步骤 5　点击 Add Input Parameter 图标 ( )。

系统将显示 Add Input Parameter 弹出窗口。

步骤 6　在 **Name** 字段中键入参数名称并使用 **Type** 下拉菜单选择类型，然后点击 **OK**。

新参数将在 **Input Parameters** 菜单中显示。

步骤 7　重复上述步骤，直到所需的参数全部定义完成。

步骤 8　点击 **OK**。

为此模板保存新的输入参数，并且再次显示 Report Sections 页面。

如果重新使用报告模板，可以更改任何输入参数的名称和类型，以更好地反映新报告的目的。

要为报告模板编辑用户定义的输入参数，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　点击要编辑的模板的编辑图标 ( )。

系统将显示 Report Sections 页面。

步骤 4　点击 **Advanced**。

系统将显示 Advanced Settings 弹出窗口。 **Input Parameters** 部分列出报告模板的所有可用用户定义参数。

步骤 5　点击编辑图标 ( )。

系统将显示 Edit Input Parameter 弹出窗口。

步骤 6　在 **Name** 字段中更改参数名称并使用 **Type** 下拉菜单更改参数类型，然后点击 **OK**。

更改的参数在 **Input Parameters** 部分中显示。

步骤 7　重复上述步骤，直到所需的参数全部定义完成。点击 **OK**。

更改保存完毕，并再次显示 Report Sections。

要为报告模板删除用户定义的输入参数，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　点击要编辑的模板的编辑图标 ( )。

系统将显示 Report Sections 页面。

步骤 4　点击 **Advanced**。

系统将显示 Advanced Settings 弹出窗口。 **Input Parameters** 部分列出报告模板的所有可用用户定义参数。

步骤 5　点击输入参数旁边的删除图标 ( ) 并确认。

步骤 6　点击 **OK**。

输入参数删除完毕，并再次显示 Report Sections 页面。

使用输入参数可扩展搜索的实用性。输入参数指示系统在生成时从请求报告的人员那里收集值。这样，可以在生成时动态地限制报告显示特定数据子集，而无需更改搜索。例如，可以为深度提供部门级安全事件的报告部分的 **Destination IP** 字段提供输入参数。当生成报告时，可以输入特定部门的 IP 网段，以仅获得该部门的数据。

要使用用户定义的输入参数限制报告模板中的搜索，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　点击要编辑的模板的编辑图标 ( )。

系统将显示 Report Sections 页面。

步骤 4　在部分中点击 **Search** 字段旁边的编辑图标 ( )。

系统将显示 Search Editor 弹出窗口。可接受输入参数的字段标有输入参数图标 ( )。

步骤 5　点击字段旁边的输入参数图标 ( )，然后从下拉菜单中选择输入参数。用户定义的输入参数标有图标 ( )

输入参数显示在字段中。

注　定义的输入参数仅适用于与其参数类型匹配的搜索字段。例如，**Network/IP** 类型的参数仅适用于接受 CIDR 格式的 IP 地址或网段的字段。

步骤 6　添加完所有必要的输入参数时，点击 **OK**。

Report Sections 页面显示，提供更改的内容。

编辑报告模板中的文档属性

许可证：任何环境

在生成报告之前，可以设置影响报告外观的文档属性。这些属性包括可选封面和目录。对一些属性是否支持取决于所选的报告格式：PDF、HTML 或 CSV。下表提供有关格式对属性支持的详细信息。

表 57-7　　文档属性支持

属性	是否支持 PDF？	是否支持 HTML？	是否支持 CSV？
封面页	是，具有可选徽标和自定义外观	是，具有可选徽标和自定义外观	否
目录	是	是	否
页眉和页脚	是，在任意字段中均具有可选文本或徽标	否	否
自定义开始页码	是	否	否
不显示首页页码的选项	是	否	否

要设置 PDF 和 HTML 报告的文档属性，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　点击要编辑的报告模板的编辑图标 ( )。

系统将显示 Report Sections 页面。

步骤 4　点击 **Advanced**。

系统将显示 Advanced Settings 弹出窗口。

步骤 5　选择 **Include Cover Page** 添加封面。

步骤 6　点击 **Cover Page Design** 字段旁边的编辑图标 ( ) 编辑封面设计。

有关详细信息，请参阅第 57-21 页上的自定义封面。

步骤 7　选择 **Include Table of Contents** 添加目录。

步骤 8　使用三个 **Header** 和 **Footer** 字段的下拉列表配置页眉和页脚。从下拉菜单中选择页眉和页脚内容：徽标、日期和页码等。

如果选择 **Logo**，默认徽标图像显示在所选字段中。要更改默认徽标图像，请参阅第 57-22 页上的管理徽标。

步骤 9　在 **Page Number Start** 字段中，选择报告首页的页码。

选择 **Number First Page?**在封面后面的第一页上显示页码。如果选择，则封面没有页码。

步骤 10　点击 **OK**。

文档属性保存完毕，并再次显示 Report Sections 页面。

自定义封面

许可证：任何环境

可以自定义报告模板的封面。封面可包含使用多种字体大小和样式 （如粗体、斜体等）的富文本，以及输入参数和导入的图像。有关输入参数的信息，请参阅第 57-16 页上的使用输入参数。

要自定义报告模板封面，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Report Templates** 选项卡。

系统将显示 Report Templates 页面并显示模板列表。

步骤 3　点击报告模板的编辑图标 ( )。

系统将显示 Report Sections 页面。

步骤 4　点击 **Advanced**。

系统将显示 Advanced Settings 弹出窗口。

步骤 5　点击 **Cover Page Design** 旁边的编辑图标 ( )。

Edit Cover Page 窗口显示，展示默认封面设计。

步骤 6　在富文本编辑器中编辑封面设计。

步骤 7　点击 **OK**。

封面设计保存完毕，并再次显示 Advanced Settings 窗口。

管理徽标

许可证：任何环境

可以在防御中心上存储多个徽标，并将其与其他报告模板关联。在设计模板时设置徽标关联。如果导出模板，导出包会包含徽标。

有关可以将徽标插入报告的位置的信息，请参阅第 57-20 页上的编辑报告模板中的文档属性。

请参阅以下相关步骤以了解详细信息：

- 第 57-22 页上的添加新徽标
- 第 57-23 页上的更改报告模板的徽标
- 第 57-23 页上的删除徽标

添加新徽标

许可证：任何环境

上传到防御中心的徽标适用于该防御中心上的所有报告模板。徽标图像必须是 JPG 格式。

要将徽标添加到防御中心：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　点击要编辑的报告模板的编辑图标 ( )。

系统将显示 Report Sections 页面。

步骤 4　点击 **Advanced**。

系统将显示 Advanced Settings 弹出窗口。当前与模板相关联的徽标显示在 **General Settings** 中的 **Logo** 下。

步骤 5　点击徽标的编辑图标 ( )。

Select Logo 窗口显示，提供当前已上传的徽标图像。

步骤 6　点击 **Upload Logo**。

系统将显示 Upload Logo 弹出窗口。

步骤 7　执行以下一项操作选择要上传的徽标：

- 输入徽标文件的位置
- 点击 **Browse** 按钮并浏览至文件的位置

步骤 8　点击 **Upload**。

将图像上传到防御中心并显示在 Select Logo 弹出窗口中。

步骤 9　或者，选择新徽标并点击 **OK** 将其与当前模板相关联。

Advanced Settings 窗口再次显示，提供相关联的徽标图像。

更改报告模板的徽标

许可证：任何环境

可以将报告中的徽标更改为上传到防御中心的任何 JPG 图像。例如，如果重复使用模板，可以将另一个公司的徽标与报告关联。

要更改报告模板的徽标，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　点击要编辑的报告模板的编辑图标 ( )。

系统将显示 Report Sections 页面。

步骤 4　点击 **Advanced**。

系统将显示 Advanced Settings 弹出窗口。当前与模板相关联的徽标显示在 **General Settings** 中的 **Logo** 下。

步骤 5　点击徽标的编辑图标 ( )。

Select Logo 窗口显示，提供当前已上传的徽标图像。

步骤 6　选择要与报告模板关联的徽标。

突出显示所选徽标。

步骤 7　点击 **OK**。

Advanced Settings 窗口再次显示，提供相关联的徽标图像。

删除徽标

许可证：任何环境

可以从防御中心删除徽标。删除徽标会从使用其的所有模板删除徽标。删除操作无法撤消。

请注意，无法删除预定义的思科徽标。

要从防御中心删除徽标，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　点击要编辑的报告模板的编辑图标 ( )。

系统将显示 Report Sections 页面。

步骤 4　点击 **Advanced**。

系统将显示 Advanced Settings 弹出窗口。当前与模板相关联的徽标显示在 **General Settings** 中的 **Logo** 下。

步骤 5　点击徽标的编辑图标 ( )。

Select Logo 窗口显示，提供当前已上传的徽标图像。

步骤 6　选择要删除的徽标。

突出显示所选徽标。

步骤 7　点击 **Delete Logo**。

已删除的徽标不在 Select Logo 弹出窗口中显示。

步骤 8　点击 **OK**。

更改保存完毕，并再次显示 Advanced Settings 窗口。

生成并查看报告

许可证：任何环境

创建并自定义报告模板后便可生成报告了。在生成过程中，可以选择报告格式（HTML、PDF 或 CSV）。还可以调整报告的全局时间段，它对所有部分应用一致的时间范围，但您排除的时间范围除外。有关设置报告时间段的信息，请参阅第 57-14 页上的设置模板及其部分的时间段。

如果报告模板的搜索规格中包括用户输入参数，生成过程会提示输入值，将报告的这次运行定制为数据的一个子集。有关输入参数的信息，请参阅第 57-16 页上的使用输入参数。

Reports 选项卡列出所有以前生成的报告，提供报告名称、生成日期和时间、生成用户以及报告是在本地还是远程存储的信息。状态栏指示报告是已生成，处于生成队列中 （例如，对于计划任务）还是无法生成 （例如，由于磁盘空间不足）。

Reports 选项卡页面显示所有本地存储的报告。如果当前配置了远程存储，该页面也显示远程存储的报告。当前配置的报告存储位置显示在页面的底部，提供本地、 NFS 和 SMB 存储的磁盘使用量。如果使用 SSH 访问远程存储，则不提供磁盘使用量的数据。有关设置远程存储的信息，请参阅第 57-27 页上的为报告使用远程存储。

注　如果在远程存储后又切换回本地存储，则远程存储中的报告不在 Reports 选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

在 PDF 报告中不支持使用 Unicode (UTF - 8) 字符的文件名。如果生成 PDF 格式的报告，包含特殊 Unicode 文件名的任何报告部分 （例如，文件或恶意活动中显示的那些文件名）以转换形式显示这些文件名。

如已配置 DNS 服务器且启用 IP 地址解析，则当解析成功时，报告包含主机名。有关详细信息，请参阅第 64-8 页上的配置管理接口和第 71-3 页上的事件首选项。

执行以下操作步骤生成和查看报告。请注意，具有管理员访问权限的用户可以查看所有报告；其他用户只能查看自己所生成的报告。有关管理报告文件的信息，请参阅第 57-30 页上的下载报告和第 57-30 页上的删除报告。

要从报告模板生成报告，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　点击 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　对要使用的模板点击其生成报告图标 ( )。

系统将显示 Generate Report 弹出对话框。

步骤 4　或者，在 **File Name** 字段中键入新名称。这会设置已生成报告文件的名称。也可使用输入参数图标 ( ) 向文件名添加一个或多个输入参数。有关输入参数的信息，请参阅第 57-16 页上的使用输入参数。

步骤 5　点击相应的图标，选择报告的输出格式：HTML、 PDF 或 CSV。

步骤 6　或者，点击时间段图标 ( ) 以更改全局时间段。

系统将显示 Events Time Window 弹出窗口。有关设置事件时间段的信息，请参阅第 58-19 页上的设置事件时间限制。

注　只有当单个报告部分配置为继承全局设置时，设置全局时间段才会影响单个报告的内容。有关报告部分对全局时间段的继承的信息，请参阅第 57-14 页上的设置模板及其部分的时间段。

步骤 7　为 **Input Parameters** 部分中显示的任何字段键入值。

提示　通过在字段中键入 * 通配符，可以忽略用户参数。这会消除对搜索的用户参数限制。

步骤 8　或者，如果系统策略中配置了邮件中继主机，点击 **Email** 可在邮件生成时自动通过邮件传送报告。有关邮件传送功能的详细信息，请参阅第 57-26 页上的生成时通过邮件分发报告。

步骤 9　显示提示时，点击 **OK** 进行确认。

系统将显示 Report Generation Complete 弹出窗口，其中包括可查看报告的链接。

步骤 10　点击以下其中一项：

- 报告链接，打开新窗口显示报告，或者
- **OK**，返回 Report Section 页面，您可以在该页面修改报告设计。

最初生成后也可以查看已完成的报告。

步骤 11　或者，也可以管理您的报告文件。有关详细信息，请参阅第 57-30 页上的下载报告和第 57-30 页上的删除报告。

要查看生成的报告，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　点击 **Reports** 选项卡。

随即显示“报告”页面。

步骤 3　点击报告的名称。

本地主机上的默认程序在新窗口中打开报告。

步骤 4　查看完文档时，使用浏览器返回到 **Reports** 选项卡。

使用报告生成选项

许可证：任何环境

在生成报告时还有几个其他选项。可以自动计划报告生成、通过邮件发送报告以及远程存储生成的报告。有关详细信息，请参阅：

- 第 57-26 页上的使用计划程序生成报告
- 第 57-26 页上的生成时通过邮件分发报告
- 第 57-27 页上的为报告使用远程存储

使用计划程序生成报告

许可证：任何环境

可以使用计划 FireSIGHT 系统程序自动生成报告。可以在每日、每周和每月等全程时间范围上自定义计划。有关详细信息，请参阅第 62-7 页上的自动化生成报表。

如果还要使用调度程序分发邮件报告，必须在安排任务**之前**配置您的报告模板和邮件中继主机。有关详细信息，请参阅第 57-26 页上的生成时通过邮件分发报告和第 63-17 页上的配置邮件中继主机和通知地址。

生成时通过邮件分发报告

许可证：任何环境

从其模板生成报告时，可以选择将报告作为邮件附件自动发送到一组收件人。

注　必须具有适当配置的邮件中继主机，才能通过邮件传送报告。如果以前没有设置过邮件主机，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

要在生成时通过邮件发送报告，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　点击生成要使用的模板的生成报告图标 ( )。

系统将显示 Generate Report 弹出窗口。

步骤 4　展开窗口的 **Email** 部分。

步骤 5　在 **Email Options** 字段中，选择 **Send Email**。

步骤 6　在 **Recipient List**、 **CC** 和 **BCC** 字段中，键入用逗号隔开的收件人邮件地址。

步骤 7　在 **Subject** 字段中，键入邮件的主题。

提示　可以在 **Subject** 和邮件正文中提供输入参数，以动态生成邮件中的信息，例如时间戳或防御中心名称。有关详细信息，请参阅第 57-16 页上的使用输入参数。

步骤 8　根据需要在邮件正文中键入附函。可用的富文本功能包括各种字体、编号和项目符号列表等。

步骤 9　当 Generate Report 窗口中所有字段均正确时，点击 **OK** 进行确认。

系统会通过邮件分发生成的报告。可以在系统策略中的 **Email Notification** 下配置邮件的 From 地址。有关详细信息，请参阅第 63-1 页上的管理系统策略。

为报告使用远程存储

许可证：任何环境

可以配置报告系统，在配置的远程存储位置中放置新生成的报告文件。也可以将任何本地存储的报告转移到远程存储位置。

注　无法将远程存储的报告转移到本地存储。

要使用远程存储，必须先配置远程存储位置。配置完时，远程存储位置显示在报告列表的底部。位置提供的是 NFS 和 SMB 而不是 SSH 的已加载存储的当前磁盘使用量。有关配置信息，请参阅第 64-14 页上的管理远程存储。

要在生成报告时远程存储报告，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Reports** 选项卡。

随即显示“报告”页面。

步骤 3　选择页面底部的 **Enable Remote Storage of Reports** 复选框。

防御中心将新生成的报告存储在页面底部指示的远程位置。这些报告的 **Location** 列数据是 `Remote`。

可以按批量处理模式或单个地将本地存储的报告转移到远程存储位置。

要将生成的报告从本地转移到远程存储，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Reports** 选项卡。

随即显示“报告”页面。

步骤 3　选择要转移的报告旁边的复选框，然后点击 **Move**。

提示　选择页面左上角的复选框以转移页面上的所有报告。如果报告有多页，会再显示一个复选框，可以选择该复选框转移所有页面上的全部报告。

步骤 4　确认要转移报告。

报告转移完毕。

管理报告模板和报告文件

许可证：任何环境

除了创建和编辑模板之外，还可以执行以下模板管理任务：

- 第 57-28 页上的导出和导入报告模板
- 第 57-29 页上的删除报告模板

也可以为生成的报告文件执行以下管理任务：

- 第 57-30 页上的下载报告
- 第 57-30 页上的删除报告

导出和导入报告模板

许可证：任何环境

导出报告模板时生成的文件包含要在另一个防御中心上创建相同报告所需的所有必要数据。导出文件是专有 SFO 格式，包括：

- 报告模板，具有所有部分设计元素和文档属性
- 报告中使用的所有已保存搜索
- 报告中使用的所有图像
- 报告中使用的所有自定义表

将模板导入到另一个防御中心上后可能需要的唯一配置是自动报告生成计划。

注　导入和导出报告模板需要两个防御中心处于相同的软件版本级别。

要导出报告模板，请执行以下操作：

访问：管理

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　点击要导出的模板的导出图标 ( )。

系统生成一个带有 .sfo 扩展名的配置包文件，并打开 Opening Object 弹出窗口显示配置包的文件名。

步骤 4　选择 **Save file**，然后选择 **OK** 将文件保存到本地计算机。

步骤 5　可以将 .sfo 配置包的名称更改为更具描述性的名称，以方便使用。导入配置包时，不论其名称如何，导入防御中心都会为模板指定其在源防御中心上所具有的名称。

从防御中心导出的 SFO 文件包含将报告模板添加到另一个防御中心所需的所有元素。因此，导入过程仅要求将配置包上传到第二个防御中心并运行导入过程。

要导入报告模板，请执行以下操作：

访问：管理

步骤 1　选择 **System > Tools > Import/Export**。

Import/Export 页面显示，包含防御中心上的报告模板列表。

步骤 2　点击 **Upload Package**。

系统将显示 Package Name 页面。

步骤 3　此时您有两种选择：

- 键入要上传的配置包的路径。
- 点击 **Browse** 找到配置包。

步骤 4　点击 **Upload**。

配置列表的 **Report Template** 部分显示，展示要导入的模板。

步骤 5　选择模板旁边的复选框并点击 **Import**。

模板显示在目标防御中心的配置列表中。

删除报告模板

许可证：任何环境

报告模板始终列出在 Report Templates 选项卡上供重复使用，直到删除为止。请注意，无法删除思科提供的报告模板。

注　安全分析人员仅可删除由其创建的报告模板。

要删除报告模板，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Report Templates** 选项卡。

系统将显示 Report Templates 页面。

步骤 3　在要删除的模板旁边，点击删除图标 ( ) 并确认。

模板名称不在列表中显示。

下载报告

许可证：任何环境

可以将任何报告文件下载到本地计算机。由此，可以通过邮件发送报告，或者通过其他可用的手段以电子方式分发。有关如何在生成时通过邮件自动分发报告的信息，请参阅第 57-26 页上的生成时通过邮件分发报告。

要下载报告，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Reports** 选项卡。

随即显示“报告”页面。

步骤 3　选择要下载的报告旁边的复选框，然后点击 **Download**。

提示　选择页面左上角的复选框下载页面上的所有报告。如果报告有多页，会再显示一个复选框，可以选择该复选框下载所有页面上的全部报告。

步骤 4　根据浏览器提示下载报告。

如果选择多份报告，它们以单个 `.zip` 文件形式下载。

删除报告

许可证：任何环境

可以随时删除报告文件。此步骤会完全删除文件，并且无法恢复。尽管仍然有生成了报告的报告模板，但如果时间段已扩展或滑动，就可能难以重新生成特定报告文件。有关时间段的信息，请参阅第 57-11 页上的编辑报告模板的各部分。如果模板使用输入参数，重新生成可能也很困难。

有关使用输入参数的信息，请参阅第 57-16 页上的使用输入参数。

要删除报告，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Overview > Reporting**。

步骤 2　选择 **Reports** 选项卡。

随即显示“报告”页面。

步骤 3　选择要删除的报告旁边的复选框，然后点击 **Delete**。

提示　选择页面左上方的复选框删除页面上的所有报告。如果报告有多页，会再显示一个个复选框，可以选择该复选框删除所有页面上的全部报告。

步骤 4　确认删除。

报告删除完毕。

了解和使用工作流程

工作流程是防御中心网络界面中可供分析师用于评估系统生成的事件的定制系列的数据页面。防御中心提供三种类型的工作流程：

- *预定义工作流程*，此类工作流程是系统上安装的无法修改或删除的预设工作流程。
- *已保存自定义工作流程*，此类工作流程是可以修改或删除的预定义的自定义工作流程。
- *自定义工作流程*，此类工作流程是为特定需求创建和自定义的工作流程。

例如，分析入侵事件时，可以从专为任务创建的若干预定义工作流程中进行选择。

请注意，工作流程中显示的数据通常取决于多个因素，例如，如何许可和部署受管设备，是否配置提供数据的功能，以及在使用 2 系列设备和 用于 Blue Coat X-系列的思科 NGIPS的情况下设备是否支持数据提供功能。例如，由于 DC500 防御中心和 2 系列设备都不支持按类别和信誉进行 URL 过滤，因此 DC500 防御中心不显示此功能的数据，并且 2 系列设备不检测此数据。

有关使用预定义和自定义工作流程的详细信息，请参阅：

- 第 58-1 页上的工作流程的组件
- 第 58-13 页上的使用工作流程
- 第 58-34 页上的使用自定义工作流程

提示 还可以使用自定义工作流程作为事件报告的基础。有关详情，请参见第 57-1 页上的使用报告。

工作流程的组件

许可证：任何环境

工作流程可以包含若干类型的页面，如以下部分中所述。

表视图

表视图对应于工作流程所基于的数据库中的每个字段包含一列。

例如，发现事件的表视图包含 Time、 Event、 IP Address、 User、 MAC Address、 MAC Vendor、 Port、 Description 和 Device 列。

相反，服务器的表视图包含 Last Used、 IP Address、 Port、 Protocol、 Application Protocol、 Vendor、 Version、 Web Application、 Application Risk、 Business Relevance、 Hits、 Source Type、 Device 和 Current User 列。

向下钻取页面

向下钻取页面包含数据库中可用的列的子集。

例如，发现事件的向下钻取页面可能仅包含 IP Address、 MAC Address 和 Time 列。另一方面，入侵事件的向下钻取页面可能包含 Priority、 Impact Flag、 Inline Result 和 Message 列。

通常，向下钻取页面是在移至表视图页面之前用于将调查范围缩小到若干事件的中间页面。

图

基于连接数据的工作流程可以包含图页面，也称为*连接图*。

例如，连接图可能会显示列出了随时间推移系统检测到的连接数的曲线图。通常，连接图是类似于向下钻取页面的中间页面，用于缩小调查范围。有关详细信息，请参阅第 39-13 页上的使用连接图。

最终页面

工作流程的最终页面取决于工作流程所基于的事件的类型。

- 主机视图是基于应用、应用详情、发现事件、主机、危害表现 (IOC) 、服务器或任何类型的漏洞的工作流程的最终页面。通过从此页面查看主机配置文件，可以轻松查看与具有多个地址的主机关联的所有 IP 地址上的数据。有关详细信息，请参阅第 49-1 页上的使用主机配置文件。
- 用户详细信息视图是基于用户和用户活动的工作流程的最终页面。有关详细信息，请参阅第 50-55 页上的了解用户详细信息和主机历史记录。
- 漏洞详细视图是基于思科漏洞的工作流程的最终页面。有关详细信息，请参阅第 49-24 页上的查看漏洞细节。
- 数据包视图是基于入侵事件的工作流程的最终页面。有关详细信息，请参阅第 41-19 页上的使用数据包视图。

基于其他类型的事件 （例如，审核日志事件和恶意软件事件）的工作流程没有最终页面。

有关工作流程的详细信息，请参阅：

- 第 58-3 页上的比较预定义和自定义工作流程
- 第 58-3 页上的比较预定义表和自定义表的工作流程
- 第 58-3 页上的预定义入侵事件工作流程
- 第 58-5 页上的预定义恶意软件工作流程
- 第 58-6 页上的预定义文件工作流程
- 第 58-6 页上的预定义捕获文件工作流程
- 第 58-6 页上的预定义连接数据工作流程
- 第 58-7 页上的预定义安全情报工作流程
- 第 58-8 页上的预定义主机工作流程
- 第 58-8 页上的预定义危害表现工作流程
- 第 58-8 页上的预定义应用工作流程
- 第 58-9 页上的预定义应用详情工作流程
- 第 58-9 页上的预定义服务器工作流程
- 第 58-10 页上的预定义主机属性工作流程
- 第 58-10 页上的预定义发现事件工作流程
- 第 58-10 页上的预定义用户工作流程

比较预定义和自定义工作流程

许可证：任何环境

FireSIGHT 系统随附可用于分析事件及其收集的其他数据的*预定义*工作流程集（在后面各节中进行了描述）。

自定义工作流程是为满足贵公司的特有需求而创建的工作流程。创建自定义工作流程时，请选择工作流程所基于的事件（或数据库表）类型。在防御中心中，可以将自定义工作流程基于自定义表。还可以选择自定义工作流程包含的页面；自定义工作流程可以包含向下钻取页面、表视图页面和主机页面或数据包视图页面。

防御中心随附若干*已保存自定义工作流程*，这些工作流程基于也随附于防御中心的已保存自定义表。基于预定义表和自定义表的工作流程之间的差异在下一节比较预定义表和自定义表的工作流程中进行了描述。

比较预定义表和自定义表的工作流程

许可证：FireSIGHT

可以使用自定义表功能创建使用来自两种或多种类型的事件的数据的表。这有所帮助，因为可以例如创建将入侵事件数据与发现数据关联的表和工作流程，从而允许对影响关键系统的事件进行简单搜索。有关创建自定义表的信息，请参阅第 59-1 页上的使用自定义表。

默认情况下，每个自定义表都具有可用于查看与表关联的事件的工作流程。工作流程中的功能根据所使用的表类型而异。例如，基于入侵事件表的自定义表工作流程始终以数据包视图结尾。但是，基于发现事件的自定义表工作流程以主机视图结尾。

与基于预定义事件表的工作流程不同，基于自定义表的工作流程不具有指向其他类型的工作流程的链接。

预定义入侵事件工作流程

许可证：保护

下表描述 FireSIGHT 系统随附的预定义入侵事件工作流程。有关访问这些工作流程的信息，请参阅第 41-7 页上的查看入侵事件和第 41-14 页上的审核入侵事件。

表 58-1　预定义入侵事件工作流程

工作流程名称	说明
目的端口	由于目标端口通常绑定到应用，因此该工作流程可以帮助检测遭遇异常高的警报量的应用。Destination Port 列可以帮助识别不应存在于网络上的应用。 此工作流程以其中显示了与入侵事件关联的目标端口的页面开头，后跟其中显示了已生成的事件类型的页面。然后，可以看到事件信息的表视图（称为事件表视图），后跟其中显示了与每个事件关联的数据包的已解码内容的数据包视图。
Event-Specific	此工作流程提供两个有用的功能。频繁发生的事件可能指示： • 误报 • 蠕虫 • 配置错误的网络 偶尔发生的事件很可能指示针对性攻击和特别关注事项。 此工作流程以其中显示了已生成的事件类型的页面开头。然后，可以查看包含两个表的页面，一个表列出与事件关联的源 IP 地址，另一个表显示与事件关联的目标 IP 地址。工作流程中的最终页面为事件表视图和数据表视图。
Events by Priority and Classification	此工作流程按事件优先级列出事件及其类型，随之还列出一个表明每个事件已发生的次数的计数。 此工作流程以包含所列的每个事件的优先级、分类和计数的向下钻取页面开头。工作流程中的最终页面为事件表视图和数据表视图。
Events to Destinations	此工作流程提供受攻击主机 IP 地址和攻击性质的高级视图；在适用情况下，还可查看有关攻击中涉及的国家/地区的信息。 此工作流程以由成对的事件类型和目标 IP 地址组成的页面开头，该页面可用于调查哪些事件类型面向特定 IP 地址。工作流程中的最终页面为事件表视图和数据表视图。
IP-Specific	此工作流程显示哪些主机 IP 地址生成最多警报。事件数最多的主机面向公众并接收蠕虫类型流量（指示适合进行调整的位置），或者需要进一步调查以确定警报原因。具有最低计数的主机也有必要进行调查，因为它们可能是针对性攻击的对象。低计数还可指示主机可能不属于该网络。 此工作流程以其中显示了两个表的页面开头，一个表示与事件关联的源 IP 地址，另一个表示与事件关联的目标 IP 地址。下一页显示生成的事件类型。工作流程中的最终页面为事件表视图和数据表视图。
Impact and Priority	通过此工作流程，可以快速查找重大影响复发事件。报告的影响级别通过事件已发生的次数进行显示。使用此信息，可以识别复发最频繁的重大影响事件，此类事件可能指示攻击在网络上范围广泛。 此工作流程以其中显示了与每个事件关联的影响级别、优先级和计数的页面开头。接下来，系统将显示含有每个事件的源 IP 地址和目标 IP 地址的向下钻取页面。第二页上的事件按计数排序。工作流程中的最终页面为事件表视图和数据表视图。
Impact and Source	此工作流程可帮助识别进行中的攻击的源。报告的影响级别通过事件的关联源 IP 地址进行显示。例如，如果具有 1 级影响的事件重复来自同一源 IP 地址，则这些事件可能指示攻击者已识别易受攻击的系统并在针对这些系统。 此工作流程以其中显示了与每个事件关联的影响级别、源 IP 地址、优先级和计数的页面开头。在每个事件级别内，事件依次按计数和优先级排序。接下来，系统将显示含有每个事件的源 IP 地址和目标 IP 地址的向下钻取页面。第二页上的事件按计数排序。工作流程中的最终页面为事件表视图和数据表视图。

表 58-1　预定义入侵事件工作流程 （续）

工作流程名称	说明
Impact to Destination	可以使用此工作流程识别在易受攻击计算机上重复发生的事件，从而能够处理这些系统上的漏洞并停止进行中的任何攻击。 此工作流程以其中显示了与每个事件关联的影响级别、内联结果 （数据包已被丢弃还是本会被丢失）、目标 IP 地址、优先级和计数，目标 IP 地址、优先级和计数的页面开头。在每个事件级别内，事件依次按计数和优先级排序。接下来，系统将显示含有每个事件的源 IP 地址和目标 IP 地址的向下钻取页面。第二页上的事件按计数排序。工作流程中的最终页面为事件表视图和数据表视图。
源端口	此工作流程指示哪些服务器生成最多警报。可以使用此信息标识需要调整的方面，以及决定需要注意的服务器。 此工作流程以其中显示了与入侵事件关联的源端口的页面开头，后跟其中显示了已生成的事件类型的页面。工作流程中的最终页面为事件表视图和数据表视图。
Source and Destination	此工作流程识别共享高级警报的主机 IP 地址。列表顶部的对可能是误报，并可确定需要调整的方面。可以检查列表底部的对来查找针对性攻击、访问其不应访问的资源的用户或不属于该网络的主机。 此工作流程以其中显示了每个事件的源 IP 地址和目标 IP 地址的页面开头，后跟其中显示了已生成的事件类型的页面。工作流程中的最终页面为事件表视图和数据表视图。

预定义恶意软件工作流程

许可证：任何环境

受支持的设备：因功能而异

受支持的防御中心：因功能而异

下表描述防御中心中包含的预定义恶意软件工作流程。所有预定义恶意软件工作流程都使用恶意软件事件表视图。

请注意，由于 DC500 2 系列防御中心、 2 系列设备和 用于 Blue Coat X-系列的思科 NGIPS不支持高级恶意软件防护， DC500防御中心 不显示此功能的数据，并且 2 系列设备和 用于 Blue Coat X-系列的思科 NGIPS不检测此数据。

有关访问恶意软件事件的信息，请参阅第 40-14 页上的使用恶意软件事件。

表 58-2　预定义恶意软件工作流程

工作流程名称	说明
Malware Summary	此工作流程提供在网络流量中或由基于终端的 FireAMP 连接器检测到的恶意软件列表，按个别威胁分组。
Malware Event Summary	此工作流程提供不同恶意软件事件类型和子类型的快速细分。
接收恶意软件的主机	此工作流程提供已接收恶意软件的主机 IP 地址列表，按恶意软件文件的关联性质分组。
发送恶意软件的主机	此工作流程提供已发送恶意软件的主机 IP 地址列表，按恶意软件文件的关联性质分组。
引入恶意软件的应用	此工作流程提供已接收文件的主机 IP 地址列表，按这些文件的关联恶意软件性质分组。

预定义文件工作流程

许可证：保护

下表描述防御中心中包含的预定义文件事件工作流程。所有预定义文件事件工作流程都使用文件事件表视图。有关访问文件事件的信息，请参阅第 40-6 页上的使用文件事件。

表 58-3　预定义文件工作流程

工作流程名称	说明
File Summary	此工作流程提供不同文件事件类别和类型以及任何关联恶意软件性质的快速细分。
接收文件的主机	此工作流程提供已接收文件的主机 IP 地址列表，按这些文件的关联恶意软件性质分组。
发送文件的主机	此工作流程提供已发送文件的主机 IP 地址列表，按这些文件的关联恶意软件性质分组。

预定义捕获文件工作流程

许可证：恶意软件

受支持的设备：因功能而异

受支持的防御中心：因功能而异

下表描述防御中心中包含的预定义捕获文件工作流程。所有预定义捕获文件工作流程都使用捕获文件表视图。

请注意，由于 DC500 2 系列防御中心、 2 系列设备和 用于 Blue Coat X-系列的思科 NGIPS不支持高级恶意软件防护， DC500防御中心 不显示此功能的数据，并且 2 系列设备和 用于 Blue Coat X-系列的思科 NGIPS不检测此数据。

有关访问捕获文件的信息，请参阅第 40-25 页上的使用捕获的文件。

表 58-4　预定义捕获文件工作流程

工作流程名称	说明
Captured File Summary	此工作流程根据类型、类别和威胁评分提供捕获文件的细分。
Dynamic Analysis Status	此工作流程根据是否已提交捕获文件进行动态分析来提供此类文件的计数。

预定义连接数据工作流程

许可证：FireSIGHT

下表描述防御中心中包含的预定义连接数据工作流程。所有预定义连接数据工作流程都使用连接数据表视图。有关访问连接数据的信息，请参阅第 39-12 页上的查看连接和安全情报数据。

表 58-5　预定义连接数据工作流程

工作流程名称	说明
Connection Events	此工作流程提供基本连接和检测到的应用信息的摘要视图，然后可以使用该视图向下钻取到事件表视图。
按应用划分的连接	此工作流程包含从检测到的连接数来看监控网段上 10 个最活跃应用的图形。

表 58-5　预定义连接数据工作流程 （续）

工作流程名称	说明
Connections by Initiator	此工作流程包含从连接数来看监控网段上 10 个最活跃的发起了连接事务的主机 IP 地址的图形。
按端口划分的连接	此工作流程包含从检测到的连接数来看监控网段上 10 个最活跃端口的图形。
Connections by Responder	此工作流程包含从连接数来看监控网段上 10 个最活跃的主机 IP 为连接事务中的响应方的主机 IP 地址的图形。
随时连接	此工作流程包含某个时间跨度的监控网段上的连接总数的图形。
按应用划分的流量	此工作流程包含从传输的数据量来看监控网段上 10 个最活跃应用的图形。
Traffic by Initiator	此工作流程包含从每个地址传输的总数据量来看监控网段上 10 个最活跃主机 IP 地址的图形。
按端口划分的流量	此工作流程包含从传输的数据量来看监控网段上 10 个最活跃端口的图形。
Traffic by Responder	此工作流程包含从每个地址接收的总数据量来看监控网段上 10 个最活跃主机 IP 地址的图形。
一段时间内的流量	此工作流程包含某个时间跨度的监控网段上传输的总数据量的图形。
Unique Initiators by Responder	此工作流程包含从已联系每个地址的唯一发起方数量来看监控网段上 10 个最活跃响应主机 IP 地址的图形。
Unique Responders by Initiator	此工作流程包含从已联系地址的唯一响应方数量来看监控网段上 10 个最活跃发起主机 IP 地址的图形。

预定义安全情报工作流程

许可证：保护

受支持的设备：任何防御中心，除了 2 系列

受支持的防御中心：除 DC500 外的所有型号

下表描述 防御中心 中包含的预定义安全情报工作流程。所有预定义安全情报工作流程都使用安全情报事件表视图。有关访问安全情报事件数据的详细信息，请参阅第 39-12 页上的查看连接和安全情报数据。

表 58-6　预定义安全情报 工作流程

工作流程名称	说明
Security Intelligence Events	此工作流程提供基本安全情报和检测到的应用信息的摘要视图，然后可以使用该视图向下钻取到事件表视图。
Security Intelligence Summary	此工作流程与 Security Intelligence Events 工作流程相同，但是以其中仅按类别和计数列出了安全情报事件的 Security Intelligence Summary 页面开头。

预定义主机工作流程

许可证：FireSIGHT

下表描述可与主机数据配合使用的预定义工作流程。

表 58-7　　预定义主机工作流程

工作流程名称	说明
主机	此工作流程包含主机表视图，后跟主机视图。通过基于 Hosts 表的工作流程视图可轻松查看与主机关联的所有 IP 地址上的数据。有关详情，请参见第 50-17 页上的查看主机。
Operating System Summary	可以使用此工作流程分析网络上正在使用中的操作系统。此工作流程提供以网络上的操作系统和操作系统供应商的列表开头，后跟运行该操作系统的各版本的主机数的一系列页面。下一页按关键性、 IP 地址和 NetBIOS 名称以及主机的关联操作系统和操作系统供应商列出主机。此工作流程以主机表视图后跟主机视图结尾。有关详情，请参见第 50-17 页上的查看主机。

预定义危害表现工作流程

许可证：FireSIGHT

下表描述可与 IOC （危害表现）数据配合使用的预定义工作流程。

表 58-8　　预定义危害表现 工作流程

工作流程名称	说明
危害表现	此工作流程以按计数和类别分组的 IOC 数据的摘要视图开头，后跟按事件类型进一步细分摘要数据的详细视图。接下来是 IOC 数据的完整表视图。该工作流程以主机视图结尾。有关查看和解释 IOC 数据的详细信息，请参阅第 50-28 页上的使用危害表现。
按主机划分的危害表现	可以使用此工作流衡量网络上哪些主机最可能受损 （基于 IOC 数据）。此工作流程包含按 IOC 数据计数分组的主机 IP 地址视图，后跟 IOC 数据表视图并以主机视图结尾。有关查看和解释 IOC 数据的详细信息，请参阅第 50-28 页上的使用危害表现。

预定义应用工作流程

许可证：FireSIGHT

下表描述可与应用数据配合使用的预定义工作流程。

表 58-9　　预定义应用工作流程

工作流程名称	说明
Application Business Relevance	可以使用此工作流程分析网络上正在运行的各估算业务相关性级别的应用，从而能够监控网络资源的相应使用。此工作流程以运行各相关性级别的应用的主机的计数开头，后跟带有其业务相关性级别和主机计数的单个应用的表、应用表视图和主机视图。有关详情，请参见第 50-36 页上的查看应用。
Application Category	可以使用此工作流程分析网络上正在运行的各类别的应用 （如邮件、搜索引擎或社交网络），从而能够监控网络资源的相应使用。此工作流程以运行各类别的应用的主机的计数开头，后跟运行单个应用的主机的计数、应用表视图和主机视图。有关详情，请参见第 50-36 页上的查看应用。

表 58-9　预定义应用工作流程 （续）

工作流程名称	说明
Application Risk	可以使用此工作流程分析网络上正在运行的各估算安全风险级别的应用，从而能够估算用户活动的潜在风险并采取相应措施。此工作流程以运行各风险级别的应用的主机的计数开头，后跟带有其业务相关性级别和主机计数的单个应用的表、应用表视图和主机视图。有关详情，请参见第 50-36 页上的查看应用。
Application Summary	可以使用此工作流程获取有关网络上的应用和关联主机的详细信息，从而能够仔细检查主机应用活动。此工作流程以运行应用的单个主机 IP 地址的列表开头，后跟应用表视图和主机视图。
应用	可以使用此工作流程分析网络上正在运行的应用，从而能够大致了解网络的使用方式。此工作流程以运行单个应用的主机的计数开头，后跟应用表视图和主机视图。有关详情，请参见第 50-36 页上的查看应用。

预定义应用详情工作流程

许可证：FireSIGHT

下表描述可与应用详情和客户端数据配合使用的预定义工作流程。

表 58-10　预定义应用详情工作流程

工作流程名称	说明
Application Details	可以使用此工作流程更详细地分析网络上的客户端应用。此工作流程包含以网络上的客户端应用和应用产品列表以及运行各应用的主机数的计数开头的一系列页面。然后，可以查看运行该应用程序的各版本的主机数。通过下一页可识别在特定主机上对哪些应用的访问最频繁。然后，工作流程提供客户端应用表视图，后跟主机视图。有关详情，请参见第 50-40 页上的查看应用详情。
客户端	此工作流程包含客户端应用表视图，后跟主机视图。有关详情，请参见第 50-40 页上的查看应用详情。

预定义服务器工作流程

许可证：FireSIGHT

下表描述可与服务器数据配合使用的预定义工作流程。

表 58-11　预定义服务器工作流程

工作流程名称	说明
Network Applications by Count	可以使用此工作流程分析网络上最频繁使用的应用。此工作流程包含其中显示了应用及出现各应用的主机计数，然后添加各应用的供应商和版本的一系列页面。然后，工作流程以列出了每个主机的应用的表视图后跟主机视图结尾。有关详情，请参见第 50-32 页上的查看服务器。
Network Applications by Hit	可以使用此工作流程分析网络上最活跃的应用。此工作流程包含其中显示了应用及各应用受访频率的计数，然后添加各应用的供应商和版本信息的一系列页面。然后，工作流程以一个包含列出了每个主机的应用的表视图后跟主机视图的页面结尾。有关详情，请参见第 50-32 页上的查看服务器。
Server Details	可以使用此工作流程详细分析检测到的服务器应用协议的供应商和版本。此工作流程包含与其供应商关联的服务器列表，后跟与供应商和版本均相关的服务器列表，并以服务器表视图和主机视图结尾。
服务器	此工作流程包含应用表视图，后跟主机视图。有关详情，请参见第 50-32 页上的查看服务器。

预定义主机属性工作流程

许可证：FireSIGHT

下表描述可与主机属性数据配合使用的预定义工作流程。

表 58-12　预定义主机属性工作流程

工作流程名称	说明
Attributes	可以使用此工作流程监控网络上主机的 IP 地址和主机状态。此工作流程以列出了单个 IP 地址及当前用户、主机重要性、注释和白名单合规性的主机属性表视图开头。它以主机视图结尾。有关详细信息，请参阅第 50-24 页上的查看主机属性。

预定义发现事件工作流程

许可证：FireSIGHT

下表描述可与发现事件数据配合使用的预定义工作流程。

表 58-13　预定义发现事件工作流程

工作流程名称	说明
Discovery Events	此工作流程以表视图形式提供发现事件的详细列表，后跟主机视图。有关详细信息，请参阅第 50-14 页上的了解发现事件表。

预定义用户工作流程

许可证：FireSIGHT

下表描述防御中心中包含的预定义用户工作流程。

表 58-14　预定义用户工作流程

工作流程名称	说明
用户	此工作流程提供从用户事件或从 LDAP 服务器连接收集的用户信息列表。有关用户身份工作流程的详细信息，请参阅第 50-53 页上的查看用户。

预定义漏洞工作流程

许可证：FireSIGHT

下表描述防御中心中包含的预定义漏洞工作流程。

表 58-15　预定义漏洞工作流程

工作流程名称	说明
漏洞	可以使用此工作流程审查其中显示了数据库中所有漏洞的漏洞表视图，然后审查仅含应用于网络上检测到的主机的活动漏洞的表视图。此工作流程以漏洞详细视图结尾，其中包含满足限制的每个漏洞的详细描述。有关详细信息，请参阅第 50-44 页上的查看漏洞。

预定义第三方漏洞工作流程

许可证：FireSIGHT

下表描述防御中心中包含的预定义第三方漏洞工作流程。

表 58-16　预定义第三方漏洞工作流程

工作流程名称	说明
Vulnerabilities by IP Address	可以使用此工作流程快速了解监控网络上每个主机 IP 地址检测到的第三方漏洞数量。此工作流程以第三方漏洞表视图后跟主机视图结尾。有关详细信息，请参阅第 50-48 页上的查看第三方漏洞。
Vulnerabilities by Source	可以使用此工作流程快速了解每个第三方漏洞源 （如 QualysGuard 扫描程序）检测到的第三方漏洞数量。此工作流程提供有关中间向下钻取页面上的漏洞的一些详细信息，然后以第三方漏洞表视图和主机视图结尾。有关详细信息，请参阅第 50-48 页上的查看第三方漏洞。

预定义相关性和白名单工作流程

许可证：FireSIGHT

各类型的相关性数据、白名单事件、白名单违例和修复状态事件具有对应的预定义工作流程。

表 58-17　预定义关联工作流程

工作流程名称	说明
Correlation Events	此工作流程包含关联事件表视图。有关详情，请参见第 51-48 页上的使用关联事件。
White List Events	此工作流程包含白名单事件表视图。有关详情，请参见第 52-26 页上的处理白名单事件。
Host Violation Count	此工作流程提供列出了违反至少一个白名单的所有主机 IP 地址的一系列页面。第一页根据每个地址的违例数对地址进行排序，其中违例数最多的 IP 地址位于列表顶部。如果主机 IP 地址违反多个白名单，则对应于每个违例的白名单存在单独的一行。此工作流程还包含列出了所有违例的白名单违例表视图，其中最新检测到的违例位于列表顶部。该表中的每一行都包含一个检测到的违规事件。有关详情，请参见第 52-30 页上的处理白名单的违规事件。
White List Violations	此工作流程包含列出了所有违例的白名单违例表视图，其中最新检测到的违例位于列表顶部。该表中的每一行都包含一个检测到的违规事件。有关详情，请参见第 52-30 页上的处理白名单的违规事件。
状态	此工作流程包含修复状态表视图，其中包括违反的策略的名称以及应用的修复的名称和状态。有关详情，请参见第 54-15 页上的处理补救状态事件。

预定义系统工作流程

许可证：任何环境

FireSIGHT 系统随附一些其他工作流程，包括系统事件 （如审核事件和运行状况事件），以及列出了规则更新导入和活动扫描的结果的工作流程。

表 58-18　其他预定义工作流程

工作流程名称	说明
审核日志	此工作流程包含列出了审核事件的审核日志表视图。有关详情，请参见第 69-2 页上的查看审计记录。
Health Events	此工作流程显示运行状况监控策略所触发的事件。有关详情，请参见第 68-46 页上的处理运行状况事件表视图。
规则更新导入日志	此工作流程包含列出了有关成功和失败规则更新导入的信息的表视图。有关详细信息，请参阅第 66-13 页上的导入规则更新和本地规则文件。
Scan Results	此工作流程包含列出了已完成的各扫描的表视图。有关详细信息，请参阅第 47-17 页上的处理主动扫描结果。

已保存自定义工作流

许可证：保护 + FireSIGHT

除无法修改的预定义工作流程以外，防御中心包含若干已保存自定义工作流程。其中每个工作流程基于自定义表，并且可以修改。有关访问这些工作流程的信息，请参阅第 59-8 页上的根据自定义表查看工作流程。

表 58-19　已保存自定义工作流程

工作流程名称	说明
Events by Impact, Priority, and Host Criticality	可以使用此工作流程快速选取并关注对于网络重要、当前易受攻击和当前可能受攻击的主机。 默认情况下，此工作流程以依次按影响级别、主机重要性和事件发生次数排序的事件摘要开头。可以使用工作流程的第二页向下钻取和查看发生特定事件的源地址和目标地址。此工作流程以 Intrusion Events with Destination Criticality 表视图后跟数据包视图结尾。此工作流程基于 Intrusion Events with Destination Criticality 自定义表。有关详细信息，请参阅第 59-1 页上的了解自定义表。
Events by Priority and Classification	此工作流程按事件优先级列出事件及其类型，随之还列出一个表明每个事件已发生的次数的计数。 此工作流程以包含所列的每个事件的优先级、分类和计数的向下钻取页面开头。工作流程中的最终页面为事件表视图和数据表视图。此工作流程基于 Intrusion Events 自定义表。有关详细信息，请参阅第 59-1 页上的了解自定义表。
Events with Destination, Impact, and Host Criticality	可以使用此工作流程查找对于网络重要且当前易受攻击的主机上的最新攻击。 默认情况下，此工作流程以按影响级别排序的最新事件列表开头。此工作流程的下一页提供 Intrusion Events with Destination Criticality 表视图，后跟数据包视图。此工作流程基于 Intrusion Events with Destination Criticality 自定义表。有关详细信息，请参阅第 59-1 页上的了解自定义表。
Hosts with Servers Default Workflow	可以使用此工作流程快速查看 Hosts with Servers 自定义表中的基本信息。 默认情况下，此工作流程以具有服务器的主机的表视图开头，后跟主机视图。此工作流程基于 Hosts with Servers 自定义表。有关详细信息，请参阅第 59-1 页上的了解自定义表。

表 58-19　已保存自定义工作流程（续）

工作流程名称	说明
Intrusion Events with Destination Criticality Default Workflow	可以使用此工作流程快速查看 Intrusion Events with Destination Criticality 自定义表中的基本信息。 默认情况下，此工作流程以 Intrusion Events with Destination Criticality 表视图开头，后跟数据包视图。此工作流程基于 Intrusion Events with Destination Criticality 自定义表。有关详细信息，请参阅第 59-1 页上的了解自定义表。
Intrusion Events with Source Criticality Default Workflow	可以使用此工作流程快速查看 Intrusion Events with Source Criticality 自定义表中的基本信息。 默认情况下，此工作流程以 Intrusion Events with Source Criticality 表视图开头，后跟数据包视图。此工作流程基于 Intrusion Events with Source Criticality 自定义表。有关详细信息，请参阅第 59-1 页上的了解自定义表。
Server and Host Details	可以使用此工作流程确定哪些服务器在网络上使用最频繁以及哪些主机在运行这些服务器。 默认情况下，此工作流程以具有各设备的访问频率的服务器摘要开头。下一页按操作系统供应商和版本列出服务器。此工作流程以具有服务器的主机的表视图后跟主机视图结尾。此工作流程基于 Hosts with Servers 自定义表。有关详细信息，请参阅第 59-1 页上的了解自定义表。

使用工作流程

许可证：任何环境

通过工作流程中的向下钻取页面和表视图页面，可以快速缩小数据视图的范围，从而能够专注于对于分析至关重要的事件。虽然各类型的工作流程中的数据不同，但是所有工作流程都共享公共的功能集。以下各节描述这些功能并说明如何对其进行使用：

- 第 58-14 页上的选择工作流程描述工作流程选择页面以及如何选择要使用的工作进程。
- 第 58-15 页上的了解工作流程工具栏描述工作流程中可用的工具栏选项。
- 第 58-16 页上的使用工作流程页面描述所有工作流程页面上显示的功能并说明如何对其进行使用。
- 第 58-19 页上的设置事件时间限制描述如何设置基于事件的工作流程的时间范围。工作流程包括在指定时间范围内生成的事件。
- 第 58-26 页上的限制事件描述在工作流程中用于限制或缩小工作流程中数据视图的范围和前进浏览工作流程页面的功能。
- 第 58-28 页上的使用复合限制说明可任何使用复合限制并提供示例。
- 第 58-29 页上的对向下钻取工作流程页面进行排序描述用于对工作流程中显示的数据进行排序以及用于移除和恢复要查看的表列的功能。
- 第 58-30 页上的选择工作流程页面上的行描述如何在显示的表中选择要分析或要对其执行其他某个操作的数据行。
- 第 58-30 页上的导航到工作流程中的其他页面描述如何使用限制 （包括任何所选事件）从当前工作流程打开其他工作流程。
- 第 58-31 页上的在工作流程之间导航描述 **Jump to** 下拉列表并说明可如何使用它将当前限制应用到其他工作流程。
- 第 60-1 页上的搜索事件提供有关用于搜索事件数据的功能的信息。
- 第 58-32 页上的使用书签描述如何创建、管理和使用书签。

选择工作流程

许可证：任何环境

FireSIGHT 系统提供下表中所列的数据类型的预定义工作流程。

表 58-20　使用工作流程的功能

特性	菜单路径	选项
入侵事件	Analysis > Intrusions	活动 Reviewed Events Clipboard 事件
恶意事件	Analysis > Files	Malware Events
文件事件	Analysis > Files	File Events
Captured files	Analysis > Files	Captured Files
连接事件	Analysis > Connections	活动
安全情报事件	Analysis > Connections	Security Intelligence Events
主机事件	Analysis > Hosts	Network Map 主机 危害表现 应用 Application Details 服务器 Host Attributes Discovery Events
用户事件	Analysis > Users	用户活动 用户
漏洞事件	Analysis > Vulnerabilities	漏洞 Third-Party Vulnerabilities
关联事件	Analysis > Correlation	Correlation Events White List Events White List Violations 状态
审核事件	System > Monitoring	审核
运行状况事件	Health > Health Events	不适用
规则更新导入日志	System > Updates	不适用
Scan Results	Policies > Actions > Scanners	不适用

查看上表中描述的任何种类的数据时，事件显示在该数据的默认工作流程的第一页上。

另请注意，工作流程访问取决于用户角色 （请参阅第 61-45 页上的配置用户角色），如下所示：

- Administrator 用户可以访问任何工作流程，并且是仅有的可访问审核日志、扫描结果和规则更新导入日志的用户。
- Maintenance User 可以访问运行状况事件。
- Security Analyst 和 Security Analyst (Read Only) 用户可以访问入侵、恶意软件、文件、连接、发现、漏洞、相关性和运行状况工作流程。

要使用除默认值以外的工作流程查看数据，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择适当的菜单路径和选项，如使用工作流程的功能表中所述。

系统将显示该数据类型的默认工作流程的第一页。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

步骤 2　或者，使用其他工作流程。点击工作流程标题旁边的 **(switch workflow)**，然后选择要使用的工作流程。

步骤 3　系统将显示所选工作流程的第一页。

了解工作流程工具栏

许可证：任何环境

工作流程中的每个页面包含用于提供对相关功能的快速访问的工具栏。下表描述工具栏上的每个链接

表 58-21　工作流程工具栏链接

特性	说明
Bookmark This Page	将当前页面加入书签，以便稍后可以返回到该页面。加入书签可捕获所查看的页面上已生效的限制，以便稍后能够返回到同一数据 （假设数据仍然存在）。有关创建书签的信息，请参阅第 58-32 页上的使用书签。
Report Designer	以当前受限工作流程作为选择标准打开报告设计器。有关创建报告的信息，请参阅第 57-8 页上的从事件视图创建报告模板。
控制面板	打开与当前工作流程相关的控制面板。例如， Connection Events 工作流程链接到 Connection Summary 控制面板。有关使用控制面板的信息，请参阅第 55-1 页上的使用控制面板。
View Bookmarks	显示可从中进行选择的已保存书签列表。有关创建和管理书签的信息，请参阅第 58-32 页上的使用书签。
搜索	显示可在其中对工作流程中的数据执行高级搜索的 Search 页面。也可以点击向下箭头图标以选择并使用已保存的搜索。有关搜索工作流程的信息，请参阅第 60-1 页上的搜索事件。

使用工作流程页面

许可证：任何环境

可以在工作流程页面上执行的操作取决于页面类型。表视图页面和向下钻取页面包含许多可用于限制要查看的事件集或浏览工作流程的功能。有关各类型的页面上可用的功能的详细信息，请参阅：

- 第 58-16 页上的使用通用表视图或向下钻取页面功能
- 第 58-17 页上的使用地理定位
- 第 58-19 页上的使用表视图页面
- 第 58-19 页上的使用向下钻取页面
- 第 58-19 页上的使用主机视图、数据包视图或漏洞详细信息页面

使用通用表视图或向下钻取页面功能

许可证：任何环境

表视图和向下钻取工作流程页面在表头和表行中提供可用于对所显示数据执行操作的一组图标和其他功能。

下表中对功能进行了描述。

表 58-22　　表视图和向下钻取页面功能

特性	说明
	点击蓝色向下箭头图标以显示工作流程的下一页中的对应行。
（无害） （恶意软件） （自定义检测） （未知） （不可用）	点击显示在文件名和 SHA-256 哈希值列中的网络文件轨迹图标，以在新窗口中查看文件的轨迹图。有关详细信息，请参阅第 40-32 页上的分析网络文件轨迹。 请注意，由于 DC500 防御中心、2 系列设备和 用于 Blue Coat X-系列的思科 NGIPS不支持高级恶意软件防护，因此无法在这些设备上查看基于网络的恶意软件和文件事件的网络文件轨迹。
 （潜在受损） （已列入黑名单） （已列入黑名单，设置进行监控）	点击显示在 IP 地址列中的主机配置文件图标，以在弹出窗口中显示与该 IP 地址关联的主机配置文件。有关详细信息，请参阅第 49-1 页上的使用主机配置文件。 已被所触发的危害表现 (IOC) 规则标记为潜在受损的主机显示带有受损主机图标而不是正常图标。有关 IOC 的详细信息，请参阅第 45-17 页上的了解危害表现。 如果主机配置文件图标灰显，则无法查看主机配置文件，因为该主机不能位于网络映射中 （例如， `0.0.0.0`）。 如果是根据安全情报数据执行流量过滤，则连接事件视图中列入黑名单的 IP 地址和受监控 IP 地址旁边的主机图标略有不同。这有助于识别连接中列入黑名单的主机。请注意，DC500 防御中心和 2 系列设备都不支持安全情报数据。
（低威胁评分） （中等威胁评分） （高威胁评分） （超高威胁评分）	点击显示在危险评分列中的威胁评分图标，以查看与文件关联的最高威胁评分的 Dynamic Analysis Summary 报告。 请注意，由于 DC500 防御中心、2 系列设备和 用于 Blue Coat X-系列的思科 NGIPS支持高级恶意软件防护，因此无法在这些设备上查看 Dynamic Analysis Summary 报告。

表 58-22　表视图和向下钻取页面功能 （续）

特性	说明
	点击显示在用户身份列中的用户图标，以查看用户配置文件信息。有关详细信息，请参阅第 50-55 页上的了解用户详细信息和主机历史记录。 如果用户图标灰显，则无法查看用户配置文件，因为该用户不能位于数据库中（FireAMP连接器用户）。
	点击显示在第三方漏洞 ID 列中的漏洞图标，以查看有关第三方漏洞的漏洞详细信息。有关详细信息，请参阅第 49-24 页上的查看漏洞细节。
复选框	按页面上的两行或多行选择复选框，以指示要影响哪些行，然后点击该页面底部的按钮之一 （例如， **View** 按钮）。还可以选择行顶部的复选框以选择页面上的所有行。
国家/地区旗帜和代码	在某些工作流程页面 （如对应于连接事件、入侵事件、文件事件和恶意软件事件的页面）中，可路由 IP 地址包含关联国家/地区的有关信息。当此*地理定位*信息可用时，国家/地区的旗帜和 ISO 代码显示在相应的列中 （如 Source Country）。将指针悬停在旗帜上方以查看国家/地区名称。查看个别 （而不是聚集）数据点时，可以点击旗帜图标以查看进一步地理定位详细信息。有关详情，请参见第 58-17 页上的使用地理定位。 请注意， DC500 防御中心不支持地理定位数据。
搜索限制	列出值 （如果有），从而对数据视图加以限制。点击展开箭头 (▶) 以显示活动限制和已禁用列列表，或者点击折叠箭头 (▼) 以隐藏列表。默认情况下，此列表已折叠，这在限制列表过长并占据过多屏幕时有用。 要移除单一限制，请点击该限制。要移除复合限制，请点击 **Compound Constraints**。 点击 **Edit Search** 或 **Save Search** 以打开使用当前单一限制预填充的搜索页面。有关详情，请参见第 58-26 页上的限制事件。 **注**　复合限制是根据含有多个非计数值的行创建的限制。不能对复合限制执行搜索或保存搜索操作。
时间范围	位于页面右上角的日期范围为工作流程中要包含的事件设置时间范围。有关详情，请参见第 58-19 页上的设置事件时间限制。 请注意，如果按时间限制事件视图，则在设备配置的时间段外生成的事件 （无论是全局或特定事件）可能显示在事件视图中。即使已经为设备配置一个滑动时间窗，这种情况仍然可能发生。
工作流程页面链接	工作流程页面链接显示在预定义工作流程表视图和向下钻取页面左上角，位于事件上方和工作流程名称下方。点击工作流程页面链接，以使用任何活动限制显示该页面。
工作流程名称	工作流程的名称显示在页面顶部。其旁边 （适用时）是 **(switch workflows)** 链接，可用于选择同一类型的其他工作流程。

使用地理定位

许可证：FireSIGHT

受支持的设备：因功能而异

受支持的防御中心：除 DC500 外的所有型号

在监控网络时，*地理定位*功能提供有关可路由 IP 地址的地理源的其他数据 （国家/地区和大陆等）。可以使用此数据确定例如连接是起源于还是终止于与贵公司无关联的国家/地区。

地理定位信息可用于入侵事件、连接事件、文件事件、恶意软件事件、主机配置文件和用户配置文件。地理定位信息在 Context Explorer 和控制面板中也可用。

可以使用地理定位数据 （源和目标国家/地区/大陆）作为访问控制规则的条件，并为此创建自定义地理定位对象。还可以使用源/目标国家/地区数据作为相关性规则和流量量变曲线的条件。有关详细信息，请参阅第 3-46 页上的使用地理定位对象、第 15-3 页上的按网络或地理位置控制流量、第 51-2 页上的创建关联策略规则和第 53-3 页上的指定流量量变曲线条件。

通过安装地理定位数据库 (GeoDB) 更新，可以查看 Geolocation Details 页面，其中含有可用于 IP 地址的详细信息，如邮政编码、坐标、时区、自治系统编号 (ASN)、互联网服务提供商 (ISP)、使用类型 （家庭或企业）、公司、域名、连接类型和代理信息。还可以使用四种第三方映射工具中的任意一种精确定位检测到的位置。如果没有 GeoDB 更新，仅会显示旗帜图标和国家/地区名称；无法查看 Geolocation Details 页面。有关安装和更新 GeoDB 的信息，请参阅第 66-24 页上的更新地理定位数据库。可以通过点击 **Help > About** 查看 GeoDB 更新的当前版本。

根据可用性，Geolocation Details 页面上可能会显示多个字段；未显示无信息的字段。下表包含有关这些字段的信息。

表 58-23　　地理定位详细信息字段

字段	目录
国家/地区	与主机的 IP 地址关联的国家/地区，伴有国家/地区的旗帜。在括号中列出了大陆。示例：`United States (North America)` 和 `Equatorial Guinea (Africa)`
地区	主机所在的国家/地区的州、省或其他子区域。示例：`VA` 和 `35`
城市	主机所在的城市。示例：`Seattle` 和 `Fukuoka`
Postal Code	主机所在区域的邮政编码。示例：`361000` 和 `90210`
Latitude/Longitude	主机位置的精确坐标。示例：`40.0375, -76.1053; 53.4050, -0.5484`
地图	指向外部映射站点的链接 （谷歌地图、雅虎地图、必应地图和 OpenStreetMap）。点击任意链接以查看主机的大致位置的情景地图。
时区	主机位置的时区，在适用情况下会标注夏令时。示例：`GMT+8:00` 和 `GMT-4:00 (In DST)`
ASN	与主机 IP 地址关联的自治系统编号 (ASN)，以及与该 ASN 有关的任何其他信息。示例：`14618 (Amazon.com Inc.); 4837 (Cncgroup China169 Backbone)`
ISP	与主机 IP 地址关联的互联网服务提供商 (ISP)。示例：`Atlantic Broadband; China Unicom Ip Network`
Home/Business	主机的连接是用于 `Home` 还是 `Business` 用途。
组织	与主机 IP 地址关联的公司。示例：`Amazon.com` 和 `Bank of America`
域名	与主机 IP 地址关联的域名。示例：`amazonaws.com` 和 `xmcnc.net`
连接类型	与主机 IP 地址关联的连接类型。示例：`Broadband` 和 `DSL`
代理类型	使用的代理类型。示例：`Anonymous` 和 `Corporate`

要查看地理定位详细信息，请执行以下操作：

访问：任何环境

步骤 1　在事件视图、主机配置文件或其他支持地理定位的页面中，点击显示在单个数据点旁边的国家/地区小旗帜图标或 ISO 国家/地区代码。（尽管有旗帜图标，但是无法在诸如 Connection Summary 之类的控制面板上查看地理定位详细信息来获取汇总的地理定位信息。）

提示　在事件视图中，将指针悬停在旗帜图标上方以查看国家/地区的名称提示。

系统在新窗口中显示 Geolocation Details 页面。

使用表视图页面

许可证：任何环境

表*视图*包含对应于数据库中各字段的列（如果默认情况下启用了该列）。请注意，禁用表视图中的列时，如果禁用该列会创建两个或多个相同的行，则 FireSIGHT 系统将向事件视图中添加 Column 列。点击表视图页面中的某个值时，即受该值限制。创建自定义工作流程时，通过点击 **Add Table View** 向其中添加表视图。

表视图页面提供向下钻取、主机视图、数据包视图或漏洞详细信息页面中不可用的一些附加功能。下表提供有关这些功能的详细信息。

表 58-24　附加表视图页面功能

特性	说明
✖	点击要隐藏的列标题中的此图标。在显示的弹出窗口中，点击 **Apply**。 **提示**　要隐藏或显示其他列，选择或清除相应的复选框，然后点击 **Apply**。
Disabled Columns 列表	从页面中移除列或者列在默认情况下已禁用时，列名显示在位于表上方并默认隐藏的 Disabled Columns 列表中。 要将已禁用列重新添加到事件视图中，请点击 Search Constraints 展开箭头（▶）以展开搜索限制，然后点击 Disabled Columns 下的列名。 有关详情，请参见第 58-29 页上的对向下钻取工作流程页面进行排序。

使用向下钻取页面

许可证：任何环境

向下钻取页面包含数据库中可用的列的子集。请注意，预定义工作流程的向下钻取页面始终具有 Count 列。通过向下钻取页面，可以缩小所查看的事件范围并在工作流程中前进。例如，如果点击向下钻取页面中的某个值，即受该值限制并会移至工作流程中的下一页，从而更密切关注与所选值匹配的事件。点击向下钻取页面中的值并不会禁用该值所在的列，即使前进到的页面是表视图也如此。创建自定义工作流程时，通过点击 **Add Page** 向其中添加向下钻取页面。

有关在完成工作流程时使用向下钻取页面上的功能限制事件集的详细信息，请参阅第 58-16 页上的使用通用表视图或向下钻取页面功能。

使用主机视图、数据包视图或漏洞详细信息页面

许可证：任何环境

发现活动、主机、主机属性、危害表现、服务器、客户端应用或连接数据工作流程的最终页面为主机视图。漏洞工作流程中的最终页面为漏洞详细信息页面。入侵事件工作流程始终以数据包视图结尾。在工作流程的最终页面上，可以展开详细信息部分以查看有关该工作流程期间所关注的集合中各对象的特定信息。尽管网络界面没有在工作流程的最终页面上列出限制，但是先前设置的限制会保留并应用到数据集。

设置事件时间限制

许可证：任何环境

每个事件具有指示事件发生时间的时间戳。可以通过设置时间段（有时称为时间范围）限制某些工作流程中显示的信息。

基于可按时间限制的事件的工作流程在页面顶部包含一条时间范围线，如下图所示。

默认情况下，思科设备上的工作流程使用设置为前一小时的扩展式时间段。例如，如果您在上午 11:30 登录，将会看到发生在上午 10:30 和上午 11:30 之间的事件。随着时间的推进，时间段进行扩展。在中午 12:30，您将会看到发生在上午 10:30 和中午 12:30 之间的事件。

可以通过设置自己的默认时间段更改此行为，该时间段管理三个属性：

- 时间段类型 （静态、扩展式或滑动式）
- 时间段长度
- 时间段数量 （多个时间段或单个全局时间段）

有关默认时间段的常规信息，请参阅第 71-5 页上的默认时间段。

无论默认时间段设置如何，都可以在事件分析期间手动更改时间段，方法是点击页面顶部的时间范围，该页面会显示 Date/Time 弹出窗口。根据配置的时间段数量和使用的设备类型，还可以使用 Date/Time 窗口更改所查看的事件类型的默认时间段。

最后，可以暂停时间段，借此能够检查工作流程提供的数据，而时间段不会更改以及移除或添加无关的事件。请注意，为避免在不同工作流程页面上显示相同事件，在点击页面底部的链接以显示另一页的事件时，时间段会自动暂停；准备就绪后，可以取消暂停时间段。

有关详细信息，请参阅：

- 第 58-20 页上的更改时间段
- 第 58-24 页上的更改事件类型的默认时间段
- 第 58-26 页上的暂停时间窗口

更改时间段

许可证：任何环境

无论默认时间段设置如何，都可以在事件分析期间手动更改时间段。

注　手动时间段设置仅对当前会话有效。在注销然后重新登录时，时间段会重置为默认值。

根据配置的时间段数量，更改一个工作流程的时间段可能会影响设备上的其他工作流程。例如，如果具有单个全局时间段，则更改一个工作流程的时间段会更改设备上所有其他工作流程的时间段。另一方面，如果使用的是多个时间段，则更改审核日志或运行状况事件工作流程时间段对于任何其他时间段没有影响，而更改其他种类的事件的时间段则会影响可按时间限制的所有事件（审核事件和运行状况事件除外）。

请注意，由于并非所有工作流程都可按时间限制，因此时间段设置对基于主机、主机属性、应用、应用详情、漏洞、用户或白名单违例的工作流程没有影响。

使用 Date/Time 窗口上的 Time Window 选项卡手动配置时间段。根据在默认时间段设置中配置的时间段数量，选项卡的标题为以下之一：

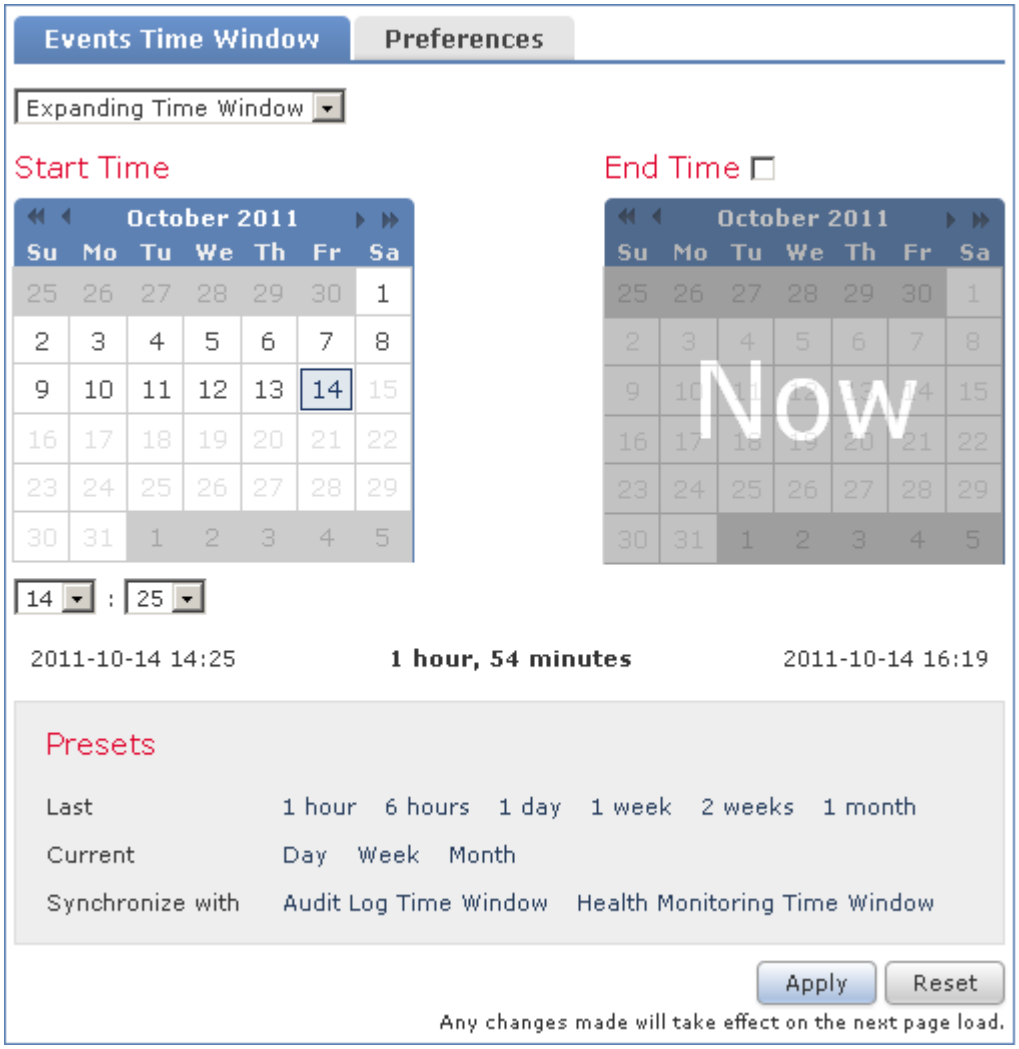
- **Events Time Window** （如果配置了多个时间段，并且是为除审核日志和运行状况事件工作流程以外的工作流程设置时间段）
- **Health Monitoring Time Window** （如果配置了多个时间段，并且是为运行状况事件工作流程配置时间段）

- **Audit Log Time Window** （如果配置了多个时间段，并且是为审核日志配置时间段）
- **Global Time Window** （如果配置了单个时间段）

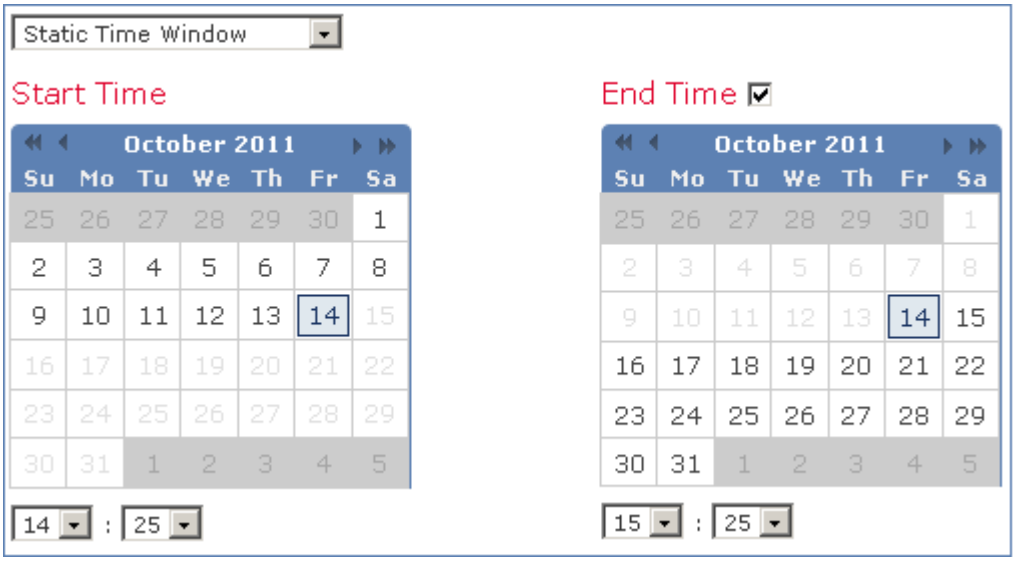
配置时间段时必须首先决定要使用的时间段的类型。

- *静态*时间段显示从特定开始时间到特定结束时间生成的所有事件。
- *扩展式*时间段显示从特定开始时间到目前生成的所有事件；随着时间的推进，时间段进行扩展，并会将新事件添加到事件视图中。
- *滑动式*时间段显示从特定开始时间 （例如，一周前）到目前生成的所有事件；随着时间的推进，时间段会“滑动”，以便仅显示已配置的范围 （在此示例中是上周）的事件。

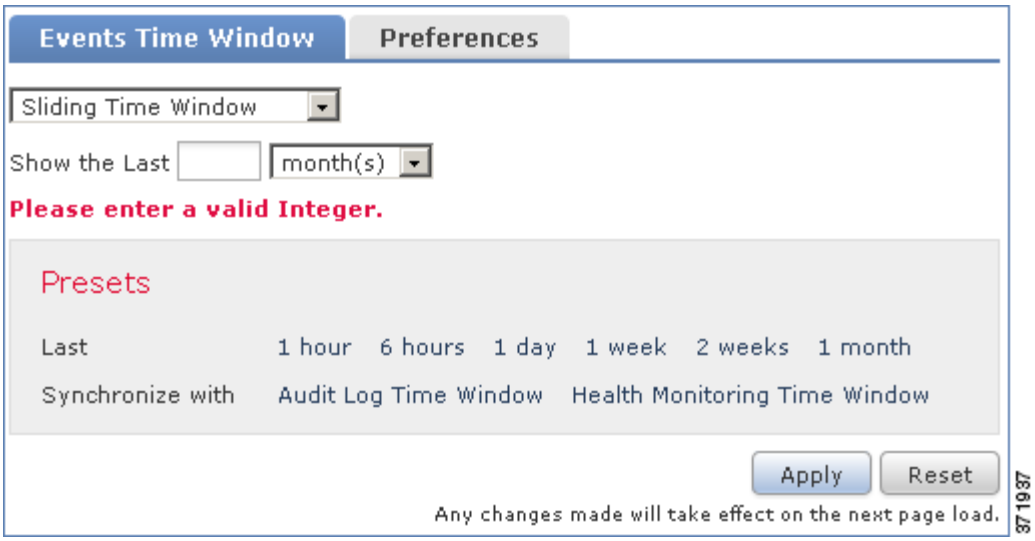
根据选择的类型，Date/Time 窗口会更改以提供不同配置选项。下图显示 Date/Time 窗口，指定要使用扩展式时间段。使用扩展式时间段时， End Time 日历会灰显并指定结束时间为“Now”。



如果使用静态时间段，则可以设置结束时间。



如果选择使用滑动式时间段，则选项会进一步更改。



注 FireSIGHT 系统根据在时区首选项中指定的时间使用 24 小时制时间。有关配置时区的信息，请参阅第 71-6 页上的设置默认时区。

下表说明可在 Time Window 选项卡上配置的各种设置。

表 58-25　时间段设置

环境	时间段类型	说明
时间段类型下拉列表	不适用	选择要使用的时间段类型：静态、扩展式或滑动式。 请注意，如果按时间限制事件视图，则在设备配置的时间段外生成的事件（无论是全局或特定事件）可能显示在事件视图中。即使已经为设备配置一个滑动时间窗，这种情况仍然可能发生。
Start Time 日历	静态和扩展式	指定时间段的开始日期和时间。所有时间段的最大时间范围都是从 1970 年 1 年 1 日午夜 (UTC) 到 2038 年 1 月 19 日凌晨 3:14:07 (UTC)。 **提示**　可以使用 Presets 选项而不是使用日历，如下所述。
End Time 日历	static	指定时间段的结束日期和时间。所有时间段的最大时间范围都是从 1970 年 1 年 1 日午夜 (UTC) 到 2038 年 1 月 19 日凌晨 3:14:07 (UTC)。 请注意，如果使用的是扩展式时间段，则 End Time 日历会灰显并指定结束时间为“Now”。 **提示**　可以使用 Presets 选项而不是使用日历，如下所述。
显示 Last 字段和下拉列表	滑动式	配置滑动式时间段的长度。
Presets: Last	全部	根据设备的本地时间，点击列表中的其中一个时间范围以更改时间段。例如，点击 **1 week** 会将时间段更改为反映上周。点击预设会将日历更改为反映选择的预设。
Presets: Current	静态和扩展式	根据设备的本地时间和日期，点击列表中的其中一个时间范围以更改时间段。点击预设会将日历更改为反映选择的预设。 请注意： • 当日在午夜开始 • 当周在星期天午夜开始 • 当月在月份第一日午夜开始
Presets: Synchronize with	所有（如果使用的是全局时间段则不适用）	点击其中一项： • **Events Time Window** 将当前时间段与事件时间段同步 • **Health Monitoring Time Window** 将当前时间段与运行状况监控时间段同步 • **Audit Log Time Window** 将当前时间段与审核日志时间段同步

要在事件分析期间更改时间段，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　在按时间限制的工作流程上，点击时间范围图标 ()。

系统将显示 Date/Time 窗口。

步骤 2　在 **Time Window** 选项卡上，按时间段设置表中所述设置时间段。

提示　点击 **Reset** 以将时间段重新更改为默认设置。

步骤 3　点击**应用 (Apply)**。

窗口关闭，并且事件视图页面显示新时间范围内的事件。

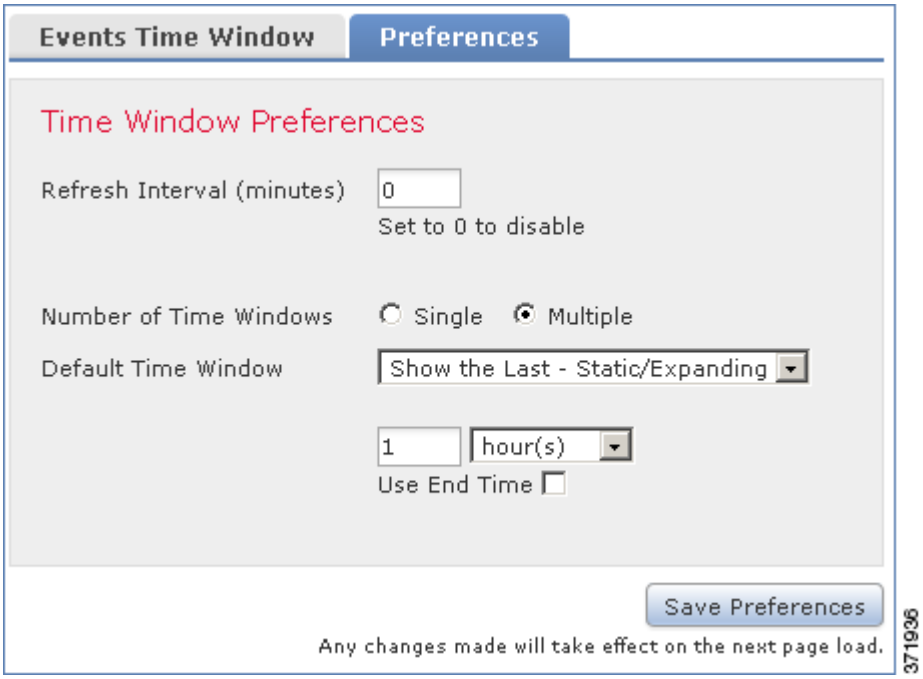
更改事件类型的默认时间段

许可证：任何环境

在事件分析期间，可以使用 Date/Time 窗口上的 Preferences 选项卡更改所查看的事件类型的默认时间段，而不必使用事件视图设置 （请参阅第 71-5 页上的默认时间段）。

请记住，以此方式更改默认时间段仅会更改所查看的事件类型的默认时间段。例如，如果配置了多个时间段，则更改 Preferences 选项卡上的默认时间段会更改事件、运行状况监控或审核日志窗口的设置，换句话说，以第一个选项卡指示的时间段为准。如果配置了单个时间段，则更改 Preferences 选项卡上的默认时间段会更改所有事件类型的默认时间段。

下图显示配置有多个时间段的设备上的防御中心版本的 Preferences 选项卡。



下表说明可在 Preferences 选项卡上配置的各种设置。

表 58-26　　时间段首选项

偏好	说明
Refresh Interval	设置事件视图的刷新间隔 （以分钟为单位）。输入零会禁用刷新选项。
Number of Time Windows	指定要使用的时间段数量： • 选择 **Multiple** 以根据可按时间限制的事件为审核日志、运行状况事件和工作流程配置单独的默认时间段。 • 选择 **Single** 以使用适用于所有事件的全局时间段。

表 58-26　　时间段首选项 （续）

偏好	说明
Default Time Window: Show the Last - Sliding	此设置允许配置指定长度的滑动式默认时间段。 设备显示在某个特定开始时间 （例如， 1 小时前）和当前时间期间生成的所有事件。当更改事件查看，时间段会“滑动”，以便始终可查看最近一小时的事件。
Default Time Window: Show the Last - Static/Expanding	此设置允许配置指定长度的静态或扩展式默认时间段。 对于**静态**时间段 （启用 **Use End Time** 复选框），设备显示从特定开始时间 （例如， 1 小时前）到首次查看事件时生成的所有事件。更改事件查看后，时间段会固定，以便只可查看在静态时间段内发生的事件。 对于**扩展式**时间段 （禁用 **Use End Time** 复选框），设备显示从特定开始时间 （例如， 1 小时前）到目前生成的所有事件。在更改事件查看后，时间段会扩展为当前时间。
Default Time Window: Current Day - Static/Expanding	此设置允许配置当日的静态或扩展式默认时间段。当日从午夜开始，基于当前会话的时区设置。 对于**静态**时间段 （启用 **Use End Time** 复选框），设备显示从午夜到首次查看事件时生成的所有事件。更改事件查看后，时间段会固定，以便只可查看在静态时间段内发生的事件。 对于**扩展式**时间段 （禁用 **Use End Time** 复选框），设备显示从午夜到目前生成的所有事件。在更改事件查看后，时间段会扩展为当前时间。请注意，如果分析在注销之前持续超过 24 小时，则时间段可能会超过 24 小时。
Default Time Window: Current Week - Static/Expanding	此设置允许配置当周的静态或扩展式默认时间段。当周从上一周日的午夜开始，基于当前会话的时区设置。 对于**静态**时间段 （启用 **Use End Time** 复选框），设备显示从午夜到首次查看事件时生成的所有事件。更改事件查看后，时间段会固定，以便只可查看在静态时间段内发生的事件。 对于**扩展式**时间段 （禁用 **Use End Time** 复选框），设备显示从星期天午夜到目前生成的所有事件。在更改事件查看后，时间段会扩展为当前时间。请注意，如果在您注销之前，分析持续 1 周以上，则此时间段可以超过 1 周。

要在事件分析期间更改时间段首选项，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　在按时间限制的工作流程上，点击时间范围图标 ()。

系统将显示 Date/Time 窗口。

步骤 2　选择 **Preferences** 选项卡并更改首选项，如时间段首选项表中所述。

步骤 3　点击**保存首选项**。

首选项保存成功。

步骤 4　此时您有两种选择：

- 要将新的默认时间段设置应用于所使用的事件视图，请点击 **Apply** 以关闭 Date/Time 窗口并刷新事件视图。
- 要继续分析而不应用默认时间段设置，请关闭 Date/Time 窗口而不点击 **Apply**。

暂停时间窗口

许可证：任何环境

可以暂停时间段，从而能够检查工作流程提供的数据快照。这会有所帮助，因为已取消暂停的工作流程在更新时，可能会移除要检查的事件，或者添加无关的事件。

请注意，不能暂停静态时间段。此外，暂停事件时间段对控制面板没有影响，而暂停控制面板对暂停事件时间段也没有任何影响。

完成分析后，可以取消暂停时间段。取消暂停时间段将根据您的喜好对其进行更新，并且还更新事件视图以反映已取消暂停的时间段。

如果数据库包含的事件数超过单个工作流程页面上可显示的事件数，则可点击页面底部的链接以显示更多事件（请参阅第 58-30 页上的导航到工作流程中的其他页面）。执行此操作时，时间段自动暂停，以便不重复显示相同的事件。当您准备就绪时，可以取消暂停时间段。

要暂停时间段，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　在时间范围控件上，点击暂停图标 (❚❚)。

时间段暂停，直到将其取消暂停为止。

要取消暂停时间段，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　在时间范围控件上，点击播放图标 (▶)。

时间段取消暂停并根据您的喜好进行更新。事件视图更新为反映当前时间段。

限制事件

许可证：任何环境

工作流程页面上显示的信息由实施的限制来确定。例如，最初打开事件工作流程时，信息限制为前一小时生成的事件。

要前进到工作流程中的下一页并通过特定值限制所查看的数据，请选择页面上具有这些值的行，然后点击 **View**。要前进到工作流程中的下一页并保留当前限制和传递所有事件，请选择 **View All**。

注　如果选择含有多个非计数值的行并点击 **View**，则会创建复合限制。有关复合限制的详细信息，请参阅第 58-28 页上的使用复合限制。

限制工作流程中的数据有第三种方法。要将页面限制为含有选定值的行，并且还将选定值添加到页面顶部的限制列表中，请点击页面上某一行中的值。

例如，如果在具有以下事件的页面上点击 Initiator IP 列中的 **10.10.60.119**：

	First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 22:19:28	Block	10.10.60.119	10.1.1.57	753 (rrh) / tcp
	2013-03-10 16:13:39	Block	10.10.32.124	10.10.60.165	856 / tcp

372156

...则受限页面仅包含具有该 IP 地址的事件：

▼ Search Constraints (Edit Search Save Search)

Initiator IP 10.10.60.119

Connections | Intrusion | Malware | Files | Hosts | Applications | Application Details | Server

	First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Ty
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 22:19:28	Block	10.10.60.119	10.1.1.57	753 (rrh) / tcp
	2013-03-09 23:21:59	Block	10.10.60.119	10.1.1.57	822 / tcp

提示 根据监控规则条件来限制连接事件的过程略有不同，可能需要采取一些额外步骤。此外，不能按关联文件或入侵信息来限制连接事件。有关详细信息，请参阅第 39-24 页上的使用连接和安全情报数据表。

还可以使用搜索来限制工作流程中的信息。在搜索页面上输入的搜索条件会列为页面顶部的限制，并且产生的事件相应地受限制。在防御中心中，除非当前限制是复合限制，否则导航到其他工作流程时也会应用这些限制（请参阅第 58-31 页上的在工作流程之间导航）。

在搜索时，必须特别注意搜索限制是否适用于所搜索的表。例如，客户端数据在连接摘要中不可用。如果根据连接中检测到的客户端搜索连接事件，然后在连接摘要事件视图中查看结果，则防御中心会显示连接数据，如同其完全未受限制一样。无效限制会标示为不适用 (N/A)，并以删除线进行标记。

下表描述应用限制时可执行的每个操作。

表 58-27　搜索限制功能

要.....	点击.....
将视图限制为与单个值匹配的事件	表中的值。 例如，如果查看的是已记录连接的列表，并要使用访问控制将该列表仅限于允许的连接，请点击 **Action** 列中的 **Allow**。又例如，如果查看的是入侵事件，并要将列表仅限于目标端口为 80 的事件，请点击 **DST Port/ICMP Code** 列中的 **80 (http)/tcp**。
将视图限制为与多个值匹配的事件	具有这些值的事件的对应复选框，然后点击 **View**。 请注意，如果行包含多个非计数值，则会添加复合限制。有关复合限制的详细信息，请参阅第 58-28 页上的使用复合限制。
移除限制	Search Constraints 框中限制的名称。
使用搜索页面编辑限制	Search Constraints 框中的 **Edit Search**。 要再次限制一列中的多个值时，请使用此功能。例如，如果要查看与两个 IP 地址相关的事件，请点击 **Edit Search**，然后修改 Search 页面上相应的 IP 地址字段以将两个地址均包含在内，然后点击 **Search**。
将限制另存为已保存的搜索	Search Constraints 框中的 **Save Search** 并指定查询名称。 请注意，不能保存包含复合限制的查询。有关复合限制的详细信息，请参阅第 58-28 页上的使用复合限制。
对其他事件视图使用相同限制	**Jump to** 并选择事件视图。有关详情，请参见第 58-31 页上的在工作流程之间导航。 请注意，在切换到其他工作流程时，不会保留复合限制。有关复合限制的详细信息，请参阅第 58-28 页上的使用复合限制。
切换限制的显示	展开箭头 (▶)。这在限制列表较大并占据大部分屏幕时有用。

使用复合限制

许可证：任何环境

复合限制基于特定事件的所有非计数值。选择含有多个非计数值的行时，复合限制仅检索与该页面上的该行中所有非计数值匹配的事件。例如，如果选择源 IP 地址为 `10.10.31.17` 且目标 IP 地址为 `10.10.31.15` 的行以及源 IP 地址为 `172.10.10.17` 且目标 IP 地址为 `172.10.10.15` 的行，则会检索下列所有内容：

- 源 IP 地址为 10.10.31.17 且目标 IP 地址为 10.10.31.15 的事件

  或者

- 源 IP 地址为 172.10.31.17 且目标 IP 地址为 172.10.31.15 的事件

将复合限制与简单限制组合时，简单限制分布在各复合限制集合中。例如，如果在以上所列的复合限制中为协议值 `tcp` 添加了一条简单限制，则会检索下列所有内容：

- 源 IP 地址为 10.10.31.17 且目标 IP 地址为 10.10.31.15 且协议为 tcp 的事件

  或者

- 源 IP 地址为 172.10.31.17 且目标 IP 地址为 172.10.31.15 且协议为 tcp 的事件

不能对复合限制执行搜索或保存搜索操作。也不能在使用事件视图链接或点击 **(switch workflow)** 以切换到其他工作流程时保留复合限制。如果将应用了复合限制的事件视图加入书签，则不使用书签保存限制。

要清除所有复合限制，请点击 **Compound Constraints**。

对表视图页面进行排序并更改其布局

许可证：任何环境

查看工作流程中的数据时，可以根据任何可用列对数据进行排序，以及移除和恢复要查看的列。可以按列以升序或降序对数据进行排序。

提示　如果创建自定义工作流程，则可以完全自定义页面上列的排列并预定义页面排序顺序。有关详情，请参见第 58-34 页上的创建自定义工作流程。

表 58-28　　排序和布局功能

要.....	点击.....
对列进行排序	列标题。再次点击列标题以反转排列顺序。 **提示**　方向图标 (▼) 指示数据按哪一列排序，以及排序是升序 （上指图标）还是降序 （下指图标）。
从表视图中移除列	要隐藏的列标题中的关闭图标 (✖)。在显示的弹出窗口中，点击 **Apply**。 禁用列时，该列在会话持续时间内处于禁用状态 （除非稍后重新添加该列）。请注意，禁用第一列时，会添加 Count 列。不能禁用 Count 列。 **提示**　要隐藏或显示其他列，选择或清除相应的复选框，然后点击 **Apply**。要将已禁用的列重新添加到视图中，请点击展开箭头 (▶) 以展开搜索限制，然后点击 Disabled Columns 下的列名。
将已禁用列重新添加到视图中	Disabled Columns 下的列名。 启用默认情况下禁用的列时，该列在会话持续时间内处于启用状态 （除非稍后将其禁用）。请注意，如果启用未产生相同的行，则会移除 Count 列。

对向下钻取工作流程页面进行排序

许可证：任何环境

查看工作流程或事件视图中的数据时，可以根据任何可用列对数据进行排序，以及移除和恢复要查看的列。可以按列以升序或降序对数据进行排序。方向图标 (▼) 指示数据按哪一列排序，以及排序是升序 （上指图标）还是降序 （下指图标）。

提示　如果创建自定义工作流程，则可以完全自定义页面上列的排列并预定义页面排序顺序。有关详情，请参见第 58-34 页上的创建自定义工作流程。

要对列进行排序，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　点击列标题。

要反转排列顺序，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　再次点击列标题。

选择工作流程页面上的行

许可证：任何环境

有多种方法可选择然后处理工作流程页面上的行：

- 要选择页面上的所有行，请选择页面顶部的复选框。

  然后，可以点击页面底部的任何按钮 （**View** 和 **Delete** 等）以对该页面上的所有事件执行该操作。
- 要选择单行，请选择单个行旁边的复选框。

  然后，可以点击页面底部的任何按钮以仅对与该行关联的事件执行该操作。
- 要选择单行并在工作流程的下一页查看其关联事件，请点击箭头图标 ( )。

注　不能一次从多个页面中选择行。

导航到工作流程中的其他页面

许可证：任何环境

如果数据库包含的事件数超过单个工作流程页面上可显示的事件数，则可点击页面底部的链接以显示更多事件。

点击其中一个链接时，时间段自动暂停，以便不会重复显示相同事件；当您准备就绪时，可以取消暂停时间段。有关详细信息，请参阅第 58-19 页上的设置事件时间限制。

下表描述如何使用导航链接。

表 58-29　　导航页面

要.....	点击.....
查看其他页面	页码，进入希望查看的页面，然后按 Enter
查看下一页	>
查看上一页	<

表 58-29　　导航页面 （续）

要.....	点击.....
跳至最后一页	>|
跳至第一页	|<

在工作流程之间导航

许可证：任何环境

可以使用工作流程页面上的 **Jump to...** 下拉列表中的链接导航到其他工作流程。选择下拉列表以查看并选择其他工作流程。

选择新工作流程时，所选行共享的属性和所设置的限制用于新工作流程中 （如果其适用）。如果配置的限制或事件属性没有映射到新工作流程中的字段，则表明其已丢弃。此外，从一个工作流程切换到另一个工作流程时未保留复合限制。此外，捕获的文件工作流程中的限制仅传输到文件和恶意软件事件工作流程。

注　查看某个时间范围的事件计数时，事件的总数可能无法反映为其提供了更详细数据的事件的数量。因为系统有时会删掉较旧的事件详情以管理磁盘空间使用情况，所以会发生这种情况。要将事件详情删除的情况降到最少，您可以微调事件日志记录，以只记录对部署最重要的事件。有关详细信息，请参阅第 38-1 页上的记录网络流量中的连接。

请注意，除非已暂停时间段或已配置静态时间段，否则在更改工作流程时时间段会更改。有关详细信息，请参阅第 58-19 页上的设置事件时间限制。

Jump to 下拉列表为下表提供对工作流程的快速访问：

- 连接事件
- 安全情报事件
- 入侵事件
- 恶意软件事件
- 文件事件
- 主机
- 危害表现
- 应用
- 应用详情
- 服务器
- 主机属性
- 发现事件
- 用户
- 漏洞
- 第三方漏洞
- 关联事件
- 白名单事件

此功能可增强您调查可疑活动的能力。例如，如果查看的是连接数据并发现内部主机在向外部站点传送异常大量的数据，则可以选择响应方 IP 地址和端口作为限制，然后跳至 **Applications** 工作流程。应用工作流程将使用响应方 IP 地址和端口作为 IP Address 和 Port 限制，并显示有关应用的其他信息，如应用的种类。也可以点击页面顶部的 **Hosts** 以查看远程主机的主机配置文件。

在找到有关应用的详细信息后，可以选择 **Correlation Events** 以返回到连接数据工作流程，从限制中移除 Responder IP，向限制中添加 Initiator IP，然后选择 **Application Details** 以了解发起主机上的用户在将数据传输到远程主机时使用了哪个客户端。请注意，Port 限制未转移到 Application Details 页面。保持本地主机作为限制时，也可以使用其他导航按钮查找其他信息。

- 要发现本地主机是否已违反任何策略，请保持 IP 地址作为限制并从 **Jump to** 下拉列表中选择 **Correlation Events**。
- 要了解是否对主机触发了指示危害的入侵规则，请从 **Jump to** 下拉列表中选择 **Intrusion Events**。
- 要查看本地主机的主机配置文件并确定主机是否易受可能已被利用的任何漏洞的攻击，请从 **Jump to** 下拉列表中选择 **Hosts**。

使用书签

许可证：任何环境

如果要在事件分析中快速返回到特定位置和时间，请创建书签。书签保留以下有关信息：

- 使用的工作流程
- 查看的工作流程部分
- 工作流程中的页码
- 任何搜索限制
- 任何已禁用列
- 使用的时间范围

创建的书签可供具有书签访问权限的所有用户帐户使用。这意味着，如果发现需要深入分析的事件集，则可以轻松创建书签并将调查移交给具有相应特权的其他用户。

注　如果删除书签中显示的事件 （直接由用户删除或通过自动数据库清除），则书签不再显示原始事件集。

有关使用书签的详细信息，请参阅：

- 第 58-33 页上的创建书签描述如何创建新书签。
- 第 58-33 页上的查看书签描述如何查看并使用现有书签。
- 第 58-33 页上的删除书签描述如何删除书签。

创建书签

许可证：任何环境

使用以下过程创建新书签：

要创建书签，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　在事件分析期间，显示了有关事件的情况下，点击 **Bookmark This Page**。

系统将显示 Create a Bookmark 页面。

步骤 2　在 **Bookmark Name** 字段中，键入书签的名称 （最多 80 个字母数字字符和空格），然后点击 **Save Bookmark**。

系统保存书签，并会再次显示已加入书签的事件页面。

查看书签

许可证：任何环境

使用以下过程查看并使用现有书签。

要查看书签，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　从任意事件视图点击 **View Bookmarks**。

系统将显示 Bookmarks 页面。

步骤 2　在要使用的书签旁，点击 **View**。

系统将显示已加入书签的页面。

注　如果删除书签中最初显示的事件 （直接由用户删除或通过自动数据库清除），则书签不再显示原始事件集。

删除书签

许可证：任何环境

使用以下过程删除书签。请注意，删除书签不会影响该书签检索到的事件。

要删除书签，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　从任意事件视图点击 **View Bookmarks**。

系统将显示 Bookmarks 页面。

步骤 2　点击要移除的书签旁边的 **Delete**。

系统删除书签。

使用自定义工作流程

许可证：任何环境

如果预定义工作流程和思科提供的自定义工作流无法满足需求，则可以创建自定义工作流程。

有关详情，请参阅：

- 第 58-34 页上的创建自定义工作流程以了解创建自定义工作流程的过程
- 第 58-36 页上的创建自定义连接数据工作流程以了解根据连接数据创建自定义工作流程的过程
- 第 58-37 页上的查看自定义工作流程以了解根据事件和自定义表查看自定义工作流程的过程
- 第 58-38 页上的编辑自定义工作流程以了解编辑自定义工作流程的过程
- 第 58-39 页上的删除自定义工作流程以了解删除自定义工作流程的过程

创建自定义工作流程

许可证：任何环境

如果预定义工作流程和思科提供的自定义工作流无法满足需求，则可以创建自定义工作流程。

提示　可以从其他设备导出自定义工作流程，然后将其导入到设备上，而不是创建新的自定义工作流程。然后，可以编辑已导出工作流程来满足需求。有关详细信息，请参阅第 A-1 页上的导入和导出配置。

创建自定义工作流程时，请执行以下操作：

- 选择要作为工作流程源的表
- 提供工作流程名称
- 向工作流程中添加向下钻取页面和表视图页面

对于工作流程中的各向下钻取页面，可以：

- 提供显示在网络界面中页面顶部的名称
- 每页包含最多五列
- 指定默认排序顺序 （升序或降序）

可以在工作流程页面序列中的任何位置添加表视图页面。它们不具有任何可编辑属性，如页面名称、排序顺序或用户可定义的列位置。

自定义工作流程的最终页面取决于工作流程所基于的表，如下表所述。创建工作流程时，默认情况下会添加这些最终页面。

表 58-30　自定义工作流程最终页面

基于下列各项的工作流程	具有以下最终页面.....
发现事件	主机
漏洞	漏洞详细信息
第三方漏洞	主机
用户	用户
危害表现	主机
入侵事件	数据包

设备不是根据其他种类的事件 （例如，审核日志或恶意软件事件）向自定义工作流程中添加最终页面。

注　根据连接数据创建自定义工作流程的过程略有不同。有关详细信息，请参阅下一节，创建自定义连接数据工作流程。

要创建自定义工作流程，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Custom > Custom Workflows**。

系统将显示 Custom Workflows 页面。

步骤 2　点击 **Create Custom Workflow**。

系统将显示 Edit Custom Workflow 页面。

步骤 3　在 **Name** 字段中键入工作流程的名称。

可以在名称中使用最多 60 个字母数字字符和空格。

步骤 4　或者，在 **Description** 字段中键入工作流程的说明。

可以使用最多 80 个字母数字字符和空格。

步骤 5　从 **Table** 下拉列表中选择要包含的表。

步骤 6　或者，点击 **Add Page** 以向工作流程中添加一个或多个向下钻取页面。

系统将显示向下钻取页面部分。

首先在 **Page Name** 字段中使用最多 80 个字母数字字符 （但无空格）键入页面的名称。

在 Column 1 下，选择排序优先级和表列。此列将显示在页面最左侧的列中。例如，要创建显示所针对的目标端口的页面，并要按计数对页面进行排序，请从 **Sort Priority** 下拉列表中选择 **2**，并从 **Field** 下拉列表中选择 **DST Port/ICMP Code**。

继续选择要包含的字段并设置其排序优先级，直到指定要在页面上显示的所有字段为止。每页可以指定最多五个字段。

注　如果在第 5 步中选择 **Vulnerabilities** 作为 Table Type，然后添加 **IP Address** 作为表列，则除非使用搜索功能限制工作流程以查看特定 IP 地址或地址块，否则在使用自定义工作流程查看漏洞时不会显示 IP Address 列。有关搜索漏洞的详细信息，请参阅第 50-46 页上的搜索漏洞。

步骤 7　或者，点击 **Add Table View** 以向工作流程中添加表视图页面。

注　必须向自定义工作流程中添加至少一个向下钻取页面或事件表视图。

步骤 8　点击 **Save**。

新工作流程保存并添加到自定义工作流程列表中。

创建自定义连接数据工作流程

许可证：FireSIGHT

基于连接数据的自定义工作流程与其他自定义工作流程类似，不同在于可以包含连接数据图形页面以及向下钻取页面和表视图页面。可以按任意顺序在工作流程中包含尽可能多的各类型的页面。每个连接数据图形页面包含单个图形，可以是折线图、条形图或饼图。在折线图和条形图中，可以包含多个数据集。有关连接数据的详细信息，包括连接摘要、连接图形和数据集，请参阅第 39-2 页上的了解连接和安全情报数据。

提示　可以从其他设备导出自定义工作流程，然后将其导入到设备上，而不是创建新的自定义工作流程。然后，可以编辑已导出工作流程来满足需求。有关详细信息，请参阅第 A-1 页上的导入和导出配置。

要根据连接数据创建自定义工作流程，请执行以下操作：

访问：管理

步骤 1　选择 **Analysis > Custom > Custom Workflow**。

步骤 2　点击 **Create Custom Workflow**。

系统将显示 Edit Custom Workflow 页面。

步骤 3　在 **Name** 字段中键入工作流程的名称。

可以使用最多 60 个字母数字字符和空格。

步骤 4　或者，在 **Description** 字段中键入工作流程的说明。

可以使用最多 80 个字母数字字符和空格。

步骤 5　从 **Table** 下拉列表中，选择 **Connection Events**。

步骤 6　或者，向工作流程中添加一个或多个向下钻取页面。

- 要添加包含有关单个连接的数据的向下钻取页面，请点击 **Add Page**。
- 要添加包含连接摘要数据的向下钻取页面，请点击 **Add Summary Page**。

在任一情况下，都会显示向下钻取页面部分。

首先在 **Page Name** 字段中使用最多 80 个字母数字字符 （但无空格）键入页面的名称。

在 **Column 1** 下，选择排序优先级和表列。此列将显示在页面最左侧的列中。

继续选择要包含的字段并设置其排序优先级，直到指定要在页面上显示的所有字段为止。每页可以指定最多五个字段。

例如，要创建显示通过监控网络传输的流量的页面，并要按传输了最多流量的响应方对页面进行排序，请从 **Sort Priority** 下拉列表中选择 **1**，并从 **Field** 下拉列表中选择 **Responder Bytes**。

步骤 7　或者，点击 **Add Graph** 以向工作流程中添加一个或多个图形页面。

系统将显示图形部分。

首先在 **Graph Name** 字段中使用最多 80 个字母数字字符 （但无空格）键入页面的名称。

然后，选择要包含在页面中的图形的类型：折线图、条形图或饼图。

然后，通过选择图形的 x 轴和 y 轴指定要图形化的数据种类。在饼图中，x 轴表示独立变量，y 轴表示因变量。

最后，选择要包含在图形中的数据集。请注意，饼图只能包含一个数据集。

步骤 8　或者，通过点击 **Add Table View** 添加连接数据表视图。

步骤 9　点击 **Save**。

新工作流程保存并添加到自定义工作流程列表中。

查看自定义工作流程

许可证：任何环境

用于查看工作流程的方法取决于工作流程是基于其中一个预定义事件表还是基于自定义表。

如果自定义工作流程基于预定义事件表，请以与访问设备随附的工作流程相同的方式对其进行访问。例如，要根据 Hosts 表访问自定义工作流程，请选择 **Analysis Hosts**。另一方面，如果自定义工作流程基于自定义表，则必须从 Custom Tables 页面对其进行访问。

提示　可以将自定义工作流程设置为任何事件类型的默认工作流程；请参阅第 71-3 页上的配置事件查看设置。

有关详情，请参阅：

- 第 58-37 页上的查看预定义表的自定义工作流程
- 第 58-38 页上的查看自定义表的自定义工作流程

查看预定义表的自定义工作流程

许可证：任何环境

使用以下过程查看**不是**基于自定义表的自定义工作流程。请记住，工作流程访问取决于平台和用户角色，如第 58-14 页上的选择工作流程中所述。

要根据预定义表查看自定义工作流程，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　为自定义工作流程所基于的表选择适当的菜单路径和选项，如使用工作流程的功能表中所述。

系统将显示该表的默认工作流程的第一页。要使用其他工作流程，包括自定义工作流程，请点击当前工作流程标题旁边的 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示事件并且可按时间限制工作流程，则可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

查看自定义表的自定义工作流程

许可证：FireSIGHT

使用以下过程查看不是基于自定义表的自定义工作流程。

要根据自定义表查看自定义工作流程，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Custom > Custom Tables**。

系统将显示 Custom Tables 页面，其中列出了可用的自定义表。

步骤 2　点击要查看的自定义表旁边的查看图标，或者点击自定义表的名称。

系统将显示该表的默认工作流程的第一页。要使用其他工作流程，包括自定义工作流程，请点击当前工作流程标题旁边的 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示事件并且可按时间限制工作流程，则可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

编辑自定义工作流程

许可证：任何环境

如果事件评估过程更改，则可以编辑自定义工作流程来满足新的需求。请注意，不能编辑任何预定义工作流程。

要编辑自定义工作流程，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Custom > Custom Workflows**。

系统将显示 Custom Workflows 页面，其中列出了现有自定义工作流程。

步骤 2　点击要编辑的工作流程名称旁边的编辑图标 ( )。

系统将显示 Edit Workflow 页面。

步骤 3　对工作流程进行所希望的任何更改，然后点击 **Save**。

系统保存已对工作流程进行的保存。

删除自定义工作流程

许可证：任何环境

以下过程说明如何删除不再需要的自定义工作流程。

要删除自定义工作流程，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Custom > Custom Workflows**。

系统将显示 Custom Workflows 页面，其中列出了可用的自定义工作流程。

步骤 2　点击要删除的工作流程名称旁边的删除图标 ( )。

系统删除工作流程。

使用自定义表

FireSIGHT 系统 收集有关网络的信息，防御中心 则将这些信息存储在一系列数据库表中。当您使用工作流程查看生成的信息时，防御中心会从其中一个表提取数据。例如， Network Applications by Count 工作流程的每个页面的列取自 Applications 表中的字段。

如果您确定通过组合不同表中的字段会增强对网络上活动的分析，则可创建自定义表。例如，可以将预定义 Host Attribute 表中的主机重要性信息与预定义 Connection Data 表中的字段进行组合，然后在新的上下文中检查连接数据。

请注意，您可以为预定义表或自定义表创建自定义工作流程。有关创建自定义工作流程的详细信息，请参阅。

以下章节介绍如何创建和使用您自己的自定义表：

了解自定义表

许可证：FireSIGHT

自定义表包含两个或多个预定义表中的字段。 FireSIGHT 系统随附多个系统定义的自定义表，但是，您可以创建其他仅包含符合自身特定需求的信息的自定义表。

例如， FireSIGHT 系统随附用于将入侵事件数据与主机数据相关联的系统定义的自定义表，因此，您可以搜索会影响关键系统的事件并在一个工作流程中查看搜索结果。下表介绍系统随附的自定义表。

表 59-1　　系统定义的自定义表

表	说明
Hosts with Servers	包含 Hosts 和 Servers 表中的字段，提供有关检测到的在网络上运行的应用的信息，以及有关运行这些应用的主机的基本操作系统信息。
Intrusion Events with Destination Criticality	包含 Intrusion Events 表和 Hosts 表中的字段，提供有关入侵事件的信息，以及每个入侵事件涉及的目标主机的主机重要性。 **提示**　使用此表可搜索涉及主机重要性高的目标主机的入侵事件。
Intrusion Events with Source Criticality	包含 Intrusion Events 表和 Hosts 表中的字段，提供有关入侵事件的信息，以及每个入侵事件涉及的源主机的主机重要性。 **提示**　使用此表可搜索涉及主机重要性高的源主机的入侵事件。

了解可能的表组合

许可证：FireSIGHT + 保护

创建自定义表时，可以组合具有相关数据的预定义表中的字段。下表列出了可以组合创建新的自定义表的预定义表。请记住，您可以创建将两个以上的预定义自定义表中的字段进行组合的自定义表。

表 59-2　　自定义表组合

可以将这些表中的字段...	与这些表中的字段进行组合...
应用	• Correlation Events • Intrusion Events • Connection Summary Data • Host Attributes • Application Details • Discovery Events • Connection Events • 主机 • 服务器 • White List Events
Correlation Events	• 应用 • Host Attributes • 主机
Intrusion Events	• 应用 • Host Attributes • 主机 • 服务器

表 59-2　　自定义表组合 （续）

可以将这些表中的字段...	与这些表中的字段进行组合...
Connection Summary Data	• 应用 • Host Attributes • 主机 • 服务器
Indications of Compromise	• 应用 • Application Details • Captured Files • Connection Events • Connection Summary Data • Correlation Events • Discovery Events • Host Attributes • 主机 • Intrusion Events • Security Intelligence Events • 服务器 • White List Events
Host Attributes	• 应用 • Correlation Events • Intrusion Events • Connection Summary Data • Application Details • Discovery Events • Connection Events • 主机 • 服务器 • White List Events
Application Details	• 应用 • Host Attributes • 主机
Discovery Events	• 应用 • Host Attributes • 主机

表 59-2　　自定义表组合 （续）

可以将这些表中的字段...	与这些表中的字段进行组合...
Connection Events	• 应用 • Host Attributes • 主机 • 服务器
Security Intelligence Events	• 应用 • Host Attributes • 主机 • 服务器
主机	• 应用 • Correlation Events • Intrusion Events • Connection Summary Data • Host Attributes • Application Details • Discovery Events • Connection Events • 服务器 • White List Events
服务器	• 应用 • Intrusion Events • Connection Summary Data • Host Attributes • Connection Events • 主机
White List Events	• 应用 • Host Attributes • 主机

有时，一个表中的字段会映射到另一个表中的多个字段。例如，预定义的 **Intrusion Events with Destination Criticality** 自定义表将 Intrusion Events 表和 Hosts 表中的字段进行组合。Intrusion Events 表中的每个事件具有两个与其关联的 IP 地址：源 IP 地址和目标 IP 地址。但是， Hosts 表中的每个“事件”表示单个主机 IP 地址 （主机可能有多个 IP 地址）。因此，根据 Intrusion Events 表和 Hosts 表创建自定义表时，必须选择从 Hosts 表显示的数据适用于 Intrusion Events 表中的主机源 IP 地址还是主机目标 IP 地址。

创建新的自定义表时，会自动创建显示表中所有列的默认工作流程。此外，如同预定义表一样，您可以搜索自定义表来获取要在网络分析中使用的数据。您还可以根据自定义表生成报告，就像使用预定义表时一样。

有关创建自定义表的详细信息，请参阅：

创建自定义表

许可证：FireSIGHT

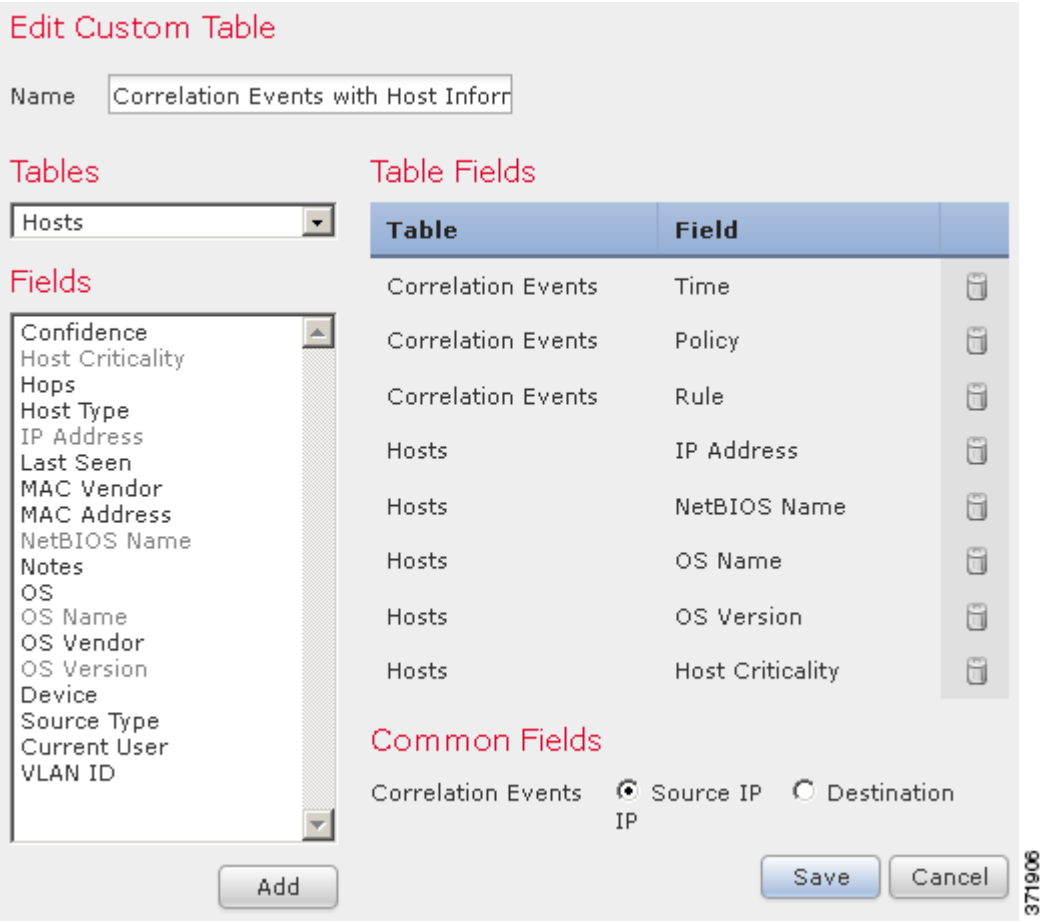
如果您确定通过组合不同表中的字段会增强对网络上活动的分析，则可创建自定义表。

提示 可以从另一个防御中心导出自定义表，然后将其导入到您的防御中心，而不是创建新的自定义表。然后，您可以根据自身需求对导入的自定义表进行编辑。有关详细信息，请参阅第 A-1 页上的导入和导出配置。

要创建自定义表，请确定 FireSIGHT 系统随附的哪些预定义表含有要在自定义表中包含的字段。然后，可以选择要包含的字段，如有必要，请为所有公共字段配置字段映射。

提示 借助涉及 Hosts 表的数据，可以查看与来自一台主机的所有 IP 地址而不是一个特定 IP 地址相关的数据。

例如，不妨考虑将 Correlation Events 表和 Hosts 表中的字段组合起来以创建自定义表。通过这样的自定义表，您可以获取有关涉及任何关联策略违例的主机的详细信息。请注意，您必须决定从 Hosts 表显示与 Correlation Events 表中的源 IP 地址还是目标 IP 地址匹配的数据。



如果查看此自定义表的事件表视图，则它会显示相关性事件 （每行一个）。包含以下信息：

- 事件的生成日期和时间
- 违例的关联策略的名称
- 触发违例的规则的名称
- 与相关性事件中涉及的源主机 （又称为发起主机）相关的 IP 地址
- 源主机的 NetBIOS 名称
- 源主机运行的操作系统和版本
- 源主机的关键性

提示　可以创建类似的自定义表来显示目标主机 （又称为响应主机）的以上信息。

要构建上一示例中所述的自定义表，请执行以下操作：

访问：管理

步骤 1　选择 **Analysis > Custom > Custom Tables**。

系统将显示 Custom Tables 页面。

步骤 2　点击 **Create Custom Table**。

系统将显示 Create Custom Table 页面。

步骤 3　在 **Name** 字段中，键入自定义表的名称，例如 `Correlation Events with Host Information (Src IP)`。

步骤 4　从 **Tables** 下拉列表中，选择 **Correlation Events**。

Correlation Events 表中的字段将会显示在 **Fields** 列表中。

步骤 5　在 **Fields** 下，选择 **Time** 并点击 **Add** 以添加生成相关性事件的日期和时间。

步骤 6　重复第 5 步以添加 **Policy** 和 **Rule** 字段。

提示　按住 Ctrl 或 Shift 键并点击可选择多个字段。也可以点击并拖动以选择多个相邻值。但是，如果要指定字段在与表关联的事件表视图中的出现顺序，请一次添加一个字段。

步骤 7　从 **Tables** 下拉列表中，选择 **Hosts**。

Hosts 表中的字段将会显示在 **Fields** 列表中。有关这些字段的详细信息，请参阅第 50-18 页上的了解主机表。

步骤 8　向自定义表添加 **IP Address**、 **NetBIOS Name**、 **OS Name**、 **OS Version** 和 **Host Criticality** 字段。

步骤 9　在 **Common Fields** （位于 **Correlation Events** 旁边）下，选择 **Source IP**。

这样，自定义表即配置为显示在第 8 步中选择的有关相关性事件中涉及的源主机 （又称为发起主机）的主机信息。

提示　可以按照以上步骤创建显示有关相关性事件中涉及的目标主机 （又称为响应主机）的主机详细信息的自定义表，但在操作过程中应选择 **Destination IP** 而不是 **Source IP**。

步骤 10　点击 **Save**。

即会保存自定义表。

修改自定义表

许可证：FireSIGHT

您可以根据自身需求在自定义表中添加或删除字段。

要修改自定义表，请执行以下操作：

访问：任何角色/管理员

步骤 1　选择 **Analysis > Custom > Custom Tables**。

系统将显示 Custom Tables 页面。

步骤 2　点击要编辑的表旁边的编辑图标 ( )。

系统将显示 Edit Custom Table 页面。有关可更改的各种配置的信息，请参阅第 59-5 页上的创建自定义表。

步骤 3　或者，点击要删除的字段旁边的删除图标 ( )，从表中删除字段。

注　如果您删除报告中当前正在使用的字段，则系统将提示您确认是否要删除使用这些报告中的这些字段的部分。

步骤 4　根据需要进行其他更改，然后点击 **Save**。

即会更新您的自定义表。

删除自定义表

许可证：FireSIGHT

可以删除不再需要的自定义表。如果删除自定义表，同时会删除使用该自定义表的已保存搜索。

要删除自定义表，请执行以下操作：

访问：任何角色/管理员

步骤 1　选择 **Analysis > Custom > Custom Tables**。

系统将显示 Custom Tables 页面。

步骤 2　点击要删除的自定义表旁边的删除图标 ( )。

即会删除该表。

根据自定义表查看工作流程

许可证：FireSIGHT

创建自定义表时，系统会自动为其创建默认工作流程。默认工作流程的第一页显示事件表视图。如果在自定义表中包含入侵事件，则工作流程的第二页是数据包视图。否则，工作流程的第二页是主机页面。您也可以根据自定义表创建自己的自定义工作流程。

提示　根据某个自定义表创建自定义工作流程后，可以将创建的自定义工作流程指定为该自定义表的默认工作流程。有关详细信息，请参阅第 71-3 页上的配置事件查看设置。

您可以使用相同方法查看自定义表中根据预定义表用于事件视图的事件。有关详情，请参见第 58-16 页上的使用工作流程页面。

要根据自定义表查看工作流程，请执行以下操作：

访问：任何角色/管理员

步骤 1　选择 **Analysis > Custom > Custom Tables**。

系统将显示 Custom Tables 页面。

步骤 2　点击要查看的工作流程创建时所依据的自定义表旁边的查看图标 ( )。

系统将显示该自定义表的默认工作流程的第一页。要使用其他工作流程，请点击按工作流程标题 **(switch workflow)**。有关如何指定其他默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示事件并且可按时间限制工作流程，则可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

搜索自定义表

许可证：FireSIGHT

可以创建和保存面向自定义表的搜索。您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。请注意，如果删除自定义表，同时会删除已为该自定义表保存的所有搜索。

您可以使用的搜索条件与用于构建自定义表的预定义表的条件相同。有关可以使用的搜索条件的详细信息，请参阅下表中列出的各个章节。

表 59-3　　表搜索条件

有关以下自定义表的搜索条件.....	请参阅.....
Audit Events	第 69-8 页上的搜索审计记录
Application Details	第 50-42 页上的搜索应用详情
Correlation Events	第 51-51 页上的搜索关联事件
连接数据	第 39-27 页上的搜索连接和安全情报数据
主机	第 50-21 页上的搜索主机
Host Attributes	第 50-26 页上的搜索主机属性
Hosts with Applications	第 50-21 页上的搜索主机 和 第 50-34 页上的搜索服务器
Intrusion Events	第 41-36 页上的搜索入侵事件
Intrusion Events with Destination Criticality	第 41-36 页上的搜索入侵事件 和 第 50-21 页上的搜索主机
Intrusion Events with Source Criticality	第 41-36 页上的搜索入侵事件 和 第 50-21 页上的搜索主机
Status Events	第 54-18 页上的搜索补救状态事件
Discovery Events	第 50-15 页上的搜索发现事件
User Events	第 50-59 页上的搜索用户活动
规则更新导入日志	第 66-22 页上的搜索规则更新导入日志
应用	第 50-38 页上的搜索应用
Security Intelligence Events	第 39-27 页上的搜索连接和安全情报数据
用户	第 50-55 页上的搜索用户
漏洞	第 50-46 页上的搜索漏洞
White List Events	第 52-29 页上的搜索合规白名单事件
White List Violations	第 52-33 页上的搜索白名单的违规事件

要在表搜索中执行这些条件，请参阅以下过程。

要对自定义表执行搜索，请执行以下操作：

访问：任何角色/管理员

步骤 1　选择 **Analysis > Custom > Custom Tables**。

系统将显示 Custom Tables 页面。

步骤 2　点击要搜索的自定义表旁边的查看图标 ( )。

系统将显示该自定义表的默认工作流程的第一页。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示事件并且可按时间限制工作流程，则可能需要调整时间范围；请参阅第 58-19 页上的设置事件时间限制。

步骤 3　点击 **Search**。

系统将显示自定义表的搜索页面。

提示　要在数据库中搜索另一类型的事件或数据，请从表下拉列表选择它。

步骤 4　在相应字段输入搜索条件。有关选择搜索条件的详细信息，请参阅表搜索条件表。

如果您输入多个字段的条件，搜索只返回符合所有字段指定搜索条件的记录。

提示　点击搜索字段旁边的对象图标 ( ) 可将对象用作搜索条件。有关搜索的更多信息（包括有关特殊搜索语法、在搜索中使用对象以及保存并载入搜索的信息），请参阅第 60-1 页上的执行和保存搜索。

步骤 5　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 6　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功（如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功（如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 7　点击 **Search** 开始搜索。

搜索结果显示在自定义表的默认工作流程中，通过当前时间范围（如适用）进行约束。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

搜索事件

思科设备生成的信息作为事件存储在数据库表中。事件包含多个字段，描述导致设备生成事件的活动。

FireSIGHT 系统提供预定义搜索，既可将其用作示例，又可借助其快速访问关于网络的重要信息。可针对网络环境修改预定义搜索中的字段，然后保存搜索，以供日后重复使用。还可使用自己的搜索条件。

可使用的搜索条件取决于搜索类型，但搜索技巧相同。请参阅以下各节，了解有关如何执行搜索和在搜索字段中使用正确语法的详细信息。

执行和保存搜索

许可证：任何环境

可为任何不同的事件类型创建和保存搜索。创建搜索时，请为其命名，并指定此搜索仅供您自己使用还是供设备的所有用户使用。如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

有关详细信息，请参阅以下各节：

注 要搜索自定义表，请遵循略有不同的步骤；请参阅第 59-9 页上的搜索自定义表。

执行搜索

许可证：任何环境

对于某些事件类型， FireSIGHT 系统提供预定义搜索，既可将其用作示例，又可借助其快速访问关于网络的重要信息。可针对网络环境修改预定义搜索中的字段，然后保存搜索，以供日后重复使用。还可使用自己的搜索条件。

要执行搜索，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中，选择想搜索的事件或数据的类型

系统将用相应搜索约束更新页面。

步骤 3　在相应字段输入搜索条件：

- 所有字段都接受求反 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 搜索仅返回与所有字段的指定搜索条件匹配的记录。
- 许多字段接受一个或多个星号 (*) 作为通配符。
- 在任一字段指定 `n/a` 以便识别信息不适用于该字段的事件；使用 `!n/a` 识别字段填充事件。
- 点击搜索字段旁边的添加对象图标 (✚)，使用对象作为搜索条件。

步骤 4　请参阅以下各节，了解有关可使用的搜索条件的详细信息。

- 第 69-8 页上的搜索审计记录
- 第 50-38 页上的搜索应用
- 第 50-42 页上的搜索应用详情
- 第 40-28 页上的搜索捕获文件
- 第 52-29 页上的搜索合规白名单事件
- 第 39-27 页上的搜索连接和安全情报数据
- 第 51-51 页上的搜索关联事件
- 第 50-15 页上的搜索发现事件
- 第 40-11 页上的搜索文件事件

- 第 68-50 页上的搜索运行状况事件
- 第 50-26 页上的搜索主机属性
- 第 50-21 页上的搜索主机
- 第 41-36 页上的搜索入侵事件
- 第 40-22 页上的搜索恶意软件事件
- 第 66-22 页上的搜索规则更新导入日志
- 第 54-18 页上的搜索补救状态事件
- 第 47-21 页上的搜索扫描结果
- 第 50-34 页上的搜索服务器
- 第 50-50 页上的搜索第三方漏洞
- 第 50-55 页上的搜索用户
- 第 50-59 页上的搜索用户活动
- 第 50-46 页上的搜索漏洞
- 第 52-33 页上的搜索白名单的违规事件

步骤 5　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 6　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 7　点击 **Search** 开始搜索。

搜索结果出现在正在搜索的表的默认工作流程中，受时间约束 （如适用）。要使用不同的工作流程，包括自定义工作流程，请按照工作流程标题点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。请注意，**不能**将不同的工作流程用于扫描结果。

加载已保存的搜索

许可证：任何环境

如果先前保存了一个搜索，则可加载该搜索，做出任何必要更改，然后开始搜索。

要加载已保存的搜索，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　您有以下选项：

- 从工作流程的任意页面，点击 **Search**。
- 选择 **Analysis > Search**，然后选择想搜索的事件的类型。

系统将显示 Search 页面。

步骤 2　选择您要从 Custom Searches 列表或 Predefined Searches 列表加载的搜索。

系统用已保存搜索中的设置填充搜索约束。

步骤 3　或者，更改搜索约束。

步骤 4　点击 **Search**。

系统显示符合搜索约束的事件。

删除已保存的搜索

许可证：任何环境

如有已保存的搜索，可从 Search 页面删除这些搜索。

要删除已保存的搜索，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1　您有以下选项：

- 从工作流程的任意页面，点击 **Search**。
- 选择 **Analysis > Search**，然后为想删除的搜索选择事件类型。

系统将显示 Search 页面。

步骤 2　从 Custom Searches 列表中，选择要删除的搜索并点击搜索名称旁的删除图标 (✖)。

搜索删除成功。

在搜索中使用通配符和符号

许可证：任何环境

在搜索页面的许多文本字段中，可使用星号 (*) 匹配字符串中的字符。例如，指定 `net*` 匹配 `network`、`netware`、`netscape` 等等。

如果想要搜索非字母数字字符 （包括星号字符），请用引号将搜索字符串引起来。例如，要搜索字符串：

```
Find an asterisk (*)
```

输入：

```
"Find an asterisk (*)"
```

请注意，在允许输入通配符的文本字段中，如要匹配部分字符串**必须**使用通配符。例如，如在审计日志中搜索所有涉及页面视图 （即，消息为 Page View) 的审计记录，搜索 `Page` 将不返回结果。因此，请指定 `Page*`。

在搜索中使用对象和应用过滤器

许可证：任何环境

FireSIGHT 系统可用于创建可用作网络配置一部分的已命名对象、对象组和应用过滤器。执行或保存搜索时，可使用这些对象、组和过滤器作为搜索条件。

执行搜索时，对象、对象组和应用过滤器以 `${object_name}` 格式显示。例如，有对象名称 `ten_ten_network` 的网络对象在搜索中显示为 `${ten_ten_network}`。

在可使用对象作为搜索条件的搜索字段旁边，可点击添加对象图标 (+)。

在搜索中指定时间约束

许可证：任何环境

可使用多种格式指定时间搜索约束。可输入要匹配的时间以及 （或者）小于 (<) 或大于 (>) 运算符，与已输入时间之前或之后的时间相匹配。

下表显示了采用时间值的搜索条件字段接受的格式。

表 60-1　　搜索字段中的时间规范

时间格式	示例
today [at HH:MMam|pm]	`today` `today at 12:45pm`
YYYY-MM-DD HH:MM:SS	`2006-03-22 14:22:59`

可在时间值前输入下列运算符/关键字之一。

表 60-2　　时间规格运算符

运算符	示例	说明
<	`< 2006-03-22 14:22:59`	返回时间戳早于 2006 年 3 月 22 日下午 2:23 的事件。
>	`> today at 2:45pm`	返回时间戳晚于今天下午 2:45 的事件。

在搜索中指定 IP 地址

许可证：任何环境

在搜索中指定 IP 地址时，可输入单个 IP 地址、用逗号隔开的地址列表、地址块或者一系列用连字符 (-) 隔开的 IP 地址。也可使用求反。

对于支持 IPv6 的搜索 （例如，入侵事件、连接数据和关联事件搜索），可输入 IPv4 和 IPv6 地址与 CIDR/前缀长度地址块的任意组合。

使用 CIDR 或前缀长度表示法指定 IP 地址块时，FireSIGHT 系统只使用前缀长度指定的网络 IP 地址部分。例如，如果键入 `10.1.2.3/8`， FireSIGHT 系统 使用 `10.0.0.0 /8`。

下表包含 IP 地址有效输入方式的示例。因为 IP 地址可以用网络对象表示，所以，也可点击 IP 地址搜索字段旁边的添加网络对象图标 (✚)，使用网络对象作为 IP 地址搜索条件。有关详细信息，请参阅第 60-5 页上的在搜索中使用对象和应用过滤器。

表 60-3　　可接受的 IP 地址语法

指定的对象	键入的内容	示例
单个 IP 地址	IP 地址。	`192.168.1.1` `2001:db8::abcd`
多个 IP 地址，使用列表	用逗号隔开的 IP 地址列表。请**不要**在逗号前后添加空格。	`192.168.1.1,192.168.1.2` `2001:db8::b3ff,2001:db8::0202`
可以使用 CIDR 块或前缀长度指定的一系列 IP 地址	采用 IPv4 CIDR 或 IPv6 前缀长度表示法的 IP 地址块。	`192.168.1.0/24` 这可在子网掩码为 255.255.255.0 的 192.168.1.0 网络中指定任意 IP，即 192.168.1.0 至 192.168.1.255。有关详细信息，请参阅第 1-16 页上的IP 地址约定。
不能使用 CIDR 块或前缀指定的 IP 地址范围	使用连字符的 IP 地址范围。请**不要**在连字符前后添加空格。	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

用于指定 IP 地址或 IP 地址范围的任何其他方法的求反	在 IP 地址、块或范围前面输入感叹号。	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

在搜索中指定设备

许可证：任何环境

在使用受管设备作为限制创建搜索时，您可以在 **Device** 搜索条件字段指定以下任一项：

- 受管设备名称、 IP 地址或主机名
- 设备组名称
- 设备堆栈名称
- 设备集群名称

如果系统找到组、集群或堆栈的一个匹配项，系统会用用于执行搜索的相应成员设备名称替换组、集群或堆栈名称。在设备字段保存使用了设备组、集群或堆栈的搜索时，系统会保存设备字段中指定的名称，并且每次执行搜索时都会再次执行设备名称替换。

有关详细信息，请参阅：

- 第 4-16 页上的处理设备
- 第 4-23 页上的管理设备组
- 第 4-37 页上的管理堆叠设备
- 第 4-25 页上的集群设备

在搜索中指定端口

许可证：任何环境

FireSIGHT 系统 接受搜索中端口号的特定语法。可输入：

- 单个端口号
- 用逗号隔开的端口号列表。
- 两个用连字号隔开的端口号，代表端口号范围
- 后接协议缩写、并用正斜杠隔开的端口号 （仅限搜索入侵事件时）
- 一个端口号或端口号范围，前面带有感叹号，表示指定端口的求反

注 指定端口号或范围时，请**不要**使用空格。

下表包含输入端口作为搜索约束的有效方法的示例。

\

表 60-4　　端口语法示例

示例	说明
`21`	返回端口 21 上的所有事件，包括 TCP 和 UDP 事件。
`!23`	返回除端口 23 上的事件以外的所有事件。
`25/tcp`	返回端口 25 上的所有与 TCP 相关的入侵事件。
`21/tcp,25/tcp`	返回端口 21 和 25 上所有与 TCP 相关的入侵事件
`21-25`	返回端口 21 到 25 上的所有事件。

停止长期查询

许可证：任何环境

受支持的设备：任意防御中心

系统管理员可以使用基于外壳的查询管理工具找到和停止长期查询。

注 退出网络界面的搜索页面不会停止查询。需要很长时间才返回结果的查询在运行时会影响总体系统性能。

借助于查询管理工具，可找到并停止运行时间超过指定分钟数的查询。停止查询时，此工具会将事件记入审计日志和系统日志。

请注意，只有在本地创建并且在防御中心上拥有外壳访问权限的用户才是 admin 用户。如果使用授予外壳访问权限的外部身份验证对象，匹配外壳访问过滤器的用户也可以登录外壳。

用法：

```
query_manager [-v] [-l [minutes]] [-k query_id [...]]
[--kill-all minutes]
```

选择：

`-h, --help`
打印简短的帮助消息。

`-l, --list [minutes]`
列出所有运行时间超过已用分钟数的查询。的

默认情况下，它将显示所有运行时间超过 1 分钟的查询。

`-k, --kill query_id [...]`
中止 ID 中带有指定分钟数的查询。此选项可以采用

多个 ID。

`--kill-all minutes`
中止运行时间超过指定分钟数的所有查询。

`-v, --verbose`
包含完整 SQL 查询的详细输出。

注意事项　外壳访问权应仅限于系统管理员。

要停止防御中心上的查询，请执行以下操作：

访问：admin 或其他被授予外壳访问权限的用户

步骤 1　通过 ssh 连接至防御中心。

步骤 2　使用上文描述的语法在 sudo 下面运行 query_manager。

管理用户

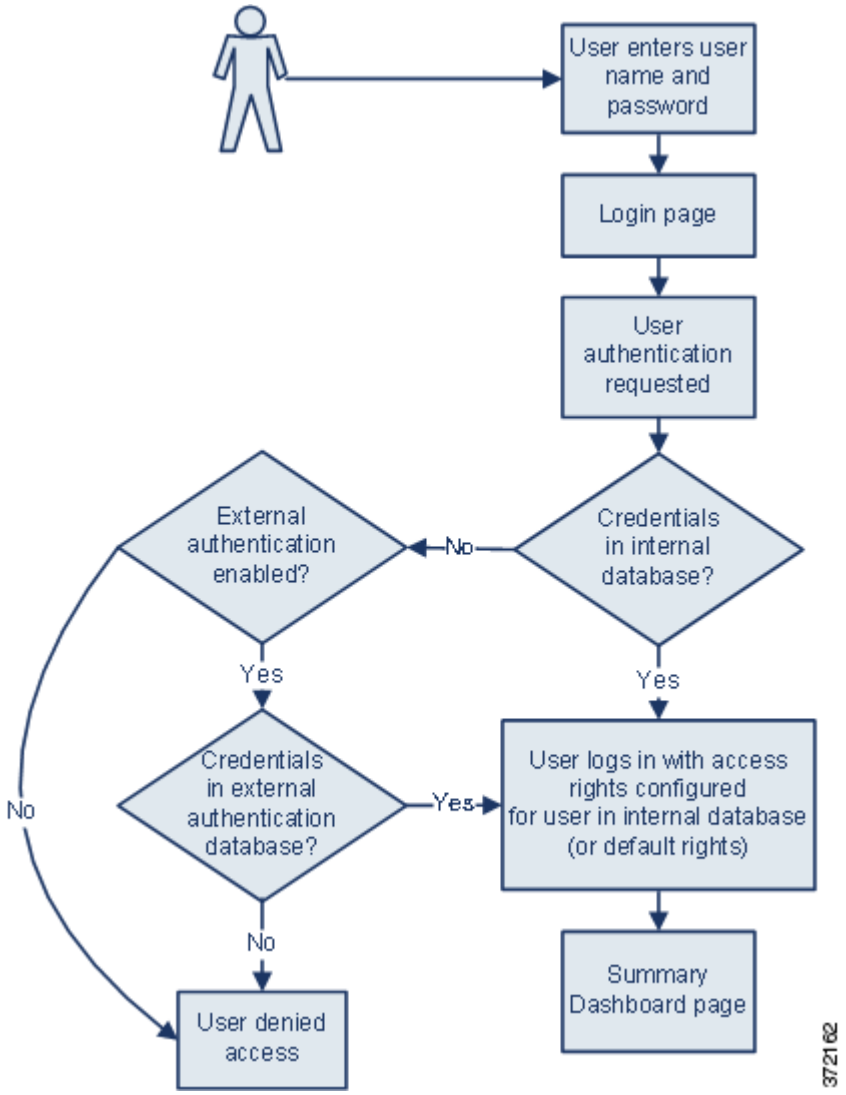
如果用户帐户具有管理员访问权，则可以管理能够访问防御中心或受管设备上的 Web 界面的用户帐户。在防御中心上，还可以通过外部身份验证服务器而不是通过内部数据库来设置用户身份验证。

有关详细信息，请参阅：

了解思科用户身份验证

许可证：任何环境

当用户登录到 Web Web 界面中时，设备会在用户本地列表中查找用户名和密码的匹配项。此过程称为*身份验证*。有两种身份验证：内部和外部。如果用户帐户使用*内部身份验证*，则身份验证过程检查本地数据库以获取此列表。如果帐户使用*外部身份验证*，则该过程会检查本地数据库以查看其中是否存在该用户，如果在本地找不到该用户，则会查询诸如轻量目录访问协议 (LDAP) 目录服务器或远程身份验证拨入用户服务 (RADIUS) 身份验证服务器之类的外部服务器来获取用户列表。



对于带有内部或外部身份验证的用户，可以控制用户权限。除非手动更改用户权限，否则带有外部身份验证的用户会接收其所属的组或访问列表的权限，或者接收基于在服务器身份验证对象中或在管理防御中心上的系统策略中设置的默认用户访问角色的权限。

有关详细信息，请参阅：

- 第 61-2 页上的了解内部身份验证
- 第 61-3 页上的了解外部身份验证
- 第 61-3 页上的了解用户权限

了解内部身份验证

许可证：任何环境

默认情况下， FireSIGHT 系统在用户登录时使用内部身份验证检查用户凭证。根据内部 FireSIGHT 系统数据库中的记录验证用户名和密码时，即发生内部身份验证。如果在创建用户时不启用外部身份验证，则会在内部数据库中管理用户凭证。

由于是手动创建每个进行内部身份验证的用户，因此在创建用户时设置访问权限，并且无需设置默认设置。

注　请注意，在以下情况下，进行内部身份验证的用户会转换为外部身份验证：启用外部身份验证，对于外部服务器上的用户存在同一用户名，用户使用在外部服务器上为该用户存储的密码进行登录。内部身份验证用户转换为外部身份验证用户后，无法还原为该用户的内部身份验证。

了解外部身份验证

许可证：任何环境

当防御中心或受管设备从外部存储库（例如，LDAP 目录服务器或 RADIUS 身份验证服务器）检索用户凭证时，即发生外部身份验证。 LDAP 身份验证和 RADIUS 身份验证是外部身份验证类型。请注意，只能为设备使用一种形式的外部身份验证。

如果要使用外部身份验证，必须为要请求用户信息的每个外部身份验证服务器都配置*身份验证对象*。身份验证对象包含用于连接到该服务器和从中检索用户数据的设置。然后，可以在主管防御中心上的系统策略中启用该对象，并将策略应用到要启用身份验证的设备。当任何外部身份验证用户登录时， Web 界面会检查每个身份验证服务器，以查看是否按照服务器在系统策略中的列出顺序列出该用户。

创建用户时，可以指定对该用户进行内部还是外部身份验证。

注　在3 系列 受管设备上启用外部身份验证之前，请移除与外壳访问过滤器中包含的外部身份验证用户具有相同用户名的所有内部身份验证外壳用户。

可以将系统策略推送到受管设备，以在该设备上启用外部身份验证，但是不能从设备的 Web 界面控制身份验证对象。为新用户选择身份验证类型时，将会对设备上的外部身份验证进行唯一配置。如果要在受管设备上禁用外部身份验证，请在管理防御中心上的系统策略中将其禁用，并将策略重新应用到该设备。如果将在受管设备上创建的本地系统策略应用到设备本身，则还会禁用外部身份验证。

提示　可以使用导入/导出功能导出系统策略。导出已启用外部身份验证的策略时，身份验证对象随该策略导出。然后，可以在另一个防御中心上导入策略和对象。**请勿**将含有身份验证对象的策略导入到受管设备上。

有关特定类型的外部身份验证的详细信息，请参阅：

- 第 61-5 页上的 LDAP 身份验证
- 第 61-28 页上的 RADIUS 身份验证

了解用户权限

许可证：任何环境

通过 FireSIGHT 系统，可以根据用户的角色分配用户权限。例如，分析师通常需要访问事件数据以分析监控网络的安全性，但是，可能从不需要访问 FireSIGHT 系统本身的管理功能。可以授予分析师预定义角色（如 Security Analyst 和 Discovery Admin）并为管理 FireSIGHT 系统的网络管理员保留管理员角色。也可以创建具有根据贵组织需求定制的访问权限的自定义用户角色。

在防御中心上的系统策略中，为所有进行外部身份验证的用户设置默认访问角色。外部身份验证用户首次登录后，可以在 User Management 页面上添加或移除该用户的访问权限。如果没有修改用户权限，则用户仅具有默认授予的权限。由于是手动创建内部身份验证用户，因此在创建这些用户时设置访问权限。

如果通过 LDAP 组配置访问权限的管理，则用户的访问权限基于其在 LDAP 组中的成员资格。他们接收其所属的具有最高访问级别的组的默认访问权限。如果他们不属于任何组，并且您已配置组访问权，则他们会接收在 LDAP 服务器的身份验证对象中配置的默认用户访问权限。如果配置组访问权，则这些设置会覆盖系统策略中的默认访问设置。

同样，如果将用户分配到 RADIUS 身份验证对象中的特定用户角色列表，则除非其中一个或多个角色互不兼容，否则该用户会接收分配的所有角色。如果用户在两个互不兼容角色的列表上，则用户会接收具有最高访问级别的角色。如果用户不属于任何列表，并且您已在身份验证对象中配置默认访问角色，则用户会接收该角色。如果已在身份验证对象中配置默认访问，则这些设置会覆盖系统策略中的默认访问设置。

根据已许可的功能， FireSIGHT 系统支持下列预定义用户角色 （按优先顺序列出）：

- *Access Admin* 可以查看并修改访问控制和文件策略，但是无法应用其策略更改。
- *Administrator* 可以设置设备的网络配置，管理用户帐户和综合安全智能云连接，以及配置系统策略和系统设置。承担管理员角色的用户具有所有其他角色的所有权限 （不同在于这些特权的版本更少且受限制）。
- *Discovery Admin* 可以审查、修改和删除网络发现策略，但是无法应用其策略更改。
- *外部数据库*用户可以使用支持 JDBC SSL 连接的外部应用来查询 FireSIGHT 系统数据库。在 Web 界面上，他们可以访问联机帮助和用户首选项。
- *Intrusion Admin* 有权访问所有入侵策略、入侵规则和网络分析策略功能。 Intrusion Admin 有权访问 **Policies** 菜单中与入侵相关的选项。请注意， Intrusion Admin 无法将入侵策略或网络分析策略应用为访问控制策略的一部分。
- *Maintenance User* 可以访问监控功能 （包括运行状况监控、主机统计、性能数据和系统日志）和维护功能 （包括任务安排和备份系统）。

  请注意，维护人员无权访问 **Policies** 菜单中的功能，只能从 **Analysis** 菜单访问控制面板。
- *Network Admin* 可以审查、修改和应用设备配置，以及审查和修改访问控制策略。
- *Security Approver* 可以查看和应用 （但不创建）配置和策略更改。
- *Security Analyst* 可以审查、分析和删除入侵、发现、用户活动、连接、相关性和网络更改事件。他们可以审查、分析及 （适用时）删除主机、主机属性、服务、漏洞和客户端应用。 Security Analyst 还可以生成报告和查看 （但不删除或修改）运行状况事件。
- *Security Analyst (Read Only)* 具有与 Security Analyst 相同的所有权限，不同在于其无法删除事件。

除以上预定义角色外，还可以配置具有专用访问权限的自定义用户角色。任何角色都可以是外部身份验证用户的默认访问角色。

可以向外部身份验证用户帐户授予用户角色升级权限；还可以使用外部身份验证用户的密码作为升级密码。有关详细信息，请参阅第 61-60 页上的管理用户角色升级。

管理身份验证对象

许可证：任何环境

身份验证对象是外部身份验证服务器的服务器配置文件，其中包含这些服务器的连接设置和身份验证过滤器设置。可以在防御中心上创建、配置和删除身份验证对象，并使用其管理向 LDAP 或 RADIUS 服务器进行的外部身份验证。有关详细信息，请参阅：

- 第 61-5 页上的 LDAP 身份验证
- 第 61-28 页上的 RADIUS 身份验证
- 第 61-39 页上的删除身份验证对象

LDAP 身份验证

许可证：任何环境

通过 LDAP （或轻量目录访问协议），可以在网络上设置一个目录，用于在一个集中位置组织对象，如用户凭证。然后，多个应用可以访问这些凭证和用于描述凭证的信息。如果需要更改用户凭证，则可以在一个位置对其进行更改，而不必在每个 FireSIGHT 系统设备上都进行更改。

有关详细信息，请参阅：

- 第 61-5 页上的了解 LDAP 身份验证
- 第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证
- 第 61-11 页上的准备创建 LDAP 身份验证对象
- 第 61-11 页上的创建基本 LDAP 身份验证对象
- 第 61-15 页上的创建高级 LDAP 身份验证对象
- 第 61-24 页上的 LDAP 身份验证对象示例
- 第 61-28 页上的编辑 LDAP 身份验证对象

了解 LDAP 身份验证

许可证：任何环境

可以在防御中心上创建 LDAP 身份验证对象，但不能在其他 FireSIGHT 系统设备上创建这些对象。不过，可以在任何设备 （虚拟设备或 用于 Blue Coat X-系列的思科 NGIPS除外）上使用外部身份验证对象，方法是将已启用此对象的系统策略应用到该设备。应用策略时，会将对象复制到设备上。

注　在3 系列 受管设备上启用外部身份验证之前，请移除与外壳访问过滤器中包含的外部身份验证用户具有相同用户名的所有内部身份验证外壳用户。

请注意，可以将 LDAP 命名标准用于地址规范以及用于身份验证对象中的过滤器和属性语法。有关详细信息，请参阅轻量目录访问控制协议 (v3) 中列出的 RFC：“Technical Specification, RFC 3377” （技术规范， RFC 3377）。本过程各处提供了语法示例。请注意，如果将身份验证对象设置为连接到 Microsoft Active Directory Server，可以在引用包含域的用户名时使用互联网 RFC 822 （ARPA 互联网文本消息格式的标准）规范中记录的地址规范语法。例如，为引用用户对象，可能会在使用 Microsoft Active Directory Server 时键入 `JoeSmith@security.example.com` 而不是等效的用户基础可分辨名称 `cn=JoeSmith,ou=security, dc=example,dc=com`。

注　当前， FireSIGHT 系统在 LDAP 服务器 （在 Windows Server 2003 和 Windows Server 2008 上运行 Microsoft Active Directory，在 Windows Server 2003 和 Windows Server 2008 上运行 Oracle Directory Server Enterprise Edition 7.0，或在 Linux 上运行 OpenLDAP）上支持 LDAP 外部身份验证。但是，FireSIGHT 系统不支持虚拟设备或 用于 Blue Coat X-系列的思科 NGIPS的外部身份验证。

有关详细信息，请参阅：

了解默认值

许可证：任何环境

可以根据计划连接到的服务器类型使用默认值填充若干字段。选择服务器类型并设置默认值时，默认值传播 User Name Template、 UI Access Attribute、 Shell Access Attribute、 Group Member Attribute 和 Group Member URL Attribute 字段。

了解基础 DN

许可证：任何环境

当本地设备搜索 LDAP 服务器以检索身份验证服务器上的用户信息时，它需要该搜索的起点。可以通过提供基础可分辨名称 （或基础 *DN*）指定本地设备应搜索的树。

通常，基础 DN 具有指示公司领域和运营单位的基础结构。例如， Example 公司的 Security 部门的基础 DN 可能为 `ou=security,dc=example,dc=com`。

识别主服务器后，可以自动从中检索可用基础 DN 的列表并选择相应的基础 DN。

了解基本过滤器

许可证：任何环境

您可以添加一个设置特定属性特定值的*基本过滤器*（最多 450 个字符，包括附带的括号）。基本过滤器通过仅检索基础 DN 中具有过滤器中设置的属性值的对象来专注搜索。请将基本过滤器用括号括起来。例如，要仅对具有以 F 开头的公共名称的用户进行过滤，请使用过滤器 `(cn=F*)`。

要通过输入测试用户名和密码更具体地测试基本过滤器，请参阅第 61-34 页上的测试用户身份验证。

了解模拟帐户

许可证：任何环境

要允许本地设备访问用户对象，必须为模拟帐户提供用户凭证。*模拟帐户*是具有按基础 DN 浏览目录名称并检索要检索的用户对象的适当权限的用户帐户。请记住，所指定用户的可分辨名称对于服务器树必须唯一。

了解 LDAP 连接

许可证：任何环境

可以管理 LDAP 连接的加密方法。可以选择不加密、传输层安全 (TLS) 或安全套接字层 (SSL) 加密。

请注意，如果在通过 TLS 或 SSL 进行连接时使用证书进行身份验证，则证书中 LDAP 服务器的名称**必须**与在 Host Name/IP Address 字段中使用的名称匹配。例如，如果在外部身份验证设置中输入 `10.10.10.250` 并在证书中输入 `computer1.example.com`，则连接失败。将外部身份验证设置中的服务器名称更改为 `computer1.example.com` 可成功连接。

了解用户名模板

许可证：任何环境

选择用户名模板可通过将字符串转换字符 (`%s`) 映射到用户的 UI 访问属性或外壳访问属性的值来指示应如何格式化登录时输入的用户名。用户名模板是用于身份验证的可分辨名称的格式。当用户将用户名输入到登录页面中时，该名称会替换字符串转换字符，产生的可分辨名称用于搜索用户凭证。

例如，要为 Example 公司的 Security 部门设置用户名模板，可能会输入 `%s@security.example.com`。如果要将对象用于 CAC 身份验证和授权，**必须**输入与 UI 访问属性值对应的用户名模板值。有关详细信息，请参阅第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。

了解连接超时

许可证：任何环境

如果指定备份身份验证服务器，则可以为对主服务器进行的连接尝试设置超时。如果在经过超时期后主身份验证服务器没有响应，则设备将查询备份服务器。例如，如果主服务器已禁用 LDAP，则设备将查询备份服务器。

但是，如果 LDAP 是在主 LDAP 服务器的端口上运行，并且因某种原因而拒绝服务请求（由于配置错误或其他问题），则不会故障转移到备份服务器。

了解用于管理访问的属性

许可证：任何环境

不同类型的 LDAP 服务器使用不同属性来存储用户数据。有关 UI 和外壳访问属性的说明，请参阅以下章节。

UI 访问属性

如果 LDAP 服务器使用 UI 访问属性 `uid`，则本地设备会检查树中由所设置的基础 DN 指示的各对象的 `uid` 属性值。如果没有设置特定 UI 访问属性，则本地设备会检查 LDAP 服务器上各用户记录的可分辨名称以查看其是否与用户名匹配。如果其中一个对象具有匹配的用户名和密码，表明用户登录请求已进行身份验证。

可以替换其他 LDAP 属性，以使本地设备将用户名与该属性而不是可分辨名称值匹配。选择服务器类型并设置默认值将会填写适合于该类型的服务器的 UI 访问属性。如果其中一个对象具有匹配的用户名，而且对于非 CAC 对象，还具有作为您所指定属性的值的密码，系统会对用户登录请求进行身份验证。如果属性的值是 FireSIGHT 系统Web 界面的有效用户名，则可以使用任何属性。有效用户名是唯一的，并且可以包含下划线 (_)、句号 (.)、连字符 (-) 和字母数字字符。如果要将对象用于 CAC 身份验证和授权，**必须**输入与用户名模板值对应的 UI 访问属性值。有关详细信息，请参阅第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。

外壳访问属性

如果 LDAP 服务器使用 `uid` 作为 外壳访问属性，则本地设备会按照 `uid` 的属性值检查在登录时输入的用户名。也可以设置自定义外壳访问属性而非 `uid`。

请注意，选择服务器类型并设置默认值将会预填充通常适合于该类型的服务器的外壳访问属性。如果属性的值是外壳访问的有效用户名，则可以使用任何属性。有效用户名是唯一的，并且可以包含下划线 (_)、句号 (.)、连字符 (-) 和字母数字字符。

了解用于管理访问的组成员资格

许可证：任何环境

如果首选将默认访问权限基于 LDAP 组中的用户成员资格，则可以为 FireSIGHT 系统使用的各访问角色指定 LDAP 服务器上现有组的可分辨名称。执行此操作时，可以为 LDAP 检测到的不属于任何指定组的用户配置默认访问设置。当用户登录时， FireSIGHT 系统动态检查 LDAP 服务器并根据用户的当前组成员资格分配访问权限。

当 LDAP 服务器执行身份验证的用户首次登录到本地 FireSIGHT 系统设备中时，用户会接收其所属的组的访问权限，或者，如果组未进行配置，则会接收在系统策略中选择的默认访问设置。

除非通过组成员资格授予设置，否则之后可以修改这些设置。

了解外壳访问

许可证：任何环境

可以使用 LDAP 服务器对受管设备或防御中心上的外壳访问帐户进行身份验证。指定用于为要向其授予外壳访问的用户检索条目的搜索过滤器。请注意，只能为系统策略中的第一个身份验证对象配置外壳访问。有关管理身份验证对象顺序的详细信息，请参阅第 63-11 页上的启用外部身份验证。

除管理员帐户以外，外壳访问完全通过所设置的外壳访问属性进行控制。外壳用户配置为设备上的本地用户。此处设置的过滤器确定 LDAP 服务器上可登录到外壳中的用户集。

请注意，各外壳用户的主目录是在登录时创建的，并且禁用 LDAP 外壳访问用户帐户后 （通过禁用 LDAP 连接），该目录仍然保留，但是用户外壳在 `/etc/password` 中设置为 `/bin/false` 以禁用外壳。如果之后重新启用用户，则会使用同一主目录重置外壳。

如果基础 DN 中限定的所有用户也有资格获取外壳访问权限，则可以配置外壳访问过滤器，通过选择 **Same as Base Filter** 来更高效地进行搜索。通常，用来检索用户的 LDAP 查询会将基本过滤器与外壳访问过滤器进行组合。如果键入与基本过滤器相同的外壳访问过滤器，则同一查询会运行两次，从而不必要地耗时。

外壳用户可以使用小写字母用户名登录。外壳的登录身份验证区分大小写。

注意事项　在 3 系列 防御中心上，所有外壳用户都具有 `sudoers` 权限。请确保适当地限制具有外壳访问的用户列表。在 3 系列 和虚拟设备上，授予外部身份验证用户的外壳访问默认为 **Configuration** 级别的命令行访问，它还授予 `sudoers` 权限。

了解通过 CAC 进行 LDAP 身份验证

许可证：任何环境

如果贵组织使用通用访问卡 (CAC)，则可以配置 LDAP 身份验证来对登录到 Web 界面中的用户进行身份验证，并根据组成员资格或默认访问权限来授权访问特定功能。在已配置 CAC 身份验证和授权的情况下，用户可以选择直接登录，而不用为设备提供单独的用户名和密码。

注　您**必须**在浏览器中具有有效的用户证书（在这种情况下，即通过您的 CAC 传递至您的浏览器的证书），才能在 CAC 配置流程中启用用户证书。配置 CAC 身份验证和授权之后，网络上的用户**必须**在其浏览会话的持续时间内维持 CAC 连接。如果在会话期间移除或替换 CAC，则网络浏览器会终止该会话，并且系统会注销 Web 界面。

有关配置和管理 CAC 身份验证和授权的详细信息，请参阅：

- 第 61-9 页上的配置 CAC 身份验证和授权
- 第 61-10 页上的管理 CAC 身份验证和授权

配置 CAC 身份验证和授权

许可证：任何环境

受支持的设备：任意（虚拟设备或 X -系列 除外）

受支持的防御中心：任意（虚拟设备或 X -系列 除外）

具有适当权限的用户必须完成 CAC 身份验证和授权的多步配置过程，然后网络上的用户才能使用其 CAC 凭证进行登录。

要配置和启用 CAC 身份验证和授权，请执行以下操作：

访问：管理员/网络管理员

步骤 1　按照贵组织的指导插入 CAC。

步骤 2　将浏览器定向到 `https://hostname/`，其中 *hostname* 与防御中心的主机名对应。

步骤 3　如有提示，请输入与步骤1中插入的 CAC 关联的 PIN。

系统接受您的 PIN。

步骤 4　如有提示，请从下拉列表中选择相应的证书。

浏览器接受您的选择并显示 Login 页面。

步骤 5　在 **Username** 和 **Password** 字段，以具备管理员权限的用户身份登录。用户名区分大小写。

提示　**不能**使用 CAC 凭证进行登录，直到已完全配置 CAC 身份验证和授权为止。

系统将显示默认开始页面。

步骤 6　导航到 **System > Local > User Management** 并点击 **External Authentication** 选项卡。遵循第 61-11 页上的准备创建 LDAP 身份验证对象和第 61-15 页上的创建高级 LDAP 身份验证对象中概括的过程专门为 CAC 身份验证和授权创建 LDAP 身份验证对象。必须配置以下内容：

- **LDAP-Specific Parameters** 部分的高级选项中的 **User Name Template**。有关详细信息，请参阅第 61-7 页上的了解用户名模板。

- **Attribute Mapping** 部分中的 **UI Access Attribute**。有关详细信息，请参阅第 61-7 页上的了解用于管理访问的属性。
- **Group Controlled Access Roles** 部分中现有 LDAP 组的可分辨名称 （如果要通过 LDAP 组成员资格预配置访问权限）。有关详细信息，请参阅第 61-8 页上的了解用于管理访问的组成员资格。

提示 请注意，**不能**在同一身份验证对象中配置 CAC 身份验证和外壳访问。如果还要授权用户进行外壳访问，请创建单独的身份验证对象并在系统策略中分别将其启用。

步骤 7 点击 **Save**。

系统将显示 External Authentication 页面，其中会列出新对象。

步骤 8 导航到 **System > Local > System Policy**。遵循第 63-11 页上的启用外部身份验证中所述的步骤在系统策略中启用外部身份验证，再启用 CAC 身份验证。

注意事项 更改**不**生效，直到将系统策略应用到防御中心及其受管设备为止。有关详情，请参见第 63-4 页上的应用系统策略。

步骤 9 导航到 **System > Local > Configuration** 并点击 **HTTPS Certificate**。如有必要，请遵循第 64-5 页上的上传服务器证书中概括的过程导入 HTTPS 服务器证书。

注 同一身份验证中心 (CA) **必须**在 CAC 上发行计划用于身份验证和授权的 HTTPS 服务器证书和用户证书。

Current HTTPS Certificate 页面会更新以反映新证书。

步骤 10 在 **HTTPS User Certificate Settings** 下，选择 **Enable User Certificates**。有关详细信息，请参阅第 64-5 页上的要求用户证书。

步骤 11 或者，在用户首次登录后，导航到 **System > Local > User Management** 以手动添加或移除该用户的访问权限。如果没有修改用户权限，则用户仅具有默认授予的权限。有关详细信息，请参阅第 61-3 页上的了解用户权限和第 61-50 页上的修改用户权限和选项。

有关在 CAC 用户初始登录后更改其角色的详细信息，请参阅下一节第 61-10 页上的管理 CAC 身份验证和授权。

管理 CAC 身份验证和授权

配置并启用 CAC 身份验证和授权后，网络上的用户可以使用其 CAC 凭证登录到设备的 Web 界面中。有关详细信息，请参阅第 2-1 页上的登录设备。

CAC 身份验证用户在系统中通过其电子数据交换个人标识符 (EDIPI) 号码进行识别。用户使用其 CAC 凭证首次登录后，可以在 User Management 页面上手动添加或移除这些用户的访问权限。如果未使用组控制的访问角色预配置用户的权限，则该用户仅具有系统策略中默认授予的权限。有关详细信息，请参阅第 61-3 页上的了解用户权限、第 61-8 页上的了解用于管理访问的组成员资格和第 61-50 页上的修改用户权限和选项。

请注意，系统在 CAC 身份验证用户经过 24 小时的非活动状态后将其从 User Management 页面中清除时，将会清除手动配置的访问权限。每次后续登录后会将用户恢复到该页面，但是必须重新配置对其访问权限的所有手动更改。

准备创建 LDAP 身份验证对象

许可证：任何环境

在配置与 LDAP 服务器的连接之前，应该收集创建 LDAP 身份验证对象所需的信息。有关特定方面的配置的详细信息，请参阅第 61-5 页上的了解 LDAP 身份验证。

所有身份验证对象都需要下列信息：

- 计划连接的服务器的服务器名称或 IP 地址
- 计划连接的服务器的服务器类型
- 具有浏览 LDAP 树的足够权限的用户帐户的用户名和密码
- 防火墙中用于允许传出连接的条目 （如果设备和 LDAP 服务器之间存在防火墙）
- 用户名驻留所在的服务器目录的基础可分辨名称 （如有可能）

请注意，可以使用第三方 LDAP 客户端浏览 LDAP 树和查看基础 DN 和属性描述。还可以使用该客户端确认所选用户是否可以浏览选择的基础 DN。请求 LDAP 管理员为 LDAP 服务器推荐已批准的 LDAP 客户端。

根据计划如何定制 LDAP 身份验证对象配置，还可能需要下表中的信息。

表 61-1　　其他 LDAP 配置信息

要.....	您需要.....
通过除 389 以外的端口进行连接	端口号
通过加密连接进行连接	用于连接的证书
根据属性值过滤可以访问设备的用户	进行过滤所依据的属性-值对
使用一个属性作为 UI 访问属性，而不是检查用户可分辨名称	属性的名称
使用一个属性作为外壳登录属性，而不是检查用户可分辨名称	属性的名称
根据属性值过滤可以通过外壳访问设备的用户	进行过滤所依据的属性-值对
将组与特定用户角色关联	各组的可分辨名称以及组成员属性 （如果组是静态组）或组成员 URL 属性 （如果组是动态组）
使用 CAC 进行身份验证和授权	CAC、由发行 CAC 的同一 CA 签名的服务器证书，以及两个证书的证书链

创建基本 LDAP 身份验证对象

许可证：任何环境

可以设置用于定制许多值的 LDAP 身份验证对象。但是，如果只希望对特定目录中的所有用户进行身份验证，则可以使用该目录的基础 DN 创建基本身份验证对象。如果将默认值设置为适用于服务器类型的默认值，并为用于从服务器检索用户数据的帐户提供身份验证凭证，则可以快速创建身份验证对象。请遵循以下步骤执行此操作。

注　如果在创建身份验证对象 （例如，以配置 CAC 身份验证和授权）时首选考虑并可能定制各身份验证设置，请使用第 61-15 页上的创建高级 LDAP 身份验证对象中的过程创建对象。如果计划加密与服务器的连接，设置用户超时，定制用户名模板或根据 LDAP 组成员资格分配 FireSIGHT 系统用户角色，则还应该使用高级过程。

在配置与 LDAP 服务器的连接之前，应该收集创建 LDAP 身份验证对象所需的信息。有关特定方面的配置的详细信息，请参阅第 61-5 页上的了解 LDAP 身份验证。

要创建基本身份验证对象，需要以下信息：

- 计划连接的服务器的服务器名称或 IP 地址
- 计划连接的服务器的服务器类型
- 具有浏览 LDAP 树的足够权限的用户帐户的用户名和密码；思科建议为此使用域管理员用户帐户

或者，如果要进一步限制用户搜索，可以添加基本过滤器来为特定属性设置特定值。基本过滤器通过仅检索基础 DN 中具有过滤器中设置的属性值的对象来专注搜索。请将基本过滤器用括号括起来。例如，要仅对具有以 F 开头的公共名称的用户进行过滤，请使用过滤器 `(cn=F*)`。保存身份验证对象时，本地设备使用基本过滤器测试该对象来进行查询，并且指示过滤器是否看似正确。

要创建 LDAP 身份验证对象，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击 **External Authentication** 选项卡。

系统将显示 External Authentication 页面。

步骤 3　点击 **Create External Authentication Object**。

步骤 4　从 **Authentication Method** 下拉列表中选择 **LDAP**。

系统将显示 LDAP 配置选项。

步骤 5　在 **Name** 和 **Description** 字段中键入身份验证服务器的名称和描述。

步骤 6　从 **Server Type** 下拉列表中选择服务器类型，然后点击 **Set Defaults** 按钮以配置该类型的默认设置。您有以下选项：

- 如果是连接到 Microsoft Active Directory Server，请选择 **MS Active Directory**，然后点击 **Set Defaults**。
- 如果是连接到 Sun Java Systems Directory Server 或 Oracle Directory Server，请选择 **Oracle Directory**，然后点击 **Set Defaults**。
- 如果是连接到 OpenLDAP 服务器，请选择 **OpenLDAP**，然后点击 **Set Defaults**。
- 如果是连接到除上述所列以外的服务器并要清除默认设置，请选择 **Other**，然后点击 **Set Defaults**。

步骤 7　在 **Primary Server Host Name/IP Address** 字段中键入要在其中获取身份验证数据的主服务器的 IP 地址或主机名。

注　如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

步骤 8　要获取所有基础 DN 的列表，请点击 **Fetch DNs** 并从下拉列表中选择相应的基础 DN。

例如，要对 Example 公司的 Security 部门中的名称进行身份验证，请选择 `ou=security,dc=example,dc=com`。

步骤 9　或者，要设置仅检索目录中指定为基础 DN 的特定对象的过滤器，请在 **Base Filter** 字段中键入要用作过滤器的属性类型、比较运算符和属性值 （最多 450 个字符，包括附带的括号）。

例如，如果树中的用户对象具有 physicalDeliveryOfficeName 属性，并且 New York 办公室中的用户对于该属性具有属性值 `NewYork`，要仅检索 New York 办公室中的用户，请键入 `(physicalDeliveryOfficeName=NewYork)`。

步骤 10　在 **User Name** 和 **Password** 字段中，键入具有浏览 LDAP 服务器的足够凭证的用户的可分辨名称和密码。

例如，如果是连接到 OpenLDAP 服务器，其中用户对象具有 `uid` 属性，并且 example 公司的 Security 部门中管理员的对象的 `uid` 值为 `NetworkAdmin`，则可能会键入 `uid=NetworkAdmin,ou=security,dc=example,dc=com`。

注意事项　如果是连接到 Microsoft Active Directory Server，则不能提供以 `$` 字符结尾的服务器用户名。

步骤 11　在 **Confirm Password** 字段中重新键入密码。

步骤 12　或者，要检索外壳访问用户，请在 **Shell Access Attribute** 字段中键入要按其进行过滤的属性类型。

例如，在 Microsoft Active Directory Server 上，通过在 **Shell Access Attribute** 字段中键入 `sAMAccountName` 来使用 `sAMAccountName` 外壳访问属性检索外壳访问用户。

注　外壳身份验证不支持 IPv6 地址。

步骤 13　在 **User Name** 和 **Password** 字段中，键入其凭证应该用于验证对 LDAP 服务器的访问的用户的 `uid` 值或外壳访问属性值和密码。另请注意，与 Microsoft Active Directory Server 关联的服务器用户名不能以字符 `$` 结尾。

例如，要测试以了解是否可以在 Example 公司检索 `JSmith` 用户凭证，请键入 `JSmith`。

步骤 14　点击 **Test** 以测试连接。

系统将显示一条消息，指示测试成功或者详细说明缺少或需要更正的设置。如果测试成功，则在页面底部会显示测试输出，包括连接检索到的用户的列表。如果测试中显示的用户数受 LDAP 服务器返回的用户记录数的限制，则测试输出会指示此限制。

步骤 15　此时您有两种选择：

- 如果测试成功，请点击 **Save**。

  系统将显示 External Authentication 页面，其中会列出新对象。

  要使用设备上的对象启用 LDAP 身份验证，必须将已启用该对象的系统策略应用到此设备。有关详细信息，请参阅第 63-11 页上的启用外部身份验证和第 63-4 页上的应用系统策略。

- 如果测试失败，或者如果要优化检索到的用户列表，请进入下一节第 61-14 页上的调整基本 LDAP 身份验证连接。

调整基本 LDAP 身份验证连接

许可证：任何环境

如果创建 LDAP 身份验证对象，并且其无法成功连接到选择的服务器或无法检索所需的用户列表，则可以调整该对象中的设置。

如果在测试连接时该连接失败，请尝试以下建议对配置进行故障排除。

- 使用屏幕顶部和测试输出中显示的消息确定对象的哪些方面导致问题。
- 检查用于对象的用户名和密码是否有效。
- 检查用户是否有权通过使用第三方 LDAP 浏览器连接到 LDAP 服务器来浏览至基础可分辨名称中指示的目录。
- 检查用户名对于 LDAP 服务器的目录信息树是否唯一。
- 检查用户名是否仅包含下划线、句号、连字符和字母数字字符。
- 如果在测试输出中显示 LDAP 绑定错误 49，则表明用户的用户绑定失败。请尝试通过第三方应用向服务器身份验证，以了解通过该连接进行的绑定是否也失败。
- 检查是否已正确识别服务器：
- 检查服务器 IP 地址或主机名是否正确。
- 检查是否有从本地设备到要连接的身份验证服务器的 TCP/IP 访问。
- 检查对服务器的访问是否未被防火墙阻止，以及已在对象中配置的端口是否打开。
- 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与用于服务器的主机名匹配。
- 如果是对外壳访问进行身份验证，请检查是否未对服务器连接使用 IPv6 地址。
- 如果使用了服务器类型默认值，请检查是否具有正确的服务器类型，并再次点击 **Set Defaults** 以重置默认值。

  有关详细信息，请参阅第 61-16 页上的识别 LDAP 身份验证服务器。
- 如果键入了基础可分辨名称，请点击 **Fetch DNs** 以检索服务器上的所有可用基础可分辨名称，然后从列表中选择名称。
- 如果使用的是任意过滤器、访问属性或高级设置，请检查各项是否有效且正确键入。
- 如果使用的是任意过滤器、访问属性或高级设置，请尝试移除各设置并测试没有此设置的对象。
- 如果使用的是基本过滤器或外壳访问过滤器，请确保用括号将过滤器括起来，并且使用的是有效的比较运算符。有关详细信息，请参阅第 61-6 页上的了解基本过滤器和第 61-8 页上的了解外壳访问。
- 要测试受限更多的基本过滤器，请尝试将其设置为基础可分辨名称，以使用户仅检索该用户。
- 如果使用的是加密连接：
- 检查证书中 LDAP 服务器的名称是否与用于连接的主机名匹配。
- 检查是否未对加密服务器连接使用 IPv6 地址。
- 如果使用的是测试用户，请确保正确键入用户名和密码。
- 如果使用的是测试用户，请移除用户凭证并测试对象。
- 通过要从中进行连接的设备上的命令行使用以下语法连接到 LDAP 服务器来测试所使用的查询：

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

例如，如果是尝试使用 domainadmin@myrtle.example.com 用户和基本过滤器 (cn=*) 连接到 myrtle.example.com 上的安全域，则可以使用以下语句测试连接：

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

如果可以成功测试连接，但在应用系统策略后身份验证不起作用，请检查在应用到设备的系统策略中是否已启用要使用的身份验证和对象。

如果成功连接，但要调整连接检索到的用户列表，则可以添加或更改基本过滤器或外壳访问过滤器，或者使用限制较多或较少的基础 DN。有关详细信息，请参阅：

- 第 61-6 页上的了解基础 DN
- 第 61-6 页上的了解基本过滤器
- 第 61-17 页上的配置特定于 LDAP 的参数

创建高级 LDAP 身份验证对象

许可证：任何环境

可以创建 LDAP 身份验证对象来为设备提供用户身份验证服务。

创建身份验证对象时，可定义用于连接到身份验证服务器的设置。还可以选择要用于从服务器检索用户数据的目录上下文和搜索条件。或者，可以配置外壳访问身份验证。

确保具有从本地设备到要连接的身份验证服务器的 TCP/IP 访问。

尽管可以使用服务器类型的默认设置快速设置基本 LDAP 配置，但也可以定制高级设置，以控制设备是否与 LDAP 服务器建立加密连接，连接超时，以及服务器会检查哪些属性来获取用户信息。

对于特定于 LDAP 的参数，可以使用 LDAP 命名标准和过滤器及属性语法。有关详细信息，请参阅轻量目录访问控制协议 (v3) 中列出的 RFC：“Technical Specification, RFC 3377”（技术规范， RFC 3377）。本过程各处提供了语法示例。请注意，如果将身份验证对象设置为连接到 Microsoft Active Directory Server，可以在引用包含域的用户名时使用互联网 RFC 822 （ARPA 互联网文本消息格式的标准）规范中记录的地址规范语法。例如，为引用用户对象，可能会在使用 Microsoft Active Directory Server 时键入 JoeSmith@security.example.com 而不是等效的用户基础可分辨名称 cn=JoeSmith,ou=security, dc=example,dc=com。

注　如果是配置用于 CAC 身份验证的 LDAP 身份验证对象，**请勿**移除在计算机中插入的 CAC。启用用户证书后，**必须**一直插入 CAC。有关详细信息，请参阅第 64-5 页上的要求用户证书和第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。

要创建高级身份验证对象，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击 **External Authentication** 选项卡。

系统将显示 External Authentication 页面。

步骤 3　点击 **Create External Authentication Object**。

系统将显示 Create External Authentication Object 页面。

步骤 4　识别要在其中检索用户数据以进行外部身份验证的身份验证服务器。有关详细信息，请参阅第 61-16 页上的识别 LDAP 身份验证服务器。

步骤 5　配置身份验证设置以构建用于检索要进行身份验证的用户的搜索请求。指定用户名模板以格式化用户在登录时输入的用户名。有关详细信息，请参阅第 61-17 页上的配置特定于 LDAP 的参数。

步骤 6　或者，配置 LDAP 组以用作默认访问角色分配的基础。有关详细信息，请参阅第 61-21 页上的按组配置访问权限。

提示　如果计划将此对象用于 CAC 身份验证和授权，思科建议配置 LDAP 组以管理访问角色分配。有关详细信息，请参阅第 61-10 页上的管理 CAC 身份验证和授权。

步骤 7　或者，配置外壳访问的身份验证设置。有关详细信息，请参阅第 61-22 页上的配置外壳访问。

步骤 8　通过输入可成功身份验证的用户的名称和密码来测试配置。有关详细信息，请参阅第 61-23 页上的测试用户身份验证。

已保存您的更改。请记住，必须将已启用对象的系统策略应用到设备，然后身份验证更改才会在该设备上生效。有关详细信息，请参阅第 63-11 页上的启用外部身份验证和第 63-4 页上的应用系统策略。

识别 LDAP 身份验证服务器

许可证：任何环境

创建身份验证对象时，首先指定希望受管设备或防御中心连接以进行身份验证的主服务器和备用服务器及服务器端口。

要识别 LDAP 身份验证服务器，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击 **External Authentication** 选项卡。

系统将显示 External Authentication 页面。

步骤 3　点击 **Create External Authentication Object**。

系统将显示 Create External Authentication Object 页面。

步骤 4　从 **Authentication Method** 下拉列表中选择 **LDAP**。

系统将显示 LDAP 配置选项。

步骤 5　或者，如果计划将此身份验证对象用于 CAC 身份验证和授权，请选择 **CAC** 的对应复选框。

有关配置 CAC 身份验证和授权的概述，请参阅第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。

步骤 6　在 **Name** 和 **Description** 字段中键入身份验证服务器的名称和描述。

步骤 7　或者，在 **Server Type** 字段中，选择计划连接到的 LDAP 服务器的类型，然后点击 **Set Defaults** 以使用默认值填充 **User Name Template**、**UI Access Attribute**、**Shell Access Attribute**、**Group Member Attribute** 和 **Group Member URL Attribute** 字段。您有以下选项：

- 如果是连接到 Microsoft Active Directory Server，请选择 **MS Active Directory**，然后点击 **Set Defaults**。
- 如果是连接到 Sun Java Systems Directory Server 或 Oracle Directory Server，请选择 **Oracle Directory**，然后点击 **Set Defaults**。

- 如果是连接到 OpenLDAP 服务器，请选择 **OpenLDAP**，然后点击 **Set Defaults**。
- 如果是连接到除上述所列以外的 LDAP 服务器并要清除默认设置，请选择 **Other**，然后点击 **Set Defaults**。

步骤 8　在 **Primary Server Host Name/IP Address** 字段中键入要在其中获取身份验证数据的主服务器的 IP 地址或主机名。

注　如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

步骤 9　或者，在 **Primary Server Port** 字段中修改主身份验证服务器使用的端口。

步骤 10　或者，在 **Backup Server Host Name/IP Address** 字段中键入要在其中获取身份验证数据的备份服务器的 IP 地址或主机名。

步骤 11　或者，在 **Backup Server Port** 字段中修改主身份验证服务器使用的端口。

进入下一节第 61-17 页上的配置特定于 LDAP 的参数。

配置特定于 LDAP 的参数

许可证：任何环境

特定于 LDAP 的参数部分中的设置确定设备搜索用户名所在的 LDAP 目录区域，并且控制有关设备如何连接到 LDAP 服务器的详细信息。

配置这些设置时，请注意有效用户名是唯一的，并且可以包含下划线 (_)、句号 (.) 和连字符 (-)，否则仅支持字母数字字符。

此外对于大多数特定于 LDAP 的设置而言，可以使用 LDAP 命名标准和过滤器及属性语法。有关详细信息，请参阅轻量目录访问控制协议 (v3) 中列出的 RFC：“Technical Specification, RFC 3377”（技术规范， RFC 3377）。本过程各处提供了语法示例。请注意，如果将身份验证对象设置为连接到 Microsoft Active Directory Server，可以在引用包含域的用户名时使用互联网 RFC 822（ARPA 互联网文本消息格式的标准）规范中记录的地址规范语法。例如，为引用用户对象，可能会在使用 Microsoft Active Directory Server 时键入 `JoeSmith@security.example.com` 而不是等效的用户基础可分辨名称 `cn=JoeSmith,ou=security, dc=example,dc=com`。

下表描述每个特定于 LDAP 的参数。

表 61-2　LDAP 特定参数

环境	说明	示例
基础DN	提供设备搜索有关 LDAP 服务器的用户信息所在的目录的基础可分辨名称。 通常，基础 DN 具有指示公司领域和运营单位的基础结构。 请注意，识别主服务器之后，可以从该服务器自动检索可用基础 DN 列表并选择相应的基础 DN。	例如，Example 公司的 Security 部门的基础 DN 可能为 `ou=security, dc=example,dc=com`
Base Filter	通过仅检索基础 DN 中具有过滤器中设置的属性-值对的对象来专注搜索。请注意，必须用括号将基本过滤器括起来。 要通过输入测试用户名和密码更具体地测试基本过滤器，请参阅第 61-23 页上的测试用户身份验证。	要仅对具有以 F 开头的公共名称的用户进行过滤，请使用过滤器 `(cn=F*)`。

表 61-2　　LDAP 特定参数 （续）

环境	说明	示例
User Name/ Password	允许本地设备访问用户对象。为对于要检索的身份验证对象具有适当权限的用户提供用户凭证。所指定用户的可分辨名称对于 LDAP 服务器的目录信息树必须唯一。请注意，与 Microsoft Active Directory Server 关联的服务器用户名不能以字符 $ 结尾。	Example 公司的 Security 部门中 admin 用户的用户名可能为 cn=admin, ou=security, dc=example,dc=com
加密	确定通信是否加密及如何加密。可以选择不加密、传输层安全 (TLS) 或安全套接字层 (SSL) 加密。请注意，如果在通过 TLS 或 SSL 进行连接时使用证书进行身份验证，则证书中 LDAP 服务器的名称**必须**与用于连接的名称匹配。 如果在指定端口后更改加密方法，则端口重置为所选服务器类型的默认值。	如果在外部身份验证设置中输入 10.10.10.250 并在证书中输入 computer1.example.com，则连接失败，即使 computer1.example.com 的 IP 地址为 10.10.10.250 也如此。将外部身份验证设置中的服务器名称更改为 computer1.example.com 可成功连接。
SSL Certificate Upload Path	指示本地计算机上要用于加密的证书的路径。	c:/server.crt
User Name Template	通过将字符串转换字符 (%s) 映射到用户的外壳访问属性值，指示应如何格式化在登录时输入的用户名。用户名模板是用于身份验证的可分辨名称的格式。当用户将用户名输入到登录页面中时，设备会将名称替换为字符串转换字符，并使用产生的可分辨名称搜索用户凭证。 如果要将此对象用于 CAC 身份验证和授权，**必须**输入与 **UI Access Attribute** 值对应的值。有关详细信息，请参阅第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。	%s@security.example.com、 %s@mail.com、 %s@mil、 % s@smil.mil、
超时	为对主服务器进行的连接尝试设置超时，以使连接滚动转移到备份服务器。如果在经过此字段中指示的秒数 （或 LDAP 服务器上的超时）后主身份验证服务器没有响应，则设备将查询备份服务器。 但是，如果 LDAP 是在主 LDAP 服务器的端口上运行，并且因某种原因而拒绝服务请求，则不会故障转移到备份服务器。	如果主服务器已禁用 LDAP，则设备将查询备份服务器。
UI Access Attribute	告知本地设备与特定属性的值而不是用户可分辨名称值匹配。如果属性的值是 FireSIGHT 系统 Web 界面的有效用户名，则可以使用任何属性。如果其中一个对象具有匹配的用户名和密码，表明用户登录请求已进行身份验证。 选择服务器类型并设置默认值将会使用通常适合于该类型的服务器的值预填充 **UI Access Attribute**。 如果将此字段留空，则本地设备会检查 LDAP 服务器上各用户记录的用户可分辨名称值，以查看其是否与用户名匹配。 如果要将此对象用于 CAC 身份验证和授权，**必须**输入与 **UI Name Template** 值对应的值。有关详细信息，请参阅第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。	sAMAccountName、 userPrincipalName、 mail

表 61-2　　LDAP 特定参数 （续）

环境	说明	示例
Shell Access Attribute	如果要检查外壳访问凭证的特定属性，必须将此字段显式设置为与该属性匹配。如果属性的值是外壳访问的有效用户名，则可以使用任何属性。 如果将此字段留空，则用户可分辨名称用于外壳访问身份验证。 请注意，选择服务器类型并设置默认值将会使用通常适合于该类型的服务器的属性预填充此字段。	sAMAccountName

要为服务器配置特定于 LDAP 的参数，请执行以下操作：

访问：管理

步骤 1　在 Create External Authentication Object 页面的 **LDAP-Specific Parameters** 部分中，有两个用于设置基础 DN 的选项。

- 要获取所有可用域的列表，请点击 **Fetch DNs** 并从下拉列表中选择相应的基本域名。
- 在 **Base DN** 字段中键入要访问的 LDAP 目录的基础可分辨名称。

例如，要对 Example 公司的 Security 部门中的名称进行身份验证，请选择 `ou=security,dc=example,dc=com`。

步骤 2　或者，要设置仅检索目录中指定为基础 DN 的特定对象的过滤器，请在 **Base Filter** 字段中键入要用作过滤器的属性类型、比较运算符和属性值 （用括号括起来）。

例如，如果目录树中的用户对象具有 physicalDeliveryOfficeName 属性，并且 New York 办公室中的用户对于该属性具有属性值 `NewYork`，要仅检索 New York 办公室中的用户，请键入 `(physicalDeliveryOfficeName=NewYork)`。

步骤 3　在 **User Name** 和 **Password** 字段中键入其凭证应该用于验证对 LDAP 目录的访问的用户的可分辨名称和密码。

例如，如果是连接到 OpenLDAP 服务器，其中用户对象具有 `uid` 属性，并且 example 公司的 Security 部门中管理员的对象的 `uid` 值为 `NetworkAdmin`，则可能会键入 `uid=NetworkAdmin,ou=security,dc=example,dc=com`。

注意事项　如果是连接到 Microsoft Active Directory Server，则不能提供以 `$` 字符结尾的服务器用户名。

步骤 4　在 **Confirm Password** 字段中重新键入密码。

步骤 5　配置特定于 LDAP 的基本参数后，有若干选项：

- 要访问高级选项，请点击 **Show Advanced Options** 旁边的箭头并继续执行下一步。
- 如果要根据 LDAP 组成员资格配置用户默认角色，请进入下一节第 61-21 页上的按组配置访问权限。
- 如果不是使用 LDAP 组进行身份验证，请进入下一节第 61-22 页上的配置外壳访问。

步骤 6　或者，选择以下加密模式之一：

- 要使用安全套接字层 (SSL) 进行连接，请选择 **SSL**。
- 要使用传输层安全 (TLS) 进行连接，请选择 **TLS**。
- 要在不加密的情况下进行连接，请选择 **None**。

注　请注意，如果在指定端口后更改加密方法，则会将端口重置为该方法的默认值。对于 None 或 TLS，端口使用默认值 389。如果选择 SSL 加密，则端口使用默认值 636。

步骤 7　如果选择 TLS 或 SSL 加密并要使用证书进行身份验证，请点击 **Browse** 以浏览至有效 TLS 或 SSL 证书的位置，或者在 **SSL Certificate Upload Path** 字段中键入证书的路径。

系统将显示一条消息，指示证书上传成功。

注　如果之前已上传证书并要将其替换，请上传新证书并将系统策略重新应用到设备来复制转移新证书。

步骤 8　或者，在 **User Name Template** 字段中，键入用于从 **UI Access Attribute** 中找到的值确定用户名的字符串转换字符 (`%s`)。

例如，要通过连接到外壳访问属性为 `uid` 的 OpenLDAP 服务器来对 example 公司的 Security 部门中工作的所有用户进行身份验证，可能会在 **User Name Template** 字段中键入 `uid=%s,ou=security,dc=example,dc=com`。对于 Microsoft Active Directory Server，可以键入 `%s@security.example.com`。

如果要使用 CAC 凭证进行身份验证和授权，**必须**在 **User Name Template** 字段中输入值。有关详细信息，请参阅第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。

步骤 9　或者，在 **Timeout** 字段中，键入在滚动转移到备份连接之前应经过的秒数。

步骤 10　或者，要根据属性而不是 Base DN 和 Base Filter 检索用户，有两个选项：

- 点击 **Fetch Attrs** 以检索可用属性的列表并选择相应的属性。
- 在 **UI Access Attribute** 字段中键入属性。

例如，在 Microsoft Active Directory Server 上，可能要使用 UI Access Attribute 检索用户，因为在 Active Directory Server 用户对象上可能没有 `uid` 属性。相反，可以通过在 **UI Access Attribute** 字段中键入 `userPrincipalName` 来搜索 `userPrincipalName` 属性。

如果要使用 CAC 凭证进行身份验证和授权，**必须**在 **User Access Attribute** 字段中输入值。有关详细信息，请参阅第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。

步骤 11　或者，要检索外壳访问用户，请在 **Shell Access Attribute** 字段中键入要按其进行过滤的属性。

例如，在 Microsoft Active Directory Server 上，通过在 **Shell Access Attribute** 字段中键入 `sAMAccountName` 来使用 `sAMAccountName` 外壳访问属性检索外壳访问用户。

注　请注意，**不能**在同一身份验证对象中配置 CAC 身份验证和授权及外壳访问。选择 **CAC** 复选框会禁用页面上的外壳访问配置选项。相反，创建单独的身份验证对象并在系统策略中分别将其启用。有关详细信息，请参阅第 63-11 页上的启用外部身份验证。

步骤 12　对于下一步，您有三种选择：

- 如果要根据 LDAP 组成员资格配置用户默认角色，请进入下一节第 61-21 页上的按组配置访问权限。
- 如果**不是**使用 LDAP 组进行身份验证但要配置外壳访问，请进入下一节第 61-22 页上的配置外壳访问。
- 如果**不是**使用 LDAP 组进行身份验证且**不**希望配置外壳访问，请进入下一节第 61-23 页上的测试用户身份验证。

按组配置访问权限

许可证：任何环境

如果首选将默认访问权限基于 LDAP 组中的用户成员资格，则可以为 FireSIGHT 系统使用的各访问角色指定 LDAP 服务器上现有组的可分辨名称。执行此操作时，可以为 LDAP 检测到的不属于任何指定组的用户配置默认访问设置。当用户登录时， FireSIGHT 系统动态检查 LDAP 服务器并根据用户的当前组成员资格分配默认访问权限。

如果计划将对象用于 CAC 身份验证和授权，思科建议配置 LDAP 组以管理 CAC 身份验证用户的访问角色分配。有关详细信息，请参阅第 61-10 页上的管理 CAC 身份验证和授权。

引用的任何组都必须存在于 LDAP 服务器上。可以引用静态 LDAP 组或动态 LDAP 组。静态 LDAP 组是成员资格由指向特定用户的组对象属性确定的组，动态 LDAP 组是通过创建根据用户对象属性检索组用户的 LDAP 搜索来确定成员资格的组。角色的组访问权限仅影响身为组成员的用户。

用户登录到 FireSIGHT 系统中时授予的访问权限取决于 LDAP 配置：

- 如果没有为 LDAP 服务器配置组访问权限，则在新用户登录时， FireSIGHT 系统利用 LDAP 服务器对用户进行身份验证，然后根据系统策略中设置的默认最低访问角色授予用户权限。
- 如果配置任何组设置，则属于指定组的新用户将继承其所属的组的最低访问设置。
- 如果新用户不属于任何指定组，则会为用户分配在身份验证对象的 Group Controlled Access Roles 部分中指定的默认最低访问角色。
- 如果用户属于多个已配置组，则用户会接收具有最高访问的组的访问角色作为最低访问角色。

由于 LDAP 组成员资格，不能使用 FireSIGHT 系统用户管理页面移除已分配到访问角色的用户的最低访问权限。但是，可以分配其他权限。修改外部身份验证用户的访问权限时， User Management 页面上的 Authentication Method 列提供状态 **External - Locally Modified**。

注　如果使用动态组，则完全按照 LDAP 查询在 LDAP 服务器上的配置来使用 LDAP 查询。因此，FireSIGHT 系统将搜索的递归数限制为 4，以防止搜索语法错误导致无限循环。如果在这些递归中未建立用户的组成员资格，则会向用户授予 Group Controlled Access Roles 部分中定义的默认访问角色。

要根据组成员资格配置默认角色，请执行以下操作：

访问：管理

步骤 1　在 Create External Authentication Object 页面上，点击 **Group Controlled Access Roles** 旁边的向下箭头。

此部分随即展开。

步骤 2　或者，按组成员资格配置访问默认值。

在与 FireSIGHT 系统用户角色对应的 **DN** 字段中，键入包含应向其分配这些角色的用户的 LDAP 组的可分辨名称。

例如，可能会在 **Administrator** 字段中键入以下内容来对 `Example` 公司的信息技术部门中的名称进行身份验证：

```
cn=itgroup,ou=groups, dc=example,dc=com
```

有关用户访问角色的详细信息，请参阅第 61-41 页上的添加新用户帐户。

步骤 3　从 **Default User Role** 列表中，选择不属于任何指定组的用户的默认最低访问角色。

提示　点击角色名称的同时按 Ctrl 键以选择多个角色。

步骤 4　如果使用静态组，请在 **Group Member Attribute** 字段中键入用于指定静态组中的成员资格的 LDAP 属性。

例如，如果 `member` 属性用于指示为默认 Security Analyst 访问引用的静态组中的成员资格，请键入 `member`。

步骤 5　如果使用动态组，请在 **Group Member URL Attribute** 字段中键入包含用于确定动态组中的成员资格的 LDAP 搜索字符串的 LDAP 属性。

例如，如果 `memberURL` 属性包含用于检索为默认管理员访问指定的动态组的成员的 LDAP 搜索，请键入 `memberURL`。

步骤 6　进入下一节第 61-22 页上的配置外壳访问。

配置外壳访问

许可证：任何环境

还可以使用 LDAP 服务器对受管设备或防御中心上的外壳访问帐户进行身份验证。指定用于为要向其授予外壳访问的用户检索条目的搜索过滤器。

请注意，**不能**在同一身份验证对象中配置 CAC 身份验证和授权及外壳访问。相反，创建单独的身份验证对象并在系统策略中分别将其启用。外壳访问的身份验证对象必须是系统策略中的第一个身份验证对象。有关管理身份验证对象顺序的详细信息，请参阅第 63-11 页上的启用外部身份验证。

注　思科不支持虚拟设备或 用于 Blue Coat X-系列的思科 NGIPS的外部身份验证。此外，外壳访问身份验证不支持 IPv6。

除管理员帐户以外，外壳访问完全通过所设置的外壳访问属性进行控制。所设置的外壳访问过滤器确定 LDAP 服务器上可登录到外壳中的用户集。

请注意，各外壳用户的主目录是在登录时创建的，并且禁用 LDAP 外壳访问用户帐户后 （通过禁用 LDAP 连接），该目录仍然保留，但是用户外壳在 `/etc/password` 中设置为 `/bin/false` 以禁用外壳。如果之后重新启用用户，则会使用同一主目录重置外壳。

如果基础 DN 中限定的所有用户也有资格获取外壳访问权限，则通过 **Same as Base Filter** 复选框可更高效地进行搜索。通常，用来检索用户的 LDAP 查询会将基本过滤器与外壳访问过滤器进行组合。如果外壳访问过滤器与基本过滤器相同，则同一查询会运行两次，从而不必要地耗时。可以使用 **Same as Base Filter** 选项仅运行一次查询来实现两个目的。

外壳用户可以使用小写字母用户名登录。外壳的登录身份验证区分大小写。

注意事项　在 3 系列 防御中心上，所有外壳用户都具有 `sudoers` 权限。请确保适当地限制具有外壳访问的用户列表。在 3 系列 和虚拟设备上，授予外部身份验证用户的外壳访问默认为 **Configuration** 级别的命令行访问，它还授予 `sudoers` 权限。

要配置外壳帐户身份验证，请执行以下操作：

访问：管理

步骤 1　或者，在 Create External Authentication Object 页面上，设置外壳访问帐户过滤器。您有多个选择：

- 要根据属性值检索管理用户条目，请在 **Shell Access Filter** 字段中键入要用作过滤器的属性名、比较运算符和属性值 （用括号括起来）。

- 要使用配置身份验证设置时指定的同一过滤器，请选择 **Same as Base Filter**。
- 要防止对外壳访问进行 LDAP 身份验证，请将此字段留空。如果选择不指定外壳访问过滤器，则在保存身份验证对象时会显示警告，要求确认是否意图将过滤器留空。

例如，如果所有网络管理员都具有属性值为 `shell` 的 `manager` 属性，则可以设置基本过滤器 `(manager=shell)`。

步骤 2　进入下一节第 61-23 页上的测试用户身份验证。

测试用户身份验证

许可证：任何环境

在配置 LDAP 服务器和身份验证设置后，可以为应该能够进行身份验证以测试这些设置的用户指定用户凭证。

对于用户名，可以为要用于测试的用户输入 `uid` 属性的值。如果是连接到 Microsoft Active Directory Server 并提供外壳访问属性来代替 `uid`，请使用该属性的值作为用户名。还可以为用户指定完全限定的可分辨名称。

测试输出列出有效和无效的用户名。有效用户名是唯一的，并且可以包含下划线 (_)、句号 (.) 和连字符 (-)，否则仅支持字母数字字符。无效用户名是包含其他非字母数字字符 （例如空格）的用户名。

请注意，由于Web 界面页面大小限制，测试与具有 1000 个以上用户的服务器的连接仅返回 1000 个用户。

提示　如果测试用户的名称或密码键入不正确，即使服务器配置正确，测试也会失败。请首先测试没有其他测试参数的服务器配置。如果成功，请提供要通过特定用户进行测试的用户名和密码。

要测试用户身份验证，请执行以下操作：

访问：管理

步骤 1　在 **User Name** 和 **Password** 字段中，键入其凭证应该用于验证对 LDAP 服务器的访问的用户的 `uid` 值或外壳访问属性值和密码。

例如，要测试以了解是否可以在 Example 公司检索 `JSmith` 用户凭证，请键入 `JSmith`。

步骤 2　点击 **Test**。

系统将显示一条消息，指示测试成功或者详细说明缺少或需要更正的设置。此时您有两种选择：

- 如果测试成功，则页面底部会显示测试输出。点击 **Save**。系统将显示 External Authentication 页面，其中会列出新对象。

  要使用设备上的对象启用 LDAP 身份验证，必须将已启用该对象的系统策略应用到此设备。有关详细信息，请参阅第 63-11 页上的启用外部身份验证和第 63-4 页上的应用系统策略。
- 如果测试失败，请参阅第 61-14 页上的调整基本 LDAP 身份验证连接，以获取有关对连接进行故障排除的建议。请注意，显示的错误消息指示导致连接失败的原因。

LDAP 身份验证对象示例

许可证：任何环境

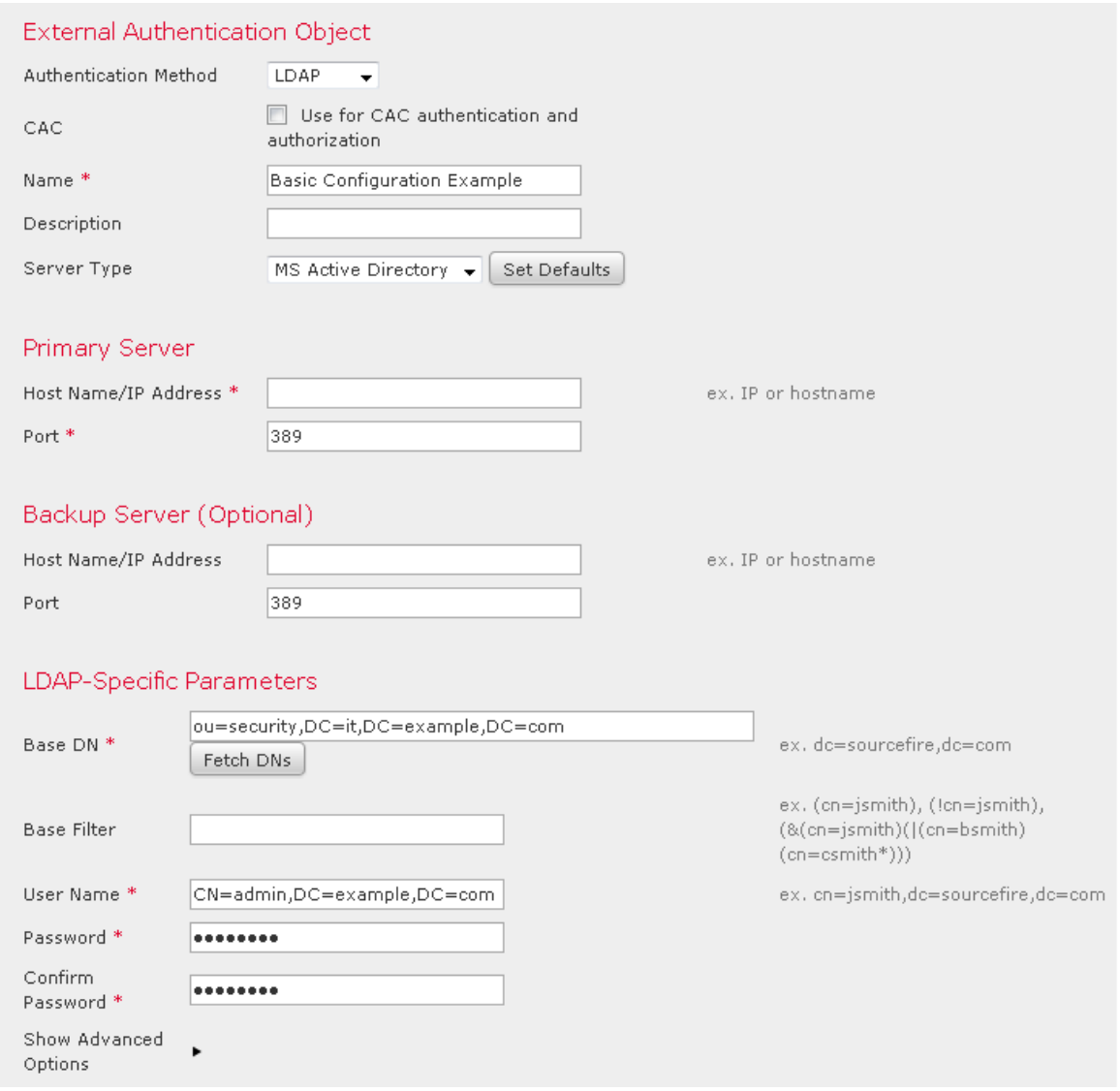
以下各节提供使用基本设置的 LDAP 配置示例和使用更高级配置选项的示例：

- 第 61-24 页上的示例：基本 LDAP 配置
- 第 61-25 页上的示例：高级 LDAP 配置

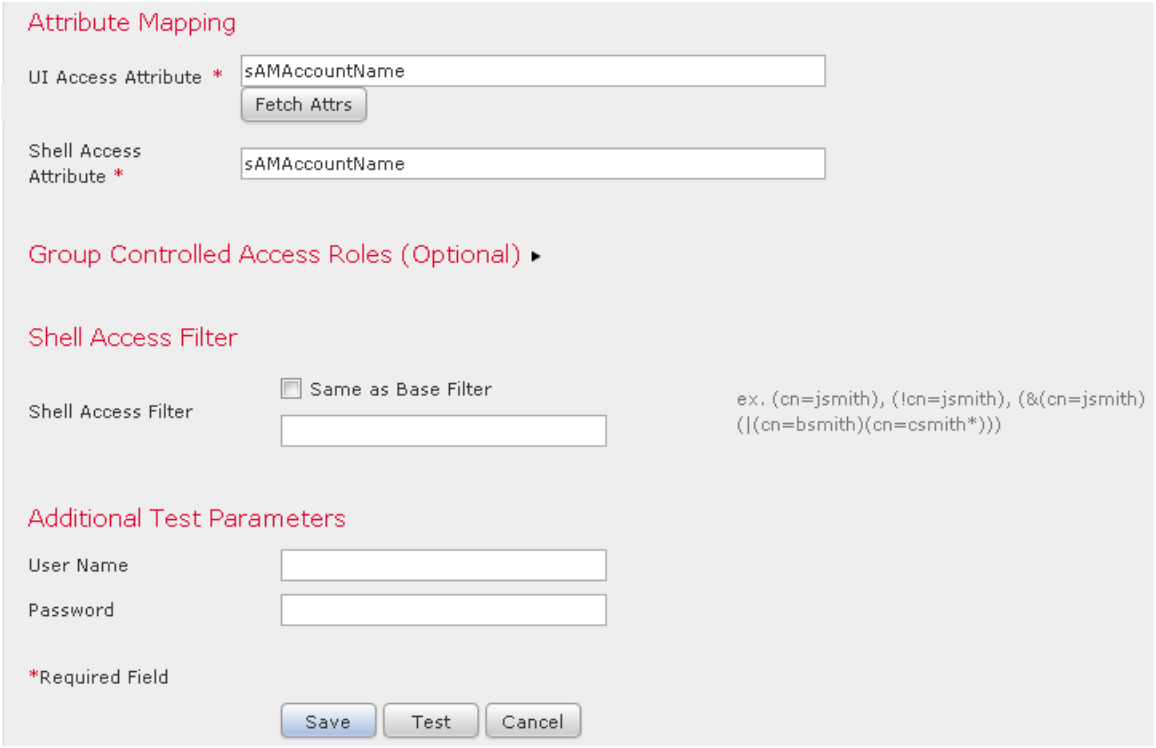
示例：基本 LDAP 配置

许可证：任何环境

下图说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的基本配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 389 进行访问。



此示例显示对于 Example 公司的信息技术领域中的 security 部门使用基础可分辨名称 `OU=security,DC=it,DC=example,DC=com` 的连接。



但是，由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。选择 MS Active Directory 服务器类型并点击 **Set Defaults** 会将 UI Access Attribute 设置为 `sAMAccountName`。因此，当用户尝试登录 FireSIGHT 系统时， FireSIGHT 系统会检查各对象的 `sAMAccountName` 属性以查找匹配的用户名。

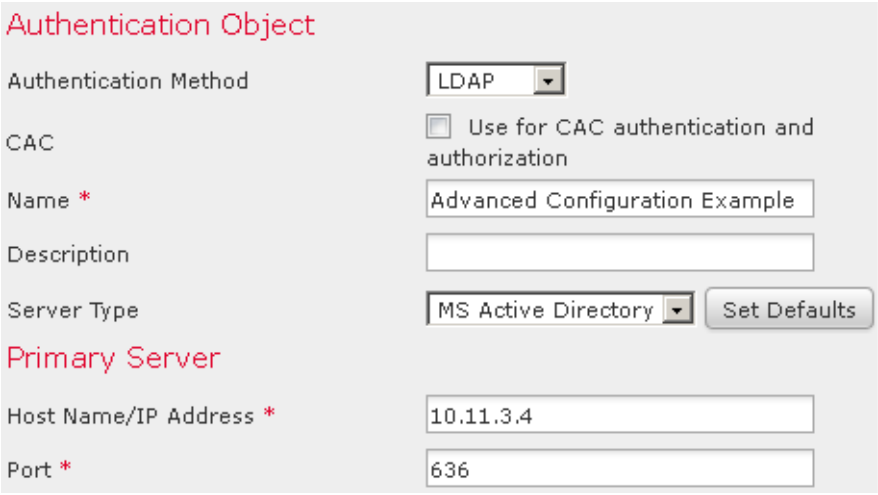
此外，当用户登录到设备上的外壳帐户中时， Shell Access Attribute 为 `sAMAccountName` 会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

请注意，由于未对此服务器应用基本过滤器，因此 FireSIGHT 系统会检查目录中基础可分辨名称所指示的所有对象的属性。经过默认时间段 （或 LDAP 服务器上设置的超时期）后，与服务器的连接将超时。

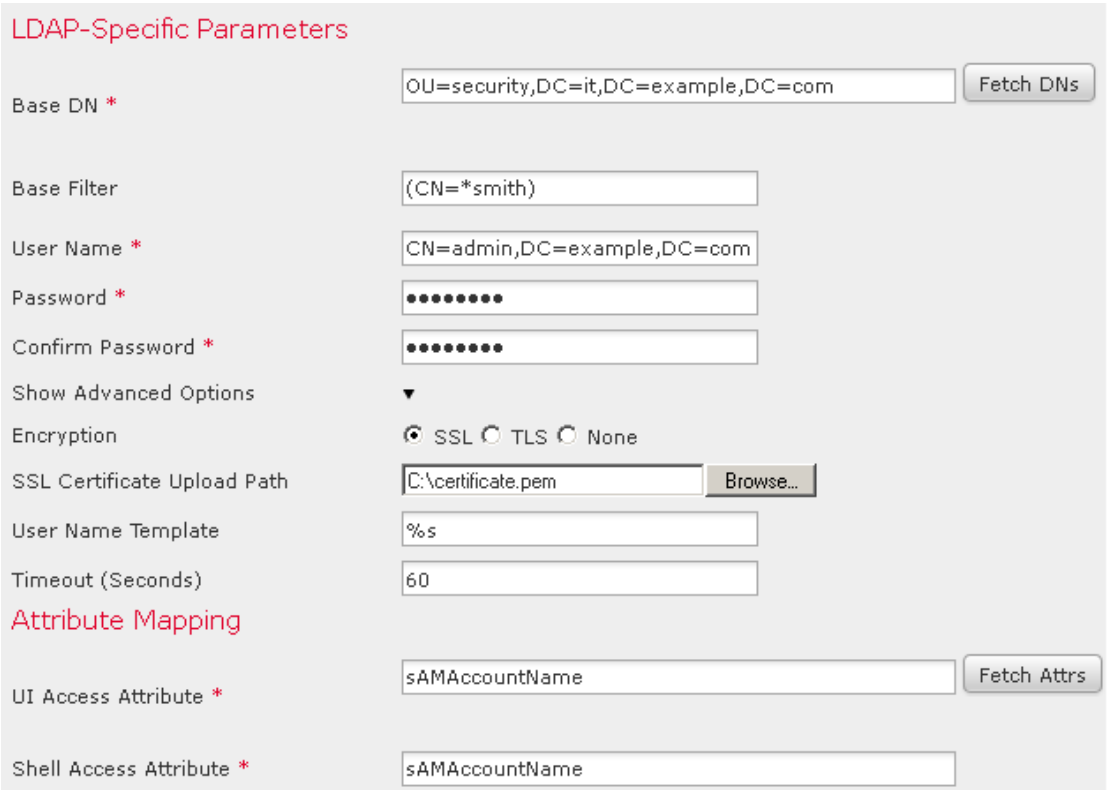
示例：高级 LDAP 配置

许可证：任何环境

此示例说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的高级配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 636 进行访问。



此示例显示对于 Example 公司的信息技术领域中的 security 部门使用基础可分辨名称 `OU=security,DC=it,DC=example,DC=com` 的连接。但请注意，此服务器具有基本过滤器 `(cn=*smith)`。过滤器将从服务器检索的用户限制为具有以 `smith` 结尾的常见名称的用户。

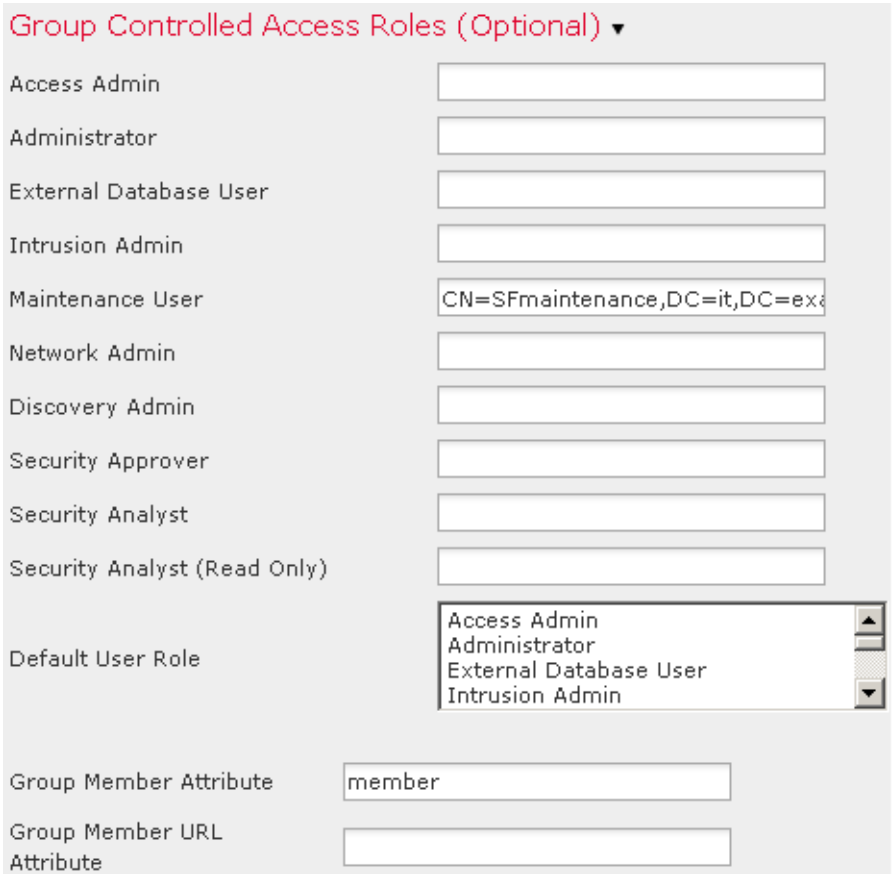


与服务器的连接使用 SSL 进行加密，并且会为该连接使用一个名为 `certificate.pem` 的证书。此外，由于 **Timeout** 设置，与服务器的连接在 60 秒后将超时。

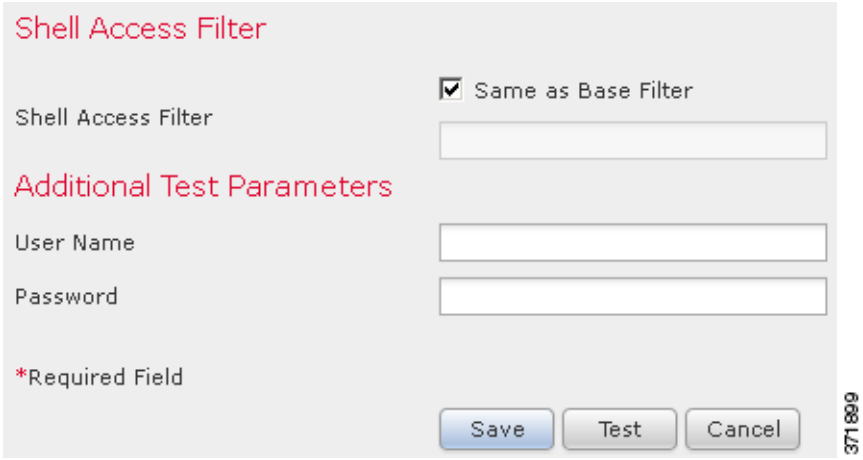
由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。请注意，配置包括 UI Access Attribute `sAMAccountName`。因此，当用户尝试登录 FireSIGHT 系统时， FireSIGHT 系统会检查各对象的 `sAMAccountName` 属性以查找匹配的用户名。

此外，当用户登录到设备上的外壳帐户中时， Shell Access Attribute 为 `sAMAccountName` 会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

此示例还具有相应的组设置。维护人员角色会自动分配给具有 `member` 组属性且基本域名为 `CN=SFmaintenance,DC=it,DC=example,DC=com`. 的组的所有成员。



外壳访问过滤器设置为基本过滤器相同，因此相同用户可以通过外壳访问设备，如同通过Web 界面进行访问一样。



编辑 LDAP 身份验证对象

许可证：任何环境

可以编辑现有身份验证对象。直到重新应用策略后，更改才会生效。

要编辑身份验证对象，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击 **External Authentication** 选项卡。

系统将显示 External Authentication 页面。

步骤 3　点击要编辑的对象旁边的编辑图标 ( )。

系统将显示 Create External Authentication Object 页面。

步骤 4　根据需要修改对象设置。

步骤 5　点击 **Test**。

系统将显示一条消息，指示测试成功或者详细说明缺少或需要更正的设置。如果测试成功，则页面底部会显示测试输出。

如果测试失败，请参阅第 61-14 页上的调整基本 LDAP 身份验证连接，以获取有关对连接进行故障排除的建议。请注意，显示的错误消息指示导致连接失败的原因。

步骤 6　点击 **Save**。

系统保存更改并显示 External Authentication 页面。请记住，必须将已启用对象的系统策略应用到设备，然后身份验证更改才会在该设备上生效。有关详细信息，请参阅第 63-11 页上的启用外部身份验证和第 63-4 页上的应用系统策略。

RADIUS 身份验证

远程身份验证拨入用户服务 (RADIUS) 是用于身份验证、授权和阐释对网络资源的用户访问的一种身份验证协议。可以为符合 RFC 2865 的任何 RADIUS 服务器创建身份验证对象。

有关详细信息，请参阅：

- 第 61-29 页上的了解 RADIUS 身份验证
- 第 61-29 页上的创建 RADIUS 身份验证对象
- 第 61-30 页上的配置 RADIUS 连接设置
- 第 61-31 页上的配置 RADIUS 用户角色
- 第 61-32 页上的配置管理外壳访问
- 第 61-33 页上的定义自定义 RADIUS 属性

了解 RADIUS 身份验证

许可证：任何环境

在 RADIUS 服务器上进行身份验证的用户首次登录时，该用户会接收在身份验证对象中为其指定的角色。如果没有为任何用户角色列出该用户，则会接收在身份验证对象中选择的默认访问角色。如果在身份验证对象中未选择默认访问角色，则会接收系统策略中的默认访问角色。除非通过身份验证对象中的用户列表对设置进行授权，否则在需要时可以修改用户的角色。请注意，在 RADIUS 服务器上使用属性匹配进行身份验证的用户首次尝试登录时，会因已创建该用户帐户而被拒绝登录。用户必须再次登录。

注　在3 系列 受管设备上启用外部身份验证之前，请移除与外壳访问过滤器中包含的外部身份验证用户具有相同用户名的所有内部身份验证外壳用户。

RADIUS 的 FireSIGHT 系统实施支持使用 SecurID® 令牌。使用 SecurID 通过服务器来配置身份验证时，利用该服务器进行身份验证的用户会将 SecurID 令牌追加到其 SecurID PIN 的末尾，并在其登录到思科设备中时将此用作其密码。只要 SecurID 正确配置为在 FireSIGHT 系统外部对用户进行身份验证，这些用户即可使用其 PIN 以及 SecurID 令牌登录到 FireSIGHT 系统设备中，而无需在设备上进行任何其他配置。

创建 RADIUS 身份验证对象

许可证：任何环境

创建 RADIUS 身份验证对象时，可定义用于连接到身份验证服务器的设置。另外将用户角色授予特定用户和默认用户。如果 RADIUS 服务器为计划进行身份验证的任何用户返回自定义属性，必须定义这些自定义属性。或者，也可以配置外壳访问身份验证。

请注意，要创建身份验证对象，需要从本地设备到要连接的身份验证服务器的 TCP/IP 访问。

要创建身份验证对象，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击 **External Authentication** 选项卡。

系统将显示 External Authentication 页面。

步骤 3　点击 **Create External Authentication Object**。

系统将显示 Create External Authentication Object 页面。

步骤 4　识别要在其中检索用于外部身份验证的用户数据并设置超时值和重试值的主身份验证服务器及备份身份验证服务器。有关详细信息，请参阅第 61-30 页上的配置 RADIUS 连接设置。

步骤 5　设置默认用户角色。或者，指定要接收特定 FireSIGHT 系统访问角色的用户的用户或用户属性值。有关详细信息，请参阅第 61-31 页上的配置 RADIUS 用户角色。

步骤 6　或者，配置管理外壳访问。有关详细信息，请参阅第 61-32 页上的配置管理外壳访问。

步骤 7　如果要进行身份验证的任何用户的配置文件返回自定义 RADIUS 属性，请定义这些属性。有关详细信息，请参阅第 61-33 页上的定义自定义 RADIUS 属性。

步骤 8　通过输入可成功进行身份验证的用户的名称和密码来测试配置。有关详细信息，请参阅第 61-34 页上的测试用户身份验证。

已保存您的更改。请记住，必须将已启用对象的系统策略应用到设备，然后身份验证更改才会在该设备上生效。有关详细信息，请参阅第 63-11 页上的启用外部身份验证和第 63-4 页上的应用系统策略。

配置 RADIUS 连接设置

许可证：任何环境

创建 RADIUS 身份验证对象时，首先指定希望受管设备或防御中心连接以进行身份验证的主服务器和备用服务器及服务器端口。

注　为使 RADIUS 正常工作，必须在防火墙上打开其身份验证和记帐端口 （默认情况下为1812 和 1813）。

如果指定备份身份验证服务器，则可以为对主服务器进行的连接尝试设置超时。如果在经过 **Timeout** 字段中指示的秒数 （或 LDAP 服务器上的超时）后主身份验证服务器没有响应，则设备将重新查询主服务器。

在设备按照 **Retries** 字段中指示的次数重新查询身份验证服务器，并且再次经过 **Timeout** 字段中指示的秒数而主身份验证服务器没有响应后，设备将滚动转移到备份服务器。

例如，如果主服务器已禁用 RADIUS，则设备将查询备份服务器。但是，如果 RADIUS 是在主 RADIUS 服务器的端口上运行，并且因某种原因而拒绝服务请求 （由于配置错误或其他问题），则不会故障转移到备份服务器。

要识别 RADIUS 身份验证服务器，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击 **External Authentication** 选项卡。

系统将显示 External Authentication 页面。

步骤 3　点击 **Create External Authentication Object**。

系统将显示 Create External Authentication Object 页面。

步骤 4　从 **Authentication Method** 下拉列表中选择 **RADIUS**。

系统将显示 RADIUS 配置选项。

步骤 5　在 **Name** 和 **Description** 字段中键入身份验证服务器的名称和描述。

步骤 6　在 **Primary Server Host Name/IP Address** 字段中键入要在其中获取身份验证数据的主 RADIUS 服务器的 IP 地址或主机名。

注　外壳身份验证不支持 IPv6 地址。要在对主 RADIUS 服务器使用 IPv6 地址时允许外壳身份验证，请使用服务器的 IPv4 地址设置身份验证对象，并使用该 IPv4 对象作为系统策略中的第一个身份验证对象。

步骤 7　或者，在 **Primary Server Port** 字段中修改主 RADIUS 身份验证服务器使用的端口。

注　如果身份验证端口号和记帐端口号不连续，请将此字段留空。然后，系统根据设备的 `/etc/services` 文件中的 `radius` 和 `radacct` 数据确定 RADIUS 端口号。

步骤 8　在 **RADIUS Secret Key** 字段中键入主 RADIUS 身份验证服务器的密钥。

步骤 9　在 **Backup Server Host Name/IP Address** 字段中键入要在其中获取身份验证数据的备份 RADIUS 身份验证服务器的 IP 地址或主机名。

步骤 10　或者，在 **Backup Server Port** 字段中修改备份 RADIUS 身份验证服务器使用的端口。

注　如果身份验证端口号和记帐端口号不连续，请将此字段留空。然后，系统根据设备的 `/etc/services` 文件中的 `radius` 和 `radacct` 数据确定 RADIUS 端口号。

步骤 11　在 **RADIUS Secret Key** 字段中键入备份 RADIUS 身份验证服务器的密钥。

步骤 12　在 **Timeout** 字段中键入重试连接之前应经过的秒数。

步骤 13　在 **Retries** 字段中键入主服务器连接在滚动转移到备份服务器之前应尝试的次数。

步骤 14　进入下一节第 61-31 页上的配置 RADIUS 用户角色。

配置 RADIUS 用户角色

许可证：任何环境

可以通过列出 FireSIGHT 系统使用的各访问角色的用户名来指定 RADIUS 服务器上现有用户的访问角色。执行此操作时，还可以为 RADIUS 检测到的没有为特定角色指定的用户配置默认访问设置。

当用户登录时， FireSIGHT 系统会根据 RADIUS 配置检查 RADIUS 服务器并授予访问权限：

- 如果没有为用户配置特定访问权限且未选择默认访问角色，则新用户登录时， FireSIGHT 系统会按照 RADIUS 服务器对用户进行身份验证，然后根据系统策略中设置的一个或多个默认访问角色授予用户权限。
- 如果未在任何列表上指定新用户，并在身份验证对象的 **Default User Role** 列表中选择了默认访问角色，则会为该用户分配这些访问角色。
- 如果为一个或多个特定角色向列表中添加用户，则该用户会接收所有已分配的访问角色。

也可以使用属性-值对而不是用户名来识别应接收特定用户角色的用户。例如，如果您知道所有应为 Security Analyst 的用户对于其 `User-Category` 属性具有值 `Analyst`，则可以在 Security Analyst List 字段中键入 `User-Category=Analyst`，以将该角色授予这些用户。请注意，需要定义所有自定义属性，然后再使用其设置用户角色成员资格。有关详细信息，请参阅第 61-33 页上的定义自定义 RADIUS 属性。

可以分配一个或多个要分配给已进行外部身份验证但没有为特定角色列出的任何用户的默认用户角色。可以选择 **Default User Role** 列表上的多个角色。

有关 FireSIGHT 系统支持的用户角色的详细信息，请参阅第 61-31 页上的配置 RADIUS 用户角色。

由于 RADIUS 用户列表成员资格，无法通过 FireSIGHT 系统用户管理页面移除已为其分配访问角色的用户的最低访问权限。但是，可以分配其他权限。

注意事项 如果要更改用户的最低访问设置，则不仅必须在 RADIUS Specific Parameters 部分中将用户从一个列表移至另一个列表或在 RADIUS 服务器上更改用户属性，还必须重新应用系统策略，并且必须在用户管理页面上移除已分配的用户权限。

要根据用户列表进行访问，请执行以下操作：

访问：管理

步骤 1 在与 FireSIGHT 系统用户角色对应的字段中，键入各用户的名称或应分配给这些角色的标识属性-值对。将用户名和属性-值对以逗号分隔。

例如，要将 Administrator 角色授予用户 `jsmith` 和 `jdoe`，请在 **Administrator** 字段中键入 `jsmith, jdoe`。

又例如，要将 Maintenance User 角色授予 `User-Category` 值为 `Maintenance` 的所有用户，请在 **Maintenance User** 字段中键入 `User-Category=Maintenance`。

有关用户访问角色的详细信息，请参阅第 61-45 页上的配置用户角色。

步骤 2 从 **Default User Role** 列表中为不属于任何指定组的用户选择默认最低访问角色。

提示 点击角色名称的同时按 Ctrl 键以选择多个角色。

步骤 3 进入下一节第 61-32 页上的配置管理外壳访问。

配置管理外壳访问

许可证：任何环境

也可以使用 RADIUS 服务器对本地设备 （受管设备或防御中心）上的外壳访问帐户进行身份验证。指定要向其授予外壳访问的用户的用户名。请注意，只能为系统策略中的第一个身份验证对象配置外壳访问。有关管理身份验证对象顺序的详细信息，请参阅第 63-11 页上的启用外部身份验证。

注 外壳身份验证不支持 IPv6 地址。如果使用 IPv6 地址配置主 RADIUS 服务器，并且还配置管理外壳访问，则会忽略外壳访问设置。要在对主 RADIUS 服务器使用 IPv6 地址时允许外壳身份验证，请使用服务器的 IPv4 地址设置其他身份验证对象，并使用该 IPv4 对象作为系统策略中的第一个身份验证对象。

除管理帐户以外，在 RADIUS 身份验证对象上设置的外壳访问列表完全控制设备上的外壳访问。应用系统策略后，外壳用户配置为设备上的本地用户。请注意，在 RADIUS 服务器上使用属性匹配进行身份验证的用户首次尝试登录时，会因已创建该用户帐户而被拒绝登录。用户必须再次登录。

请注意，各外壳用户的主目录是在登录时创建的，并且禁用 RADIUS 外壳访问用户帐户后 （通过禁用 RADIUS 连接），该目录仍然保留，但是用户外壳在 `/etc/password` 中设置为 `/bin/false` 以禁用外壳。如果之后重新启用用户，则会使用同一主目录重置外壳。

外壳用户可以使用小写字母用户名登录。外壳的登录身份验证区分大小写。

注意事项 在3 系列 防御中心上，所有外壳用户都具有 sudoers 权限。请确保适当地限制具有外壳访问的用户列表。在3 系列 和虚拟设备上，授予外部身份验证用户的外壳访问默认为 **Configuration** 级别的命令行访问，它还授予 sudoers 权限。

要配置外壳帐户身份验证，请执行以下操作：

访问：管理

步骤 1 在 **Administrator Shell Access User List** 字段中键入以逗号分隔的用户名。

注 如果选择不指定外壳访问过滤器，则在保存身份验证对象时会显示警告，要求确认是否意图将过滤器留空。

步骤 2 进入下一节第 61-33 页上的定义自定义 RADIUS 属性。

定义自定义 RADIUS 属性

许可证：任何环境

如果 RADIUS 服务器返回 /etc/radiusclient/ 中 dictionary 文件内不包含的属性值，并且计划使用这些属性来设置具有这些属性的用户的用户角色，则需要在登录身份验证对象中定义这些属性。

可以通过查看 RADIUS 服务器上的用户配置文件来查找为用户返回的属性。

定义属性时，请提供属性的名称，其中包含字母数字字符。请注意，属性名称中的单词应以破折号而不是空格进行分隔。另请提供属性 ID，它应为整数且不应与 etc/radiusclient/dictionary 文件中的任何现有属性 ID 冲突。还请指定属性的类型：字符串、 IP 地址、整数或日期。

例如，如果在含有思科路由器的网络上使用了 RADIUS 服务器，则可能要使用 Ascend-Assign-IP-Pool 属性向从特定 IP 地址池登录的所有用户授予特定角色。Ascend-Assign-IP-Pool 是一个整数属性，用于定义允许用户登录的地址池，其中整数指示已分配的 IP 地址池的编号。要声明自定义属性，请创建属性名称为 Ascend-IP-Pool-Definition、属性 ID 为 218 且属性类型为 integer 的自定义属性。然后，可以在 **Security Analyst (Read Only)** 字段中键入 Ascend-Assign-IP-Pool=2，以将只读安全分析师权限授予 Ascend-IP-Pool-Definition 属性值为 2 的所有用户。

创建 RADIUS 身份验证对象时，会在 FireSIGHT 系统设备上的 /var/sf/userauth 目录中创建该对象的新目录文件。添加到身份验证对象的所有自定义属性都会添加到字典文件。

要定义自定义属性，请执行以下操作：

访问：管理

步骤 1 点击箭头以展开 Define Custom RADIUS Attributes 部分。

系统将显示属性字段。

步骤 2 在 **Attribute Name** 字段中键入由字母数字字符和破折号组成的属性名称 （不含空格）。

步骤 3 在 **Attribute ID** 字段中以整数形式键入属性 ID。

步骤 4 从 **Attribute Type** 下拉列表中选择属性的类型。

步骤 5　点击 **Add** 以将自定义属性添加到身份验证对象。

提示　可以通过点击自定义属性旁边的 **Delete** 从身份验证对象中移除该属性。

步骤 6　进入下一节第 61-34 页上的测试用户身份验证。

测试用户身份验证

许可证：任何环境

在配置 RADIUS 连接、用户角色和自定义属性设置后，可以为应该能够进行身份验证以测试这些设置的用户指定用户凭证。

对于用户名，可以输入要测试的用户的用户名。

请注意，由于 UI 页面大小限制，测试与具有 1000 个以上用户的服务器的连接仅返回 1000 个用户。

提示　如果测试用户的名称或密码键入不正确，即使服务器配置正确，测试也会失败。要验证服务器配置正确，请点击 **Test**，而无需首先在 **Additional Test Parameters** 字段中输入用户信息。如果成功，请提供要通过特定用户进行测试的用户名和密码。

要测试用户身份验证，请执行以下操作：

访问：管理

步骤 1　在 **User Name** 和 **Password** 字段中，键入其凭证应该用于验证对 RADIUS 服务器的访问的用户的用户名和密码。

例如，要测试以了解是否可以在 example 公司检索 `jsmith` 用户凭证，请键入 `jsmith`。

步骤 2　选择 **Show Details** 并点击 **Test**。

系统将显示一条消息，指示测试成功或者详细说明缺少或需要更正的设置。

步骤 3　如果测试成功，请点击 **Save**。

系统将显示 External Authentication 页面，其中会列出新对象。

要使用设备上的对象启用 RADIUS 身份验证，必须将已启用该对象的系统策略应用到此设备。有关详细信息，请参阅第 63-11 页上的启用外部身份验证和第 63-4 页上的应用系统策略。

RADIUS 身份验证对象示例

许可证：任何环境

本节提供 RADIUS 服务器身份验证对象示例以说明可如何使用 FireSIGHT 系统 RADIUS 身份验证功能。有关详细信息，请参阅：

- 第 61-35 页上的示例：使用 RADIUS 对用户进行身份验证
- 第 61-37 页上的示例：使用自定义属性对用户进行身份验证

示例：使用 RADIUS 对用户进行身份验证

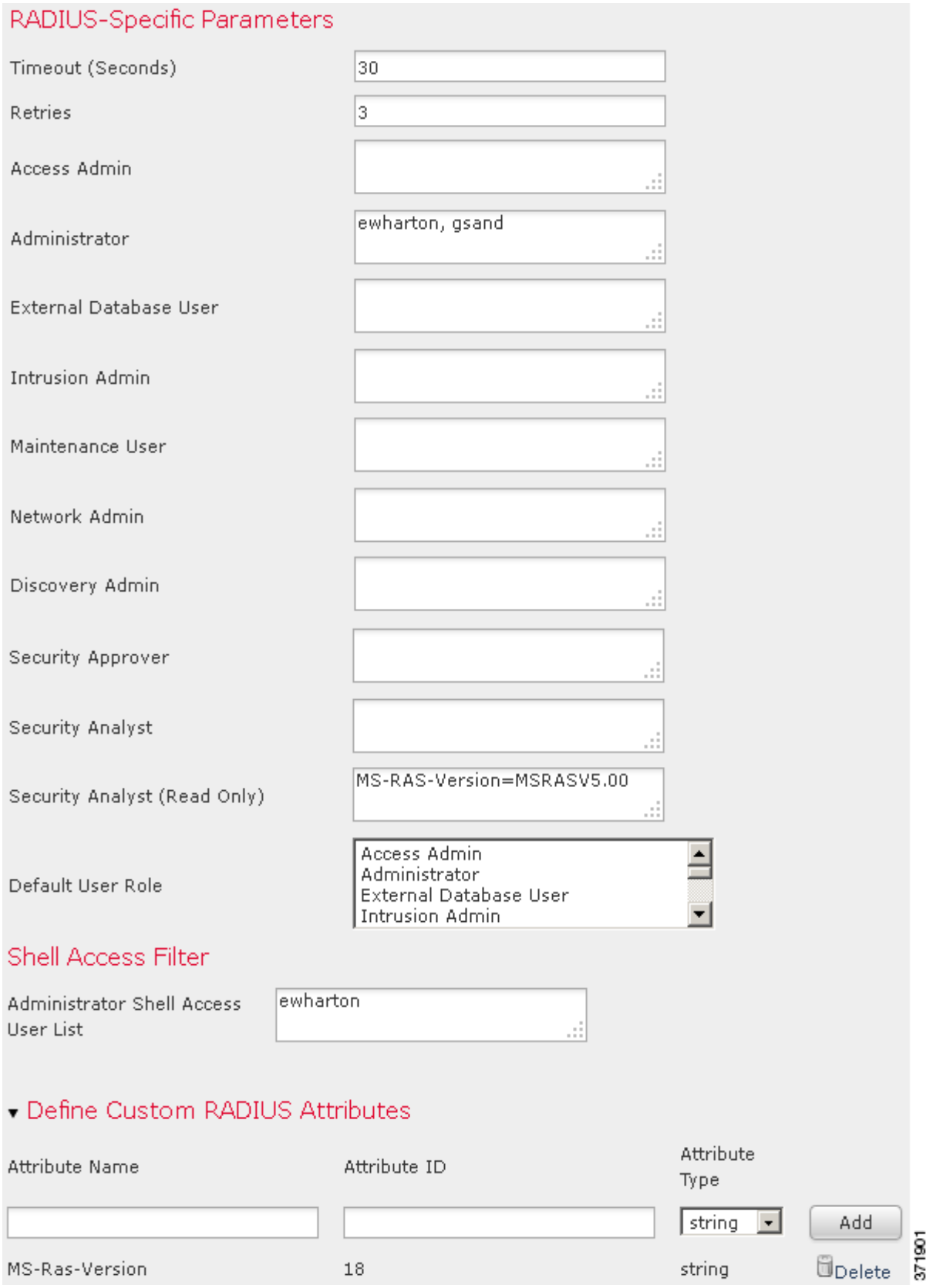
许可证：任何环境

下图说明 IP 地址为 10.10.10.98 的运行 FreeRADIUS 的服务器的样本 RADIUS 登录身份验证对象。请注意，连接使用端口 1812 进行访问，并请注意，与服务器的连接在停用 30 秒后将超时，然后重试三次后会尝试连接到备份身份验证服务器。

此示例说明 RADIUS 用户角色配置的重要方面：

- 用户 `ewharton` 和 `gsand` 被授予对已启用此身份验证对象的 FireSIGHT 系统设备的管理访问权。
- 用户 `cbronte` 被授予对已启用此身份验证对象的 FireSIGHT 系统设备的 Maintenance User 访问权。
- 用户 `jausten` 被授予对已启用此身份验证对象的 FireSIGHT 系统设备的 Security Analyst 访问权。
- 用户 `ewharton` 可以使用外壳帐户登录到设备中。

下图说明示例的角色配置：



示例：使用自定义属性对用户进行身份验证

许可证：任何环境

可以使用属性-值对识别应接收特定用户角色的用户。如果使用的属性是自定义属性，必须定义该自定义属性。

下图说明与前一示例中相同的 FreeRADIUS 服务器的样本 RADIUS 登录身份验证对象中的角色配置和自定义属性定义。

但是，在此示例中，由于正在使用 Microsoft 远程访问服务器，因此为一个或多个用户返回了 `MS-RAS-Version` 自定义属性。请注意，`MS-RAS-Version` 自定义属性为字符串。在此示例中，通过 Microsoft v5.00 远程访问服务器登录到 RADIUS 的所有用户 都应接收 Security Analyst (Read Only) 角色，因此请在 **Security Analyst (Read Only)** 字段中键入属性-值对 `MS-RAS-Version=MSRASV5.00`。

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	ewharton, gsand
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Discovery Admin	
Security Approver	
Security Analyst	
Security Analyst (Read Only)	MS-RAS-Version=MSRASV5.00
Default User Role	Access Admin Administrator External Database User Intrusion Admin

Shell Access Filter

Administrator Shell Access User List	ewharton

Define Custom RADIUS Attributes

Attribute Name	Attribute ID	Attribute Type	
		string	Add
MS-Ras-Version	18	string	Delete

371901

编辑 RADIUS 身份验证对象

许可证：任何环境

可以编辑现有身份验证对象。如果该对象正在系统策略中进行使用，则应用该策略时相应的设置保持生效，直到重新引用策略为止。

要编辑身份验证对象，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击 **External Authentication** 选项卡。

系统将显示 External Authentication 页面。

步骤 3　点击要编辑的对象旁边的编辑图标 ( )。

系统将显示 Create External Authentication Object 页面。

步骤 4　根据需要修改对象设置。

步骤 5　点击 **Save**。

系统保存更改并显示 External Authentication 页面。请记住，必须将已启用对象的系统策略应用到设备，然后身份验证更改才会在该设备上生效。有关详细信息，请参阅第 63-11 页上的启用外部身份验证和第 63-4 页上的应用系统策略。

删除身份验证对象

许可证：任何环境

如果系统策略中当前未启用身份验证对象，则可以删除该对象。

要删除身份验证对象，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击 **External Authentication** 选项卡。

系统将显示 External Authentication 页面。

步骤 3　点击要删除的对象旁边的删除图标 ( )。

系统将删除对象并显示 External Authentication 页面。

管理用户帐户

许可证：任何环境

如果您具有管理员访问权限，则可以在防御中心或受管设备上使用Web 界面查看和管理用户帐户，包括添加、修改和删除帐户。还可以创建和修改自定义用户角色及配置用户角色升级。没有管理员访问权限的用户帐户被限制访问管理功能。导航菜单的外观对于各类型的用户有所不同。

有关管理用户帐户的详细信息，请参阅以下各节：

- 第 61-40 页上的查看用户帐户说明如何访问可在其中添加、激活、停用、编辑和删除用户帐户的 User Management 页面。
- 第 61-41 页上的添加新用户帐户描述在添加新用户帐户时可以使用的不同选项。
- 第 61-42 页上的管理命令行访问描述如何向 3 系列或虚拟设备上的本地设备用户分配命令行界面访问权限。
- 第 61-43 页上的管理外部身份验证用户帐户说明如何添加外部身份验证用户以及可在 FireSIGHT 系统中管理的用户配置方面。
- 第 61-50 页上的修改用户权限和选项说明如何访问和修改现有用户帐户。
- 第 61-51 页上的了解受限用户访问属性说明如何将可用数据限制到数据访问受限制的用户帐户。
- 第 61-52 页上的删除用户帐户说明如何删除用户帐户。
- 第 61-52 页上的用户帐户权限包含列出各类型的用户帐户可访问的菜单和选项的表。

查看用户帐户

许可证：任何环境

从 User Management 页面中，可以查看、编辑和删除现有帐户。可以从 **Authentication Method** 列查看用户的身份验证类型。 **Password Lifetime** 列指示每个用户的密码的剩余天数。通过 **Action** 列中的图标，可以更详细地编辑用户并将用户设置为活动或非活动状态。请注意，对于外部身份验证用户，如果已禁用服务器的身份验证对象，则 **Authentication Method** 列会显示 **External (Disabled)**。

要访问 User Management 页面，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面，其中显示各用户，并带有用于激活、停用、编辑或删除用户帐户的选项。

有关可在 User Management 页面上执行的操作的信息，请参阅：

- 第 61-41 页上的添加新用户帐户
- 第 61-45 页上的配置用户角色
- 第 61-50 页上的修改用户权限和选项
- 第 61-51 页上的了解受限用户访问属性
- 第 61-51 页上的修改用户密码
- 第 61-52 页上的删除用户帐户

添加新用户帐户

许可证：任何环境

受支持的设备：因功能而异

设置新用户帐户时，可以控制帐户能够访问的系统部分。可以在创建期间设置用户帐户的密码到期和强度设置。对于 3 系列设备上的本地帐户，还可以配置用户将具有的命令行访问级别。

要添加新用户，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击 **Create User**。

系统随即会显示“创建用户”页面。

步骤 3　在 **User Name** 字段中，键入新用户的名称。

新用户名必须包含不带空格的字母数字字符或连字符，并且必须不超过 32 个字符。用户名区分大小写。

步骤 4　如果希望此用户在登录时向外部目录服务器进行身份验证，请选择 **Use External Authentication Method**。

如果启用此选项，则密码管理选项会消失。跳至第 8 步，以继续为用户配置访问角色。

请注意，为使用户向外部目录服务器进行身份验证，必须使用防御中心为要使用的服务器创建身份验证对象，然后应用已启用身份验证的系统策略。此外，外部身份验证服务器必须可用，以使这些用户登录到 FireSIGHT 系统设备中。有关详细信息，请参阅第 61-5 页上的管理身份验证对象和第 63-11 页上的启用外部身份验证。

步骤 5　在 **Password** 和 **Confirm Password** 字段中，键入密码 （最多 32 个字母数字字符）。

如果启用密码强度检查，则密码必须是至少八个大小写混合的字母数字字符，并且必须包含至少一个数字字符和一个特殊字符。它不能是字典中出现的单词或包含连续的重复字符。

注　如果在设备上启用 STIG 合规性，请参阅 *FireSIGHT 系统 STIG 版本说明*以获取有关外壳访问用户的密码设置的详细信息。

步骤 6　配置其余用户帐户登录选项。

有关详细信息，请参阅用户帐户登录选项表。

步骤 7　如果是通过 3 系列 设备的 Web 界面创建本地用户，可以为用户分配 **Command-Line Interface Access** 级别：

- 选择 **None** 可为用户禁用对命令行的访问。
- 选择 **Basic** 可允许用户登录到外壳中并访问命令的特定子集。
- 选择 **Configuration** 可允许用户登录到外壳中并使用任何命令行选项，包括专家模式 （如果在该设备上允许）。

  有关命令行访问的详细信息，请参阅第 61-42 页上的管理命令行访问。

步骤 8　选择要向用户授予的访问角色。

注　对于所有物理受管设备，思科提供的预定义用户角色限用于 Administrator、 Maintenance User 和 Security Analyst。

有关详细信息，请参阅第 61-45 页上的配置用户角色。

步骤 9　点击 **Save**。

系统创建用户并再次显示 User Management 页面。

提示　点击 User Management 页面上内部身份验证用户的名称旁边的滑块以重新激活该用户，或者禁用活动用户帐户而不将其删除。

管理命令行访问

许可证：任何环境

受支持的设备：3 系列、虚拟设备

在3 系列 或虚拟设备上，可以将命令行界面访问分配给本地设备用户。

请注意，也可以在虚拟设备上为用户分配命令行访问，但是从命令行界面使用命令。有关详细信息，请参阅第 D-1 页上的命令行参考。

用户可以运行的命令取决于分配给用户的访问级别。将 **Command-Line Interface Access** 设置为 **None** 时，用户无法在命令行上登录到设备中。当用户提供凭证时，用户启动的任何会话都将关闭。创建用户时，访问级别默认为 **None**。将 **Command-Line Interface Access** 设置为 **Basic** 时，用户可以运行特定命令集。

表 61-3　　基本命令行命令

configure password	接口
end	lcd
exit	link-state
帮助	log-ips-connection
历史	managers
logout	memory
?	型号
??	mpls-depth
access-control-config	NAT
alarms	网络
arp-tables	network-modules
audit-log	ntp
bypass	perfstats
集群	portstats
cpu	power-supply-status
database	process-tree

表 61-3　　基本命令行命令（续）

device-settings	processes
disk	routing-table
disk-manager	serial-number
dns	堆叠
expert	小结
fan-status	时间
fastpath-rules	traffic-statistics
gui	位置
主机名	virtual-routers
hyperthreading	virtual-switches
inline-sets	

将 **Command-Line Interface Access** 设置为 **Configuration** 时，用户可以访问任何命令行选项。请谨慎将此访问级别分配给用户。

注意事项　向外部身份验证用户授予的外壳访问默认为 **Configuration** 级别的命令行访问，从而将权限授予所有命令行实用程序。有关外部身份验证用户的外壳访问的详细信息，请参阅第 61-8 页上的了解外壳访问和第 61-22 页上的配置外壳访问。

管理外部身份验证用户帐户

许可证：任何环境

当外部身份验证用户登录到已启用内部身份验证的设备中时，该设备通过在身份验证对象中指定组成员资格授予用户所设置的默认访问角色。如果未配置访问组设置，设备将授予在系统策略中设置的默认用户角色。但是，如果在用户登录到设备中之前以本地方式添加这些用户，则在 User Management 页面上配置的用户权限会覆盖默认设置。

有关选择默认用户角色的详细信息，请参阅第 63-11 页上的启用外部身份验证和第 61-3 页上的了解用户权限。请注意，可以将预定义用户角色和自定义用户角色均设置为外部身份验证用户的默认用户角色。有关详细信息，请参阅第 61-45 页上的配置用户角色。

当以下所有条件存在时，内部身份验证用户会转换为外部身份验证。

- 启用 LDAP（带有或不带 CAC）或 RADIUS 身份验证。
- 对于 LDAP 或 RADIUS 服务器上的用户存在同一用户名。
- 用户使用在 LDAP 或 RADIUS 服务器上为该用户存储的密码进行登录。

请注意，只能在防御中心上的系统策略中启用外部身份验证。如果要在受管设备上使用外部身份验证，必须使用防御中心将策略应用到这些受管设备。

在外部身份验证用户首次登录到设备中之后，该设备通过创建本地用户记录将这些凭证与权限集相关联。有关用户登录的详细信息，请参阅第 2-1 页上的登录设备。在初始登录后，除非通过组或列表成员资格授予该本地用户记录的权限，否则可以修改这些权限，如下所示：

- 如果外部身份验证用户帐户的默认角色设置为特定访问角色，则用户可以使用其外部帐户凭证登录到设备中，而无需系统管理员进行任何其他配置。
- 如果帐户已进行外部身份验证并在默认情况下没有接收任何访问权限，则用户可以登录但无法访问任何功能。然后，您（或您的系统管理员）可以更改权限以授予对用户功能的适当访问。

提示 系统不会为外壳访问用户创建本地用户帐户。外壳访问完全通过为 LDAP 服务器设置的外壳访问过滤器或 PAM 登录属性进行控制，或者通过 RADIUS 服务器上的外壳访问列表来控制。

有关修改用户访问的详细信息，请参阅第 61-50 页上的修改用户权限和选项。请注意，不能通过 FireSIGHT 系统界面管理外部身份验证用户的密码或停用外部身份验证用户。对于外部身份验证用户，由于 LDAP 组或 RADIUS 列表成员资格或属性值，不能通过 FireSIGHT 系统用户管理页面移除已分配有访问角色的用户的最低访问权限。在外部身份验证用户的 Edit User 页面上，由于外部身份验证服务器上的设置而授予的权限以状态 **Externally Modified** 进行标记。

但是，可以分配其他权限。修改外部身份验证用户的访问权限时， User Management 页面上的 Authentication Method 列提供状态 **External - Locally Modified**。

外壳用户可以使用小写字母用户名登录。外壳的登录身份验证区分大小写。

注意事项 在 3 系列 防御中心上，所有外壳用户都具有 `sudoers` 权限。请确保适当地限制具有外壳访问的用户列表。在 3 系列 和虚拟设备上，授予外部身份验证用户的外壳访问默认为 **Configuration** 级别的命令行访问，它还授予 `sudoers` 权限。有关设置外壳访问的详细信息，请参阅第 61-8 页上的了解外壳访问和第 61-22 页上的配置外壳访问。

管理用户登录设置

许可证：任何环境

可以控制每个用户帐户密码的更改方式和时间，以及用户帐户的禁用时间。如果为 Web 界面登录会话配置了超时，则可以使用户避免此超时。下表描述可用于管理密码和帐户访问的一些选项。

请注意，对于 3 系列 受管设备上的本地身份验证用户，更改用户的 Web 界面密码还会更改命令行界面的密码。

如果启用 **Check Password Strength** 选项，则最小密码长度自动设置为 8 个字符。如果还为 **Minimum Password Length** 设置超过 8 个字符的值，则更高的值适用。

注 启用 **Use External Authentication Method** 后，不再显示登录选项。使用外部身份验证服务器管理登录设置。

表 61-4　　用户帐户登录选项

选项	说明
Use External Authentication Method	如果希望此用户的凭证进行外部身份验证，请选择此复选框。 **注**　如果为用户选择此选项，并且外部身份验证服务器不可用，则该用户可以登录到 Web 界面中，但无法访问任何功能。
Maximum Number of Failed Logins	输入不含空格的整数，用于确定每个用户在登录尝试失败后且帐户锁定之前可以尝试的最大次数。默认设置为五次尝试；使用 0 允许失败登录数不受限制。
Minimum Password Length	输入不含空格的整数，用于确定用户密码的最小所需长度 （以字符数为单位）。默认设置为 `8`。值为 `0` 指示无需最小长度。
Days Until Password Expiration	输入用户密码到期之前经过的天数。默认设置为 `0`，指示密码永不过期。

表 61-4　用户帐户登录选项（续）

选项	说明
Days Before Password Expiration Warning	输入用户在其密码实际到期之前必须更改其密码的警告天数。默认设置为 0 天。 ⚠ **注意事项** 警告天数必须**小于**密码到期之前的天数。
Force Password Reset on Login	选择此选项以强制用户在其首次登录时更改其密码。
Check Password Strength	选择此选项以要求强密码。强密码必须为至少八个大小写混合的字母数字字符，并且必须包含至少一个数字字符和一个特殊字符。它不能是字典中出现的单词或包含连续的重复字符。
Exempt from Browser Session Timeout	如果不希望用户的登录会话由于不活动而终止，请选择此选项。具有 Administrator 角色的用户无法获得豁免。有关会话超时的详细信息，请参阅第 63-26 页上的配置用户界面设置。

配置用户角色

许可证：任何环境

每个 FireSIGHT 系统用户都具有一个或多个关联用户访问角色。例如，分析师需要访问事件数据以分析网络的安全性，但是可能无需访问 FireSIGHT 系统本身的管理功能。例如，使用用户角色，可以向分析师授予 Security Analyst 访问权限，同时为管理 FireSIGHT 系统的一个或多个用户保留 Administrator 角色。 FireSIGHT 系统包含为各种管理员和分析师设计的 10 个预定义用户角色。还可以创建具有专用访问权限的自定义用户角色。

用户可以访问的Web 界面中的菜单和其他选项取决于其角色。预定义用户角色具有预先确定的访问权限集，而自定义用户角色具有其创建者确定的精细访问权限。

可在 User Roles 页面上配置用户角色。

要访问 User Roles 页面，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击**用户角色**选项卡。

系统将显示 User Roles 页面，其中显示所有预定义和自定义用户角色，并带有用于激活、停用、编辑、复制、删除和导出角色的选项。

有关配置两种类型的用户角色的详细信息，请参阅：

- 第 61-46 页上的管理预定义用户角色
- 第 61-48 页上的管理自定义用户角色
- 第 61-49 页上的创建预定义用户角色的自定义副本
- 第 61-50 页上的删除自定义用户角色

管理预定义用户角色

许可证：任何环境

FireSIGHT 系统包含 10 个预定义用户角色，提供一系列访问权限集来满足贵组织的需求。在 User Roles 页面上，预定义角色标示为“思科 Provided”。请注意，受管设备仅有权访问 10 个预定义用户角色中的三个：Administrator、 Maintenance User 和 Security Analyst。

虽然无法编辑预定义用户角色，但是可以使用其访问权限集作为自定义用户角色的基础。有关创建和编辑自定义用户角色的信息，请参阅第 61-48 页上的管理自定义用户角色。此外，因为无法编辑预定义用户角色，因此无法对其进行配置以升级到其他用户角色。有关详细信息，请参阅第 61-60 页上的管理用户角色升级。

下表简要描述可供使用的预定义角色。有关每个角色可用的菜单和选项的列表，请参阅第 61-52 页上的用户帐户权限。

表 61-5　　预定义用户角色

用户角色	权限
Access Admin	提供对访问控制、 SSL 检查和文件策略功能的访问。但是请注意， Access Admin 无法应用访问控制策略。Access Admin 有权访问 **Policies** 菜单中的访问控制、SSL 检查及文件相关选项。
管理员	提供对分析和报告功能、规则和策略配置、系统管理和所有维护功能的访问。Administrator 有权访问所有菜单选项；其会话如果受攻击会有更高安全风险，因此不能使其免于登录会话超时。 请注意，出于安全原因，应限制 Administrator 角色的使用。 此角色在受管设备上也可用。
Discovery Admin	提供对网络发现、相关性和用户活动功能的访问。Discovery Admin 有权访问 **Policies** 菜单中的相关选项。
External Database User	使用支持 JDBC SSL 连接的应用对 FireSIGHT 系统数据库的只读访问。请注意，为使第三方应用向 FireSIGHT 系统设备进行身份验证，必须在系统设置中启用数据库访问，如第 64-6 页上的启用数据库访问中所述。在 Web 界面上， External Database User 仅有权访问 **Help** 菜单中与联机帮助相关的选项。由于此角色的功能不涉及Web 界面，因此提供访问只是为便于支持和密码更改。
Intrusion Admin	提供对所有入侵策略、入侵规则和网络分析策略功能的访问。 Intrusion Admin 有权访问 **Policies** 菜单中与入侵相关的选项。请注意， Intrusion Admin 无法将入侵策略或网络分析策略应用为访问控制策略的一部分。
Maintenance User	提供对监控和维护功能的访问。 Maintenance User 有权访问 **Health** 和 **System** 菜单中与维护相关的选项。 此角色在受管设备上也可用。
网络管理员	提供对访问控制、SSL 检查和设备配置功能的访问。 Network Admin 有权访问 **Policies** 和 **Devices** 菜单中的访问控制、 SSL 检查和设备相关选项。
安全分析师	提供对安全事件分析功能的访问，包括事件视图、报告、主机、主机属性、服务、漏洞、客户端应用及运行状况事件只读访问。 Security Analyst 有权访问 **Overview**、 **Analysis**、**Health** 和 **System** 菜单中与分析相关的选项。 此角色在受管设备上也可用。

表 61-5　预定义用户角色 （续）

用户角色	权限
Security Analyst (Read Only)	提供对安全事件分析功能的只读访问，包括事件视图、报告、主机、主机属性、服务、漏洞、客户端应用和运行状况事件。 Security Analyst 有权访问 **Overview**、**Analysis**、**Health** 和 **System** 菜单中与分析相关的选项。
Security Approver	提供对访问控制、入侵、文件、SSL 和网络发现策略的有限访问。 Security Approver 可以查看这些策略并应用网络发现、入侵和访问控制策略，但是无法进行策略更改。他们有权访问 **Policies** 菜单中适用的与策略相关的选项。

除向用户分配事件分析师角色以外，可以限制该用户的删除权限，以仅允许删除由该用户创建的报告配置文件、搜索、书签、自定义表和自定义工作流程。有关详细信息，请参阅第 61-41 页上的添加新用户帐户。

请注意，如果没有为外部身份验证用户分配其他角色，则根据 LDAP 或 RADIUS 身份验证对象中以及系统策略中的设置，他们仅有最低访问权限。可以向这些用户分配其他权限，但是要移除或更改最低访问权限，必须执行以下任务：

- 在身份验证对象中将用户从一个列表移至另一个列表，或者在外部身份验证服务器上更改用户的属性值或组成员资格。
- 重新应用系统策略。
- 使用 User Management 页面从该用户帐户中移除访问权。

不能删除预定义用户角色，但是可以将其停用。停用角色会从已分配有该角色的任何用户从移除该角色和所有关联权限。

注意事项　如果已停用的角色是分配给指定用户的唯一角色，则该用户可以登录并访问 User Preferences 菜单，但是无法以其他方式访问 FireSIGHT 系统。

要激活或禁用用户角色，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击**用户角色**选项卡。

系统将显示 User Roles 页面。

步骤 3　点击要激活或停用的用户角色旁边的滑块。

注　如果在具有某个角色的用户已登录时通过远端控制管理停用，然后重新启用该角色，或者在该用户的登录会话期间从备份恢复用户或用户角色，则该用户必须重新登录到 Web 界面中才能重新获取对 IPMItool 命令的访问。有关详细信息，请参阅第 64-23 页上的使用无人值守管理。

管理自定义用户角色

许可证：任何环境

除以上预定义角色外，还可以配置具有专用访问权限的自定义用户角色。自定义用户角色可以具有任何基于菜单的权限集和系统权限集，并且可能完全是原始的或基于预定义用户角色。与预定义用户角色类似，自定义角色可以充当外部身份验证用户的默认角色。与预定义角色不同，可以修改和删除自定义角色。

可选择的权限分层并且基于 FireSIGHT 系统菜单布局。如果权限具有子页面，并且其具有比简单页面访问更精细的权限可用，则可以展开这些权限。在此情况下，父权限授予页面查看访问权以及对该页面的相关功能的子精细访问。例如，Correlation Events 权限授予对 Correlation Events 页面的访问，而 Modify Correlation Events 复选框则允许用户编辑和删除该页面上可用的信息。包含单词“Manage”的权限授予编辑和删除其他用户创建的信息的能力。

提示 对于菜单中结构不包括的页面或功能，由父级或相关页面授予权限。例如，通过 Modify Intrusion Policy 权限还您还可以修改网络分析策略。

可以对自定义用户角色应用受限搜索。这些会限制用户在事件查看器中可查看的数据。可以配置受限搜索，方法是先创建专用已保存搜索，然后在适当的基于菜单的权限下从“Restricted Search”下拉菜单中选择该搜索。有关详细信息，请参阅第 60-2 页上的执行搜索。

在防御中心上配置自定义用户角色时，所有基于菜单的权限都可供授予。在受管设备上配置自定义用户角色时，只有与设备功能相关的部分权限可用。有关可以配置的基于菜单的权限及其与预定义用户角色的关系的详细信息，请参阅：

- 第 61-53 页上的 Analysis 菜单
- 第 61-56 页上的 Policies 菜单
- 第 61-57 页上的 Devices 菜单
- 第 61-58 页上的对象管理器
- 第 61-58 页上的 Health 菜单
- 第 61-59 页上的系统菜单
- 第 61-60 页上的 Help 菜单

通过 System Permissions 下的可选选项，可以创建能够对外部数据库进行查询或升级到目标用户角色的权限的用户角色。有关详细信息，请参阅第 64-6 页上的启用数据库访问和第 61-60 页上的管理用户角色升级。

或者，可以从其他设备导出自定义用户角色，然后将其导入到您的设备上，而不是创建新的自定义用户角色。然后，在应用已导入的角色之前，可以对其进行编辑以满足需求。有关详细信息，请参阅第 A-1 页上的导出配置和第 A-4 页上的导入配置。

要创建自定义用户角色，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击**用户角色**选项卡。

系统将显示 User Roles 页面。

步骤 3　点击 **Create User Role**。

系统将显示 User Role Editor 页面。

步骤 4　在 **Name** 字段中，键入新用户角色的名称。

可以使用不含空格的字母数字字符或连字符。角色名称必须不超过 75 个字符。用户角色名称区分大小写。

步骤 5　或者，在 **Description** 字段中添加新角色的描述。

角色描述必须不超过 255 个字符。

步骤 6　选择新角色的权限。

选择未选定的权限时，会选择其所有子级，多值权限选择第一个值。如果清除选择高级权限，则也会清除其所有子级。未选择所有子级的已选权限以斜体文本显示。

请注意，选择复制要用作自定义角色基础的预定义用户角色将预先选择与该预定义角色关联的权限。有关复制预定义用户角色的详细信息，请参阅第 61-49 页上的创建预定义用户角色的自定义副本。

当前升级目标角色列出在角色升级复选框旁边。如果选择此复选框，即可选择通过已分配用户的密码或通过其他指定用户角色的密码对升级进行身份验证。有关详细信息，请参阅第 61-60 页上的管理用户角色升级。

步骤 7　点击 **Save**。

系统创建自定义用户角色并再次显示 User Roles 页面。

创建预定义用户角色的自定义副本

许可证：任何环境

可以复制现有角色以用作新的自定义角色的基础。这会在 User Role Editor 中预先选择现有角色的权限，从而可以对角色进行相互建模。

要创建预定义用户角色的自定义副本，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击**用户角色**选项卡。

系统将显示 User Roles 页面。

步骤 3　点击要复制的用户角色旁边的复制图标 ()。

系统将显示 User Role Editor 页面，其中已预先选择复制角色的权限。

请注意，自定义和预定义用户角色均可通过此方式进行复制。

删除自定义用户角色

许可证：任何环境

与预定义用户角色不同，可以删除不再必要的自定义角色。如果要禁用自定义角色而不完全将其移除，可以改为将其禁用；有关详细信息，请参阅第 61-46 页上的管理预定义用户角色中的过程。请注意，不能删除自己的用户角色或在系统策略中设置为默认用户角色的角色。有关详细信息，请参阅第 63-11 页上的启用外部身份验证。

要删除自定义用户角色，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击**用户角色**选项卡。

系统将显示 User Roles 页面。

步骤 3　点击要删除的自定义角色旁边的删除图标 ( )。

系统删除自定义角色。

如果已删除的角色是分配给指定用户的唯一角色，则该用户可以登录并访问 User Preferences 菜单，但是无法以其他方式访问 FireSIGHT 系统。

修改用户权限和选项

许可证：任何环境

将用户帐户添加到系统中后，可以随时修改访问权限、帐户选项或密码。请注意，密码管理选项不适用于向外部目录服务器身份验证的用户。请在外部服务器上管理这些设置。但是，必须配置所有帐户的访问权限，包括进行外部身份验证的帐户。

对于外部身份验证用户，由于 LDAP 组或 RADIUS 列表成员资格或属性值，不能通过 FireSIGHT 系统用户管理页面移除已分配有访问角色的用户的最低访问权限。但是，可以分配其他权限。修改外部身份验证用户的访问权限时， User Management 页面上的 Authentication Method 列提供状态 **External - Locally Modified**。

请注意，如果将用户的身份验证从外部身份验证更改为内部身份验证，必须为该用户提供新密码。

要修改用户帐户权限，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击要修改的用户旁边的编辑图标 ( )。

系统随即会显示“更改用户”页面。

步骤 3　根据需要修改一个或多个帐户：

- 有关可如何通过外部服务器来对用户进行身份验证的描述，请参阅第 61-43 页上的管理外部身份验证用户帐户。

- 有关更改内部身份验证用户的密码设置的信息，请参阅第 61-44 页上的管理用户登录设置。
- 有关配置用于授予 FireSIGHT 系统功能访问权的角色的详细信息，请参阅第 61-45 页上的配置用户角色。

了解受限用户访问属性

许可证：任何环境

可以通过对用户角色应用受限搜索来限制该角色在事件查看器中可查看的数据。可以在创建或编辑分配给用户的角色时指定此信息。要创建具有受限访问的自定义角色，必须从 Menu Based Permissions 列表中选择要限制的表，然后从 Restrictive Search 下拉列表中选择专用已保存搜索。有关详细信息，请参阅第 61-48 页上的管理自定义用户角色。

修改用户密码

许可证：任何环境

可以从 User Management 页面为内部身份验证用户修改用户密码。请注意，必须在 LDAP 或 RADIUS 服务器上管理外部身份验证用户密码。

注　如果在设备上启用 STIG 合规性或无人值守管理 (LOM)，则适用不同的密码限制。有关已启用 STIG 合规性的系统上的外壳访问用户密码设置的详细信息，请参阅 *FireSIGHT 系统 STIG 版本说明*。有关 LOM 用户的系统密码设置的详细信息，请参阅第 64-21 页上的启用无人值守管理用户访问。

要更改用户密码，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　在用户名旁边，点击编辑图标 ( )。

系统随即会显示“更改用户”页面。

步骤 3　在 **Password** 字段中，键入新密码 （最多 32 个字母数字字符）。

步骤 4　在 **Confirm Password** 字段中，重新键入新密码。

如果为用户帐户启用密码强度检查，则密码必须具有至少八个大小写混合的字母数字字符，以及至少一个数字和一个特殊字符。它不能是字典中出现的单词或包含连续的重复字符。

步骤 5　进行要对用户配置进行的任何其他更改：

- 有关密码选项的详细信息，请参阅第 61-44 页上的管理用户登录设置。
- 有关用户角色的详细信息，请参阅第 61-45 页上的配置用户角色。

步骤 6　点击 **Save**。

系统将更改密码并保存任何其他更改。

删除用户帐户

许可证：任何环境

除无法删除的管理员帐户以外，可以随时从系统中删除用户帐户。

要删除用户帐户，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　在要删除其帐户的用户旁边，点击删除图标 ( )。系统将删除帐户。

用户帐户权限

许可证：任何环境

以下各节提供 FireSIGHT 系统中可配置用户权限的列表以及可以访问这些权限的用户角色。此处所列的权限按照创建自定义用户角色时显示的 Menu Based Permissions 列表的顺序。并非所有权限在受管设备上都可用；仅在防御中心上可用的权限相应进行了标记。有关详细信息，请参阅第 61-48 页上的管理自定义用户角色。

请注意，由于 DC500 防御中心和 2 系列设备支持受限功能集，因此并非所有权限都适用于这些设备。请参阅按设备型号支持的访问控制功能表，了解2 系列设备功能的摘要。

有关后续表中以及本文档各处使用的访问符号的详细信息，请参阅第 1-16 页上的访问约定。以下各节参考与基于网络的界面中每个主菜单关联的用户角色权限：

Overview 菜单

许可证：任何环境

下表按顺序列出访问 Overview 菜单中的各选项所需的用户角色权限以及用户角色是否有权访问其中的子权限。Security Approver、Discovery Admin、Intrusion Admin、Access Admin、Network Admin 和 External Database User 角色在 Overview 菜单中没有权限。

表 61-6　Overview 菜单

权限	管理	Maint User	安全分析师	Security Analyst (RO)
控制面板	是	是	是	是
Manage Dashboards	是	否	否	否
Appliance Information Widget	是	是	是	是
Appliance Status Widget *（仅限防御中心）*	是	是	是	是
Correlation Events Widget	是	否	是	是
Current Interface Status Widget	是	是	是	是
Current Sessions Widget	是	否	否	否
Custom Analysis Widget *（仅限防御中心）*	是	否	是	是
Disk Usage Widget	是	是	是	是
Interface Traffic Widget	是	是	是	是
Intrusion Events Widget *（仅限防御中心）*	是	否	是	是
Network Correlation Widget *（仅限防御中心）*	是	否	是	是
Product Licensing Widget *（仅限防御中心）*	是	是	否	否
Product Updates Widget	是	是	否	否
RSS Feed Widget	是	是	是	是
System Load Widget	是	是	是	是
System Time Widget	是	是	是	是
White List Events Widget *（仅限防御中心）*	是	否	是	是
Reporting *（仅限防御中心）*	是	否	是	是
Manage Report Templates *（仅限防御中心）*	是	否	是	是
小结	是	否	是	是
Intrusion Event Statistics *（仅限防御中心）*	是	否	是	是
Intrusion Event Performance	是	否	否	否
Intrusion Event Graphs *（仅限防御中心）*	是	否	是	是
Discovery Statistics *（仅限防御中心）*	是	否	是	是
Discovery Performance *（仅限防御中心）*	是	否	否	否
Connection Summary *（仅限防御中心）*	是	否	是	是

Analysis 菜单

许可证：任何环境

下表按顺序列出访问 Analysis 菜单中的各选项所需的用户角色权限以及用户角色是否有权访问其中的子权限。在不同标题下多次出现的权限将仅列于其第一次出现的表中，不同在于指示的是子菜单标题。 Security Approver、 Intrusion Admin、 Access Admin、 Network Admin 和 External Database User 角色在 Analysis 菜单中没有权限。 Analysis 菜单仅在防御中心上可用。

表 61-7　Analysis 菜单

菜单	管理	Discovery Admin	Maint User	安全分析师	Security Analyst (RO)
Application Statistics	是	否	否	是	是
Geolocation Statistics	是	否	否	是	是
用户统计信息	是	否	否	是	是
URL Category Statistics	是	否	否	是	是
URL Reputation Statistics	是	否	否	是	是
SSL statistics	是	否	否	是	是
Intrusion Event Statistics by Application	是	否	否	是	是
Intrusion Event Statistics by User	是	否	否	是	是
Security Intelligence Category Statistics	是	否	否	是	是
File Storage Statistics by Disposition	是	否	否	是	是
File Storage Statistics by Type	是	否	否	是	是
Dynamic File Analysis Statistics	是	否	否	是	是
情景管理器	是	否	否	是	是
Connection Events	是	否	否	是	是
Modify Connection Events	是	否	否	是	否
Connection Summary Events	是	否	否	是	是
Modify Connection Summary Events	是	否	否	是	否
Security Intelligence Events	是	否	否	是	是
Modify Security Intelligence Events	是	否	否	是	否
入侵	是	否	否	是	是
Intrusion Events	是	否	否	是	是
Modify Intrusion Events	是	否	否	是	否
View Local Rules	是	否	否	是	是
Reviewed Events	是	否	否	是	是
Clipboard	是	否	否	是	是
事件	是	否	否	是	是
文件	是	否	否	是	是
Malware Events	是	否	否	是	是
Modify Malware Events	是	否	否	是	否
File Events	是	否	否	是	是
Modify File Events	是	否	否	是	否
Captured Files	是	否	否	是	是
Modify Captured Files	是	否	否	是	否
文件轨迹	是	否	否	是	是
File Download	是	否	否	是	是

表 61-7　Analysis 菜单 （续）

菜单	管理	Discovery Admin	Maint User	安全分析师	Security Analyst (RO)
Dynamic File Analysis	是	否	否	是	否
主机	是	否	否	是	是
Network Map	是	否	否	是	是
主机	是	否	否	是	是
Modify Hosts	是	否	否	是	否
危害表现	是	否	否	是	是
Modify Indications of Compromise	是	否	否	是	否
服务器	是	否	否	是	是
Modify Servers	是	否	否	是	否
漏洞	是	否	否	是	是
Modify Vulnerabilities	是	否	否	是	否
Host Attributes	是	否	否	是	是
Modify Host Attributes	是	否	否	是	否
应用	是	否	否	是	是
Application Details	是	否	否	是	是
Modify Application Details	是	否	否	是	否
Host Attribute Management	是	否	否	否	否
Discovery Events	是	否	否	是	是
Modify Discovery Events	是	否	否	是	否
用户	是	是	否	是	是
用户活动	是	是	否	是	是
Modify User Activity Events	是	是	否	是	否
用户	是	是	否	是	是
Modify Users	是	是	否	是	否
漏洞	是	否	否	是	是
Third-party Vulnerabilities	是	否	否	是	是
Modify Third-party Vulnerabilities	是	否	否	是	否
互联	是	是	否	是	是
Correlation Events	是	是	否	是	是
Modify Correlation Events	是	是	否	是	否
White List Events	是	是	否	是	是
Modify White List Events	是	是	否	是	否
White List Violations	是	是	否	是	是
Remediation Status	是	是	否	否	否
Modify Remediation Status	是	是	否	否	否

表 61-7　Analysis 菜单 （续）

菜单	管理	Discovery Admin	Maint User	安全分析师	Security Analyst (RO)
自定义	是	否	否	是	是
自定义工作流程	是	否	否	是	是
Manage Custom Workflows	是	否	否	是	是
Custom Tables	是	否	否	是	是
Manage Custom Tables	是	否	否	是	是
搜索	是	否	是	是	是
管理搜索	是	否	否	否	否
书签	是	否	否	是	是
Manage Bookmarks	是	否	否	是	是

Policies 菜单

许可证：任何环境

下表按顺序列出访问 Policies 菜单中的各选项所需的用户角色权限以及用户角色是否有权访问其中的子权限。 External Database User、 Maintenance User、 Security Analyst 和 Security Analyst (Read Only) 角色在 Policies 菜单中没有权限。 Policies 菜单仅在防御中心上可用。

请注意，还可以通过 Intrusion Policy 和 Modify Intrusion Policy 权限创建和修改网络分析策略。

表 61-8　Policies 菜单

菜单	Access Admin	管理	Discovery Admin	Intrusion Admin	网络管理员	Security Approver
访问控制	是	是	否	否	是	是
访问控制列表	是	是	否	否	是	是
Modify Access Control Policy	是	是	否	否	是	否
Modify Administrator Rules	是	是	否	否	是	否
Modify Root Rules	是	是	否	否	是	否
Apply Intrusion Policies	否	是	否	否	否	是
Apply Access Control Policies	否	是	否	否	否	是
入侵	是	是	否	是	否	是
Intrusion Policy	否	是	否	是	否	是
Rule Editor	否	是	否	是	否	否
电子邮件	否	是	否	是	否	否
Modify Intrusion Policy	否	是	否	是	否	否
File Policy	是	是	否	否	否	否
Modify File Policy	是	是	否	否	否	否
网络发现	否	是	是	否	否	是
Custom Fingerprinting	否	是	是	否	否	否

表 61-8　　Policies 菜单 （续）

菜单	Access Admin	管理	Discovery Admin	Intrusion Admin	网络管理员	Security Approver
Custom Topology	否	是	是	否	否	否
Modify Network Discovery	否	是	是	否	否	否
Apply Network Discovery	否	是	否	否	否	是
SSL	是	是	否	否	是	是
Modify SSL Policy	是	是	否	否	是	否
Modify Administrator Rules	是	是	否	否	是	否
Modify Root Rules	是	是	否	否	是	否
Apply SSL Policy	否	是	否	否	否	是
Application Detectors	否	是	是	否	否	否
User 3rd Party Mappings	否	是	是	否	否	否
Custom Product Mappings	否	是	是	否	否	否
用户	否	是	否	否	否	否
互联	否	是	否	否	否	否
策略管理	否	是	否	否	否	否
规则管理	否	是	否	否	否	否
White List	否	是	否	否	否	否
Traffic Profiles	否	是	否	否	否	否
行动	否	是	是	否	否	否
警报	否	是	是	否	否	否
Impact Flag Alerts	否	是	是	否	否	否
Discovery Event Alerts	否	是	是	否	否	否
Scanners	否	是	是	否	否	否
Scan Results	否	是	是	否	否	否
Modify Scan Results	否	是	是	否	否	否
群组	否	是	否	否	否	否
模块	否	是	否	否	否	否
Instances	否	是	否	否	否	否

Devices 菜单

许可证：任何环境

Devices 菜单表按顺序列出访问 Devices 菜单中的各选项及其中的子权限所需的用户角色权限。 X 指示用户角色具有访问权。 Access Admin、 Discovery Admin、 External Database User、 Intrusion Admin、Maintenance User、Security Approver、Security Analyst 和 Security Analyst (Read Only) 在 Devices 菜单中没有权限。 Devices 菜单仅在防御中心上可用。

表 61-9　Devices 菜单

菜单	管理	网络管理员
设备管理	是	是
Modify Devices	是	是
Apply Device Changes	是	是
NAT	是	是
NAT List	是	是
Modify NAT Policy	是	是
Apply NAT Rules	是	否
VPN	是	是
Modify VPN	是	是
Apply VPN Changes	是	是

对象管理器

许可证：任何环境

对象管理器权限可供 Access Admin、Administrator 和 Network Admin 用户角色使用。对象管理器权限仅在防御中心上可用。

FireAMP

许可证：任何环境

FireAMP权限仅可供 Administrator 用户角色使用。此权限仅在防御中心上可用。

Health 菜单

许可证：任何环境

下表按顺序列出访问 Health 菜单中的各选项所需的用户角色权限以及用户角色是否有权访问其中的子权限。Access Admin、Discovery Admin、Intrusion Admin、External Database User、Network Admin 和 Security Approver 角色在 Health 菜单中没有权限。 Health 菜单仅在防御中心上可用。

表 61-10　Health 菜单

菜单	管理	Maint User	安全分析师	Security Analyst (RO)
健康政策	是	是	否	否
Modify Health Policy	是	是	否	否
Apply Health Policy	是	是	否	否
Health Events	是	是	是	是
Modify Health Events	是	是	否	否

系统菜单

许可证：任何环境

下表按顺序列出访问 System 菜单中的各选项所需的用户角色权限以及用户角色是否有权访问其中的子权限。 Access Admin、 Discovery Admin、 Intrusion Admin、 External Database User 和 Security Analyst (Read Only) 角色在系统菜单中没有权限。

表 61-11　　系统菜单

菜单	管理	Maint User	网络管理员	Security Approver	安全分析师
本地	是	否	否	否	否
配置	是	否	否	否	否
注册	是	否	否	否	否
高*可用性 （仅限 DC1000、 DC1500、 DC2000、 DC3000、 DC3500、 DC4000）*	是	否	否	否	否
eStreamer	是	否	否	否	否
Host Input Client *（仅限*防御中心）	是	否	否	否	否
用户管理	是	否	否	否	否
用户	是	否	否	否	否
用户角色	是	否	否	否	否
Login Authentication *（仅限*防御中心）	是	否	否	否	否
System Policy *（仅限*防御中心）	是	否	否	否	否
Apply System Policy *（仅限*防御中心）	是	否	否	否	否
Modify System Policy *（仅限*防御中心）	是	否	否	否	否
更新	是	否	否	否	否
Rule Updates *（仅限*防御中心）	是	否	否	否	否
Rule Update Import Log *（仅限*防御中心）	是	否	否	否	否
许可证	是	否	否	否	否
监控	是	是	是	是	是
审核	是	否	否	否	否
Modify Audit Log	是	否	否	否	否
Syslog	是	是	否	否	否
任务状态	是	是	是	是	是
View Other Users' Tasks	是	否	否	否	否
统计信息	是	是	否	否	否
工具	是	是	否	否	是
Backup Management	是	是	否	否	否
Restore Backup	是	是	否	否	否
调度	是	是	否	否	否
Delete Other Users' Scheduled Tasks	是	否	否	否	否
Import/Export	是	否	否	否	否

表 61-11　　系统菜单 （续）

菜单	管理	Maint User	网络管理员	Security Approver	安全分析师
Discovery Data Purge （*仅限*防御中心）	是	否	否	否	是
Whois	是	是	否	否	是

Help 菜单

许可证：任何环境

Help 菜单及其权限可供所有用户角色访问。不能限制 Help 菜单选项。

管理用户角色升级

许可证：任何环境

可以通过密码为自定义用户角色提供权限，以除基本角色的权限以外，暂时获取其他目标用户角色的权限。借此可以在用户缺勤期间将一个用户替换为另一个用户，或者更密切地跟踪高级用户权限的使用。

例如，其基本角色的权限非常有限的用户可以升级到 Administrator 角色以执行管理操作。可以配置此功能，以便用户可以使用其自己的密码，或者因此使用所指定的其他用户的密码。通过第二个选项，可以轻松管理所有适用用户的一个升级密码。有关详细信息，请参阅第 61-61 页上的为升级配置自定义用户角色。

请注意，一次仅有一个用户角色可以是升级目标角色。可以使用自定义或预定义用户角色。每次升级持续时长为登录会话的持续时间，并会记录在审计日志中。

有关配置和使用此功能的详细信息，请参阅：

- 第 61-60 页上的配置升级目标角色
- 第 61-61 页上的为升级配置自定义用户角色
- 第 61-62 页上的升级用户角色

配置升级目标角色

许可证：任何环境

可以分配任何用户角色 （预定义或自定义）来充当系统范围的升级目标角色。这是任何其他角色可升级到的角色 （如果其有能力）。

要配置升级目标角色，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击 **User Roles**。

系统将显示 User Roles 页面。

步骤 3　点击 **Configure Permission Escalation**。

系统将显示 Configure Permission Escalation 对话框。

步骤 4　从下拉列表中选择用户角色。

步骤 5　点击 **OK**，保存更改。

系统将保存更改并显示 User Roles 页面。

注　更改升级目标角色立即生效。已升级会话中的用户现在具有新升级目标的权限。

为升级配置自定义用户角色

许可证：任何环境

要使用用户角色升级功能，必须首先配置具有升级权限的自定义用户角色，选择其升级密码，然后将该角色分配给用户。有关详细信息，请参阅第 61-41 页上的添加新用户帐户和第 61-45 页上的配置用户角色。

为自定义角色配置升级密码时，请考虑贵组织的需求。如果要轻松管理多个升级用户，可能需要选择其密码充当升级密码的其他用户。如果更改该用户的密码或停用该用户，则需要该密码的所有升级用户都会受影响。借此可以更高效地管理用户角色升级，尤其是在选择可以集中管理的外部身份验证用户的情况下。

要为升级配置自定义用户角色，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　点击 **User Roles**。

系统将显示 User Roles 页面。

步骤 3　点击 **Create User Role** 以创建新的自定义用户角色，或者点击现有自定义用户角色旁边的编辑图标 ( )。

系统将显示 User Role Editor 页面。

步骤 4　选择自定义用户角色的名称、描述和基于菜单的权限。

有关详细信息，请参阅第 61-48 页上的管理自定义用户角色中的过程。

步骤 5　在 System Permissions 中，选择 **Set this role to escalate to:** 复选框。

系统将显示升级密码选项。

步骤 6　选择此角色用于升级的密码。此时您有两种选择：

- 如果希望具有此角色的用户在升级时使用其自己的密码，请选择 **Authenticate with the assigned user's password**。
- 如果希望具有此角色的用户使用其他用户的密码，请选择 **Authenticate with the specified user's password** 并键入该用户名。

注　在使用其他用户的密码进行验证时，可以输入任何用户名，甚至是已停用或不存在的用户的用户名。停用其密码用于升级的用户会使具有需要该密码的角色的用户无法升级。如有必要，可以使用此功能快速移除升级能力。

步骤 7　点击 **Save**。

系统保存更改并再次显示 User Roles 页面。具有此角色的用户现在可以升级到目标用户角色。有关如何向用户分配角色的详细信息，请参阅第 61-41 页上的添加新用户帐户。

升级用户角色

许可证：任何环境

当用户具有带升级权限的已分配自定义用户角色时，该用户可以随时升级到目标用户的权限。请注意，升级对用户首选项没有影响。如果没有为用户角色升级配置已分配的用户角色，则不会显示 User 菜单中的 **Escalate Permissions** 选项。

要升级用户权限，请执行以下操作：

访问：任何环境

步骤 1　选择 **Local > User > Escalate Permissions**。

系统将显示 Escalate User Permissions 对话框。

步骤 2　输入身份验证密码。

步骤 3　点击 **Escalate**。

除当前角色以外，您现在具有升级目标角色的所有权限。

请注意，升级持续至登录会话结束。要仅返回到基本角色的权限，必须注销，然后开始新会话。

配置从思科安全管理器单点登录

许可证：任何环境

受支持的设备：ASA FirePOWER

单点登录 (SSO) 支持思科安全管理器 (CSM) V4.7 或更高版本与防御中心之间的集成，从而可以从 CSM 访问防御中心，而无需其他身份验证以进行登录。在管理 ASA FirePOWER 设备的 ASA 模块时，可能要修改应用于设备的 FirePOWER 模块的策略。可以选择 CSM 中的主管防御中心并在网络浏览器中将其启动。如果主管防御中心是高可用性对的成员，则使用 SSO 会导航到主对等体。

如果您根据用户角色具有访问权限，则对于 CSM 中从中交叉启动的设备，系统会将您导航到 Device Management 页面的 Device 选项卡。否则，系统导航到 Summary Dashboard 页面 (**Overview > Dashboards**)，但没有控制面板访问权的用户帐户除外，它们使用 Welcome 页面。

在单点登录到防御中心之前，必须设置从 CSM 到防御中心的单向、加密身份验证路径。在 NAT 环境中，防御中心和 CSM 必须驻留在 NAT 边界的同一侧。要启用通信，必须提供以下条件以使 CSM 和防御中心相互识别：

- 从 CSM 中，必须生成用于识别连接的 SSO 共享加密密钥。必须在防御中心上输入此密钥。
- 在防御中心上，提供 CSM 服务器主机名或 IP 地址，以及服务器端口。如果使用的是高可用性，请在主对等体上配置 SSO。
- 要验证加密的身份验证参数，您必须将相同的用户名 （不区分大小写）在套件以及防御中心都 SSO 的所有用户。

为防御中心启用 STIG 合规性后，系统会禁用 SSO。.有关详情，请参见第 63-22 页上的启用 STIG 合规性。

注　如果贵组织使用 CAC 进行身份验证，则无法通过单点登录进行登录。有关详细信息，请参阅第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。

要设置单点登录，请执行以下操作：

访问：管理

步骤 1　从 CSM 中，生成 SSO 共享加密密钥。

有关详细信息，请参阅 CSM 文档。

步骤 2　从防御中心中，选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 3　选择 **CSM Single Sign-on**。

系统将显示 CSM Single Sign-on 页面。

步骤 4　输入 **CSM 主机名**或 **IP** 地址和服务器**端口**。

步骤 5　输入从 CSM 生成的**共享密钥**。

步骤 6　或者，如果您要使用防御中心的代理服务器与 CSM 进行通信，请选择 **Use Proxy For Connection** 复选框。有关详细信息，请参阅第 64-8 页上的了解管理接口选项。

步骤 7　点击**提交**。

系统将显示 CSM 证书。

步骤 8　点击 **Confirm Certificate** 以保存证书。

您现在可以从 CSM 登录到防御中心而无需其他登录。

安排任务

可安排许多不同类型的管理任务在指定时间运行一次或反复运行。

注 有些任务（例如，那些涉及自动化软件更新的任务，或者要求将更新推送到受管设备的任务）可能会显著增加低带宽网络的负载。应安排此类任务在网络使用量较低的时段运行。

有关详细信息，请参阅以下各节：

- 第 62-2 页上的配置周期性任务解释如何设置预定任务，使其按固定时间间隔运行。
- 第 62-3 页上的自动运行备份作业提供备份作业的安排步骤。
- 第 62-4 页上的自动执行证书撤销列表下载提供设备证书撤销列表 (CRL) 的自动刷新步骤。
- 第 62-5 页上的自动运行 Nmap 扫描提供 Nmap 扫描的安排步骤。
- 第 62-6 页上的自动应用入侵策略提供应用到受管设**受支持的防御中心：**备上的入侵策略的排队步骤。
- 第 62-7 页上的自动化生成报表提供报告安排步骤。
- 第 62-8 页上的自动运行地理定位数据库更新提供地理定位数据库 (GeoDB) 自动更新的安排步骤。
- 第 62-9 页上的自动 FireSIGHT 生成建议提供入侵规则状态建议自动更新的安排步骤。
- 第 62-10 页上的自动执行软件更新提供软件更新下载、推送和安装的安排步骤。
- 第 62-14 页上的自动更新漏洞数据库提供 VDB 更新下载和安装的安排步骤。
- 第 62-16 页上的自动更新 URL 过滤提供 URL 过滤数据的自动更新步骤。
- 第 62-17 页上的查看任务描述如何在安排任务之后进行查看和管理。
- 第 62-19 页上的编辑预定任务描述如何编辑现有任务。
- 第 62-19 页上的删除预定任务描述如何删除一次性任务和周期性任务的所有实例。

配置周期性任务

许可证：任何环境

使用相同流程为所有类型的任务设置周期性任务的频率。

请注意，网络界面上大多数页面中显示的时间为本地时间，由您在本地配置中指定的时区决定。此外，在适当时候，防御中心自动针对夏时令 (DST) 调整其本地时间显示。然而，跨越从 DST 到标准时间以及从标准时间到 DST 的过渡日期的周期性任务不因过渡而自行调整。也就是说，如果创建一个任务，预定在标准时间的凌晨 2:00 运行，则它将在 DST 期间的凌晨 3:00 运行。同样，如果创建一个任务，预定在 DST 期间的凌晨 2:00 运行，则它将在标准时间的凌晨 1:00 运行。

要配置周期性任务，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表中，选择想安排的任务类型。

可安排的每种任务类型均在其各自的部分有详细说明。

步骤 4　对于 **Schedule task to run** 选项，请选择 **Recurring**。

页面重新加载周期性任务选项。

步骤 5　在 **Start On** 字段中，指定想要开始周期性任务的日期。可使用下拉列表选择年、月、日。

步骤 6　在 **Repeat Every** 字段中，指定想要任务重复的频率。可指定小时数、天数、周数或月数。

提示　可键入数字，或者点击向上图标 (▲) 和向下图标 (▼) 指定时间间隔。例如，键入 2，选择 Days，让任务每两天运行一次。

步骤 7　在 **Run At** 字段中，指定想要开始周期性任务的时间。

步骤 8　如果已为 **Repeat Every** 选择 `Weeks`，则显示 **Repeat On** 字段。选择想要运行任务的一星期中天数旁边的复选框。

步骤 9　如果已为 **Repeat Every** 选择 `Months`，则显示 **Repeat On** 字段。使用下拉列表，选择想要运行任务的日期。

New Task 页面上的剩余选项取决于正在创建的任务。有关详细信息，请参阅：

- 第 62-3 页上的自动运行备份作业
- 第 62-4 页上的自动执行证书撤销列表下载
- 第 62-5 页上的自动运行 Nmap 扫描
- 第 62-7 页上的自动化生成报表
- 第 62-9 页上的自动 FireSIGHT 生成建议
- 第 62-10 页上的自动执行软件更新
- 第 62-14 页上的自动更新漏洞数据库
- 第 62-16 页上的自动更新 URL 过滤

自动运行备份作业

许可证：任何环境

受支持的设备：2 系列和 3 系列

受支持的防御中心：任何环境

可以使用调度程序自动化防御中心或物理受管设备的备份。必须先设计备份配置文件，然后才能将备份配置为预定任务。有关详细信息，请参阅第 70-5 页上的创建备份配置文件。

您**无法**执行虚拟受管设备、用于 Blue Coat X-系列的思科 NGIPS 或具备 FirePOWER 服务的 Cisco ASA 防火墙 的定期备份。要执行物理受管设备上配置数据的定期备份，请从设备自身的网络界面中安排此任务。要执行事件数据定期备份，请执行管理防御中心的定期备份。

要自动运行备份任务，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表中，选择 **Backup**。

页面重新加载，显示备份选项。

步骤 4　指定您想如何安排备份， **Once** 或 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 62-2 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　从 **Backup Profile** 列表中，选择相应的备份配置文件。

有关新建备份配置文件的详细信息，请参阅第 70-5 页上的创建备份配置文件。

步骤 7　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 8　或者，在 **Email Status To:** 字段中，键入任务状态消息要发送到的邮件地址（或多个邮件地址，用逗号隔开）。

必须在防御中心上配置一台有效的邮件中继服务器，以发送状态消息。有关配置中继主机的详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 9　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动执行证书撤销列表下载

许可证：任何环境

可使用调度程序，在启用用户证书的设备上，自动刷新设备网络服务器的证书撤销列表 (CRL)。在本地设备配置中启用 CRL 提取时自动创建 Download CRL 任务在，因此，此流程解释如何打开预定任务以设置频率。

提示　必须启用并配置用户证书，设置 CRL 下载 URL，然后才能安排任务。有关配置用户证书的信息，请参阅第 64-5 页上的要求用户证书。

要自动下载证书撤销列表，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　在 Task Details 中找到 **download CRL** 任务，点击编辑图标 ( )。

系统将显示 Edit Task 页面，其中显示了下载选项。

步骤 3　指定想要如何安排 CRL 下载， **Once** 或 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 62-2 页上的配置周期性任务。

步骤 4　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 5　或者，在 **Email Status To:** 字段中，键入任务状态消息要发送到的邮件地址 （或多个邮件地址，用逗号隔开）。

必须在防御中心上配置一台有效的邮件中继服务器，以发送状态消息。有关配置中继主机的详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 6　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动运行 Nmap 扫描

许可证：FireSIGHT

可在网络上安排定期 Nmap 目标扫描。自动化扫描允许您刷新 Nmap 扫描之前提供的信息。因为 FireSIGHT 系统无法更新 Nmap 提供的数据，所以，需要定期重新扫描，保持数据更新。还可安排扫描，使其自动在网络主机上测试未识别的应用或服务器。有关详细信息，请参阅：

- 为 Nmap 扫描准备系统
- 安排 Nmap 扫描

请注意，发现管理员也可使用 Nmap 扫描作为补救。例如，主机上发生的操作系统冲突可能会触发 Nmap 扫描。运行扫描可以获取主机的最新操作系统信息，解决冲突。有关详细信息，请参阅第 54-11 页上的 Nmap 扫描补救。

为 Nmap 扫描准备系统

许可证：FireSIGHT

如果之前未曾使用 Nmap 扫描功能，必须先完成若干 Nmap 配置步骤，然后才能定义预定扫描。有关详细信息，请参阅以下各节：

- 第 47-8 页上的创建 Nmap 扫描实例提供有关设置 Nmap 服务器连接配置文件的信息。
- 第 47-8 页上的创建 Nmap 扫描目标提供有关设置扫描目标的信息。
- 第 47-10 页上的创建 Nmap 补救提供有关设置补救定义的信息。

安排 Nmap 扫描

许可证：FireSIGHT

可使用 Nmap 实用程序，安排扫描网络中的一台或多台主机。

Nmap 使用 Nmap 扫描结果替换系统检测到的主机操作系统、应用或服务器之后，系统不再更新 Nmap 替换的主机信息。 Nmap 提供的服务和操作系统数据保持不变，直至运行另一次 Nmap 扫描。如果计划使用 Nmap 扫描主机，则可能想要设置定期扫描，使 Nmap 提供的操作系统、应用或服务器信息保持最新。如从网络删除主机并重新添加，则将丢弃任何 Nmap 扫描结果，系统假设监控主机的所有操作系统和服务数据。

要自动运行 Nmap 扫描，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表，选择 **Nmap Scan**。

页面重新加载，显示用于自动运行 Nmap 扫描的选项。

步骤 4　指定想要如何安排任务， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。

- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 62-2 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　在 **Nmap Remediation** 字段中，选择在运行扫描时要使用的 Nmap 补救。

步骤 7　在 **Nmap Target** 字段中，选择扫描目标，定义想要扫描的目标主机。

步骤 8　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 9　或者，在 **Email Status To:** 字段中，键入任务状态消息要发送到的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 10　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动应用入侵策略

许可证：保护

可对应用到受管设备的入侵策略进行排队。在任务运行时，如果引用了入侵策略的访问控制策略应用于所选设备，则此任务仅应用入侵策略。否则，任务未完成就会中止。

安排此任务之前，必须将入侵策略与访问控制策略相关联，并向设备应用访问控制策略；请参阅第 18-1 页上的使用入侵和文件策略控制流量。

要对应用到受管设备的策略进行排队，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示当前月份的安排日历页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表中，选择 **Queue Intrusion Policy Apply**。

此页面重新加载，显示用于对策略应用进行排队的选项。

步骤 4　指定想要如何安排任务， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明防御中心上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 62-2 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　在 **Intrusion Policy** 字段中，可进行以下选择：

- 选择要应用至所选目标设备的入侵策略。
- 选择 **All intrusion policies**，将所有已应用的入侵策略应用到在 **Device** 字段中所选的设备。

步骤 7　在 **Device** 字段中，可进行以下选择：

- 选择想要将在 **Intrusion Policy** 字段中选择的入侵策略应用到的设备。
- 选择 **All targeted devices**，将已选择的入侵策略应用到已应用该入侵策略的所有受监控设备。

提示　此字段仅显示已应用在 **Intrusion Policy** 字段中选择的入侵策略的设备。

步骤 8　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段出现在安排日历页面底部的 Tasks Details 部分，因此，应限制注释的长短。

步骤 9　或者，在 **Email Status To:** 字段中，键入任务状态消息要发送到的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 10　点击 **Save**。

任务添加成功。在日历页面的 Task Details 部分，可查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

步骤 11　要编辑已保存的任务，请在任务出现在安排日历页面上的任何位置点击任务。

Task Details 部分出现在页面底部。要做出任何更改，请点击编辑图标 ( )。

自动化生成报表

许可证：任何环境

受支持的设备：除 X -系列外的任何设备

可自动生成报告，以使它们按固定间隔运行。然而，必须设计报告模板，然后才能将报告配置为预定任务。有关如何使用报告设计程序创建报告模板的详细信息，请参阅第 57-1 页上的了解报告模板。

如果还要使用调度程序分发邮件报告，必须在安排任务**之前**配置您的报告模板和邮件中继主机。有关详细信息，请参阅第 57-26 页上的生成时通过邮件分发报告和第 63-17 页上的配置邮件中继主机和通知地址。

要自动生成报告，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示当前月份的安排日历页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表，选择 **Report**。

页面重新加载，显示的选项可用于将报告设置为自动运行。

步骤 4　指定想要如何安排任务， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明防御中心上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 62-2 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　在 **Report Template** 字段，从下拉列表中选择要使用的报告模板。有关详细信息，请参阅第 57-3 页上的创建和编辑报告模板。

步骤 7　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段出现在安排日历页面底部的 Tasks Details 部分，因此，应限制注释的长短。

步骤 8　或者，在 **Email Status To:** 字段中，键入任务状态消息要发送到的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

注　配置此选项**不会**分发报告。有关详细信息，请参阅第 57-26 页上的生成时通过邮件分发报告。

步骤 9　如果不想在报告没有数据（例如，当报告期间未发生特定类型的事件时）时接收报告邮件附件，请选择 **If report is empty, still attach to email** 复选框。

步骤 10　点击 **Save**。

任务添加成功。在日历页面的 Task Details 部分，可查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

步骤 11　要编辑已保存的任务，请在任务出现在安排日历页面上的任何位置点击任务。

Task Details 部分出现在页面底部。要做出任何更改，请点击编辑图标 ( )。

自动运行地理定位数据库更新

许可证：FireSIGHT

受支持的防御中心：除 DC500 外的所有型号

可使用调度程序，自动运行周期性地理定位数据库 (GeoDB) 更新。周期性 GeoDB 更新每 7 天（每周）运行一次；可配置每周更新运行时间。有关 GeoDB 更新的详细信息，请参阅第 66-24 页上的更新地理定位数据库。

要自动运行地理定位数据库更新，请执行以下操作：

访问：管理

步骤 1　选择 **System > Updates**。

系统将显示 Product Updates 页面。

步骤 2　点击 **Geolocation Updates** 选项卡。

系统将显示 Geolocation Updates 页面。

步骤 3　在 **Recurring Geolocation Updates** 下方，选择 **Enable Recurring Weekly Updates** 复选框。

系统将显示 Update Start Time 字段。

步骤 4　在 **Update Start Time** 字段中，指定想要每周 GeoDB 更新运行的周日和时间。

步骤 5　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动 FireSIGHT 生成建议

许可证：保护

可使用自定义入侵策略中最近保存的配置设置，根据网络发现数据，自动生成规则状态建议。

注　如果系统自动为入侵策略生成预定建议并且不保存更改，则必须丢弃在入侵策略中所做出的更改，而且如果想要策略反映自动生成的建议，还必须执行此策略。有关详情，请参见第 23-13 页上的解决冲突和提交策略更改。

当任务运行时，系统会自动生成建议的规则状态。或者，视乎策略配置，还可根据 第 33-1 页上的为您的网络资产定制入侵防御 中所述条件，修改入侵规则的状态。修改的规则状态将在下一次应用入侵策略时生效。

要自动生成规则状态建议，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表，选择 **FireSIGHT Recommended Rules**。

页面重新加载，显示用于生成 FireSIGHT 建议的选项。

步骤 4　或者，点击 **Job Type** 字段旁边的 **policies** 链接，显示 Detection & Prevention 页面，在其中，可配置入侵策略中的 FireSIGHT Recommended Rules。

步骤 5　指定想要如何安排任务， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 62-2 页上的配置周期性任务。

步骤 6　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 7　在 **Policies** 旁，选择想要在其中生成建议的一个或多个策略。您有以下选项：

- 在 **Policies** 字段中，选择一个或多个策略。使用 Shift 和 Ctrl 键选择多个策略。
- 点击 **All Policies** 复选框，选择所有策略。

步骤 8　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 9　或者，在 **Email Status To:** 字段中，键入要用于接收任务状态消息的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 10　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动执行软件更新

许可证：任何环境

可自动下载大多数修补程序和主要版本，并将其应用到 FireSIGHT 系统。

注　在两种情况下，必须手动上传和安装更新。第一，无法安排 FireSIGHT 系统的主要更新。第二，无法为不能访问支持网站的设备安排更新，或者无法安排来自这些设备的推送。如果设备未直接连接至互联网，应按第 64-8 页上的配置管理接口中所述设置一个代理，以便它从支持网站下载更新。有关手动更新 FireSIGHT 系统的信息，请参阅第 66-1 页上的更新系统软件。

必须安排安装软件更新的任务因正在更新防御中心还是正在使用防御中心更新受管设备而异。思科**强烈**建议使用防御中心更新其管理的设备。

要更新防御中心，请使用 Install Latest Update 任务安排软件安装。要使用防御中心自动对其受管设备执行软件更新，必须安排两个任务：

步骤 1　使用 Push Latest Update 任务将更新推送（复制）至受管设备。

步骤 2　使用 Install Latest Update 任务在受管设备上安装更新。

安排更新时，安排推送和安装任务连续发生。这就是说，要自动在受管设备上执行软件更新，必须首先将更新推送到设备，然后才能安装它。（请注意，在手动更新过程中，不必在安装前将更新推送到受管设备。有关详细信息，请参阅第 66-8 页上的更新受管设备。）

注　不能为集群或堆栈配置中的受管设备创建单个更新任务。

始终在任务之间预留充分的时间，以便完成相关过程。至少将任务间隔安排为 30 分钟。例如，如果安排一个更新安装任务，而且更新尚未完成从防御中心到设备的复制，则安装任务将不成功。然而，如果安排的安装任务每天重复一次，它将在第二天运行时安装推送的更新。

如果想要加大对此过程的控制，可在得知更新已发布之后，在非高峰时段使用 **Once** 选项下载和安装更新。

有关详细信息，请参阅：

- 第 62-11 页上的自动下载软件
- 第 62-12 页上的自动推送软件
- 第 62-13 页上的自动安装软件

自动下载软件

许可证：任何环境

可创建一个预定任务，自动从思科下载最新软件更新。可使用此任务安排下载计划手动安装的更新。

要自动下载软件更新，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表，选择 **Download Latest Update**。

系统重新加载 New Task 页面，显示更新选项。

步骤 4　指定想要如何安排任务， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 62-2 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　在 **Update Items** 部分，选择 **Software**。

步骤 7　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 8　或者，在 **Email Status To:** 字段中，键入任务状态消息要发送到的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 9　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动推送软件

许可证：任何环境

如果想要在受管设备上自动安装软件更新，必须先将更新推送至设备，然后再安装。

将更新推送至受管设备后， Tasks 页面上将报告有关推送过程状态的信息。有关详情，请参见第 C-1 页上的查看长时间运行任务的状态。

创建向受管设备推送软件更新的任务时，确保在推送任务与预定安装任务之间预留充分时间，以便将更新复制至设备。

要向受管设备推送软件更新，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表，选择 **Push Latest Update**。

页面重新加载，显示用于推送更新的选项。

步骤 4　指定想要如何安排任务， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 62-2 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　从 **Device** 列表，选择想接收更新的设备。

步骤 7　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 8　或者，在 **Email Status To:** 字段中，键入要用于接收任务状态消息的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 9　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动安装软件

许可证：任何环境

如在使用防御中心创建在受管设备上安装软件更新的任务，确保在向设备推送更新的任务与更新安装任务之间预留充分的时间。有关向受管设备推送更新的信息，请参阅第 62-12 页上的自动推送软件。

注意事项　视乎正在安装的更新，设备可能在安装软件之后重新启动。

要安排软件安装任务，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表，选择 **Install Latest Update**。

系统重新加载页面，显示用于安装更新的选项。

步骤 4　指定想要如何安排任务， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 62-2 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　从 **Device** 列表，可以进行以下选择：

- 选择要安装更新的设备。
- 选择要安装更新的防御中心的名称。

步骤 7　在 **Update Items** 部分，选择 **Software**。

步骤 8　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 9　或者，在 **Email Status To:** 字段中，键入要用于接收任务状态消息的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 10　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动更新漏洞数据库

许可证：FireSIGHT

思科使用漏洞数据库 (VDB) 更新扩展 FireSIGHT 系统识别的网络资产、流量和漏洞列表。可使用排程功能，在防御中心上下载和安装最新的 VDB 更新，从而确保正在使用最新信息评估网络主机。

注　不能为无法访问支持网站的设备安排更新。如果设备未直接连接至互联网，应按第 64-8 页上的配置管理接口中所述设置一个代理，以便它从支持网站下载更新。有关手动更新 FireSIGHT 系统的信息，请参阅第 66-1 页上的更新系统软件。

自动更新 VDB 时，必须自动完成两个独立的步骤：

步骤 1　下载 VDB 更新。

步骤 2　安装 VDB 更新。

始终在任务之间预留充分的时间，以便完成相关过程。例如，如果安排一个更新安装任务，并且更新尚未完全下载，安装任务将不成功。然而，如果安排的安装任务每天重复一次，它将在第二天运行时安装已下载的 VDB 更新。

如想加大对此过程的控制，可在得知更新已发布之后，在非高峰时段使用 **Once** 选项下载和安装 VDB 更新。

注　安装 VDB 更新会导致短暂停止流量和处理，还可能会导致遗漏检查一些数据包。

有关详细信息，请参阅：

- 第 62-14 页上的自动下载 VDB 更新
- 第 62-15 页上的自动安装 VDB 更新

自动下载 VDB 更新

许可证：FireSIGHT

可在 防御中心 上创建一个预定任务，自动从思科下载最新的 VDB 更新。

要自动下载 VDB 更新，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表，选择 **Download Latest Update**。

系统重新加载 New Task 页面，显示更新选项。

步骤 4　指定想要如何安排任务， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 62-2 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　在 **Update Items** 部分，选择 **Vulnerability Database**。

步骤 7　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 8　或者，在 **Email Status To**: 字段中，键入任务状态消息要发送到的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 9　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动安装 VDB 更新

许可证：FireSIGHT

应在 VDB 更新下载任务与更新安装任务之间预留充分的时间；有关详细信息，请参阅第 62-14 页上的自动下载 VDB 更新。

注　安装 VDB 更新会导致短暂停止流量和处理，还可能会导致遗漏检查一些数据包。

要安排 VDB 更新，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表，选择 **Install Latest Update**。

系统重新加载页面，显示用于安装更新的选项。

步骤 4　指定想要如何安排任务，**Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。**Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 62-2 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　从 **Device** 下拉列表，选择 防御中心 的名称。

步骤 7　在 **Update Items** 部分，选择 **Vulnerability Database**。

步骤 8　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 9　或者，在 **Email Status To:** 字段中，键入任务状态消息要发送到的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 10　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动更新 URL 过滤

许可证：URL 过滤

受支持的防御中心：除 DC500 外的所有型号

可使用调度程序，自动从综合安全智能云更新 URL 过滤数据。要成功完成 URL 过滤更新任务：

- 防御中心必须能够访问互联网，否则无法连接云。
- 必须启用 URL 过滤，如第 64-25 页上的启用云通信中所述。

请注意，启用 URL 过滤时，也可启用自动更新。这会强制防御中心每 30 分钟连接一次云，获取 URL 过滤数据更新。如已启用自动更新，则不应创建预定任务以更新 URL 过滤数据。

虽然每日更新通常是小量更新，但是，如果距离上一次更新超过五天，新的 URL 过滤数据最多可能需要 20 分钟才能下载完（具体取决于带宽）。然后，执行更新也可能最多需要 30 分钟。

要自动运行 URL 过滤数据任务，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表，选择 **Update URL Filtering Database**。

页面重新加载，显示 URL 过滤更新选项。

步骤 4　指定想要如何安排更新， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 62-2 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 7　或者，在 **Email Status To** 字段中，键入任务状态消息要发送到的邮件地址 （或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 8　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

查看任务

许可证：任何环境

添加预定任务后，即可查看这些任务，评估它们的状态。在页面的 View Options 部分，查使用日历和预定任务列表查看预定任务。

有关详细信息，请参阅：

- 第 62-17 页上的使用日历
- 第 62-18 页上的使用任务列表

使用日历

许可证：任何环境

Calendar 视图选项可用于查看哪些预定任务在哪天发生。

要使用日历查看预定任务，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　可使用日历视图执行以下任务：

- 点击左向双箭头图标 (<<)，向后移动一年：
- 点击左向单箭头图标 (<)，向后移动一个月。
- 点击右向单箭头图标 (>)，向前移动一个月。
- 点击右向双箭头图标 (>>)，向前移动一年。
- 点击 **Today**，返回当前月份和年份。
- 点击 **Add Task**，安排新任务。
- 点击一个日期，在日历下方的任务列表中查看所有预定任务的特定日期。
- 点击在某个日期发生的特定任务，在日历下方的任务列表中查看此任务。

注　有关使用任务列表的详细信息，请参阅使用任务列表。

使用任务列表

许可证：任何环境

Task List 显示一列任务及其状态。打开日历时，任务列表出现在日历下方。此外，从日历中选择日期或任务，也可访问列任务列表。有关详情，请参见第 62-17 页上的使用日历。

表 62-1　任务列表列

列	说明
字段名称	显示预定任务的名称及与其关联的注释。
类型	显示预定任务的类型。
开始时间	显示预定任务的开始日期和时间。
频率	显示任务的运行频率。
状态	描述预定任务的当前状态。 • 对号图标 ( ) 指明任务已成功运行。 • 问号图标 ( ) 指明任务处于未知状态。 • 感叹号图标 ( ) 指明任务已失败。
创建者	显示创建预定任务的用户的名称。
编辑	编辑预定任务。
删除	删除预定任务。

编辑预定任务

许可证：任何环境

可编辑先前创建的预定任务。如果想要测试一次预定任务，确保参数正确，此功能特别有用。稍后，任务成功完成后，即可将其更改为周期性任务。

要编辑现有预定任务，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击要编辑的任务，或者任务出现的日期。

系统将显示 Task Details 表，其中包含选定的一项或多项任务。

步骤 3　在表中找到要编辑的任务，点击编辑图标 ( )

系统将显示 Edit Task 页面，其中显示选定任务的详细信息。

步骤 4　根据自己的需求编辑任务，包括开始时间、作业名称、注释以及任务运行频率，一次或反复。不能更改作业类型。

剩余选项取决于正在编辑的任务。有关详细信息，请参阅：

- 第 62-3 页上的自动运行备份作业
- 第 62-4 页上的自动执行证书撤销列表下载
- 第 62-5 页上的自动运行 Nmap 扫描
- 第 62-7 页上的自动化生成报表
- 第 62-9 页上的自动 FireSIGHT 生成建议
- 第 62-10 页上的自动执行软件更新
- 第 62-14 页上的自动更新漏洞数据库
- 第 62-16 页上的自动更新 URL 过滤

步骤 5　点击 **Save**，保存编辑。

更改保存成功，再次显示 Scheduling 页面。

删除预定任务

许可证：任何环境

可从 Schedule View 页面执行两类删除。可删除尚未运行的特定一次性任务，也可删除周期性任务的每个实例。如果删除周期性任务的一个实例，该任务的所有实例均将删除。如果删除预定运行一次的任务，则仅删除该任务。

以下各节描述如何删除任务：

- 要删除任务的所有实例，请参阅第 62-20 页上的删除周期性任务。
- 要删除任务的单个实例，请参阅第 62-20 页上的删除一次性任务。

删除周期性任务

许可证：任何环境

删除周期性任务的一个实例时，将自动删除该任务的所有实例。

要删除周期性任务，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　在日历上，选择要删除的周期性任务的实例。

页面重新加载，在日历下方显示任务表。

步骤 3　在表中找到要删除的周期性任务的实例，点击删除图标 ( )。

该周期性任务的所有实例均将删除。

删除一次性任务

许可证：任何环境

可使用任务列表删除预定的一次性任务，或删除以前运行过的预定任务的记录。

要删除单项任务，或者如果其已运行，请删除任务记录：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击要删除的任务或者任务出现的日期。

系统将显示一个表，其中包含选定的一项或多项任务。

步骤 3　在表中找到要删除的任务，点击删除图标 ( )。

选定任务的实例删除成功。

管理系统策略

系统策略允许您在自己的FireSIGHT 系统设备上管理以下内容：

- 访问控制首选项
- 设备访问列表
- 审核日志设置
- 外部身份验证
- 控制面板设置
- 数据库事件限制
- DNS 缓存属性
- 邮件中继主机和通知地址
- 跟踪入侵和网络分析策略更改
- 指定其他语言
- 自定义登录横幅
- SNMP 轮询设置
- 同步时间
- STIG 合规性
- 从防御中心提供时间
- 用户界面和命令行界面超时设置
- 映射服务器的漏洞

可以使用系统策略来控制防御中心中那些可能类似于部署中其他设备的方面。例如，贵组织的安全策略可能会要求当用户登录时，设备应该显示“No Unauthorized Use”消息。借助系统策略，可以在防御中心的系统策略中一次性设置登录横幅，然后将该策略应用于它所管理的所有设备。

在防御中心上设置多个系统策略也有好处。例如，如果您有用于不同环境下的不同的邮件中继主机，或者您要测试不同的数据库限制，则可以创建多个系统策略并在它们之间切换，而非编辑单个策略。

系统策略和系统设置有着显著不同，前者用于控制设备的若干方面 （这些方面在整个部署中可能是相似的），后者很可能仅针对单个设备。有关详细信息，请参阅第 64-1 页上的配置设备设置。

有关详细信息，请参阅：

- 第 63-2 页上的创建系统策略
- 第 63-3 页上的编辑系统策略
- 第 63-4 页上的应用系统策略

创建系统策略

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

创建系统策略时，可以为其指定名称和说明。然后，可以配置策略的各个方面，每个方面都在其各自的部分中进行了描述。

可不必创建新策略，而是从其他设备导出系统策略，再将该策略导入到您的设备。在应用导入的策略前，您可以进行编辑以满足需求。有关详细信息，请参阅第 A-1 页上的导入和导出配置。

要创建系统策略，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

Policy Name 列包含系统策略描述。 **Applied To** 列指明应用了策略的设备的数量，还指明之前应用的策略已更改且应重新应用策略的**过期**设备的数量。

步骤 2　点击 **Create Policy**。

系统将显示 Create Policy 页面。

步骤 3　从下拉列表中，选择现有策略作为新系统策略的模板。

步骤 4　在 **New Policy Name** 字段中，输入新策略的名称。

步骤 5　在 **New Policy Description** 字段中，输入对新策略的描述。

步骤 6　点击 **Create**。

即会保存系统策略并显示 Edit System Policy 页面。有关配置系统策略各方面的详细信息，请参阅：

- 第 63-22 页上的启用 STIG 合规性
- 第 63-24 页上的同步时间
- 第 63-25 页上的从防御中心提供时间
- 第 63-26 页上的配置用户界面设置
- 第 63-27 页上的映射服务器的漏洞

编辑系统策略

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

可以编辑现有的系统策略。如果编辑的系统策略当前已应用于某一设备，请在保存更改后重新应用该策略。有关详细信息，请参阅第 63-4 页上的应用系统策略。

要编辑现有的系统策略，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面，其中包含现有系统策略的列表。

步骤 2　点击要编辑的系统策略旁边的编辑图标 ( )。

系统将显示 Edit Policy 页面。可以更改策略名称和策略描述。有关配置系统策略各方面的详细信息，请参阅：

- 第 63-7 页上的配置访问控制策略首选项
- 第 63-8 页上的配置设备的访问列表
- 第 63-9 页上的配置审核日志
- 第 63-11 页上的启用外部身份验证
- 第 63-13 页上的配置控制面板设置
- 第 63-14 页上的配置控制面板事件限制
- 第 63-16 页上的配置 DNS 缓存属性
- 第 63-17 页上的配置邮件中继主机和通知地址
- 第 63-18 页上的配置网络分析策略首选项
- 第 63-19 页上的配置入侵策略首选项
- 第 63-20 页上的指定其他语言
- 第 63-20 页上的添加自定义登录横幅
- 第 63-21 页上的配置SNMP 轮询
- 第 63-24 页上的同步时间
- 第 63-25 页上的从防御中心提供时间
- 第 63-26 页上的配置用户界面设置
- 第 63-27 页上的映射服务器的漏洞

注　如果编辑的系统策略已应用于某一设备，请务必在完成编辑后重新应用更新后的策略。请参阅第 63-4 页上的应用系统策略。

步骤 3　点击 **Save Policy and Exit** 保存所做的更改。即会保存更改并显示 System Policy 页面。

应用系统策略

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

可以将系统策略应用于设备。对于已应用的系统策略，您做的所有更改只有在重新应用该策略后才会生效。

注　**不能**将系统策略应用于用于 Blue Coat X-系列的思科 NGIPS。

要应用系统策略，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　点击要应用的系统策略旁边的应用图标 ( )。

系统将显示 Apply 页面。

步骤 3　选择要应用系统策略的设备。

提示　可以按组、型号、运行状况或已应用的系统策略对设备进行排序。可以选择单个设备或整个组。

步骤 4　点击 **Apply**。

系统将显示 System Policy 页面。系统会显示一条消息，以指明系统策略的应用状态。

比较系统策略

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

可以比较两个系统策略，也可以比较同一个系统策略的两个版本，具体取决于可以访问的系统策略。这样，您可以审核策略更改，以符合贵组织的标准或优化系统性能。要将有效的系统策略与另一策略快速进行比较，您可以选择 **Running Configuration** 选项。或者，完成比较后，您可以生成 PDF 报告，以记录不同系统策略或同一系统策略不同版本之间的区别。

有两个工具可用于比较不同的系统策略或同一系统策略的不同版本：

- 比较视图以并排形式显示两个系统策略或同一系统策略的两个版本之间的区别。每个策略或策略版本的名称显示在比较视图左右两侧的标题栏中。

  您可以使用该工具在网络界面上查看和导航两个策略修订版，其中突出显示其差异。

- 比较报告记录了两个系统策略或同一系统策略的两个版本，其格式类似于系统策略报告，但文件格式为 PDF。

  可以使用此工具来保存、复制、打印和共享策略比较，供未来检查使用。

使用系统策略比较视图

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

比较视图以并排形式显示两个系统策略或策略版本，每个策略或策略版本的名称显示在比较视图左右两侧的标题栏中。对于所有版本，系统策略比较视图会在策略名称右侧显示上次修改时间和上一个用户。

两个系统策略或同一系统策略的两个版本的差异会突出显示：

- 蓝色表示两个策略或两个版本中此突出显示的设置不同。并且用红色文本注明其不同之处。
- 绿色表示突出显示的设置出现在一个策略或策略版本中，但未出现在另一个策略或策略版本中。

您可以执行下表中的任何操作。

表 63-1　　系统策略比较视图操作

要.....	**您可以.....**
逐一浏览更改	在标题栏上方选择 **Previous** 或 **Next**。 在左右两侧之间以双箭头图标 (◂▸) 为中心移动，**Difference** 数字调整为识别您正在查看哪个差异。
生成新的系统策略比较视图	选择 **New Comparison**。 系统将显示 **Select Comparison** 窗口。有关详细信息，请参阅使用系统策略比较报告。
生成系统策略比较报告	选择 **Comparison Report**。 系统策略比较报告是一个 PDF 文件，其中包含的信息与系统策略比较视图中的相同。

使用系统策略比较报告

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

系统策略比较报告记录系统策略比较视图中识别出的两个系统策略或同一系统策略的两个版本之间的差异，其文件格式为 PDF。可以使用此报告进一步分析两个系统策略配置之间的差异，以及保存并分享分析结果。

对于您能够访问的任何系统策略，都可以通过比较视图生成系统策略比较报告。只有在保存更改之后，对系统策略所做的更改才会出现在系统策略比较报告中。

系统策略比较报告可以包含一个或多个部分，具体取决于配置。每个分区使用相同的格式并提供相同级别的详细信息。请注意， Value A 和 Value B 列代表您在比较视图中配置的策略或策略修订版。

提示　您可以使用类似的操作步骤比较 SSL、网络分析、入侵、文件、访问控制、运行状况策略。

要比较两个系统策略或同一策略的两个版本，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　点击 **Compare Policies**。

系统将显示 Select Comparison 弹出窗口。

步骤 3　从 **Compare Against** 下拉列表中选择要进行比较的类型：

- 要比较两个不同的策略，请选择 **Other Policy**。
- 要比较同一策略的两个修订版，请选择 **Other Revision**。
- 要将其他策略与当前的有效策略进行比较，请选择 **Running Configuration**。

步骤 4　根据您选择的比较类型，有以下选项可供选择：

- 如果您比较两个不同的策略，请从 **Policy A** 和 **Policy B** 下拉列表中选择要比较的策略。
- 如果您比较同一策略的两个修订版，请从 **Policy** 下拉列表中选择该策略，然后从 **Revision A** 和 **Revision B** 下拉列表中选择要比较的修订版。
- 如果要将当前应用的配置与另一策略进行比较，请从 **Target/Running Configuration A** 下拉列表中选择当前运行的配置，然后从 **Policy B** 下拉列表中选择另一策略。

步骤 5　点击 **OK** 显示系统策略比较视图。

系统将显示比较视图。

步骤 6　点击 **Comparison Report** 以生成系统策略比较报告。

系统将显示系统策略比较报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

删除系统策略

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

即使系统策略正在使用中，您也可以将其删除。使用中的策略将会一直使用下去，直至应用新的策略。不能删除默认系统策略。

要删除系统策略，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　点击要删除的系统策略旁边的删除图标 ( )。要删除策略，请点击 **OK**。

系统将显示 System Policy 页面。系统会显示弹出消息，确认策略已删除。

配置系统策略

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

可以配置多种系统策略设置。有关配置系统策略各方面的详细信息，请参阅：

- 第 63-7 页上的配置访问控制策略首选项
- 第 63-8 页上的配置设备的访问列表
- 第 63-9 页上的配置审核日志
- 第 63-11 页上的启用外部身份验证
- 第 63-13 页上的配置控制面板设置
- 第 63-14 页上的配置控制面板事件限制
- 第 63-16 页上的配置 DNS 缓存属性
- 第 63-17 页上的配置邮件中继主机和通知地址
- 第 63-18 页上的配置网络分析策略首选项
- 第 63-19 页上的配置入侵策略首选项
- 第 63-20 页上的指定其他语言
- 第 63-20 页上的添加自定义登录横幅
- 第 63-24 页上的同步时间
- 第 63-25 页上的从防御中心提供时间
- 第 63-26 页上的配置用户界面设置
- 第 63-27 页上的映射服务器的漏洞

配置访问控制策略首选项

许可证：保护

受支持的设备：任何防御中心，除了 X -系列

可以对系统进行配置，从而当用户添加或修改访问控制策略中的规则时，提示他们输入规则注释。这样做可以跟踪用户更改策略的原因。如果您针对访问控制规则的更改启用了注释功能，您可以将规则注释设置为可选或必填项。每次保存对规则所做的新更改时，系统都会提示用户输入注释。

当用户保存规则时，系统会将注释添加到规则的注释历史记录中。有关详细信息，请参阅第 14-11 页上的将注释添加到规则中。

要配置访问控制策略规则的注释设置，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的访问控制策略设置，请点击系统策略旁边的编辑图标 ( )。
- 要将访问控制策略设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **Access Control Preferences**。

系统将显示 Access Control Preferences 页面。

步骤 4　您有以下选项：

- 从下拉列表中选择 **Disabled**，以允许用户添加或修改访问控制策略的规则，而无需输入注释。
- 从下拉列表中选择 **Optional**，以在用户保存访问控制策略的更改时显示 Description of Changes (Optional) 窗口。这让用户可以根据需要在注释中描述更改。
- 从下拉列表中选择 **Required**，以在用户保存访问控制策略的更改时显示 Description of Changes (Required) 窗口。这要求用户在保存更改前，必须在注释中对更改进行描述。

步骤 5　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

配置设备的访问列表

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

Access List 页允许您控制哪些计算机可在特定端口上访问您的设备。默认情况下，用于访问网络接口的 443 端口 （超文本传输安全协议或 HTTPS）和用于访问命令行的 22 端口 （安全外壳或 SSH）面向所有 IP 地址启用。也可以添加 161 端口上的 SNMP 访问权限。请注意，对于您计划用于轮询 SNMP 信息的所有计算机，都必须为其添加 SNMP 访问权限。

注意事项　默认情况下，对设备的访问**不**受限制。要在更安全的环境中使用设备，请考虑为特定的 IP 地址添加对设备的访问权限，然后删除默认的 `any` 选项。

访问列表是系统策略的一部分。可以通过创建新的系统策略或编辑现有的系统策略来指定访问列表。无论采用何种方式，访问列表仅在您应用系统策略后才会生效。

请注意，访问列表不会同时控制外部数据库的访问权限。有关外部数据库访问列表的详细信息，请参阅第 64-6 页上的启用数据库访问。

要配置访问列表，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的访问列表，请点击系统策略旁边的编辑图标 ( )。
- 要将访问列表配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　或者，要删除某一当前设置，请点击删除图标 ( )。

即会删除设置。

注意事项　对于您目前用来连接到设备接口的 IP 地址，如果您删除了它的访问权限，而且无“`IP=any port=443`”这一条目，那么当您应用该策略时，您将失去对系统的访问权限。

步骤 4　或者，要添加对一个或多个 IP 地址的访问权限，请点击 **Add Rules**。

系统将显示 Add IP Address 页面。

步骤 5　在 **IP Address** 字段中，可根据要添加的 IP 地址从以下选项中进行选择：

- 精确的 IP 地址 （例如，`192.168.1.101`）
- 使用 CIDR 表示法的 IP 地址块 （例如，`192.168.1.1/24`）

  有关在 FireSIGHT 系统中使用 CIDR 的信息，请参阅第 1-16 页上的 IP 地址约定。
- `any`，指定任意 IP 地址

步骤 6　选择 **SSH**、 **HTTPS**、 **SNMP** 或它们的组合，以指定要为这些 IP 地址启用哪些端口。

步骤 7　点击 **Add**。

系统再次显示 Access List 页面，其中反映出您所做的更改。

步骤 8　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

配置审核日志

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

可以配置系统策略，以使设备将审核日志发送到外部主机。

注　必须确保外部主机可正常工作，且可以通过发送审核日志的设备进行访问。

发送主机的名称是发送的信息的一部分。可以使用工具、严重性级别和可选标记来进一步识别审核日志数据流。设备会在您应用系统策略之后发送审核日志。

应用启用了此功能的策略且目标主机已配置为接收审核日志之后，系统日志才会发送出去。以下是输出结构的示例：

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

其中，本地日期、时间和主机名称位于括号内的可选标记之前，发送设备名称在审核日志消息之前。

例如：

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3000: admin@10.1.1.2, Operations > Monitoring, Page View
```

要配置审核日志设置，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的审核日志设置，请点击系统策略旁边的编辑图标 ( )。
- 要将审核日志设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **Audit Log Settings**。

系统将显示 Audit Log Settings 页面。

步骤 4　从 **Send Audit Log to Syslog** 下拉菜单中选择 **Enabled**。（默认设置为 **Disabled**。）

步骤 5　在 **Host** 字段中，使用 IP 地址或完全限定的主机名称指定审核信息的目标主机。默认端口 (514) 已被使用。

注意事项　对于您配置用于接收审核日志的计算机，如果未将其设置为可接收远程消息，主机将不会接受审核日志。

步骤 6　从 **Facility** 字段中选择系统日志工具。

步骤 7　从 **Severity** 字段中选择严重性级别。

步骤 8　或者，在 **Tag （可选）**字段中插入参考标记。

步骤 9　要将常规审核日志发送到外部 HTTP 服务器，请从 **Send Audit Log to HTTP Server** 下拉列表中选择 **Enabled**。默认设置为 **Disabled**。

步骤 10　在 **URL to Post Audit** 字段中，指定要用于发送审核信息的 URL。必须输入与将会监听下列 HTTP POST 变量的监听程序相对应的 URL：

- `subsystem`
- `actor`
- `event_type`
- `讯息`
- `action_source_ip`
- `action_destination_ip`

- 第一
- 时间
- tag （如果已如上所述进行了定义）

注意事项 要允许发送加密的信息，您必须使用 HTTPS URL。请注意，将审核信息发送到外部 URL 可能会影响系统性能。

步骤 11 点击 **Save Policy and Exit**。

系统策略更新成功。只有在将系统策略应用于防御中心及其管理的设备后，所做的更改才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

启用外部身份验证

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

通常，当用户登录设备时，设备会将用户凭证与设备的本地数据库中存储的用户帐户进行比较，以验证用户凭证。但是，如果您创建引用了外部身份验证服务器的身份验证对象，则可在系统策略中启用外部身份验证，以使登录到防御中心或受管设备的用户对该服务器进行身份验证，而非使用本地数据库。

将启用了外部身份验证的系统策略应用于某设备时，该设备会参照 LDAP 或 RADIUS 服务器上的用户来验证用户凭证。此外，如果用户启用了本地的内部身份验证，而且用户凭证未在内部数据库中找到，则设备将会检查外部服务器以寻找一组匹配的凭证。如果用户在多个系统上有相同的用户名，则其所有密码在所有服务器上都可使用。但请注意，如果在可用的外部身份验证服务器上进行身份验证时失败，设备不会将验证方式恢复为检查本地数据库。

启用外部身份验证时，对于采用外部身份验证的所有用户，都可为其设置默认的用户角色。您可以选择多个角色，但它们必须可以组合在一起。例如，如果启用外部身份验证以仅检索贵公司的“网络安全”组中的用户，则可将默认用户角色设置为包含安全分析师这一角色，以便用户可以访问收集到的事件数据，同时您无需进行任何额外的用户配置。但是，如果外部身份验证不仅检索该安全组，还检索其他人员的记录，则您可能希望不选择默认角色。有关可用用户角色的详细信息，请参阅第 61-3 页上的了解用户权限。

如果未选择访问角色，用户可以登录但无法访问任何功能。在用户尝试登录后，其帐户会在 User Management 页面上列出，您可在该页面上编辑帐户以授予额外的权限。有关修改用户角色的详细信息，请参阅第 61-50 页上的修改用户权限和选项。

提示 如果您将系统策略配置为使用一个用户角色且应用了该策略，后来又修改了策略以使用不同的默认用户角色并重新应用了策略，则在修改帐户或删除帐户并重新创建它们之前，在修改前创建的所有用户帐户都会保留第一个用户角色。

如果要指定可参照 LDAP 服务器成功进行身份验证以进行外壳访问的用户组，必须首先在 LDAP 身份验证对象中设置外壳访问属性及其他设置，然后才能在系统策略中启用外部身份验证。有关详细信息，请参阅第 61-17 页上的配置特定于 LDAP 的参数和第 61-8 页上的了解外壳访问。

如果要指定可参照 LDAP 服务器成功进行身份验证以进行 CAC 身份验证和授权的用户组，必须首先在 LDAP 身份验证对象中设置 UI 访问属性、用户名模板及其他设置，然后才能在系统策略中启用外部身份验证。有关详细信息，请参阅第 61-17 页上的配置特定于 LDAP 的参数和第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。

注　如果要在设备上同时启用外壳访问和 CAC 身份验证，**必须**分别创建身份验证对象并在系统策略中分别启用它们。

完成自定义身份验证对象后，必须在防御中心的某一系统策略中启用外部身份验证，然后将该策略推送到受管设备。将策略应用于某一设备后，符合条件的通过外部身份验证的用户可以登录到该设备。要更改外部身份验证设置，您必须修改防御中心上的系统策略，然后将该策略再次应用于设备。要在受管设备上禁用身份验证，您可以在防御中心上的系统策略中将其禁用并将该策略推送到该设备。

请注意，只能在物理和虚拟防御中心及受管设备上启用外部身份验证。在用于 Blue Coat X-系列的思科 NGIPS 上，不支持通过应用系统策略的方式启用外部身份验证。

如果采用内部身份验证的用户尝试登录，设备首先会检查该用户是否存在于本地用户数据库中。如果该用户存在，设备会参照本地数据库检查用户名和密码。如果找到匹配项，用户可成功登录。但是，如果登录失败且外部身份验证已启用，则设备会按照系统策略中显示的身份验证顺序，对照各个外部身份验证服务器来检查用户。如果用户名和密码与外部服务器中的结果相匹配，设备会将用户更改为带有针对该身份验证对象的默认权限的用户。

如果外部用户尝试登录，设备会参照外部身份验证服务器检查用户名和密码。如果找到匹配项，用户可成功登录。如果登录失败，则用户登录尝试会被拒绝。外部用户无法参照本地数据库中的用户列表进行身份验证。如果用户是新的外部用户，则本地数据库中会创建一个外部用户帐户，该帐户具有来自外部身份验证对象的默认权限。

要在外部服务器上为用户启用身份验证，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的外部身份验证设置，请点击系统策略旁的编辑图标 ( )。
- 要将外部身份验证设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **External Authentication**。

系统将显示 External Authentication 页面。

步骤 4　从 **Status** 下拉列表中，选择 **Enabled**。

步骤 5　从 **Default User Role** 下拉列表中，选择用户角色以确定要授予进行了外部身份验证的用户的默认权限。

提示　按住 Ctrl 键可同时选择多个默认角色。请注意，尽管可以同时选择“安全分析师”角色及其对应的“安全分析师 （只读）”角色，但只有“安全分析师”角色会得到应用。

步骤 6　如果还想用外部服务器对外壳访问帐户进行身份验证，请从 **Shell Authentication** 下拉列表中选择 **Enabled**。

步骤 7　如果要启用 CAC 身份验证和授权，请从 **CAC Authentication** 下拉列表中选择可用的 CAC 身份验证对象。

有关配置 CAC 身份验证和授权的完整步骤，请参阅第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。

步骤 8　要启用预配置的身份验证对象，请选择相应对象旁边的复选框。**必须**选择至少一个身份验证对象以启用外部身份验证。

提示　如果在第 6 步中启用了外壳身份验证，则**必须**选择某一被配置为允许外壳访问的身份验证对象。请注意，在同一系统策略中，**必须**使用不同的身份验证对象以管理外壳访问和 CAC 身份验证。有关详细信息，请参阅第 61-8 页上的了解外壳访问和第 61-9 页上的了解通过 CAC 进行 LDAP 身份验证。

步骤 9　或者，可以使用向上和向下箭头来更改出现身份验证请求时访问身份验证服务器的顺序。

注　请注意，外壳访问用户**只能**参照在配置文件中排在第一位的身份验证对象对服务器进行身份验证。

步骤 10　点击 **Save Policy and Exit**。

系统策略更新成功。只有在将系统策略应用于防御中心及其管理的设备后，所做的更改才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

配置控制面板设置

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

可以配置系统策略，以使控制面板上能启用 Custom Analysis 构件。控制面板通过使用构件提供当前系统状态的概要视图；构件是一些独立的小组件，可提供有关 FireSIGHT 系统的不同方面的信息。

借助 Custom Analysis 构件，可以根据设备数据库中事件的灵活、用户可配置的查询语句来直观地呈现这些事件。有关如何使用自定义构件的详细信息，请参阅第 55-10 页上的了解 Custom Analysis 构件。

要启用 Custom Analysis 构件，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的控制面板设置，请点击系统策略旁边的编辑图标 ( )。
- 要将控制面板设置配置为新系统策略的一部分，请点击 **Create Policy**。如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **Dashboard**。

系统将显示 Dashboard Settings 页面。

步骤 4　选择 **Enable Custom Analysis Widgets** 复选框，以允许用户将 Custom Analysis 构件添加到控制面板。清除此复选框可禁止用户使用这些构件。

步骤 5　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

配置控制面板事件限制

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

使用 Database 页面指定防御中心可存储的各类事件的最大数量。请注意，审核记录的设置也适用于受管设备。为提高性能，应将事件数量限制设置为您通常处理的事件数量。对于某些事件类型，可以禁用存储功能。下表列出了对于各种事件类型可以存储的最大和最小记录数量。

表 63-2　　数据库事件限制

事件类型	事件数上限	事件数下限
intrusion events	250 万 (DC500) 1000 万 （DC1000，虚拟防御中心） 2000 万 (DC750) 3000 万 (DC1500) 6000 万 (DC2000) 1 亿 (DC3000) 1.5 亿 (DC3500) 3 亿 (DC4000)	10,000
discovery events	1000 万 2000 万 （DC2000、 DC4000）	0 （禁用存储）
connection events Security Intelligence Events	1000 万 （DC500， DC1000，虚拟防御中心） 5000 万 (DC750) 1 亿 （DC1500、 DC3000） 3 亿 (DC2000) 500 万 (DC3500) 10 亿 (DC4000) 事件数上限由连接事件和安全情报事件分摊；为这两种事件配置的事件数总和不能超过上限。	0 （禁用存储）
connection summaries (aggregated connection events)	1000 万 （DC500， DC1000，虚拟防御中心） 5000 万 (DC750) 1 亿 （DC1500、 DC3000） 3 亿 (DC2000) 500 万 (DC3500) 10 亿 (DC4000)	0 （禁用存储）
correlation and compliance white list events	100 万 200 万 （DC2000、 DC4000）	一个
malware events	1000 万 2000 万 （DC2000、 DC4000）	10,000
file events	1000 万 2000 万 （DC2000、 DC4000）	0 （禁用存储）

表 63-2　　数据库事件限制 （续）

事件类型	事件数上限	事件数下限
health events	100 万	0 （禁用存储）
audit records	100,000	一个
remediation status events	1000 万	一个
the white list violation history of the hosts on your network	30 天的违例历史记录	1 天历史记录
user activity (user events)	1000 万	一个
user logins (user history)	1000 万	一个
rule update import log records	100 万	一个

如果入侵事件数据库中的事件数超过上限，最早的事件和数据包文件会被删除，直到数据库中事件的数量低于上限才会恢复。有关自动删除事件时自动生成邮件通知的信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

有关手动删除发现和用户数据库的信息，请参阅第 B-1 页上的从数据库清除发现数据。

此外，还可以配置邮件地址，以接收当系统从数据库中删除入侵事件和审核记录时发送的通知。

要配置数据库中记录的最大数量，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的数据库设置，请点击系统策略旁边的编辑图标 ( )。
- 要将数据库设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access Control Preferences 页面。

步骤 3　点击 **Database**。

系统将显示 Database 页面。

步骤 4　对于每个数据库，请输入要存储的记录的数量。

有关每个数据库可维护的记录的数量，请参阅数据库事件限制。

步骤 5　或者，在 **Data Pruning Notification Address** 字段中，输入用于接受通知的邮件地址，以接收当系统从数据库中删除入侵事件、发现事件、审核记录、安全情报数据或 URL 过滤数据时发送的通知。

请注意，还必须配置邮件服务器。有关详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 6　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

配置 DNS 缓存属性

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

如果在 Network 页面上配置了 DNS 服务器，可以在事件视图页面上将设备配置会自动解析 IP 地址。如果用户分配为管理员角色，您还可以为设备执行的 DNS 缓存配置基本属性。配置 DNS 缓存让您可以识别之前解析过的 IP 地址，而无需执行额外查找。这样，启用 IP 地址解析后，可以减少网络上的流量并加快事件页面的显示速度。

要配置 DNS 缓存属性，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的 DNS 缓存设置，请点击系统策略旁边的编辑图标 ( )。
- 要将 DNS 缓存设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **DNS 缓存**。

系统将显示 DNS Cache 页面。

步骤 4　从 **DNS Resolution Caching** 下拉列表中选择 **Enabled** 以启用缓存。选择 **Disabled** 可禁用缓存。

注　DNS 解析缓存是针对整个系统的设置，它允许对以前解析过的 DNS 查找进行缓存。要对每个用户帐户配置 IP 地址解析，用户还必须从 **User Preferences** 菜单中选择 **Event View Settings**，启用 **Resolve IP Addresses**，然后点击 **Save**。有关配置 DNS 服务器的信息，请参阅第 64-8 页上的配置管理接口。有关配置事件视图首选项的信息，请参阅第 71-3 页上的配置事件查看设置。

步骤 5　在 **DNS Cache Timeout (in minutes)** 字段中，输入 DNS 条目在内存中缓存的时间 （以分钟为单位）；超过该时间后，条目将因无活动而被删除。

默认设置为 300 分钟 （5 小时）。

步骤 6　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

注意事项　尽管已为设备启用了 DNS 缓存，但 IP 地址解析并非为每个具体的用户启用 - 除非已通过 User Preferences 菜单访问了 Events page 页面并在上面进行了配置。

配置邮件中继主机和通知地址

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

如果要执行以下操作，必须配置邮件主机：

- 通过邮件发送基于事件的报告
- 通过邮件发送有关已安排的任务的报告
- 通过邮件发送更改调节报告
- 通过邮件发送数据删除通知
- 通过邮件发送发现事件、影响标志和关联事件警报
- 通过邮件发送入侵事件警报
- 通过邮件发送运行状况事件警报

可以为设备和邮件中继主机之间的通信选择加密方法，并可根据需要为邮件服务器提供身份验证凭证。配置完设置后，可以测试设备与采用指定设置的邮件服务器之间的连接。

要配置邮件中继主机，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的邮件设置，请点击系统策略旁边的编辑图标 ( )。
- 要将邮件设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **Email Notification**。

系统将显示 Configure Email Notification 页面。

步骤 4　在 **Mail Relay Host** 字段中，键入要使用的邮件服务器的主机名或 IP 地址。

注　输入的邮件主机必须允许从设备进行访问。

步骤 5　在 **Port Number** 字段中，输入要在邮件服务器上使用的端口号。常用端口包括 25 （未采用加密时使用）、 465 （采用 SSLv3 时使用）和 587 （采用 TLS 时使用）。

步骤 6　要选择加密方法，有以下选项可供选择：

- 要对设备与使用传输层安全的邮件服务器之间的通信进行加密，请从 **Encryption Method** 下拉列表中选择 **TLS**。
- 要对设备与使用安全套接字层的邮件服务器之间的通信进行加密，请从 **Encryption Method** 下拉列表中选择 **SSLv3**。
- 要允许设备与邮件服务器之间进行未经加密的通信，请从 **Encryption Method** 下拉列表中选择 **None**。

请注意，设备和邮件服务器之间的加密通信不要求进行证书验证。

步骤 7　在 **From Address** 字段中，输入有效的邮件地址，以作为设备所发送的消息的源邮件地址。

步骤 8　或者，要在连接到邮件服务器时提供用户名和口令，请选择 **Use Authentication**。在 **Username** 名字段中输入用户名。在 **Password** 字段中输入密码。

步骤 9　要使用已配置的邮件服务器发送测试邮件，请点击 **Test Mail Server Settings**。

系统会在按钮旁边显示一条消息，以指明测试是否成功。

步骤 10　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

配置网络分析策略首选项

许可证：保护

受支持的设备：任何防御中心，除了 X -系列

可以将系统配置为会在用户修改网络分析策略时提示他们添加注释。这样做可以跟踪用户更改策略的原因。如果对网络分析策略更改启用了注释功能，则可将注释设置为可选或必填项。系统会将更改说明写入审核日志中。

您也可以将所有网络分析策略更改写入审核日志中。有关审核日志的详细信息，请参阅第 69-1 页上的管理审计记录。

要配置网络分析策略注释设置，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的网络分析策略首选项，请点击系统策略旁的编辑图标 ( )。
- 要将网络分析策略首选项配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **Network Analysis Policy Preferences**。

系统将显示 Network Analysis Policy Preferences 页面。

步骤 4　可以从 **Comments on policy change** 下拉列表中选择以下任一选项：

- 选择 **Disabled** 以允许用户修改网络分析策略，而无需输入更改说明。
- 选择 **Optional**，以在用户保存网络分析策略更改时显示 Description of Changes 窗口。这让用户可以根据需要在注释中描述更改。
- 选择 **Required**，以在用户保存网络分析策略更改时显示 Description of Changes 窗口。这要求用户在保存更改前，必须在注释中对更改进行描述。

步骤 5　或者，如果要将所有网络分析策略更改写入审核日志中，请选择 **Write changes in Network Analysis Policy to audit log**。

步骤 6　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

配置入侵策略首选项

许可证：保护

受支持的设备：任何防御中心，除了 X -系列

可以将系统配置为会在用户修改入侵策略时提示他们添加注释。这样做可以跟踪用户更改策略的原因。如果对入侵策略更改启用了注释功能，可以将注释设置为可选或必填项。系统会将更改说明写入审核日志中。

您也可以将所有入侵策略更改写入审核日志中。有关审核日志的详细信息，请参阅第 69-1 页上的管理审计记录。

要配置入侵政策注释设置，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的入侵策略首选项，请点击系统策略旁边的编辑图标 ()。
- 要将入侵策略首选项配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **Intrusion Policy Preferences**。

系统将显示 Intrusion Policy Preferences 页面。

步骤 4　可以从 **Comments on policy change** 下拉列表中选择以下任一选项：

- 选择 **Disabled** 以允许用户修改入侵策略，而无需输入更改说明。
- 选择 **Optional**，以在用户保存入侵策略更改时显示 Description of Changes 窗口。这让用户可以根据需要在注释中描述更改。
- 选择 **Required**，以在用户保存入侵策略更改时显示 Description of Changes 窗口。这要求用户在保存更改前，必须在注释中对更改进行描述。

步骤 5　或者，如果要将所有入侵策略更改写入审核日志中，请选择 **Write changes in Intrusion Policy to audit log**。

步骤 6　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

指定其他语言

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

可以使用 Language 页面为网络界面指定不同的语言。

注意事项　在该页面上选择的语言将用于每个用户登录到设备时所用的网络界面。

要为用户界面选择不同的语言，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的语言设置，请点击系统策略旁边的编辑图标 ( )。
- 要将语言设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **Language**。

系统将显示 Language 页面。

步骤 4　选择要使用的语言。

步骤 5　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

添加自定义登录横幅

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

可以创建自定义登录横幅，当用户使用 SSH 登录设备时，该横幅会在网络界面的登录页面上显示。横幅可以包含除小于号 (<) 和大于号 (>) 以外的任何可打印字符。

要添加自定义横幅，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的登录横幅，请点击系统策略旁边的编辑图标 ( )。

- 要将登录横幅配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **Login Banner**。

系统将显示 Login Banner 页面。

步骤 4　在 **Custom Login Banner** 字段中，输入要与此系统策略一同使用的登录横幅。

步骤 5　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

配置SNMP 轮询

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

对于使用此系统策略的设备，可以启用简单网络管理协议 (SNMP) 轮询功能。 SNMP 功能支持使用 SNMP 协议第 1 版、第 2 版和第 3 版。

此功能允许访问：

- 设备的标准管理信息库 (MIB)，包括联系人、管理、位置、服务信息、 IP 寻址和路由信息以及传输协议使用统计信息等系统详细信息。
- 受管设备的其他 MIB，包括通过物理接口、逻辑接口、虚拟接口、 ARP、 NDP、虚拟网桥和虚拟路由器的流量的统计信息。

请注意，启用系统策略 SNMP 功能不会导致设备发送 SNMP 陷阱；这样做只会使 MIB 中的信息可供网络管理系统轮询。

注　对于要用于轮询设备的任何计算机，都必须为其添加 SNMP 访问权限。有关详细信息，请参阅第 63-8 页上的配置设备的访问列表。请注意， SNMP MIB 包含可用于攻击设备的信息。思科建议您将 SNMP 访问权限的访问列表限制为将被用于轮询 MIB 的特定主机。思科还建议您针对网络管理访问权限使用 SNMPv3 和强密码。

要配置 SNMP 轮询，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的 SNMP 轮询设置，请点击系统策略旁边的编辑图标 ( )。
- 要将 SNMP 轮询设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Create**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　对于要用于轮询设备的各台计算机，如果还没有为其添加 SNMP 访问权限，请立即添加。有关详细信息，请参阅第 63-8 页上的配置设备的访问列表。

步骤 4　点击 **SNMP**。

系统将显示 SNMP 页面。

步骤 5　从 **SNMP** 下拉列表中，选择要使用的 SNMP 版本。

所选的版本显示在下拉列表中。

步骤 6　您有以下选项：

- 如果选择了 **Version1** 或 **Version 2**，请在 **Community String** 字段中键入 SNMP 团体名称。转至第 15 步。
- 如果选择了 **Version 3**，请点击 **Add User** 显示用户定义页面。

步骤 7　在 **Username** 名字段中输入用户名。

步骤 8　从 **Authentication Protocol** 下拉列表中选择要用于身份验证的协议。

步骤 9　在 **Authentication Password** 字段中键入使用 SNMP 服务器进行身份验证时所需的密码。

步骤 10　在 **Verify Password** 字段 （位于 **Authentication Password** 字段下方）中重新键入身份验证密码。

步骤 11　从 **Privacy Protocol** 列表中，选择要使用的隐私协议；或选择 **None** 以不使用隐私协议。

步骤 12　在 **Privacy Password** 字段中，输入 SNMP 服务器要求的 SNMP 隐私密钥。

步骤 13　在 **Verify Password** 字段 （位于 **Privacy Password** 字段下方）中重新键入隐私密码。

步骤 14　点击 **Add**。

用户添加成功。可以重复步骤 613 以添加其他用户。点击删除图标 ( ) 可删除用户。

步骤 15　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

启用 STIG 合规性

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

美国联邦政府内部的组织有时需要遵守 《安全技术实施指南》 (STIG) 中规定的一系列安全检查要求。 STIG Compliance 选项会启用一些设置，这些设置旨在为遵守美国国防部规定的特定要求提供支持。

如果在部署中的任一设备上启用了 STIG 合规性，则必须在所有设备上都将其启用。不符合 STIG 规定的受管设备无法注册到符合 STIG 规定的防御中心，同样，符合 STIG 规定的设备无法注册到不合规的防御中心。

启用 STIG 合规性不能保证严格遵守所有适用的 STIG 规定。有关针对此版本产品使用此模式时的 FireSIGHT 系统 STIG 合规性详细信息，请与支持人员联系以获取 FireSIGHT 系统 5.4.1 版的 STIG 版本说明。

启用 STIG 合规性时，本地外壳访问帐户的密码复杂性和保留规则会发生更改。有关这些设置的详细信息，请参阅 FireSIGHT 系统 5.4.1 版的 STIG 版本说明。此外，在 STIG 合规性模式下，无法使用 SSH 远程存储。

请注意，应用启用了 STIG 合规性的系统策略会强制设备重新启动。如果某设备已启用了STIG，当您将启用了 STIG 的系统策略应用于该设备时，该设备不会重新启动。如果某设备已禁用了 STIG，当您将启用了 STIG 的系统策略应用于该设备时， STIG 将保持启用状态，且该设备不会重新启动。

对于从版本 5.2.0 之前的版本进行升级的设备，在应用启用了合规性的策略时，会同时生成合规性证书；因此，需要重新注册已注册的受管设备或对等设备。

注意事项　需在支持人员的协助下才能禁用此设置。此外，此设置可能会显著影响系统性能。思科除为了满足美国国防部的安全要求外，不建议启用 STIG 合规性。

要启用 STIG 合规性，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的时间设置，请点击系统策略旁边的编辑图标 ( )。
- 要将时间设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **STIG Compliance**。

系统将显示 STIG Compliance 页面。

步骤 4　如果要*永久地*在设备上启用 STIG 合规性，请选择 **Enable STIG Compliance**。

注意事项　在应用启用了 STIG 合规性的策略之后，将无法在设备上禁用 STIG 合规性。要禁用合规性，请与支持人员联系。

步骤 5　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

请注意，将启用 STIG 合规性的系统策略应用于某设备时，该设备会重新启动。另请注意，如果某设备已启用了STIG，当您将启用了 STIG 的系统策略应用于该设备时，该设备不会重新启动。

另外，如果设备是从版本 5.2.0 之前的版本进行升级的，在启用 STIG 合规性后，需要重新注册设备。

同步时间

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

可以使用 Time Synchronization 页面管理设备上的时间同步。可通过以下方式之一来同步时间：

- 手动
- 使用一个或多个 NTP 服务器 （其中一个可以是防御中心）

时间设置是系统策略的一部分。可以通过创建新的系统策略或编辑现有策略来指定时间设置。无论执行哪一种操作，时间设置都只在您应用系统策略后才会生效。

请注意，在设备的大多数页面上，时间设置是以您在 Time Zone 页面 （默认为美国/纽约时区）上设置的本地时间显示的，但在设备自身上存储时用的是 UTC 时间。此外，当前时间以 UTC 显示在 Time Synchronization 页面的顶部（本地时间显示在 Manual 时钟设置选项中，如果此选项已启用）。

必须使用本地应用 （例如，命令行界面或操作系统界面）来管理用于 Blue Coat X-系列的思科 NGIPS 的时间设置。从同一物理设备或 NTP 服务器同步用于 Blue Coat X-系列的思科 NGIPS 及其管理防御中心的时间。有关详细信息，请参阅 《*思科 X 系列专用软件安装指南*》。

可以使用外部时间服务器来同步设备。如果指定远程 NTP 服务器，则设备必须可通过网络访问该服务器。请勿指定不受信任的 NTP 服务器。与 NTP 服务器之间的连接不使用已配置的代理设置。要将防御中心作为 NTP 服务器，请参阅第 63-25 页上的从防御中心提供时间。

思科建议您将虚拟设备同步到物理 NTP 服务器。请勿将受管设备 （虚拟或物理设备）同步到虚拟防御中心。

注　同步时间后，请确保防御中心和受管设备上的时间相匹配。否则，当受管设备与防御中心通信时，可能会发生意外的后果。

同步时间的步骤可能会略有差异，具体取决于是在防御中心上还是受管设备上使用网络界面。下面分别说明各个步骤。

要同步时间，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的时间设置，请点击系统策略旁边的编辑图标 ( )。
- 要将时间设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **Time Synchronization**。

系统将显示 Time Synchronization 页面。

步骤 4　要为受管设备提供防御中心的时间，请在 **Serve time via NTP** 下拉列表中选择 **Enabled**。

步骤 5　要指定防御中心上的时间同步方式，有以下选项可供选择：

- 要手动设置时间，请选择 **Manually in Local Configuration**。有关应用系统策略后设置时间的信息，请参阅第 64-12 页上的手动设置时间。
- 要通过 NTP 接收来自另一服务器的时间，请选择 **Via NTP from**，然后在文本框中键入要使用的 NTP 服务器的 IP 地址 （以逗号分隔）；或者，如果启用了 DNS，请键入完全限定的主机名和域名。

注意事项　如果设备已重新启动，并且 DHCP 服务器设置了不同于您在这里指定的记录的 NTP 服务器记录，则会使用 DHCP 提供的 NTP 服务器。为避免这种情况，请将 DHCP 服务器配置为会设置相同的 NTP 服务器。

步骤 6　要指定任何受管设备上的时间同步方式，有以下选项可供选择：

- 选择 **Manually in Local Configuration** 以手动设置时间。有关应用系统策略后设置时间的信息，请参阅第 64-12 页上的手动设置时间。
- 选择 **Via NTP from 防御中心**以通过 NTP 接收来自防御中心的时间。有关详细信息，请参阅第 63-25 页上的从防御中心提供时间。
- 选择 **Via NTP from** 以通过 NTP 接收来自不同服务器的时间。在文本框中键入 NTP 服务器的 IP 地址 （以逗号分隔）；或者，如果启用了 DNS，请键入完全限定的主机名和域名。

注　受管设备与已配置的 NTP 服务器进行同步可能需要几分钟时间。此外，如果要将受管设备与配置为 NTP 服务器的防御中心进行同步，且防御中心自身已配置为使用 NTP 服务器，则时间同步可能需要一些时间。这是因为，防御中心必须首先与其配置的 NTP 服务器同步，然后才能为受管设备提供时间。

步骤 7　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

从防御中心提供时间

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

可以将防御中心配置为使用 NTP 的时间服务器，然后用它来同步防御中心和受管设备之间的时间。

请注意，将防御中心使配置为使用 NTP 提供时间后，将无法手动设置时间。如果要手动更改时间，应在将防御中心配置为使用 NTP 提供时间**之前**进行。将防御中心配置为 NTP 服务器**之后**，如果要手动更改时间，请禁用 **Via NTP** 选项并点击 **Save**，手动更改时间并点击 **Save**，然后启用 **Via NTP** 并点击 **Save**。

注　如果将防御中心配置为使用 NTP 提供时间，然后又将其禁用，受管设备上的 NTP 服务仍会尝试与防御中心同步时间。必须从受管设备的网络界面上禁用 NTP 以阻止同步尝试。

要将防御中心配置为 NTP 服务器，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的 NTP 服务器设置，请点击系统策略旁边的编辑图标 ( )。
- 要将 NTP 服务器设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **Time Synchronization**。

系统将显示 Time Synchronization 页面。

步骤 4　从 **Serve Time via NTP** 下拉列表中，选择 **Enabled**。

步骤 5　在受管设备的 **Set My Clock** 选项中，选择 **Via NTP from 防御中心**。

步骤 6　点击 **Save Policy and Exit**。

系统策略更新成功。只有在将系统策略应用于防御中心及其管理的设备后，所做的更改才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

注　防御中心与其受管设备进行同步可能需要几分钟时间。

配置用户界面设置

许可证：任何环境

受支持的设备：任何防御中心，除了 X -系列

FireSIGHT 系统网络界面或命令行界面的自动登录会话可能意味着安全风险。可以配置用户的登录会话因无活动而超时之前允许经过的空闲时间，以分钟为单位。也可以为外壳 （命令行）会话设置类似的超时时间。

在部署中，可能有一些用户打算被动、安全、长时间地监控网络界面。可以通过某一用户配置选项来使用户免受网络界面会话超时的影响。（具有管理员角色的用户拥有对菜单选项的完整访问权限，如果这些访问权限受损会构成额外风险，因此他们不能获得会话超时豁免。）有关详细信息，请参阅第 61-44 页上的管理用户登录设置。

如果必须限制对系统的外壳访问，第三个选项允许您永久禁用命令行中的 `expert` 命令。在设备上禁用 expert 模式可阻止所有用户 （即使是有 Configuration 外壳访问权限的用户）进入外壳的专家模式。当用户在命令行中进入专家模式后，用户可以运行适用于外壳的任何 Linux 命令。不在专家模式时，命令行用户只能运行命令行界面提供的命令。请注意， 2 系列设备不支持命令行界面。

有关命令行界面命令的详细信息，请参阅第 D-1 页上的命令行参考。有关设置用户的命令行访问权限的信息，请参阅第 61-42 页上的管理命令行访问和第 D-1 页上的命令行参考 （适用于虚拟设备 CLI 用户管理）。

要配置用户界面设置，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的用户界面设置，请点击系统策略旁边的编辑图标 ( )。
- 要将用户界面设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **User Interface**。

系统将显示 User Interface 页面。

步骤 4　您有以下选项：

- 要配置网络界面的会话超时，请在 **Browser Session Timeout (Minutes)** 字段中输入超时时间 （分钟）。默认值为 `60`；最大值为 `1440` （24 小时）。

  有关如何使用户免受会话超时影响的信息，请参阅第 61-44 页上的管理用户登录设置。
- 要配置命令行界面的会话超时，请在 **Shell Timeout (Minutes)** 字段中输入超时时间 （分钟）。默认值为 `0`；最大值为 `1440` （24 小时）。
- 要在命令行界面中永久禁用 `expert` 命令，请选择 **Permanently Disable Expert Access** 复选框。

注意事项　在将禁用了专家模式的系统策略应用于某一设备后，将无法通过网络界面或命令行恢复访问专家模式功能。要恢复专家模式功能，必须联系支持人员。

步骤 5　点击 **Save Policy and Exit**。

系统策略更新成功。只有在将系统策略应用于防御中心及其管理的设备后，所做的更改才会生效。会话超时间隔的更改在进行下次登录会话时才会生效。

映射服务器的漏洞

许可证：保护

受支持的设备：任何防御中心，除了 X -系列

当服务器在发现事件数据库中拥有应用 ID 且数据包报头包含供应商和版本时，FireSIGHT 系统会针对从主机 IP 地址收到或发送的所有应用协议流量自动将漏洞映射到该地址。

但是，许多服务器不包含供应商和版本信息。对于系统策略中列出的服务器，可以将系统配置为是否针对供应商和无版本号的服务器将漏洞与服务器关联起来。

例如，在某一主机提供的 SMTP 流量中，其报头不含供应商或版本号。如果在系统策略的 Vulnerability Mapping 页面上启用 SMTP 服务器，然后将该策略应用于管理流量检测器的防御中心上，那么，所有与 SMTP 服务器相关联的漏洞都将被添加到该主机的主机配置文件。

尽管检测器会收集服务器信息并将其添加到主机配置文件中，但应用协议检测器不会被用于进行漏洞映射，这是因为您无法为自定义的应用协议检测器指定供应商或版本，同时无法在系统策略中为漏洞映射选择服务器。

要配置服务器的漏洞映射，请执行以下操作：

访问：管理员

步骤 1　选择 **System > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的漏洞映射设置，请点击系统策略旁边的编辑图标 ( )。
- 要将漏洞映射设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 63-2 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　点击 **Vulnerability Mapping**。

系统将显示 Vulnerability Mapping 页面。

步骤 4　您有以下选项：

- 要阻止服务器的漏洞被映射到接收不含供应商或版本信息的应用协议流量的主机上，请为相应服务器清除此复选框。
- 要使服务器的漏洞映射到接收不含供应商或版本信息的应用协议流量的主机上，请为相应服务器选择此复选框。

提示　可以使用 **Enabled** 旁边的复选框一次性选择或清除所有复选框。

步骤 5　点击 **Save Policy and Exit**。

系统策略更新成功。只有在将系统策略应用于防御中心及其管理的设备后，所做的更改才会生效。有关详细信息，请参阅第 63-4 页上的应用系统策略。

配置设备设置

FireSIGHT 系统设备的*本地配置* (**System > Local > Configuration**) 是一组可能特定于单一设备的设置。与本地配置相比，系统策略 （第 63-1 页上的管理系统策略）控制在整个部署中可能类似的设备设置。

下表汇总了设备的本地配置。

表 64-1 本地配置选项

选项	说明	有关详细信息，请参阅.....
信息	您可以查看有关设备的当前信息。您也可以更改设备名称。	第 64-2 页上的查看和修改设备信息
HTTPS 证书	在需要时，允许您从可信机构请求 HTTPS 服务器证书，然后将证书上传到您的设备。	第 64-3 页上的使用自定义 HTTPS 证书
数据库	让您能够启用对设备数据库的外部只读访问权限，并为您提供客户端驱动程序供下载。	第 64-6 页上的启用数据库访问
管理接口	使您能够更改选项 （例如，在安装时初始设置的设备 IP 地址、主机名和代理设置）。还可以查看和修改设备管理接口的设置。	第 64-8 页上的配置管理接口
流程	允许您关闭或重新启动设备，然后重新开始与 FireSIGHT 系统相关的流程。	**受支持的设备：**
时间	显示当前时间。如果设备的当前系统策略中的时间同步设置设置为 **Manually in Local Configuration**，则可以使用此页面更改时间。	第 64-12 页上的手动设置时间
Remote Storage Device	在防御中心上，允许您配置用于备份和报告的远程存储。	第 64-14 页上的管理远程存储
Change Reconciliation	允许您通过邮件接收有关过去 24 小时内出现的系统变化的详细报告。	第 64-18 页上的了解更改调节
Console Configuration	允许您配置控制台通过 VGA 端口、串行端口或无人值守管理 (LOM) 访问 FireSIGHT 系统设备，从而让您可以在远离设备的情况下执行有限的监控和管理任务。	第 64-19 页上的管理远程控制台访问
云服务	在防御中心上，允许您从综合安全智能云下载 URL 过滤数据，执行未归类 URL 查找，以及向思科发送有关所检测到文件的诊断信息。	第 64-25 页上的启用云通信
VMware 工具	在虚拟防御中心上，允许您启用和使用 VMware 工具。	第 64-27 页上的启用 VMware 工具

查看和修改设备信息

许可证：任何环境

Information 页面提供有关设备的信息。信息包括只读信息，例如产品名称和型号、操作系统和版本以及当前设备级策略。该页面还提供了更改设备名称的选项。

下表介绍了每个字段。

表 64-2　　设备信息

字段	说明
字段名称	您为设备指定的名称。请注意，此名称仅在 FireSIGHT 系统环境中使用。尽管您可以使用主机名作为设备的名称，但在此字段中输入其他名称不会更改主机名。
产品型号	设备的型号名称。
软件版本	当前安装的软件版本。
序列号	设备的机箱序列号。
Store Events Only on 防御中心	如果要在防御中心上存储事件数据，但不在受管设备上存储，请选择此复选框。如果要在两个设备上都存储事件数据，请清除此复选框。
Prohibit Packet Transfer to the 防御中心	选择受管设备上的此复选框可阻止受管设备发送有关事件的数据包。清除此复选框即允许在防御中心上存储有关事件的数据包。
操作系统	当前在设备上运行的操作系统。
Operating System Version	当前设备上运行的操作系统的版本。
IPv4 Address	设备默认 (`eth0`) 管理接口的 IPv4 地址。如果设备的 IPv4 管理处于禁用状态，此字段会予以指出。
IPv6 Address	设备默认 (`eth0`) 管理接口的 IPv6 地址。如果设备的 IPv6 管理处于禁用状态，此字段会予以指出。
Current Policies	当前应用的设备级策略。如果策略自上一次应用以来已更新，则策略的名称以斜体显示。
型号编号	设备的型号。此编号可能对于故障排除非常重要。

要修改设备信息，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　要更改设备名称，请在 **Name** 字段中键入新的名称。

名称**必须**是字母数字字符，并且不能仅包含数字字符。

步骤 3　要保存更改，请点击 **Save**。

页面刷新，您所做的更改被保存。

使用自定义 HTTPS 证书

许可证：任何环境

思科防御中心和支持基于网络的用户界面的受管设备包括默认 SSL （安全套接字层）证书，可以使用该证书建立网络浏览器与设备之间的加密通信通道。但是，因为设备的默认证书并非由受到任何全球知名的证书颁发机构 (CA) 信任的 CA 颁发，所以您可以用全球知名的或内部受信任的 CA 签署的自定义证书来代替默认证书。

可以通过设备的本地配置管理证书。有关详情，请参阅：

- 第 64-3 页上的查看当前 HTTPS 服务器证书
- 第 64-4 页上的生成服务器证书签名请求
- 第 64-5 页上的上传服务器证书
- 第 64-5 页上的要求用户证书

查看当前 HTTPS 服务器证书

许可证：任何环境

可以查看设备当前使用的服务器证书的详细信息。该证书提供以下信息：

表 64-3　　HTTPS 服务器证书信息

字段	说明
标的	对于安装证书的设备，提供 commonName、 countryName、organizationName 和 organizationalUnitName。
Issuer	对于签发证书的设备，提供 commonName、 countryName、organizationName 和 organizationalUnitName。
有效性	指明证书有效的时间段。
版本	指明证书版本。
序列号	指明证书序列号。
Signature Algorithm	指明用于签署证书的算法。

要查看证书详细信息，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **HTTPS Certificate**。

系统将显示 HTTPS Certificate 页面，其中提供设备当前证书的详细信息。

生成服务器证书签名请求

许可证：任何环境

可以根据设备信息和您提供的识别信息生成证书请求。可将生成的请求发送至证书颁发机构以请求服务器证书。如果安装有受浏览器信任的内部证书颁发机构 (CA)，那么还可以使用生成的请求对证书进行自签。生成的密钥采用 Base-64 编码 PEM 格式。

请注意，当通过本地配置 HTTPS Certificate 页面生成证书请求时，仅可为单一服务器生成证书。必须准确键入服务器的完全限定域名，因为它将出现在 **Common Name** 字段的证书中。如果公用名称与 DNS 主机名不匹配，那么当连接至设备时，您将接收到警告。同样，如果安装了并非由全球知名的或内部受信任的 CA 签署的证书，那么当连接至设备时，您将接收到安全警告。

要生成证书请求，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **HTTPS Certificate**。

系统将显示 HTTPS Certificate 页面。

步骤 3　点击 **Generate New CSR**。

将会弹出 Generate Certificate Signing Request 窗口。

步骤 4　在 **Country Name (two-letter code)** 字段中键入您所在国家/地区的双字母国家/地区代码。

步骤 5　在 **State or Province** 字段中键入您所在州或省的邮政缩写。

步骤 6　在 **Locality or City** 字段中键入您所在的地区或城市。

步骤 7　在 **Organization** 字段中键入您的组织名称。

步骤 8　在 **Organizational Unit (Department)** 字段中键入部门名称。

步骤 9　在 **Common Name** 字段中键入要为其申请证书的服务器的完全限定名称 （应与要在证书中显示的完全一致）。

步骤 10　点击 **Generate**。

将会弹出 Certificate Signing Request 窗口。

步骤 11　打开一个文本编辑器。

步骤 12　复制证书请求中的整个文本块 （包括 `BEGIN CERTIFICATE REQUEST` 和 `END CERTIFICATE REQUEST` 行），然后将其粘贴到一个空白文本文件中。

步骤 13　将该文件另存为 *`servername`*`.csr`，其中，*`servername`* 是您打算将证书用于其中的服务器的名称。

步骤 14　将该 CSR 文件上传至您想要向其请求证书的证书颁发机构，或者使用该 CSR 文件来创建自签证书。

上传服务器证书

许可证：任何环境

获得证书颁发机构 (CA) 的签名证书后，可以上传该证书。如果生成证书的签署机构要求您信任一个中间 CA，那么您还必须提供一个证书链（有时称为证书路径）。如果您需要用户证书，这些证书必须由其中间机构包括在证书链中的证书颁发机构生成。

要上传证书，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **HTTPS Certificate**。

系统将显示 HTTPS Certificate 页面。

步骤 3　点击 **Import HTTPS Certificate**。

将会弹出 Import HTTPS Certificate 窗口。

步骤 4　在文本编辑器中打开服务器证书，复制整个文本块（包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行），然后将其粘贴到 **Server Certificate** 字段中。

步骤 5　或者，打开私有密钥文件，复制整个文本块（包括 `BEGIN RSA PRIVATE KEY` 和 `END RSA PRIVATE KEY` 行），然后将其粘贴到 **Private Key** 字段中。

步骤 6　打开您需要提供的每一个中间证书，复制整个文本块，然后将其复制到 **Certificate Chain** 字段中。

步骤 7　点击 **Save** 上传证书。

此时将会上传证书，并更新 HTTPS Certificate 页面以反映新证书。

要求用户证书

许可证：任何环境

可使用客户端浏览器证书检查功能来限制对FireSIGHT 系统网络服务器的访问。启用用户证书时，网络服务器会检查用户的浏览器客户端是否选择了有效的用户证书。所选的用户证书必须由生成服务器证书的同一个可信证书颁发机构生成。如果用户在浏览器中选择的证书无效，或者并非由设备上证书链中的证书颁发机构生成，那么浏览器将无法加载网络界面。

您还可以加载服务器的证书撤销列表 (CRL)。 CRL 列出证书颁发机构已撤销的所有证书，以便网络服务器能够验证客户端浏览器证书是否已被撤销。如果用户选择在 CRL 中列为已撤销证书的证书，浏览器将无法加载网络界面。设备支持上传采用可区别编码规则 (DER) 格式的 CRL。对一台服务器只能上传一个 CRL。

要确保撤销证书列表是最新的，您可以创建计划任务来更新 CRL。界面中会列出 CRL 的最新更新。

请确保使用的是用于服务器证书的同一证书颁发机构，并且已上传证书的中间证书。有关详细信息，请参阅第 64-5 页上的上传服务器证书。

注　要启用用户证书以便访问网络界面，浏览器中**必须**存在有效的用户证书（或者您的读卡器中已插入 CAC）。

要请求提供有效用户证书，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **HTTPS Certificate**。

系统将显示 HTTPS Certificate 页面。

步骤 3　选择 **Enable User Certificates**。如有提示，请从下拉列表中选择相应的证书。

系统将显示 Enable Fetching of CRL 选项。

步骤 4　或者，选择 **Enable Fetching of CRL**。

系统将显示其余的 CRL 配置选项。

步骤 5　键入现有 CRL 文件的有效 URL，然后点击 **Refresh CRL**。

所提供的 URL 的当前 CRL 会加载到服务器。

注　启用 CRL 获取功能会创建计划任务来定期更新 CRL。编辑任务以设置更新的频率。有关详细信息，请参阅第 62-4 页上的自动执行证书撤销列表下载。

步骤 6　验证您是否拥有由创建服务器证书的同一证书颁发机构生成的有效用户证书。

注意事项　当保存包含已启用用户证书的配置时，如果在您的浏览器证书存储中无有效用户证书，则会禁用对设备的所有网络服务器访问。请确保在保存设置之前已安装有效证书。

步骤 7　要对网络服务器应用用户证书配置，请点击 **Save**。

请注意，如果您已启用证书，但发现您的用户证书未启用访问，那么您可以通过命令行禁用用户证书执行。有关详细信息，请参阅第 D-42 页上的 disable-http-user-cert。

启用数据库访问

许可证：任何环境

可以配置防御中心以允许第三方客户端对其数据库进行只读访问。这样，您可以通过以下任何方式使用 SQL 来查询数据库：

- 行业标准报告工具（例如， Actuate BIRT、 JasperSoft iReport 或 Crystal Reports）
- 其他任何支持 JDBC SSL 连接的报告应用（包括自定义应用）
- 思科提供的命令行 Java 应用名为 RunQuery，可以交互方式运行或用于获取单一查询的以逗号分隔的结果

从 Database Settings 本地配置页面中，可以启用数据库访问并建立允许选定主机查询数据库的访问列表。请注意，该访问列表不用于控制设备访问。有关设备访问列表的详细信息，请参阅第 63-8 页上的配置设备的访问列表。

您也可以下载包含以下工具的软件包：

- RunQuery（这是思科提供的数据库查询工具）

- InstallCert （可以用于从要访问的防御中心检索和接受 SSL 证书的工具）
- 连接到数据库时必须使用的 JDBC 驱动程序

请注意，从外部客户端连接到数据库时，必须提供与防御中心上的管理员或外部数据库用户的用户名和密码匹配的用户名和密码。有关详细信息，请参阅第 61-41 页上的添加新用户帐户。

有关配置对FireSIGHT 系统数据库的外部访问的详细信息 （包括有关数据库架构和支持的查询的信息），请参阅 《*FireSIGHT 系统数据库访问指南*》。

要启用数据库访问，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **Database**。

系统将显示 Database Settings 页面。

步骤 3　选择 **Allow External Database Access** 复选框。

系统将显示 **Access List** 字段。有关详细信息，请参阅第 6 步。

步骤 4　根据您的第三方应用要求，在 **Server Hostname** 字段中键入防御中心的完全限定域名 (FQDN)、IPv4 地址或 IPv6 地址。

如果键入 FQDN，必须确保客户端能够解析防御中心的 FQDN。如果键入 IP 地址，必须确保客户端能够连接到使用该 IP 地址的防御中心。

步骤 5　在 **Client JDBC Driver** 旁边，点击 **Download** 并按照浏览器提示下载 `client.zip` 软件包。

有关使用下载包中的工具来配置数据库访问的信息，请参阅 《*FireSIGHT 系统数据库访问指南*》。

步骤 6　要添加一个或多个 IP 地址的数据库访问，请点击 **Add Hosts**。

此时， **Access List** 字段中将会显示 **IP Address** 字段。

步骤 7　在 **IP Address** 字段中，可根据要添加的 IP 地址从以下选项中进行选择：

- 确切的 IP 地址 （例如 192.168.1.101）
- 使用 CIDR 表示法的 IP 地址块 （例如 192.168.1.1/24）

  有关在 FireSIGHT 系统中使用 CIDR 的信息，请参阅第 1-16 页上的 IP 地址约定。
- `any`，指定任意 IP 地址

步骤 8　点击 **Add**。

IP 地址将被添加到数据库访问列表。

步骤 9　或者，要删除数据库访问列表中的条目，请点击删除图标 ( )。

步骤 10　点击 **Save**。

这样即会保存数据库访问设置。

提示　点击 **Refresh** 可恢复到上次保存的设置。

配置管理接口

许可证：任何环境

首次设置设备时，应配置设备的网络设置，以便其可在内部受保护的网络中通信。当您首次设置设备和配置其他网络设置 （例如代理）时，可以更改您创建的所有网络设置。在 3 系列 设备和虚拟防御中心上，您可以启用流量通道和配置其他管理接口以提高性能，并且创建路由来管理和隔离防御中心和不同网络上设备之间的流量。在 3 系列 设备上，也可以启用或禁用设备上的 LCD 面板访问。要更改这些设置和配置其他网络设置 （例如代理），请使用 Network Interfaces 页面 （**System > Local > Configuration**，然后点击 **Network Interfaces**）。

注 必须使用命令行工具修改虚拟设备的网络和代理设置，以及修改用于 Blue Coat X-系列的思科 NGIPS 的网络设置。请注意，用于 Blue Coat X-系列的思科 NGIPS 不支持代理。有关详细信息，请参阅《*FireSIGHT 系统虚拟安装指南*》和《*用于 Blue Coat X-系列的思科 NGIPS 安装和配置指南*》。

有关配置选项和步骤，请参阅：

- 第 64-8 页上的了解管理接口选项
- 第 64-10 页上的编辑管理接口

了解管理接口选项

可以更改设置以改进性能，启用不同功能，或者修改部署中的网络配置。在 3 系列设备上，还可以配置流量通道，启用其他管理接口，并创建路由以隔离来自其他网络设备的流量。有关详细信息，请参阅第 4-3 页上的了解管理接口。

接口

FireSIGHT 系统为 IPv4 和 IPv6 管理环境提供了双堆栈实现。可以选择这两个协议或其中之一；如果不想使用，也可以禁用协议 （如果有）。

对于每个管理协议，必须指定默认 (`eth0`) 管理接口的 IP 地址、子网掩码或前缀长度和默认网关。可以手动设置这些设置，或者将设备配置为会从本地 DHCP 服务器或 IPv6 路由器检索这些设置。请注意，必须手动配置您所启用的每个其他 （`eth1` 等）管理接口。

可以对管理接口配置以下选项：

- **Enabled** - 启用管理接口。在启用并保存另一管理接口之前，请勿禁用默认管理接口。
- **Channels** - 启用接口上的 **Management Traffic** 和 **Event Traffic** 通道。

  可以启用流量通道 （管理流量和/或事件流量），以便在管理接口的通信通道中创建不同的连接。此外，还可以在多个管理接口上建立流量信道，从而合并两个接口的吞吐量以进一步提高性能。有关详细信息，请参阅第 4-3 页上的了解管理接口。
- **Mode** - 可更改默认“自动协商”或指定链路模式。请注意，您对“自动协商”值做出的所有更改将被千兆接口忽略。

  向防御中心注册 8000 系列受管设备时，必须在连接两端自动协商或在两端设置相同的静态速度，以确保稳定的网络链路。 8000 系列受管设备不支持半双工网络链路，也不支持两端的速度或双工配置存在差异的连接。
- **MTU** - 可更改默认设置。

注意事项 更改最大传输单位 (MTU) 会中断设备上的流量。 MTU 的设置范围可能因 FireSIGHT 系统设备型号和接口类型而异。

下表列出了管理接口的 MTU 配置范围：

表 64-4　　按设备列出的管理接口 MTU 范围

设备型号	MTU 范围
2 系列 （3D6500 和 3D9900 除外）	576 - 1518
3D6500、 3D9900、虚拟设备	576 - 9018
3 系列默认 (`eth0`)	576 - 9234
3 系列非默认 （`eth1` 等）	1518 - 9018

由于系统会自动从配置的 MTU 值中修剪 18 个字节，因此任何低于 1298 的值都不符合 1280 的最小 IPv6 MTU 设置，并且任何低于 594 的值都不符合 576 的最小 IPv4 MTU 设置。例如，系统自动将配置值 576 调整为 558。

- **MDI/MDIX** - 可更改默认 **Auto-MDIX** 设置。
- **IPv4 Configuration** - 允许配置 **Static**、 **DHCP** 或 **Disabled**。
  - 选择 **Static** 可输入 IPv4 管理 IP 地址和子网掩码。
  - 选择 **DHCP** 可从 DHCP 服务器检索网络设置。（仅适用于 `eth0`）
  - 选择 **Disabled** 将会禁用协议。请勿同时禁用 IPv4 和 IPv6。
- **IPv6 Configuration** - 允许配置 **Static**、 **DHCP**、 **Router Assigned** 或 **Disabled**。
  - 选择 **Static** 可输入 IPv4 管理 IP 地址和子网掩码。
  - 选择 **DHCP** 可从 DHCP 服务器检索网络设置。（仅适用于 `eth0`）
  - 选择 **Router Assigned** 可从本地 IPv6 路由器检索网络设置。
  - 选择 **Disabled** 将会禁用协议。请勿同时禁用 IPv4 和 IPv6。

路由

点击 Edit 图标可查看或编辑到默认管理接口的路由，点击 View 图标可查看路由统计信息。

可以创建到其他网络的新路由。点击 Add 图标将会显示一个弹出窗口，可以在该窗口中输入目标网络 IP 地址、子网掩码或前缀长度、接口下拉列表 （`eth0` 等）和网关。以下示例显示了一些可以用来路由到其他网络的方法：

- 在防御中心上，可以创建到其他网络上设备的路由，以使一个防御中心能够管理和隔离来自其他网络上设备的流量。
- 在设备上，可以创建路由并向两个不同网络上的防御中心注册设备，以配置更广泛部署中防御中心的高可用性。

您可以在特定管理接口上配置以下设置来创建通向某个网络的路由：

- **Destination** - 要创建路由的网络的目标地址。
- **Netmask** 或 **Prefix Length** - 网络的子网掩码 (IPv4) 或前缀长度 (IPv6)
- **Interface** - 设备上分配给新路由的管理接口。
- **Gateway** - 新网络的网关。

共享设置

无论管理环境如何，都可以指定最多三个 DNS 服务器以及设备的主机名和域名。

可以更改管理端口。 FireSIGHT 系统设备使用双向、 SSL 加密的通信信道 （默认情况下在端口 8305 上）进行通信。尽管思科**强烈**建议保留默认设置，但如果管理端口与网络上的其他通信冲突，则可以选择其他端口。

注意事项　如果更改管理端口，则必须为部署中需要相互通信的所有设备更改该端口。

LCD 面板

3 系列 设备允许您使用设备正面的 LCD 面板查看设备信息。在 3 系列 Management Interfaces 页面上，您还可以允许相关人员使用 LCD 面板更改网络设置。

如果使用 LCD 面板编辑受管设备的 IP 地址，请确认管理防御中心上反映这些更改。在某些情况下，您可能需要手动编辑设备管理设置。有关详细信息，请参阅第 4-46 页上的编辑设备管理设置。

注意事项　允许使用 LCD 面板进行重新配置可能带来安全风险。要使用 LCD 面板配置网络设置，只需进行物理访问，而不需要进行身份验证。

代理

所有 FireSIGHT 系统设备都配置为通过 443/tcp (HTTPS) 端口和 80/tcp (HTTP) 端口直接连接到互联网；请参阅第 E-1 页上的安全、互联网接入和通信端口。除用于 Blue Coat X-系列的思科 NGIPS 以外，FireSIGHT 系统设备支持使用代理服务器（您可以通过 HTTP 摘要对代理服务器进行身份验证）。

注意事项　使用 NT LAN Manager (NTLM) 身份验证的代理无法与综合安全智能云通信以接收信息。如果要使用基于云的功能，请确保为您的代理配置不同的身份验证。有关详细信息，请参阅第 64-25 页上的启用云通信。

编辑管理接口

许可证：任何环境

可以使用 Management Interfaces 页面修改防御中心上的默认管理接口的默认设置。在 3 系列 设备和虚拟防御中心上，还可以启用和配置流量通道和其他管理接口。您对 Auto Negotiate 值做出的所有更改将被千兆接口忽略。

注意事项　除非拥有对设备的物理访问权限，否则请勿修改管理接口的设置。选择设置可能导致难以访问网络界面。

要编辑管理接口，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **Management Interfaces**。

系统将显示 Management Interfaces 页面，其中列出防御中心上每个接口的当前设置。

步骤 3　或者，在 **Interfaces** 下，点击要配置的接口旁边的 **Edit**。

可以修改默认管理接口 (`eth0`) 或启用和配置其他管理接口 （`eth1` 等）。对于每个其他管理接口，则必须分配唯一的静态 IP 地址 （IPv4 或 IPv6）或主机名。除了设置模式、链路、 MTU 和 IP 配置之外，还可以选择承载流量的流量信道。

步骤 4　或者，在 **Routes** 下，输入目标网络的 IP 地址、子网掩码或前缀长度和网关，并指定要用于该网络路由的管理接口。

还可以点击放大镜图标来查看路由统计信息。

步骤 5　或者，在 **Shared Settings** 下，指定不依赖于管理网络协议的网络设置。

可以指定最多三个 DNS 服务器以及设备的主机名和域。请注意，如果在上一步骤中选择了 **DHCP**，将无法手动指定这些共享设置。

注意事项　思科**强烈**建议保留默认设置，但是，如果管理端口冲突与网络中的其他通信冲突，可以选择其他端口。如果更改管理端口，必须更改部署中需要相互通信的**所有**设备的该端口。

步骤 6　或者，在 3 系列 设备上的 LCD Panel 下，选择 **Allow reconfiguration of network settings** 复选框，以允许使用设备的 LCD 面板更改网络设置。

注意事项　允许使用 LCD 面板进行重新配置可能带来安全风险。要使用 LCD 面板配置网络设置，只需进行物理访问，而不需要进行身份验证。网络界面会提醒您，启用此选项是潜在的安全问题。

步骤 7　或者，在 **Proxy** 下选择复选框以启用代理，然后：

- 在 **HTTP Proxy** 字段中输入代理服务器的 IP 地址或标准域名。在 **Port** 字段中输入端口。
- 或者，通过选择 **Use Proxy Authentication** 来提供身份验证凭证，然后提供 **User Name** 和 **Password**。

步骤 8　完成设备的网络设置配置后，点击 **Save**。

这样即会更改网络设置。如果更改设备的主机名，在重新启动设备之前，新名称不会反映到系统日志中。

关闭并重新启动系统

许可证：任何环境

有多种方法可以控制设备上的进程。您能够：

- 关闭设备
- 重新启动设备

- 重新启动设备上的通信、数据库和 HTTP 服务器进程 （通常用于故障排除）
- 重新启动 Snort 进程

注意事项 请勿使用电源按钮关闭设备；这样做可能导致数据丢失。应通过 Appliance Process 页面完全关闭设备。

要关闭或重新启动设备，请执行以下操作：

访问：管理

步骤 1 选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2 点击 **Process**。

系统将显示 Appliance Process 页面。

步骤 3 指定要执行的命令：

在防御中心上：

- 要关闭设备，请点击 **Shutdown防御中心**旁边的 **Run Command**。
- 要重新启动设备，请点击 **Reboot防御中心**旁边的 **Run Command**。请注意，这将使您从防御中心注销。
- 要重新启动设备，请点击 **Restart防御中心 Console** 旁边的 **Run Command**。请注意，重新启动防御中心可能导致已删除的主机重新显示在网络映射中。

注 重新启动防御中心时，系统会执行可能需要 1 小时才能完成的数据库检查。

在受管设备上：

- 要关闭设备，请点击 **Shutdown Appliance** 旁边的 **Run Command**。
- 要重新启动设备，请点击 **Reboot Appliance** 旁边的 **Run Command**。请注意，这将使您从设备注销。
- 要重新启动设备，请点击 **Restart Appliance Console** 旁边的 **Run Command**。
- 要重新启动 Snort 进程，请点击 **Restart Snort** 旁边的 **Run Command**。

注 重新启动受管设备时，系统会执行可能需要 1 小时才能完成的数据库检查。

手动设置时间

许可证：任何环境

如果当前应用的系统策略中的 Time Synchronization 设置设置为 **Manually in Local Configuration**，则可在本地配置中使用 Time 页面手动设置设备时间。

必须使用本地应用 （例如，命令行界面或操作系统接口）来管理用于 Blue Coat X-系列的思科 NGIPS的时间设置。有关详细信息，请参阅 《*用于 Blue Coat X-系列的思科 NGIPS 安装指南*》。

如果设备根据 NTP 同步其时间，您将无法手动更改时间。在这种情况下， Time 页面上的 NTP Status 部分提供以下信息：

表 64-5　　NTP 状态

列	说明
NTP 服务器	已配置的 NTP 服务器的 IP 地址和名称。
状态	NTP 服务器时间同步状态。可能会显示以下状态： • **Being Used** 表示设备已与 NTP 服务器同步。 • **Available** 表示 NTP 服务器可供使用，但时间尚未同步。 • **Not Available** 表示 NTP 服务器在您的配置中，但 NTP 后台守护程序无法使用该服务器。 • **Pending** 表示 NTP 服务器是新的或 NTP 后台守护程序最近重新启动过。随着时间的推移，此选项的值应更改为 **Being Used**、 **Available** 或 **Not Available**。 • **Unknown** 表示 NTP 服务器的状态未知。
Offset	设备时间与已配置的 NTP 服务器上时间所相差的毫秒数。负值表示设备时间晚于 NTP 服务器，正值表示设备时间早于 NFP 服务器。
上次更新	自上次与 NTP 服务器同步以来过去的秒数。 NTP 后台守护程序会根据若干条件自动调整同步时间。例如，如果显示更长的更新时间 （例如 300 秒），表示时间相对稳定，这样， NTP 后台守护程序将会确定不需要使用更小的更新增量。

有关系统策略中的时间设置的详细信息，请参阅第 63-24 页上的同步时间。

要手动配置时间，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **Time**。

屏幕上随即会显示 Time 页面。

步骤 3　从 **Set Time** 下拉列表中选择以下信息：

- year
- 月
- 天
- 小时
- 分钟

步骤 4　点击**应用 (Apply)**。

时间即会更新。有关更改时区的信息，请参阅第 71-6 页上的设置默认时区。

管理远程存储

许可证：任何环境

在防御中心不支持 MDC上，可以将本地或远程存储用于备份和报告。可以将网络文件系统 (NFS)、安全外壳 (SSH) 或服务器消息块 (SMB)/公共互联网 (CIFS) 用于备份和报告远程存储。不能将备份发送到一个远程系统而将报告发送到另一个，但是，可以选择这二者之一发送到远程系统，并将另一个存储在本地防御中心。有关备份和恢复的信息，请参阅第 70-1 页上的使用备份和恢复。

提示　在配置并选择远程存储之后，只有在未增加连接数据库限制的情况下，才可以切换回本地存储。

必须确保外部远程存储系统可正常工作且能够防御中心 进行访问。

选择其中一个备份和报告存储选项：

- 要禁用外部远程存储，并使用本地防御中心 来存储备份和报告，请参阅第 64-14 页上的使用本地存储。
- 要使用 NFS 来存储备份和报告，请参阅第 64-15 页上的将 NFS 用于远程存储。
- 要通过 SSH 使用 Secure Shell (SCP) 来存储备份和报告，请参阅第 64-15 页上的将 SSH 用于远程存储。
- 要使用 SMB 来存储备份和报告，请参阅第 64-16 页上的将 SMB 用于远程存储。

注　不能使用远程备份和恢复来管理用于 Blue Coat X-系列的思科 NGIPS上的数据。

使用本地存储

许可证：任何环境

可以将备份和报告存储在本地防御中心 上。

要在本地存储备份和报告，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **Remote Storage Device**。

系统将显示 Remote Storage Device 页面。

步骤 3　从 **Storage Type** 下拉列表中选择 **Local (No Remote Storage)**。

步骤 4　点击 **Save**。

即会保存所选的存储位置。

提示　请勿对本地存储使用 **Test** 按钮。

将 NFS 用于远程存储

许可证：任何环境

可以选择网络文件系统 (NFS) 协议来存储报告和备份。或者，选择 **Use Advanced Options** 复选框，以按照 NFS 手动安装页面中所述使用其中一个二进制安装选项。

要使用 NFS 来存储备份和报告，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **Remote Storage Device**。

系统将显示 Remote Storage Device 页面。

步骤 3　从 **Storage Type** 下拉列表中选择 **NFS**。

页面将会刷新以显示 NFS 存储配置选项。

步骤 4　添加连接信息：

- 在 **Host** 字段中输入存储系统的 IPv4 地址或主机名。
- 在 **Directory** 字段中输入存储区域的路径。

步骤 5　如果必须使用任何命令行选项，请选择 **Use Advanced Options**。

Command Line Options 字段将会显示，可以在其中输入二进制安装选项。

步骤 6　在 **System Usage** 中，选择以下一个或两个选项：

- 选择 **Use for Backups** 在指定主机上存储备份。
- 选择 **Use for Reports** 在指定主机上存储报告。
- 然后，在 **Disk Space Threshold** 中输入要备份远程存储的磁盘空间阈值。默认值为 90%。

步骤 7　或者，点击 **Test**。

测试确保防御中心可访问指定的主机和目录。

步骤 8　点击 **Save**。

此时会保存远程存储配置。

将 SSH 用于远程存储

许可证：任何环境

可以选择 SSH 以使用安全复制 (SCP) 来存储报告和备份。或者，选择 **Use Advanced Options** 复选框，以按照 SSH 手动安装页面中所述使用其中一个二进制安装选项。

注意事项　如果已在设备上启用 STIG 合规性，那么将无法对该设备使用 SSH 进行远程存储。有关详细信息，请参阅第 63-22 页上的启用 STIG 合规性。

要使用 SSH 存储备份和报告，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **Remote Storage Device**。

系统将显示 Remote Storage Device 页面。

步骤 3　在 **Storage Type** 处选择 **SSH**。

页面将会刷新以显示通过 SSH 的 SCP 存储配置选项。

步骤 4　添加连接信息：

- 在 **Host** 字段中输入存储系统的 IP 地址或主机名。
- 在 **Directory** 字段中输入存储区域的路径。
- 在 **Username** 字段中输入存储系统的用户名，在 **Password** 字段中输入该用户的密码。要指定域名，请在用户名前面加上域后跟正斜杠 (/)。
- 要使用 SSH 密钥，请将 **SSH Public Key** 字段中的内容复制到 authorized_keys 文件中。

步骤 5　如果必须使用任何命令行选项，请选择 **Use Advanced Options**。

Command Line Options 字段将会显示，可以在其中输入二进制安装选项。

步骤 6　在 System Usage 中，选择以下一个或两个选项：

- 选择 **Use for Backups** 在指定主机上存储备份。
- 选择 **Use for Reports** 在指定主机上存储报告。

步骤 7　或者，点击 **Test**。

测试确保防御中心可访问指定的主机和目录。

步骤 8　点击 **Save**。

此时会保存远程存储配置。

将 SMB 用于远程存储

许可证：任何环境

可以选择服务器消息块 (SMB) 协议来存储报告和备份。或者，选择 **Use Advanced Options** 复选框，以按照 SMB 手动安装页面中所述使用其中一个二进制安装选项。例如，使用 SMB 时，可以在 **Command Line Options** 字段中使用以下格式进入安全模式：

```
sec=mode
```

其中，*mode* 是要用于远程存储的安全模式。有关设置选项，请参阅安全模式设置表。

表 64-6　　安全模式设置

模式	说明
[无]	尝试连接为 NULL 用户 （无名称）。
krb5	使用 Kerberos V5 验证。

表 64-6　　安全模式设置 （续）

模式	说明
krb5i	使用 Kerberos 身份验证和数据包签名。
ntlm	使用 NTLM 密码散列。（默认设置）
ntlmi	使用带签名的 NTLM 密码散列 （如果 /proc/fs/cifs/PacketSigningEnabled 已启用或服务器需要签名，则可能使用默认设置）。
ntlmv2	使用 NTLMv2 密码散列。
ntlmv2i	使用带数据包签名的 NTLMv2 密码散列。

要使用 SMB 存储备份和报告，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **Remote Storage Device**。

系统将显示 Remote Storage Device 页面。

步骤 3　在 **Storage Type** 下选择 **SMB**。

页面将会刷新以显示 SMB 存储配置选项。

步骤 4　添加连接信息：

- 在 **Host** 字段中输入存储系统的 IPv4 地址或主机名。
- 在 **Share** 字段中输入存储区域共享。请注意，系统只能识别顶级共享，不能识别完整文件路径。要将指定的共享目录用作远程备份目标，必须在 Windows 系统上共享该目录。
- 或者，在 **Domain** 字段中输入远程存储系统的域名。
- 在 **Username** 字段中输入存储系统的用户名，在 **Password** 字段中输入该用户的密码。

步骤 5　如果必须使用任何命令行选项，请选择 **Use Advanced Options**。

Command Line Options 字段将会显示，可以在其中输入二进制安装命令 （例如安全模式）。有关详情，请参见第 64-16 页上的表 64-6安全模式设置。

步骤 6　在 System Usage 中，选择以下一个或两个选项：

- 选择 **Use for Backups** 在指定主机上存储备份。
- 选择 **Use for Reports** 在指定主机上存储报告。

步骤 7　或者，点击 **Test**。

测试确保防御中心可访问指定的主机和目录。

步骤 8　点击 **Save**。

此时会保存远程存储配置。

了解更改调节

许可证：任何环境

要监控用户进行的更改并确保它们符合贵组织的首选标准，可以将系统配置为会通过邮件发送有关过去 24 小时内出现的系统更改的详细报告。每当用户保存对系统的配置更改，就会生成更改快照。更改调节报告将汇总这些快照的信息以提供最新系统更改的清晰摘要。

以下示例图表显示示例更改调节报告的“用户”部分，并且列出每个配置更改前和更改后的值。如果用户多次更改同一配置，报告会按时间顺序列出每次不同更改的摘要，最近的更改最先列出。

6 User - SampleUser

6.1 User (2011-03-29 12:42:17 by admin from 10.4.4.4)

Field	Previous Value	Current Value
Name	SampleUser	
Active	Enabled	
Authentication	SHA512	
Password	*********	
Maximum Number of Failed Logins	5	
Days Until Password Expiration	Unlimited	
Days Until Expiration Warning	0	
Check Password Strength	No	
Roles		
	Administrator	

6.2 User (2011-03-29 12:42:12 by admin from 10.4.4.4)

Field	Previous Value	Current Value
Name		SampleUser
Active		Enabled

371868

可以查看过去 24 小时内所做的更改。但是，要查看以前的更改，则必须查看审核日志。有关详情，请参见第 69-7 页上的使用审计日志检查更改。

要使用更改调节功能，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **Change Reconciliation**。

系统将显示 Change Reconciliation 页面。

步骤 3　选择 **Enable** 复选框。

步骤 4　从 **Time to Run** 下拉列表中选择您希望系统每天发出更改调节报告的具体时间。

步骤 5　在 **Email to** 字段中，输入报告收件人的邮件地址。可以随时点击 **Resend Last Report** 向收件人发送最新更改调节报告的副本。

注　要接收更改调节报告，您必须先配置邮件中继主机和通知地址。有关详细信息，请参阅第 63-17 页上的配置邮件中继主机和通知地址。

步骤 6　或者，选择 **Include Policy Configuration** 以在更改调节报告中包括策略更改记录。这包括对访问控制策略、入侵策略、系统策略、运行状况策略和网络发现策略的更改。如果未选择该选项，报告将不会显示对任何策略的更改。

注　该选项在受管设备上不可用。

步骤 7　或者，选择 **Show Full Change History** 以包括更改调节报告中有关过去 24 小时内发生的所有更改的记录。如果未选择该选项，报告仅包括每个类别的更改的整合视图。

步骤 8　点击 **Save**。

已保存您的更改。报告每天在您选择的时间运行。

管理远程控制台访问

许可证：任何环境

受支持的设备：因功能而异

受支持的防御中心：因功能而异

可以通过物理设备上的 VGA 端口 （默认端口）或串行端口使用 Linux 系统控制台对任何设备进行远程访问。请选择最适合贵组织思科部署的物理布局。

可以通过 LAN 上串行 (SOL) 连接在默认 (`eth0`) 管理接口上使用无人值守管理 (LOM) 来远程监控或管理 3 系列 设备，而无需登录设备的管理接口。在带外管理连接上使用命令行界面可以执行有限的任务，例如查看机箱序列号或监控诸如风扇速度和温度之类的状况。 2 系列、虚拟设备、ASA FirePOWER 模块和用于 Blue Coat X-系列的思科 NGIPS 不支持 LOM。

必须对设备和要管理设备的用户都启用 LOM。在启用设备和用户后，使用第三方智能平台管理接口 (IPMI) 实用程序访问和管理设备。

注　这样，当主机启动时， 3D71xx、 3D82xx 或 3D83xx 设备的基板管理控制器 (BMC) 只有通过 1 Gbps 的链路速度才能访问。 设备断电时， BMC 只有在 10 Mbps 和 100 Mbps 的速度下才能建立以太网链路。 因此，如果使用 LOM 远程启动设备，只能使用 10 Mbps 和 100 Mbps 的链路速度将设备连接至网络。

有关详细信息，请参阅：

- 第 64-20 页上的配置设备上的远程控制台设置
- 第 64-21 页上的启用无人值守管理用户访问
- 第 64-22 页上的使用 LAN 上串行连接
- 第 64-23 页上的使用无人值守管理

配置设备上的远程控制台设置

许可证：任何环境

受支持的设备：因功能而异

受支持的防御中心：因功能而异

使用要远程管理的设备的网络界面来选择和配置要使用的远程控制台访问选项。

请注意，2 系列、虚拟设备、ASA FirePOWER 模块和用于 Blue Coat X-系列的思科 NGIPS 不支持 LOM。

注　使用 LOM/SOL 连接到 3 系列 设备之前，必须禁用连接到设备管理接口的所有第三方交换机设备上的生成树协议 (STP)。

要配置远程控制台设置，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　选择 **Console Configuration**：

系统将显示 Console Configuration 页面。

步骤 3　选择远程控制台访问选项：

- 选择 **VGA** 将会使用设备上的 VGA 端口。这是默认选项。
- 选择 **Physical Serial Port**，将会使用设备的串行端口或者在 3 系列、防御中心、 3D7050 或 8000 系列设备上使用 LOM/SOL。

  请注意， 3D2100、 3D2500、 3D3500 和 3D4500 受管设备没有串行端口。
- 选择 **Lights-Out Management** 将会在 7000 系列设备 （3D7050 除外）上使用 LOM/SOL。在这些设备上，不能同时使用 SOL 和常规串行连接。

如果选择 **Physical Serial Port** 或 **Lights-Out Management**，将显示 LOM 设置。

注　如果您在 70xx 子系列设备 （3D7050 除外）上将远程控制台从 **Physical Serial Port** 更改为 **Lights-Out Management**，或者从 **Lights-Out Management** 更改为 **Physical Serial Port**，则必须重新启动设备两次才会出现预期的启动提示。

步骤 4　要通过 SOL 配置 LOM，请输入适当的设置：

- 设备的 DHCP **配置** （**DHCP** 或**静态**）
- 将要用于 LOM 的 **IP 地址**

注　LOM IP 地址必须不同于设备的管理接口 IP 地址。

- 设备的**子网掩码**
- 设备的**默认网关**

步骤 5　点击 **Save**。

将会保存设备的远程控制台配置。如果配置了无人值守管理，则必须至少为一个用户启用此功能；请参阅第 64-21 页上的启用无人值守管理用户访问。

启用无人值守管理用户访问

许可证：任何环境

受支持的设备：3 系列

受支持的防御中心：3 系列

必须将“无人值守管理”权限明确授予将会使用此功能的用户。使用每个设备的本地网络界面，可以逐个设备配置 LOM 和 LOM 用户。也就是说，不能使用防御中心配置受管设备的 LOM。同样，因为用户独立于每个设备受管理，因此，在防御中心上启用或创建 LOM 用户不会将此功能转移到受管设备上的用户。

LOM 用户还有如下限制：

- 必须为用户指定管理员角色。
- 用户名最多可包含 16 个字母数字字符。不支持将短划线和更长的用户名用作 LOM 用户名。
- 密码最多可以包含 20 个字母数字字符，但 3D7100 系列设备除外。如果在 3D7110、3D7115、3D7120 或 3D7125 设备上启用 LOM，密码最多可以包含 16 个字母数字字符。对于 LOM 用户，不支持长度大于 20 或 16 个字符的密码。用户的 LOM 密码不得与该用户的系统密码相同。思科建议您为设备使用最大支持长度、不是基于字典的复杂密码，并且每三个月修改一次密码。
- 3 系列防御中心和 8000 系列设备最多可以有 13 个 LOM 用户。7000 系列设备最多可以有 8 个 LOM 用户。

请注意，如果在一个具有 LOM 权限的角色已登录时取消激活然后再重新激活该角色，或者在用户登录会话期间从备份恢复该用户或用户角色，那么该用户必须重新登录到网络界面才能重新获得对 IPMItool 命令的访问权限。有关详细信息，请参阅第 61-46 页上的管理预定义用户角色。

要启用或查看无人值守管理用户访问，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > User Management**。

系统将显示 User Management 页面。

步骤 2　您有以下选项：

- 要向现有用户授予 LOM 用户访问权限，请点击列表中用户名旁边的编辑图标 ( )。
- 要向新用户授予 LOM 用户访问权限，请点击 **Create User**。

步骤 3　在 User Configuration 下，启用管理员角色。

系统将显示管理员选项。

步骤 4　选择 **Allow Lights-Out Management Access** 复选框。

步骤 5　点击 **Save**。

用户即可获得设备的 LOM 访问权限。

使用 LAN 上串行连接

许可证：任何环境

受支持的设备：3 系列

受支持的防御中心：3 系列

使用计算机上的第三方 IPMI 实用程序可通过 LAN 上串行与设备建立连接。如果您的计算机使用类似 Linux 的环境或 Mac 环境，请使用 IPMItool；对于 Windows 环境，请使用 IPMIutil。

注 思科建议使用 IPMItool V1.8.12 或更高版本。

Linux

IPMItool 是许多发行版的标准配置，可立即使用。

Mac

必须在 Mac 上安装 IPMItool。首先，请确认 Mac 上安装了 Apple 的 XCode 开发者工具，确保安装了用于命令行开发的可选组件 （较新版本的 UNIX 开发和系统工具或较旧版本的 Command Line Support）。然后您可以安装 macports 和 IPMItool。请使用您常用的搜索引擎搜索更多信息，以下网站也可能对您帮助：

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Windows

必须在 Windows 上编译 IPMIutil。如果无法访问编译器，可以使用 IPMIutil 自身来编译。请使用您常用的搜索引擎搜索更多信息，以下网站也可能对您帮助：：

```
http://ipmiutil.sourceforge.net/
```

了解 IPMI 实用程序命令

用于 IPMI 实用程序的命令由若干段组成，如以下 IPMItool 示例：

```
ipmitool -I lanplus -H IP_address -U user_name command
```

其中：

- `ipmitool` 调用实用程序
- `-I lanplus` 启用会话加密
- `-H Ip_address` 表示要访问设备的 IP 地址
- `-U user_name` 是授权用户的名称
- `-command` 是要发出的命令的名称

注 思科建议使用 IPMItool V1.8.12 或更高版本。

对于 Windows，以上命令如下所示：

```
ipmiutil command -V 4 -J 3 -N IP_address -U user_name
```

使用此命令可连接到设备的命令行，就像您本人在设备旁边一样。系统会提示您输入密码。

要在 LAN 上创建串行连接，请执行以下操作：

访问：具有 LOM 访问权限的管理员

步骤 1　输入以下命令：

对 IPMItool：

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

注　思科建议使用 IPMItool V1.8.12 或更高版本。

对 IPMIutil：

```
ipmiutil -J 3 -H IP_address -U username sol -a
```

系统将显示设备的命令行登录对话框。系统会提示您输入密码。

使用无人值守管理

许可证：任何环境

受支持的设备：3 系列

受支持的防御中心：3 系列

通过无人值守管理，可以在默认 (eth0) 管理接口上利用 SOL 连接执行有限的系列操作，而无需登录设备。可以使用下表中列出的其中一个命令来创建 SOL 连接。命令执行完成后，连接将终止。请注意，不是所有的电源控制命令在70xx 子系列设备上都有效。

注　这样，当主机启动时， 3D71xx、 3D82xx 或 3D83xx 设备的基板管理控制器 (BMC) 只有通过 1 Gbps 的链路速度才能访问。 设备断电时， BMC 只有在 10 Mbps 和 100 Mbps 的速度下才能建立以太网链路。 因此，如果使用 LOM 远程启动设备，只能使用 10 Mbps 和 100 Mbps 的链路速度将设备连接至网络。

注意事项　在极少数情况下，如果您的计算机与设备的管理接口位于不同子网，而设备配置为使用 DHCP，尝试访问3 系列设备的 LOM 功能可能失败。如果发生这种情况，可以禁用然后在设备上重新启用 LOM，或者使用与设备位于同一子网的计算机来 ping 设备的管理接口。这样应该就可以使用 LOM。

注意事项　思科了解智能平台管理接口 (IPMI) 标准 (CVE-2013-4786) 固有的漏洞。在设备上启用无人值守管理 (LOM) 会暴露该漏洞。为了降低这种漏洞，请将您的设备部署在只有受信任用户才可以访问的安全管理网络上，并且使用最大支持长度、不是基于字典的复杂密码并且每三个月修改一次密码。为防止暴露此漏洞，请勿启用 LOM。

如果所有访问设备的尝试均失败，可以使用 LOM 远程重新启动设备。请注意，如果在 SOL 连接处于活动状态时重新启动系统， LOM 会话可能会断开连接或超时。

注意事项　请勿重新启动设备，除非它不响应任何其他的重新启动操作。远程重新启动设备不能正常重新启动系统，而且可能会丢失数据。

表 64-7　无人值守管理命令

IPMItool	IPMIutil	说明
（不适用）	`-V 4`	启用 IPMI 会话的管理员权限
`-I lanplus`	`-J 3`	启用 IPMI 会话加密
`-H`	`-N`	表示远程设备的 IP 地址
`-U`	`-U`	表示已获授权 LOM 帐户的用户名
`sol activate`	`sol -a`	开始 SOL 会话
`sol deactivate`	`sol -d`	结束 SOL 会话
`chassis power cycle`	`power -c`	重新启动设备 （在70xx 子系列设备上无效）
`chassis power on`	`power -u`	打开设备电源
`chassis power off`	`power -d`	关闭设备电源 （在 70xx 子系列设备上无效）
`sdr`	`sensor`	显示设备信息，例如风扇速度和温度

例如，显示设备信息列表的 IPMItool 命令是：

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

注　思科建议使用 IPMItool V1.8.12 或更高版本。

对于 IPMIutil 实用程序，以上命令如下：

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

要使用无人值守管理，请执行以下操作：

访问：具有 LOM 访问权限的管理员

步骤 1　输入以下命令：

对 IPMItool：

```
ipmitool -I lanplus -H IP_address -U user_name command
```

注　思科建议使用 IPMItool V1.8.12 或更高版本。

对 IPMIutil：

```
ipmiutil -J 3 -H IP_address -U username command
```

其中，*command* 是无人值守管理命令表中的一个命令。

将执行表中记录的相应操作。系统会提示您输入密码。

启用云通信

许可证：URL 过滤或恶意软件

受支持的防御中心：除 DC500 外的所有型号

FireSIGHT 系统联系思科的综合安全智能云获得各种信息：

- 如果贵组织订用了 FireAMP，您可能会接收到基于终端的恶意软件事件；请参阅第 37-21 页上的为 FireAMP 处理云连接。
- 受管设备可以利用与访问控制规则相关联的文件策略来检测在网络流量中传输的文件。防御中心使用思科云中的数据来确定文件是否为恶意软件；请参阅第 37-8 页上的了解和创建文件策略。
- 启用 URL 过滤后，防御中心可检索许多通常被访问的 URL 的类别和信誉数据，还可对未分类 URL 执行查找。然后，可以迅速创建访问控制规则的 URL 条件；请参阅第 16-8 页上的执行基于信誉的 URL 阻止。

关于基于云的文件和恶意软件功能，如果贵组织要求更高的安全性或希望限制外部连接，那么可以使用 FireAMP 私有云（而不是标准云连接）。所有文件和恶意软件云查找，以及从 FireAMP 终端的事件数据收集和中继，将通过私有云处理；当私有云与公共思科云联系时，它会通过匿名代理连接执行相关处理。尽管私有云不支持动态分析或非 FireAMP 云功能（例如，安全情报或 URL 过滤），但从用户的角度来说，私有云功能与标准公共云连接基本相同。有关配置私有云的详细信息，请参阅第 37-24 页上的与 FireAMP 私有云协作的。

使用防御中心的本地配置指定以下选项：

启用 URL 过滤

必须启用此选项以执行类别和基于信誉的 URL 过滤。

未知 URL 的云查询

当监控网络上的某人尝试浏览不在本地数据集中的 URL 时，允许系统查询云。

如果云不知道 URL 的类别或信誉，或者，如果防御中心不能与云联系，那么 URL **不会**匹配关于基于类别或信誉的 URL 条件的访问控制规则。在这种情况下，您将无法手动对该 URL 指定类别或信誉。

如果您不想让思科云对未分类 URL 进行归类（例如，出于隐私原因），请禁用此选项。

启用自动更新

允许系统定期与云联系，以获取对设备本地数据集中 URL 数据的更新。云通常每天更新一次数据，但是，启用自动更新会强制防御中心每 30 分钟检查一次，以确保您始终获得最新信息。

虽然每日更新通常是小量更新，但是，如果距离上一次更新超过五天，新的 URL 过滤数据最多可能需要 20 分钟才能下载完（具体取决于带宽）。然后，执行更新也可能最多需要 30 分钟。

如果希望严格控制系统联系云的时间，可以禁用自动更新而改为使用调度程序，如第 62-16 页上的自动更新 URL 过滤中所述。

注　思科建议启用自动更新或使用调度程序安排更新。虽然可以手动执行按需更新，但设置系统定期自动与云联系可为您提供最新、最相关的 URL 数据。

与思科共享恶意软件事件的 URI 信息

或者，防御中心可以向云发送有关网络流量中所检测到文件的信息。此信息包括与被检测的文件相关联的 URI 信息及其 SHA-256 散列值。虽然共享是可选的，但是，向思科发送这些信息有助于以后识别和跟踪恶意软件。

使用遗留 32137 端口执行网络 AMP 查找

选择此复选框允许系统使用端口 32137/tcp （之前的默认端口）执行网络云查找，而不是使用端口 443/tcp。如果将设备从 FireSIGHT 系统的先前版本进行了更新，那么默认情况下会选择此复选框。

许可

执行基于类别和信誉的 URL 过滤和基于设备的恶意软件检测要求您在受管设备上启用的相应许可证；请参阅第 65-1 页上的许可 FireSIGHT 系统。

如果您在防御中心上不具有URL 过滤 或 恶意软件 许可证，那么您将**不能**配置云连接选项。如果您只有这两个许可证当中的其中一个，那么 Cloud Services 本地配置页面将仅显示您获得许可的选项。拥有已到期许可证的 防御中心不能与云联系。

请注意，除了导致 URL 过滤选项对话框出现，自动添加URL 过滤许可证到防御中心还会启用 **Enable URL Filtering** 和 **Enable Automatic Updates**。如有需要，可以手动禁用该选项。

请注意，使用 FireAMP 订用接收基于终端的恶意软件事件不需要许可证，也不需要指定要允许或拦截的单个 URL 或 URL 组。有关详细信息，请参阅第 37-2 页上的了解恶意软件防护和文件控制和第 16-10 页上的执行手动 URL 阻止。

互联网访问和高可用性

系统使用 80/HTTP 和 443/HTTPS 端口与思科云联系，并支持使用代理；请参阅第 64-8 页上的配置管理接口。

尽管所有 URL 过滤配置和信息在高可用性部署中的防御中心之间同步，但只有主防御中心会下载 URL 过滤数据。如果主防御中心发生故障，必须确保辅助防御中心可直接接入互联网，并可使用辅助防御中心上的 网络界面来晋升为主用设备。有关详细信息，请参阅第 4-13 页上的监控和更改高可用性状态。

另一方面，尽管它们会共享文件策略和相关配置，但高可用性对中的防御中心不共享云连接和恶意软件处置。为了确保业务连续性并确保在两个防御中心上对检测到文件的恶意软件的处置一致，主和辅助防御中心必须都有权访问云。

健康监控

默认运行状况策略包括跟踪防御中心云连接的状态和稳定性的以下模块：

- URL 过滤监控 （如果防御中心无法将类别和信誉更新推送到其受管设备，此模块还会发出警告）
- 高级恶意软件防护

提示 另一个模块 （FireAMP 状态监控）为 FireAMP 订阅持有人跟踪防御中心与思科云之间的连接。有关运行状况监控的详细信息，请参阅第 68-37 页上的使用运行状况监视器。

以下步骤说明如何启用与思科云的通信以及执行 URL 数据的按需更新。请注意，如果有更新正在进行，则不能启动按需更新。

要启用与云的通信，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **Cloud Services**。

系统将显示 Cloud Services 页面。如果您有 URL 过滤许可证，该页面会显示上次更新 URL 数据的时间。

步骤 3　如上所述配置云连接选项。

必须先启用 **Enable URL Filtering**，然后才能启用 **Enable Automatic Updates** 或 **Query Cloud for Unknown URLs**。

步骤 4　点击 **Save**。

即会保存设置。如果启用 URL 过滤，防御中心会从云检索 URL 过滤数据 （具体取决于上一次启用 URL 过滤的时间，或者是不是首次启用 URL 过滤）。

要执行系统的 URL 数据按需更新，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **URL Filtering**。

系统将显示 URL Filtering 页面。

步骤 3　点击 **Update Now**。

防御中心联系云并更新其 URL 过滤数据 （如果有更新可用）。

启用 VMware 工具

许可证：任何环境

受支持的防御中心：虚拟化

VMware 工具是专用于提高虚拟机性能的一套实用工具。通过这些实用工具，您可以充分利用 VMware 产品方便的功能。该系统在所有虚拟设备上均支持以下插件：

- guestInfo
- powerOps
- timeSync
- vmbackup

也可以在所有受支持的 ESXi 版本上启用 VMware 工具。有关受支持的版本列表，请参阅《*FireSIGHT 系统虚拟安装指南*》。有关 VMware 工具全部功能的详细信息，请参阅 VMware 网站 (http://www.vmware.com/)。

以下步骤说明如何使用网络界面上的 Configuration 菜单启用虚拟防御中心上的 VMware 工具。因为虚拟设备没有网络界面，所以必须使用命令行界面在虚拟设备上启用 VMware 工具；请参阅《*FireSIGHT 系统虚拟安装指南*》。

要在虚拟防御中心上启用 VMware 工具，请执行以下操作：

访问：管理

步骤 1　选择 **System > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **VMware Tools**。

系统将显示 VMware Tools 页面。

步骤 3　点击 **Enable VMware Tools**，然后点击 **Save**。

已保存您的更改。

许可 FireSIGHT 系统

您可许可各种功能，为贵公司创建最佳 FireSIGHT 系统部署。您可使用防御中心为其本身及其管理的设备管理许可证

有关详情，请参阅：

了解许可

许可证：任何环境

您可许可各种功能，为贵公司创建最佳 FireSIGHT 系统部署。 FireSIGHT 许可证随附于防御中心中，执行主机、应用和用户发现要求使用此许可证。

附加的型号特定许可证可供受管设备执行各种功能，包括：

- 入侵检测和阻止
- 安全情报过滤
- 文件控制和高级恶意软件防护
- 应用、用户和 URL 控制
- 交换和路由
- 设备集群
- 网络地址转换 (NAT)
- 虚拟专用网 (VPN) 部署

有多种方式可能让您失去对 FireSIGHT 系统中许可功能的访问权。可防御中心移除许可证，这将影响其所有受管设备。也可在特定受管设备上禁用已许可的功能。最后，某些许可证可能过期。虽然有一些例外情况，但不能使用与已到期或删除的许可证关联的功能。

有关详情，请参阅：

- 第 65-6 页上的许可 2 系列设备
- 第 65-6 页上的了解 FireSIGHT 主机和用户许可证限制

许可证类型和限制

许可证：任何环境

本节介绍 FireSIGHT 系统部署中可用的许可证类型。可在某设备上启用的许可证取决于其型号、版本和 （对于受管设备）已启用的其他许可证。

对于虚拟和 3 系列 设备，许可证因型号而异；不能在受管设备上启用许可证，除非许可证与设备的型号完全相符。例如，不能使用 3D8250 保护许可证启用 3D8140 设备上的保护功能。随着贵组织和部署的扩展，可为额外的受管设备购买额外的许可证。

2 系列设备自动配有保护功能 （安全情报过滤除外）。虽然不需要在 2 系列设备上明确启用保护，但也不能启用任何其他许可证。

另请注意，尽管可在虚拟设备或 ASA FirePOWER 设备上启用可控性以执行用户和应用控制，但这些设备不支持交换、路由，堆栈或集群。

下表概述了 FireSIGHT 系统许可证。

表 65-1　　FireSIGHT 系统许可证

许可证	平台	授予的功能	需要
FireSIGHT	防御中心s	能源成本	无
保护 （已许可）	3 系列、虚拟设备、 X -系列和 ASA FirePOWER	入侵检测和阻止 文件控制 安全情报过滤	无
保护 （自动）	2 系列	入侵检测和阻止 文件控制	无
可控性	虚拟、 ASA FirePOWER	用户和应用控制	保护
可控性	3 系列	用户和应用控制 交换和路由 集群	保护
恶意软件	3 系列、虚拟、 ASA FirePOWER	高级恶意软件防护 （基于网络的恶意软件检测和拦截）	保护
URL 过滤	3 系列、虚拟设备、 X -系列和 ASA FirePOWER	基于类别和信誉的 URL 过滤	保护
VPN	3 系列	部署虚拟专用网络	可控性

请注意， DC500 防御中心不支持 URL 过滤或恶意软件许可证所提供的功能。

有关详情，请参阅：

- 第 65-3 页上的 FireSIGHT
- 第 65-3 页上的保护
- 第 65-4 页上的可控性
- 第 65-5 页上的恶意软件

- 第 65-4 页上的 URL 过滤
- 第 65-5 页上的 VPN

FireSIGHT

许可证：FireSIGHT

FireSIGHT 许可证随防御中心提供，执行主机、应用和用户发现需要该许可证 发现数据可供系统为网络创建完整且最新的配置文件，并将威胁、终端和网络智能与用户身份信息相关联。可使用发现数据执行流量剖析、评估网络合规性并实施关联策略。

FireSIGHT 许可证还决定可用防御中心及其受管设备可监控的主机和用户数量。请注意，用户限制*独立*适用于以下各项：

- 用户数据库，其中包含 FireSIGHT 系统检测的每个用户的记录
- 在访问控制规则中可用于执行用户控制的用户数量，也称为*访问受控用户*

有关到达许可限制的后果，请参阅第 65-6 页上的了解 FireSIGHT 主机和用户许可证限制。

没有 FireSIGHT 许可证，仍可执行基本系统配置、监控、网络访问控制（区域、网络、 VLAN 和端口规则条件）、连接日志记录和报告。此外，还可从综合安全智能云接收基于终端的恶意软件事件，无需 FireSIGHT 许可证，不过，贵组织确实需要订用 FireAMP。

提示 本指南中的许可声明假设您的防御中心有 FireSIGHT 许可证。但是，如果防御中心之前运行版本 4.10.x，则可使用旧版 RNA 主机和 RUA 用户许可证替代 FireSIGHT 许可证。有关详细信息，请参阅第 65-3 页上的保护。

保护

许可证：保护

受支持的设备：3 系列、虚拟设备、 X -系列和 ASA FirePOWER

保护许可证可用于执行入侵检测和阻止、文件控制和安全情报过滤：

- *入侵检测和阻止*可用于分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。
- *文件*控制可用于检测且或者阻止用户通过特定应用程序协议上传 （发送）或下载 （接收）特定类型的文件。借助于恶意软件许可证 （请参阅第 65-5 页上的恶意软件），还可根据恶意软件布置检查并拦截这些文件类型的有限集。
- *安全情报过滤*可用于在流量将接受访问控制规则的分析之前，拉黑-拒绝源自和进入特定 IP 地址的流量。动态源可用于根据最新智能立即拉黑连接。或者，可将“仅监控”设置用于安全情报过滤。

虽然可以配置访问控制策略以执行保护相关的检查，而无需许可证，但不能应用该策略，直至先添加 保护许可证至防御中心，然后在作为该策略目标的设备上启用它。

如从保护删除防御中心许可证，或在受管设备上禁用保护，防御中心停止确认源自受影响设备的入侵和文件事件。因此，使用这些事件作为触发器条件的关联规则停止开启。此外，防御中心将不会连接互联网获取思科提供的信息或第三方安全情报信息。重新启用保护之前，无法重新应用现有策略。

由于 URL 过滤、恶意软件和可控性许可证需要保护许可证，因此，删除或禁用保护许可证与删除或禁用 URL 过滤、恶意软件或可控性许可证有相同效果。

注　2 系列设备自动配有大多数保护功能；无需为这些设备购买或启用保护许可证。然而， 2 系列设备无法执行安全情报过滤。

可控性

许可证：可控性

受支持的设备：3 系列、虚拟、 ASA FirePOWER

受支持的防御中心：因功能而异

可控性许可证可用于实施用户和应用控制，只需将用户和应用条件添加至访问控制规则。它也可用于配置 3 系列受管设备以执行交换和路由（包括 DHCP 中继和 NAT），以及集群受管设备。要在受管设备上启用可控性，您还必须启用保护。

注　虽然可在虚拟设备、或 ASA FirePOWER 设备启用 可控性许可证，但这些设备**不**支持交换、路由，堆栈或集群。

虽然可向访问控制规则添加用户和应用条件，而无需可控性许可证，但不能应用策略，除非首先添加可控性许可证至防御中心，然后在作为该策略目标的设备上启用它。

请注意， DC500 防御中心不支持在访问控制规则中添加用户条件。

没有可控性许可证，就无法在受管设备上创建交换、路由或混合接口；创建 NAT 条目；或配置虚拟路由器的 DHCP 中继。尽管可创建虚拟交换机和路由器，但没有交换和路由接口来填充它们，它们就没有用。而且，不能向未启用可控性的受管设备应用包括交换或路由的设备配置。此外，在受管设备之间建立集群需要为可控性启用这些设备。

如从可控性删除防御中心许可证，又在单台设备上禁用可控性，受影响设备不会停止执行交换或路由，设备集群也**不会**中断。尽管可编辑和删除现有配置，但不能对受影响设备就应用更改。不能添加新的交换，路由或混合接口，也无法添加新的 NAT 入口、配置 DHCP 中继或建立设备集群。最后，如果现在访问控制策略包含的规则带有用户或应用条件，则无法重新应用该策略。

URL 过滤

许可证：URL 过滤

受支持的设备：3 系列、虚拟设备、 X -系列和 ASA FirePOWER

受支持的防御中心：除 DC500 外的所有型号

URL 过滤可用于编写访问控制规则，以根据受监控主机请求的 URL 确定可横越网络且与这些 URL 的相关信息关联的流量，可通过思科从防御中心云获取该流量。要启用 URL 过滤，您还必须启用保护许可证。

提示　没有 URL 过滤许可证，可指定要许可或拦截的单一 URL 或 URL 组。这将对网络流量进行精细和自定义控制，但是，不允许使用 URL 类别和信誉数据来过滤网络流量。

URL 过滤需要基于订用的 URL 过滤许可证。虽然可添加基于类别和信誉的 URL 条件至访问控制规则，无需 URL 过滤许可证，防御中心将不会联系云获取 URL 信息。只有首先添加 URL 过滤许可证至防御中心，才能应用访问控制策略，然后在该策略针对的设备上启用它。

如从防御中心删除许可证或在受管设备上禁用 URL 过滤，则可能无法访问 URL 过滤。此外，URL 过滤许可证可能过期。如果许可证过期，或如果删除或禁用许可证，带 URL 条件的访问控制规则将立即停止过滤 URL，防御中心再也不能联系云。如果现有访问控制策略包括的规则带有基于类别和信誉的 URL 条件，则不能应用该等策略。

恶意软件

许可证：恶意软件

受支持的设备：3 系列、虚拟、 ASA FirePOWER

受支持的防御中心：除 DC500 外的所有型号

恶意软件许可证可用于执行高级恶意软件防护，也即是说，使用受管设备检测并拦截通过网络传输的文件中的恶意软件。要在受管设备上启用恶意软件，您还必须启用保护。

注 启用了恶意软件许可证的受管设备会定期尝试连接到思科云，即使未配置动态分析。因此，设备的接口流量控制板小组件显示传输的流量；这是预期行为。

配置恶意软件检测作为文件策略的一部分，然后与一个或多个访问控制规则相关联。文件策略可以通过特定应用协议检测用户是否上传或下载特定类型的文件。恶意软件许可证可用于在这些文件类型受限集中检查恶意软件，以及下载并提交特定文件类型至思科云供执行动态和 Spero 分析，以确定其是否包含恶意软件。恶意软件许可证还可用于添加特定文件至文件列表并在文件策略中启用文件列表，从而在检测时自动允许或拦截这些文件。

虽然可添加恶意软件检测文件策略至访问控制规则，而无需恶意软件许可证，在访问控制规则编辑器中，文件策略标有警告图标 ( )。在文件策略中，恶意软件云查找规则也标有警告图标。在可应用包括恶意软件检测文件策略的访问控制策略之前，**必须**添加恶意软件许可证，然后在作为该策略目标的设备上启用它。如果稍后禁用设备上的许可证，而且现有访问控制策略包括的文件策略执行恶意软件检测，则无法向这些设备重新应用现有访问控制策略。

如果删除所有恶意软件许可证或这些许可证全都过期，防御中心停止执行恶意软件云查找，并停止确认从思科云发送的回顾性事件。如果现有访问控制策略包括的文件策略执行恶意软件检测，则将无法重新应用现有访问控制策略。请注意，在恶意软件许可证已过期或被删除后的极短时间内，系统可将缓存布置用于恶意软件云查找文件规则检测的文件。在时窗过期后，系统将向这些文件分配不可用的布置，而不是执行查找。

请注意，只有想要系统检测网络流量中的恶意软件时，才需要 恶意软件 许可证。没有恶意软件许可证，如果贵组织有 FireAMP 订用，则防御中心可从思科云接收基于终端的恶意软件事件。有关详细信息，请参阅第 37-2 页上的了解恶意软件防护和文件控制。

VPN

许可证：VPN

受支持的设备：3 系列

VPN 可用于在终端之间通过公共资源建立安全隧道，例如互联网或其他网络。可配置 FireSIGHT 系统在思科受管设备的虚拟路由器之间构建安全 VPN 隧道。要启用 VPN，您还必须启用保护和可控性许可证。

没有 VPN 许可证，就不能用受管设备配置 VPN 部署。虽然可创建部署，但不用至少启用一个 VPN 的路由接口填充部署，则部署无用。

如从 VPN 删除防御中心许可证，或在每台设备上禁用 VPN，则受影响设备将**不**中断当前 VPN 部署。尽管可编辑和删除现有部署，但不能对受影响设备应用更改。

许可高可用性对。

许可证：任何环境

受支持的防御中心：DC1000、 DC1500、 DC2000、 DC3000、 DC3500 和 DC4000

高可用性对中的防御中心不共享许可证。必须向该对的每个成员应用等效许可证。由于思科根据每个防御中心的唯一许可证密钥生成许可证，因此，不能在不同防御中心上使用相同许可证。

许可堆栈和集群设备

许可证：任何环境

受支持的设备：因功能而异

每台设备只有具备等效许可证才能得以堆栈或集群。堆栈设备后，可更改整个堆栈的许可证。但是，不能在设备集集上更改已启用的许可证。

可以堆栈符合第 4-37 页上的管理堆叠设备中所述要求的 3D8140、 3D8200 系列、 3D8300 系列和相同型号的 3D9900 设备。可集群两台符合 3 系列中所述要求、相同第 4-25 页上的集群设备型号的设备。

许可 2 系列设备

许可证：保护

受支持的设备：2 系列

除外 DC500K，2 系列与 3 系列防御中心许可等效。由于 DC500 不支持 URL 过滤或基于网络的恶意软件检测，因此，无法利用 URL 过滤和恶意软件许可证。

2 系列设备自动配有保护许可证启用的功能，但安全情报除外。不能在 2 系列设备上禁用保护许可证，不能启用其他许可证。

有关详细信息，请参阅以下各节：

- 第 65-2 页上的许可证类型和限制介绍在 FireSIGHT 系统部署中可用的许可证类型。
- 第 1-4 页上的按受管设备型号汇总受支持功能概述 2 系列设备上支持和不支持的功能。

了解 FireSIGHT 主机和用户许可证限制

许可证：FireSIGHT

防御中心上的FireSIGHT 许可证决定了利用防御中心及其受管设备可以监控多少单独的主机和用户以及可以利用多少用户来执行用户控制。 FireSIGHT 主机和用户许可证限制因型号而异，如下表所列。

表 65-2　　按防御中心型号 列出的 FireSIGHT 限制

防御中心 型号	FireSIGHT 主机和用户限制
DC500	1000
DC750	2000
DC1000	20,000

表 65-2　按防御中心型号 （续）列出的 FireSIGHT 限制

防御中心 型号	FireSIGHT 主机和用户限制
DC1500	50,000
DC2000	100,000
DC3000	100,000
DC3500	300,000
DC4000	600,000
虚拟化	50,000

例如，可通过 DC500 监控 1000 台主机和 1000 个用户。

如果防御中心之前运行 4.10.x 版本的 FireSIGHT 系统，且您使用 ISO 文件将设备“恢复”至版本 5.x 出厂默认设置，则可使用旧版 RNA 主机和 RUA 用户许可证替代 FireSIGHT 许可证。

有关详细信息，请参阅：

- 第 65-7 页上的了解 FireSIGHT 主机限制
- 第 65-8 页上的了解 FireSIGHT 用户限制
- 第 65-8 页上的了解访问受控用户限制
- 第 65-3 页上的保护

了解 FireSIGHT 主机限制

许可证：FireSIGHT

FireSIGHT 上的防御中心许可证确定通过防御中心及其受管设备所监控的主机数量，以及因此可在网络映射中可存储的主机数量。

请注意，系统分别从 IP 地址和 MAC 地址识别的主机对仅 MAC 主机进行计数。与一台主机关联的所有 IP 地址均视为一台主机共同计数。

当系统在受监控网络中检测到与具有 IP 地址的主机关联的活动 （由网络发现策略界定）时，该主机将添加至网络映射。

如果到达主机限制，并且系统检测到新主机，新主机是否添加至网络映射取决于网络发现策略中的 **When Host Limit Reached**。可将系统配置为停止添加新主机至数据库，或更换一直处于非活动状态时间最长的主机。

注　即使不能添加新主机至网络映射，系统仍对该主机的网络流量执行访问控制。虽然到达 FireSIGHT 主机限制并不阻止对达到许可限制后发现的主机执行访问控制，但无法查看使用了主机配置文件数据的主机或对其执行分析。例如，不能使用合规性白名单来监视那些主机的网络合规性，或者在主机配置文件限定条件中使用这些主机，等等。

可手动删除主机，整个子网或网络映射中的所有主机。然而，请记住，如果系统检测到与已删除主机关联的活动，它将重新添加该主机至网络映射。

另请注意，如果系统未从网络发现策略中指定的最后一个**主机超时**时段中的主机检测到网络流量，主机从网络映射中移除。默认设置为 10080 分钟 （7 天）。

为了帮助对您的主机许可证进行的使用，当剩下的主机许可证数量少于可配置数量时， FireSIGHT 主机许可证限制运行模式将警告您。

了解 FireSIGHT 用户限制

许可证：FireSIGHT

防御中心中的 FireSIGHT 许可证确定可监控的用户数量。当系统检测到新用户的活动时，该用户将添加至用户数据库。可以通过以下方式检测用户：

- 可使用网络发现策略将受管设备配置为被动检测 LDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP)、 FTP、 HTTP、 MDNS 和 SMTP 用户的登录。
- 可在 Microsoft Active Directory LDAP 服务器上安装 User Agents 以检测对 Active Directory 凭证进行的身份验证。

如果达到许可的限制，多数情况下，系统会停止向数据库添加新用户。要添加新用户，您必须手动从数据库中删除用户，或从数据库清除所有用户。

但是，系统支持授权用户登录。如果达到许可的限制，并且系统检测到之前未检测到用户的授权用户登录，系统删除保持非活动状态时间最长的非授权用户，替换为新用户。

提示 请注意，如在使用受管设备检测用户活动，可按协议限制客户日志记录，以最大程度低减少用户名干扰并保留 FireSIGHT 用户许可证。例如，通过 AIM、 POP3 和 IMAP 发现的监控用户，可添加由于从承包商、访客和其他访客进行网络访问而与贵组织无关的用户。有关详细信息，请参阅第 45-25 页上的限制用户日志记录。

了解访问受控用户限制

许可证：可控性

受支持的设备：3 系列、虚拟、 ASA FirePOWER

防御中心中的 FireSIGHT 许可证不仅确定可监控的用户数量，而且确定可在访问控制规则中用于执行用户控制的用户数量。这些用户称为*访问受控用户*。

注 要执行用户控制，贵组织**必须**使用 Microsoft Active Directory。系统使用在 Active Directory 服务器上运行的 User Agents 将访问受控用户与 IP 地址相关联，这就是允许访问控制规则触发的应用程序。

通过在防御中心与 Active Directory 服务器之间配置连接 （称为*用户意识对象*） ,可以指定访问受控用户必须属于的组。然后，防御中心定期查询服务器，在您在身份验证对象中指定的组中检索用户列表。然后，可使用这些用户执行访问控制。

您**必须**确保在身份验证对象中指定的组中的用户总数少于 FireSIGHT 用户许可证。如果您的参数范围过大，防御中心获取尽量多用户的信息，报告未能在任务队列中检索的用户数量。出于执行和许可原因，思科建议仅指定能代表要在访问控制使用的用户的组。

查看您的许可证

许可证：任何环境

使用 Licenses 页面查看防御中心及其受管设备的许可证。对于您的部署中的每种类型的设备，该页面列出您所拥有的许可证总数以及那些在使用的许可证。

谨记，在此页面，正在使用的 FireSIGHT 用户许可证的数量代表 FireSIGHT 系统检测到的用户数量，也就是用户数据库中的用户数量。它不代表用于执行访问控制的访问受控用户的数量。有关详细信息，请参阅第 65-6 页上的了解 FireSIGHT 主机和用户许可证限制。

Licenses 页面还提供了每个许可证的详细信息。对于每种型号，均可看到您拥有的每种类型许可证的数量，以及用每种类型许可证许可的受管设备数量。针对有期限的许可证，该页面向您提供过期日期。

除了 Licenses 页面之外，还有其他一些方法可用于查看许可证数量和许可限制：

- Product Licensing 控制面板小组件提供了许可证概览。
- Device Management 页面 (**Devices > Device Management**) 列出已应用于每台受管设备的许可证。
- 两个运行模块、许可证监控器和 FireSIGHT 主机许可证限制，在运行策略中使用时传达许可证状态。

要查看许可证，请执行以下操作：

访问：管理

步骤 1　选择 **System > Licenses**。

系统将显示 Licenses 页面。

添加许可证至防御中心

许可证：任何环境

添加许可证至防御中心之前，确保拥有在购买许可证时思科提供的激活密钥。

除了 FireSIGHT，还**必须**在受管设备上启用许可证，才能使用许可的功能。可通过以下两种试启用许可证：在将设备添加至防御中心时，或在添加设备之后编辑设备的一般属性。请注意，因为 2 系列设备自动配有保护功能，除安全情报过滤外，不能禁用这些功能，也无法向 2 系列设备应用其他许可证。请参阅第 65-10 页上的更改设备的已许可功能。

注　如果在备份完成后添加许可证，即使备份恢复，这些许可证不会删除也不会被覆盖。为防止恢复时出现冲突，请在恢复备份之前移除这些许可证，记住许可证使用位置，并在恢复备份之后添加和重新配置它们。如果发生冲突，请与技术支持部门联系。

要添加许可证，请执行以下操作：

访问：管理

步骤 1　选择 **System > Licenses**。

系统将显示 Licenses 页面。

步骤 2　点击 **Add New License**。

系统将显示 Add License 页面。

步骤 3　您是否收到带有许可证的邮件？

- 如果是，从邮件复制许可证，将其粘贴至 **License** 字段，然后点击 **Submit License**。

  如果许可证正确，则许可证添加成功。跳过该步骤的其他部分。

- 否则，点击 **Get License**。

  系统将显示 Licensing Center 网站。如果无法访问 Internet，请切换至可访问 Internet 的计算机。记住页面底部的许可证密钥并浏览至 https://keyserver.sourcefire.com/。

步骤 4　按照屏幕上的说明获取许可证，将通过邮件发送许可证。

提示　在登录支持网站后，还可在 **Licenses** 选项卡上申请许可证。

步骤 5　从邮件复制许可证，将其粘贴至防御中心网络界面中的 **License** 字段，然后点击 **Submit License**。

如果许可证有效，则许可证添加成功。现在，可在受管理设备中启用许可证的功能，如第 65-10 页上的更改设备的已许可功能中所述。

删除许可证

许可证：任何环境

如果由于任何原因需要删除许可证，请执行以下步骤。谨记：因为思科根据每个防御中心的唯一许可证密钥生成许可证，因此，不能从一个防御中心删除许可证，然后在另一个防御中心上重复使用它。

在大多数情况下，删除许可证后，就无法使用该许可证启用的功能。有关详细信息，请参阅第 65-2 页上的许可证类型和限制。

要删除许可证，请执行以下操作：

访问：管理

步骤 1　选择 **System > Licenses**。

系统将显示 Licenses 页面。

步骤 2　在要删除的许可证旁边，点击删除图标 ( )。

如果删除许可证，则将从使用该许可证的所有设备移除已许可的功能。例如，如果您的保护许可证对 100 台受管设备有效且在该等设备上已启用，删除该许可证之后，将从所有 100 台设备移除保护功能。

步骤 3　确认要删除许可证。

许可证删除成功。

更改设备的已许可功能

许可证：任何环境

受支持的设备：3 系列、虚拟设备、 X -系列和 ASA FirePOWER

要更改 3 系列 设备、虚拟设备、用于 Blue Coat X-系列的思科 NGIPS 或 ASA FirePOWER 设备的已许可功能，请在 Device Management 页面编辑设备的一般属性。尽管有一些例外，但如果在受管设备上禁用许可证，就无法使用与该许可证关联的功能。

2 系列 设备自动配有 保护 功能，安全情报过滤除外。不能禁用这些功能，也不能向 2 系列设备应用其他许可证。注意，虽然不能通过 DC500 防御中心使用恶意软件或 URL 过滤许可证，但可使用 DC500 启用或更改 3 系列设备、虚拟设备 用于 Blue Coat X-系列的思科 NGIPS、或 ASA FirePOWER 设备的这些和其他已许可功能。

有关可启用的许可证的详细信息，包括版本、型号和其他要求，请参阅第 65-2 页上的许可证类型和限制。

要启用或禁用设备的已许可功能，请执行以下操作：

访问：管理员/网络管理员

步骤 1　选择 **Devices > Device Management**。

系统将显示 Device Management 页面。

步骤 2　在要启用或禁用许可证的设备旁，单击编辑图标 ( )。

系统将显示该设备的 Interfaces 选项卡。

步骤 3　点击 **Device**。

系统将显示 Device 选项卡。

步骤 4　点击 License 部分旁边的编辑图标 ( )。

系统将显示 License 弹出窗口。

步骤 5　清除或选择相应的复选框以启用或禁用设备的已许可功能。

步骤 6　单击 **Save**。

更改保存成功，但只有应用设备配置，更改才能生效；请参阅第 4-22 页上的对设备应用更改。

更新系统软件

思科以电子形式分配多种不同类型的更新，其中包括系统软件本身的主要和次要更新、规则更新、地理定位数据库 (GeoDB) 更新以及漏洞数据库 (VDB) 更新。

注意事项 本章包含有关更新 FireSIGHT 系统的一般信息。在更新 FireSIGHT 系统的任何部分 （包括包括 VDB、 GeoDB 或入侵规则）之前，**必须**阅读更新随附的版本说明或建议性文本。版本说明提供重要信息，包括支持的平台、兼容性、先决条件、警告以及具体安装和卸载说明。

除非版本说明或建议性文本另有说明，否则，更新设备不会修改其配置；设备设置将保持不变。

有关详细信息，请参阅：

了解更新类型

许可证：任何环境

思科以电子形式分配多种不同类型的更新，其中包括系统软件本身的主要和次要更新、入侵规则更新和 VDB 更新。

下表介绍了思科提供的更新类型。对于大多数更新类型，可以安排下载和安装；请参阅第 62-1 页上的安排任务和第 66-16 页上的使用周期性规则更新。

表 66-1 FireSIGHT 系统更新类型

更新类型	说明	安排？	卸载？
FireSIGHT 系统的补丁	补丁包括数量有限的修补程序 （通常更改版本号中的第四位数字；例如， 5.4.0.1）。	是	是
FireSIGHT 系统的功能更新	功能更新比补丁更全面，通常包括新功能 （通常更改版本号中的第三位数字；例如， 5.4.1）。	是	是

表 66-1　FireSIGHT 系统更新类型

更新类型	说明	安排？	卸载？
FireSIGHT 系统的主要更新（主要和次要版本发布）。	主要更新 （有时称为升级）包括新功能，并且可能需要对产品进行大规模更改 （通常改变版本号中的第一位或第二位数字；例如， 5.3 或 5.4）。	否	否
VDB	VDB 更新会影响 FireSIGHT 系统报告的漏洞以及检测到的操作系统、应用和客户端。	是	否
入侵规则	入侵规则更新提供新的和更新后的入侵规则和预处理器规则、现有规则的修改后状态以及修改后的默认入侵策略设置。规则更新还可以删除规则，提供新规则类别和默认变量，以及修改默认变量值。	是	否
地理定位数据库 (GeoDB)	GeoDB 提供有关系统可通过可路由 IP 地址与之关联的物理位置、连接类型等等方面的更新信息。地理定位数据可用作访问控制规则中的条件。必须安装 GeoDB 才能查看地理定位详细信息。 DC500 防御中心不支持此功能。	是	否

请注意，可以卸载 FireSIGHT 系统的补丁和其他次要更新，但不能卸载主要更新，也不能恢复到 VDB、 GeoDB 或入侵规则的上一版本。如果已将设备更新为 FireSIGHT 系统新的主要版本，但需要恢复为旧版本，请联系支持部门。

进行软件更新

许可证：任何环境

更新 FireSIGHT 系统部署有一些基本步骤。首先，**必须**为更新做好准备，包括阅读版本说明以及完成必要的更新前任务。然后，开始更新 - 首先更新防御中心，然后更新其管理的设备。必须监控更新进度直至更新完成，然后验证更新是否成功。最后，完成必要的更新后步骤。

有关详细信息，请参阅：

- 第 66-2 页上的制定更新计划
- 第 66-4 页上的了解更新过程
- 第 66-6 页上的更新 防御中心
- 第 66-8 页上的更新受管设备
- 第 66-9 页上的监控主要更新状态

制定更新计划

许可证：任何环境

开始更新之前，必须仔细阅读并理解版本说明 （可从支持网站下载）。版本说明介绍支持的平台、新功能、已知问题、已解决的问题以及产品兼容性。版本说明还包含有关先决条件、警告以及具体安装和卸载说明的重要信息。

以下各节概述了制定更新计划时必须考虑的一些因素。

FireSIGHT 系统版本要求

必须确保设备（包括基于软件的设备）运行的是正确的 FireSIGHT 系统版本。版本说明指明所需的版本。如果运行的是早期版本，可从支持网站获取更新。

操作系统要求

确定安装了基于软件的设备的计算机运行的是正确的操作系统版本。版本说明指明所需的版本。有关虚拟设备支持的操作系统的详细信息，请参阅 *FireSIGHT 系统虚拟安装指南*。有关用于 Blue Coat X-系列的思科 NGIPS 支持的操作系统的详细信息，请参阅 《*用于 Blue Coat X-系列的思科 NGIPS 安装指南*》。

时间和磁盘空间要求

确定有足够的可用磁盘空间并且更新时间足够。更新受管设备时，要求防御中心上有额外磁盘空间。版本说明指明磁盘空间和时间方面的要求。

配置和事件备份准则

开始主要更新之前，思科建议删除设备上已复制到外部位置的所有备份。此外，不管更新类型如何，都应该将当前事件和配置数据备份到外部位置。更新过程中不会备份事件数据。

防御中心可用于备份其自身的及其管理的设备的事件和配置数据；请参阅第 70-1 页上的使用备份和恢复。

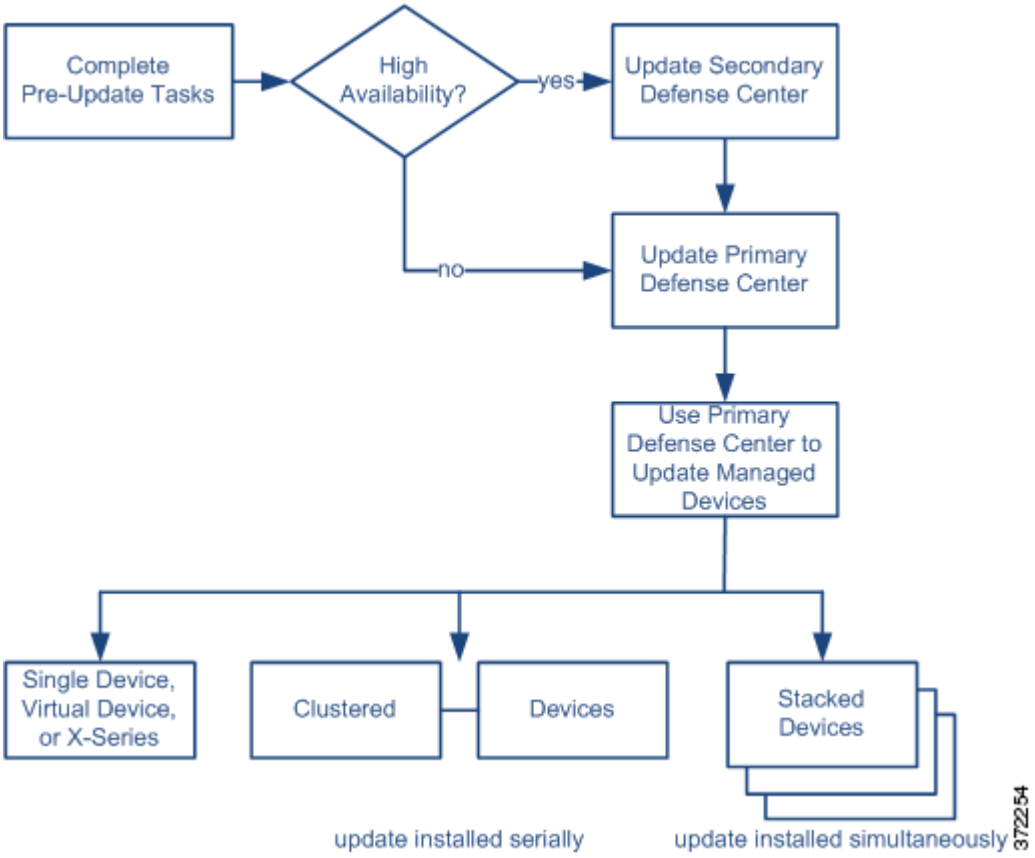
何时进行更新

由于更新过程可能会影响流量检查、流量和链路状态，而且数据相关器在更新过程中处于禁用状态，因此，思科建议在维护窗口中或者中断对部署造成的影响最小时进行更新。

了解更新过程

许可证：任何环境

下图总结了更新过程。



更新顺序

必须先更新防御中心，再更新其管理的设备。

使用防御中心进行更新

思科建议使用防御中心的网络界面更新其本身以及其管理的设备。**必须**使用防御中心更新没有网络界面的受管设备，例如虚拟设备和用于 Blue Coat X-系列的思科 NGIPS。对用于 Blue Coat X-系列的思科 NGIPS进行主要更新时，可能需要卸载其旧版本并安装新版本。有关详细信息，请参阅《*用于 Blue Coat X-系列的思科 NGIPS 安装指南*》。

Product Updates 页面 (**System > Updates**) 显示每项更新的版本以及更新的生成日期和时间。此外，该页面还指明更新过程中是否需要重新启动。

将从支持部门获得的更新上传到设备后，这些更新会显示在该页面中。该页面还显示补丁和功能更新的卸载程序；请参阅第 66-10 页上的卸载软件更新。在防御中心上，该页面可能列出 VDB 更新。

提示 对于补丁和功能更新，可以利用自动更新功能；请参阅第 62-10 页上的自动执行软件更新。

更新成对防御中心

开始更新高可用性对中的一个防御中心时，如果它尚未就绪，另一个防御中心将会变为主防御中心。此外，成对防御中心将会停止共享配置信息；成对防御中心在常规同步过程不会接收软件更新。

为确保操作的连续性，请**勿**同时更新成对防御中心。首先，完成辅助防御中心的更新过程，再更新主防御中心。

更新集群设备

在集群设备或集群堆栈上安装更新时，系统会逐一在每台设备或堆栈上进行更新。更新开始后，系统首先将更新应用到备份设备或堆栈；此时，备份设备或堆栈会进入维护模式，当有必要的进程重新启动后，备份设备或堆栈会重新开始处理流量。然后，系统以同样的方式将更新应用到活动设备或堆栈。

要更新集群堆栈中的设备，必须同时更新所有集群成员上的管理防御中心；不能直接从设备进行更新设备。

更新堆叠设备

在堆叠设备上安装更新时，系统同时进行更新。更新完成后，设备恢复正常运行。请注意：

- 如果主设备*先于*所有辅助设备完成更新，在所有设备完成更新之前，堆栈以受限的混合版本状态运行。
- 如果主设备*晚于*所有辅助设备完成更新，堆栈在主设备完成更新后恢复正常运行。

流量和检查

从受管设备安装或卸载更新时，以下功能可能会受到影响：

- 流量检查，包括应用和用户感知与控制、 URL 过滤、安全情报过滤、入侵检测与防御以及连接日志记录
- 流量，包括交换、路由及相关功能
- 链路状态

数据相关器在系统更新期间不运行。更新完成后，它会恢复正常运行。

网络流量中断的方式和持续时间取决于受更新影响的 FireSIGHT 系统的组件、设备的配置和部署方式，以及更新是否会重新启动设备。有关特定更新如何和何时影响网络流量的详细信息，请参阅版本说明。

提示　更新集群设备时，系统一次更新一台设备，以避免流量中断。

在更新过程中使用网络界面

不管更新类型如何，请**勿**在进行更新时使用设备的网络界面执行除监控更新以外的任何其他任务。

为避免在主要更新期间使用设备，并方便监控主要更新进度，系统简化了设备的网络界面。可在任务队列 (**System > Monitoring > Task Status**) 中监控次要更新进度。尽管在进行次要更新时可以使用网络界面，但思科并不建议这样做。

提示　要监控防御中心的受管设备的更新，可使用防御中心上的任务队列。

即使对于次要更新，进行更新时也可能无法使用正在更新的设备的网络界面，或者设备可能会注销您的登录。这是预期行为。如果出现这种情况，请再次登录以查看任务队列。如果仍在进行更新，**必须**避免使用网络界面，直至更新完成。请注意，在更新过程中，受管设备可能会重新启动两次；这也是预期行为。

注意事项　如果更新出现问题（例如，网络界面显示更新失败；再如，手动刷新任务队列或 Update Status 页面后不显示进度），请**勿**重新开始更新。在这种情况下，请联系支持部门。

更新后

必须完成版本说明中列出的所有更新后任务，以确保部署正常运行。

最重要的更新后任务是重新应用访问控制策略，在更新防御中心及其受管设备后需要分别执行这个步骤。请注意，应用访问控制策略可能会造成短暂停止流量和处理，还可能会导致遗漏检查一些数据包；请参阅第 12-13 页上的应用访问控制策略。

此外，还应：

- 确认更新是否成功。
- 确保部署中的所有设备都能够成功通信
- 如有必要，更新入侵规则、 VDB 和 GeoDB
- 根据版本说明中的信息更改任何必要的配置
- 进行版本说明中列出的任何其他更新后任务

更新 防御中心

许可证：任何环境

可使用以下两种方法之一来更新防御中心，具体取决于更新类型以及防御中心能否访问互联网：

- 如果防御中心能访问互联网，可使用防御中心直接从支持网站获取更新。这种方法**不**适用于主要更新。
- 可手动从支持网站下载更新，然后将更新上传到防御中心。如果防御中心不能访问互联网或者要进行主要更新，可采用这种方法。

注意事项　为确保操作的连续性，请**勿**同时更新成对防御中心；请参阅第 66-5 页上的更新成对防御中心。

对于主要更新，更新防御中心会删除之前更新的卸载程序。

更新防御中心

访问：管理

步骤 1　阅读版本说明并完成必要的更新前任务。

更新前任务包括确保防御中心运行的是正确的思科软件版本，确保有足够的可用磁盘空间进行更新，确保预留了足够时间来进行更新，确保已经备份事件和配置数据，等等。

步骤 2　将更新上传到防御中心。您有两种选择，具体取决于更新类型以及防御中心能否访问互联网：

- 对于主要更新以外的所有其他更新，如果防御中心能访问互联网，请选择 **System > Updates**，然后点击 **Download Updates** 以检查最新更新。对于主要更新，或者，如果防御中心无法访问互联网，您必须首先手动下载更新。从以下任何一个支持网站下载更新：

  - **对于所有 Sourcefire 更新：**(https://support.sourcefire.com/)
  - **对于思科更新：**

    物理防御中心
    (http://software.cisco.com/download/navigator.html?mdfid=278875421)
    虚拟防御中心_
    (http://software.cisco.com/download/type.html?mdfid=286259687&catid=null)

- 选择 **System > Updates**，然后点击 **Upload Update**。浏览到更新并点击 **Upload**。

注　可直接从支持网站下载更新 （手动下载，或者点击 Product Updates 选项卡上的 **Download Updates** 进行下载）。如果通过邮件传输更新文件，可能会损坏更新文件。

更新成功上传到防御中心。

步骤 3　确定部署中的设备可成功通信，且运行状况监控器没有报告任何问题。

步骤 4　选择 **System > Monitoring > Task Status** 以查看任务队列，并确定没有作业正在执行。

正在运行的任务会在更新开始时停止，不得恢复这些任务；必须在更新完成后手动将这些任务从任务队列删除。任务队列每 10 秒钟自动刷新一次。必须等到所有长时间运行的任务都完成后，才能开始更新。

步骤 5　选择 **System > Updates**。

系统将显示 Product Updates 页面。

步骤 6　点击上传的更新旁边的安装图标。

系统将显示 Install Update 页面。

步骤 7　选择防御中心并点击 **Install**。如果出现提示，请确认是否要安装更新并重新启动防御中心。

更新过程开始。监控更新的方式取决于更新是主要更新还是次要更新。请参阅 FireSIGHT 系统更新类型表和版本说明来确定更新类型：

- 对于次要更新，可在任务队列 (**System > Monitoring > Task Status**) 中监控更新进度。
- 对于主要更新，可在任务队列中监控更新进度。但是，在防御中心完成必要的更新前检查后，系统会注销您的登录。当您重新登录时，系统会显示 Upgrade Status 页面。有关信息，请参阅第 66-9 页上的监控主要更新状态。

注意事项　不管更新类型如何，请**勿**在更新完成前使用网络界面执行除监控更新以外的任何其他任务；如有必要，防御中心会重新启动。有关详细信息，请参阅第 66-5 页上的在更新过程中使用网络界面。

步骤 8　更新完成后，若有必要，登录防御中心。

在完成主要更新后，如果是第一次登录，可能会显示最终用户许可证协议 (EULA)。必须阅读并接受 EULA 才能继续。

步骤 9　清除浏览器缓存并强制浏览器重新加载。否则，用户界面可能会出现意外行为。

步骤 10　选择 **Help > About** 并确认所列软件版本是否正确。另请注意防御中心上的规则更新和 VDB 的版本；稍后需要使用这些信息。

步骤 11　验证所有受管设备都能够成功地与防御中心进行通信。

步骤 12　如果支持网站上的可用规则更新比防御中心上的规则新，请导入最新的规则。

有关详细信息，请参阅第 66-13 页上的导入规则更新和本地规则文件。

步骤 13　重新应用访问控制策略。

应用访问控制策略可能会造成短暂停止流量和处理，还可能会导致遗漏检查一些数据包。有关详细信息，请参阅第 12-13 页上的应用访问控制策略。

步骤 14　如果支持网站上的可用 VDB 比防御中心上的 VDB 新，请安装最新的 VDB。

安装 VDB 更新会导致短暂停止流量和处理，还可能会导致遗漏检查一些数据包。有关详细信息，请参阅第 66-12 页上的更新漏洞数据库。

步骤 15　进入下一节 （更新受管设备），更新思科管理的设备上的防御中心软件。

更新受管设备

许可证：任何环境

思科建议使用更新后的防御中心来更新其管理的设备。**必须**使用防御中心更新没有网络界面的受管设备，例如虚拟设备和用于 Blue Coat X-系列的思科 NGIPS。对用于 Blue Coat X-系列的思科 NGIPS进行主要更新时，可能需要卸载其旧版本并安装新版本。

更新受管设备分两步进行：首先，从以下任何一个支持网站下载更新，并将更新上传到管理防御中心：

- **Sourcefire：**(https://support.sourcefire.com/)
- **思科：**(http://www.cisco.com/cisco/web/support/index.html)

接着，安装软件。

注　在更新过程中，流量检查、流量和链路状态可能会受到影响，具体取决于设备的配置和部署方式、受更新影响的组件以及更新时是否会重新启动设备。有关特定更新如何和何时影响网络流量的详细信息，请参阅更新的版本说明。

要更新受管设备，请执行以下操作：

访问：管理

步骤 1　阅读版本说明并完成必要的更新前任务。

更新前任务可能包括更新管理防御中心，备份事件和配置数据，以及确保满足以下条件：设备运行的是正确的思科软件版本；安装了基于软件的设备的计算机运行的是正确的操作系统版本；有足够的可用磁盘空间进行更新；有足够的时间进行更新；等等。

步骤 2　更新设备的管理防御中心上的 FireSIGHT 系统软件；请参阅第 66-6 页上的更新 防御中心。

步骤 3　从以下任何一个支持网站下载更新：

- **对于所有 Sourcefire 更新：**(https://support.sourcefire.com/)
- **对于思科更新：**

物理受管设备：(http://software.cisco.com/download/navigator.html?mdfid=278875421)
虚拟受管设备：(http://software.cisco.com/download/type.html?mdfid=286259690&flowid=70802)
不同的设备型号可能使用不同的最新。有关可下载的更新的信息，请参阅版本说明。

注　可直接从支持网站下载更新。如果通过邮件传输更新文件，可能会损坏更新文件。

步骤 4　确定部署中的设备可成功通信，且运行状况监控器没有报告任何问题。

步骤 5　在管理防御中心上，选择 **System > Updates**。

系统将显示 Product Updates 页面。

步骤 6　点击 **Upload Update** 以浏览到下载的最新，然后点击 **Upload**。

更新成功上传到防御中心。 Product Updates 选项卡显示刚上传的更新的类型以及更新的生成日期和时间。此外，该页面还指明更新过程中是否需要重新启动。

步骤 7　点击要安装的更新旁边的安装图标。

系统将显示 Install Update 页面。

步骤 8　选择要安装最新的设备，然后点击 **Install**；可以同时安装多个使用相同更新的设备。如果出现提示，请确认是否要安装更新并重新启动设备。

更新过程开始。在所有设备上安装更新可能需要一些时间，具体取决于文件大小。可在防御中心的任务队列 (**System > Monitoring > Task Status**) 中监控更新进度。请注意，在更新过程中，受管设备可能会重新启动两次；这是正常现象。

注意事项　如果更新出现问题 （例如，任务队列指出更新失败；再如，手动刷新任务队列后不显示进度），请**勿**重新开始更新。在这种情况下，请联系支持部门。

步骤 9　如有需要，完成主要更新后，可登录设备的本地网络界面。

在完成主要更新后，如果是第一次登录，可能会显示最终用户许可证协议 (EULA)。必须阅读并接受 EULA 才能继续。请注意，如果第一次登录是通过命令行界面而非网络界面进行的，也可能显示 EULA；必须接受 EULA。

步骤 10　在防御中心上，选择 **Devices > Device Management**，并确认更新的设备是否列出正确的版本。

步骤 11　验证更新的设备能够成功地与防御中心进行通讯。

步骤 12　重新应用访问控制策略。

应用访问控制策略可能会造成短暂停止流量和处理，还可能会导致遗漏检查一些数据包。有关详细信息，请参阅第 12-13 页上的应用访问控制策略。

监控主要更新状态

许可证：任何环境

对于主要更新， FireSIGHT 系统提供有简化的网络界面，以方便监控更新过程。这个简化界面还可防止使用网络界面来执行除监控更新以外的任何其他任务。

可在任务队列 (**System > Monitoring > Task Queue**) 中监控更新进度。但是，在设备完成必要的更新前检查后，系统会将您及所有其他用户从网络界面注销。只有管理员或维护人员方才可以在更新完成前重新登录。

当管理员重新登录时，会出现简化的更新页面。

如果要使用防御中心更新受管设备，思科建议从防御中心的任务队列监控更新进度。但请注意，在设备完成必要的更新前检查后，登录设备的本地网络界面时会出现简化的更新页面，可使用该更新页面监控更新进度。

该页面显示FireSIGHT 系统更新前的版本、更新后的版本以及自更新开始以来已过去的时间。此外，该页面还显示进度条并提供有关当前运行的脚本的详细信息。

提示　点击 **show log for current script** 可查看更新日志。点击 **hide log for current script** 可隐藏更新日志。

如果出于任何原因更新失败，页面会显示错误消息，其中指明失败的时间和日期、更新失败时正在运行的脚本，并提供有关如何联系支持部门的说明。请**勿**重新开始更新。

注意事项　如果更新出现任何其他问题 （例如，手动刷新页面后很长时间都没有显示进度），请**勿**重新开始更新。在这种情况下，请联系支持部门。

更新完成后，设备显示成功消息并重新启动。设备重新启动后，请刷新页面进行登录，并完成必要的更新后步骤。

卸载软件更新

许可证：任何环境

将补丁或功能更新应用到思科设备时，更新过程中会创建卸载程序；可通过设备的网络界面使用该卸载程序从设备移除更新。

卸载更新时，产生的思科软件版本取决于设备的更新路径。例如，假设您直接将设备从版本 5.0 更新为版本 5.0.0.2。卸载版本 5.0.0.2 补丁可能会产生运行版本 5.0.0.1 的设备，尽管您从未安装版本 5.0.0.1 更新。有关卸载更新时产生的思科软件版本的信息，请参阅版本说明。

注　主要更新不支持从网络界面卸载。如果已将设备更新为 FireSIGHT 系统新的主要版本，但需要恢复为旧版本，请联系支持部门。

卸载顺序

卸载顺序与安装顺序刚好相反。也就是说，先卸载受管设备，再卸载防御中心。

使用本地网络界面卸载更新

必须使用本地网络界面卸载更新；不得使用防御中心从受管设备卸载更新。有关从没有本地网络接口的设备 （例如，虚拟设备或用于 Blue Coat X-系列的思科 NGIPS）卸载补丁的信息，请参阅版本说明。

请注意，尽管这种方法可用于卸载用于 Blue Coat X-系列的思科 NGIPS的次要更新，但不得用于从 X -系列平台卸载用于 Blue Coat X-系列的思科 NGIPS 应用。有关详细信息，请参阅 《*用于 Blue Coat X-系列的思科 NGIPS安装指南*》。

从集群设备或成对设备卸载更新

集群设备和高可用性对中的防御中心必须运行同一版本的 FireSIGHT 系统。尽管卸载过程会触发自动故障转移，错配的对或集群中的设备不会共享配置信息，也不会在同步过程中安装或卸载更新。如果需要从冗余设备卸载更新，应紧接着上一个过程进行。

如果卸载导致这些设备恢复为不支持集群堆栈的旧版本，将无法从集群堆栈中的设备卸载更新。

为确保操作的连续性，请逐一从集群设备和成对防御中心卸载更新。首先，从辅助设备卸载更新。等待卸载过程完成，然后立即从主设备卸载更新。

注意事项 如果集群设备或成对防御中心的更新卸载失败，请**勿**重新开始卸载或更改其对等设备上的配置。在这种情况下，请联系支持部门。

从堆叠设备卸载更新

堆栈中的所有设备必须运行同一版本的 FireSIGHT 系统。从任何堆叠设备卸载更新会导致该堆栈中的设备进入受限的混合版本状态。

为最大程度减轻对部署的影响，思科建议同时从所有堆叠设备卸载更新。堆栈中所有设备的更新完成，堆栈会恢复正常运行。

如果卸载导致这些设备恢复为不支持集群堆栈的旧版本，将无法从集群堆栈中的设备卸载更新。

流量和检查

从受管设备卸载更新可能会影响流量检查、流量和链路状态。有关特定更新如何和何时影响网络流量的详细信息，请参阅版本说明。

卸载后

更新卸载完毕后，可采取几个步骤来确保部署正常运行。这些步骤包括验证卸载是否成功以及部署中的所有设备是否能够成功地进行通信。有关每项更新的详细信息，请参阅版本说明。

要使用本地网络界面卸载补丁或功能更新，请执行以下操作：

访问：管理

步骤 1 选择 **System > Updates**。

系统将显示 Product Updates 页面。

步骤 2 点击要移除的更新的卸载程序旁边的安装图标。

- 在 防御中心上， Install Update 页面显示。选择防御中心并点击 **Install**。
- 在受管设备上，不会显示干预页面。

在这两种情况下，如果出现提示，都需要确认是否要卸载更新并重新启动设备。

卸载过程开始。可在任务队列 (**System > Monitoring > Task Status**) 中监控查询进度。

注意事项 在卸载完成之前，请**勿**使用网络界面执行除监控更新以外的任何其他任务；如有必要，设备会重新启动。有关详细信息，请参阅第 66-5 页上的在更新过程中使用网络界面。

步骤 3 卸载完成后，若有必要，登录设备。

步骤 4 清除浏览器缓存并强制浏览器重新加载。否则，用户界面可能会出现意外行为。

步骤 5 选择 **Help > About** 并确认所列软件版本是否正确。

步骤 6 验证卸载了补丁的设备是否能够成功地与其受管设备 （对于防御中心）或其管理防御中心 （对于受管设备）进行通信。

更新漏洞数据库

许可证：任何环境

思科漏洞数据库 (VDB) 收集了可能影响主机的已知漏洞以及操作系统指纹、客户端指纹和应用指纹。 FireSIGHT 系统会将指纹与漏洞关联起来，以帮助确定特定主机是否会增加网络泄密的风险。思科漏洞研究团队 (VRT) 定期发布 VDB 更新。

要更新 VDB，请使用防御中心上的 Product Updates 页面。将从支持部门获得的 VDB 更新上传到设备后，这些更新以及 FireSIGHT 系统更新和卸载程序更新都会显示在该页面中。

更新漏洞映射所需的时间取决于网络映射中主机的数量。您可能想将更新安排在系统不繁忙的时间进行，以最大程度减少系统停机造成的影响。一般来说，可以用网络上主机的数量除以 1000 来确定进行更新的适当时间。

注　VDB 中更新的应用检测器和操作系统指纹需要重新应用访问控制策略，才能生效。在完成 VDB 更新后，将所有过时的访问控制策略重新应用于受管设备。请记住安装 VDB 或重新应用访问控制策略可能导致受管设备上的流量传输和处理短时间暂停，还可能导致一些数据包未经检查就通过。有关详细信息，请参阅第 12-13 页上的应用访问控制策略。

本节说明如何计划和执行手动 VDB 更新。可使用自动更新功能来安排 VDB 更新；请参阅第 62-14 页上的自动更新漏洞数据库。

要更新漏洞数据库，请执行以下操作：

访问：管理

步骤 1　阅读适用于具体更新的 VDB 更新建议性文本。

建议性文本包括有关在更新过程中对 VDB 所做更改的信息以及产品兼容性信息。

步骤 2　选择 **System > Updates**。

系统将显示 Product Updates 页面。

步骤 3　将更新上传到防御中心：

- 如果防御中心能够访问互联网，请点击 **Download Updates** 以检查以下任何一个支持网站上的最新更新：
  - **Sourcefire：**(https://support.sourcefire.com/)
  - **思科：**(http://www.cisco.com/cisco/web/support/index.html)
- 如果防御中心不能访问互联网，请手动从以下任何一个支持网站下载更新，然后点击 **Upload Update**。浏览到更新并点击 **Upload**：
  - **Sourcefire：**(https://support.sourcefire.com/)
  - **思科：**(http://www.cisco.com/cisco/web/support/index.html)

注　可直接从支持网站下载更新 （手动下载，或者点击 **Download Updates**）。如果通过邮件传输更新文件，可能会损坏更新文件。

更新成功上传到防御中心。

步骤 4　点击 VDB 更新旁边的安装图标。

系统将显示 Install Update 页面。

步骤 5　选择防御中心，然后点击 **Install**。

更新过程开始。安装更新可能需要一些时间，具体取决于网络映射中主机的数量。可在任务队列 (**System > Monitoring > Task Status**) 中监控更新进度。

注意事项　在完成更新之前，请**勿**使用网络界面执行与映射的漏洞相关的任务。如果更新出现问题 （例如，任务队列指出更新失败；再如，手动刷新任务队列后不显示进度），请**勿**重新开始更新。在这种情况下，请联系支持部门。

步骤 6　更新完成后，选择 **Help > About** 确认 VDB 内部版本号是否与安装的更新相匹配。

必须重新应用所有过时的访问控制策略，VDB 更新才会生效；请参阅第 12-13 页上的应用访问控制策略。

导入规则更新和本地规则文件

许可证：任何环境

随着发现新漏洞，思科研究团队 (VRT) 发布规则更新，您可以首先将该规则更新导入防御中心，然后通过应用受影响的访问控制、网络分析和入侵策略到受管设备来实施该规则更新。

规则更新是累加性的，并且思科建议您始终导入最新的更新。不能导入与当前安装的规则的版本匹配或早于该版本的规则更新。如果您的部署包括防御中心的高可靠性对，请仅在主防御中心上导入更新。辅助防御中心会在常规同步过程中接收规则更新。

注　规则更新可能包含新的二进制文件，因此，请确保您的下载和安装过程符合您的安全策略。此外，规则更新可能很大，请确保在网络使用较少的时段导入规则。

规则更新可能提供以下内容：

- **新的和修改的规则和规则状态** - 规则更新提供新的和更新的入侵和预处理器规则。对于新的规则，每个系统提供的入侵规则中的规则状态可能不同。例如，某个新规则在 Security over Connectivity 入侵策略中可能是启用状态，在 Connectivity over Security 入侵策略中则可能是禁用状态。规则更新也可以更改现有规则的默认状态，或者完全删除现有规则。
- **新规则类别** - 规则更新可能包括新规则类别，总是添加。
- **修改的预处理程序和高级设置** - 设置更新可能更改系统提供的入侵策略中的高级设置以及系统提供的网络分析策略中的预处理器设置。它们也可以更新访问控制策略中的高级预处理和性能选项。
- **新的和修改的变量** - 规则更新可能修改现有默认变量的默认值，但是，这并不会覆盖您的更改。总是会添加新变量。

理解规则更新何时修改策略

规则更新可能影响系统提供和自定义网络分析策略，以及所有访问控制策略：

- **系统提供** - 对系统提供的网络分析和入侵策略的更改，以及对高级访问控制设置的所有更改，将在您更新后重新应用策略时自动生效。
- **自定义** - 因为每个自定义网络分析和入侵策略使用系统提供的策略作为其基础，或作为策略链中的事件基础，规则更新可能会影响自定义网络分析和入侵策略。但是，您可以阻止规则更新自动执行这些更改。这使您能够根据独立于规则更新导入的计划手动更新系统提供的基本策

略。无论您的选择（在每个自定义策略基础上实施），对统提供的策略的更新**不会**覆盖您自定义的设置。有关详细信息，请参阅第 24-4 页上的允许规则更新修改系统提供的基本策略。

请注意，导入规则更新会丢弃所有网络分析和入侵策略的已缓存更改。为了方便起见， Rule Updates 页面列出了包含已缓存更改的策略以及做出这些更改的用户。有关详细信息，请参阅第 23-13 页上的解决冲突和提交策略更改。

重新应用策略

要使规则更新所做的更改生效，必须重新应用所有修改的策略。在导入规则更新时，您可以配置系统自动重新应用入侵或访问控制策略到其目标设备。如果允许规则更新修改系统提供的基本策略，这种方法尤其有用。

- 重新应用访问控制策略也重新应用关联的 SSL、网络分析和文件策略，但**不**重新应用入侵策略。还会更新所有修改的高级设置的默认值。由于您无法独立应用网络分析策略，因此如果要更新网络分析策略中的预处理器设置，**必须**重新应用访问控制策略。
- 重新应用入侵策略允许您更新规则和其他更改的入侵策略设置。您可以同时重新应用入侵策略和访问控制策略，也可以仅应用入侵策略，从而更新入侵规则不更新任何其他访问控制配置。

如果规则更新包含共享对象规则，在导入规则后首次应用访问控制或入侵策略会导致流量和处理暂时停止，还可能导致遗漏检查一些数据包。有关应用访问控制和入侵策略的详细信息，包括要求、其他影响和建议，请参阅第 12-13 页上的应用访问控制策略。

有关导入规则更新的详细信息，请参阅：

- 第 66-14 页上的使用一次性规则更新说明如何从支持网站导入单个规则更新。
- 第 66-16 页上的使用周期性规则更新说明如何使用网络界面上的自动功能从支持网站下载和安装规则更新。
- 第 66-17 页上的导入本地规则文件说明如何导入在本地计算机上创建的标准文本规则文件的副本。
- 第 66-19 页上的查看规则更新日志说明规则更新日志。

使用一次性规则更新

许可证：任何环境

有两种方法可使用一次性规则更新：

- 第 66-14 页上的使用手动一次性规则更新说明如何从支持网站将规则更新手动下载到本地计算机，然后手动安装规则更新。
- 第 66-15 页上的使用自动一次性规则更新说明如何使用网络界面上的自动功能从支持网站搜索并上传新的规则更新。

使用手动一次性规则更新

许可证：任何环境

以下步骤说明如何手动导入新的规则更新。如果防御中心不能访问互联网，这种方法尤其有用。

要手动导入规则更新，请执行以下操作：

访问：管理

步骤 1　从可访问互联网的计算机访问以下任何一个网站：

- **Sourcefire**：(https://support.sourcefire.com/)
- **思科**：(http://www.cisco.com/cisco/web/support/index.html)

步骤 2　点击 **Download**，然后点击 **Rules**。

步骤 3　浏览到最新的规则更新。

规则更新是累积的；您无法导入匹配发布日期与当前安装的规则相同或更早的规则更新。

步骤 4　点击要下载的规则更新文件并保存到计算机。

步骤 5　登录到设备的网络界面。

步骤 6　选择 **System > Updates**，然后选择 **Rule Updates** 选项卡。

系统将显示 Rule Updates 页面。

提示　也可以点击 Rule Editor 页面 (**Policies > Intrusion > Rule Editor**) 上的 **Import Rules**。

步骤 7　或者，依次点击 **Delete All Local Rules** 和 **OK**，以将创建或导入的所有用户定义规则移到被删除的文件夹。有关详情，请参见第 36-97 页上的删除自定义规则。

步骤 8　选择 **Rule Update or text rule file to upload and install**，然后点击 **Choose File** 以浏览并选择规则更新文件。

步骤 9　或者，在更新完成后，重新对受管设备应用策略：

- 选择 **Reapply intrusion policies after the rule update import completes** 以自动重新应用入侵策略。仅选择此选项更新规则和其他已更改的入侵策略设置，无需更新您进行的所有其它访问控制配置。您**必须**选择此选项与访问控制策略一起重新应用入侵策略；重新应用访问控制策略在这种情况下不执行全面的应用。
- 选择 **Reapply access control policies after the rule update import completes** 以自动重新应用访问控制策略及其关联的 SSL、网络分析和文件策略，但不重新应用入侵策略。选择此选项也更新所有修改的访问控制高级设置的默认值。由于您无法独立于其父访问控制策略应用网络分析策略，因此如果要更新网络分析策略中的预处理器设置，**必须**重新应用访问控制策略。

步骤 10　点击 **Import**。

系统安装规则更新并显示 Rule Update Log 详细视图；请参阅第 66-21 页上的了解 Rule Update Import Log 详细视图。系统还应用在上一步中指定的策略；请参阅第 12-13 页上的应用访问控制策略和第 31-7 页上的应用入侵策略。

注　如果在安装规则更新时出现错误消息，请联系支持部门。

使用自动一次性规则更新

许可证：任何环境

以下步骤说明如何通过自动连接到支持网站导入新的规则更新。只有在设备可访问互联网时才能使用这种方法。

要自动导入规则更新，请执行以下操作：

访问：管理

步骤 1　选择 **System > Updates**，然后选择 **Rule Updates** 选项卡。

系统将显示 Rule Updates 页面。

提示　也可以点击 Rule Editor 页面 (**Policies > Intrusion > Rule Editor**) 上的 **Import Rules**。

步骤 2　或者，点击 **Delete All Local Rules**，然后点击 **OK**，以将创建或导入的所有用户定义规则移到被删除的文件夹。有关详情，请参见第 36-97 页上的删除自定义规则。

步骤 3　选择 **Download new Rule Update from the Support Site**。

步骤 4　或者，在更新完成后，重新对受管设备应用策略：

- 选择 **Reapply intrusion policies after the rule update import completes** 以自动重新应用入侵策略。仅选择此选项更新规则和其他已更改的入侵策略设置，无需更新您进行的所有其它访问控制配置。您**必须**选择此选项与访问控制策略一起重新应用入侵策略；重新应用访问控制策略在这种情况下不执行全面的应用。
- 选择 **Reapply access control policies after the rule update import completes** 以自动重新应用访问控制策略及其关联的 SSL、网络分析和文件策略，但不重新应用入侵策略。选择此选项也更新所有修改的访问控制高级设置的默认值。由于您无法独立于其父访问控制策略应用网络分析策略，因此如果要更新网络分析策略中的预处理器设置，**必须**重新应用访问控制策略。

步骤 5　点击 **Import**。

系统安装规则更新并显示 Rule Update Log 详细视图；请参阅第 66-21 页上的了解 Rule Update Import Log 详细视图。系统还应用在上一步中指定的策略；请参阅第 12-13 页上的应用访问控制策略和第 31-7 页上的应用入侵策略。

注　如果在安装规则更新时出现错误消息，请联系支持部门。

使用周期性规则更新

许可证：任何环境

可以在 Rule Updates 页面上设置为按日、周或月导入规则更新。如果您的部署包括防御中心的高可靠性对，请仅在主防御中心上导入更新。辅助防御中心会在常规同步过程中接收规则更新。

规则更新导入中的适用子任务按如下出现：下载，安装，基本策略更新，策略重新应用。完成一个子任务后，才会开始下一个子任务。请注意，如果配置了周期性导入，只能应用设备之前应用的策略。

要安排周期性规则更新，请执行以下操作：

访问：管理

步骤 1　选择 **System > Updates**，然后选择 **Rule Updates** 选项卡。

系统将显示 Rule Updates 页面。

提示　也可以点击 Rule Editor 页面 (**Policies > Intrusion > Rule Editor**) 上的 **Import Rules**。

步骤 2　或者，点击 **Delete All Local Rules**，然后点击 **OK**，以将创建或导入的所有用户定义规则移到被删除的文件夹。有关详情，请参见第 36-97 页上的删除自定义规则。

步骤 3　选择 **Enable Recurring Rule Update Imports**。

页面展开，其中显示用于配置周期性导入的选项。导入状态消息显示在 **Recurring Rule Update Imports** 部分下方。保存设置即会启用周期性导入。

提示　要禁用周期性导入，请清除 **Enable Recurring Rule Update Imports** 复选框并点击 **Save**。

步骤 4　在 **Import Frequency** 字段中，从下拉列表选择 **Daily**、 **Weekly** 或 **Monthly**。

如果选择每周或每月导入频率，请使用出现的下拉列表选择您要在星期几或几号导入规则更新。通过多次点击或键入您的选项的首字母或数字并按 Enter 键，从周期性任务下拉列表中选择。

步骤 5　在 **Import Frequency** 字段中，指定要开始周期性规则更新导入的时间。

步骤 6　或者，在更新完成后，重新对受管设备应用策略：

- 选择 **Reapply intrusion policies after the rule update import completes** 以自动重新应用入侵策略。仅选择此选项更新规则和其他已更改的入侵策略设置，无需更新您进行的所有其它访问控制配置。您**必须**选择此选项与访问控制策略一起重新应用入侵策略；重新应用访问控制策略在这种情况下不执行全面的应用。
- 选择 **Reapply access control policies after the rule update import completes** 以自动重新应用访问控制策略及其关联的 SSL、网络分析和文件策略，但不重新应用入侵策略。选择此选项也更新所有修改的访问控制高级设置的默认值。由于您无法独立于其父访问控制策略应用网络分析策略，因此如果要更新网络分析策略中的预处理器设置，**必须**重新应用访问控制策略。

步骤 7　点击 **Save** 以按照设置启用周期性规则更新导入。

Recurring Rule Update Imports 部分下方的状态信息会发生变化，以指明尚未运行规则更新。在计划的时间，系统安装规则更新并应用在上一步中指定的策略；请参阅第 12-13 页上的应用访问控制策略和第 31-7 页上的应用入侵策略。

在导入之前或导入过程中，可注销或使用网络界面执行其他任务。在导入过程中访问时， Rule Update Log 显示红色状态图标 （ ），此外，还可以在 Rule Update Log 详细视图中查看消息。根据规则更新大小和内容，状态消息可能几分钟之后才会显示。有关详细信息，请参阅第 66-19 页上的查看规则更新日志。

注　如果在安装规则更新时出现错误消息，请联系支持部门。

导入本地规则文件

许可证：任何环境

本地规则是一个自定义标准文本规则，即从本地计算机导入的采用 ASCII 或 UTF - 8 编码的一个明文文本文件。可按照 Snort 用户手册中的说明创建本地规则 （可在 http/www.snort.org 上获得该手册）。

导入本地规则时，请注意：

- 文本文件名称可包含字母数字字符和空格，不可包含除下划线 (_)、句号 (.) 和破折号 (-) 以外的其他特殊字符。
- 不一定要指定生成器 ID (GID)；如果要这样做，可以仅为标准文本规则指定 GID 1，为敏感数据规则指定 GID 138。

- 首次导入规则时，请**勿**指定 Snort ID (SID) 或版本号；这样做是为了避免与其他规则 （包括已删除的规则）的 SID 发生冲突。

  系统会自动为规则分配下一个可用的自定义规则 SID （1000000 或更高）以及版本号 1。
- 导入之前已经导入的本地规则的更新版本时，**必须**包含系统分配的 SID 以及高于当前版本号的版本号。

  要在 Rule Editor 页面 (**Policies > Intrusion > Rule Editor**) 上查看某个当前本地规则的版本号，请点击本地规则类别以展开文件夹，然后点击规则该旁边的 **Edit**。
- 可以恢复已删除的本地规则，方法是，导入使用系统分配的 SID 且版本号高于当前版本号的规则。请注意，删除本地规则时，系统会自动增加版本号；这样方便恢复本地规则。

  要在 Rule Editor 页面 (**Policies > Intrusion > Rule Editor**) 上查看某个已删除的本地规则的版本号，请点击已删除规则类别以展开文件夹，然后点击该规则旁边的 **Edit**。
- 不能导入包含 SID 大于 2147483647 的规则的规则文件；这种导入将会失败。
- 如果导入包含长于 64 个字符的源端口列表或目标地主机列表，导入将会失效。
- 系统始终将导入的本地规则设置为禁用状态；必须手动设置本地规则的状态后，才能将它们用于入侵策略中。有关详情，请参见第 32-18 页上的设置规则状态。
- 必须确保文件中的规则不包含任何转义字符。
- 规则导入程序要求以 ASCII 或 UTF-8 编码格式导入所有自定义规则。
- 所有导入的本地规则都会自动保存在本地规则类别中。
- 所有已删除的本地规则从会从本地规则类别转移到已删除规则类别。
- 系统会导入以一个井号 (#) 开头的本地规则。
- 系统会忽略以两个井号 (##) 开头的本地规则，也就是说，不导入这样的规则。
- 思科强烈建议在高可用性对中的主防御中心上导入本地规则，以避免 SID 编号问题。
- 如果启用某个导入的本地规则，而该规则将弃用的 `threshold` 关键字与某个入侵策略中的入侵事件阈值功能结合起来使用，策略验证将会失败。有关详情，请参见第 32-20 页上的配置事件阈值。

要导入本地规则文件，请执行以下操作：

访问：管理

步骤 1　选择 **Policies > Intrusion > Rule Editor**。

系统将显示 Rule Editor 页面。

步骤 2　点击 **Import Rules**。

系统将显示 Import Rules 页面。

提示　还可以选择 **System > Updates**，然后选择 **Rule Updates** 选项卡。

步骤 3　选择 **Rule Update or text rule file to upload and install**，然后点击 **Browse** 以浏览到规则文件。请注意，以这种方式上传的所有规则保存在本地规则类别中。

提示　您**仅**可导入采用 ASCII 或 UTF - 8 编码的明文文本文件。

步骤 4　点击 **Import**。

规则文件成功导入。确保在入侵策略中启用适当的规则。下次应用受影响的策略时，导入的规则才会激活。

注　在应用入侵策略之前，受管设备**不**使用为检查设置的新规则。有关步骤，请参阅第 12-13 页上的应用访问控制策略。

查看规则更新日志

许可证：任何环境

防御中心会为导入的规则更新和本地规则文件生成记录。

每个记录都包含时间戳、导入文件的用户名称以及指明导入成功或失败的状态图标。可保留导入的所有规则更新和本地规则文件的列表，删除列表中的任何记录，以及访问有关所有导入的规则和规则更新组成部分的详细记录。下表介绍规则更新日志中的字段。

表 66-2　　规则更新日志操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 66-20 页上的了解规则更新日志表中获得详细信息。
删除导入日志中的导入文件记录（包括有关文件中所有对象的详细记录）	点击导入文件名称旁边的删除图标 ( )。 **注**　删除日志中的文件并不会删除导入到导入文件中的任何对象，而只是删除导入日志记录。
查看导入到规则更新或本地规则文件中的每个对象的详细信息	点击导入文件名称旁边的查看图标 ( )。

有关详细信息，请参阅以下各节：

- 第 66-20 页上的了解规则更新日志表介绍导入的规则更新和本地规则文件的列表中的字段。
- 第 66-20 页上的查看规则更新导入日志详细信息介绍导入到规则更新或本地规则文件中的每个对象的详细记录。
- 第 66-21 页上的了解 Rule Update Import Log 详细视图介绍 Rule Update Log 详细视图中的每个字段。
- 第 66-22 页上的搜索规则更新导入日志说明如何搜索特定记录或与搜索条件匹配的所有记录。

要查看规则更新日志，请执行以下操作：

访问：管理

步骤 1　选择 **System > Updates**，然后选择 **Rule Updates** 选项卡。

系统将显示 Rule Updates 页面。

提示　也可以点击 Rule Editor 页面（依次选择 **Policies > Intrusion > Rule Editor** 可显示此页面）上的 **Import Rules**。

步骤 2　点击 **Rule Update Log**。

系统将显示 Rule Update Log 页面。该页面列出每个导入的规则更新和本地规则文件。

了解规则更新日志表

许可证：任何环境

下表介绍导入的规则更新和本地规则文件列表中的字段。

表 66-3　　规则更新日志字段

字段	说明
小结	导入文件的名称。如果导入失败，文件名称下方会显示有关导入失败原因的简要说明。
时间	导入开始的时间和日期。
用户 ID	触发导入的用户的用户名。
状态	导入有以下状态： • 成功 ( ) • 失败或进行中 ( ) **提示**　导入过程中， Rule Update Log 页面上会显示红色状态图标，表示导入失败或未完成；成功完成导入后，该红色状态图标会变为绿色状态图标。

点击规则更新或文件名称旁边的查看图标 ( ) 可查看规则更新或本地规则文件的 Rule Update Log 详细视图，点击删除图标 ( ) 可删除文件记录以及与文件一起导入的所有详细对象记录。

提示　导入规则更新时，可查看详细导入信息。

查看规则更新导入日志详细信息

许可证：任何环境

Rule Update Import Log 详细视图列出导入到规则更新或本地规则文件中的每个对象的详细记录。此外，还可以根据列出的记录创建仅包含符合特定需求的信息的自定义工作流程或报告。

下表介绍可在 Rule Update Import Log 详细视图工作流程页面上执行的具体操作。

表 66-4　　Rule Update Import Log 详细视图操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 66-21 页上的了解 Rule Update Import Log 详细视图中获得详细信息。
分类和限制当前工作流程页面上的记录	在第 58-29 页上的对向下钻取工作流程页面进行排序中获得详细信息。

表 66-4　Rule Update Import Log 详细视图操作 （续）

要.....	您可以.....
暂时使用不同的工作流程	点击 (**switch workflows**)。有关选择工作流程的信息，请参阅第 58-14 页上的选择工作流程。有关创建自定义工作流程的信息，请参阅第 58-34 页上的创建自定义工作流程。
为当前页面添加书签以便快速返回到该页面	点击 **Bookmark This Page**。有关详细信息，请参阅第 58-32 页上的使用书签。
导航到书签管理页面	点击 **View Bookmarks**。有关详细信息，请参阅第 58-32 页上的使用书签。
根据当前视图中的数据生成报告	点击 **Report Designer**。有关详细信息，请参阅第 57-8 页上的从事件视图创建报告模板。
在整个规则更新导入日志数据库中搜索规则更新导入记录	点击 **Search**。有关详细信息，请参阅第 66-22 页上的搜索规则更新导入日志。
打开事先填充了当前单个限制条件的搜索页面	选择 Search Constraints 旁边的 **Edit Search** 或 **Save Search**。有关详细信息，请参阅表视图和向下钻取页面功能表。

要查看 Rule Update Import Log 详细视图，请执行以下操作：

访问：管理

步骤 1　选择 **System > Updates**，然后选择 **Rule Updates** 选项卡。

系统将显示 Rule Updates 页面。

提示　也可以点击 Rule Editor 页面 （依次选择 **Policies > Intrusion > Rule Editor** 可显示此页面）上的 **Import Rules**。

步骤 2　点击 **Rule Update Log**。

系统将显示 Rule Update Log 页面。

步骤 3　点击要查看的详细记录的文件的旁边的查看图标 ( )。

系统将显示详细记录的表视图。

了解 Rule Update Import Log 详细视图

许可证：任何环境

可以查看导入到规则更新或本地规则文件中的每个对象的详细记录。下表介绍 Rule Update Log 详细视图中的字段。

表 66-5　Rule Update Import Log 详细视图字段

字段	说明
时间	导入开始的时间和日期。
字段名称	导入对象的名称 （对于规则，对应的是规则 Message 字段；对于规则更新，对应的是组成部分名称）。

表 66-5　Rule Update Import Log 详细视图字段 （续）

字段	说明
类型	导入对象的类型，可以是以下类型之一： • `rule update component` （已导入的组成部分，例如规则包或策略包） • `rule` （对于规则而言，是指新的或更新后的规则；请注意，在版本 5.0.1 中，此值替换为 `update` 值，后者已被弃用） • `policy apply` （为导入启用了 **Reapply intrusion policies after the Rule Update import completes** 选项）
操作	指明对对象类型执行了以下其中一项操作： • `new` （对于规则而言，是指第一次把规则存储在设备上） • `changed` （对于规则更新组成部分或规则而言，规则更新组成部分已被修改，或者规则的版本号更高且 GID 和 SID 相同） • `collision` （对于规则更新组成部分或规则而言，由于版本与设备上的现有组成部分或规则冲突，因此跳过导入） • `deleted` （对于规则而言，已从规则更新删除规则） • `enabled` （对于规则更新编辑而言，已在思科提供的默认策略中启用了预处理器、规则或其他功能） • `disabled` （对于规则而言，已在思科提供的默认策略中禁用了规则） • `drop` （对于规则而言，已在思科提供的默认策略中将规则设置为 Drop and Generate Events） • `error` （对于规则更新或本地规则文件而言，导入失败） • `apply` （为导入启用了 **Reapply intrusion policies after the Rule Update import completes** 选项）
默认操作	规则更新定义的默认操作。当导入对象类型是 `rule` 时，默认操作是 `Pass`、 `Alert` 或 `Drop`。对于所有其他导入对象类型，没有默认操作。
GID	规则的生成器 ID。例如， `1` (标准文本规则) 或 `3` (共享对象规则)。有关详情，请参见第 41-34 页上的表 41-7。
SID	规则的 SID。
Rev	规则的版本号。
策略	对于导入的规则而言，此字段显示为 `All`，表示导入的规则包含在所有默认入侵策略中。对于其他导入对象类型，此字段为空白。
详细信息	组成部分或规则独有的字符串。对于规则、 GID、 SID 以及已更改规则的上一个版本号，此字段显示为 `previously (GID:SID:Rev)`。对于未更改的规则，此字段为空白。
计数	记录数 (`1`)。当表受限时， Count 字段显示在表视图中，而且在默认情况下， Rule Update Log 详细视图受限于规则更新记录。

搜索规则更新导入日志

许可证：任何环境

注　试用版用户：此功能将在文档最终版本中详细解释。

可以搜索特定记录或与搜索条件匹配的所有记录。可以创建自定义搜索并将其保存以供日后使用。

提示 即使是通过在仅显示单个导入文件的记录的 Rule Update Import Log 详细视图中工具栏上点击 **Search** 发起搜索，也可以搜索整个规则更新导入日志数据库。确保将时间限制条件设置为包含所有搜索中要包含的对象。有关详情，请参见第 60-5 页上的在搜索中指定时间约束。

下表介绍可用的搜索条件。请注意，记录搜索不区分大小写。例如，搜索 `RULE` 或 `rule` 将会得到相同的结果。

表 66-6　规则更新导入日志搜索条件

搜索字段	说明	示例
时间	指定记录生成的日期和时间。有关时间输入语法，请参阅第 60-5 页上的在搜索中指定时间约束。	`> 2006-01-15 13:30:00` 将返回在 2006 年1月 15 日下午 1 点 30 分后导入的所有规则记录。
字段名称	指定规则 Message 字段的全部或部分内容。您可以在该字段中使用星号 (*) 作为通配符。	`*dhcp*` 返回 Message 字段中带有 DHCP 的所有规则记录。
类型	指定记录类型，可以是 `rule update component`、`rule`、或 `policy apply`。 请注意，可使用 `update` 搜索值搜索在版本 5.0.1 之前导入的规则。	`update` 返回导入的规则更新组成部分，例如规则包或策略包；`rule` 返回规则更新 （包括新规则）；`policy apply` 返回在更新后自动重新应用的入侵策略的规则更新的信息的表格行。
操作	指定要查看的对象的操作。有关可指定操作的列表，请参阅Rule Update Import Log 详细视图字段表。	当类型是 `rule` 时，`new` 返回设备上第一次导入的所有规则。
GID	指定规则的生成器 ID。	`3` 返回所有共享对象规则。
SID	指定规则的签名 ID 或 SID 范围。	`923` 返回 SID 为 923 的规则的记录。
Rev	指定规则的版本号。	`3` 返回版本号为 3 的规则。
策略	指定规则导入到的默认策略。	`All` 返回导入到所有默认策略的规则。
Rule Update	指定规则更新的文件名。	*`filename`* 返回指定的导入文件的所有记录。
详细信息	指定导入的对象的详细信息。	`previously*` 返回已更改的所有规则的记录。

有关搜索的详细信息，包括如何加载和删除已保存搜索，请参阅第 60-1 页上的搜索事件。

要搜索规则更新导入日志，请执行以下操作：

访问：管理员/入侵管理员

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从 **Table** 下拉列表选择 **Rule Update Import Log**。

页面根据适当限制条件重新加载。

提示 还可以在 Rule Update Log 详细视图中点击 **Search**；请参阅第 66-20 页上的查看规则更新导入日志详细信息。

步骤 3　或者，如要保存搜索，请在 **Name** 字段中输入该搜索的名称。

如果没有输入名称，保存时，网络界面会自动创建一个名称。

步骤 4　在相应字段中输入搜索条件，如规则更新导入日志搜索条件表中所述。如果输入多个条件，搜索将会返回符合所有条件的记录。

步骤 5　如果想要保存搜索，以供其他用户访问，请清除 **Save As Private** 复选框。否则，请将该复选框保持选中状态，将搜索另存为私有搜索。

如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 6　您有以下选项：

- 点击 **Search** 开始搜索。

  搜索结果显示在默认的 Rule Update Import Log 详细视图工作流程中。要使用其他工作流程（包括自定义工作流程），请点击 (**switch workflows**)。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。
- 如果正在修改现有搜索并想要保存更改，请点击 **Save**。
- 点击 **Save as New Search** 保存搜索条件。搜索保存成功 （并且已与您的用户帐户相关联，如已选择 **Save As Private**），以便以后运行。

更新地理定位数据库

许可证：FireSIGHT

受支持的防御中心：除 DC500 外的所有型号

思科地理定位数据库 (GeoDB) 是包含地理数据 （例如，国家/地区、城市、坐标等等）以及与可路由 IP 地址相关联的连接相关数据 （例如，互联网服务提供商、域名、连接类型等等）的数据库。系统检测与已经检测到的 IP 地址匹配的 GeoDB 信息时，可查看与 IP 地址相关的地理定位信息。要查看除国家/地区或大洲以外的任何地理定位详细信息，必须在系统上安装 GeoDB。思科定期发布 GeoDB 更新。

要更新 GeoDB，请使用防御中心上的 Geolocation Updates 页面 (**System > Updates > Geolocation Updates**)。将从支持部门获得的 GeoDB 更新上传到设备后，这些更新会显示在该页面中。

更新 GeoDB 所需的时间取决于设备；安装过程一般需要 30 到 40 分钟。虽然 GeoDB 更新不会中断任何其他系统功能 （包括持续收集地理定位信息），但是，这个过程确实会耗用系统资源。制定更新计划时需要考虑这一点。

本节说明如何计划和执行手动 GeoDB 更新。还可以利用自动更新功能安排 GeoDB 更新；有关详细信息，请参阅第 62-8 页上的自动运行地理定位数据库更新。有关地理定位的详细信息，请参阅第 58-17 页上的使用地理定位。

要更新地理定位数据库，请执行以下操作：

访问：管理

步骤 1　选择 **System > Updates**。

系统将显示 Product Updates 页面。

步骤 2　点击 **Geolocation Updates** 选项卡。

系统将显示 Geolocation Updates 页面。

步骤 3　将更新上传到防御中心。

- 如果防御中心能够访问互联网，请点击 **Download and install geolocation update from the Support Site** 以检查以下任何一个支持网站上的最新更新：

  - **Sourcefire**：(https://support.sourcefire.com/)
  - **思科**：(http://www.cisco.com/cisco/web/support/index.html)
- 如果防御中心不能访问互联网，请手动从以下任何一个支持网站下载更新，然后点击 **Upload and install geolocation update**。浏览到更新并点击 **Import**：
  - **Sourcefire**：(https://support.sourcefire.com/)
  - **思科**：(http://www.cisco.com/cisco/web/support/index.html)

注　可直接从支持网站下载更新 （手动下载，或者点击 Geolocation Updates 页面上的 **Download and install geolocation update from the Support Site**）。如果通过邮件传输更新文件，可能会损坏更新文件。

更新过程开始。安装更新大约需要 30 到 40 分钟；所需时间可能因设备硬件而异。可在任务队列 (**System > Monitoring > Task Status**) 中监控更新进度。

步骤 4　完成更新后，返回到 Geolocation Updates 页面，或者选择 **Help > About** 以确认 GeoDB 内部版本号是否与安装的更新相匹配。

GeoDB 更新将会覆盖之前的所有 GeoDB 版本并立即生效。更新 GeoDB 时，防御中心会自动更新其受管设备。尽管 GeoDB 需要几分钟时间方可在部署中生效，但完成更新后，无需重新应用访问控制策略。

监控系统

FireSIGHT 系统提供许多有用的监控功能，帮您实现在一个页面对系统进行日常管理。例如，在 Host Statistics 页面，您可以监控基本主机统计信息和入侵事件信息，以及当日 Data Correlator 和网络发现进程的统计信息。您还可以监控防御中心或受管设备上当前运行的所有进程的摘要和详细信息。以下各节提供有关该系统提供的监控功能的详细信息：

- 第 67-1 页上的查看主机统计信息描述如何查看主机信息，例如：
- 系统运行时间
- 磁盘和内存使用情况
- Data Correlator 统计信息
- 系统进程
- 入侵事件信息
- 在防御中心中，您也可以使用运行状况监控在磁盘空间较低的情形下监控磁盘使用情况和警报。有关详细信息，请参阅第 68-1 页上的了解运行状况监控。
- 第 67-3 页上的监控系统状态和磁盘空间使用情况介绍如何查看基本事件和磁盘分区信息。
- 第 67-4 页上的查看系统进程状态介绍如何查看基本进程状态。
- 第 67-6 页上的了解运行的进程介绍设备上运行的基本系统进程。

您可以使用 **Overview > Summary** 中的选项查看和用图形表示入侵和发现事件的统计信息。有关详情，请参阅：

- 第 41-2 页上的查看入侵事件统计信息
- 第 41-7 页上的查看入侵事件图表
- 第 50-2 页上的查看发现事件统计数据
- 第 50-5 页上的查看发现性能 图表

查看主机统计信息

许可证：任何环境

Statistics 页面列出如下统计信息的当前状态：

- 一般主机统计信息；有关详细信息，请参阅主机统计信息表
- Data Correlator 统计信息 （仅限防御中心，需要 FireSIGHT）；有关详细信息，请参阅 Data Correlator 进程统计信息表
- 入侵事件信息 （需要保护）；有关详细信息，请参阅入侵事件信息表

下表介绍了 Statistics 页面列出的主机统计信息。

表 67-1　主机统计信息

类别	说明
时间	系统当前时间。
正常运行时间	系统上次启动后持续的天数 （如果适用）、小时数和分钟数。
内存使用率	正使用的系统内存的百分比。
Load Average	过去 1 分钟、 5 分钟和 15 分钟内 CPU 队列的平均进程数。
磁盘使用情况	正使用的磁盘空间的百分比。点击箭头查看更详细的主机统计信息。有关详情，请参见第 67-3 页上的监控系统状态和磁盘空间使用情况。
流程	系统中运行的进程摘要。有关详情，请参见第 67-4 页上的查看系统进程状态。

如果 FireSIGHT 系统部署包括一个防御中心和一个 FireSIGHT 许可证，您也可以查看当日 Data Correlator 和网络发现进程的统计信息。当受管设备执行数据收集、解码和分析时，网络发现进程将数据与指纹和漏洞数据库相关联，然后由防御中心上运行的 Data Correlator 处理成二进制文件。 Data Correlator 分析二进制文件的信息后生成事件，然后创建发现网络映射。

网络发现和 Data Correlator 中显示的统计信息为当日的平均值，使用每台设备从 12:00 AM 到 11:59 PM 之间搜集的统计信息。

下表介绍了 Data Correlator 进程显示的统计信息。

表 67-2　Data Correlator 进程统计信息

类别	说明
事件/秒	Data Correlator 每秒钟接收和处理的发现事件的数量
Connections/Sec	Data Correlator 每秒钟接收和处理的连接的数量
CPU Usage - User (%)	当日用户进程占 CPU 时间的平均百分比
CPU Usage - System (%)	当日系统进程占 CPU 时间的平均百分比
VmSize (KB)	当日分配给 Data Correlator 的平均内存大小，单位为千字节
VmRSS (KB)	当日 Data Correlator 使用的平均内存使用量，单位为千字节

在受管设备和管理设备的防御中心上，您也可以查看上次入侵事件的日期和时间、过去一小时和昨天发生的事件总数，以及数据库的事件总数。

注　Statistics 页面 Intrusion Event Information 部分的信息依据是受管设备上存储的入侵事件，而不是发送到防御中心的信息。如果您管理自己的设备，导致入侵事件没有存储到本地，此页面不会列出入侵事件信息。不能在本地存储事件的受管设备也是如此。

下表介绍了 Statistics 页面 Intrusion Event Information 部分显示的统计信息。

表 67-3　入侵事件信息

统计	说明
Last Alert Was	上次事件发生的日期和时间
Total Events Last Hour	过去一个小时内发生的事件总数

表 67-3　　入侵事件信息 （续）

统计	说明
Total Events Last Day	过去 24 小时内发生的事件总数
Total Events in Database	时间数据库中的事件总数

要查看 Statistics 页面，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Monitoring > Statistics**。

系统将显示 Statistics 页面。

步骤 2　在防御中心中，您还可以列出受管设备的统计信息。在 **Select Device(s)** 框中点击 **Select Devices**。您可以使用 Shift 和 Ctrl 键一次性选择多台设备。

所选设备 Statistics 页面完成统计信息的更新。

监控系统状态和磁盘空间使用情况

许可证：任何环境

Statistics 页面的 Disk Usage 部分提供磁盘使用情况快览，可以按类别和分区状态进行查看。如果您在设备上安装了一个恶意软件存储包，您还可以查看分区状态。您可以随时监控此页面，确保系统进程和数据库有充足的磁盘空间可用。

提示　在防御中心中，您也可以使用运行状况监控在磁盘空间较低的情形下监控磁盘使用情况和警报。有关详细信息，请参阅第 68-1 页上的了解运行状况监控。

要访问磁盘使用情况信息，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Monitoring > Statistics**。

系统将显示 Statistics 页面。

步骤 2　在 By Category 层叠图中将指针悬停在一个磁盘使用类别上以 （按顺序）查看：

- 该类别使用的可用磁盘空间百分比
- 该磁盘的实际存储空间
- 该类别的总可用磁盘空间

有关磁盘使用类别的详细信息，请参阅第 55-22 页上的了解 Disk Usage 构件。

步骤 3　点击 **Total** 旁边的向下箭头将其展开。

Disk Usage 部分将展开，显示分区使用情况。如果您安装有一个恶意软件存储包，系统也会显示 `/var/storage` 分区使用情况。

如果您的部署包括多个受管设备，您可能想要限制特定设备的磁盘使用量数据。

在防御中心中，要查看特定设备的磁盘使用信息，请执行以下操作：

访问：管理员/维护人员

步骤 1　从 **Select Device(s)** 框中选择设备名称，然后点击 **Select Devices**。

页面将重新加载，其中列出所选每台设备主机的统计信息。

步骤 2　点击 **Disk Usage** 旁边的向下箭头将其展开。

Disk Usage 部分将展开。

查看系统进程状态

许可证：任何环境

在 Host Statistics 页面的 Processes 部分，您可以查看一台设备上正在运行的进程。它为每个运行的进程提供常规进程信息和特定信息。如果您正使用防御中心管理设备，可以使用防御中心的网站界面查看任何受管设备的进程状态。

下表介绍了进程列表中显示的各列。

表 67-4　　进程状态

列	说明
Pid	进程 ID 编号
用户名	运行进程的用户或组的名称
Pri	进程优先级
Nice	*nice* 值是表示一个进程计划优先级的值。值范围为 -20（最高优先级）到 19 （最低优先级）
规格	进程使用的内存大小 （以千字节计，除非数值后是 m，即表示兆字节）
Res	内存中常驻页面文件的数量 （以千字节计，除非数值后是 m，即表示兆字节）
州	进程状态： • D - 进程处于不可中断休眠 （通常 Input/Output） • N - 进程有一个正优先值 • R - 进程可运行 （在运行队列中） • S - 进程处于休眠模式 • T - 进程被跟踪或停止 • W - 进程在分页 • X - 进程已废弃 • Z - 进程已失效 • < - 进程有一个负优先值
时间	进程运行的时间 （格式为小时:分钟:秒）
Cpu	进程正在使用的 CPU 的百分比
命令	进程的可执行名称

要展开进程列表，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Monitoring > Statistics**。

系统将显示 Statistics 页面。

步骤 2　在防御中心中，从 **Select Device(s)** 框中选择您想要查看进程统计信息的一个或多台设备，然后点击 **Select Devices**。

步骤 3　点击 **Processes** 旁边的向下箭头。

进程列表将展开，列出常规进程状态信息，其中包括运行任务数量和类型、当前时间、当前系统正常运行时间、系统平均负载、 CPU、内存和交换信息，以及每个运行进程的特定信息。

Cpu(s) 列出以下 CPU 使用信息：

- 用户进程使用百分比
- 系统进程使用百分比
- 优先使用情况百分比 （拥有负优先值进程的 CPU 使用情况，表示更高优先级）

  优先值是指系统进程的计划优先级，范围为 -20 （最高优先级）到 19 （最低优先级）。
- 空闲使用百分比

Mem 列出如下内存使用信息：

- 内存中千字节总数
- 内存中已使用千字节总数
- 内存中空闲的千字节总数
- 内存中缓存的千字节总数

Swap 列出如下交换使用信息：

- 交换空间中千字节总数
- 交换空间中已使用千字节总数
- 交换空间中空闲的千字节总数
- 交换空间中缓存的千字节总数

注　有关设备上运行进程类型的详细信息，请参阅第 67-6 页上的了解运行的进程。

要折叠进程列表，请执行以下操作：

访问：管理员/维护人员

步骤 1　点击 **Processes** 旁边的向上箭头。

进程列表将折叠。

了解运行的进程

许可证：任何环境

设备上运行有两个不同类型的进程：后台守护程序和可执行文件。后台守护程序始终运行，可执行文件在需要时运行。

有关详细信息，请参阅：

- 第 67-6 页上的了解系统后台守护程序
- 第 67-7 页上的了解可执行文件和系统实用程序

了解系统后台守护程序

许可证：任何环境

后台守护程序在设备上持续运行。他们确保服务可用，并在需要时产生进程。下表列出了 Process Status 页面可以看到的后台守护程序，并对其功能进行简要说明。

注　下表并非一台设备上可运行的所有进程的详尽列表。

表 67-5　　系统后台守护程序

后台守护程序	说明
crond	管理计划命令的实施 （cron 作业）
dhclient	管理动态主机 IP 地址
fpcollect	管理客户端和服务器指纹集合
httpd	管理 HTTP （Apache 网络服务器）进程
httpsd	管理 HTTPS （使用 SSL 的 Apache 网络服务器）服务，检查正在运行的 SSL 和有效的证书身份验证；在后台运行，为设备提供安全的网络接入
keventd	管理 Linux 内核事件通知消息
klogd	管理 Linux 内核消息监听和记录
kswapd	管理 Linux 内核交换内存
kupdated	管理 Linux 内核更新进程，执行磁盘同步
mysqld	管理FireSIGHT 系统数据库进程
ntpd	管理网络时间协议 (NTP) 进程
pm	管理所有思科进程，启动所需进程，重新启动所有意外发生故障的进程
reportd	管理报告
safe_mysqld	管理数据库安全模式操作；如果出现错误，重新启动数据库后台守护程序，并向文件中记录运行时间信息
SFDataCorrelator	管理数据传输
sfestreamer （仅限防御中心）	管理使用事件流转换器的第三方客户端应用的连接
sfmgr	使用到一台设备的 sftunnel 连接，为远程管理和配置该设备提供 RPC 服务

表 67-5　　系统后台守护程序 （续）

后台守护程序	说明
SFRemediateD （仅限防御中心 - 需要 FireSIGHT）	管理补救响应
sftimeserviced （仅限防御中心）	将时间同步消息转发到受管设备
sfmbservice （需要保护）	使用到设备的 sftunnel 连接，为在远程设备上运行的 sfmb 消息代理进程提供接入服务。目前只有运行状况监控功能使用此程序，将运行状况事件和警报从一个受管设备发送到防御中心，或在高可用环境中在防御中心之间进行发送。
sftroughd	侦听进入套接字的连接，然后调用正确的可执行程序 （通常是思科消息代理、 sfmb）处理请求
sftunnel	为需要与远程设备通信的所有进程提供安全的通信通道
sshd	管理安全外壳 (SSH) 进程；在后台运行，为设备提供 SSH 接入
syslogd	管理系统日志 (syslog) 流程

了解可执行文件和系统实用程序

许可证：任何环境

系统会有许多可执行文件，它们在其他进程或用户操作执行时开始运行。下表介绍了在 Process Status 页面可能会看到的可执行程序。

表 67-6　　系统可执行程序和实用程序

可执行程序	说明
awk	执行用 `awk` 编程语言书写的程序的实用程序
bash	GNU Bourne-Again SHell
cat	读取文件并将内容写入标准输出的实用程序
chown	更改用户和组文件权限的实用程序
chsh	更改默认登录外壳的实用程序
SFDataCorrelator （仅限防御中心 - 需要 FireSIGHT）	分析 FireSIGHT 创建的二进制文件来生成事件、连接数据和网络映射
cp	复制文件的实用程序
df	列出设备可用空间量的实用程序
echo	将内容写入标准输出的实用程序
egrep	按特定输入搜索文件和文件夹、支持标准 grep 不支持的正则表达式扩展集的实用程序
find	按特定输入循环搜索目录的实用程序
grep	按特定输入搜索文件和目录的实用程序
halt	停用服务器的实用程序
httpsdctl	处理安全 Apache 网络进程

表 67-6　系统可执行程序和实用程序 （续）

可执行程序	说明
hwclock	允许访问硬件时钟的实用程序
ifconfig	表示网络配置可执行程序。确保 MAC 地址保持不变
iptables	根据 Access Configuration 页面所做的更改处理访问限制。有关访问配置的详细信息，请参阅第 63-8 页上的配置设备的访问列表。
iptables-restore	处理 iptables 文件恢复
iptables-save	处理对 iptables 保存的更改
kill	可用来结束会话和进程的实用程序
killall	可用来结束所有会话和进程的实用程序
ksh	Korn Shell 的公共域版本
记录器	提供通过命令行访问系统日志后台守护程序方法的实用程序
md5sum	为指定文件打印校验和以及块数量的实用程序
mv	移动 （重命名）文件的实用程序
myisamchk	指数据库表校验和修复
mysql	指数据库进程；可能出现多个实例
openssl	指创建身份验证证书
perl	指一个 perl 进程
ps	将进程信息写入标准输出的实用程序
sed	用来编辑一个或多个文本文件的实用程序
sfheartbeat	识别心跳广播，表示设备处于活动状态；心跳用来保持设备和防御中心之间的联络
sfmb	表示消息代理进程；处理防御中心和设备之间的通信。
sh	Korn Shell 的公共域版本
shutdown	关闭设备的实用程序
sleep	在指定秒数内暂停进程的实用程序
smtpclient	启用邮件事件通知功能后，处理邮件传输的邮件客户端
snmptrap	将 SNMP 陷阱数据转发到启用 SNMP 通知功能后指定的 SNMP 陷阱服务器
snort （需要保护）	表示 Snort 正在运行
ssh	表示与设备连接的安全外壳 (SSH)
sudo	指 sudo 进程，其允许管理员以外的用户运行可执行程序
顶部	显示最大 CPU 进程信息的实用程序
touch	用来更改指定文件的访问和修改时间的实用程序
vim	用来编辑文本文件的实用程序
wc	执行指定文件行、字和字节计数的实用程序

使用运行状况监控

运行状况监视器提供许多测试，以确定防御中心的设备的运行状况。您可以使用运行状况监视器创建一个测试集合（称为*运行状况策略*），并将该运行状况策略应用到一个或多个设备上。您可以为系统中的每个设备创建一个运行状况策略、为计划应用运行状况策略的特定设备定制一个运行状况策略，或者使用默认的运行状况策略。您也可以导入从另一个防御中心导出的运行状况策略。

测试（称为*运行状况模块*）是用来测试您指定的标准的脚本。您可以通过启用或禁用测试或者通过更改测试设置来修改运行状况策略，可以删除不再需要的运行状况策略。您还可以将来自所选设备的消息加入黑名单，从而抑制这些消息。

运行状况策略中的测试以所配置的时间间隔自动运行。您还可以按需运行所有测试或特定测试。运行状况监视器基于配置的测试条件收集运行状况事件。或者，您还可以配置回应运行状况事件而作出的邮件、 SNMP 或者系统日志警报。

在防御中心中，您可以查看整个系统或者特定设备的运行状况信息。完全可定制的事件视图使您可以快速轻松地分析运行状况监视器所收集的运行状况事件。这些事件视图使您可以搜索和查看事件数据，并访问可能与正调查的事件有关的其他信息。

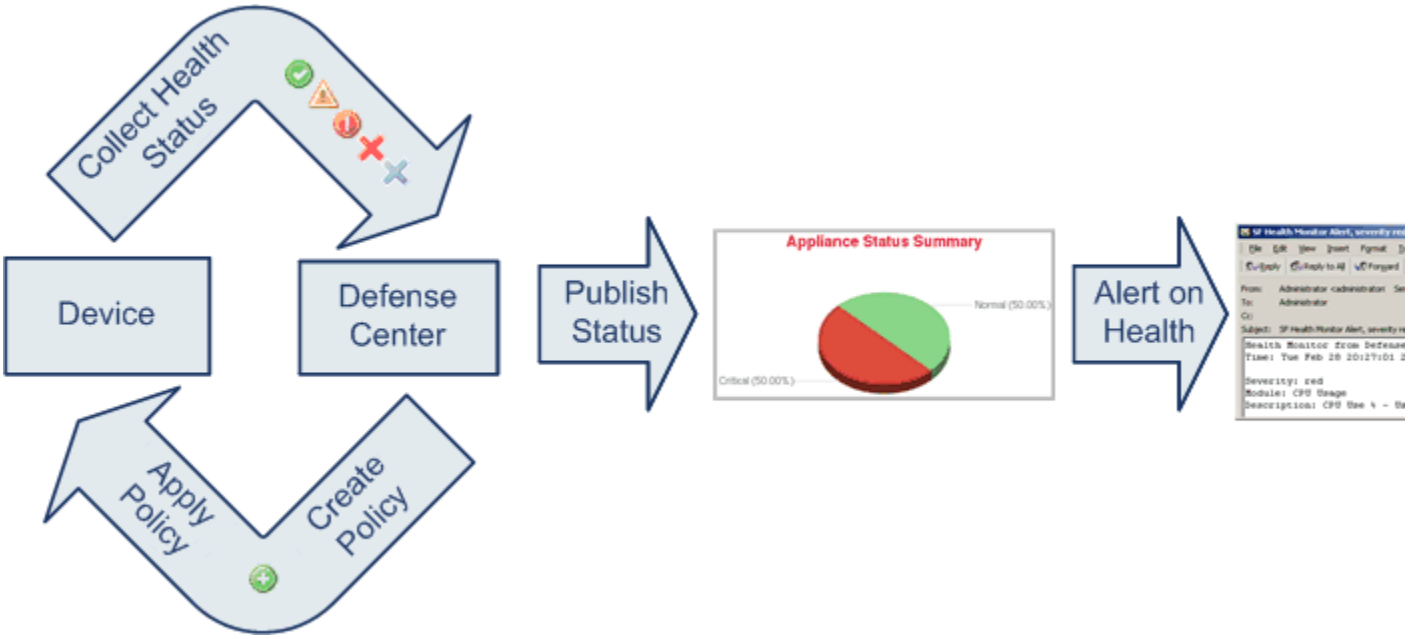
如果支持人员要求您为设备生成故障排除文件，您也可以执行此操作。

有关详细信息，请参阅：

了解运行状况监控

许可证：任何环境

您可以使用运行状况监视器检查整个 FireSIGHT 系统部署中关键功能的状态。通过防御中心监控整个 FireSIGHT 系统的运行状况，方式是将运行状况策略应用到每个受管设备上并且收集防御中心上得到的运行状况数据。 Health Monitor 页面上的饼图和状态表直观地展示监控设备的运行状况，因此您可以迅速检查状态，然后在需要时向下钻取到状态的详细信息。



您可以使用运行状况监视器访问整个系统或特定设备的运行状况信息。 Health Monitor 页面提供系统中所有设备的状态的直观摘要。单个设备运行状况监视器使您可以向下钻取到特定设备的运行状况详细信息。

您还可以在标准 FireSIGHT 系统表视图中查看运行状况事件。通过单个设备的运行状况监视器，您可以打开一个特定事件的状况的表视图，或者检索该设备的所有运行状况事件。您还可以搜索特定运行状况事件。例如，如果要查看用一定百分比表示的 CPU 使用率的所有状况，您可以搜索 CPU 使用率模块并输入百分比值。

您还可以配置回应运行状况事件而作出的邮件、 SNMP 或者系统日志警报。*运行状况警报*是指标准警报和运行状况级别之间的关联。例如，如果要确保设备不会因硬件过载出现故障，您可以设置邮件警报。然后，您可以创建运行状况警报，每当 CPU、磁盘或内存占用率达到您在该设备所应用的运行状况策略中配置的“警告”级别时，就可以触发该邮件警报。您可以设置警报阈值，以最小化您收到的重复警报的数量。

由于运行状况监控是管理活动，因此只有具有管理员用户角色权限的用户才可以访问系统运行状况数据。有关分配用户权限的详细信息，请参阅第 61-50 页上的修改用户权限和选项。

注　默认情况下，除了防御中心， FireSIGHT 系统设备没有适用于它们的运行状况监控策略。受管设备通过硬件告警运行状况模块自动报告硬件状态；如果要使用其他模块监控受管设备，您必须将运行状况策略应用到该设备上。有关适用于设备的思科提供的默认运行状况策略的详细信息，请参阅第 68-6 页上的了解默认运行状况策略。有关创建定制的运行状况策略的详细信息，请参阅第 68-7 页上的创建运行状况策略。有关应用策略的详细信息，请参阅第 68-26 页上的应用运行状况策略。

有关可运行以测试系统运行状况的运行状况策略和运行状况模块的详细信息，请参阅：

- 第 68-3 页上的了解运行状况策略
- 第 68-3 页上的了解运行状况模块
- 第 68-5 页上的了解运行状况监控配置

了解运行状况策略

许可证：任何环境

*运行状况策略*是适用于设备的运行状况模块设置的集合，可以定义防御中心在检查设备运行状况时使用的标准。运行状况监视器跟踪各种运行状况指标，以确保 FireSIGHT 系统硬件和软件正常工作。

在您创建运行状况策略时，可以选择运行哪些测试来确定设备运行状况。您也可以将默认的运行状况策略应用到任意设备上。

了解运行状况模块

许可证：任何环境

运行状况模块（有时也称为*运行状况测试*）是用来测试您在运行状况策略中指定的标准的脚本。下表中介绍可用的运行状况模块。

表 68-1　　运行状况模块

模块	说明
高级恶意软件防护	如果基于文件策略配置，防御中心无法联系综合安全智能云、无法为网络流量中检测的文件检索文件性质信息，或者无法提交文件进行动态分析，或者如果网络流量中检测到过多的文件，则该模块发出警报。如果私有云无法连接到公共思科云，则通过 FireAMP 私有云进行的连接也会生成警报。 该模块在所有防御中心中运行，但 DC500 除外，因为它不支持高级恶意软件防护功能。
设备心跳	该模块确定设备是否正监听设备心跳并基于设备心跳状态发出警报。
自动应用旁路状态	该模块确定，由于设备在旁路阈值设置的秒数内不响应所以设备是否被绕过，以及发生旁路时该模块是否发出警报。
CPU 使用率	该模块检查设备上的 CPU 未过载，并且在 CPU 使用率超过为模块配置的百分比时发出警报。 该模块不能用于在 3D9900 设备上应用的运行状况策略。
卡重置	该模块检查由于硬件故障而重新启动的网卡，并且在发生重置时发出警报。
磁盘状态	该模块检测硬盘的性能和设备上的恶意软件存储包（如果已安装）。硬盘和 RAID 控制器（如果已安装）处于存在故障的危险时，或者，如果恶意软件包在安装之后未检测到或者不可信时，则该模块发出警报。
磁盘使用率	该模块将设备的硬盘驱动器和恶意软件存储包中的磁盘使用率与为该模块配置的限值进行对比，并在使用率超过为模块配置的百分比时发出警报。基于模块阈值，当系统删除过多的监控磁盘使用类别的文件，或者当这些类别以外的磁盘使用率达到过高级别时，该模块也发出警报。
FireAMP 状态监视器	如果在初始连接成功后，防御中心无法连接到思科云，或者您使用 FireAMP 门户取消注册云连接，或者您的私有云无法与公共思科云通信，该模块会发出警报。 该模块仅在防御中心上运行。
FireSIGHT 主机许可证限制	该模块确定是否有足够的 FireSIGHT 主机许可证，并基于为该模块配置的警告级别发出警报。 该模块仅在防御中心上运行。

表 68-1　运行状况模块 （续）

模块	说明
硬件告警	该模块确定 3 系列或 3D9900 设备上的硬件是否需要更换并基于硬件状态发出警报。该模块还报告硬件相关的后台程序的状态和集群设备的状态。 有关为这些设备报告的详细信息，请参阅第 68-47 页上的解释 3D9900 设备的硬件警报详细信息和第 68-47 页上的解释 3 系列设备的硬件警报详细信息。
运行状况监视器流程	该模块监控运行状况监视器本身的状态，并且如果防御中心最后收到运行状况事件后的分钟数超过“警告”或“严重”限值，则发出警报。 该模块仅在防御中心上运行。
内联链路不匹配告警	该模块监控与内联集相关的端口，并且如果内联对的两个接口协商不同的速度，则发出警报。
入侵事件速率	该模块将每秒钟入侵事件的数量与为该模块配置的限值进行对比。如果超过限值，则该模块发出警报。如果入侵事件速率为零，则入侵流程可能已关闭或者受管设备可能没有发送事件。选择 **Analysis > Intrusions > Events**，以检查是否正从该设备接收事件。
接口状态	此模块确定设备当前是否收集流量并根据物理接口和汇聚接口的流量状态发出警报。对于物理接口，信息包括接口名称、链路状态和带宽。对汇聚接口，信息包括接口名称、活动链路的数量和总汇聚带宽。
许可证监控	该模块确定是否有足够的 可控性、保护、URL 过滤、恶意软件和 VPN 许可证。当堆栈中的设备与许可证集不匹配时，该模块也发出警报。基于为该模块自动配置的警告级别，该模块发出警报。您无法更改该模块的配置。 该模块仅在防御中心上运行。
链路状态传播	该模块确定成对的内联集中链路发生故障的时间，并且触发链路状态传播模式。
内存使用率	该模块将设备的内存使用率与为模块配置的限值进行对比，并在使用率超过为该模块配置的级别时发出警报。
电源	该模块确定设备的电源是否需要更换，并基于电源状态发出警报。 该模块在这些防御中心上运行：DC1500、 DC2000、 DC3500、 DC4000。 该模块在这些设备上运行：3D3500、 3D4500、 3D6500、 3D9900 和 3 系列。
进程状态	该模块确定设备上的进程是否在进程管理器外部退出或终止。如果进程在进程管理器外部被故意退出，模块状态变更为“警告”，并且运行状况事件消息指示哪一个进程被退出，直到该模块再次运行、该进程重新启动为止。如果进程在进程管理器外部异常终止或者崩溃，模块状态变更为“严重”，并且运行状况事件消息指示被终止的进程，直到该模块再次运行、该进程重新启动为止。
重新配置检测	该模块确定注册的受管设备上策略应用失败后，检测功能是否继续运行。如果策略应用失败之后，检测功能显示为无法运行，则模块会生成运行状况警报，直至重新建立检测功能。
RRD 服务器进程	该模块确定存储时序数据的轮询数据服务器是否正常运行，并且基于最近 RRD 服务器重新启动的次数发出警报。 该模块仅在防御中心上运行。
安全情报	在涉及安全情报过滤的各种情况 （包括源更新、源损坏和内存问题）下，该模块发出警报。 该模块在所有防御中心中运行，但 DC500 除外，因为它不支持安全情报过滤功能。
时序数据监视器	该模块跟踪已损坏文件在存储时序数据 （例如合规性事件计数）的目录中的存在情况，并且在文件标记为已损坏和已移除时发出警报。 该模块仅在防御中心上运行。

表 68-1　运行状况模块 （续）

模块	说明
时间同步状态	该模块跟踪将 NTP 与 NTP 服务器上的时钟配合使用以获取时间的设备时钟的同步状态，并且在两个时钟的时间差超过十秒钟时发出警报。
URL 过滤监视器	该模块跟踪防御中心和思科云之间的通信，系统在该云处获取经常被访问的 URL 的 URL 过滤 （类别和信誉）数据。如果防御中心无法成功与该云通信或者无法从该云检索更新，则该模块发出警报。 该模块还跟踪防御中心和您启用 URL 过滤的任何受管设备之间的通信。如果防御中心无法将 URL 过滤数据推送到那些设备上，则该模块发出警报。 该模块仅在所有防御中心中运行，但 DC500 除外，因为它不支持 URL 过滤功能。
用户代理状态监视器	当没有为连接到防御中心的任何用户代理检测到心跳时，该模块发出警报。 该模块仅在防御中心上运行。
VPN 状态	当系统检测到 VPN 功能不起作用时，该模块发出警报。 该模块仅在防御中心上运行。

了解运行状况监控配置

许可证：任何环境

需要执行若干步骤设置 FireSIGHT 系统上的运行状况监控，如以下步骤所示：

步骤 1　为设备创建运行状况策略。

您可以为 FireSIGHT 系统中的每种设备设定特定策略、仅为该设备执行适当的测试。

提示　如果要快速启用运行状况监控，而不定制监控行为，您可以应用出于该目的而提供的默认策略。

有关设置运行状况策略的详细信息，请参阅第 68-6 页上的配置运行状况策略。

步骤 2　将运行状况策略应用到要跟踪运行状况的每台设备上。有关可即时应用的默认运行状况策略的信息，请参阅第 68-6 页上的了解默认运行状况策略。

步骤 3　或者，配置运行状况监视器警报。

您可以设置在运行状况级别达到特定运行状况模块的特定严重性级别时触发的邮件、系统日志或 SNMP 警报。

有关设置运行状况监视器警报的详细信息，请参阅第 68-35 页上的配置运行状况监视警报。

在系统中设置运行状况监控之后，您可以随时在 Health Monitor 页面或 Health Events 表视图中查看运行状况。有关查看系统运行状况数据的详细信息，请参阅：

- 第 68-37 页上的使用运行状况监视器
- 第 68-38 页上的使用设备运行状况监视器
- 第 68-43 页上的处理运行状况事件

配置运行状况策略

许可证：任何环境

运行状况策略包含为若干模块配置的运行状况测试标准。您可以控制根据每个设备要运行的运行状况模块、配置每个模块运行的测试中所用的具体限值。有关可在运行状况策略中配置的运行状况模块的详细信息，请参阅第 68-1 页上的了解运行状况监控。

您可以创建在系统中每个设备上应用的一个运行状况策略、定制您计划在特定设备上应用的每个运行状况策略，或者使用为您提供的默认运行状况策略。您也可以导入从另一个防御中心导出的运行状况策略。

当配置运行状况策略时，您决定是否为该策略启用每个运行状况模块。您可以选择用来控制每个已启用模块在每次访问进程的运行状况时报告的运行状况的标准。

有关在防御中心不支持 MDC自动应用的默认运行状况策略的详细信息，请参阅第 68-6 页上的了解默认运行状况策略。

有关详细信息，请参阅：

- 第 68-6 页上的了解默认运行状况策略
- 第 68-7 页上的创建运行状况策略
- 第 68-26 页上的应用运行状况策略
- 第 68-27 页上的编辑运行状况策略
- 第 68-29 页上的比较运行状况策略
- 第 68-31 页上的删除运行状况策略

了解默认运行状况策略

许可证：任何环境

防御中心运行状况监视器包括让您可以轻松、快速实现设备运行状况监控的默认运行状况策略。默认的运行状况策略自动应用到防御中心上。您无法编辑默认的运行状况策略，但是，您可以基于其配置进行复制以创建自定义策略。有关详细信息，请参阅第 68-7 页上的创建运行状况策略。

如果还要监控设备运行状况，您可以将运行状况策略推送到受管设备上。

注　您不能将运行状况策略应用到用于 Blue Coat X-系列的思科 NGIPS上。

在默认的运行状况策略中，运行平台上可用的大多数运行状况模块都可自动启用。下表详细说明在防御中心和受管设备默认策略中激活的模块信息。

表 68-2　　默认活动运行状况模块

模块	防御中心	受管设备
高级恶意软件防护	是	否
设备心跳	是	否
自动应用旁路	否	是
CPU 使用情况	否	否
卡重置	否	否
磁盘状态	是	是

表 68-2　默认活动运行状况模块 （续）

模块	防御中心	受管设备
磁盘使用情况	是	是
FireAMP 状态监视器	是	否
FireSIGHT 主机许可证限制	是	否
硬件告警	否	是
运行状况监视器流程	否	否
内联链路不匹配告警	否	是
接口状态	否	是
入侵事件速率	否	是
许可证监控	是	否
链路状态传播	否	是
内存使用率	是	是
电源	否	是
进程状态	是	是
重新配置检测	否	是
RRD 服务器进程	是	否
安全智能	是	否
时序数据监视器	是	否
时间同步状态	是	是
URL 过滤监视器	是	否
用户代理状态监视器	是	否
VPN 状态	是	否

创建运行状况策略

许可证：任何环境

如果要定制用于设备的运行状况策略，您可以创建一个新策略。策略中的设置初始填充您选定为新策略基础的运行状况策略的设置。您可以按需启用或禁用策略内的模块并更改每个模块的警报标准。

提示　如果不创建新策略，您可以导出另一个防御中心的运行状况策略，然后将其导入防御中心。在应用导入的策略前，您可以进行编辑以满足需求。有关详细信息，请参阅第 A-1 页上的导入和导出配置。

要创建运行状况策略，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **Health > Health Policy**。

系统将显示 Health Policy 页面。

步骤 2　点击 **Create Policy**。

系统将显示 Create Health Policy 页面。

步骤 3　从 **Copy Policy** 下拉列表中选择要用作新策略基础的现有策略。

步骤 4　输入策略名称。

步骤 5　输入策略说明。

步骤 6　选择 **Save** 以保存策略信息。

系统将显示 Health Policy Configuration 页面，其中包括模块列表。

步骤 7　配置要用来测试设备运行状况的每个模块的设置，如以下各节所述：

- 第 68-9 页上的配置策略运行时间间隔
- 第 68-9 页上的配置高级恶意软件防护监控
- 第 68-10 页上的配置设备心跳监控
- 第 68-11 页上的配置自动应用旁路监控
- 第 68-11 页上的配置 CPU 使用率监控
- 第 68-12 页上的配置卡重置监控
- 第 68-12 页上的配置磁盘状态监控
- 第 68-13 页上的配置磁盘使用率监控
- 第 68-14 页上的配置 FireAMP 状态监控
- 第 68-15 页上的配置 FireSIGHT 主机使用情况监控
- 第 68-15 页上的配置硬件告警监控
- 第 68-16 页上的配置运行状况监控
- 第 68-17 页上的配置内联链路不匹配告警监控
- 第 68-17 页上的配置接口状态监控
- 第 68-18 页上的配置入侵事件速率监控
- 第 68-19 页上的了解许可证监控
- 第 68-19 页上的配置链路状态传播监控
- 第 68-19 页上的配置内存使用率监控
- 第 68-20 页上的配置电源监控
- 第 68-21 页上的配置进程状态监控
- 第 68-22 页上的配置重新配置检测监控
- 第 68-22 页上的配置 RRD 服务器进程监控
- 第 68-23 页上的配置安全情报监控
- 第 68-24 页上的配置时序数据监控
- 第 68-24 页上的配置时间同步监控
- 第 68-25 页上的配置 URL 过滤监控
- 第 68-25 页上的配置用户代理状态监控
- 第 68-26 页上的配置 VPN 状态监控

注　对于在配置设置时要运行的测试每个 Health Policy Configuration 页面上运行状况的各个模块，确保已启用。即使包含模块的策略已应用到设备上，禁用的模块也不产生运行状况反馈。

步骤 8　点击 **Save Policy and Exit** 保存策略。

您必须将该策略应用到每个设备以使其生效。有关应用运行状况策略的详细信息，请参阅第 68-26 页上的应用运行状况策略。

配置策略运行时间间隔

许可证：任何环境

您可以通过修改运行状况策略的策略运行时间间隔来控制运行状况测试的运行频率。您可以设置的最大运行时间间隔为 99999 分钟。

注意事项　勿将运行时间间隔设置为少于五分钟。

要配置策略运行时间间隔，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面上，选择 **Policy Run Time Interval**。

系统将显示 Health Policy Configuration - Policy Run Time Interval 页面。

步骤 2　在 **Run Interval (mins)** 字段中，输入在自动重复测试之间经过的分钟数。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置高级恶意软件防护监控

许可证：恶意软件

该模块跟踪防御中心查询思科云和检测网络流量中的文件的能力状态和稳定性。如果系统检测到与该云的连接已中断，用于连接的加密密钥无效，或者在时间范围内检测到的文件数过大时，该模块状态分类变更为“警告”，并且该模块生成运行状况警报。请注意，如果您使用 FireAMP 私有云而且此私有云无法与公共思科云通信，此私有云自身会生成警报；有关详细信息，请参阅*《FireAMP 私有云管理门户用户指南》*。

注　如果防御中心丢失与互联网的连接，系统最多可能需要 30 分钟才能生成一个高级恶意软件防护运行状况警报。

要配置高级恶意软件防护运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面上，选择 Advanced Malware Protection。

系统将显示 Health Policy Configuration - Advanced Malware Protection 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置设备心跳监控

许可证：任何环境

每隔两分钟或每隔 200 个事件 （以先发生的为准），防御中心从其受管设备接收一次心跳，作为设备正在运行和与防御中心正常通信的标志。使用设备心跳运行状况模块跟踪防御中心是否从受管设备接收心跳。如果防御中心检测不到来自设备的心跳，该模块的状态分类变更为“严重”。该状态数据馈送到运行状况监视器中。

要配置设备心跳运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **Appliance Heartbeat**。

系统将显示 Health Policy Configuration - Appliance Heartbeat 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置自动应用旁路监控

许可证：任何环境

使用该模块检测受管设备何时被绕过，因为它在配置为旁路阈值的数秒钟内不做出响应。如果发生旁路，该模块生成警报。该状态数据馈送到运行状况监视器中。

有关自动应用旁路的详细信息，请参阅第 4-47 页上的自动应用旁路。

要配置自动应用旁路监控状态，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面，选择 **Automatic Application Bypass Status**。

系统将显示 Health Policy Configuration - Automatic Application Bypass Status 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的受管设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置 CPU 使用率监控

许可证：任何环境

受支持的设备：任意设备，除了 3D9900 之外

受支持的防御中心：任何环境

CPU 过度使用情况可能表示您需要升级硬件或存在未正常运行的进程。使用 CPU 使用率运行状况模块来设置 CPU 使用率限值。

如果监控设备的 CPU 使用率超过“警告”限值，该模块的状态分类变更为“警告”。如果监控设备的 CPU 使用率超过“重要”限值，该模块的状态分类变更为“严重”。该状态数据馈送到运行状况监视器中。

您可以为每种限值设置的最大百分比是 100%，“严重”限值必须高于告“警告”限值。

要配置 CPU 使用率限值，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面上，选择 **CPU Usage**。

系统将显示 Health Policy Configuration - CPU Usage 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　在 **Critical Threshold %** 字段中，输入应触发严重运行状况的 CPU 使用率百分比。

步骤 4　在 **Warning Threshold %** 字段中，输入应触发警告运行状况的 CPU 使用率百分比。

步骤 5　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置卡重置监控

许可证：任何环境

使用卡重置监控运行状况模块来跟踪何时由于硬件故障导致网卡重启。如果发生重置，该模块生成警报。该状态数据馈送到运行状况监视器中。

要配置卡重置监控，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面，选择 **Card Reset**。

系统将显示 Health Policy Configuration - Card Reset Monitoring 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的防御中心上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置磁盘状态监控

许可证：任何环境

使用磁盘状态运行状况模块监控您的设备硬盘和恶意软件存储包 （如果安装）当前的状态。当硬盘和 RAID 控制器 （如果安装）存在发生故障的危险时，或者，如果安装的其他安装硬盘驱动器不是恶意软件包时，该模块生成“警告” （黄色）运行状况警报。当无法检测到已安装恶意软件存储包时，该模块生成“警报” （红色）运行状况警报。

要配置磁盘状态运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面上，点击 **Disk Status**。

系统将显示 Health Policy Configuration - Disk Status 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置磁盘使用率监控

许可证：任何环境

没有足够的磁盘空间，设备就不能运行。运行状况监视器可以识别在空间用光之前，设备硬盘驱动器和恶意软件存储包的低磁盘空间状况。在硬盘驱动器文件耗尽发生得太频繁时，运行状况监视器还可以发出警报。使用磁盘使用率运行状况模块监控设备上的 `/` 和 `/volume` 分区的磁盘使用率并跟踪耗尽频率。

注　尽管磁盘使用率模块将 `/boot` 分区列为监控分区，但是分区的大小是静态的，因此该模块在引导分区中不发出警报。

如果监控设备的整体磁盘使用率超过警告限值，该模块的状态分类变更为警告。如果监控设备的整体磁盘使用率超过“严重”限值，该模块的状态分类变更为“严重”。您可以为每种限值设置的最大百分比是 100%，“严重”限值必须高于告“警告”限值。

如果系统删除未处理的事件，该模块的状态分类变更为“警告”。如果基于模块阈值，系统耗尽任何磁盘使用率类别中文件的频率太频繁，或者，如果基于模块阈值，不在监控磁盘使用率类别中的文件的磁盘使用率增长太大，则该模块的状态分类变更为“关键”。有关磁盘使用率类别的详细信息，请参阅第 55-22 页上的了解 Disk Usage 构件。

要配置磁盘使用运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面上，选择 **Disk Usage**。

系统将显示 Health Policy Configuration - Disk Usage 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　在 **Critical Threshold %** 字段中，输入应触发严重运行状况的磁盘使用率百分比。

步骤 4　在 **Warning Threshold %** 字段中，输入应触发警告运行状况的磁盘使用率百分比。

步骤 5　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置 FireAMP 状态监控

许可证：任何环境

使用 FireAMP 状态监控模块在以下情况下将您发出警报：

- 在初始连接成功后，防御中心无法连接到思科云
- 您使用 FireAMP 门户取消注册云连接
- 您的 FireAMP 私有云无法与公共思科云通信

在这些情况下，模块状态变更为“严重”并且提供与失败的连接相关的云名称。有关配置云连接的信息，请参阅第 37-21 页上的为 FireAMP 处理云连接。

要配置 FireAMP 状态监控模块的设置，请参阅：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面，选择 **FireAMP Status Monitor**。

系统将显示 Health Policy Configuration - FireAMP Status Monitor 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行 FireAMP 状态监控。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到防御中心上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置 FireSIGHT 主机使用情况监控

许可证：FireSIGHT

使用 FireSIGHT 主机许可证限制运行状况模块来设置 FireSIGHT 主机数量警告限制。如果监控设备上剩余 FireSIGHT 主机的数量低于“警告主机”限值，该模块的状态分类变更为“警告”。如果监控设备上剩余 FireSIGHT 主机的数量低于“严重主机”限值，该模块的状态分类变更为“严重”。该状态数据馈送到运行状况监视器中。

您可以为每种限值设置的最大主机数是 1000，“严重”主机限值数必须低于“警告”限值。

要配置 FireSIGHT 主机许可证限制运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1 在 Health Policy Configuration 页面中，选择 **FireSIGHT Host License Limit**。

系统将显示 Health Policy Configuration - FireSIGHT Host License Limit 页面。

步骤 2 为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3 在 **Critical number Hosts** 字段中，输入应触发严重运行状况的剩余可用主机的数量。

步骤 4 在 **Warning number Hosts** 字段中，输入应触发警告运行状况的剩余可用主机的数量。

步骤 5 您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置硬件告警监控

许可证：任何环境

受支持的设备：3 系列、 3D9900

使用硬件告警运行状况模块来检测 **3 系列**或 3D9900 设备上的硬件故障。如果硬件告警模块找到已经出现故障的硬件组件或者已集群互相不通信的设备的硬件组件，该模块的状态分类变更为“严重”。该状态数据馈送到运行状况监视器中。

有关可以导致 3D9900 设备发出硬件警告的硬件状态条件的详细信息，请参阅第 68-47 页上的解释 3D9900 设备的硬件警报详细信息。

要配置硬件告警运行状况模块的设置，请参阅：

访问：管理员/维护人员

步骤 1 在 Health Policy Configuration 页面上，选择 **Hardware Alarms**。

系统将显示 Health Policy Configuration - Hardware Alarm Monitor 页面。

步骤 2 为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置运行状况监控

许可证：任何环境

使用运行状况监视器流程模块监控防御中心上运行状况监视器的运行状况，方式为当监控设备收到的运行状况事件之间经过太多分钟数时生成警报。

例如，如果防御中心 (`myrtle.example.com`) 监控设备 (`dogwood.example.com`)，您在启用运行状况监视器流程模块的运行状况策略应用到 `myrtle.example.com`。运行状况监视器流程模块然后报告事件，指示自接收到来自 `dogwood.example.com` 的最后事件以来经过多少分钟数。

您可以配置导致生成警报的在事件之间经过的持续时间，以分钟为单位。如果等待的时间超过自上次事件限制以来“警告分钟数”中配置的分钟数，该模块的状态分类变更为“警告”。如果等待的时间超过自上次事件限制以来的“严重分钟数”，该模块的状态分类变更为“严重”。该状态数据馈送到运行状况监视器中。

您可以为每种限值设置的最长分钟数是 144，“严重”限值必须高于“警告”限值。最短分钟数是 5。

要配置运行状况监视器流程模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **Health Monitor Process**。

系统将显示 Health Policy Configuration - Health Monitor Process 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　在 **Critical Minutes since last event** 字段中，输入在触发严重运行状况之前在事件之间可以等待的最长分钟数。

步骤 4　在 **Warning Minutes since last event** 字段中，输入在触发警告运行状况之前在事件之间可以等待的最长分钟数。

步骤 5　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

您必须将运行状况策略应用到防御中心中以使设置生效。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置内联链路不匹配告警监控

许可证：任何环境

使用内联链路不匹配告警运行状况模块来跟踪在内联集的任一侧接口何时协商不同的连接速度。如果检测到不同的协商速度，该模块生成警报。

要配置内联链路不匹配监控，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **Inline Link Mismatch Alarms**。

系统将显示 Health Policy Configuration - Inline Link Mismatch Alarms 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的防御中心上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置接口状态监控

许可证：FireSIGHT

使用接口状态运行状况模块可检测设备是否接收到流量。如果接口状态模块确定设备未接收流量，则该模块的状态分类会变更为 Critical。该状态数据馈送到运行状况监视器中。

注　标记为 `DataPlaneInterfacex` 的接口（其中 `x` 是一个数值）是 ASA 内部接口（不是用户定义的），涉及系统中的数据包流。

要配置接口状态运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **Interface Status**。

系统将显示 Health Policy Configuration — Interface Status 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。

- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置入侵事件速率监控

许可证：保护

使用入侵事件速率运行状况模块来设置触发运行状况更改的每秒钟数据包数量的限值。如果监听设备上的事件速率超过每秒事件 （警告）限值中配置的每秒事件的数量，该模块的状态分类变更为“警告”。如果事件速率超过每秒事件 （严重）限值中配置的每秒事件的数量，该模块的状态分类变更为“严重”。该状态数据馈送到运行状况监视器中。

通常，网段的事件速率平均为每秒 20 个事件。对于具有本平均速率的网段，每秒事件 （严重）数应设置为 50，每秒事件 （警告）数应该设置 为30。要确定系统的限值，请在 Statistics 页面找到设备的 Events/Sec 值 (**System > Monitoring > Statistics**)，然后使用以下公式计算限值：

- 每秒事件 （严重）数 = Events/Sec * 2.5
- 每秒事件 （警告）数 = Events/Sec * 1.5

您可以为每种限值设置的最大事件数是 999，“严重”限值必须高于“警告”限值。

要配置入侵事件速率监控运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **Intrusion Event Rate**。

系统将显示 Health Policy Configuration - Intrusion Event Rate 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　在 **Events per second (Critical)** 字段中，输入应触发严重运行状况的每秒钟事件的数量。

步骤 4　在 **Events per second (Warning)** 字段中，输入应触发警告运行状况的每秒钟事件的数量。

步骤 5　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

了解许可证监控

许可证：任何环境

使用许可证监控运行状况模块来确定是否有足够的许可证可用于可控性、保护、 URL 过滤、恶意软件和 VPN。如果剩余的许可证数量较低或不足，则该模块发出警报。

如果系统检测到堆叠配置中的设备不匹配许可证集 （堆叠的设备必须有相同的许可证集），则该模块也发出警报。

许可证监控模块自动进行配置。由于您无法更改或禁用该模块，因此它不会显示在 Health Policy Configuration 页面上。

配置链路状态传播监控

许可证：任何环境

使用链路状态传播运行状况模块来检测内联对中的链路状态传播状态。如果链路状态传播到该对，该模块的状态分类变更为“严重”，并且状态读作：

```
Module Link State Propagation: ethx_ethy is Triggered
```

其中 *x* 和 *y* 为成对的接口编号。

要配置链路状态传播运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **Link State Propagation**。

系统将显示 Health Policy Configuration - Link State Propagation monitor 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置内存使用率监控

许可证：任何环境

使用内存使用率运行状况模块来设置内存使用率限值。该模块通过考虑可用内存、缓存内存和交换内存来计算可用内存。如果监控设备的内存使用率超过“警告”限值，该模块的状态分类变更为“警告”。如果监控设备的内存使用率超过“严重”限值，该模块的状态分类变更为“严重”。该状态数据馈送到运行状况监视器中。

对于内存超过 4 GB 的设备而言，基于一个公式来预设警报阈值，该公式计算在可能导致系统问题的可用内存中所占的比例。

注　在内存超过 4 GB 的设备上，因为“警告”和“严重”阈值之间的时间间隔可能非常短，所以思科建议您将 **Warning Threshold %** 值手动设置为 50。这将进一步确保您及时收到设备的内存警报来解决问题。

您可以为每种限值设置的最大百分比是 100%，“严重”限值必须高于告“警告”限值。

注　如果您应用启用了许多 FireSIGHT 功能（例如安全情报、文件捕获、具有许多规则的入侵策略或 URL 过滤）的访问控制策略，则当某些低端 ASA FirePOWER 设备的内存分配已达到最大容许程度时，设备可能生成短暂的内存使用率警告。

要配置内存使用率运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面上，选择 **Memory Usage**。

系统将显示 Health Policy Configuration - Memory Usage 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　在 **Critical Threshold %** 字段中，输入应触发严重运行状况的内存使用率百分比。

步骤 4　在 **Warning Threshold %** 字段中，输入应触发警告运行状况的内存使用率百分比。

步骤 5　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置电源监控

许可证：任何环境

受支持的设备：3D3500、 3D4500、 3D6500、 3D9900、 3 系列

受支持的防御中心：DC1500、 DC2000、 DC3500、 DC4000

使用电源运行状况模块来检测任何支持的平台上的电源故障。如果该模块找到没有电的电源，该模块的状态分配变更为“无电”。如果该模块没有检测到电源的存在，状态变更为“严重错误”。该状态数据馈送到运行状况监视器中。您可以在运行状况监视器上展开警报详细信息列表上的电源项目，以查看每个电源的特定状态项。

要配置电源运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面上，选择 **Power Supply**。

系统将显示 Health Policy Configuration - Power Supply 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置进程状态监控

许可证：任何环境

使用进程状态运行状况模块来监控在设备上运行的进程在进程管理器外部退出或终止的状况。进程状态模块对进程结束的响应取决于进程如何结束。

- 如果进程在进程管理器内部终止，该模块不报告任何运行状况事件。
- 如果进程在进程管理器外部被故意退出，模块状态变更为“警告”，并且运行状况事件消息指示哪一个进程被退出，直到该模块再次运行、该进程重新启动为止。
- 如果进程在进程管理器外部异常终止或者崩溃，模块状态变更为“严重”，并且运行状况事件消息指示被终止的进程，直到该模块再次运行、该进程重新启动为止。

要配置进程状态运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **Process Status**。

系统将显示 Health Policy Configuration - Process Status 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置重新配置检测监控

许可证：任何环境

使用重新配置检测监控模块可确定向受管设备应用某策略后检测功能的状态。如果策略应用失败并且检测停止运行，则模块会在 Health Events 中生成警报。

要配置时序数据监控的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **Reconfiguring Detection**。

系统将显示 Health Policy Configuration — Reconfiguring Detection 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块生成运行状况警报。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置 RRD 服务器进程监控

许可证：任何环境

使用 RRD 服务器进程模块查看存储时序数据的 RRD 服务器是否正常工作。如果自上次 RRD 服务器更新后其重新启动，则该模块将发出警报；如果在 RRD 服务器重新启动后连续更新的次数达到模块配置中指定的次数，则该模块将输入“严重”或“警告”状态。

要配置 RRD 服务器进程监控的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **RRD Server Process**。

系统将显示 Health Policy Configuration - RRD Server Process 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　在 **Critical Number of restarts** 字段中，输入应触发严重运行状况的检测到的连续 RRD 服务器重置的次数。

步骤 4　在 **Warning Number of restarts** 字段中，输入应触发警告运行状况的检测到的连续 RRD 服务器重置的次数。

步骤 5　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。

- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置安全情报监控

许可证：保护

受支持的防御中心：除 DC500 外的所有型号

使用安全情报模块以在涉及安全情报过滤的各种情况下向您发出警告。如果安全情报正在使用中并且发生以下状况，该模块发出警报：

- 防御中心无法更新源，或者如果源数据损坏或不包含可识别的 IP 地址
- 受管设备在从防御中心接收安全情报数据方面存在问题
- 由于内存问题，受管设备无法加载防御中心为其提供的所有安全情报数据

提示 如果在运行状况监视器中显示安全情报内存警告，则您可以重新应用受影响的设备的访问控制策略以增加分配给安全情报的内存；请参阅第 12-13 页上的应用访问控制策略。

有关安全情报过滤的详细信息，请参阅第 13-1 页上的使用安全情报 IP 地址信誉实施黑名单和第 3-4 页上的使用安全情报列表和源。

要配置安全情报模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **Security Intelligence**。

系统将显示 Health Policy Configuration - Security Intelligence 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行安全情报监控。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置时序数据监控

许可证：任何环境

使用时序数据监视器模块来监控系统已存储的时序数据的状态（例如合规性事件列表）。该模块扫描已损坏文件的时序数据存储目录。如果该模块找到损坏的数据，它进入“警告”状态并报告所有受影响文件的名称。

要配置时序数据监控的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **Time Series Data Monitor**。

系统将显示 Health Policy Configuration - Time Series Data Monitor 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置时间同步监控

许可证：任何环境

使用时间同步状态模块来检测何时使用 NTP 从 NTP 服务器获取时间的受管设备的时间与服务器时间有 10 秒或更长时间的差异。

要配置时间同步监控设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **Time Synchronization Status**。

系统将显示 Health Policy Configuration - Time Synchronization Status 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置 URL 过滤监控

许可证：URL 过滤

受支持的防御中心：除 DC500 外的所有型号

使用 URL 过滤监视器模块来跟踪防御中心和思科云之间的通信，系统在该云处获取通常被访问的 URL 的 URL 过滤 （类别和信誉）数据。如果防御中心无法成功与该云通信或者无法从该云检索更新，则该模块的状态变更为“严重”。

在高可用性配置中，只有主防御中心和 URL 过滤云通信；该模块的所有数据仅指该主要设备。

URL 过滤监视器模块也跟踪防御中心和您已启用 URL 过滤的任何受管设备之间的通信。如果防御中心与该云成功通信，并且防御中心无法将新 URL 过滤数据推送到其受管设备，该模块状态变更为“警告”。

要配置 URL 过滤监视器运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **URL Filtering Monitor**。

系统将显示 Health Policy Configuration - URL Filtering Monitor 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到防御中心上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置用户代理状态监控

许可证：FireSIGHT

可以使用用户代理状态监控器运行状况模块来监控与防御中心连接的代理的心跳。如果您在应用的运行状况策略中启用该模块，并且防御中心未检测到防御中心配置的任何代理的心跳，则该模块生成运行状况警报。

要配置用户代理状态监视器运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面中，选择 **User Agent Status Monitor**。

系统将显示 Health Policy Configuration - User Agent Status Monitor 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。

- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到防御中心上。有关详情，请参见第 68-26 页上的应用运行状况策略。

配置 VPN 状态监控

许可证：VPN

受支持的防御中心：任何防御中心，除了 2 系列

使用 VPN 状态运行状况模块来监控您配置的网关 VPN 隧道当前的状态；系统将显示每个隧道的信息。当任何 VPN 隧道不工作时，该模块生成一个“严重”（红色）运行状况警报。

要配置 VPN 状态运行状况模块的设置，请执行以下操作：

访问：管理员/维护人员

步骤 1　在 Health Policy Configuration 页面上，点击 **VPN Status**。

系统将显示 Health Policy Configuration - VPN Status 页面。

步骤 2　为 **Enabled** 选项选择 **On**，以允许使用该模块进行运行状况测试。

步骤 3　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

如果想要设置生效，必须将运行状况策略应用到适当的设备上。有关详情，请参见第 68-26 页上的应用运行状况策略。

应用运行状况策略

许可证：任何环境

当您将运行状况策略应用到设备时，您在策略中启用的所有模块的运行状况测试自动监控设备上的进程和硬件的运行状况。然后，运行状况测试继续以您在策略中配置的时间间隔运行，为设备收集运行状况数据并将该数据转发到防御中心。

如果您在运行状况策略中启用一个模块，然后将该策略应用到不需要该运行状况测试的设备，则运行状况监视器报告该运行状况模块的状态为禁用。

如果您将启用所有模块的策略应用到设备中，它从该设备移除所有已应用的运行状况策略，以便不应用任何运行状况策略。

当您将不同的策略应用到已应用策略的设备时，请基于新应用的测试在显示新数据时使用一些延迟。

注　在高可用性对中在防御中心中创建的自定义运行状况策略将复制到两台设备上。但是，对默认运行状况策略的变更不会复制；每台设备使用为该设备配置的本地默认运行状况策略。

要应用运行状况策略，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **Health > Health Policy**。

系统将显示 Health Policy 页面。

步骤 2　点击要应用的策略旁的应用图标 ( )。

系统将显示 Health Policy Apply 页面。

提示　Health Policy 列旁边的状态图标 ( ) 指示该设备的当前运行状况。System Policy 列旁边的状态图标 ( ) 指示防御中心与设备之间的通信状态。请注意，您可以通过点击移除图标来移除当前应用的策略 ( )。

步骤 3　选择要应用运行状况策略的设备。

步骤 4　点击 **Apply** 以将该策略应用到所选设备上。

系统将显示 Health Policy 页面，其中显示一条消息，指示该策略应用是否成功。只要成功应用该策略，设备监控即开始。

编辑运行状况策略

许可证：任何环境

您可以通过启用或禁用模块或者更改模块设置来修改运行状况策略。如果您修改已应用到设备的策略，直到您重新应用该策略，更改都不会生效。

下表列出各种设备的适用运行状况模块。

表 68-3　　适用于设备的运行状况模块

模块	适用的设备
高级恶意软件防护	防御中心，除了 DC500 之外
设备心跳	防御中心
自动应用旁路状态	任何受管设备
CPU 使用情况	任意设备，除了 3D9900 之外
卡重置	任何受管设备
磁盘状态	任何环境
磁盘使用情况	任何环境
FireAMP 状态监视器	防御中心
FireSIGHT 主机许可证限制	防御中心
硬件告警	3 系列、 3D9900

表 68-3　适用于设备的运行状况模块 （续）

模块	适用的设备
运行状况监视器流程	防御中心
内联链路不匹配告警	任何受管设备
接口状态	任何受管设备
入侵事件速率	带保护的受管设备
许可证监控	防御中心
链路状态传播	带保护的受管设备
内存使用率	任何环境
电源	防御中心：DC1500、 DC2000、 DC3500、 DC4000 设备：3D3500、 3D4500、 3D6500、 3D9900、 3 系列
进程状态	任何环境
重新配置检测	
RRD 服务器进程	防御中心
安全智能	防御中心，除了 DC500 之外
时序数据监视器	防御中心
时间同步状态	任何环境
URL 过滤监视器	防御中心，除了 DC500 之外
用户代理状态监视器	防御中心
VPN 状态	防御中心

要编辑运行状况策略，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **Health > Health Policy**。

系统将显示 Health Policy 页面。

步骤 2　点击要修改的策略旁边的编辑图标 ( )。

系统将显示 Health Policy Configuration 页面，其中选定 Policy Run Time Interval 设置。

步骤 3　根据需要修改设置，如以下各节所述：

- 第 68-9 页上的配置策略运行时间间隔
- 第 68-9 页上的配置高级恶意软件防护监控
- 第 68-10 页上的配置设备心跳监控
- 第 68-11 页上的配置自动应用旁路监控
- 第 68-11 页上的配置 CPU 使用率监控
- 第 68-12 页上的配置卡重置监控
- 第 68-12 页上的配置磁盘状态监控
- 第 68-13 页上的配置磁盘使用率监控

- 第 68-14 页上的配置 FireAMP 状态监控
- 第 68-15 页上的配置 FireSIGHT 主机使用情况监控
- 第 68-15 页上的配置硬件告警监控
- 第 68-16 页上的配置运行状况监控
- 第 68-17 页上的配置内联链路不匹配告警监控
- 第 68-18 页上的配置入侵事件速率监控
- 第 68-19 页上的了解许可证监控
- 第 68-19 页上的配置链路状态传播监控
- 第 68-19 页上的配置内存使用率监控
- 第 68-20 页上的配置电源监控
- 第 68-21 页上的配置进程状态监控
- 第 68-22 页上的配置重新配置检测监控
- 第 68-22 页上的配置 RRD 服务器进程监控
- 第 68-23 页上的配置安全情报监控
- 第 68-24 页上的配置时序数据监控
- 第 68-24 页上的配置时间同步监控
- 第 68-25 页上的配置 URL 过滤监控
- 第 68-25 页上的配置 URL 过滤监控
- 第 68-25 页上的配置用户代理状态监控
- 第 68-26 页上的配置 VPN 状态监控

步骤 4　您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对该模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

步骤 5　将该策略重新应用到适当的设备中，如第 68-26 页上的应用运行状况策略所述。

比较运行状况策略

许可证：任何环境

要查看遵守公司标准或优化运行状况监控性能的策略更改，您可以检查两个运行状况策略之间的差异。对于您可以访问的运行状况策略，您可以比较任意两个运行状况策略或者同一运行状况策略的两个修订版。要将活动运行状况策略与另一个策略进行快速比较，您可以选择 **Running Configuration** 选项。比较之后，可以生成 PDF 报告，记录两个策略或两个版本的策略之间的区别。

您可以使用两个工具来比较运行状况策略或运行状况策略修订版：

- 比较视图以并列格式仅显示两个运行状况策略或运行状况策略修订版之间的差异；每个策略或策略修订版的名称显示在比较视图左右两侧的标题栏中。

  您可以使用该工具在网络界面上查看和导航两个策略修订版，其中突出显示其差异。

- 比较报告创建仅包含两个运行状况策略或运行状况策略修订版之间差异的记录，采用的格式类似于运行状况策略报告，但是为 PDF 格式。

  可以将其用于保存、复制、打印和共享策略比较，以备进一步检查。

有关了解和使用运行状况策略比较工具的详细信息，请参阅：

- 第 68-30 页上的使用运行状况策略比较视图
- 第 68-30 页上的使用运行状况策略比较报告

使用运行状况策略比较视图

许可证：任何环境

比较视图以并列格式显示两个运行状况策略或策略修订版，每个策略或策略修订版在比较视图的左右两侧标题栏上通过名称来识别。最近一次修改的时间和执行最后一次修改的用户显示在策略名称右侧。请注意， Health Policy 页面显示上次修改策略的时间，用本地时间表示，但是运行状况策略报告列出的时间修改为以 UTC 表示。

系统突出显示两个运行状况策略或策略修订版之间的差异：

- 蓝色表示两个策略或两个版本中此突出显示的设置不同。并且用红色文本注明其不同之处。
- 绿色表示此突出显示的设置在一个策略或一个版本中出现了，而在另一个策略或版本中却没有出现。

您可以执行下表中的任何操作。

表 68-4　　运行状况策略比较视图操作

要.....	您可以.....
逐一浏览更改	点击标题栏上方的 **Previous** 或 **Next**。 在左右两侧之间以双箭头图标 (◂▸) 为中心移动， **Difference** 数字调整为识别您正在查看哪个差异。
生成新的运行状况策略比较视图	点击 **New Comparison**。 系统将显示 **Select Comparison** 窗口。有关详情，请参见使用运行状况策略比较报告。
生成运行状况策略比较报告	点击 **Comparison Report**。 运行状况策略比较报告创建一个 PDF，其中包含的信息与比较视图相同。

使用运行状况策略比较报告

许可证：任何环境

运行状况策略比较报告是运行状况策略比较视图识别的两个运行状况策略或同一运行状况策略的两个修订版的所有差异的记录，以 PDF 格式呈现。您可以使用此报告进一步检查两个运行状况策略配置之间的差异并且保存和发布结果。

您可以从已访问的任何运行状况策略的比较视图生成运行状况策略比较报告。请记住，在生成运行状况策略报告之前，需要提交任何潜在的变更；只有提交的更改才显示在报告中。

根据您的配置，运行状况策略比较报告可以包含一个或多个部分。每个分区使用相同的格式并提供相同级别的详细信息。请注意， Value A 和 Value B 列代表您在比较视图中配置的策略或策略修订版。

提示　您可以使用类似的操作步骤比较 SSL、网络分析、入侵、文件、系统或访问控制策略。

要比较两个运行状况策略或同一策略的两个修订版，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **Health > Health Policy**。

系统将显示 Health Policy 页面。

步骤 2　点击 **Compare Policies**。

系统将显示 Select Comparison 窗口。

步骤 3　从 **Compare Against** 下拉列表中选择要进行比较的类型：

- 要比较两个不同的策略，请选择 **Other Policy**。
- 要比较同一策略的两个修订版，请选择 **Other Revision**。
- 要将另一策略与当前活动的策略进行比较，请选择 **Running Configuration**。

请记住，在生成运行状况策略报告之前，需要提交任何变更；只有提交的更改才显示在报告中。

步骤 4　根据您选择的比较类型，有以下选项可供选择：

- 如果您比较两个不同的策略，请从 **Policy A** 和 **Policy B** 下拉列表中选择要比较的策略。
- 如果您比较同一策略的两个修订版，请从 **Policy** 下拉列表中选择该策略，然后从 **Revision A** 和 **Revision B** 下拉列表中选择要比较的修订版。
- 如果您将正运行的配置与另一策略进行比较，请从 **Policy B** 下拉列表中选择第二个策略。

步骤 5　点击 **OK** 显示运行状况策略比较视图。

系统将显示比较视图。

步骤 6　点击 **Comparison Report** 生成运行状况策略比较报告。

系统将显示运行状况策略报告。根据浏览器设置，报告可能会显示在弹出窗口中，或者系统会提示您将报告保存到您的计算机上。

删除运行状况策略

许可证：任何环境

您可以删除不再需要的运行状况策略。如果您删除仍然应用于设备的策略，直到您应用不同的策略，该策略设置仍然有效。此外，如果您删除应用到设备的运行状况策略，直到您禁用基础的相关警报响应，该设备仍在生效的任何运行状况监控警报仍然处于活动状态；请参阅第 43-7 页上的启用和禁用警报响应。

提示　要停止设备的运行状况监控，请创建一个所有模块都禁用的运行状况策略并将其应用到设备。有关创建运行状况策略的详细信息，请参阅第 68-7 页上的创建运行状况策略。有关应用运行状况策略的详细信息，请参阅第 68-26 页上的应用运行状况策略。

要删除运行状况策略，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **Health > Health Policy**。

系统将显示 Health Policy 页面。

步骤 2　点击要删除的策略旁边的删除图标 ( )。

系统将显示一则消息，指示删除是否成功。

使用运行状况监视器黑名单

许可证：任何环境

在正常的网络维护过程中，您禁用设备或使其暂时不可用。因为这些中断是故意为之的，您不希望来自这些设备的运行状况影响防御中心上的摘要运行状况。

您可以使用运行状况监视器黑名单功能禁用对设备或模块的运行状况监控状态报告。例如，如果您知道一个网段将不可用，因为到该网段上受管设备的连接失效，所以您可以临时禁用对该设备的运行状况监控，以禁止防御中心上的运行状况显示警告或严重状态。

当您禁用运行状况监控状态时，仍会生成运行状况事件，但是它们处于禁用状态，不会影响运行状况监视器的运行状况。如果您从黑名单移除设备或模块，列入黑名单过程中生成的事件继续显示禁用的状态。

要在设备上临时禁用运行状况事件，请转到黑名单配置页面并将设备添加至黑名单。在设置生效后，系统在计算整体运行状况时，不再包含列入黑名单的设备。 Health Monitor Appliance Status Summary 列出处于禁用状态的设备。

有时，只将设备上的单个运行状况监控模块列入黑名单可能更实用。例如，当用完设备上的 FireSIGHT 主机许可证时，您可以将 FireSIGHT 主机许可证限制状态消息列入黑名单。

请注意，在 Health Monitor 主页面，如果您通过点击该状态行上的箭头来展开以查看具有特定状态的设备列表，就可以区分被列入黑名单的设备。有关展开该视图的详细信息，请参阅第 68-37 页上的使用运行状况监视器。

在您展开被列入黑名单或部分被列入黑名单的设备的视图后，可以看见黑名单图标 ( ) 和注释。

注　在防御中心，运行状况监视器黑名单设置是本地配置设置。因此，如果您将设备列入黑名单，接着将其删除，然后使用防御中心重新注册，黑名单设置保持不变。最近重新注册的设备仍旧被列入黑名单。

有关详情，请参阅：

- 第 68-33 页上的将运行状况策略或设备列入黑名单
- 第 68-33 页上的将设备列入黑名单
- 第 68-34 页上的将运行状况策略模块列入黑名单

将运行状况策略或设备列入黑名单

许可证：任何环境

如果要为具有特定运行状况策略的所有设备禁用运行状况事件，您可以将该策略列入黑名单。如果您需要禁用一组设备的运行状况监控的结果，可以将该组设备列入黑名单。在黑名单设置生效后，设备在 Health Monitor Appliance Module Summary 和 Device Management 页面显示为禁用状态。设备的运行状况事件具有禁用的状态。

请注意，如果防御中心采用高可用性配置，您可以将高可用性对等体而不是另一个对等体上的受管设备列入黑名单。您还可以将高可用性对等体列入黑名单，使其标记其所生成的事件，并将从其接收运行状况事件的设备标记为禁用。在高可用性对中的 防御中心可以选择将其对等体完全或部分列入黑名单中。

要将整个运行状况策略或一组设备列入黑名单，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **Health > Blacklist**。

系统将显示 Blacklist 页面。

步骤 2　使用右侧的下拉列表按组、策略或型号对列表进行排序。（防御中心上的组是受管设备。）

请注意，将某些但不是全部运行状况模块列入黑名单的设备将显示为 **(Partially Blacklisted)**。如果您在黑名单主页面编辑其黑名单状态，可以将那些设备上的所有模块列入黑名单或者移除列入黑名单的所有条目。有关将设备上的单个运行状况模块列入黑名单的信息，请参阅第 68-34 页上的将运行状况策略模块列入黑名单。

提示　Health Policy 列 () 旁边的状态图标指示该设备的当前运行状况。System Policy 列 () 旁边的状态图标指示防御中心与设备之间的通信状态。

步骤 3　此时您有两种选择：

- 要将组、型号或策略类别中的所有设备列入黑名单，请选择该类别，然后点击 **Blacklist Selected Devices**。
- 要将在组、型号或策略类别中的所有设备都清除出黑名单，请选择该类别，然后点击 **Clear Blacklist on Selected Devices**。

页面刷新，现在指示设备的新黑名单状态。

将设备列入黑名单

许可证：任何环境

如果需要将单个设备的事件和运行状况设置为禁用，您可以将该设备列入黑名单。在黑名单设置生效后，该设备在 Health Monitor Appliance Module Summary 上显示为禁用，并且该设备的运行状况事件具有禁用状态。

要将单个设备列入黑名单，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **Health > Blacklist**。

系统将显示 Blacklist 页面。

步骤 2　使用右侧的下拉列表按设备组、型号或者策略对列表进行排序。

步骤 3　此时您有两种选择：

- 要将组、型号或策略类别中的所有设备列入黑名单，请选择该类别，然后点击 **Blacklist Selected Devices**。
- 要将在组、型号或策略类别中的所有设备都清除出黑名单，请选择该类别，然后点击 **Clear Blacklist on Selected Devices**。

页面刷新并显示设备的新黑名单状态。点击 **Edit** 并查看第 68-34 页上的将运行状况策略模块列入黑名单以将单个运行状况策略模块列入黑名单。

将运行状况策略模块列入黑名单

许可证：任何环境

您可以将设备上的单个运行状况策略模块列入黑名单。您可能想要执行此操作以禁止来自模块的事件将设备的状态变更为警告或严重。

当模块的任何部分被列入黑名单时，该模块行以黑体形式显示在防御中心网络界面上。

提示　在黑名单设置生效后，设备在 Blacklist 页面和 Appliance Health Monitor Module Status Summary（但是仅在 Appliance Status Summary 主页面的展开的视图中）上显示为 **Partially Blacklisted** 或 **All Modules Blacklisted**。确保您跟踪单独列入黑名单的模块，以便您可以在需要时重新激活它们。如果您意外地禁用模块，则可能漏掉所需的警告或严重消息。

要将单个运行状况策略模块列入黑名单，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **Health > Blacklist**。

系统将显示 Blacklist 页面。

步骤 2　按 Group、 Policy 或 Model 排序，然后点击 **Edit** 显示设备的运行状况策略模块列表。

系统将显示运行状况策略模块。

步骤 3　选择要列入黑名单的每个模块。

步骤 4　点击 Save。

配置运行状况监视警报

许可证：任何环境

您可以设置警报以在运行状况策略中的模块状态变更时，通过电子邮件、 SNMP 或系统日志通知您。您可以将现有警报响应与运行状况事件级别相关联，以在特定级别的运行状况事件发生时触发和发出警报。

例如，如果您担心设备可能用尽硬盘空间，可以在剩余磁盘空间达到警告级别时自动向系统管理员发送一封电子邮件。如果硬盘驱动器继续加载，您可以在硬盘驱动器达到严重性级别时发送第二封电子邮件。

有关详细信息，请参阅：

- 第 68-35 页上的创建运行状况监视器警报
- 第 68-36 页上的解释运行状况监控器警报
- 第 68-36 页上的编辑运行状况监视器警报
- 第 68-37 页上的删除运行状况监视器警报

创建运行状况监视器警报

许可证：任何环境

当您创建运行状况监视器警报时，您可以在严重性级别、运行状况模块和警报响应之间建立关联。您可以使用现有警报或特别配置新的警报以报告系统运行状况。当选定的模块发生严重性级别时，警报触发。

请注意，如果您以复制现有阈值的方式创建或更新阈值，将会收到冲突通知。当存在重复的阈值时，运行状况监视器使用生成最少警报的阈值并忽略其他阈值。该阈值的超时值必须介于 5 和 4,294,967,295 分钟之间。

要创建运行状况监视器警报，请执行以下操作：

访问：管理

步骤 1　选择 **Health > Health Monitor Alerts**。

系统将显示 Health Monitor Alerts 页面。

步骤 2　在 **Health Alert Name** 字段中键入一个运行状况警报的名称。

步骤 3　从 **Severity** 列表中选择要用来触发警报的严重性级别。

步骤 4　从 **Module** 列表中选择您希望警报适用于的模块。

提示　要选择多个模块上，请按 Shift + Ctrl 键并点击模块名称。

步骤 5　从 **Alert** 列表中选择在达到选定的严重性级别时您希望触发的警报响应。

提示　点击 **Alerts** 打开 Alerts 页面。有关创建警报的详细信息，请参阅第 43-2 页上的使用警报响应。

步骤 6　或者，在 **Threshold Timeout** 字段中，键入在每个阈值期间结束和阈值计数重置之前应过去的分钟数。默认值为 5 分钟。

请注意，即使策略运行时间间隔值小于阈值超时值，给定模块的两个已报告运行状况事件之间的时间间隔也始终更大，即如果阈值超时为 8 分钟并且策略运行时间间隔为 5 分钟，则两个已报告事件之间将有 10 分钟的时间间隔 (5 x 2)。

步骤 7　点击 **Save** 保存运行状况警报。

系统将显示一则消息，指示警报配置是否保存成功。 Active Health Alerts 列表现在包括您创建的警报。

解释运行状况监控器警报

许可证：任何环境

运行状况监控器生成的警报包含以下信息：

- 严重程度，指明警报的严重性级别。
- 模块，指定其测试结果触发警报的运行状况模块。
- 说明，包括触发警报的运行状况测试结果。

有关运行状况警报严重性级别的详细信息，请参阅下表。

表 68-5　　警报严重程度

严重性	说明
严重	运行状况测试结果符合触发“严重”警报状态的标准。
警告	运行状况测试结果符合触发“警告”警报状态的标准。
正常状态	运行状况测试结果符合触发“正常”警报状态的标准。
错误	运行状况测试未运行。
已恢复	运行状况测试结果符合在“严重”或“警告”警报状态之后返回到正常警报状态的条件。

有关运行状况模块的详细信息，请参阅第 68-3 页上的了解运行状况模块。

编辑运行状况监视器警报

许可证：任何环境

您可以编辑现有运行状况监视器警报以更改与运行状况监控器警报相关的严重性级别、运行状况模块或警报响应。

要编辑运行状况监视器警报，请执行以下操作：

访问：管理

步骤 1　选择 **Health > Health Monitor Alerts**。

系统将显示 Health Monitor Alerts 页面。

步骤 2　选择您要在 **Active Health Alerts** 列表中修改的警报。

步骤 3　点击 **Load** 加载选定警报的配置设置。

步骤 4　根据需要修改设置。有关详细信息，请参阅第 68-35 页上的创建运行状况监视器警报。

步骤 5　点击 **Save** 修改运行状况警报。

系统将显示一则消息，指示警报配置是否保存成功。

删除运行状况监视器警报

许可证：任何环境

您可以删除现有的运行状况监视器警报。

注　删除运行状况监视器警报不会删除相关的警报响应。您必须禁用或删除基础的警报响应，以确保不会继续发出警报。有关详细信息，请参阅第 43-7 页上的启用和禁用警报响应和第 43-7 页上的删除警报响应。

要删除运行状况监视器警报，请执行以下操作：

访问：管理

步骤 1　选择 **Health > Health Monitor Alerts**。

系统将显示 Health Monitor Alerts 页面。

步骤 2　选择您要在 **Active Health Alerts** 列表中删除的警报。

步骤 3　点击**删除 (Delete)**。

系统将显示一则消息，指示警报配置是否删除成功。

使用运行状况监视器

许可证：任何环境

Health Monitor 为防御中心管理的所有设备以及防御中心提供已编译的运行状况。状态表通过整体运行状况为此防御中心提供受管设备的数量。饼图提供运行状况细目的另一个视图，指示设备当前在每个运行状况类别中的百分比。

要使用运行状况监视器，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　点击 **Health > Health Monitor**。

系统将显示 Health Monitor 页面。

步骤 2　将表的 Status 列或饼图的适当部分选择适当的状态到具有该状态的列表设备中。

提示 如果表示状态级别的该行的箭头方向向下，则该状态的设备列表显示在下方的表中。如果箭头方向向右，则设备列表已隐藏。

下列主题提供有关在 Health Monitor 页面可执行的任务的详细信息。

- 第 68-38 页上的解释运行状况监视器状态
- 第 68-38 页上的使用设备运行状况监视器
- 第 68-6 页上的配置运行状况策略
- 第 68-35 页上的配置运行状况监视警报

解释运行状况监视器状态

许可证：任何环境

按严重程度划分的可用状态类别包括错误、严重、警告、正常、已恢复和已禁用，如下表所述。

表 68-6　运行状况指示灯

状态级别	状态图标	状态颜色	说明
错误		白	表示设备中的至少一个运行状况监控模块出现故障，并且自故障发生后未能成功重新运行。请与您的技术支持代表联系以获得对运行状况监控模块的更新。
严重		红色	表示对于设备中的至少一个运行状况模块而言，已超过严重限值，并且该问题尚未解决。
警告		黄色	表示对于设备中的至少一个运行状况模块而言，已超过警告限值，并且该问题尚未解决。
正常状态		绿色	表示设备中的所有运行状况模块都在应用于该设备的运行状况策略中配置的限值内运行。
已恢复		绿色	表示设备中的所有运行状况模块（包括处于“严重”或“警告”状态的模块）都在应用于该设备的运行状况策略中配置的限值内运行。
关闭		蓝色	表示设备被禁用或列入黑名单，设备没有应用运行状况策略，或者设备当前无法访问。

使用设备运行状况监视器

许可证：任何环境

设备运行状况监视器提供设备的运行状况的详细视图。

注 在会话处于不活动状态达到 1 小时 （或配置的其他时间间隔）之后，会话通常注销。如果您计划长时间被动监控运行状况监视器，请考虑免除某些用户实现会话超时或者变更系统超时设置。有关详细信息，请参阅第 61-44 页上的管理用户登录设置和第 63-26 页上的配置用户界面设置。

要查看特定设备的状态摘要，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　选择 **Health > Health Monitor**。

系统将显示 Health Monitor 页面。

步骤 2　要显示具有特定状态的设备列表，请点击该状态行中的箭头。

提示　如果表示状态级别的该行的箭头方向向下，则该状态的设备列表显示在下方的表中。如果箭头方向向右，则设备列表已隐藏。

步骤 3　在设备列表的 **Appliance** 列中，点击要在运行状况监视器工具栏中查看详细信息的设备的名称。

系统将显示 Health Monitor Appliance 页面。

步骤 4　或者，在 **Module Status Summary** 图中，点击要查看的事件状态类别的颜色。警报详细信息列表切换显示内容以显示或隐藏事件。

有关详细信息，请参阅：

- 第 68-3 页上的了解运行状况模块
- 第 68-38 页上的解释运行状况监视器状态
- 第 68-39 页上的按状态查看警报
- 第 68-40 页上的运行设备的所有模块
- 第 68-40 页上的运行特定运行状况模块
- 第 68-41 页上的生成运行状况模块警报图形
- 第 68-42 页上的使用运行状况监视器进行故障排除

按状态查看警报

许可证：任何环境

您可以按状态显示或隐藏警报的类别。

要按状态显示警报，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　点击对应要查看的警报运行状况的饼图中的状态图标或色段。该类别的警报显示在警报详细信息列表中。

要按状态隐藏警报，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　点击对应要查看的警报运行状况的饼图中的状态图标或色段。警报详细信息列表中该类别的警报消失。

运行设备的所有模块

许可证：任何环境

在您创建运行状况策略时配置的策略运行时间间隔内，运行状况模块测试自动运行。但是，您也可以按需运行所有运行状况模块测试以收集该设备的最新运行状况信息。

要为该设备运行所有运行状况模块，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　选择 **Health > Health Monitor**。

系统将显示 Health Monitor 页面。

步骤 2　要展开设备列表以显示具有特定状态的设备，请点击该状态行中的箭头。

提示　如果表示状态级别的该行的箭头方向向下，则该状态的设备列表显示在下方的表中。如果箭头方向向右，则设备列表已隐藏。

步骤 3　在设备列表的 **Appliance** 列中，点击要查看详细信息的设备的名称。

系统将显示 Health Monitor Appliance 页面。

步骤 4　点击 **Run All Modules**。

状态栏指示测试进程，然后 Health Monitor Appliance 页面刷新。

注　当您手动运行运行状况模块时，第一次自动发生的刷新可能不会影响自动运行测试的数据。如果没有为您手动运行的模块更改该值，请等待几秒钟，然后点击设备名称来刷新该页面。您还可以等待页面再次自动刷新。

运行特定运行状况模块

许可证：任何环境

在您创建运行状况策略时配置的策略运行时间间隔内，运行状况模块测试自动运行。但是，您也可以按需运行一个运行状况模块测试以收集该模块的最新运行状况信息。

要运行特定的运行状况模块，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　选择 **Health > Health Monitor**。

系统将显示 Health Monitor 页面。

步骤 2　要展开设备列表以显示具有特定状态的设备，请点击该状态行中的箭头。

提示　如果表示状态级别的该行的箭头方向向下，则该状态的设备列表显示在下方的表中。如果箭头方向向右，则设备列表已隐藏。

步骤 3　在设备列表的 **Appliance** 列中，点击要查看详细信息的设备的名称。

系统将显示 Health Monitor Appliance 页面。

步骤 4　在 Health Monitor Appliance 页面的 **Module Status Summary** 图中，点击要查看的运行状况警报状况类别的颜色。

警报详细信息列表展开以列出该状态类别的选定设备的运行状况警报。

步骤 5　在要查看其事件列表的警报的 **Alert Detail** 行，请点击 **Run**。

状态栏指示测试进程，然后 Health Monitor Appliance 页面刷新。

注　当您手动运行运行状况模块时，第一次自动发生的刷新可能不会影响自动运行测试的数据。如果没有为您手动运行的模块更改该值，请等待几秒钟，然后点击设备名称来刷新该页面。您还可以等待页面再次自动刷新。

生成运行状况模块警报图形

许可证：任何环境

您可以图表表示特定设备的特定运行状况测试的一段时间内的结果。

要生成运行状况模块警报图形，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　选择 **Health > Health Monitor**。

系统将显示 Health Monitor 页面。

步骤 2　要展开设备列表以显示具有特定状态的设备，请点击该状态行中的箭头。

提示　如果表示状态级别的该行的箭头方向向下，则该状态的设备列表显示在下方的表中。如果箭头方向向右，则设备列表已隐藏。

步骤 3　在设备列表的 **Appliance** 列中，点击要查看详细信息的设备的名称。

系统将显示 Health Monitor Appliance 页面。

步骤 4　在 Health Monitor Appliance 页面的 **Module Status Summary** 图中，点击要查看的运行状况警报状况类别的颜色。

警报详细信息列表展开以列出该状态类别的选定设备的运行状况警报。

步骤 5　在要查看其事件列表的警报的 **Alert Detail** 行，请点击 **Graph**。

系统将显示一个图形，其中显示随时间推移的事件的状态。图形下的“警报详细信息”小节列出选定设备的所有运行状况警报。

提示　如果未显示事件，您可能需要调整时间范围。有关详情，请参见第 58-19 页上的设置事件时间限制。

使用运行状况监视器进行故障排除

许可证：任何环境

某些情况下，如果您的设备有问题，支持人员可能要求您生成故障排除文件以帮助诊断该问题。您可以选择下表中列出的任何选项以定制运行状况监视器报告的故障排除数据。

表 68-7　　可选择的故障排除选项

该选项.....	报告.....
Snort Performance and Configuration	与设备上的 Snort 相关的数据和配置设置
Hardware Performance and Logs	与设备硬件性能相关的数据和日志
System Configuration, Policy, and Logs	与设备的当前系统配置相关的配置设置、数据和日志
Detection Configuration, Policy, and Logs	与对设备的检测相关的配置设置、数据和日志
Interface and Network Related Data	与设备的内联集和网络配置相关的配置设置、数据和日志
Discovery, Awareness, VDB Data, and Logs	与设备上的当前发现和感知配置相关的配置设置、数据和日志
Upgrade Data and Logs	与设备的前期升级相关的数据和日志
All Database Data	包含在故障排除报告中的所有数据库相关数据
All Log Data	设备数据库收集的所有日志
Network Map Information	当前网络拓扑数据

请注意，在所报告的数据方面，某些选项重叠，但是无论您选择什么选项，故障排除文件都不会包含冗余备份。

有关详细信息，请参阅：

- 第 68-42 页上的生成设备故障排除文件
- 第 68-43 页上的下载故障排除文件

生成设备故障排除文件

许可证：任何环境

使用以下步骤生成可以发送给支持人员的定制的故障排除文件。

注　您**无法**使用高可用性配置中的主要防御中心为辅助防御中心生成故障排除文件，反之亦然。您必须从防御中心自己的网络界面生成故障排除文件。

要生成故障排除文件，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　选择 **Health > Health Monitor**。

系统将显示 Health Monitor 页面。

步骤 2　要展开设备列表以显示具有特定状态的设备，请点击该状态行中的箭头。

提示　如果表示状态级别的该行的箭头方向向下，则该状态的设备列表显示在下方的表中。如果箭头方向向右，则设备列表已隐藏。

步骤 3　在设备列表的 **Appliance** 列中，点击要查看详细信息的设备的名称。

系统将显示 Health Monitor Appliance 页面。

步骤 4　点击 **Generate Troubleshooting Files**。

系统将显示 Troubleshooting Options 弹出窗口。

步骤 5　选择 **All Data** 以生成所有可能的故障排除数据或选择单个复选框来自定义报告。有关详细信息，请参阅可选择的故障排除选项表。

步骤 6　点击 **OK**。

防御中心生成故障排除文件。您可以监控任务队列中的文件生成进程 (**System > Monitoring > Task Status**)。

步骤 7　继续执行下一节下载故障排除文件中的操作步骤。

下载故障排除文件

许可证：任何环境

使用以下步骤下载所生成的故障排除文件的副本。

要下载故障排除文件，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　选择 **System > Monitoring > Task Status**。

系统将显示 Task Status 页面。

步骤 2　找出对应所生成的故障排除文件的任务。

步骤 3　在设备生成故障排除文件并且任务状态变更为 `Completed` 之后，点击 **Click to retrieve generated files**。

步骤 4　按照浏览器的提示下载文件。

文件下载到单个 `.tar.gz` 文件中。

步骤 5　按照支持人员的指示将故障排除文件发送给思科。

处理运行状况事件

许可证：任何环境

防御中心提供完全可定制的事件视图，使您可以快速轻松地分析运行状况监视器所收集的运行状况事件。这些事件视图使您可以搜索和查看事件数据，并轻松访问可能与正调查的事件有关的其他信息。

您可以在运行状况事件视图页面执行的许多功能在所有事件视图页面中都固定不变。有关这些常见步骤的详细信息，请参阅第 68-44 页上的了解运行状况事件视图。

从 **Health > Health Events** 菜单选项，您查看运行状况事件，并可以搜索特定事件。

有关查看事件的详细信息，请参阅以下各节：

- 第 68-44 页上的了解运行状况事件视图介绍 FireSIGHT 生成的事件的类型。
- 第 68-44 页上的查看运行状况事件介绍如何访问和使用事件视图页面。
- 第 68-50 页上的搜索运行状况事件介绍如何使用 Event Search 页面来搜索特定事件。

了解运行状况事件视图

许可证：任何环境

防御中心 运行状况监视器记录您在 Health Event View 页面可以看到的运行状况事件。如果您了解每个运行状况模块测试的条件，就可以更有效地配置运行状况事件的警报。有关生成运行状况事件的不同类型运行状况模块的详细信息，请参阅第 68-3 页上的了解运行状况模块。

有关查看和搜索运行状况事件的详细信息，请参阅：

- 第 68-44 页上的查看运行状况事件
- 第 68-49 页上的了解运行状况事件表
- 第 68-50 页上的搜索运行状况事件

查看运行状况事件

许可证：任何环境

您能够以若干方式查看运行状况监视器收集的设备运行状况数据。

有关详细信息，请参阅：

- 第 68-44 页上的查看所有运行状况事件
- 第 68-45 页上的按模块和设备查看运行状况事件
- 第 68-46 页上的处理运行状况事件表视图
- 第 68-47 页上的解释 3D9900 设备的硬件警报详细信息
- 第 68-47 页上的解释 3 系列设备的硬件警报详细信息

查看所有运行状况事件

许可证：任何环境

Table View of Health Events 页面提供所选设备上所有运行状况事件的列表。有关生成您可以在该页面看到的事件的运行状况模块的介绍，请参阅第 68-3 页上的了解运行状况模块。

当您在防御中心中从 Health Monitor 页面访问运行状况事件时，您可以检索所有受管设备的所有运行状况事件。

要查看所有受管设备上的所有运行状况事件，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　选择 **Health > Health Events**。

系统将显示 Events 页面，其中包含所有运行状况事件。

注　如果未显示事件，您可能需要调整时间范围。有关详情，请参见第 58-19 页上的设置事件时间限制。

提示　您可以为该视图添加书签，使您可以返回到其中包含事件的运行状况事件表的运行状况事件工作流程页面。加入书签的视图检索您当前正查看的时间范围内的事件，但是如果需要，您可以稍后修改时间范围以使用较新的信息更新该表。有关详细信息，请参阅第 58-19 页上的设置事件时间限制。

按模块和设备查看运行状况事件

许可证：任何环境

您可以查询特定设备上的特定运行状况模块所生成的事件。

要查看特定模块的运行状况事件，请查看以下信息：

访问：管理员/维护人员/任何安全分析师

步骤 1　选择 **Health > Health Monitor**。

系统将显示 Health Monitor 页面。

步骤 2　要展开设备列表以显示具有特定状态的设备，请点击该状态行中的箭头。

提示　如果表示状态级别的该行的箭头方向向下，则该状态的设备列表显示在下方的表中。如果箭头方向向右，则设备列表已隐藏。

步骤 3　在设备列表的 Appliance 列中，点击要查看详细信息的设备的名称。

系统将显示 Health Monitor Appliance 页面。

步骤 4　在 Health Monitor Appliance 页面的 **Module Status Summary** 图中，点击要查看的运行状况警报状况类别的颜色。

警报详细信息列表展开以列出该状态类别的选定设备的运行状况警报。

步骤 5　在要查看其事件列表的警报的 Alert Detail 行，点击 **Events**。

系统将显示 Health Events 页面，其中包含作为限制的具有设备名称的查询的查询结果以及选定运行状况警报模块的名称。

如果未显示事件，您可能需要调整时间范围。有关详情，请参见第 58-19 页上的设置事件时间限制。

步骤 6　如果要查看选定设备的所有运行状况事件，请展开 **Search Constraints** 并点击 **Module Name** 限制将其移除。

处理运行状况事件表视图

许可证：任何环境

下表介绍了您可以通过事件视图页面执行的每个操作。

表 68-8　　运行状况事件视图功能

要.....	您可以.....
了解有关运行状况事件视图中显示的列的内容	在第 68-49 页上的了解运行状况事件表中获得详细信息。
修改在运行状况表视图中列出的事件的时间和日期范围	在第 58-19 页上的设置事件时间限制中获得详细信息。 请注意，如果按时间限制事件视图，则在设备配置的时间段外生成的事件（无论是全局或特定事件）可能显示在事件视图中。即使已经为设备配置一个滑动时间窗，这种情况仍然可能发生。
对显示的事件进行排序，更改事件表中显示哪些列，或者限制显示的事件	在第 58-29 页上的对向下钻取工作流程页面进行排序中获得详细信息。
删除运行状况事件	选中要删除的事件旁边的复选框，并点击 **Delete**。要删除当前受限制视图中的所有事件，请点击 **Delete All**，然后确认要删除所有事件。
通过事件视图页面导航	在第 58-30 页上的导航到工作流程中的其他页面中获得详细信息。
导航至其他事件表以查看相关的事件	在第 58-31 页上的在工作流程之间导航中获得详细信息。
为当前页面添加书签以便快速返回到该页面	点击 **Bookmark This Page**，为书签提供名称并点击 **Save**。有关详情，请参见第 58-32 页上的使用书签。
导航到书签管理页面	从任何事件视图中点击 **View Bookmarks**。有关详情，请参见第 58-32 页上的使用书签。
基于表视图中的数据生成报告	点击 **Report Designer**。有关详情，请参见第 57-8 页上的从事件视图创建报告模板。
选择另一个运行状况事件工作流程	点击 **(switch workflow)**。有关详情，请参见第 58-14 页上的选择工作流程。
查看与单个运行状况事件相关的详细信息	点击事件左侧的向下箭头链接。
查看多个运行状况事件的事件详细信息	选择对应要查看其详细信息的事件的行旁边的复选框，然后点击 **View**。
查看视图中所有事件的事件详细信息	点击 **View All**。
查看特定状态的所有事件	点击具有该状态的事件的 Status 列中的状态图标。

解释 3D9900 设备的硬件警报详细信息

许可证：任何环境

对于 3D9900 设备型号，响应下表中所述事件的硬件警报生成。警报的消息详细信息中可以发现触发的条件。

表 68-9　　对 3D9900 设备进行监控的条件

监控的条件	黄色或红色错误条件的原因
NFE 卡存在情况	如果检测对设备无效的 NFE 硬件，硬件告警模块的运行状况变为红色，消息详细信息中包括对 NFE 卡存在情况的参考。
NFE 温度	如果 NFE 温度超过 95 摄氏度，硬件告警模块的运行状况变为黄色，消息详细信息中包括对 NFE 温度的参考。 如果 NFE 温度超过 99 摄氏度，硬件告警模块的运行状况变为红色，消息详细信息中包括对 NFE 温度的参考。
NFE 平台守护程序	如果 NFE 平台守护程序关闭，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。
NFE 消息守护程序	如果 NFE 消息守护程序关闭，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。
NFE TCAM 守护程序	如果 NFE TCAM 守护程序关闭，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。
LBIM 存在情况	如果负载均衡接口模块 (LBIM) 开关组件不存在或不进行通信，硬件告警模块的运行状况变为红色，消息详细信息包括对 LBIM 存在情况的参考。
Scmd 守护程序	如果 Scmd 守护程序关闭，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。
Psls 守护程序	如果 Psls 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。
Ftwo 守护程序	如果 Ftwo 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。
Rulesd （主机规则）守护程序	如果 Rulesd 守护程序断开，硬件告警模块的运行状况变为黄色，消息详细信息中包括对守护程序的参考。
nfm_ipfragd （主机碎片）守护程序	如果 nfm_ipfragd 守护程序关闭，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。

解释 3 系列设备的硬件警报详细信息

对于 3 系列设备，响应下表中所述事件的硬件警报生成。触发的条件显示在警报的消息详细信息中。

表 68-10　　为 3 系列设备监控的条件

监控的条件	黄色或红色错误条件的原因
集群状态	如果集群的设备彼此不再通信 （例如，由于布线问题），硬件告警模块变为红色。
ftwo 守护程序状态	如果 ftwo 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。

表 68-10　为 3 系列设备监控的条件 （续）

监控的条件	黄色或红色错误条件的原因
检测到的 NFE 卡	表示系统中检测到的 NFE 卡的数量。如果该值不匹配设备的预期 NFE 计数，硬件告警模块变为红色。
NFE 硬件状态	如果一个或多个 NFE 卡不进行通信，硬件告警模块变为红色，并且适用的卡显示在消息详细信息中。
NFE 心跳	如果系统检测不到 NFE 心跳，硬件告警模块变为红色，消息详细信息中包括对相关卡的参考。
NFE 内部链路状态	如果 NMSB 和 NFE 卡之间的链路断开，硬件告警模块变为红色，消息详细信息中包括对相关端口的参考。
NFE 消息守护程序	如果 NFE 消息守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序 （以及 NFE 卡号 [如果适用]）的参考。
NFE 温度	如果 NFE 温度超过 97 摄氏度，硬件告警模块的运行状况变为黄色，消息详细信息中包括对 NFE 温度 （以及 NFE 卡号 [如果适用]）的参考。 如果 NFE 温度超过 102 摄氏度，硬件告警模块的运行状况变为红色，消息详细信息中包括对 NFE 温度 （以及 NFE 卡号 [如果适用]）的参考。
NFE 温度状态	表示给定的 NFE 卡的当前温度状态。硬件告警模块用绿色表示“正常”，用黄色表示“警告”，用红色表示“严重” （以及 NFE 卡号 [如果适用]）。
NFE TCAM 守护程序	如果 NFE TCAM 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序 （以及 NFE 卡号 [如果适用]）的参考。
nfm_ipfragd （主机碎片）守护程序	如果 nfm_ipfragd 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序 （以及 NFE 卡号 [如果适用]）的参考。
NFE 平台守护程序	如果 NFE 平台守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序 （以及 NFE 卡号 [如果适用]）的参考。
NMSB 通信	如果媒体组件不存在或不进行通信，硬件告警模块的运行状况变为红色，消息详细信息包括对 NFE 温度 （以及 NFE 卡号 [如果适用]）的引用。
psls 守护程序状态	如果 psls 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。
Rulesd （主机规则）守护程序	如果 Rulesd 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序 （以及 NFE 卡号 [如果适用]）的参考。
scmd 守护程序状态	如果 scmd 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。

了解运行状况事件表

许可证：任何环境

您可以使用防御中心的运行状况监视器来确定 FireSIGHT 系统内关键功能的状态。您创建运行状况策略并将其应用至设备，该设备监控各个方面，包括硬件和软件状态。您选择在运行状况策略中启用的运行状况监视器模块运行各种测试，以确定设备运行状况。当运行状况满足您指定的标准时，生成一个运行状况事件。有关运行状况监控的详细信息，请参阅第 67-1 页上的监控系统。

下表介绍运行状况事件表中的字段。

表 68-11　　运行状况事件字段

字段	说明
Test Name	生成事件的运行状况模块的名称。有关运行状况模块的列表，请参阅运行状况模块表。
时间	运行状况事件的时间戳。
说明	生成事件的运行状况模块的说明。例如，当无法执行进程时生成的运行状况事件被标记为 `Unable to Execute`。
价值	生成事件的运行状况测试所获得的结果值 （单位数量）。 例如，如果其正在监控的设备使用的 CPU 资源达到 80% 或更多时防御中心生成运行状况事件，则该值可以是介于 80 到 100 之间的一个数字。
装置	结果的单位描述符。您可以使用星号 (*) 创建通配符搜索。 例如，如果其正在监控的设备使用的 CPU 资源达到 80% 或更多时防御中心生成运行状况事件，则单位描述符为百分号 (%)。
状态	为设备报告的状态 （严重、黄色、绿色或已禁用）。
设备	报告运行状况事件的设备。

要显示运行状况事件的表视图，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　选择 **Health > Health Events**。

系统显示表视图。有关处理运行状况事件的信息，请参阅第 68-43 页上的处理运行状况事件。

提示　如果您使用的自定义工作流程不包括运行状况事件表视图，请点击 **(switch workflow)**。在 Select Workflow 页面上，点击 **Health Events**。

搜索运行状况事件

许可证：任何环境

您可以搜索特定运行状况事件。您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。下表列出了可以使用的搜索条件。

表 68-12　　运行状况事件搜索条件

搜索字段	说明
Module Name	指定生成要查看的运行状况事件的模块的名称。例如，要查看度量 CPU 性能的事件，请键入 `CPU`。搜索应检索适用的 CPU 使用率和 CPU 温度事件。
价值	指定要查看的事件的运行状况测试所获得的结果值 （单位数量）。 例如，如果您在 Units 字段中指定值为 15、类型为 `CPU`，您可以检索在测试运行时设备正以 15% 利用率运行的事件。
说明	指定要查看的事件的说明。例如，您可以输入 `Unable to Execute` 来查看无法执行进程的任何运行状况事件。您可以在此字段中使用星号 (*) 来创建通配符搜索。
装置	指定要查看的事件的运行状况测试所获得的结果的设备描述符。您可以在此字段中使用星号 (*) 来创建通配符搜索。 例如，如果您在 Units 字段中键入 `%`，则检索磁盘使用率文件的所有事件，因为磁盘使用率模块在 Units 字段中有“%”标签 （没有其他文本）。 .但是，如果您在 Units 字段中键入 `*%`，则可以检索包含文本及在 Units 字段中有“%”标签的任何模块的所有事件。
状态	指定要查看的运行状况事件的状态。有效状态级别有严重、警告、正常、错误和已禁用。 例如，键入 `Critical` 以检索指示严重状态的所有运行状况事件。
设备	键入设备名称或 IP 地址或设备组、堆栈或集群名称，将搜索限制在一个或多个特定设备生成的运行状况事件范围内。有关 FireSIGHT 系统如何处理搜索中的设备字段的详细信息，请参阅第 60-6 页上的在搜索中指定设备。

有关搜索的详细信息，包括特定搜索语法以及保存和加载搜索的信息，请参阅第 60-1 页上的执行和保存搜索。

要搜索运行状况事件，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Health Events**。

页面根据相应限制进行更新。

步骤 3　在相应字段中输入搜索条件，如运行状况事件搜索条件表中所述。

如果输入多个条件，搜索仅返回符合所有条件的记录。

步骤 4　如果您计划保存搜索，也可以选择 Private 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功（如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save as New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功（如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认运行状况事件工作流程中，受到当前的时间范围的限制。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

审计系统

您可以用两种方式审计系统中的活动。作为 FireSIGHT 系统一部分的设备为每个与网络接口交互的用户生成审计记录，并在系统日志中记录系统状态消息。

以下各节提供有关该系统提供的监控功能的详细信息：

- 第 69-1 页上的管理审计记录介绍如何查看和管理系统审计信息。
- 第 69-9 页上的查看系统日志介绍如何查看包括系统状态消息的系统日志。

提示 带有保护许可证的防御中心和受管设备还可以提供完善的报告功能，该功能使您可以生成事件视图中可访问的几乎任何类型数据 （包括审计数据）的报告。有关详细信息，请参阅第 57-1 页上的使用报告。

管理审计记录

许可证：任何环境

防御中心和受管设备记录用户活动的只读审计信息。审计日志显示在标准事件视图中，您可以依据审计视图中的任何项目查看、排序和过滤审计日志消息。您可以轻松删除和报告审计信息，也可以查看用户所作更改的详细报告。

审核日志中最多可以存储 100,000 个条目。当审核日志中条目的数量超过 100,000 时，设备会从数据库中删除最旧的记录，保持数据库中条目的数量为 100,000。

注 如果重新启动3 系列 设备，然后尽快登录 CLI，除非网络界面可用，否则您执行的任何命令都不记录在审计日志中。

有关详细信息，请参阅：

- 第 69-2 页上的查看审计记录
- 第 69-4 页上的屏蔽审计记录
- 第 69-6 页上的了解审计日志表
- 第 69-7 页上的使用审计日志检查更改
- 第 69-8 页上的搜索审计记录

查看审计记录

许可证：任何环境

您可以使用设备查看审计记录表。然后，可根据要查找的信息操作视图。预定义的审计工作流程包括一个事件表视图。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。有关创建自定义工作流程的信息，请参阅第 58-34 页上的创建自定义工作流程。

下表介绍了在审计日志工作流程页面可进行的某些特定操作。

表 69-1　　审计日志操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 69-6 页上的了解审计日志表中获得详细信息。
在查看审计记录时修改使用的时间范围	在第 58-19 页上的设置事件时间限制中查找详细信息。 请注意，如果按时间限制事件视图，则在设备配置的时间段外生成的事件 （无论是全局或特定事件）可能显示在事件视图中。即使已经为设备配置一个滑动时间窗，这种情况仍然可能发生。
对当前工作流程页面上的事件进行排序和限制	在第 58-29 页上的对表视图页面进行排序并更改其布局中获得详细信息。
在当前工作流程页面中导航	在第 58-30 页上的导航到工作流程中的其他页面中获得详细信息。
在当前工作流程中的页面之间导航，同时保留当前限制条件	点击工作流程页面左上角的相应页面链接。有关详细信息，请参阅第 58-16 页上的使用工作流程页面。
向下钻取到工作流程中的下一个页面	可使用以下其中一种方法： • 要向下钻取到限制某个特定值的下一个工作流程页面，请点击某一行中的一个值。请注意，此操作仅适用于向下钻取页面。请注意，在表视图中点击某一行中的一个值时，会限制该表视图，且**不会**向下钻取到下一个页面。 • 要向下钻取到限制某些事件的下一个工作流程页面，请选择您想要在下一个工作流程页面上查看的事件旁的复选框，然后点击 **View**。 • 要向下钻取到保留当前限制的下一工作流程页面，请点击 **View All**。 **提示**　表视图的页面名称中始终包括“Table View”。 有关详细信息，请参阅第 58-26 页上的限制事件。
限制特定值	点击行中的值。 如果在详细浏览页面中点击一个值，您将进入下一个页面并限制该值。 请注意，点击表视图行中的值可限制表视图，且**不会**向下钻取到下一页。 **提示**　表视图会始终在页面名称中包括“Table View”。 有关详细信息，请参阅第 58-26 页上的限制事件。
删除审计记录	可使用以下其中一种方法： • 要删除某些项目，选择要删除的事件旁边的复选框，然后点击 **Delete**。 • 要删除当前受限制视图中的所有项目，点击 **Delete All**，然后确认要删除所有事件。
暂时使用不同的工作流程	点击 **(switch workflow)**。有关详细信息，请参阅第 58-14 页上的选择工作流程。
将当前页面加入书签，以便快速返回	点击 **Bookmark This Page**。有关详细信息，请参阅第 58-32 页上的使用书签。

表 69-1　　审计日志操作 （续）

要.....	您可以.....
导航到书签管理页面	点击 **View Bookmarks**。有关详细信息，请参阅第 58-32 页上的使用书签。
根据当前视图中的数据生成报告	点击 **Report Designer**。有关详细信息，请参阅第 57-8 页上的从事件视图创建报告模板。
查看审计日志中记录的更改摘要	点击比较图标 ( )，其位于 **Message** 列中的适用事件旁边。有关详细信息，请参阅第 69-7 页上的使用审计日志检查更改。

要查看审计记录，请执行以下操作：

访问：管理

步骤 1　选择 **System > Monitoring > Audit**。

系统将显示第一个 （唯一一个）默认审计日志工作流程页面。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。如果未显示事件，您可能需要调整时间范围。有关详细信息，请参阅第 58-19 页上的设置事件时间限制。

提示　如果您正在使用不包括审计事件表视图的自定义工作流程，请点击 **(switch workflow)**，然后选择 **Audit Log**。

使用审计事件

许可证：任何环境

您可以更改事件视图的布局或按字段值限制视图中的事件。当禁用某列时，在点击想要隐藏的列标题中的关闭图标 (✖) 后，系统会显示弹出窗口，在窗口中点击 **Apply**。禁用列时，该列在会话持续时间内处于禁用状态 （除非稍后重新添加该列）。请注意，禁用第一列时，会添加 Count 列。

要隐藏或显示其他列，或将已禁用列添加回视图中，选择或清除相应的复选框，然后点击 **Apply**。

请注意，在表视图中点击某一行中的一个值时，会限制该表视图，且不会向下钻取到下一个页面。

提示　表视图的页面名称中始终包括“Table View”。

有关详细信息，请参阅：

- 第 58-26 页上的限制事件.
- 第 58-28 页上的使用复合限制
- 第 58-29 页上的对向下钻取工作流程页面进行排序
- 第 69-6 页上的了解审计日志表

屏蔽审计记录

许可证：任何环境

如果审计策略不要求您审计特定类型的用户和 FireSIGHT 系统之间的交互，则您可以避免这些交互生成审计记录。例如，默认情况下，每次用户查看联机帮助， FireSIGHT 系统都会生成一个审计记录。如果您不需要保留这些交互记录，可以自动屏蔽它们。

要配置审计事件屏蔽，您必须具备设备的管理员用户帐户权限，且必须能够访问设备的控制台或打开一个安全外壳。

注意事项　确保仅授权人员可以访问设备及其管理员帐户。

要屏蔽审计记录，必须在下表中的 `/etc/sf` 目录下创建一个或多个文件：

`AuditBlock.`*`type`*

其中 *`type`* 为 `address`、 `message`、 `subsystem` 或 `user`。

注　如果您为特定类型的审计信息创建了一个 `AuditBlock.`*`type`* 文件，但之后确定不再想屏蔽它们，则您必须删除 `AuditBlock.`*`type`* 文件的内容，但在 FireSIGHT 系统中保留文件本身。

每种审计块类型的内容都必须为特定格式，如下表所述。确保您使用的是正确的文件名大写字母。另请注意，文件的内容区分大小写。

表 69-2　　审计块类型

类型	说明
地址	创建一个以 `AuditBlock.address` 命名的文件，并包括您想要从审计日志中屏蔽的各 IP 地址，每行一个。您可以使用部分 IP 地址，前提是它们从地址开始处映射。例如，部分地址 `10.1.1` 匹配从 `10.1.1.0` 到 `10.1.1.255` 的地址。
通信	创建一个命名为 `AuditBlock.message` 的文件，并包括您想要屏蔽的消息子字符串，每行一个。 请注意，子字符串匹配，这样，如果您的文件中包括 `backup`，则包括文字 `backup` 的所有消息都将被屏蔽。
Subsystem	创建一个命名为 `AuditBlock.subsystem` 的文件，并包括您想要屏蔽的各子系统，每行一个。 请注意，子字符串**不**匹配。您必须使用准确的字符串。有关所审计的子系统列表，请参阅子系统名称表。
用户	创建一个命名为 `AuditBlock.user` 的文件，并包括您想要屏蔽的各用户帐号，每行一个。您可以使用部分字符串匹配，前提是它们从用户名开始处映射。例如，部分用户名 `IPSAnalyst` 匹配用户名 `IPSAnalyst1` 和 `IPSAnalyst2`。

请注意，当您添加 `AuditBlock` 文件时，带 `Audit` 子系统和 `Audit Filter` *`type`* `Changed` 消息的审计记录会被添加到审计事件中。出于安全原因，该审计记录**不能**被屏蔽。

下表列出了经审计的子系统。

表 69-3　　子系统名称

字段名称	包括与下列各项的用户交互...
管理	管理功能，例如系统和访问配置、时间同步、备份和恢复、设备管理、用户帐户管理和调度
警报	警报功能，例如邮件、 SNMP 和系统警报
审核日志	审计事件视图
Audit Log Search	审计事件搜索
命令行	命令行界面
配置	邮件警报
COOP	操作功能连续性
日期	事件视图的日期和时间范围
Default Subsystem	没有已分配子系统的选项
Detection & Prevention Policy	入侵策略的菜单选项
错误	系统级错误
eStreamer	eStreamer 配置
EULA	审核最终用户许可协议
活动	入侵和发现事件视图
Events Clipboard	入侵事件剪贴板
Events Reviewed	经审核的入侵事件
Events Search	任何事件搜索
Failed to install rule update *rule_update_id*	安装规则更新
标题栏	用户登录后用户界面的初次展示
运营状况	运行状况监控
Health Events	运行状况监控事件视图
帮助	联机帮助
高可用性	高可用性功能
IDS Impact Flag	影响标记配置
IDS Policy	入侵策略
IDSPolicy > *policy_name* > Appliance > *det_engine_name*	应用入侵策略
IDSRule sid:*sig_id* rev:*rev_num*	按 SID 划分的入侵规则
事件	入侵事故
Insert Policy Apply Job	应用策略
安装	安装更新
Intrusion Events	入侵事件
登录	网络界面登录和注销功能

表 69-3　　子系统名称 （续）

字段名称	包括与下列各项的用户交互...
菜单	任何菜单选项
Configuration export > *config_type* > *config_name*	导入特定类型和名称的配置
Permission Escalation	用户角色升级
偏好	用户首选项，例如，用户帐户和单个事件首选项的时区
策略	任何策略，包括入侵策略
注册	在防御中心上注册设备
RemoteStorageDevice	配置远程存储设备
报告	报告列表和报告设计者功能
规则	入侵规则，包括规则编辑器和规则导入进程
规则更新导入日志	查看规则更新导入日志
Rule Update Install	安装规则更新
状态	系统日志以及主机和性能统计数据
系统	各种系统范围设置
System Policy > *policy_name* Appliance > *appliance_name*	应用系统策略
Task Queue	查看任务队列
用户	创建和修改用户帐户和角色

了解审计日志表

许可证：任何环境

每台设备都会为与网络界面的各个用户交互生成审计事件。每个事件都包括一个时间戳、其操作生成事件的用户的用户名、一个源 IP，以及描述事件的文本。审计日志表中的字段见下表。

表 69-4　　审计日志字段

字段	说明
时间	设备生成审计记录的时间和日期。
用户	触发审计事件的用户的用户名。
Subsystem	用户通过其生成审计记录的菜单路径。例如， **System > Monitoring > Audit** 就是查看审计日志的菜单路径。 对于菜单路径不相关的少数情况，Subsystem 字段仅显示事件类型。例如，**Login** 分类用户登录尝试。

表 69-4　　审计日志字段 （续）

字段	说明
通信	用户执行的操作。 例如， `Page View` 表示用户简单查看了子系统中显示的页面，而 `Save` 意味着用户点击了页面上的 **Save** 按钮。 对 FireSIGHT 系统做出的更改在显示时带有一个比较图标 (FireSIGHT 系统)，点击该图标即可查看更改摘要。 FireSIGHT 系统有关详细信息，请参阅第 69-7 页上的使用审计日志检查更改。
源 IP：	与用户使用的主机相关联的 IP 地址。
计数	与每行中所显示的信息匹配的事件数。请注意，仅在您运用了某个创建了两个或多个相同行的限制之后， Count 字段才显示。

使用审计日志检查更改

许可证：任何环境

您可以使用审计日志查看系统更改的详细报告。这些报告会比较系统的当前配置和特定更改之前的最近配置。

比较图标 ( ) 显示在反映系统更改的审计日志事件旁边。您可以点击比较图标以评估 Compare Configurations 页面并查看更改的详细报告。

Compare Configurations 页面显示更改前的系统配置和采用并行格式的运行配置之间的差异。审计事件类型、最后修改时间、作出更改的用户名称会在每个配置上的标题栏中显示。

两种配置之间的差异会突出显示：

- 蓝色表示突出显示设置的设置在两个配置中有所不同，差异会以红色文本标记。
- 绿色表示突出显示的设置在一个配置中显示，但在另一个配置中不显示。

要检查审计日志的更改，请执行以下操作：

访问：管理

步骤 1　选择 **System > Monitoring > Audit**。

系统将显示默认审计日志工作流程的第一个页面。

如果您正在使用不包括审计事件表视图的自定义工作流程，请点击 **(switch workflow)**，然后选择 **Audit Log**。

步骤 2　点击比较图标 ( )，其位于 **Message** 列的适用审计日志事件旁边。

系统将显示 Compare Configurations 页面。请注意，您可以点击标题栏上方的 **Previous** 或 **Next** 在不同更改间切换。如果更改摘要长度超过一个页面，您也可以使用右侧的滚动条查看其他的更改。

搜索审计记录

许可证：任何环境

您可以搜索审计记录以查找某个用户、具体子系统或审计记录消息的特定信息。

您可能想要创建为自己的网络环境订制的搜索，然后保存这些搜索以便以后再用。下表介绍可用的搜索条件。请注意，审计搜索不区分大小写。例如，搜索 `Analyst01` 或 `analyst01` 将获得相同的结果。

表 69-5　　审计记录搜索条件

搜索字段	说明	示例
用户	输入触发您想要查看的审计事件的用户的用户名。您可以在该字段中使用星号 (*) 作为通配符。	`jsmith` 会返回所有涉及用户 jsmith 的审计记录。
Subsystem	输入用户会采用的完整菜单路径以生成您想要查看的审计记录。您可以在该字段中使用星号 (*) 作为通配符。	`System > Monitoring > Audit` 和 `*Audit` 均会返回涉及使用审计日志的审计记录。 `*Audit*` 会返回所有上述记录，以及涉及审计记录搜索的记录。
通信	用户执行的操作或用户在页面上点击的按钮。您可以在该字段中使用星号 (*) 作为通配符。	`Apply` 会返回用户运用了入侵策略的审计记录。 `Save Rule` 会在用户保存某个关联性规则时返回审计记录。 `Page View` 会在用户查看页面时返回审计记录。
时间	指定审计记录生成的日期和时间。有关时间输入语法，请参阅第 60-5 页上的在搜索中指定时间约束。	`> 2006-01-15 13:30:00` 会返回 2006 年 1 月 15 日下午 1:30 之后所生成的所有审计记录。
源 IP：	输入您想要查看审计记录的主机的 IP 地址。 **注**　您**必须**输入特定 IP 地址。在搜索审计日志时，您不能使用 IP 范围。	`172.16.1.37` 会返回用户从 172.16.1.37 IP 地址生成的所有审计记录。
Configuration Change	指定是否要查看配置更改的审计记录。	`Yes` 会返回配置更改的审计记录。

有关搜索的详细信息，包括如何加载和删除已保存搜索，请参阅第 60-1 页上的搜索事件。

要搜索审计记录，请执行以下操作：

访问：管理

步骤 1　选择 **Analysis > Search**。

系统将显示 Search 页面。

步骤 2　从表下拉列表中选择 **Audit Log Events**。

系统将显示 Audit Log 搜索页面。

提示　要在数据库中搜索另一类型的事件，请从表下拉列表选择它。

步骤 3　在相应字段中输入搜索条件，如审计记录搜索条件表中所述。

如果您输入多个字段的条件，搜索只返回符合所有字段指定搜索条件的记录。

步骤 4　如果您计划保存搜索，也可以选择 **Private** 复选框，将搜索保存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示　如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 5　或者，您可以保存搜索，以备以后使用。您有以下选项：

- 点击 **Save**，保存搜索条件。

  对于新的搜索，系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。如果为之前即已存在的搜索保存新的条件，则不会显示提示。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。

  系统将显示一个对话框，提示您提供搜索的名称；请输入一个唯一的搜索名称，然后点击 **Save**。搜索保存成功 （如果您选择了 **Private**，则只对您的帐户显示），您以后可以运行此搜索。

步骤 6　点击 **Search** 开始搜索。

搜索结果显示在默认审计日志工作流程中，受限在当前时间范围。要使用不同的工作流程，包括自定义工作流程，请点击 **(switch workflow)**。有关指定不同默认工作流程的信息，请参阅第 71-3 页上的配置事件查看设置。

查看系统日志

许可证：任何环境

System Log (syslog) 页面上提供了设备的系统日志信息。系统日志显示系统生成的每条消息。以下项目会按顺序列出：

- 生成消息的日期
- 生成消息的时间
- 生成消息的主机
- 消息本身

注　系统日志信息是本地消息。例如，您**不能**使用防御中心查看受管设备上系统日志中的系统状态消息。

您可以使用过滤功能查看特定组件的系统日志消息。有关详细信息，请参阅第 69-10 页上的过滤系统日志消息。

要查看系统日志，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Monitoring > Syslog**。

系统将显示 System Log 页面。

提示　在 3D9900 上，Load Balancing Interface Module (LBIM) 向设备的系统日志转发消息。您可以通过在 `lbim` 上过滤来找到这些消息。

过滤系统日志消息

许可证：任何环境

您可以使用过滤功能查看特定组件的系统日志消息。过滤功能使您可以根据内容搜索特定的消息。

过滤功能使用 UNIX 文件搜索实用程序 Grep，正因如此，您可以使用 Grep 接受的大部分语法。这包括使用与 Grep 兼容的正则表达式实现模式匹配。您可以使用一个单词作为过滤器，也可以使用 Grep 支持的正则表达式搜索内容。

下表显示了在系统日志过滤器中可以使用的正则表达式语法：

表 69-6　　系统日志过滤器语法

语法构成	说明	示例
.	匹配任意字符或空格	`Admi.`匹配 `Admin`、 `AdmiN`、 `Admi1` 和 `Admi&`
`[[:alpha:]]`	匹配任意字母字符	`[[:alpha:]]dmin` 匹配 `Admin`、 `bdmin` 和 `Cdmin`
`[[:upper:]]`	匹配任意大写字母字符	`[[:upper:]]dmin` 匹配 `Admin`、 `Bdmin` 和 `Cdmin`
`[[:lower:]]`	匹配任意小写字母字符	`[[:lower:]]dmin` 匹配 `admin`、 `bdmin` 和 `cdmin`
`[[:digit:]]`	匹配任意数字字符	`[[:digit:]]dmin` 匹配 `0dmin`、 `1dmin` 和 `2dmin`
`[[:alnum:]]`	匹配任意字母数字字符	`[[:alnum:]]dmin` 匹配 `1dmin`、 `admin`、 `2dmin` 和 `bdmin`
`[[:space:]]`	匹配任意空格，包括选项卡	`Feb[[:space:]]29` 匹配从 2 月 29 日起的日志。
*	匹配其符合的字符或表达式的零个或更多实例	`ab*` 匹配 `a`、 `ab`、 `abb`、 `ca`、 `cab` 和 `cabb` `[ab]*` 匹配所有字符
?	匹配零个或一个实例	`ab?`匹配 `a` 或 `ab`。
\	您可以搜索一般会被解释为正则表达式语法的字符	`alert\?`匹配 `alert?`。

下表显示了您可在 System Log 页面使用的某些示例过滤器。

表 69-7　　系统日志过滤器示例

要搜索所有下列日志条目.....	使用.....
在 11 月 5 日生成	`Nov[[:space:]]*5`
包含用户名“Admin”	管理
包含 11 月 5 日的授权调试信息	`Nov[[:space:]]*5.*AUTH.*DEBUG`

要在系统日志中搜索特定消息内容，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Monitoring > Syslog**。

系统将显示 System Log 页面。

步骤 2　在 Filter 字段中输入单词或查询。

有关可以使用的过滤器语法的详细信息，请参阅上表。

注　支持仅与 Grep 兼容的搜索语法。例如，您可使用 `ntp` 作为过滤器搜索所有 NTP 相关的系统日志消息，或将 `Nov` 用作过滤器搜索在 11 月生成的所有消息。您可以使用 `Nov[[:space:]]*27` 或 `Nov.*27` 查看从 11 月 27 日起生成的消息，但您无法使用 `Nov 27` 或 `Nov*27` 查看此类消息。

步骤 3　或者，要使您的搜索区分大小写，选择 **Case-sensitive**。（默认情况下，过滤器不区分大小写。）

步骤 4　或者，勾选 **Exclusion** 搜索**不**符合所输入标准的所有系统日志消息。

步骤 5　点击 **Go**。

系统将显示匹配过滤器的消息。

使用备份和恢复

备份和恢复是所有系统维护计划的重要部分。当每个组织的备份计划极具个性化时， FireSIGHT 系统为归档数据提供一种机制，以便可在灾难情况下恢复来自防御中心或物理受管设备的数据。

请注意有关备份和恢复的以下限制：

- 备份仅对您创建备份所使用的产品版本有效。
- 备份不包括捕获的文件数据。
- 您无法为虚拟受管设备、用于 Blue Coat X-系列的思科 NGIPS 或具备 FirePOWER 服务的 Cisco ASA 防火墙 创建或恢复备份文件。要备份所有事件数据，请对管理防御中心执行备份。
- 只有两个设备是同一型号并且运行相同版本的 FireSIGHT 系统软件，才能将备份恢复到替换设备上。

注意事项 请勿使用备份和恢复过程来在受管设备之间复制配置文件。配置文件包括设备的唯一识别信息，并且不能共享。

注意事项 如果应用了任何入侵规则更新，不会备份这些更新。在恢复**之后**，需要应用最新的规则更新。

可以将备份文件保存到设备或本地计算机。此外，如果使用的是防御中心，可以使用远程存储，如第 64-14 页上的管理远程存储中详细说明。

注意事项 请勿将 USB 驱动器插入 3D9900 的任何 USB 端口。此外，在升级或恢复设备之前，请从 3D9900 删除具有外部存储的所有设备 （例如，具有外部存储的 KVM 切换器）。

有关详细信息，请参阅：

- 有关为防御中心和物理受管设备创建备份文件的信息，请参阅第 70-2 页上的创建备份文件。
- 有关创建以后可作为备份创建模板的备份配置文件的信息，请参阅第 70-5 页上的创建备份配置文件。
- 有关从本地主机上传备份文件的信息，请参阅第 70-6 页上的从本地主机上传备份。
- 有关如何恢复设备的备份文件的信息，请参阅第 70-7 页上的从备份文档恢复设备。

创建备份文件

许可证：任何环境

受支持的设备：任何设备，虚拟设备、 X -系列 和 ASA FirePOWER 除外

受支持的防御中心：任何环境

您可以从设备本身执行物理受管设备备份、从其管理防御中心执行物理受管设备备份和防御中心的备份。系统根据您执行备份的类型备份不同数据。请注意系统**不会**备份捕获的文件数据。使用下表确定要执行哪种备份。

表 70-1　　按备份类型存储的数据

备份类型	包括配置数据？	包括事件数据？	包括统一文件？
防御中心	是	是	否
物理受管设备，从设备本身执行	是	否	否
物理受管设备，从管理防御中心执行	是	否	是

注　您**无法**为虚拟受管设备、用于 Blue Coat X-系列的思科 NGIPS 或 具备 FirePOWER 服务的 Cisco ASA 防火墙 创建或恢复备份文件。要备份事件数据，请对管理防御中心执行备份。

要查看和利用现有系统备份，请转到 Backup Management 页面。除事件数据外，还应定期保存包含恢复设备所需的所有配置文件的备份文件。在测试配置更改时也可能需要备份系统，以便可以根据需要还原已保存的配置。可以选择将备份文件保存到设备或本地计算机。

如果设备没有足够的磁盘空间，则无法创建备份文件；如果备份进程使用了 90% 以上的可用磁盘空间，备份可能会失败。如果需要，请删除旧备份文件，将旧备份文件从设备转出或使用远程存储。

此外，或者如果备份文件超过 4 GB，还可以通过 SCP 将其复制到远程主机。从本地计算机上传的备份文件不能超过 4 GB，因为网络浏览器不支持这样大的上传文件。在防御中心上，备份文件可保存到远程位置；有关详细信息，请参阅第 64-14 页上的管理远程存储。

注　当备份任务正在收集发现事件时，数据关联将暂时中断。

请注意：

- 与 PKI 对象关联的私有密钥在存储到设备时生成随机加密密钥。如果执行包含与 PKI 对象关联的私人密钥的备份，在被纳入未加密备份文件之前密钥将解密。在安全的位置存储备份文件。
- 如果您恢复包含与 PKI 对象关联的私有密钥的备份，系统会使用随机生成的密钥加密这些密钥，再将其存储在设备上。
- 如果执行备份，请删除审阅过的入侵事件，备份将恢复已删除的入侵事件，但不能恢复它们的已审阅状态。可在 Intrusion Events （而不是 Reviewed Events）下查看这些恢复的入侵事件。请参阅第 41-14 页上的审核入侵事件。
- 如果在已经包含数据的设备上恢复包含入侵事件数据的备份，将创建重复事件。为避免这种情况，仅限在不包含以往恢复入侵事件数据的设备上恢复入侵事件备份。

注意事项　如果为安全区域配置了任何接口关联，将不会备份这些关联。在恢复后，必须重新配置它们。有关详细信息，请参阅第 3-34 页上的使用安全区域。

要为防御中心创建备份文件，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Backup/Restore**。

系统将显示 Backup Management 页面。

步骤 2　点击 **防御中心 Backup**。

系统将显示 Create Backup 页面。

步骤 3　在 **Name** 字段中，键入一个备份文件名称。可以使用字母数字字符、标点符号和空格。

步骤 4　在防御中心中，有两个其他选项：

- 要归档配置，请选择 **Back Up Configuration**。
- 要归档整个事件数据库，请选择 **Back Up Events**。

步骤 5　或者，为了在备份完成时收到通知，请选择 **Email** 复选框并在随附的文本框中键入邮件地址。

注　要接收电邮通知，您必须配置中继主机，如第 63-17 页上的配置邮件中继主机和通知地址中所述。

步骤 6　或者，在防御中心中使用安全复制 (SCP) 将备份归档复制到不同的机器，选择 **Copy when complete** 复选框，然后在随附的文本框中键入以下信息：

- 在 **Host** 字段中，键入要复制备份的机器的主机名或 IP 地址
- 在 **Path** 字段中，键入要复制备份目录路径
- 在 **User** 字段中，键入要用于登录 Telnet 远程机器的用户名
- 在 **Password** 字段中，键入该用户名的密码
  如果希望使用 SSH 公共密钥而不是密码来访问远程机器，则必须将 **SSH Public Key** 字段中的内容到该机器上指定用户的 `authorized_keys` 文件中。

在此选项处于清除状态时，系统在远程服务器上存储备份期间使用的临时文件；选择此选项时，不在远程服务器上存储该临时文件。

提示　思科建议定期将备份保存到远程位置，这样才可以在系统故障时恢复设备。

步骤 7　您有以下选项：

- 要将备份文件保存到设备，请点击 **Start Backup**。

  备份文件会保存到 `/var/sf/backup` 目录中。可以直接将备份文件保存到远程位置；请参阅第 64-14 页上的管理远程存储。

  当备份过程完成后，可以在 Restoration Database 页面查看文件。有关恢复备份文件的信息，请参阅第 70-7 页上的从备份文档恢复设备。

- 要将此配置保存为可供以后使用的备份配置文件，请点击 **Save As New**。

  可以通过选择 **System > Tools > Backup/Restore**，然后点击 **Backup Profiles** 来修改或删除备份配置文件。有关详情，请参见第 70-5 页上的创建备份配置文件。

要从设备本身为物理受管设备创建备份文件，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Backup/Restore**。

系统将显示 Device Backups 页面。

步骤 2　点击 **Device Backup**。

系统将显示 Create Backup 页面。

步骤 3　在 **Name** 字段中，键入一个备份文件名称。可以使用字母数字字符、标点符号和空格。

步骤 4　或者，为了在备份完成时收到通知，请选择 **Email** 复选框并在随附的文本框中键入邮件地址。

注　要接收电邮通知，您必须配置中继主机，如第 63-17 页上的配置邮件中继主机和通知地址中所述。

步骤 5　或者，要使用安全复制 (SCP) 将备份档案复制到不同的设备上，请选择 **Copy when complete** 复选框，然后在随附的文本框中键入以下信息：

- 在 **Host** 字段中，键入要复制备份的机器的主机名或 IP 地址
- 在 **Path** 字段中，键入要复制备份目录路径
- 在 **User** 字段中，键入要用于登录 Telnet 远程机器的用户名
- 在 **Password** 字段中，键入该用户名的密码
  如果希望使用 SSH 公共密钥而不是密码来访问远程机器，则必须将 **SSH Public Key** 字段中的内容到该机器上指定用户的 `authorized_keys` 文件中。

在此选项处于清除状态时，系统在远程服务器上存储备份期间使用的临时文件；选择此选项时，不在远程服务器上存储该临时文件。

提示　思科建议定期将备份保存到远程位置，这样才可以在系统故障时恢复设备。

步骤 6　您有以下选项：

- 要将备份文件保存到设备，请点击 **Start Backup**。

  备份文件会保存到 `/var/sf/backup` 目录中。在防御中心中，可以直接将备份文件保存到远程位置；请参阅第 64-14 页上的管理远程存储。

  当备份过程完成后，可以在 Restoration Database 页面查看文件。有关恢复备份文件的信息，请参阅第 70-7 页上的从备份文档恢复设备。

- 要将此配置保存为可供以后使用的备份配置文件，请点击 **Save As New**。

  可以通过选择 **System > Tools > Backup/Restore**，然后点击 **Backup Profiles** 来修改或删除备份配置文件。有关详情，请参见第 70-5 页上的创建备份配置文件。

要从管理防御中心为物理受管设备创建备份文件，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Backup/Restore**。

系统将显示 Backup Management 页面。

步骤 2　选择 **Managed Device Backup**。

系统将显示 Create Backup 页面。

步骤 3　在 **Managed Devices** 字段，选择一个或多个受管设备。使用 Shift 或 Ctrl 键选择多个受管设备。

步骤 4　除配置数据外，如果还要包含统一文件，请选择 **Include All Unified Files** 复选框。

步骤 5　要在防御中心中保存备份文件，请选择 **Retrieve to** 防御中心 复选框。要在设备上保存每个设备的备份文件，则不选择该复选框。

注　如果选择 **Retrieve to 防御中心** 并且防御中心配置为远程存储备份，则设备备份文件将保存到所配置的远程位置，而不是防御中心本身。

步骤 6　点击 **Start Backup**。

系统将显示成功消息，备份任务创建成功。

备份文件会保存到 `/var/sf/backup` 目录中。通过使用防御中心，可以直接将备份文件保存到远程位置；请参阅第 64-14 页上的管理远程存储。

当备份过程完成后，可以在 Restoration Database 页面查看文件。有关恢复备份文件的信息，请参阅第 70-7 页上的从备份文档恢复设备。

步骤 7　或者，要将此配置另存为可供以后使用的备份配置文件，请点击 **Save As New**。

可以通过选择 **System > Tools > Backup/Restore**，然后点击 **Backup Profiles** 来修改或删除备份配置文件。有关详情，请参见第 70-5 页上的创建备份配置文件。

创建备份配置文件

许可证：任何环境

受支持的设备：任何设备，虚拟设备、 X -系列和 ASA FirePOWER 除外

受支持的防御中心：任何环境

可以使用 Backup Profiles 页面创建包含要用于不同类型备份的设置的备份配置文件。稍后可以在设备上备份文件时，选择这两个配置文件。

提示　当如所第 70-2 页上的创建备份文件述创建备份文件时，自动创建备份配置文件。

要创建配置文件，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Backup/Restore**。

系统将显示 Backup Management 页面。

步骤 2　点击 the **Backup Profiles** 选项卡。

系统将显示 Backup Profiles 页面和现有备份配置文件列表。

提示　可以点击编辑图标 ( ) 来修改现有配置文件或点击删除图标 ( ) 从列表中删除配置文件。

步骤 3　点击 **Create Profile**。

系统将显示 Create Backup 页面。

步骤 4　键入一个备份配置文件名称。可以使用字母数字字符、标点符号和空格。

步骤 5　根据需要配置备份配置文件。

有关此页面中的选项的详细信息，请参阅第 70-2 页上的创建备份文件。

步骤 6　点击 **Save As New** 来保存备份配置文件。

系统将显示 Backup Profiles 页面，此时新配置文件显示在列表中。

从本地主机上传备份

许可证：任何环境

受支持的设备：2 系列和 3 系列

受支持的防御中心：任何环境

如果使用 Backup Management 表中描述的下载功能将备份文件下载到本地主机，可以将文件上传到防御中心。

如果备份文件包含 PKI 对象，与内部 CA 和内部证书对象关联的私有密钥在上传时将通过随机生成的密钥来重新加密。

提示　无法从本地主机上传大于 4 GB 的备份，因为网络浏览器不支持这样大的上传文件。还可以使用 SCP 将备份复制到远程主机，然后从中检索。在防御中心中，备份文件可以保存到远程位置并从中检索；请参阅第 64-14 页上的管理远程存储。

要从本地主机上传备份，请执行以下操作：

访问：管理员/维护人员

步骤 1　选择 **System > Tools > Backup/Restore**。

系统将显示 Backup Management 页面。

步骤 2　点击 **Upload Backup**。

系统将显示 Upload Backup 页面。

步骤 3　单击 **Browse** 按钮并导航到要上传的备份文件。

在选择要上传的文件后，点击 **Upload Backup**。

步骤 4　点击 **Backup Management** 以返回 Backup Management 页面。

备份文件上传并在备份列表显示。在防御中心设备验证文件完整性之后，刷新 Backup Management 页面显示详细文件系统信息。

从备份文档恢复设备

许可证：任何环境

受支持的设备：2 系列和 3 系列

受支持的防御中心：任何环境

使用 Backup Management 页面，可以从备份文件恢复设备。要恢复备份，备份文件中的 VDB 版本必须与设备的当前 VDB 版本相符。完成恢复过程后，**必须**应用最新的 Sourcefire 规则更新。

注意事项 请勿将在虚拟防御中心上创建的备份恢复到物理防御中心中，这可能使系统资源不堪重负。如果必须在物理防御中心上恢复虚拟备份，请与技术支持部门联系。

如果备份文件包含 PKI 对象，与内部 CA 和内部证书对象关联的私有密钥在上传时将通过随机生成的密钥来重新加密。

如果使用本地存储，备份文件将保存到 `/var/sf/backup`， `/var` 分区中使用的磁盘空间将在 Backup Management 页面底部列出。在防御中心中，选择 Backup Management 页面顶部的 **Remote Storage** 来配置远程存储选项；然后选择 **Enable Remote Storage for Backups**复选框以在备份管理页面启用远程存储。如果使用远程存储，协议、备份系统和备份目录将列在页面底部。

注 如果在备份完成后添加许可证，即使备份恢复，这些许可证不会删除也不会被覆盖。为防止恢复时出现冲突，请在恢复备份之前移除这些许可证，记住许可证使用位置，并在恢复备份之后添加和重新配置它们。如果发生冲突，请与技术支持部门联系。

下表说明在 Backup Management 页面的各列和图标。

表 70-2　Backup Management

功能	说明
系统信息	原始设备名称、类型和版本。注意只能将备份恢复到同样的设备类型和版本。
创建日期	备份文件创建的日期和时间
文件名	备份文件的全名
VDB Version	备份时在设备上运行的漏洞数据库 (VDB) 版本。
位置	备份文件的位置
Size (MB)	备份文件的大小，以兆字节计算
Events?	“是”表示包括事件数据的备份
View	点击备份文件的名称可查看压缩备份文件中的文件列表。
恢复	点击所选的备份文件可将其恢复其到设备。如果 VDB 版本与备份文件中的 VDB 版本不相符，将禁用此选项。
下载	点击所选的备份文件可将其保存到本地计算机。
删除	点击所选的备份文件可将其删除。
升级	在防御中心中，当选择先前创建的本地备份时，点击可将备份发送到指定的远程备份位置。

要从备份文件恢复设备，请执行以下操作：

访问：管理

步骤 1　选择 **System > Tools > Backup/Restore**。

系统将显示 Backup Management 页面。

步骤 2　要查看备份文件的内容，请单击该文件的名称。

系统将显示清单，列出每个文件名称、所有者和权限及其文件大小和日期。

步骤 3　点击 **Backup Management** 以返回 Backup Management 页面。

步骤 4　选择要恢复的备份文件并点击 **Restore**。

系统将显示 Restore Backup 页面。

请注意，如果备份中的 VDB 版本与设备当前安装的 VDB 版本不相符， **Restore** 按钮会变为灰色。

注意事项　此步骤会覆盖所有配置文件，在受管设备上，会覆盖所有事件数据。

步骤 5　要恢复文件，请选择以下选项之一或两项均选择：

- **Replace Configuration Data**
- **Restore Event Data**

注　请注意，当从备份文件恢复受管设备的配置时，从设备的管理防御中心作出的所有设备配置更改也将恢复，甚至是在创建该备份文件之后所做的更改。

步骤 6　点击 **Restore** 开始恢复。

设备将使用指定的备份文件恢复。

步骤 7　重新启动设备。

步骤 8　应用最新的 Sourcefire 规则更新，从而重新应用规则更新。

步骤 9　将任何访问控制、入侵、网络发现、运行状况和系统策略重新应用到恢复的系统。

指定用户首选项

可以配置与单个用户帐户，例如主页、帐户密码、时区、控制面板和事件查看首选项相关联的首选项。

根据用户角色，可以指定用户帐户的一些首选项，包括密码、事件查看首选项、时区设置和主页首选项。有关详细信息，请参阅：

- 第 71-1 页上的更改密码说明如何更改用户帐户的密码。
- 第 71-2 页上的指定主页说明如何将其中一个现有页面用作默认主页。设置此值后，此页面将成为登录该设备后看到的第一个页面。
- 第 71-3 页上的配置事件查看设置介绍事件首选项如何影响查看事件时所看到的内容。
- 第 71-6 页上的设置默认时区说明如何设置用户帐户的时区并介绍如何影响所查看事件的时间戳。
- 第 71-7 页上的指定默认控制面板说明如何选择要用作默认控制面板的控制面板。

更改密码

许可证：任何环境

受支持的设备：2 系列、 3 系列

受支持的防御中心：任何环境

所有用户帐户均采用密码保护。可以随时更改密码，根据用户帐户设置，可能需要定期更改密码；请参阅第 71-2 页上的更改过期密码。

请注意，如果密码强度检查已启用，则密码必须至少包含 8 个大小写混合的字母数字字符，并且至少包含一个数字字符。密码中包含的单词不能是在词典中出现过的单词或包含连续的重复字符。

注 如果是 LDAP 或 RADIUS 用户，则不能通过网络界面更改密码。

要更改密码，请执行以下操作：

访问：任何环境

步骤 1 在用户名下面的下拉列表中，选择 **User Preferences**。

系统将显示 Change Password 页面。

步骤 2 在 **Current Password** 字段中，键入当前密码并点击 **Change**。

步骤 3 在 **New Password** 和 **Confirm** 字段中，键入新密码。

步骤 4　点击 **Change**。

在系统接受新密码后，一则成功消息会显示在该页面上。

更改过期密码

许可证：任何环境

受支持的设备：2 系列、 3 系列

受支持的防御中心：任何环境

根据用户帐户设置，密码可能已过期。请注意，在帐户创建完成后，系统就会设置密码过期时间段，并且无法更改。如果密码已过期，系统会显示 Password Expiration Warning 页面。

要响应密码过期警告，请执行以下操作：

访问：任何环境

步骤 1　您有两种选择：

- 点击 **Change Password**，立即更改密码。

  如果警告天数为零，则**必须**更改密码。而且，如果密码强度检查已启用，则密码必须至少包含 8 个大小写混合的字母数字字符，并且至少包含一个数字字符。密码中包含的单词不能是在词典中出现过的单词或包含连续的重复字符。

- 点击 **Skip**，稍后更改密码。

指定主页

许可证：任何环境

可以将网络界面中的页面指定为该设备的主页。默认主页是 Summary Dashboard (**Overview > Dashboards**)，不具有控制面板访问权限且使用 Welcome 的用户除外。

要指定主页，请执行以下操作：

访问：除外部数据库用户以外的任何用户

步骤 1　在用户名下面的下拉列表中，选择 **User Preferences**。

系统将显示 Change Password 页面。

步骤 2　点击 **Home Page**。

系统将显示 Home Page 页面。

步骤 3　从下拉列表中选择要用作主页的页面。

下拉列表中的选项基于用户帐户的访问权限。有关详细信息，请参阅第 61-52 页上的用户帐户权限。

步骤 4　点击 **Save**。

将会保存主页首选项

配置事件查看设置

许可证：任何环境

使用 Event View Settings 页面配置 FireSIGHT 系统中的事件查看的特征。请注意，一些事件查看配置仅对特定的用户角色可用。使用外部数据库用户角色的用户可以查看事件查看设置用户界面的某些部分，但是更改这些设置不会产生有意义的结果。有关详细信息，请参阅以下链接的各节。

要配置活动首选项，请执行以下操作：

访问：因功能而异

步骤 1　在用户名下面的下拉列表中，选择 **User Preferences**。

系统将显示 User Preferences 页面。

步骤 2　点击 **Event View Settings**。

系统将显示 Event View Settings 页面。

步骤 3　配置事件查看的基本特征。

有关详细信息，请参阅第 71-3 页上的事件首选项。

步骤 4　配置文件下载首选项。

有关详细信息，请参阅第 71-4 页上的文件首选项。

步骤 5　配置默认的时间段或多个时间段。

有关详细信息，请参阅第 71-5 页上的默认时间段。

步骤 6　配置默认工作流程。

有关详细信息，请参阅第 71-6 页上的默认工作流程。

步骤 7　点击 **Save**。

更改已实施。

事件首选项

许可证：任何环境

使用 Event View Settings 页面的 Event Preferences 区域，配置 FireSIGHT 系统中事件查看的基本特征。尽管此区域对无法查看事件的用户不重要，但所有用户角色均可使用。

以下字段显示在 Event Preferences 区域：

- **Confirm “All” Actions** 字段控制设备是否强制确认影响事件查看中所有事件的操作。

  例如，如果已启用此设置且点击事件查看上的 **Delete All**，必须确认要删除的所有事件满足当前的限制条件 （包括在当前页面未显示的活动），然后才可将其从数据库中删除。

- **Resolve IP Addresses** 字段允许设备显示主机名 （若可能），而非事件查看的 IP 地址。

  请注意，如果事件查看包含大量 IP 地址，并且已启用该选项，则该视图可能缓慢显示。另请注意，若要使此设置生效，则必须具有在系统设置中配置的 DNS 服务器；请参阅第 64-8 页上的配置管理接口。

- **Expand Packet View** 字段可供您配置入侵事件数据包视图的显示方式。默认情况下，设备以折叠方式显示数据包视图：
  - **None** - 折叠数据包视图的 Packet Information 部分的所有子部分
  - **Packet Text** - 仅展开 Packet Text 子部分
  - **Packet Bytes** - 仅展开 Packet Bytes 子部分
  - **All** - 展开所有部分

  无论默认设置如何，您始终可以手动展开数据包视图中的部分查看有关已捕获数据包的详细信息。有关数据包视图的详细信息，请参阅第 41-19 页上的使用数据包视图。
- **Rows Per Page** 字段控制要在向下页面和表视图中显示的每页事件行数。
- **Refresh Interval** 字段设置事件查看的刷新时间间隔 （以分钟为单位）。输入 0 可禁用刷新选项。请注意，此时间间隔不适用于控制面板。
- **Statistics Refresh Interval** 控制事件摘要页面 （例如， Intrusion Event Statistics 和 Discovery Statistics 页面）的刷新时间间隔。输入 0 可禁用刷新选项。请注意，此时间间隔不适用于控制面板。
- **Deactivate Rules** 字段控制哪些链接显示在标准文本规则生成的入侵事件的数据包视图上：
  - **All Policies** - 用于取消激活所有本地定义的自定义入侵规则中的标准文本规则的一个链接。
  - **Current Policy** - 用于停用仅当前应用的入侵规则中的标准文本规则的一条链接。请注意，您不能停用默认策略中的规则。
  - **Ask** - 每一这些选项的链接

  要在数据包视图上看到这些链接，您的用户帐户必须具有管理员或入侵管理员权限。

文件首选项

许可证：任何环境

受支持的设备：因功能而异

受支持的防御中心：因功能而异

使用 Event View Settings 页面的 File Preferences 部分配置本地文件下载的基本特征。此部分仅适用于具有管理员、安全分析师或安全分析师 （只读）用户角色的用户。

请注意，如果设备不支持下载捕获的文件，则这些选项会禁用。由于无法将 恶意软件 许可证用于 DC500，则无法使用这些设备下载文件或修改这些选项。

以下字段显示在 File Preferences 区域：

- **Confirm 'Download File' Actions** 复选框控制 File Download 弹出窗口是否每次都显示下载文件，同时显示警告并提示继续或取消。

注意事项 思科强烈建议您**不要**下载恶意软件，否则可能造成不利后果。下载任何文件时请保持谨慎，这些文件可能包含恶意软件。确保您在下载文件前已采取各种必要预防措施保证下载目标安全。

请注意，在下载文件时，可随时禁用此选项。有关下载文件的详细信息，请参阅第 40-3 页上的将存储的文件下载至另一位置。

- 当下载一个捕获的文件时，系统会创建包含该文件的密码保护的 .zip 归档文件。 **Zip File Password** 字段定义要用于限制 .zip 文件的访问权限的密码。如果将此字段留空，系统会创建归档文件，不需要密码。

- **Show Zip File Password** 复选框会切换显示 **Zip File Password** 字段中的纯文本或模糊字符。当清除此字段时， **Zip File Password** 显示模糊字符。

默认时间段

许可证：任何环境

时间段，有时称为时间范围，会对任何事件查看中的事件施加时间限制。使用 Event View Settings 页面的 Default Time Windows 区域控制时间段的默认行为。

此区域的用户角色访问权限列出如下：

- 管理员和维护人员可以访问完整的区域。
- 安全分析师和安全分析师 （只读）可访问除 **Audit Log Time Window** 之外的所有选项。
- 访问管理员、发现管理员、外部数据库用户、入侵管理员、网络管理员和安全审批人只可访问 **Events Time Window** 选项。

请注意，无论默认时间段设置如何，在事件分析期间，可以始终手动更改单个事件查看的时间段。另请注意，时间段设置仅对当前会话有效。在注销后重新登录时，时间段会重置为在此页面中配置的默认设置。有关详细信息，请参阅第 58-19 页上的设置事件时间限制。

可为以下三种类型的事件设置默认时间段：

- **Events Time Window** 可为按时间限制的多数事件设置单个默认时间段。
- **Audit Log Time Window** 可为审核日志设置默认时间段。
- **Health Monitoring Time Window** 可为运行状况事件设置默认时间段。

仅可以为用户帐户可访问的事件类型设置时间段。所有用户类型都可设置事件事件段。管理员、维护人员和安全分析师可以设置运行状况监控时间段。管理员和维护人员可以设置审核日志时间段。

请注意，因为不是所有的事件查看都可以受时间限制，所以时间段设置对显示主机、主机属性、应用程序、客户端、漏洞、用户身份或白名单违规的事件查看没有影响。

可以使用**多个**时间段，每种事件类型一个，也可以使用适用于所有事件的**一个**时间段。如果使用一个时间段，则不会显示三种时间段类型的设置，会显示新的 **Global Time Window** 设置。

有以下三种类型的时间段：

- *静态*，显示在某个特定开始时间和特定结束时间期间生成的所有事件
- *扩展*，显示在某个特定开始时间和当前时间期间生成的所有事件；随着时间向前推进，时间段会扩展，新的事件会添加到事件查看
- *滑动*，显示在某个特定开始时间 （例如，一天前）和当前时间期间生成的所有事件；随着时间向前推进，时间段会“滑动”，以便只可以查看所配置范围内的事件 （在本示例中，为最后一天）

所有时间段的最大时间范围都是从 1970 年 1 年 1 日午夜 (UTC) 到 2038 年 1 月 19 日凌晨 3:14:07 (UTC)。

以下选项显示在 **Time Window Settings** 下拉列表：

- **Show the Last - Sliding** 选项允许配置指定长度的默认滑动时间窗。

  设备显示在某个特定开始时间 （例如， 1 小时前）和当前时间期间生成的所有事件。当更改事件查看，时间段会“滑动”，以便始终可查看最近一小时的事件。

- **Show the Last - Static/Expanding** 选项允许配置静态或扩展指定长度的默认时间段。

  对于**静态**时间段，启用 **Use End Time** 复选框。设备会显示在某个特定开始时间 （例如， 1 小时前）和第一次查看事件时的时间期间生成的所有事件。更改事件查看后，时间段会固定，以便只可查看在静态时间段内发生的事件。

对于**扩展**时间段，禁用 **Use End Time** 复选框。设备显示在某个特定开始时间 （例如， 1 小时前）和当前时间期间生成的所有事件。在更改事件查看后，时间段会扩展为当前时间。

- **Current Day - Static/Expanding** 选项允许为当日配置静态或扩展默认时间段。当日从午夜开始，基于当前会话的时区设置。

  对于**静态**时间段，启用 **Use End Time** 复选框。设备会显示从午夜到第一次查看事件时的时间期间生成的所有事件。更改事件查看后，时间段会固定，以便只可查看在静态时间段内发生的事件。

  对于**扩展**时间段，禁用 **Use End Time** 复选框。设备会显示在午夜到当前时间期间生成的所有事件。在更改事件查看后，时间段会扩展为当前时间。请注意，如果分析在注销之前持续超过 24 小时，则时间段可能会超过 24 小时。

- **Current Day - Static/Expanding** 选项允许为当前星期配置静态或扩展默认时间段。当周从上一周日的午夜开始，基于当前会话的时区设置。

  对于**静态**时间段，启用 **Use End Time** 复选框。设备会显示从午夜到第一次查看事件时的时间期间生成的所有事件。更改事件查看后，时间段会固定，以便只可查看在静态时间段内发生的事件。

  对于**扩展**时间段，禁用 **Use End Time** 复选框。设备会显示在周日午夜到当前时间期间生成的所有事件。在更改事件查看后，时间段会扩展为当前时间。请注意，如果在您注销之前，分析持续 1 周以上，则此时间段可以超过 1 周。

默认工作流程

许可证：任何环境

工作流程是一组页面，显示分析师评估事件所使用的数据。对于每个事件类型，设备附带了至少一个预定义工作流程。例如，作为安全分析师，根据执行分析的类型，可以在十种入侵事件工作流程中选择，每种类型都会以不同的方式显示入侵事件数据。

设备会使用每种事件类型的默认工作流程进行配置。例如，按优先级和分类事件的工作流程是入侵事件的默认值。这意味着，只要查看入侵事件 （包括已审阅的入侵事件），设备都会显示按优先级和分类事件的工作流程。

但是，可以使用 Event View Settings 页面的 Default Workflows 区域更改每种事件类型的默认工作流程。

请谨记，可配置的默认工作流程取决于用户角色。例如，入侵事件分析师无法设置默认发现事件工作流程。有关工作流程的一般信息，请参阅第 58-1 页上的了解和使用工作流程。

设置默认时区

许可证：任何环境

可以更改用于显示设备使用的标准 UTC 时间内事件的时间段。当配置时区时，它仅适用于用户帐户，并且在进一步更改时区之前有效。

注意事项　时区功能假设，默认系统时钟设置为 UTC 时间。如果更改设备的系统时钟使用本地时区，则必须将其更改回 UTC 时间，以查看设备的准确本地时间。有关防御中心和受管设备之间的时间同步的详细信息，请参阅第 63-24 页上的同步时间。

要更改时区，请执行以下操作：

访问：任何环境

步骤 1　在用户名下面的下拉列表中，选择 **User Preferences**。

系统将显示 Change Password 页面。

步骤 2　点击 **Time Zone Settings**。

系统将显示 Time Zone Preference 页面。

步骤 3　从左侧列表框中，选择包含要使用时区的大陆或区域。

例如，如果要将时区标准用于北美、南美或加拿大，请选择 **America**。

步骤 4　从右侧的列表框中，选择与要使用的时区相符的时区 （城市名）。

例如，如果要使用东部标准时间，需在第一个时区框中选择 **America** 后，选择 **New York**。

步骤 5　点击 **Save**。

时区已设置。

指定默认控制面板

许可证：任何环境

可以在设备上指定一个控制面板，作为默认控制面板。选择 **Overview > Dashboards** 时，会显示默认控制面板。如果没有定义默认控制面板，系统将显示 Dashboard List 页面。有关控制面板的一般信息，请参阅第 55-1 页上的使用控制面板。

要指定默认控制面板，请执行以下操作：

访问：管理员/维护人员/任何安全分析师

步骤 1　在用户名下面的下拉列表中，选择 **User Preferences**。

系统将显示 Change Password 页面。

步骤 2　点击 **Dashboard Settings**。

系统将显示 Dashboard Settings 页面。

步骤 3　从下拉列表中选择要用作默认控制面板的控制面板。

如果选择 **None**，则在选择 **Overview > Dashboards** 时，系统会显示 Dashboard List 页面。可以选择要查看的控制面板。

步骤 4　点击 **Save**。

默认控制面板首选项已保存。

导入和导出配置

您可使用 Import/Export 功能在同类设备之间复制多种类型的配置，包括策略。配置导入和导出不应作为备份工具，但可简化将新设备添加至 FireSIGHT 系统的过程。

您可导入和导出下列配置：

- 访问控制策略及其关联网络分析、 SSL 和文件策略
- 入侵策略
- 运行状况和系统策略
- 警报响应
- 应用检测器
- 控制面板、自定义表、自定义工作流程和保存的搜索
- 自定义用户角色
- 报告模板
- 第三方产品和漏洞映射

要导入已导出的配置，两种设备必须运行相同版本的 FireSIGHT 系统。要导入一个已导出的入侵或访问控制策略，两个设备上的规则更新版本也必须相匹配。

有关详细信息，请参阅：

- 第 A-1 页上的导出配置
- 第 A-4 页上的导入配置

导出配置

许可证：任何环境

您可导出单项配置，也可立即导出一组 （相同类型或不同类型的）配置。当您稍后将软件包导入另一台设备时，您可选择要导入软件包中的哪些配置。

导出配置时，设备也导出该配置的版本信息。 FireSIGHT 系统使用该信息确定能否将该配置导入另一台设备；设备上已存在的配置版本无法导入。

此外，导出配置时，设备也导出该配置依存的系统配置，如身份验证对象。例如，如在防御中心上设置了 LDAP 服务器身份验证，然后导出启用了身份验证的防御中心系统策略，则也将导出身份验证对象。

提示 在 FireSIGHT 系统的许多列表页面中，列表项旁均包括导出图标 ()。如果该图标存在，您可将其作为下列导出步骤的快速替代项。

您可导出以下配置：

- *警报响应* - 警报响应是一组配置，可供 FireSIGHT 系统与您计划发送警报所在的外部系统进行交互。
- *自定义表* - 可构建一个自定义表，用于组合随 FireSIGHT 系统一起交付的两个或多个预定义表中的字段。
- *自定义用户角色* - 自定义用户角色是您所创建的用户角色，具有一组特殊访问权限。如果导出的自定义用户需要已保存的搜索，则也导出所有必需的已保存搜索。
- *自定义工作流* - 可创建自定义工作流，以满足贵组织的独特需求。在防御中心中，可导出您所创建的自定义工作流以及随设备一起交付的预定义自定义工作流。

  请注意，如果防御中心不允许查看已导出自定义工作流所基于的表格，虽然可导入该工作流，但无法查看它。
- *控制面板* - 控制面板是可自定义的选项卡式视图，在该视图中，当前系统状态一目了然。控制面板使用各种小组件显示与FireSIGHT 系统收集和生成的事件相关的数据，以及与部署设备的状态和整体运行状况相关的信息。

  请注意，您可查看的控制面板小组件取决于正在使用的设备类型和用户角色。有关详细信息，请参阅第 55-4 页上的了解构件可用性。
- *访问控制策略* - 可对访问控制策略包括的各个元素进行配置，以确定系统如何管理网络流量。这些组件包括访问控制规则；关联的入侵、文件、网络分析和 SSL 策略；以及规则和策略使用的对象 （包括入侵变量集）。导出访问控制策略也会导出该策略的所有设置和元素，但 URL 信誉和类别除外 （如存在），这些 URL 信誉和类别在所有设备上均相同且用户无法更改。请注意，要导入访问控制策略，在导出和导入防御中心上的规则更新版本必须匹配。

  如果您导出的访问控制策略或其调用的 SSL 策略包含引用地理位置数据的规则，则使用导入防御中心的地理位置数据库 (GeoDB) 更新版本。

  包含私有密钥信息的 PKI 对象在存储于设备上时使用随机生成的密钥加密。如果导出的访问控制策略引用的 SSL 策略使用了包含私有密钥的 PKI 对象，则在导出之前私有密钥会被解密。

  如果导出的访问控制策略引用了不受支持的 DC500 或 2 系列 设备策略功能或规则条件，将不能使用 DC500 应用该策略，且不能将该策略应用于 2 系列 设备。 DC500 和 2 系列设备均不支持用户或 URL 规则条件、 Security Intelligence 或包括使用了阻止恶意软件或恶意软件云查找操作的规则的文件策略。此外， 2 系列设备不支持应用规则条件。
- *运行状况策略* - 运行状况策略由检查部署设备运行状况 （即，检查思科硬件和软件是否正常运行）时所用的标准组成。
- *入侵策略* - 可配置入侵策略包括的各种元素，以检查网络流量是否存在入侵和政策违反之情况。检查协议报头值、负载内容和某些数据包大小特性的这些元素入侵规则；FireSIGHT 推荐的规则配置；以及其他高级设置。

  导出入侵策略也会导出该策略的所有设置。例如，如果您选择设置一条规则来生成事件，或为一条规则设置 SNMP 警报，或打开一个策略中的敏感数据预处理程序，则这些设置在已导出策略中仍保留在适当位置。自定义规则、自定义规则分类和用户定义的变量也会随策略一起导出。

  请注意，如果您导出的入侵策略与另一个入侵策略共享一个层，则该共享层将复制至正在导出的策略中，共享关系因而终止。当您将入侵策略导入另一台设备时，可根据自己的需求编辑已导入的策略，包括删除，添加和共享层。

当您在不同防御中心之间导出入侵策略时，如果第二个防御中心具有配置不同的默认变量，则已导入策略可能有不同的表现。

注 不能使用 Import/Export 功能更新思科的漏洞研究团队 (VRT) 创建的规则。相反，请下载并应用最新的规则更新版本；请参阅第 66-13 页上的导入规则更新和本地规则文件。

- *报告模板* - 报告是用于整理特定 FireSIGHT 系统数据的文件，采用 PDF、 HTML 或 CSV 格式。报告模板为报告及其各章节指定了数据搜索和格式。导出报告模板时，也将导出所有已保存的搜索、图像、在对象管理器中创建的对象以及报告所需的自定义表。
- *已保存的搜索* - 借助于已保存的搜索，权限有限的用户可访问预定义的 FireSIGHT 系统数据。当导出的自定义用户角色需要已保存的搜索时，也将导出所需的已保存搜索。还可导出各个用户定义的已保存搜索。
- *SSL 策略* - SSL 策略包括各种元素，您可以配置这些元素以确定系统如何管理网络上已加密的流量（包括 SSL 规则）及如何引用可重复使用的对象。导出 SSL 策略也会导出该策略的所有设置和元素，但 URL 信誉和类别除外 （如存在），这些 URL 信誉和类别在所有设备上均相同且用户无法更改。请注意，要导入 SSL 策略，在导出和导入防御中心上的规则更新版本必须想匹配。

  包含私有密钥信息的 PKI 对象在存储于设备上时使用随机生成的密钥加密。如果导出的 SSL 策略的 PKI 对象包含私有密钥，则私有密钥在导出之前会被解密。

  如果导出的 SSL 策略包含的规则引用了地理位置数据，则应使用导入防御中心的地理位置数据库 (GeoDB) 更新版本。
- *系统策略* - 系统策略控制一台设备可能类似于部署中其他 FireSIGHT 系统设备的各个方面，包括数据库事件限制、时间设置、登录提示等。

  如果正在导出的系统策略中已启用外部身份验证，则也将导出关联身份验证对象。

  请注意，防御中心 上系统策略包含的数据库设置不适用于受管设备。如将从受管设备导出的系统策略导入至 防御中心，则在设备上无法配置的数据库限制在防御中心上设置为默认值。
- *第三方产品映射* - 如从第三方应用导入数据，必须将产品映射至第三方名称，以分配漏洞并使用该数据执行影响关联。映射产品之后，会将思科漏洞信息与第三方产品名称相关联，以使 FireSIGHT 系统使用该数据执行影响关联。有关创建第三方产品映射的信息，请参阅第 46-27 页上的映射第三方产品。
- *第三方漏洞映射* - 要从第三方应用添加漏洞信息至漏洞数据库，您必须将每个已导入漏洞的第三方标识字符串映射至任何现有 思科、Bugtraq 或 Snort ID。为漏洞创建映射后，映射作用于导入至网络映射中主机的所有漏洞，并允许对这些漏洞进行影响关联。有关创建第三方漏洞映射的信息，请参阅第 46-30 页上的映射第三方漏洞。
- *应用检测器* - 系统分析 IP 流量时，使用检测器收集有关网络主机上运行的常用应用的信息，然后识别该应用。可导出两种检测器：用户定义的检测器和由思科专业服务部门提供的单一附加检测器。有关检测器的详细信息，请参阅第 46-14 页上的使用应用检测器。

注 导出过程可能需要几分钟，取决于正在导出的配置数量以及这些配置引用的对象数量。

要导出一项或多项配置，请执行以下操作：

访问：管理

步骤 1 确保配置导出设备与配置导入设备运行相同版本的 FireSIGHT 系统。如果导出入侵或访问控制策略，请确保规则更新版本相匹配。

如果 FireSIGHT 系统的版本 （以及规则更新版本，如适用）不匹配，导入将失败。

步骤 2　选择 **Systems > Tools > Import/Export**。

系统将显示 Import/Export 页面，其中包括设备上的配置列表。请注意，无配置需要导出的配置类别不显示在此列表中。

提示　点击配置类型旁的折叠文件夹图标 ( )，即可折叠配置列表。点击配置类型旁的展开文件夹图标 ( )，即可显示配置。

步骤 3　选择要导出的配置旁的复选框，单击 **Export**。

步骤 4　按照网页浏览器提示将已导出软件包保存至计算机。

导入配置

许可证：任何环境

可将从一台设备导出的配置导入另一台设备，只要设备支持此操作。但请注意，根据正在使用的设备类型和用户角色，有些导入的配置可能无用。

视乎正在导入的配置的类型，谨记以下要点：

- 确保配置导出设备与配置导入设备运行相同版本的 FireSIGHT 系统。如在导入一条入侵或访问控制策略，两个设备上的规则更新版本也必须匹配。如果版本不匹配，导入将失败。
- 当导入的自定义用户角色需要已保存的搜索时，也将导入所需的已保存搜索。
- 可查看的控制面板小组件取决于正在使用的设备类型和用户角色。例如，在防御中心上创建并导入受管设备 的控制面板可能显示一些无效、已禁用的小组件。
- 如果导入的访问控制策略根据区域评估流量，则必须将已导入策略中的区域映射至导入防御中心管理的设备上的区域。映射区域时，其类型必须匹配。因此，只有先在导入防御中心上创建所需的任何区域类型，然后才能开始导入。有关安全区域的详细信息，请参阅第 3-34 页上的使用安全区域。
- 如果导入的访问控制策略或已保存搜索包括名称与现有对象或对象组相同的对象或对象组，您必须重命名该对象或对象组。
- 如果导入访问控制策略或入侵策略，导入进程将用已导入默认变量取代默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。
- 如果导入的入侵策略与另一个入侵策略共享一个层，导出进程将终止此共享关系，之前的共享层将复制至软件包。换言之，已导入的入侵策略不包含共享层。

注　不能使用 Import/Export 功能更新思科的漏洞研究团队 (VRT) 创建的规则。相反，请下载并应用最新的规则更新版本；请参阅第 66-13 页上的导入规则更新和本地规则文件。

- 如果导入的 SSL 策略引用了包含私有密钥的 PKI 对象，系统会使用随机生成的密钥加密这些密钥，再将其存储在设备上。
- 导入从启用了外部身份验证的防御中心中导出的系统策略时，也将导入系统策略依存的身份验证对象。

由于可在单一软件包中导出多项配置，因此，导入软件包时必须选择将导入软件包中的哪些配置。只能导入目标设备支持的配置。

尝试导入配置时，设备会判断该配置在设备中是否已存在。如果存在冲突，则可：

- 保留现有配置，
- 使用新配置替换现有配置，
- 保留最新配置，或
- 导入该配置作为新配置。

如在目标系统上对已导入的配置做出修改，然后重新导入该配置，则必须选择要保留该配置的何种版本。

视乎正在导入的配置数量以及这些配置所引用的对象数量，导入过程可能需要几分钟。

要导入一项或多项配置，请执行以下操作：

访问：管理

步骤 1　确保配置导出设备与配置导入设备运行相同版本的 FireSIGHT 系统。要导入入侵或访问控制策略，您还必须确保规则更新版本相匹配。

如果 FireSIGHT 系统的版本 （以及规则更新版本，如适用）不匹配，导入将失败。

步骤 2　导出要导入的配置；请参阅第 A-1 页上的导出配置。

步骤 3　在要导入配置的设备上，选择 **System > Tools > Import/Export**。

系统将显示 Import/Export 页面。

提示　点击配置类型旁的折叠文件夹图标 ( )，即可折叠配置列表。点击配置类型旁的展开文件夹图标 ( )，即可显示配置。

步骤 4　点击 **Upload Package**。

系统将显示 Upload Package 页面。

步骤 5　此时您有两种选择：

- 键入要上传的配置包的路径。
- 点击 **Browse**，以浏览查找软件包。

步骤 6　点击 **Upload**。

上传结果取决于软件包的内容。

- 如果软件包的配置与设备中现有版本完全匹配，将显示一条消息表明该版本已存在。设备的配置已为最新，无需导入。
- 如果设备与软件包导出设备之间有一个 FireSIGHT 系统或 （如适用）规则更新版本不匹配，将显示一条消息，表明无法导入软件包。更新 FireSIGHT 系统或规则更新版本并重试。
- 如果软件包包含的任何配置或规则版本在设备上不存在，系统将显示 Package Import 页面。继续执行下一步。

步骤 7　选择要导入的配置并单击 **Import**。

导入进程开始解析，结果如下：

- 如果导入的配置在设备上不存在旧版本，导入将自动完成，且将显示导入成功消息。跳过该步骤的其他部分。
- 如果正在导入的访问控制策略包括安全区域，系统将显示 Access Control Import Resolution 页面。继续进行第 8 步。
- 如果导入的配置在设备上存在旧版本，系统将显示 Import Resolution 页面。继续进行第 9 步。

步骤 8　在每个导入安全区域旁，选择一个类型匹配的现有本地安全区域来进行映射，并点击 **Import**。

返回第 7 步。

步骤 9　展开每项配置并选择适当的选项。

- 要保留设备上的配置，请选择 **Keep existing**。
- 要用已导入的配置替换设备上的配置，请选择 **Replace existing**。
- 要保留最新配置，请选择 **Keep newest**。
- 要将已导入的配置另存为新配置，请选择 **Import as new**，或者，编辑配置名称。

  如果正在导入的访问控制策略包括启用了清空列表或自定义检测列表的文件策略，则 **Import as new** 选项不可用。
- 如果正在导入的访问控制策略或已保存搜索包括一个从属对象，既可接受建议的名称，也可重命名该对象。系统始终将这些从属对象作为新对象导入。无法选择保留或替换现有对象。请注意，对象和对象组在系统中的处理方式相同。

步骤 10　点击 **Import**。

配置导入成功。

从数据库清除发现数据

可以使用 Discovery Data Purge 页面从网络发现和用户发现事件数据库清除文件。请注意，清除数据库时，会重新启动相应的进程。

注意事项 清除数据库会从防御中心中移除指定的数据。删除后，数据**无法**恢复。

要清除网络和用户发现数据库，请执行以下操作：

访问：管理员/任何安全分析师

步骤 1 选择 **System > Tools > Data Purge**。

系统将显示 Data Purge 页面。

步骤 2 在 **Network Discovery** 下，执行以下任一或所有步骤：

- 选择 **Network Discovery Events** 可从数据库移除所有网络发现事件。
- 选择 **Hosts** 可从数据库移除所有主机和危害表现标志。
- 选择 **User Activity** 可从数据库移除所有用户事件。
- 选择 **User Identities** 可从数据库移除所有用户登录和用户历史记录数据。

步骤 3 在 **Connections** 下，执行以下任一或所有步骤：

- 选择 **Connection Events** 可从数据库移除所有连接数据。
- 选择 **Connection Summary Events** 可从数据库移除所有连接摘要数据。
- 选择 **Security Intelligence Events** 可从数据库移除所有安全情报数据。

注 选择 **Connection Events** 不会移除安全情报事件；带有安全情报数据的连接仍将在安全情报事件查看器中显示。相应地，选择 **Security Intelligence Events** 不会移除带有相关安全情报数据的连接事件。

步骤 4 点击 **Purge Selected Events**。

项目清除成功并重新启动相应的进程。

查看长时间运行任务的状态

某些可在 FireSIGHT 系统上执行的任务不会立即完成，而是需要运行一段时间，例如应用策略或安装更新。可在任务队列中检查这些长时间运行任务的进度。任务队列还可以在任务解决成功或失败时报告。

有关详细信息，请参阅：

- 第 C-1 页上的查看任务队列
- 第 C-2 页上的管理任务队列

查看任务队列

许可证：任何环境

执行长时间运行任务时，任务队列会报告这些任务状态，例如应用策略或安装更新。任务队列将提供有关复杂任务的信息并在任务完成时报告。

可在 Task Status 页面中查看任务队列，该页面每 10 秒钟自动刷新一次。可始终查看已启动任务的状态。如果您的用户帐户具备管理员用户角色，或具备启用了**查看其他用户任务**权限的用户角色，则可查每项任务的状态，无论任务启动者如何。有关配置用户角色的详细信息，请参阅第 61-45 页上的配置用户角色。

Job Summary 部分显示页面中列出的任务状态，如下表所述。

表 C-1　　任务队列任务类型

任务类型	说明
正在运行	当前正在进行的任务数。
正在等待	等待进行中任务完成后再运行的任务数。
已完成	成功完成的任务数。
正在重试	正在自动重试的任务数。请注意，并非所有的任务都可以重试。
已停止	由于系统更新而中断的任务数。已停止的任务不能恢复；必须手动将其从任务队列中删除。
失败	未成功完成的任务数。

Jobs 部分显示有关每项任务的信息，包括简要说明、任务启动时间、任务的当前状态，状态上一次发生变化的时间 相同类型的任务，如“网络发现策略应用”，会一起显示在一个任务组中。

为确保 Task Status 页面快速载入， FireSIGHT 系统 从队列中移除时间超过一个月的所有已完成、已失败和已停止的任务，且从包含 1000 多个任务的任何任务组中移除最早的任务，每周一次。还可以从队列中手动移除任务；请参阅管理任务队列了解相关指示。

要查看任务队列，请执行以下操作：

访问：管理员/维护人员/网络管理员/安全审批员/安全分析师

步骤 1　此时您有两种选择：

- 如果手动启动任务，请在启动任务时显示的通知框中点击 **Task Status** 链接。

  系统在弹出窗口中显示 Task Status 页面。

- 如已安排任务，或者，如果任务并非从正在查看的页面启动，请选择 **System > Monitoring > Task Status**。

  系统将显示 Task Status 页面。

有关可在 Task Status 页面执行的操作的信息，请参阅管理任务队列。

管理任务队列

许可证：任何环境

如果已向您的用户帐户分配“管理员”、“维护人员”、“网络管理员”、“安全审批员”或“安全分析师”用户角色，则在查看任务队列时可执行多项操作 （请参阅第 C-1 页上的查看任务队列），如下表所述。

表 C-2　　任务队列操作

要.....	您可以.....
从任务队列中移除所有已完成的任务	点击 **Remove Completed Jobs**。
从任务队列中移除所有已失败的任务	点击 **Remove Failed Jobs**。
从任务队列中移除一个任务	点击要删除的任务旁的删除图标 ( )。 请注意，不能删除正在运行的任务。如果需要删除正在运行的任务 （例如，如果该任务反复失败），请联系支持部门。
折叠任务组并隐藏任务	点击已展开任务组旁的已打开文件夹图标 ( )。
展开任务组并查看任务	点击已折叠任务组旁的已关闭文件夹图标 ( )。

命令行参考

本参考解释适用于 FirePOWER 设备、虚拟设备以及 ASA FirePOWER 设备的 ASA FirePOWER 模块 的命令行界面 (CLI)。您可以使用 CLI 来查看、配置 FireSIGHT 系统，以及对其进行故障排除 FireSIGHT 系统。

注 防御中心、2 系列 设备、用于 Blue Coat X-系列的思科 NGIPS 或 ASA FirePOWER 设备的 ASA 模块不支持命令行界面。

有许多 CLI 模式 （例如 `show` 和 `configure`）包含以模式名称开头的命令集。可进入一个模式，然后在该模式中输入有效命令；也可从任何模式输入完整的命令。例如，要显示有关一个名为 Analyst1 的用户帐户的信息，可在 CLI 提示符处输入以下信息：

```
show user Analyst1
```

如果之前已进入 `show` 模式，请在 CLI 提示符处输入以下信息：

```
user Analyst1
```

在每个模式中，可用于某个用户的命令取决于该用户的 CLI 访问权限。创建用户帐户时，可为其分配以下 CLI 访问级别之一：

- 基本

  用户拥有只读访问权限，不能运行会影响系统性能的命令。

- 配置

  用户拥有读写访问权限，可以运行会影响系统性能的命令。

- 無

  用户无法登录到 SHELL。

在 3 系列设备上，可在网络界面的“用户管理”页面中分配命令行权限；有关详细信息，请参阅 第 61-1 页上的管理用户。在虚拟设备和 ASA FirePOWER 设备上，可通过 CLI 本身分配命令行权限。

注 如果重新启动 3 系列设备后尽快登录 CLI，则所执行的任何命令均不记录在审核日志中，直至网络界面可用。

请注意， CLI 命令不区分大小写，但其文本不是 CLI 框架一部分的参数除外，例如用户名和搜索过滤器。

有关登录命令行的信息，请参阅 第 2-1 页上的登录设备。

以下各节介绍 CLI 命令：

基本 CLI 命令

基本 CLI 命令可用于与 CLI 交互。这些命令不影响设备的运行。基本命令可供所有 CLI 用户使用。

以下各节介绍基本命令：

configure password

允许当前用户更改其密码。发出命令后， CLI 会提示用户其当前 （或旧）密码，然后提示用户输入新密码两次。

接入

基本

语法

```
configure password
```

示例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

end

使用户返回到默认模式。（将用户从任何较低级别的 CLI 上下文向上移至默认模式。）

接入

基本

语法

```
end
```

示例

```
configure network ipv4> end
>
```

exit

将 CLI 上下文上移至下一个最高级别的 CLI 上下文。从默认模式发出此命令会使用户注销当前 CLI 会话，这相当于发出 `logout` CLI 命令。

接入

基本

语法

```
exit
```

示例

```
configure network ipv4> exit
configure network>
```

帮助

显示 CLI 语法的概述。

接入

基本

语法

```
帮助
```

示例

```
> help
```

历史

显示当前会话的命令行历史记录。

接入

基本

语法

```
history limit
```

其中，*`limit`* 设置历史记录列表的大小。要将大小设置为无限，请输入零。

示例

```
history 25
```

logout

使当前用户注销当前 CLI 控制台会话。

接入
基本

语法
```
logout
```

示例
```
> logout
```

? （问号）

为 CLI 命令和参数显示上下文相关帮助。按照以下说明使用问号 (?)：

- 要为当前 CLI 上下文中可用的命令显示帮助，请在命令提示符处输入问号 (?)。
- 要显示以特定字符集开头的可用命令的列表，请输入缩写命令，再紧接着输入问号 (?)。
- 要为命令的合法变元显示帮助，请在命令提示符处输入问号 (?) 代替变元。

请注意，问号 (?) 不会回送到控制台。

接入
基本

语法
```
?
abbreviated_command ?
command [arguments] ?
```

示例
```
> ?
```

??(double question marks)

为 CLI 命令和参数显示详细的上下文相关帮助。

接入
基本

语法
```
??
abbreviated_command end??
command [arguments] ??
```

示例
```
> configure manager add ??
```

显示命令

显示命令提供有关设备状态的信息。这些命令不会改变设备的操作模式，运行这些命令对系统运行的影响极小。大多数显示命令可供所有 CLI 用户使用；但是，只有拥有配置 CLI 权限的用户才能发出 `show user` 命令。

以下各节介绍显示命令：

access-control-config

显示当前应用的访问控制配置，包括：安全情报设置；引用的 SSL 的名称、网络分析、入侵和文件策略名称；入侵变量集数据；日志记录设置；以及其他高级设置，包括政策级别性能、预处理和常规设置。

还显示策略相关的连接信息，例如源端口和目标端口数据 （包括 ICMP 条目的类型和代码）以及与每条访问控制规则匹配的连接数 （命中次数）。

接入

基本

语法

```
show access-control-config
```

示例

```
> show access-control-config
```

alarms

显示设备上当前活动的 （故障/停机）硬件报警。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
基本

语法
```
show alarms
```

示例
```
> show alarms
```

arp-tables

显示适用于您网络的地址解析协议表。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
基本

语法
```
show arp-tables
```

示例
```
> show arp-tables
```

audit-log

按时间倒序显示审核日志；首先列出最近的审核日志事件。

接入
基本

语法
```
show audit-log
```

示例
```
> show audit-log
```

bypass

列出使用中的内联集并显示这些内联集的旁路模式状态 （常规或旁路）。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
基本

语法

```
show bypass
```

示例

```
> show bypass
```

集群

显示有关设备集群配置、状态和成员堆栈的信息。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入

基本

config

显示设备的集群配置。

语法

```
show clustering config
```

示例

```
> show clustering config
```

clustering ha-statistics

显示集群中设备的状态共享统计信息。

语法

```
show clustering ha-statistics
```

示例

```
> show clustering ha-statistics
```

cpu

显示适合用于设备上所有 CPU 的平台的当前 CPU 使用情况统计信息。对于受管设备，会显示以下值：

- CPU

  处理器编号。

- 负载线

  CPU 利用率，用 0 至 100 之间的任意数字表示。 0 表示空负载， 100 表示满负载。

对于虚拟设备和 ASA FirePOWER 设备，会显示以下值：

- CPU

  处理器编号。

- %user

  在用户级别 （应用）执行时发生的 CPU 利用率。
- %nice

  在具有 nice 优先级的用户级别执行时发生的 CPU 利用率。
- %sys

  在系统级别 （内核）执行时发生的 CPU 利用率。这不包括中断或软件中断修复时间。 softirq （软件中断）是可以同时在多个 CPU 上运行的 32 个枚举软件中断之一。
- %iowait

  当系统有未处理的磁盘 I/O 请求时 CPU 空闲时间的百分比。
- %irq

  CPU 修复中断所用时间的百分比。
- %soft

  CPU 修复软件中断所用时间的百分比。
- %steal

  当虚拟机监控程序为其他虚拟处理器提供服务时，虚拟 CPU 被强制等待时间的百分比。
- %guest

  CPU 运行虚拟处理器所用时间的百分比。
- %idle

  当系统没有未处理的磁盘 I/O 请求时 CPU 空闲时间的百分比。

接入

基本

语法

```
show cpu [procnum]
```

其中， *procnum* 是您想要显示其利用情况信息的处理器的编号。有效值为 0 至比系统的处理器总数小 1 的数值。如果 *procnum* 用于受管设备，它将被忽略，因为对于该平台，只能为所有处理器显示利用情况信息。

示例

```
> show cpu
```

database

`show database` 命令配置设备的管理接口。

接入

基本

processes

显示运行中数据库查询的列表。

接入
基本

语法
```
show database processes
```

示例
```
> show database processes
```

slow-query-log

显示数据库的慢查询日志。

接入
基本

语法
```
show database slow-query-log
```

示例
```
> show database slow-query-log
```

device-settings

显示有关当前设备专用应用旁路设置的信息。

接入
基本

语法
```
show device-settings
```

示例
```
> show device-settings
```

disk

显示当前磁盘使用情况。

接入
基本

语法
```
show disk
```

示例

```
> show disk
```

disk-manager

显示系统每个部分（包括竖井、低水位线和高水位线）的磁盘使用情况详细信息。

接入

基本

语法

```
show disk-manager
```

示例

```
> show disk-manager
```

dns

显示当前 DNS 服务器地址和搜索域。

接入

基本

语法

```
show dns
```

示例

```
> show dns
```

expert

调用 SHELL。

接入

基本

语法

```
expert
```

示例

```
> expert
```

fan-status

显示硬件风扇的当前状态。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
基本

语法
```
show fan-status
```

示例
```
> show fan-status
```

fastpath-rules

显示当前配置的快速路径规则。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
基本

语法
```
show fastpath-rules
```

示例
```
> show fastpath-rules
```

gui

显示网络界面的当前状态。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
基本

语法
```
show gui
```

示例
```
> show gui
```

主机名

显示设备的主机名和设备 UUID。如果使用 CLI 编辑设备的主机名，请确认在管理防御中心上反映更改。在某些情况下，您可能需要手动编辑设备管理设置。有关详细信息，请参阅第 4-46 页上的编辑设备管理设置。

接入
基本

语法

```
show hostname
```

示例

```
> show hostname
```

主机

显示 ASA FirePOWER 模块的 /etc/hosts 文件的内容。

接入

基本

语法

```
show hosts
```

示例

```
> show hosts
```

hyperthreading

显示超线程是处于启用状态还是禁用状态。此命令不适用于 ASA FirePOWER 设备。

接入

基本

语法

```
show hyperthreading
```

示例

```
> show hyperthreading
```

inline-sets

显示所有内联安全区域和关联接口的配置数据。此命令不适用于 ASA FirePOWER 设备。

接入

基本

语法

```
show inline-sets
```

示例

```
> show inline-sets
```

接口

如未指定参数，将显示所有已配置接口的列表。如已指定参数，将显示有关指定接口的详细信息。

接入
基本

语法
```
show interfaces [interface]
```
其中， *interface* 是想要获得其详细信息的特定接口。

示例
```
> show interfaces
```

ifconfig

显示适用于 ASA FirePOWER 模块的接口配置。

接入
基本

语法
```
show ifconfig
```

示例
```
> show ifconfig
```

lcd

显示 LCD 硬件显示器是处于启用状态还是禁用状态。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
基本

语法
```
show lcd
```

示例
```
> show lcd
```

link-aggregation

`show link-aggregation` 命令显示链路聚合组 (LAG) 的配置和统计信息。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
基本

configuration

为所配置的每个 LAG 显示配置详情，包括 LAG ID、接口数量，配置模式、负载平衡模式、LACP 信息和物理接口类型。

接入
基本

语法
```
show link-aggregation configuration
```

示例
```
> show link-aggregation configuration
```

statistics

按照接口为所配置的每个 LAG 显示统计信息，包括状态、链路状态和速度、配置模式、已接收和已传输数据包的计数器以及已接收和已传输字节的计数器。

接入
基本

语法
```
show link-aggregation statistics
```

示例
```
> show link-aggregation statistics
```

link-state

显示设备端口的类型、链路、速度、双工状态和旁路模式。此命令不适用于 ASA FirePOWER 设备。

接入
基本

语法
```
show link-state
```

示例
```
> show link-state
```

log-ips-connection

显示与记录的入侵事件相关联的连接事件日志记录是处于启用状态还是禁用状态。

接入
基本

语法
```
show log-ips-connection
```

示例
```
> show log-ips-connection
```

managers

显示 防御中心 的配置和通信状态。仅在注册处于待处理状态时，才会显示注册密钥和 NAT ID。如果设备已注册到高可用性对，将会同时显示有关两个管理 防御中心 的信息。如果设备被配置为堆叠配置中的次要设备，将会同时显示有关管理 防御中心 和主设备的信息。

接入
基本

语法
```
show managers
```

示例
```
> show managers
```

memory

显示设备的总内存、使用中内存和可用内存。

接入
基本

语法
```
show memory
```

示例
```
> show memory
```

型号

显示设备的型号信息。

接入
基本

语法

```
show model
```

示例

```
> show model
```

mpls-depth

显示在管理接口上配置的 MPLS 层的数量，有效值为 0 至 6。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入

基本

语法

```
show mpls-depth
```

示例

```
> show mpls-depth
```

NAT

`show nat` 命令显示管理接口的 NAT 数据和配置信息。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入

基本

active-dynamic

显示根据动态规则转换的 NAT 流量。当有流量与规则匹配时，这些条目会显示，直至相匹配的规则超时。因此，该列表可能不准确。超时取决于协议：ICMP 为 5 秒，UDP 为 120 秒，TCP 为 3600 秒，所有其他协议均为 60 秒。

语法

```
show nat active-dynamic
```

示例

```
> show nat active-dynamic
```

active-static

显示根据静态规则转换的 NAT 流量。一旦对设备应用规则，这些条目就会显示；该列表不会指明与静态 NAT 规则匹配的活动流量。

语法

```
show nat active-static
```

示例

```
> show nat active-static
```

allocators

为所有 NAT 分配器 （动态规则使用的转换后地址池）显示信息。

语法

```
show nat allocators
```

示例

```
> show nat allocators
```

config

显示管理接口的当前 NAT 策略配置。

语法

```
show nat config
```

示例

```
> show nat config
```

dynamic-rules

显示使用指定的分配器 ID 的动态 NAT 规则。

语法

```
show nat dynamic-rules allocator_id
```

示例

```
> show nat dynamic-rules 9
```

其中， *allocator_id* 是有效的分配器 ID 号。

flows

显示使用指定的分配器 ID 的规则的流数量。

语法

```
show nat flows allocator-id
```

示例

```
> show nat flows 81
```

其中， *allocator_id* 是有效的分配器 ID 号。

static-rules

显示所有静态 NAT 规则。

语法

```
show nat static-rules
```

示例

```
> show nat static-rules
```

netstat

显示 ASA FirePOWER 模块的活动网络连接。

接入

基本

语法

```
show netstat
```

示例

```
> show netstat
```

网络

显示管理接口、管理接口的 MAC 地址、HTTP 代理地址、端口和用户名（如已配置）的 IPv4 和 IPv6 配置。

接入

基本

语法

```
show network
```

示例

```
> show network
```

network-modules

显示所有已安装的模块及其信息 （包括序列号）。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入

基本

语法

```
show network-modules
```

示例

```
> show network-modules
```

network-static-routes

显示所有已配置的网络静态路由及其相关信息，包括接口、目标地址、网络掩码和网关地址。

接入

基本

语法

```
show network-static-routes
```

示例

```
> show network-static-routes
```

ntp

显示 ntp 配置。

接入

基本

语法

```
show ntp
```

示例

```
> show ntp
```

perfstats

显示设备的性能统计信息。

接入

基本

语法

```
show perfstats
```

示例

```
> show perfstats
```

portstats

显示安装在设备上的所有端口的统计信息。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
基本

语法
```
show portstats [copper | fiber | internal | external | all]
```
其中，`copper` 表示所有铜端口，fiber 表示所有光纤端口，internal 表示所有内部端口，external 表示所有外部端口 （铜端口和光纤端口）， all 表示所有端口 （外部端口和内部端口）。

示例
```
> show portstats fiber
```

power-supply-status

显示硬件电源的当前状态。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
基本

语法
```
show power-supply-status
```

示例
```
> show power-supply-status
```

process-tree

显示当前正在设备上运行的进程，按类型以树格式排序。

接入
基本

语法
```
show process-tree
```

示例
```
> show process-tree
```

processes

显示当前正在设备上运行的进程，按 CPU 使用情况降序排序。

接入
基本

语法

```
show processes [sort-flag] [filter]
```

其中，`sort-flag` 可以是 `-m`，表示按内存（降序）排序；可以是 `-u`，表示按用户名而非进程名称进行排序；也可以是 `verbose`，表示将会显示命令的全名和路径。*`filter`* 参数指定命令或用户名中作为过滤依据的搜索条件。标题行仍然显示。

示例

```
> show processes -u user1
```

route

显示 ASA FirePOWER 模块的路由信息。

接入

基本

语法

```
show route
```

示例

```
> show route
```

routing-table

如未指定参数，将会显示所有虚拟路由器的路由信息。如已指定参数，将会显示指定路由器的路由信息以及该路由器的指定路由协议类型（如适用）。所有参数均为可选。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入

基本

语法

```
show routing-table [name] [ ospf | rip | static ]
```

其中，*`name`* 是要获得其信息的特定路由器的名称，`ospf`、`rip` 和 `static` 指定路由协议类型。

示例

```
> show routing-table Vrouter1 static
```

serial-number

显示机箱序列号。此命令不适用于虚拟设备。

接入

基本

语法

```
show serial-number
```

示例

```
> show serial-number
```

ssl-policy-config

显示当前应用的 SSL 策略配置，包括策略说明、默认日志记录设置、所有已启用的 SSL 规则和规则配置、受信任 CA 证书以及无法解密的流量操作。

接入

基本

语法

```
show ssl-policy-config
```

示例

```
> show ssl-policy-config
```

堆叠

显示受管设备上的堆叠配置和位置；在配置为主设备的设备上，也列出所有次要设备的数据。对于集群堆栈，此命令还指明堆栈是集群成员。用户必须使用网络界面来启用或（在大多数情况下）禁用堆叠；如未启用堆叠，此命令将返回 `Stacking not currently configured`。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入

基本

语法

```
show stacking
```

示例

```
> show stacking
```

小结

显示有关设备的最常用信息（版本、类型、 UUID 等）的摘要。有关更多详细信息，请参阅下面的 `show` 命令：第 D-25 页上的位置、第 D-14 页上的接口、第 D-10 页上的 device-settings 和第 D-6 页上的 access-control-config。

接入

基本

语法

```
show summary
```

示例

```
> show summary
```

时间

以协调世界时 (UTC) 以及为当前用户配置的本地时区显示当前日期和时间。

接入
基本

语法
```
show time
```

示例
```
> show time
```

traffic-statistics

如未指定参数，将显示有关通过所有端口传输和接收的字节的详细信息。如已指定端口，则仅为指定端口显示该信息。不能为 ASA FirePOWER 设备指定端口，系统仅显示数据平面接口。

接入
基本

语法
```
show traffic-statistics [port]
```
其中，`port` 是想要获得其信息的特定端口。

示例
```
> show traffic-statistics s1p1
```

用户

仅适用于虚拟设备。显示指定用户的详细配置信息。会显示以下值：

- 登录 - 登录名
- UID - 数字用户 ID
- 身份验证 （`Local` 或 `Remote`） - 如何对用户进行身份验证
- 访问权限 （`Basic` 或 `Config`） - 用户的权限级别
- 已启用 （`Enabled` 或 `Disabled`） - 用户是否处于活动状态
- 重置 （`Yes` 或 `No`） - 用户下次登录时是否必须更改密码
- 到期 （`Never` 或一个数字） - 还剩下多少天必须更改用户密码
- 警告 （`N/A` 或一个数字） - 在密码到期前允许用户更改密码的天数
- 强度 （`Yes` 或 `No`） - 用户密码是否符合强度检查标准
- 锁定 （`Yes` 或 `No`） - 用户帐户是否因登录失败太多次而被锁定
- 最大 （`N/A` 或一个数字） - 用户帐户被锁定前允许的最多登录失败次数

接入
配置

语法
```
show user username username username ...
```
其中，*username* 指定用户的名称；用户名以空格分隔。

示例
```
> show user jdoe
```

用户

仅适用于虚拟设备。显示所有本地用户的详细配置信息。会显示以下值：

- 登录 - 登录名
- UID - 数字用户 ID
- 身份验证 （Local 或 Remote） - 如何对用户进行身份验证
- 访问权限 （Basic 或 Config） - 用户的权限级别
- 已启用 （Enabled 或 Disabled） - 用户是否处于活动状态
- 重置 （Yes 或 No） - 用户下次登录时是否必须更改密码
- 到期 （Never 或一个数字） - 还剩下多少天必须更改用户密码
- 警告 （N/A 或一个数字） - 在密码到期前允许用户更改密码的天数
- 强度 （Yes 或 No） - 用户密码是否符合强度检查标准
- 锁定 （Yes 或 No） - 用户帐户是否因登录失败太多次而被锁定
- 最大 （N/A 或一个数字） - 用户帐户被锁定前允许的最多登录失败次数

接入
配置

语法
```
show users
```

示例
```
> show users
```

位置

显示产品的版本和内部版本。如已指定 *detail* 参数，将会显示附加组件的版本。

接入
基本

语法
```
show version [detail]
```

示例

```
> show version
```

virtual-routers

如未指定参数，将会显示当前已配置的所有带有 DHCP 中继、 OSPF 和 RIP 信息的虚拟路由器的列表。如已指定参数，将会显示指定路由器 （受指定路由类型的限制）的信息。所有参数均为可选。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入

基本

语法

```
show virtual-routers [ dhcprelay | ospf | rip ] [name]
```

其中， `dhcprelay`、 `ospf` 和 `rip` 指定路由类型， *name* 是想要获得其信息的特定路由器的名称。如果指定 `ospf`，则可进一步在路由类型与路由器名称 （如存在）之间指定 `neighbors`、 `topology` 或 `lsadb`。

示例

```
> show virtual-routers ospf VRouter2
```

virtual-switches

如未指定参数，将显示当前已配置的所有交换机的列表。如已指定参数，将显示指定交换机的信息。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入

基本

语法

```
show virtual-switches [name]
```

示例

```
> show virtual-switches Vswitch1
```

vmware-tools

指明 VMware 工具当前在虚拟设备上是否已启用。此命令仅适用于虚拟设备。

VMware 工具是专用于提高虚拟机性能的一套实用工具。通过这些实用工具，您可以充分利用 VMware 产品方便的功能。该系统在所有虚拟设备上均支持以下插件：

- guestInfo
- powerOps
- timeSync
- vmbackup

有关 VMware 工具以及受支持插件的详细信息，请访问 VMware 网站 (http://www.vmware.com)。

接入
基本

语法
```
show vmware-tools
```

示例
```
> show vmware-tools
```

VPN

`show VPN` 命令显示 VPN 连接的 VPN 状态和配置信息。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
基本

config

显示所有 VPN 连接的配置。

语法
```
show vpn config
```

示例
```
> show vpn config
```

config by virtual router

显示适用于虚拟路由器的所有 VPN 连接的配置。

语法
```
show vpn config [virtual router]
```

示例
```
> show vpn config VRouter1
```

状态

显示所有 VPN 连接的状态。

语法
```
show vpn status
```

示例
```
> show vpn status
```

status by virtual router

显示适用于虚拟路由器的所有 VPN 连接的状态。

语法

```
show vpn status [virtual router]
```

示例

```
> show vpn status VRouter1
```

counters

显示所有 VPN 连接的计数器。

语法

```
show vpn counters
```

示例

```
> show vpn counters
```

counters by virtual router

显示适用于虚拟路由器的所有 VPN 连接的计数器。

语法

```
show vpn counters [virtual router]
```

示例

```
> show vpn counters VRouter1
```

配置命令

配置命令可供用户配置和管理系统。这些命令会影响系统运行；因此，除了基本级别的 `configure password` 外，只有拥有配置 CLI 访问权限的用户才能发出这些命令。

以下各节介绍配置命令：

集群

为设备上的集群禁用或配置旁路。此命令不适用于虚拟设备、 ASA FirePOWER 设备和被配置为次要堆栈成员的设备。

接入
配置

语法
```
configure clustering {disable | bypass}
```

示例
```
> configure clustering disable
```

bypass

打开或关闭内联对的旁路模式。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
配置

语法
```
configure bypass {open | close} {interface}
```
其中， *interface* 是内联对中任何一个硬件端口的名称。

示例
```
> configure bypass open s1p1
```

gui

启用或禁用设备网络界面，包括在系统主要更新期间出现的简化升级网络界面。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
配置

语法
```
configure gui {enable | disable}
```

示例
```
> configure gui disable
```

lcd

启用或禁用设备正面的 LCD 显示器。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
配置

语法
```
configure lcd {enable | disable}
```

示例
```
> configure lcd disable
```

log-ips-connections

启用或禁用与记录的入侵事件关联的连接事件日志记录。

接入
配置

语法
```
configure log-ips-connections {enable | disable}
```

示例
```
> configure log-ips-connections disable
```

管理器

`configure manager` 命令配置设备与其管理 防御中心 之间的连接。

接入
配置

add

将设备配置为接受来自管理防御中心的连接。此命令仅在设备并非处于主动托管状态时才起作用。

向 防御中心注册设备始终需要一个唯一的字母数字注册密钥。在大多数情况下，必须随注册密钥一起提供主机名或 IP 地址。但是，如有 NAT 设备将设备与 防御中心 分开，则必须随注册密钥一起输入唯一 NAT ID，并指定 DONTRESOLVE 而非主机名。

语法
```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey
[nat_id]
```
其中，{*hostname* | *IPv4_address* | *IPv6_address* | DONTRESOLVE} 指定管理此设备的 防御中心 的 DNS 主机名或 IP 地址（IPv4 或 IPv6）。如果 防御中心 无法直接寻址，请使用 DONTRESOLVE 。如果使用 DONTRESOLVE，则需要指定 *nat_id*。*regkey* 是向 防御中心 注册设备所需的唯一字母数字注册密钥。*nat_id* 是在 防御中心与设备之间的注册期间使用的可选字母数字字符串。如果主机名设置为 DONTRESOLVE，则需要此参数。

示例

```
> configure manager add DONTRESOLVE abc123 efg456
```

删除

从设备移除 防御中心 的连接信息。此命令仅在设备并非处于主动托管状态时才起作用。

语法

```
configure manager delete
```

示例

```
> configure manager delete
```

mpls-depth

在管理接口上配置 MPLS 层的数量。此命令不适用于虚拟设备和 ASA FirePOWER 设备。

接入
配置

语法

```
configure mpls-depth {depth}
```
其中，*depth* 是 0 至 6 之间的任意数字。

示例

```
> configure mpls-depth 3
```

网络

`configure network` 命令配置设备的管理接口。

接入
配置

dns searchdomains

用在命令中指定的列表替换当前的 DNS 搜索域列表。

语法

```
configure network dns searchdomains {searchlist}
```
其中，*searchlist* 是以逗号分隔的域列表。

示例

```
> configure network dns searchdomains foo.bar.com,bar.com
```

dns servers

用在命令中指定的列表替换当前的 DNS 服务器列表。

语法

```
configure nework dns servers {dnslist}
```

其中， *dnslist* 是以逗号分隔的 DNS 服务器列表。

示例

```
> configure network dns servers 10.123.1.10,10.124.1.10
```

主机名

设置设备的主机名。

语法

```
configure network hostname {name}
```

其中， *name* 是新主机名。

示例

```
> configure network hostname sfrocks
```

http-proxy

在 3 系列 和虚拟设备上，配置 HTTP 代理。发出命令后， CLI 会提示用户 HTTP 代理地址和端口，是否需要进行代理身份验证，如果需要，还会提示代理用户名、代理密码和代理密码确认。

可在虚拟设备上使用此命令配置 HTTP 代理服务器，以便虚拟设备将文件提交给综合安全智能云进行动态分析。

语法

```
configure network http-proxy
```

示例

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address:
Enter HTTP Proxy Port:
Use Proxy Authentication?(y/n) [n]:
Enter Proxy Username:
Enter Proxy Password:
Confirm Proxy Password:
```

http-proxy-disable

在 3 系列 和虚拟设备上，删除任何 HTTP 代理配置。

语法

```
configure network http-proxy-disable
```

示例

```
> configure network http-proxy-disable
Are you sure that you wish to delete the current http-proxy configuration?(y/n):
```

ipv4 delete

禁用设备管理接口的 IPv4 配置。

语法

```
configure network ipv4 delete
```

示例

```
> configure network ipv4 delete
```

ipv4 dhcp

将设备管理接口的 IPv4 配置设置为 DHCP。管理接口与 DHCP 服务器通信以获取其配置信息。

语法

```
configure network ipv4 dhcp
```

示例

```
> configure network ipv4 dhcp
```

ipv4 manual

手动配置设备管理接口的 IPv4 配置。

语法

```
configure network ipv4 manual ipaddr netmask gw
```

其中， *ipaddr* 是 IP 地址， *netmask* 是子网掩码， *gw* 是默认网关的 IPv4 地址。

示例

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

ipv6 delete

禁用设备管理接口的 IPv6 配置。

语法

```
configure network ipv6 delete
```

示例

```
> configure network ipv6 delete
```

ipv6 dhcp

将设备管理接口的 IPv6 配置设置为 DHCP。管理接口与 DHCP 服务器通信以获取其配置信息。

语法

```
configure network ipv6 dhcp
```

示例

```
> configure network ipv6 dhcp
```

ipv6 router

将设备管理接口的 IPv6 配置设置为“路由器”。管理接口与 IPv6 路由器通信以获取其配置信息。

语法

```
configure network ipv6 router
```

示例

```
> configure network ipv6 router
```

ipv6 manual

手动配置设的管理接口的 IPv6 配置。

语法

```
configure network ipv6 manual ip6addr/ip6prefix [ip6gw]
```

其中， *ip6addr/ip6prefix* 是 IP 地址和前缀长度， ip6*gw* 是默认网关的 IPv6 地址。

示例

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

management-interface disable

禁用指定的管理接口。

语法

```
configure network management-interface disable ethn
```

其中 *n* 是要禁用的管理接口的数量。

示例

```
> configure network management-interface disable eth1
```

management-interface disable-event-channel

禁用通过指定的管理接口进行的事件传输。

语法

```
configure network management-interface disable-event-channel ethn
```

其中 *n* 是要禁用的管理接口的数量。

示例

```
> configure network management-interface disable-event-channel eth1
```

management-interface disable-management-channel

禁用通过指定的管理接口进行的管理传输。

语法

```
configure network management-interface disable-management-channel ethn
```

其中 *n* 是要禁用的管理接口的数量。

示例

```
> configure network management-interface disable-management-channel eth1
```

management-interface enable

启用指定的管理接口。

语法

```
configure network management-interface enable ethn
```

其中 *n* 是要启用的管理接口的数量。

示例

```
> configure network management-interface enable eth1
```

management-interface enable-event-channel

启用通过指定的管理接口进行的事件传输。

语法

```
configure network management-interface enable-event-channel ethn
```

其中 *n* 是要启用的管理接口的数量。

示例

```
> configure network management-interface enable-event-channel eth1
```

management-interface enable-management-channel

启用通过指定的管理接口进行的管理传输。

语法

```
configure network management-interface enable-management-channel ethn
```

其中 *n* 是要启用的管理接口的数量。

示例

```
> configure network management-interface enable-management-channel eth1
```

management-interface tcpport

更改用于管理的 TCP 端口的值。

语法

```
configure network management-interface tcpport port
```

其中，*port* 是您想要配置的管理端口值。

示例

```
> configure network management-interface tcpport 8500
```

management-port

设置设备 TCP 管理端口的值。

语法

```
configure network management-port number
```

其中， *number* 是要配置的管理端口值。

示例

```
> configure network management-port 8500
```

static-routes ipv4 add

为指定的管理接口添加 IPv4 静态路由。

语法

```
configure network static-routes ipv4 add interface destination netmask gateway
```

其中 *interface* 是管理接口，*destination* 是目标 IP 地址，*netmask* 是网络掩码地址，*gateway* 是您想要添加的网关地址。

示例

```
> configure network static-routes ipv4 add eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv4 delete

为指定的管理接口删除 IPv4 静态路由。

语法

```
configure network static-routes ipv4 delete interface destination netmask gateway
```

其中 *interface* 是管理接口，*destination* 是目标 IP 地址，*netmask* 是网络掩码地址，*gateway* 是您想要删除的网关地址。

示例

```
> configure network static-routes ipv4 delete eth1 10.115.24.0 255.255.255.0
10.115.9.2
```

static-routes ipv6 add

为指定的管理接口添加 IPv6 静态路由。

语法

```
configure network static-routes ipv6 add interface destination prefix gateway
```

其中 *interface* 是管理接口，*destination* 是目标 IP 地址，*prefix* 是 IPv6 前缀长度，*gateway* 是您想要添加的网关地址。

示例

```
> configure network static-routes ipv6 add eth1 2001:DB8:3ffe:1900:4545:3:200:
f8ff:fe21:67cf 64
```

static-routes ipv6 delete

为指定的管理接口删除 IPv6 静态路由。

语法

```
configure network static-routes ipv6 delete interface destination prefix gateway
```

其中 *interface* 是管理接口，*destination* 是目标 IP 地址，*prefix* 是 IPv6 前缀长度，*gateway* 是您想要删除的网关地址。

示例

```
> configure network static-routes ipv6 delete eth1 2001:DB8:3ffe:1900:4545:3:200:f8ff:
fe21:67cf 64
```

密码

允许当前用户更改其密码。发出命令后， CLI 会提示用户其当前 （或旧）密码，然后提示用户输入新密码两次。

接入

基本

语法

```
configure password
```

示例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

stacking disable

在受管设备上，移除设备上存在的任何堆叠配置：在配置为主设备的设备上，会完全移除堆栈；在配置为次要设备的设备上，会将该设备从堆栈中移除。此命令不适用于虚拟设备或 ASA FirePOWER 设备，不能用于断开集群堆栈。

无法与堆叠层次结构中较高级别的设备建立通信时，可使用此命令。如果 防御中心 可用于通信，会显示一条消息，提示您换用 防御中心 网络界面；同样，如在主设备可用时在配置为次要设备的设备上输入 `stacking disable`，将会显示一条消息，提示您从主设备输入该命令。

接入

配置

语法

```
configure stacking disable
```

示例

```
> configure stacking disable
```

用户

configure user 命令仅适用于虚拟设备，用于管理设备的本地用户数据库。

接入
配置

接入
修改指定用户的访问级别。此命令在指定用户下次登录时生效。

语法

```
configure user access username [basic | config]
```

示例

```
> configure user access jdoe basic
```

其中，*username* 指定您想要为其修改访问权限的用户的名称，basic 指明基本访问权限，config 指明配置访问权限。

add

创建具有指定名称和访问级别的新用户。此命令提示输入用户密码。

语法

```
configure user add username [basic | config]
```

其中，*username* 指定新用户的名称，basic 指明基本访问权限，config 指明配置访问权限。

示例

```
> configure user add jdoe basic
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

aging

强制用户密码到期。

语法

```
configure user aging username max_days warn_days
```

其中，*username* 指定用户的名称，*max_days* 指明密码有效的最大天数，*warn_days* 指明密码到期前允许用户更改密码的天数。

示例

```
> configure user aging jdoe 100 3
```

删除

删除用户及其主目录。

语法

```
configure user delete username
```

其中，*username* 指定用户的名称。

示例

```
> configure user delete jdoe
```

禁用

禁用用户。被禁用的用户将无法登录。

语法

```
configure user disable username
```

其中，*username* 指定用户的名称。

示例

```
> configure user disable jdoe
```

enable

启用用户。

语法

```
configure user enable username
```

其中，*username* 指定用户的名称。

示例

```
> configure user enable jdoe
```

forcereset

强制用户在下次登录时更改密码。当用户登录并更改密码时，会自动启用强度检查。

语法

```
configure user forcereset username
```

其中，*username* 指定用户的名称。

示例

```
> configure user forcereset jdoe
```

maxfailedlogins

为指定用户设置最多登录失败次数。

语法

```
configure user maxfailedlogins username number
```

其中，*username* 指定用户的名称，*number* 指定最多登录失败次数。

示例

```
> configure user maxfailedlogins jdoe 3
```

密码

设置用户密码。此命令提示输入用户密码。

语法

```
configure user password username
```

其中， *username* 指定用户的名称。

示例

```
> configure user pasword jdoe
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

strengthcheck

启用或禁用针对用户密码的强度要求。当用户密码到期时，或者使用了 configure user forcereset 命令，此要求会在用户下次登录时自动启用。

语法

```
configure user strengthcheck username {enable | disable}
```

其中， *username* 指定用户的名称， `enable` 设置针对指定用户密码的要求， `disable` 移除针对指定用户密码的要求。

示例

```
> configure user strengthcheck jdoe enable
```

解锁

解锁超过最多登录失败次数的用户。

语法

```
configure user unlock username
```

其中， *username* 指定用户的名称。

示例

```
> configure user unlock jdoe
```

vmware-tools

在虚拟设备上启用或禁用 VMware 工具。此命令仅适用于虚拟设备。

VMware 工具是专用于提高虚拟机性能的一套实用工具。通过这些实用工具，您可以充分利用 VMware 产品方便的功能。该系统在所有虚拟设备上均支持以下插件：

- guestInfo
- powerOps
- timeSync
- vmbackup

有关 VMware 工具以及受支持插件的详细信息，请访问 VMware 网站 (http://www.vmware.com)。

接入
基本

语法
```
configure vmware-tools (enable | disable)
```

示例
```
> configure vmware-tools enable
```

系统命令

系统命令可供用户管理整个系统的文件以及访问控制设置。只有拥有配置 CLI 访问权限的用户才能在系统模式中发出命令。

以下各节介绍系统命令：

access-control

`system access-control` 命令可供用户管理设备上的访问控制配置。

接入
配置

archive

将当前应用的访问控制策略作为文本文件另存在 `/var/common`。

语法
```
system access-control archive
```

示例
```
> system access-control archive
```

clear-rule-counts

将访问控制规则命中次数重置为 0。

语法

```
system access-control clear-rule-counts
```

示例

```
> system access-control clear-rule-counts
```

rollback

将系统恢复为之前应用的访问控制配置。此命令不适用于集群设备或堆叠设备。

语法

```
system access-control rollback
```

示例

```
> system access-control rollback
```

disable-http-user-cert

移除系统中存在的所有 HTTP 用户认证。

接入
配置

语法

```
system disable-http-user-cert
```

示例

```
> system disable-http-user-cert
```

file

`system file` 命令可供用户管理设备上公共目录中的文件。

接入
配置

copy

使用 FTP 将文件传输至使用登录用户名的主机上的某个远程位置。本地文件必须位于公共目录中。

语法

```
system file copy hostname username path filenames filenames ...
```

其中，*hostname* 指定目标远程主机的名称或 IP 地址，*username* 指定远程主机上用户的名称，*path* 指定远程主机上的目标路径，*filenames* 指定要传输的本地文件；文件名以空格分隔。

示例

```
> system file copy sfrocks jdoe /pub *
```

删除

从公共目录中移除指定文件。

语法

```
system file delete filenames filenames ...
```

其中，*filenames* 指定要删除的文件；文件名以空格分隔。

示例

```
> system file delete *
```

list

如未指定文件名，将显示公共目录中所有文件的修改时间、大小和文件名。如已指定文件名，将显示与指定文件名匹配的文件的修改时间、大小和文件名。

语法

```
system file list {filenames filenames ...}
```

其中，filenames 指定要显示的文件；文件名以空格分隔。

示例

```
> system file list
```

secure-copy

使用 SCP 将文件传输至使用登录用户名的主机上的某个远程位置。本地文件必须位于 /var/common 目录中。

语法

```
system file secure-copy hostname username path filenames filenames ...
```

其中，*hostname* 指定目标远程主机的名称或 IP 地址，*username* 指定远程主机上用户的名称，*path* 指定远程主机上的目标路径，*filenames* 指定要传输的本地文件；文件名以空格分隔。

示例

```
> system file secure-copy 10.123.31.1 jdoe /tmp *
```

generate-troubleshoot

生成故障排除数据供 思科 分析。

接入

配置

语法

```
system generate-troubleshoot
```

此语法显示可选参数列表以指定应显示哪些故障排除数据。

示例

```
> system generate-troubleshoot
```

ldapsearch

使用户对指定 LDAP 服务器执行查询。请注意，所有参数均为必需。

接入

配置

语法

```
system ldapsearch host port baseDN userDN basefilter
```

其中，*host* 指定 LDAP 服务器域，*port* 指定 LDAP 服务器端口，*baseDN* 指定要在其中进行搜索的 DN （识别名），*userDN* 指定绑定到 LDAP 目录的用户的 DN，*basefilter* 指定要搜索的记录。

示例

```
> system ldapsearch ldap.example.com 389 cn=users,
dc=example,dc=com cn=user1,cn=users,dc=example,dc=com, cn=user2
```

lockdown-sensor

移除 `expert` 命令并访问设备上的 bash SHELL。

注意事项 没有支持部门提供的修复程序，就无法撤销此命令。因此，请谨慎使用此命令。

接入

配置

语法

```
system lockdown-sensor
```

示例

```
> system lockdown-sensor
```

nat rollback

将系统恢复为之前应用的 NAT 配置。此命令不适用于虚拟设备和 ASA FirePOWER 设备。此命令不适用于集群设备或堆叠设备。

接入

配置

语法

```
system nat rollback
```

示例

```
> system nat rollback
```

reboot

重新启动设备。

接入
配置

语法
```
system reboot
```

示例
```
> system reboot
```

restart

重新启动设备应用程序。

接入
配置

语法
```
system restart
```

示例
```
> system restart
```

shutdown

关闭设备。此命令不适用于 ASA FirePOWER 模块。

接入
配置

语法
```
system shutdown
```

示例
```
> system shutdown
```

安全、互联网接入和通信端口

为了保护防御中心，应将其安装在受保护的内部网络中。虽然防御中心已配置为仅拥有必需的服务和可用端口，但必须确保无法从防火墙外部攻击它 （或任何受管设备）。

如果防御中心及其受管设备位于同一个网络，则可将这些设备上管理接口连接至与防御中心相同的受保护内部网络。这样，就可以安全地从防御中心控制设备。您还可以配置多个管理接口，使防御中心能够管理和隔离来自其他网络上设备的流量。

无论如何部署设备，内部设备通信将始终加密。但是，必须采取措施确保无法中断、阻塞或篡改 FireSIGHT 系统设备之间的通信；例如，使用分布式拒绝服务 (DDoS) 或中间人攻击。

另请注意， FireSIGHT 系统的特定功能需要连接互联网。默认情况下，所有FireSIGHT 系统设备均配置为直接连接至互联网。此外，系统还要求某些端口对基本内部设备通信保持开放以实现安全的设备访问，以便特定系统功能访问其正常运行所需的本地或互联网资源。

提示 除 用于 Blue Coat X-系列的思科 NGIPS之外， FireSIGHT 系统设备支持使用代理服务器。有关详细信息，请参阅第 64-8 页上的配置管理接口和第 D-32 页上的 http-proxy。

有关详情，请参阅：

- 第 E-1 页上的互联网访问要求
- 第 E-2 页上的通信端口要求

互联网访问要求

默认情况下， FireSIGHT 系统设备会配置为直接连接至互联网的 443/tcp (HTTPS) 和 80/tcp (HTTP) 端口，这些端口在所有 FireSIGHT 系统设备上均默认打开；请参阅第 E-2 页上的通信端口要求。请注意，大多数 FireSIGHT 系统设备均支持使用代理服务器；请参阅第 64-8 页上的配置管理接口。还请注意，代理服务器不能用于 whois 访问。

为确保运营持续性，高可用性对中的两个防御中心均必须接入互联网。为实现特定功能，主防御中心将访问互联网，然后在同步过程中与辅助防御中心共享信息。因此，如果主防御中心发生故障，则应该将辅助防御中心升级为主用设备，如第 4-13 页上的监控和更改高可用性状态中所述。

下表介绍了 FireSIGHT 系统特定功能的互联网接入要求。

表 E-1　　FireSIGHT 系统功能互联网接入要求

特性	需要互联网接入以便...	设备	高可用性考虑事项
动态分析：查询	查询云端以了解之前提交以供动态分析的文件的威胁评分。	防御中心	配对的防御中心独立查询云端以了解威胁评分。
动态分析：提交	提交文件至云端以供动态分析。	所有设备， 2 系列和 X - 系列除外	不适用
FireAMP 集成	接收来自 FireAMP 云的基于终端的（思科）恶意软件事件。	防御中心	云连接未同步。在两个防御中心上配置云连接。
入侵规则、 VDB 和 GeoDB 更新	将入侵规则、 GeoDB 或 VDB 更新直接下接至设备，或安排该等下载。	防御中心	入侵规则、GeoDB 和 VDB 更新已同步。
基于网络的 AMP	执行恶意软件云查找。	防御中心	配对的防御中心独立执行云查找。
RSS 源控制面板构件	从外部源下载 RSS 源数据，包括思科。	任何设备，除了虚拟设备和 X -系列	源数据未同步。
安全情报过滤	从外部来源下载安全情报源数据，包括情报源。	防御中心	主防御中心下载源数据并将与辅助防御中心共享。如果主防御中心出现故障，促进激活辅助防御中心。
系统软件更新	将系统更新下载至设备或安排该等下载。	任何设备，除了虚拟设备和 X -系列	系统更新未同步。
URL 过滤	下载基于云的 URL 类别和信誉数据以进行访问控制，并为未分类的 URL 执行查找。	防御中心	主防御中心下载 URL 过滤数据并将其与辅助防御中心共享。如果主防御中心出现故障，促进激活辅助防御中心。
whois	请求外部主机的 whois 信息。	任何设备，除了虚拟设备和 X -系列	请求 whois 信息的任何设备均必须接入互联网。

通信端口要求

FireSIGHT 系统设备使用双向的SSL 加密通信信道进行通信。该信道默认使用端口 8305/TCP。系统**需要**此端口保持开放以进行基本设备内部通信。其他开放端口允许：

- 访问设备的网络界面。
- 与设备的安全远程连接
- 系统的某些功能访问其正常运行所需的本地或互联网资源

一般来说，功能相关端口会保持关闭，直至启用或配置关联的功能。例如，在将防御中心连接至 User Agent 之前，代理通信端口 (3306/tcp) 会一直保持关闭。又例如， 3 系列设备上的 623/udp 端口会一直保持关闭，直至启用 LOM。

注意事项　在了解此操作对部署的影响之前，请**勿**关闭打开的端口。

例如，在受管设备上关闭出站端口 25/tcp (SMTP) 将阻止该设备发送个别入侵事件的邮件通知（请参阅第 44-1 页上的配置入侵规则的外部警报）。又例如，可通过关闭端口 443/tcp (HTTPS) 禁用对物理受管设备网络接口的接入，但是，这也可能阻止设备将可疑恶意软件文件提交给云端供动态分析。

请注意，系统允许更改其某些通信端口：

- 当配置系统与身份验证服务器之间的连接时，可指定用于 LDAP 和 RADIUS 身份验证的自定义端口；请参阅第 61-16 页上的识别 LDAP 身份验证服务器和第 61-30 页上的配置 RADIUS 连接设置。
- 可更改管理端口 (8305/tcp)；请参阅第 64-8 页上的配置管理接口。但是，思科**强烈**建议保留默认设置。如果更改管理端口，则必须为部署中需要相互通信的所有设备更改该端口。
- 可使用 32137/tcp 端口，以使升级的防御中心与思科云端进行通信。但是，思科建议切换至 443 端口，该端口是版本 5.3 和更新版本的默认新安装端口。有关详细信息，请参阅第 64-25 页上的启用云通信。

下表列出了各种设备类型所要的开放端口，以便利用 FireSIGHT 系统功能。

表 E-2　　用于 FireSIGHT 系统功能和操作的默认通 信端口

端口	说明	方向	开放对象...	要.....
22/tcp	SSH/SSL	双向	任何环境	允计与设备进行安全远程连接。
25/tcp	SMTP	出站	任何环境	从设备发送邮件通知和警报。
53/tcp	DNS	出站	任何环境	使用 DNS。
67/udp 68/udp	DHCP	出站	任何设备，除了 X -系列	使用 DHCP。 **注**　　默认情况下，这些端口已**关闭**。
80/tcp	HTTP	出站	任何设备，除了虚拟设备和 X -系列	允许 RSS 源控制面板构件连接至远程网络服务器。
		双向	防御中心	通过 HTTP 更新自定义和第三方安全情报源。 下载 URL 类别和信誉数据 （还需要 443 端口）。
161/udp	SNMP	双向	任何设备，除了 X -系列	允许通过 SNMP 轮询接入设备的 MIB。
162/udp	SNMP	出站	任何环境	发送 SNMP 警报至远程陷阱服务器。
389/tcp 636/tcp	LDAP	出站	任何设备，除了虚拟设备和 X -系列	与一个 LDAP 服务器通信，以进行外部身份验证。
389/tcp 636/tcp	LDAP	出站	防御中心	获取检测到的 LDAP 用户元数据。
443/tcp	HTTPS	入站接待	任何设备，除了虚拟设备和 X -系列	接入设备的网络接口

表 E-2　　用于 FireSIGHT 系统功能和操作的默认通 （续）信端口

端口	说明	方向	开放对象...	要.....
443/tcp	HTTPS AMQP 云通信	双向	防御中心	获取： • 软件、入侵规则、 VDB 和 GeoDB 更新 • URL 类别和信誉数据 （还需要 80 端口） • 情报源和其他安全的安全情报源 • 基于终端的 (FireAMP) 恶意软件事件 • 网络流量中检测到的文件的恶意软件性质 • 已提交文件的动态分析信息
			2 系列和 3 系列设备	使用设备的本地网络界面下载软件更新。
			3 系列和虚拟设备	提交文件以供动态分析。
514/udp	系统日志	出站	任何环境	发送警报至远程系统日志服务器。
623/udp	SOL/LOM	双向	3 系列	允许使用局域网串行 (SOL) 连接执行无人值守管理
1500/TCP 2000/TCP	数据库访问	入站接待	防御中心	允许第三方客户端对数据库进行只读访问。
1812/UDP 1813/UDP	RADIUS	双向	任何设备，除了虚拟设备和 X -系列	与 RADIUS 服务器通信以进行外部身份验证和记帐。
3306/TCP	用户代理	入站接待	防御中心	与 User Agent 进行通信。
8302/tcp	eStreamer	双向	任何设备，除了虚拟设备和 X -系列	与 eStreamer 客户端通信。
8305/tcp	设备通信	双向	任何环境	在同一部署中的设备之间安全地进行通信。 **Required.**
8307/tcp	主机输入客户端	双向	防御中心	与主机输入客户端通信。
32137/tcp	云通信	双向	防御中心	允许已升级的防御中心与综合安全智能云通信。

第三方产品

FireSIGHT 系统产品包含某些提供用于与 FireSIGHT 系统产品结合使用的第三方开源代码产品。这些产品是免费的，根据其各自许可协议中规定的条款“按原样”提供。下表列出了思科提供的、用于与 FireSIGHT 系统产品结合使用的主要开源代码产品及适用的许可协议。

表 F-1　　开源软件许可

开源软件	许可协议
Apache HTTPD Web Server 2.4.3	Apache 许可证
Linux Kernel 2.6.32.24（2 系列）	GNU 通用公共许可证版本 2 (GPLv2)
Linux Kernel 2.6.35.14（3 系列）	GNU 通用公共许可证版本 2 (GPLv2)
Perl 5.10.1 及相关模块	Perl Artistic 许可证
Snort 2.9.7	GNU 通用公共许可证版本 2 (GPLv2)

可以通过登录产品命令行并查看以下路径来获得所有第三方开源代码产品的完整列表以及所有随 FireSIGHT 系统产品一起提供的适用许可协议的全文：

```
/usr/share/license-files
```

如果要将源代码接收到任何与 FireSIGHT 系统产品结合使用的第三方开源代码产品，可以将相关请求提交到支持网站。

词 汇 表

2 系列

FireSIGHT 系统设备型号的第二个系列。由于资源、架构和许可方面的限制，2 系列 设备支持的功能有限。 2 系列设备包括 3D500、 3D1000、 3D2000、 3D2100、 3D2500、 3D3500、 3D4500、 3D6500 和 3D9900。 2 系列防御中心包括 DC500、 DC1000 和 DC3000。

3 系列

FireSIGHT 系统设备型号的第三个系列。 3 系列设备包括 2 系列和 8000 系列设备，以及 DC750、 DC1500、 DC2000、 DC3500 和 DC4000 防御中心。

7000 系列

一组 3 系列受管设备。此系列的设备包括 70xx 子系列 （3D7010/7020/7030/7050 型号）和 71xx 子系列 （3D7110/7120/3D7115/3D7125 与 AMP7150 型号）。

8000 系列

一组 3 系列受管设备。此系列的设备包括 81xx 子系列 （3D8120/8130/8140 和 AMP8150 型号）、 82xx 子系列 （3D8250/8260/8270/8290 型号）以及 83xx 子系列 （3D8350/8360/8370/8390 型号）。 8000 系列设备的功能通常比 2 系列设备更强大。

ASA FirePOWER

具备 FirePOWER 服务的 Cisco ASA 防火墙的简称。

banner

请参阅服务器横幅。

CAC 身份验证和授权

一种 LDAP 身份验证，允许用户仅使用通用访问卡 (CAC) 提供的凭据登录至设备的 Web 界面。

CA

请参阅证书颁发机构。

certificate

请参阅公共密钥证书。

CLI

请参阅命令行界面 (CLI)。

Context Explorer

显示关于受监控网络的详细、交互图形信息的页面。不同的部分以生动的线条、柱状图、饼状图和环岛状图的形式展示信息，同时提供详细的列表。可以轻松创建和应用自定义过滤器来调整分析，并且可以通过点击或将光标悬停在图形区域检查数据部分。控制面板高度可自定义，可以划分成独立的各个部分而且可以实时更新；与之相比，Context Explorer 是手动更新的，旨在为其数据提供更广泛的上下文，而且具有适用于活跃的用户浏览操作的统一、一致的布局。

CRL

请参阅证书撤销列表 (CRL)。

eStreamer

FireSIGHT 系统的一种组件，用于将事件数据从防御中心或外部设备流式传输至客户端应用。

Fast-Path 规则

在设备的硬件级别使用一系列有限的条件配置的规则，从而允许流量不需要分析，绕过处理。

fingerprint

一个既定的定义，系统将其与特定的数据包包头值和其他来自网络流量的独特数据进行比较，以便识别主机的操作系统。如果系统错误识别或无法识别主机的操作系统，您可以创建可识别主机的自定义指纹。

FireAMP 订用

使组织可以将 FireAMP 用作高级恶意软件防护 (AMP) 解决方案的、单独购买的订用。请与恶意软件许可证进行比较，后者是在设备上启用的，从而执行基于网络的 AMP。

FireAMP 连接器

基于订用的 FireAMP 部署中的用户在电脑和移动设备等终端上安装的轻型代理。连接器与综合安全智能云通信，交换用于快速识别和隔离整个组织中的恶意软件的信息。它们还可以识别终端主机上的威胁表现 (IOC)。

FireAMP 门户

一个网站，您可以在其中配置组织的基于订用的 FireAMP 部署 (http://amp.sourcefire.com/)。

FireAMP 私有云

FireAMP 提供的虚拟机，对于基于 FireAMP 的 （文件和恶意软件）功能，充当受监控网络和综合安全智能云之间的安全中介。通过私有云的匿名代理连接发生与云的所有连接，而不是通过您网络上的个别代理或设备进行。

FireAMP

思科的企业级、基于终端的高级恶意软件分析和防护解决方案，可以发现、识别和阻止恶意软件入侵、持续性威胁和有针对性的攻击。如果组织有 FireAMP 订用，各个用户可以在终端 （电脑、移动设备）上安装轻型 FireAMP 连接器，然后其将与综合安全智能云通信。这样就可以快速识别和隔离恶意软件，以及在其入侵时识别入侵、跟踪其轨迹、理解其影响并了解如何成功恢复。您还可以使用 FireAMP 门户创建自定义防护、阻止特定应用的执行以及创建自定义白名单。请与基于网络的高级恶意软件防护进行比较。

FireSIGHT 建议层

入侵策略中的内置层，当您允许系统将规则状态修改为那些 FireSIGHT 建议规则功能建议的状态时存在。

FireSIGHT 建议规则

一个功能，该功能基于您网络映射中的信息建议在您的入侵策略中应启用或禁用哪些规则。您可以选择允许系统修改基于建议的规则状态，在这种情况下，系统会添加只读的 FireSIGHT 建议层。

FireSIGHT 许可证

防御中心上的默认许可证，允许执行主机、应用和用户发现。 FireSIGHT 许可证还决定您使用防御中心及其受管设备可以监控的个别主机和用户的数量，以及您可以在访问控制规则中使用以便执行用户控制的访问受控用户的数量。

GeoDB

请参阅地理定位数据库 (GeoDB)。

GID

请参阅生成器 ID (GID)。

HA 链路接口

也称为高可用性链路接口，一个您可在设备集群对的每个成员上配置的物理接口，用于充当冗余通信信道，以便在设备之间共享运行状况信息。

HTTP 响应页面

一个网页，可以用来配置系统，使其在用户的 HTTP 请求被访问控制阻止时显示该网页。您可以显示思科提供的通用响应页面，也可以提供自定义 HTML 页面。如果请求被交互阻止规则阻止，您可以允许用户点击响应页面上的按钮，以便继续访问最初请求的站点。

LDAP 身份验证

外部身份验证的一种形式，通过将用户凭据与直接存储在 LDAP 目录服务器中的轻型目录访问协议 (LDAP) 目录进行比较来验证用户凭据。

link state propagation

旁路模式下内联集的一个选项，在内联集中当一对接口中有一个被关闭时，自动关闭第二个接口。当被关闭的接口恢复运行时，第二个接口也自动恢复运行。换句话说，如果一个已配对的接口的链路状态改变，另一个接口的链路状态会自动变为与之一致的状态。

NAT 策略

使用 NAT 规则以便执行使用的 NAT 的路由的策略。

NAT 规则

配置和条件的集合，可以评估网络流量，并指定如何转换与这些限定匹配的流量。 NAT 规则会添加至现有 NAT 策略，以便执行使用 NAT 的路由。

NAT

网络地址转换，用于在专用网络上的多个主机之间共享单一互联网连接的最常用功能。使用发现，系统可将网络设备识别为负载均衡器。此外，在 FireSIGHT 系统的第 3 层部署中，您可以通过 NAT 策略来配置使用 NAT 的路由。

NetFlow

由思科开发以便在支持思科 IOS 的设备上运行的开放但专有的网络协议，用于收集 IP 流量信息。您可以使用已启用 NetFlow 的设备收集的信息来补充 FireSIGHT 系统收集的发现和连接数据，以及监控未被受管设备覆盖的网络。

NetMod

在受管设备的机箱中安装的一个模块，其包含适用于该设备的检测接口。

Nmap

网络映射器，一个开源的主动扫描器，您可以用来检测在主机上运行的操作系统和应用协议。运行 Nmap 扫描可以将检测到的信息添加至您的网络映射。

object

可重用配置，将名称与值 （例如 IP 地址或 URL）关联，以便在您想要在网络接口中使用该值时，可以使用命名对象来替代。您可以使用对象管理器创建对象。另请参阅：网络对象、安全情报对象、端口对象、 VLAN 标记对象、 URL 对象、应用过滤器、变量集、文件列表、 HA 链路接口、安全区域、密码套件列表、可辨别名称对象和 PKI 对象。

PKI 对象

代表公共密钥证书和成对私有密钥的可重用 object。

PKI

请参阅公共密钥基础结构 (PKI)。

RADIUS 身份验证

远程身份验证拨入用户服务，用于验证/授权和说明用户对网络资源的访问的一种服务。您可以创建外部身份验证对象，以便允许 FireSIGHT 系统用户通过 RADIUS 服务器进行身份验证。

RSA 密码技术

基于将一个大数因式分解为两个质数的一种加密方法。请与椭圆曲线 (EC) 密码技术对比。

SFP 模块

插入到 71xx 子系列设备上的网络模块中的小型可插拔收发器。SFP 模块上的感应接口不允许使用可配置的旁路。

SHA-256 哈希值

有时缩写为 SHA256，一个代表文件的 32 字节字符串，您可以针对其执行恶意软件云查找。哈希值使用加密哈希函数计算得出，因此具有相同 SHA-256 值的文件很可能具有相同的内容。

SID

请参阅签名 ID (Sid)。

Snort

一个开源的入侵检测系统，可在 IP 网络上执行实时流量分析和数据包记录。 Snort 可以执行协议分析、内容搜索和匹配，并且能够检测各种攻击和探测。 Snort 使用灵活的规则语言来描述其应收集或允许通过的网络流量。 FireSIGHT 系统使用 Snort 来针对解码器、预处理器和入侵规则检测数据包。

SSL 策略

用作父级访问控制策略的一部分并且在受策略目标设备监控的加密流量上执行 SSL 检查的一种策略。SSL 策略可能包括多个 SSL 规则；它还指定决定着如何处理和记录不符合任何这些规则条件的流量的默认操作。 SSL 策略也可以指定如何处理无法解密的流量，以及根据 CA 公共密钥证书信任什么加密流量。

SSL 规则操作

一个设置，决定系统如何处理符合 SSL 规则的条件的加密网络流量。您可以阻止匹配流量 （在重置或不重置连接的情况下）。您也可以不解密加密流量，用上传的私有密钥解密传入流量，用重新签署的公共密钥证书解密传出流量，或继续用其他 SSL 规则监控流量。

SSL 规则

系统用于检查加密流量并且允许 SSL 检查的一组条件。用于填充 SSL 策略的 SSL 规则可以执行简单 IP 地址匹配，或者表征涉及不同用户、应用、端口、 URL 和加密会话特征的复杂连接。 SSL 规则操作决定系统如何处理符合规则的条件的流量。其他规则设置决定如何 （以及是否）记录连接。

SSL 检查

一个功能，允许您检查、解密和记录流经网络的加密流量。您选择不解密的流量和已解密的流量都可以用访问控制进一步检查。

SSL

请参阅安全套接字层 (SSL)。

SVID

请参阅漏洞 ID。

TLS

请参阅传输层安全。

URL 对象

代表单个 URL 的可重用object。

URL 过滤许可证

允许您基于 URL 类别和 URL 信誉信息执行 URL 过滤的许可证。 URL 过滤许可证会过期。

URL 过滤

一个允许您编写访问控制规则的功能，这些规则基于受监控主机请求的 URL，并与防御中心从综合安全智能云获得的关于这些 URL 的 URL 类别和 URL 信誉信息关联，可以确定能流经网络的流量。还可以通过指定要允许或阻止的单个的 URL 或成组的 URL 对网络流量实现更细化的自定义控制。

URL 类别

URL 的通用分类，例如恶意软件或社交网络。

URL 信誉

对网站被用于违反组织的安全策略的目的的可能性之表示，由综合安全智能云确定。

UTC 时间

协调世界时。又叫做格林尼治标准时间 (GMT)， UTC 是全球各地共同使用的标准时间。虽然 FireSIGHT 系统使用 UTC，但是可以使用 Time Zone 功能设置本地时间。

VDB

请参阅漏洞数据库。

VLAN 标记对象

代表单个虚拟局域网 (VLAN)标记的可重用 object。

VLAN

请参阅虚拟局域网 (VLAN)。

VPN 许可证

一个许可证，该许可证允许您在FireSIGHT 系统受管设备的虚拟路由器之间构建安全的VPN隧道。

VPN

一个功能，该功能允许您在FireSIGHT 系统受管设备的虚拟路由器之间构建安全的VPN隧道。

VRT 分析报告

提交用于动态分析的捕获的文件的 思科 VRT 分析记录，详细描述了动态分析摘要报告中存在的信息，以及在动态分析过程中发现的其他信息。

VRT

请参阅思科 VRT。

X -系列

用于 Blue Coat X-系列的思科 NGIPS的简称。

安全策略

保护组织网络的组织准则。例如，安全策略可能禁止使用无线接入点。安全策略还可能包括可接受的使用策略 (AUP)，其为员工提供关于如何利用其组织的系统的指导。

安全情报

按照访问控制策略，根据源或目标 IP 地址，指定可以穿越网络的流量的一种功能。如果在流量接受访问控制规则分析之前，要将特定 IP 地址列入黑名单或阻止它们之间的流量，这个功能就特别有用。或者，可以为安全情报过滤使用监控器设置，让系统可以分析本应该已经列入黑名单的连接，而且可以记录符合黑名单的匹配项。

安全情报白名单

访问控制策略中的 IP 地址列表，强制要求策略使用访问控制规则检查流向和来自这些主机的流量，即不使用安全情报拒绝该流量。因为策略的白名单会覆盖其安全情报黑名单，所以您可以使用白名单来微调黑名单。白名单由安全情报对象组成，包括全局白名单。

安全情报对象

代表一个或多个 IP 地址的单个配置，您可以将其添加至访问控制策略的安全情报黑名单和安全情报白名单。安全情报对象包括安全情报列表、安全情报源以及网络对象和组。全局黑名单、全局白名单和 情报源中的类别也会被视为安全情报对象。

安全情报黑名单

访问控制策略中的 IP 地址列表，允许在流量被访问控制规则分析之前拒绝发往和来自这些主机的流量。黑名单包括安全情报对象，包括全局黑名单。访问控制策略的安全情报白名单覆盖其黑名单。

安全情报列表

IP 地址的简单静态集合，您可以作为安全情报对象手动上传至防御中心。可以使用列表来扩充和微调安全情报源以及全局黑名单和全局白名单。

安全情报事件

由安全情报黑名单阻止或监控的流量生成的连接事件。您可以与普通连接事件分开，单独查看安全情报事件并与之交互。

安全情报源

一种类型的安全情报对象，系统以您配置的间隔定期下载的 IP 地址的动态集合。由于安全情报源会定期更新，使用它们可以确保系统使用最新信息来利用安全情报功能过滤网络流量。另请参阅情报源。

安全区域

可以用于管理和分类各种策略与配置中流量流动的一个或多个内联、被动、交换或路由接口。单个区域的接口可以跨多个设备；还可以在单个设备上配置多个安全区域。您必须向安全区域分配至少一个接口，以根据该安全区域来匹配流量，并且每个接口可以仅属于一个区域。

安全套接字层 (SSL)

在传输层安全协议之前出现的加密应用层协议。 SSL 检查功能允许您解密使用 SSL 协议加密的流量。

白名单

合规性白名单、安全情报白名单、HA 链路接口或您可以在修复内配置的 IP 地址列表，用于将 IP 地址从某些操作中排除。

白名单事件

一个事件，系统检测到有效的目标主机变得不符合合规性白名单时生成。白名单事件是一种特殊的关联事件。

白名单违规

您可以在事件查看器中查看的信息，详细描述主机如何不符合合规性白名单。

保护许可证

许可证可供您执行入侵检测和防御、文件控制和安全情报过滤。没有许可证， 2 系列设备自动具备保护功能，但是安全情报除外。

报告模板

一个模板，为报告及其部分指定数据限制和格式。

被动检测

通过分析受管设备被动收集的流量执行的一系列发现数据。与主动检测进行比较。

被动接口

被配置用于分析被动部署中的流量的检测接口。

变量集

一系列变量配置，您可以将这些配置与入侵策略关联，从而可以定制在每个入侵策略中启用的入侵规则，使之与您的网络流量密切匹配。

变量

入侵规则中的常用值的一个表示。 FireSIGHT 系统使用预配置的按照变量集组织的变量定义网络和端口号。您可以更改变量值，从而定制规则，进而准确反映您的网络环境，而不是在多个规则中对这些值进行硬编码。

标记 （应用）

请参阅应用标记。

标识冲突

如果系统报告新的被动操作系统或服务器标识，而该标识与当前活动标识和先前报告的被动标识冲突，则该冲突发生。

标准文本规则

基于规则编辑器中的可用标识符、关键字和参数创建的入侵规则。您可以创建您自己的自定义标准文本规则，也可以修改思科提供的标准文本规则。标准文本规则的生成器 ID (GID) 为 1。

表视图

一种类型的工作流程页面，可以显示事件信息，数据库表格中的每个字段对应一个列。执行事件分析时，在您进入表视图之前 （该视图向您显示感兴趣的事件的相关详细信息），可以使用向下钻取页面来约束您想要调查的事件。表视图通常是系统提供的工作流程的倒数第二页。

补救模块

使用称为补救实例的配置集，启动修复的程序。 FireSIGHT 系统附带有可执行各种操作的多个补救模块，您也可以使用灵活的 API 来创建自己的模块。

补救实例

补救模块的配置集。对于每个模块，您可以配置多个实例，例如，您可以使用相同的模块，但又使用拥有不同设置的不同实例来响应不同的关联策略违规。当补救实例触发时，产生的操作称为修复。

补救状态事件

一个事件，修复启动时生成。

捕获的文件

在设备复制的网络流量中检测到的文件，用于提交至综合安全智能云进行动态分析或斯佩罗分析，或向设备进行文件存储。

操作

确定系统如何处理、检查或记录符合 （或不符合）特定条件的网络流量。操作与各种规则以及某些策略关联，作为策略的默认操作。

操作系统标识

主机上的操作系统的操作系统供应商和版本详细信息。

侧录模式

3D9900 和 3 系列设备上可用的一种高级内联集选项，其中要分析每个数据包的一个副本并且网络流量不受干扰，无需通过设备。由于处理的是数据包的副本而不是数据包本身，因此即使将访问控制和入侵策略配置为放弃、修改或阻止流量，设备都不会影响数据包数据流。

策略目标

您在其中应用策略的设备或区域。策略可能有多个目标。

策略

应用设置，通常是向设备应用设置，的一种机制。请参阅访问控制策略、关联策略、文件策略、健康策略、入侵策略、网络分析策略、网络发现策略、 SSL 策略和系统策略。

层

在入侵策略或网络分析策略中的一套完整的配置。您可以将自定义用户层添加至您策略中的内置层。高层中的设置会覆盖低层中的设置。

传输层安全

安全套接字层 (SSL)协议之后出现的加密应用层协议。 SSL 检查功能允许您解密使用 TLS 协议加密的流量。

存储的文件

保存至设备的硬盘驱动器或恶意软件存储包 （如有安装）的捕获的文件。存储的文件可以稍后下载和分析。

当前标识

对于特定网络资产，系统发现最有可能正确的标识操作系统或服务器标识。系统以多种方式使用此数据，例如，计算统计信息，分配漏洞信息，评估攻击影响，以及评估关联规则。

当前用户

系统将其与主机关联的用户。如果用户是访问受控用户，系统可以对流向或来自该主机的流量执行用户控制。如果没有访问受控用户与该主机关联，非访问受控用户可以是该主机的当前用户。然而，一名访问受控用户登录至主机后，只有另一访问受控用户进行的登录才会更改当前用户。

导出

您可以用来在设备之间转移各种配置 （例如策略）的一种方法。从一台设备导出配置后，您可以将其导入至相同类型的另一设备。

导入

可以用于将各种配置从一个设备传输至另一个设备的一种方法。您可以导入先前从相同类型的另一设备中导出的配置。

地理定位数据库 (GeoDB)

与可路由 IP 地址关联的、包含已知地理定位数据的一种数据库，此数据库定期更新。

地理定位

一个功能，该功能提供在受监控网络的流量中检测到的可路由 IP 地址的地理来源的相关数据，包括连接类型、互联网服务提供商等。您可以看到在事件和主机配置文件中的地理位置信息，并将其用于过滤访问控制策略或SSL 策略中的流量。

第三方漏洞

从第三方获得的漏洞数据。如果您的组织可以编写脚本或创建命令行导入文件来从第三方应用导入网络映射数据，您可以使用主机输入功能来导入第三方漏洞数据，从而扩充系统的漏洞数据。

丢弃规则

一个入侵规则，其规则状态设置为 Drop and Generate Events。如果恶意数据包触发内联部署中的该规则，并且您应用的入侵策略设置为内联时丢弃，系统会丢弃数据包并生成入侵事件 （具体而言，是丢弃事件）。

丢弃事件

丢弃规则触发时生成的入侵事件。在事件查看器中，丢弃事件标有黑色向下箭头。

动态分析

一种将捕获的文件从设备提交至综合安全智能云以用于恶意软件分析的方式。该云会在测试环境下运行文件，并向防御中心返回威胁评分和动态分析摘要报告。通过动态分析摘要报告，您还可以查看 VRT 分析报告。

动态分析摘要报告

一份摘要，描述为何综合安全智能云给文件分配威胁评分，包括在动态分析期间发现的所有威胁，以及在测试环境下运行文件时检测到的其他进程。从此处，您还可以查看 VRT 分析报告。

动态规则状态

针对指定时段设置的入侵规则状态，该时段是响应匹配规则的流量中检测到的速率异常的一个时段。

端口对象

可重用的object，代表使用传输层协议 （如 TCP、 UDP 或 ICMP）的开放端口。

堆叠

共享检测资源的二至四个相互连接的设备。

堆栈

允许通过在一个堆栈配置中连接二至四个物理设备，从而增加网段上检查的流量的一种功能。建立堆栈配置时，要将每个堆叠设备的资源集成到单个统一的共享配置中。

对象管理器

Web 界面上的页面，您将在此页面上管理 object 和对象组。

恶意软件存储包

您可以在特定设备中安装的由思科提供的辅助固态驱动器，用于存储捕获的文件，从而释放用于事件和配置存储的设备主硬盘驱动器上的可用空间。

恶意软件防护

请参阅高级恶意软件防护。

恶意软件检测

思科基于网络的高级恶意软件防护 (AMP) 解决方案的一个组成部分。作为全局访问控制配置组成部分向受管设备应用的文件策略检查网络流量。随后，防御中心会针对特定检测到的文件类型执行恶意软件云查找，并生成向您提示文件的恶意软件性质的事件。接着会进行 AMP 恶意软件阻止，阻止文件或允许其上传或下载。将此功能与 FireAMP 比较，后者是思科基于终端的 AMP 工具，要求采用 FireAMP 订用。

恶意软件性质缓存

防御中心上的缓存，用于存储文件的恶意软件性质和威胁评分。如果系统已经知道文件的基于其 SHA-256 哈希值的性质和威胁评分，为提高性能，防御中心将使用缓存的信息，而不是执行恶意软件云查找。特定时段过后，缓存中的信息将会超时，以便缓存数据不会过时。

恶意软件性质

综合安全智能云作出的文件是否包含恶意软件的判定，基于文件的 SHA-256 哈希值、威胁评分以及文件是处于干净列表还是处于自定义检测列表。

恶意软件许可证

允许在网络流量中执行高级恶意软件防护 (AMP) 的许可证。使用文件策略，可以配置系统，对受管设备检测的特定文件类型执行恶意软件云查找。请与 FireAMP 订用比较。

恶意软件云查找

一个过程，防御中心通过该过程与综合安全智能云通信，以便基于文件的 SHA-256 哈希值确定在网络流量中检测到的文件的恶意软件性质。

恶意软件阻止

思科基于网络的高级恶意软件防护 (AMP) 解决方案的一个组成部分。在内联部署中，如果恶意软件检测产生检测到的文件的恶意软件性质，或检测到的文件处于自定义检测列表上时，您可以阻止文件或允许其上传或下载。将此功能与 FireAMP 比较，后者是思科基于终端的 AMP 工具，要求采用 FireAMP 订用。

恶意事件

思科的高级恶意软件防护解决方案之一生成的事件。综合安全智能云返回网络流量中检测到的文件的恶意软件性质时，基于网络的恶意软件事件将会生成；该性质变化时，追溯性恶意软件事件将会生成。请与基于终端的恶意事件比较，后者是在部署的 FireAMP 连接器检测到威胁、阻止恶意软件执行或隔离或无法隔离恶意软件时生成的。

发现

FireSIGHT 系统的一种组件，使用受管设备监控网络并提供网络的完整统一视图。网络发现可以确定网络上的主机 （包括网络设备和移动设备）的数量和类型以及关于操作系统、活跃应用和这些主机上的开放端口的信息。您还可以配置受管设备来监控您网络上的用户活动，这使得您可以识别策略违反、攻击或网络漏洞的来源。

发现策略

请参阅网络发现策略。

发现规则

在网络发现策略内，指定您想要监控的网络和区域或者您想要用于对其进行监控的设备 （包括支持 NetFlow 的设备），以及您想要从监控中排除的任意端口。每个规则也可以指定您是否想要在受监控的网络上发现主机、用户或应用。

发现事件

一个事件，该事件详细描述新资产的发现或者现有资产的变化。主机输入事件 是一种特殊的发现事件。有时，“发现事件”指任何发现数据或漏洞信息。

发现数据

由发现功能收集的限定您网络资产和流量的主机、用户和应用信息。

防御中心

用于管理设备和自动聚合与关联其所生成的事件的集中管理点。

访问控制

FireSIGHT 系统的一个功能，允许您指定、检查和记录遍历网络的流量。访问控制调用安全情报、 SSL 检查、预处理器选项、入侵检测和防御、文件控制和高级恶意软件防护。它还决定您可以使用发现检查的流量。

访问控制策略

应用于管理设备从而在这些设备监控的网络流量执行访问控制的策略。访问控制策略可能包括多个访问控制规则；它还指定决定着如何处理和记录不符合任何这些规则条件的流量的默认操作。访问控制策略中的其他设置管理安全情报、 SSL 检查、性能选项、预处理器选项和其他高级配置。

访问控制规则操作

一个设置，决定系统如何处理符合访问控制规则条件的网络流量。您可以*阻止*匹配流量（在重置或不重置连接的情况下）；对于 HTTP 流量，您可以为用户提供绕过该阻止的选项。您还可以*信任*流量，允许其通过而无需进一步检查，可以*允许*匹配流量，选择使用入侵策略和文件策略对其进行检查，或者用其他访问控制规则继续*监控*流量。

访问控制规则

一组条件， FireSIGHT 系统可用来检查受监控的网络流量并实现精细访问控制。填充访问控制策略的访问控制规则可执行简单的 IP 地址匹配，或者可能描述涉及多种不同标准的复杂连接。访问控制规则操作决定系统如何处理符合规则的条件的流量。其他规则设置确定如何（以及是否）记录连接，以及入侵策略或文件策略是否检查规则允许的流量。

访问列表

IP 地址列表，在系统策略中配置，描述可以访问设备的主机。默认情况下，任何人都可以使用端口 443（HTTPS）访问设备的 Web 界面，也可以使用端口 22 (SSH) 访问命令行。还可以使用端口 161 增加 SNMP 访问。

访问受控用户

一名用户，您可以使用访问控制控制其网络使用情况。配置 Microsoft Active Directory 服务器与防御中心之间的连接时，您可以指定访问受控用户必须属于的 LDAP 组。当用户代理报告访问受控用户进行的登录时，这些用户会与 IP 地址关联，从而使得可以触发使用用户条件的访问控制规则。与非访问受控用户进行比较。

非访问受控用户

用户代理或受管设备检测到的不对其进行访问控制的任意用户。如果没有访问受控用户曾经登录主机，非访问受控用户只能是主机的当前用户。

非活动期

一个间隔，在该间隔内，关联规则不会触发。您可以配置非活动期的时间、频率和持续时间。另请参阅暂停期。

分片重组策略

一个子策略，描述 IP 分片重组预处理器（在网络分析策略中配置）应如何基于目标主机的操作系统重组分片的 IP 数据包。请注意，自适应配置文件使用自适应分片重组策略。

风险

请参阅应用风险。

服务器标识

主机上的服务器的应用协议类型、供应商和版本详细信息。

服务器横幅

对于服务器，检测到的第一个数据包的前 256 个字节，可以提供能帮助您识别服务器的额外信息。系统只会在首次检测到服务器时收集服务器横幅一次。

服务器证书

证书颁发机构颁发的加密证书，可提供服务器标识的不可改变的确认。您可以从任意证书颁发机构请求证书，并将该自定义证书上传至设备。

服务器

主机上安装的、按照应用协议流量进行识别的服务器应用 （请与客户端应用相比较）。

负载均衡器

分配流量以优化性能和资源使用的网络设备。使用发现，系统可以识别负载均衡器。

复杂约束

事件视图或事件搜索中设置的约束集，使用特定事件的所有条件来约束事件查询。

干净列表

由其 SHA-256 哈希值所代表的文件的列表。当系统检测到列表中的某个文件时，不会执行恶意软件云查找，而是将该文件视为干净文件，即使综合安全智能云中该文件的性质是恶意软件。

高级恶意软件防护

简称 AMP，FireSIGHT 系统基于网络的恶意软件检测和恶意软件阻止功能。将此功能与 FireAMP 比较，后者是思科基于终端的 AMP 工具，要求采用 FireAMP 订用。

高可用性

允许配置冗余物理防御中心来管理成群设备的一种功能。从受管设备流式传输至两种防御中心的事件数据流和大多数配置元素在两种防御中心上都会保存。如果主要防御中心出现故障，可以使用辅助防御中心监控网络，而不会中断监控。请与集群比较，后者允许指定冗余设备。

更改记录报告

过去 24 小时内的所有系统更改的详细报告，基于每当新配置保存时所生成的快照。您可以配置系统，以便每天在您指定的时间通过邮件发送这些报告。

工作流程

一系列页面，您可用于从事件数据的广泛视图开始，然后进入仅包含您感兴趣的事件、更加突出重点的视图，从而查看和评估事件。工作流程可包含三种类型的页面，每个类型执行独特的功能：向下钻取页面、表视图和最终页面。取决于工作流程类型，最终页面可能是表视图、数据包视图、主机视图、漏洞详细信息或用户详细信息。

公共密钥基础结构 (PKI)

一个系统，用于管理证书颁发机构如何向个人颁发公共密钥证书和与之成对的私有密钥。

公共密钥

与公共密钥证书关联的加密密钥，对于任何人都可用。公共密钥和与之成对的私有密钥可用于安全套接字层 (SSL)和传输层安全加密与解密。

公共密钥证书

由证书颁发机构颁发给个人的数字文档，用于确认存储在证书中的公共密钥属于该个人。

共享层

一个您允许其他策略使用的入侵策略或网络分析策略层。当您提交对共享层中的更改时，使用共享层的策略将会用这些更改进行更新。共享层只能在允许其被共享的策略中修改；它在使用它的策略中是只读的。

共享对象规则

一个入侵规则，以通过 C 语言源代码编译而成的二进制模块的形式提供。您可以使用共享对象规则，以标准文本规则无法采取的方式来检测攻击。您不能修改共享对象规则中的规则关键字和参数；您限于修改规则中使用的变量，或者修改源和目标端口与 IP 地址等方面的信息，以及将规则的新实例保存为自定义共享对象规则。共享对象规则拥有值为 3 的生成器 ID (GID)。

构件

请参阅控制面板构件。

故障保护

内联集的一个特征，如果内部流量缓冲区已满，允许数据包绕过处理并继续通过设备。

挂起 （应用协议）

如果系统既不能正确识别也不能错误识别应用协议，会将应用协议识别为应用协议。大多数情况下，系统需要收集和分析更多的数据才能识别挂起的应用协议。

关联策略

使用关联规则和合规性白名单描述构成安全策略违规的网络活动的策略。可以向策略内的每个规则或白名单指定效率低下。

关联规则

就合规性白名单而言，指定违反关联策略时网络流量必须满足的条件的方法之一。您可以使用防御中心来配置在发生特定事件或网络流量偏离流量量变曲线中描述的正常网络流量模式时要触发（并生成关联事件）的关联规则。您可以使用主机配置文件限定条件、连接跟踪器、暂停期和非活动期来约束关联规则。您还可以配置防御中心来在关联规则触发时发起响应，如警报或修复。

关联事件

关联规则触发时，防御中心生成的事件。请注意，由白名单违规生成的白名单事件是一种特殊的关联事件。

管理接口

用于管理 FireSIGHT 系统设备的网络接口。在大多数部署中，管理接口连接到内部受保护的网络。请与检测接口比较。在虚拟防御中心和所有 3 系列 设备上，您可以配置多个管理接口，从而将流量分为几个通道以提高性能，或创建指向其他网络的路由，从而允许防御中心隔离不同网络上的流量。您还可以将流量信道路由至单独的网络，从而提高吞吐量。

管理流量信道

请参阅流量信道。

规则操作

一个设置，决定系统如何处理符合规则条件的网络流量。另请参阅：访问控制规则操作、文件规则操作和 SSL 规则操作。

规则更新

视需要进行的入侵规则更新，包含新的和已更新的标准文本规则、共享对象规则和预处理器规则。规则更新也可以删除规则；修改默认入侵策略、网络分析策略和高级访问控制策略设置；以及添加或删除默认变量和规则类别。

规则

一个构造，通常位于策略内，可以提供检查网络流量时所依据的标准。另请参阅：访问控制规则、关联规则、发现规则、 Fast-Path 规则、文件规则、入侵规则、网络分析规则、预处理器规则和 SSL 规则。

规则状态

入侵策略内入侵规则是被启用 （设置为 Generate Events 或 Drop and Generate Events），还是被禁用（设置为 Disable）。如果启用规则，它将用于评估网络流量；如果禁用规则，则不使用此规则。

合规性白名单事件

请参阅白名单事件。

合规性白名单

随关联规则配合使用，是您可以指定网络流量违反关联策略所必须符合的条件的方式之一。您可以使用防御中心来配置合规性白名单，以指定哪些操作系统、应用和协议被允许在特定子网中的主机上运行。您还可以配置防御中心在白名单被违反时发起响应，如警报或修复。请注意，合规性白名单不与其他类型的白名单关联。

合规性白名单违规

请参阅白名单违规。

黑名单

请参阅运行状况监控黑名单或安全情报黑名单。

混合接口

受管设备上的一种逻辑接口，使系统可以桥接虚拟路由器和虚拟交换机之间的流量。

基本策略层

在入侵策略或网络分析策略中最低的内置层。基本策略确定基本策略层的设置，并且因而确定策略的默认设置。

基本策略

用作自定义策略的基本策略层的入侵策略或网络分析策略。

集群

一个功能，允许您在两个对等 3 系列 设备或堆叠之间实现网络功能和配置数据冗余。集群为策略应用、系统更新和注册提供了一个统一的逻辑系统。请与高可用性比较，后者允许配置冗余的防御中心。

计划任务

安排运行一次或按照一定间隔重复运行的管理任务。

监控器

记录匹配流量的一种方法，系统还可以通过此方法继续评估连接，而不是立即允许或阻止此流量。您可以监控违反安全情报黑名单，或者与访问控制规则或 SSL 规则中任意标准组合匹配的流量。

剪贴板

一个保存区域，您可以在其中复制多达 25,000 个稍后可以添加至事故的入侵事件。

检测接口

在设备上用于监控网段的网络接口。请与管理接口比较。

健康策略

检查部署中的设备的运行状况时使用的标准。运行状况策略使用运行状况模块来指示系统硬件和软件是否在正常工作。可以使用默认的健康策略，也可以自己创建。

交互阻止

一个访问控制规则操作，允许您的用户点击 HTTP 响应页面上的按钮，以便继续访问最初请求的站点。

交换机

用作多端口网桥的网络设备。利用网络发现，系统将交换机识别为网桥。此外，还可以将受管设备配置为虚拟交换机，在两个或多个网络之间执行数据包交换。

交换接口

想要用于交换第 2 层部署中流量的接口。可以设置处理不带标记的 虚拟局域网 (VLAN) 流量的物理交换接口和处理带指定 VLAN 标记的流量的逻辑交换接口。

解码器

入侵检测和防御的一个组件，在网络分析策略中配置，其将探查的数据包转换为预处理器可以识别的格式。

警报

告知系统已经生成特定事件的通知。您可以根据入侵事件 （包括其影响）、发现事件、基于网络的恶意事件、关联策略违规、运行状况状态变化以及记录的连接发出警报。在大多数情况下，可以通过邮件、系统日志或 SNMP 陷阱发出警报。

警报响应

一组配置，允许系统通过邮件、系统日志或 SNMP 陷阱发送警报。您可以使用单个警报响应来针对多种类型的事件向您发出警报。

具备 FirePOWER 服务的 Cisco ASA 防火墙

已安装 ASA FirePOWER 模块的一组思科自适应安全设备 (ASA) 受管设备。此系列中的设备包括 ASA 5506-X、 ASA5512-X、 ASA5515-X、 ASA5525-X、 ASA5545-X、 ASA5555-X、 ASA5585-X-SSP-10、 ASA5585-X-SSP-20、 ASA5585-X-SSP-40 和 ASA5585-X-SSP-60 型号。

可辨别名称对象

一种可重复使用的 object，代表公共密钥证书主题或颁发者可以辨识的名称。

可控性许可证

允许实施用户控制和应用控制的许可证。它还允许您配置受支持的受管设备以执行基于硬件的任务，例如交换和路由 （包括 DHCP 中继和NAT）、 VPN和设备集群。

可配置的旁路

内联集的一种特性，允许配置旁路模式。

客户端应用

请参阅客户端。

客户端

又叫做客户端应用，指在一个主机上运行并且依靠另一个主机 （服务器）来执行某些操作的应用。例如，邮件客户端允许发送和接收邮件。当系统检测到主机上的用户正使用特定客户端访问另一主机时，将在主机配置文件和网络映射中报告该信息，包括客户端的名称和版本 （如果有）。

控制面板构件

控制面板自带的一种小组件，用于深入了解 FireSIGHT 系统的某个方面。

控制面板

提供当前系统状态快速浏览视图的一种显示，包括显示关于系统收集和生成的事件的数据。要增加系统提供的控制面板，可以创建多个自定义控制面板，并用选择的控制面板构件填充。与就受监控网络的外观和运行方式提供广泛、简明的彩色图片的 Context Explorer 进行比较。

类别

请参阅应用类别、文件类别或 URL 类别。

连接跟踪器

一个或多个约束关联规则的条件，以便在规则的初始条件得到满足后，系统可以开始跟踪特定连接。随后，仅当受跟踪的连接满足额外的条件时，规则才会被触发。

连接

两个主机之间受监控的会话。您可以记录 FireSIGHT 系统受管设备检测到的连接以及从启用 NetFlow 的设备导入连接数据。

连接日志

请参阅连接事件。

连接事件

系统检测到受监控主机和任何其他主机之间的连接时生成的事件。安全情报事件是特殊类型的连接事件。连接事件包含检测到的流量的相关信息。各种设置使您可以精细控制记录哪些连接、何时记录以及在哪里存储数据。对于受管设备检测到的连接，您可以在连接开始和结束时记录未被阻止的连接，但是大多数受阻的连接只能在其开始时进行记录。您可以将这些连接记录至防御中心数据库，具体取决于规则或默认操作；您还可以将连接事件记录至外部系统日志或 SNMP 陷阱服务器。 NetFlow 记录可记录连接的结束事件并且始终将其保存至数据库。

连接图

一种以图形形式显示连接事件的方式。

连接摘要

在五分钟的时间间隔内汇总的连接数据。系统使用连接摘要来构建连接图和流量量变曲线。要进行汇总，多个连接必须代表连接结束，拥有相同的源 IP 地址和目标 IP 地址，并且使用响应方（目标）主机上的相同端口。 .它们必须使用相同的协议 （TCP 或 UDP）和应用协议。最后，它们必须被相同的受管设备检测到或由启用 NetFlow 的同一设备导出。

链路汇聚组 (LAG)

一个3 系列 功能，您可以通过此功能将多个物理以太网接口归为受管设备上的单一逻辑链路，此链路在提供网络之间数据包交换的第 2 层部署中配置，或在路由接口之间流量的第 3 层部署中配置。该单一汇聚逻辑链路提供更高的带宽、冗余和两个终端之间的负载平衡。

链路聚合控制协议 (LACP)

IEEE 802.3ad 规范的一个组件，其提供交换系统和端口信息的方法，以控制将若干物理端口捆绑在一起，从而形成一个叫做链路汇聚组的单个逻辑数据通道。当您启用 LACP 时，通道中任一端的每台设备都使用 LACP 来确定将哪些链路主动用于汇聚中。

列表

请参阅安全情报列表。

流量量变曲线

网络上流量的量变曲线，基于在您指定的时间跨度内记录的连接事件。您可以通过受监控网段上的所有流量创建量变曲线，也可以创建更有针对性的量变曲线。随后，您可以针对现有量变曲线评估新的流量，从而使用相关性功能来检测异常网络流量。

流量信道

您可以在 3 系列设备或虚拟防御中心的管理界面上配置的一种连接，该连接用于承载管理或事件流量。事件流量通道只承载在受管设备网段上生成的事件数据并且管理流量通道只承载内部生成的流量 （即防御中心和设备之间的管理流量）。请参阅管理接口。

漏洞 ID

与特定漏洞关联的标识号。思科漏洞数据库和第三方漏洞数据库 （例如 Bugtraq 和 CVE）有着不同的漏洞 ID 编号方案。

漏洞

关于主机容易感染的特定威胁的一种描述。防御中心在主机的主机配置文件中提供了您的每个主机容易遭受攻击的漏洞的相关信息。此外，可以使用漏洞网络映射获取系统在整个受监控网络上检测到的漏洞的整体描述。如果认为主机不再容易感染特定威胁，可以撤销特定漏洞或将其标记为无效漏洞。

漏洞数据库

又叫做 VDB，指关于主机可能感染的已知漏洞的数据库。系统将操作系统、应用协议和在每台主机上检测的客户端与 VDB 关联，从而帮助确定特定主机是否增加了遭受网络威胁的风险。 VDB 更新可能包含新的和经过更新的漏洞，以及新的和经过更新的应用检测器。

漏洞详细信息

漏洞工作流程中的最终页面。漏洞详细信息页面提供特定漏洞的相关信息，包括技术详细信息和已知解决方案。

漏洞映射

漏洞信息与发现数据的关联，以便您可以执行影响相关性。

路由接口

路由第 3 层部署中的流量的接口。可以设置处理不带标记的 虚拟局域网 (VLAN) 流量的物理路由接口和处理带指定 VLAN 标记的流量的逻辑路由接口。还可以将静态地址解析协议 (ARP) 添加到路由接口中。

路由器

位于网关上，在网络之间转发数据包的一种网络设备。使用网络发现，系统可识别路由器。此外，还可以将受管设备配置为路由两个或多个接口之间的流量的虚拟路由器。

逻辑接口

定义使用特定 虚拟局域网 (VLAN) 标记在标记的流量通过物理接口时处理流量的虚拟子接口。

密码套件列表

object，代表用于加密流量的多种密码套件。

命令行界面 (CLI)

3 系列和虚拟设备上受限制的基于文本的界面。命令行界面 (CLI) 用户可以根据用户分配到的访问级别运行系统。

默认操作

属于访问控制策略或 SSL 策略的一部分，此操作指定如何处理、检查和记录不符合策略中任何非监控器规则的流量。

目标设备

请参阅策略目标。

内部身份验证

一种在设备上的本地数据库中存储用户凭据的身份验证方法。用户登入设备时，系统将会针对数据库中的信息检查用户名和密码。与外部身份验证进行比较。

内联部署

FireSIGHT 系统的一种部署，其中受管设备以内联方式部署在网络上。在此配置中，设备可以影响网络流量。请与被动检测进行比较，在被动检测中您可以分析和响应流量，但不会影响流量。

内联集

一对或多对内联接口。

内联接口

为了处理内联部署中的流量而配置的一种检测接口。必须向内联集成对添加内联接口。

内置层

入侵策略或网络分析策略中的只读层。这些策略始终包括内置基本策略层；入侵策略也可以包括内置 FireSIGHT 建议层。

派生指纹

操作系统fingerprint，由系统通过应用公式，利用所有被动收集的指纹来为主机创建，该公式使用每个收集的指纹的置信值和标识之间的证实指纹数据的数量来计算最有可能的标识。

旁路模式

内联集的一种特性，如果组内的检测接口由于任何原因出现故障，它会让流量可以继续流动。

配置，用于导入或导出

一个配置集，如策略或自定义工作流程，在一台设备上创建，并且可从该设备导出，然后由另一设备导入。

签名 ID (Sid)

分配给每个入侵规则的唯一标识号 （也称为 Snort ID）。当您创建新规则或修改现有标准文本规则时，会赋予规则一个值为 1,000,000 或更大的 SID。FireSIGHT 系统附带的共享对象规则和标准文本规则的 SID 的值小于 1,000,000。此外，预处理器和解码器使用 SID 来标识它们检测到的不同类型的数据包。

情报源

定期更新的 IP 地址列表集合，思科 VRT 确定这些 IP 地址具有不良信誉。情报源中的每个列表代表一个特定类别：开放中继、已知攻击者、伪造 IP 地址 （虚假地址）等。在访问控制策略中，您可以通过安全情报将任意或所有类别列入黑名单。因为智能源会定期更新，使用智能源可以确保系统使用最新信息来过滤您的网络流量。

区域

请参阅安全区域。

全局白名单

一个安全情报对象，默认情况下包含在每个访问控制策略的安全情报白名单中。全局白名单适用于所有安全区域。您可以使用控制面板、 Context Explorer 和许多事件查看器页面中的 IP 地址上下文菜单，将单个 IP 地址添加至全局白名单。

全局黑名单

一个安全情报对象，默认情况下包含在每个访问控制策略的安全情报黑名单中。全局黑名单适用于所有安全区域。您可以使用控制面板、 Context Explorer 和许多事件查看器页面中的 IP 地址上下文菜单，将单个 IP 地址添加至全局黑名单。

任务队列

设备需要执行的工作的队列。当应用策略、安装软件更新以及执行其他长期的工作时，这些工作将加入队列中并且在 Task Status 页面显示它们的状态。 Task Status 页面提供工作的详细列表并且每隔十秒钟刷新一次来更新它们的状态。

入侵策略

可以配置用来检查网络流量的入侵和违反安全策略的情况的各种组件。网络流量满足访问控制规则中的条件时，您可以使用入侵策略检查该流量；您也可以将入侵策略与访问控制策略的默认操作关联。入侵策略的主要组件是检查流量的入侵规则和为网络分析策略中的关联预处理器选项生成事件的预处理器规则。您还可以添加可选 FireSIGHT 建议层，以及配置高级设置，以检查敏感数据或执行特殊入侵事件处理。入侵策略始终与变量集配对。

入侵规则

一组关键字和参数，将其应用于受监控网络流量时，其将识别潜在的入侵、违反安全策略的情况以及安全漏洞。系统将数据包与规则条件比较。如果数据包符合条件，规则触发并生成入侵事件。入侵规则包括丢弃规则和通过规则。

入侵检测和防御

对网络流量监控违反安全策略的情况，以及在内联部署中阻止或修改恶意流量的功能。在 FireSIGHT 系统中，当您用网络分析策略预处理流量时，要执行入侵检测和防御，然后将入侵策略与访问控制规则或默认操作关联。

入侵事件

记录违反入侵策略的情况的事件。入侵事件数据包括攻击出现的日期、时间和类型，以及有关攻击与其目标的其他背景信息。

入侵

在网络中出现的安全破坏、攻击或漏洞。

上下文菜单

一种弹出菜单， Web 界面的很多页面都提供此菜单，可以用作访问 FireSIGHT 系统中其他功能的快捷方式。此菜单的上下文取决于多个因素，包括当时查看的页面、当时调查的具体数据以及用户角色。

设备堆叠

请参阅堆栈。

设备集群

请参阅集群。

设备统计信息

您可以获得的关于设备的信息，包括运行时间、系统内存使用情况、负载平均值、磁盘使用情况、系统进程摘要以及防御中心上的关于数据相关器进程的信息。

设备

一个 FireSIGHT 系统防御中心、受管设备、具备 FirePOWER 服务的 Cisco ASA 防火墙 或用于 Blue Coat X-系列的思科 NGIPS。设备可以基于物理设备或软件。

设备

一种可提供一系列吞吐量的物理容错专门设计设备 （包括具备 FirePOWER 服务的 Cisco ASA 防火墙）或一种具有很多相同功能的基于软件的部署。根据您在设备上启用的许可功能，您可以使用它们来被动监控流量，从而构建网络资产、应用流量和用户活动的全面映射，以及执行访问控制。许多设备也可以执行交换、路由 （包括 DHCP 中继和 NAT）以及 VPN。您必须通过防御中心管理设备。

身份验证对象

一系列设置，您可以通过这些设置连接外部身份验证服务器，启用对 FireSIGHT 系统网络接口的外部身份验证 （RADIUS 或 LDAP）。

审核日志

与系统的用户交互的记录。审核日志包含审核事件。

审核事件

描述特定 FireSIGHT 系统用户交互的事件。每个审核事件包含时间戳、其操作生成事件的用户的名称、源 IP 地址以及描述事件的文本。审核事件记录在审核日志中。

生成器 ID (GID)

指示系统的哪个组件生成了入侵事件的一种编号。 GID 通过对事件类型进行分类，可以帮助您更有效地分析事件，其分类方式与规则的签名 ID (Sid)提供触发规则的数据包的上下文类似。

时间段

在任意事件视图中，施加给事件的时间约束。不同的事件视图可能拥有不同的默认时间段，具体情况取决于您的用户首选项。请注意，并非所有的事件视图都可以用时间来进行限制。

事故

一个或多个入侵事件，您怀疑这些事件可能涉及违反安全策略。系统提供有事故处理功能，您可以使用这些功能来收集和处理事故调查的相关信息。

事件查看器

用于查看和操作事件的系统组件。事件查看器使用工作流程来提供广泛事件视图，然后提供仅包含您感兴趣的事件、更加突出重点的事件视图。可以通过向下钻取整个工作流程或使用搜索功能，限制事件视图中的事件。

事件流处理器

请参阅eStreamer。

事件流量信道

请参阅流量信道。

事件

特定事件发生的相关详细信息的集合，您可以使用工作流程在事件查看器进行查看。事件可能表示网络上的攻击、受检测网络资产中的变更、违反组织安全和网络使用策略的情况等等。系统还会生成关于设备不断变化的运行状态、 Web 界面的使用、规则更新以及已启动的修复的信息的活动。最后，系统还会将其他信息显示为事件，即使这些“事件”不代表特定活动。例如，可以使用事件查看器查看关于受检测的主机、应用及其漏洞的详细信息。

事件抑制

一个功能，允许您在特定 IP 地址或 IP 地址范围触发入侵规则时抑制入侵事件。事件抑制对于消除误报非常有用。例如，如果您拥有一台邮件服务器，该服务器传输的数据包与特定攻击类似，对于该服务器触发的规则，您可以抑制事件，这样您只会看到真实攻击的事件。

事件阈值

一个功能，该功能允许您基于指定时段内生成的事件的数量，限制系统记录和显示入侵事件的次数。如果您收到了大量相同的事件，可以使用事件阈值。

受保护的网络

通过防火墙等设备保护不受用户或其他网络侵扰的组织内部网络。系统随附的许多入侵规则使用变量来定义受保护的网络和未受保护 （或外部）的网络。

受管设备

请参阅设备。

书签

通向事件分析中的特定位置和时间的已保存链接。书签保留有关以下各项的信息：您正在使用的工作流程、您正在查看的工作流程部分、您正在查看的工作流程内的页码、您选择的时间段、您禁用的所有列以及您施加的所有约束。

数据包视图

一种类型的工作流程页面，提供触发入侵规则的数据包或者生成入侵事件的预处理器的相关详细信息。数据包视图是基于入侵事件的工作流程中的最终页面。

数据库访问

允许第三方客户端以只读形式访问防御中心的一种功能。

数据相关器

一个程序，可使用系统收集的数据生成事件并在防御中心上创建网络映射。

私有密钥

仅成对公共密钥证书的所有者知道的加密密钥。公共密钥和私有密钥用于安全套接字层 (SSL)与传输层安全加密和解密。

私有搜索

特定表的搜索条件的命名集合，与您的用户帐户绑定。只有您和拥有管理员访问权限的用户可以使用您的私有搜索。

思科 VRT

思科的漏洞研究组。

思科云

请参阅综合安全智能云。

斯佩罗分析

将文件结构特征提交至综合安全智能云，以便进行恶意软件分析的一种方法。分析结果可以补充动态分析。

速率过滤

一种形式的异常检测，基于匹配流量的速率为规则设置新的入侵规则状态。

通过规则

一个入侵规则，触发时，不会生成入侵事件，也不会记录触发规则的数据包的详细信息。在特定的情况下，作为禁用入侵规则的替代方案，通过规则允许您防止符合特定条件的数据包生成事件。与丢弃规则进行比较。

通用访问卡 (CAC)

美国国防部颁发的用于 CAC 身份验证和授权的识别卡。

统一文件

一个二进制文件格式， FireSIGHT 系统用于记录事件数据。

透明内联模式

允许设备用作“线缆焊块”并转发其所检测到的所有网络流量 （不管其来源和目标）的一种高级内联集选项。

椭圆曲线 (EC) 密码技术

基于有限域内随机椭圆曲线上计算点的一种加密方法。请与 RSA 密码技术对比。

外部身份验证

当用户登录至 FireSIGHT 系统设备时，使用外部存储的用户凭据来对用户名和密码进行身份验证的方法 （例如 LDAP 身份验证或 RADIUS 身份验证）。与内部身份验证进行比较。

网络对象

可重用的object，表示一个或多个 IP 地址、 CIDR 块或前缀长度。

网络发现策略

指定针对特定网段，包括由支持 NetFlow 的设备监控的网络，系统收集的发现数据种类的策略（包括主机、用户和应用数据）。网络发现策略还可以管理标识冲突解决首选项、主动检测源优先级以及威胁表现 (IOC)。

网络发现

请参阅发现。

网络分析策略

您可以配置的各种预处理器，用于解码、规范化和预处理网络流量，以备以后由入侵策略进行分析。默认情况下，单一系统提供的网络分析策略预处理访问控制策略处理的所有流量。但是，您可以选择自定义网络分析策略，以执行此预处理。高级用户可以使用网络分析规则来允许多个自定义网络分析策略根据安全区域、网络或 VLAN 标记预处理流量。

网络分析规则

一组条件，高级 FireSIGHT 系统用户可以将其用于通过多个自定义网络分析策略执行目标预处理。在访问控制策略中，将网络分析规则配置为高级选项。

网络设备

在 FireSIGHT 系统中指被识别为网桥、路由器、 NAT 设备或负载均衡器的主机。

网络文件轨迹

对主机在整个网络传输文件时的文件路径的直观表示。对于具有关联的 SHA-256 哈希值的任意文件，轨迹图会显示传输过文件的所有主机的 IP 地址、检测到文件的时间、文件的恶意软件性质、关联的文件事件和恶意事件等。

网络应用

展示 HTTP 流量的内容或为其请求获取的 URL 的一种应用。

网络映射

对网络的详细展现。网络映射允许您查看关于在您网络上运行的主机、移动设备和网络设备的网络拓扑，以及与它们关联的主机属性、应用协议和漏洞。

威胁表现 (IOC)

在网络发现策略中配置的一种功能，其中系统会将 FireAMP 终端数据与受监控网络中的主机相关联。可能受到危害的主机会标有用于指示其状态的标记，这些标记在主机配置文件和相关事件视图中可见。

威胁评分

作为将文件提交至综合安全智能云进行动态分析的结果而分配给文件的 1-100 的评分，该评分可以度量文件包含恶意软件的可能性。

违反安全策略的情况

安全破坏、攻击、漏洞，或者其他不当的网络使用方式。

未知主机

一个主机，系统已分析其流量，但其操作系统与任何已知的 fingerprint 均不匹配。与无法识别的主机进行比较。

文件捕获

请参阅捕获的文件。

文件策略

系统用来执行文件控制和基于网络的高级恶意软件防护的策略。文件策略由文件规则填充，通过访问控制策略内的访问控制规则调用。

文件存储

请参阅存储的文件。

文件规则

FireSIGHT 系统用于检查网络流量的文件策略内的条件集合。如果传输的文件与规则条件匹配，规则会触发并会生成文件事件。文件规则操作决定您是阻止文件（基于文件类型或恶意软件性质），还是只是允许文件通过并记录传输。

文件规则操作

一个设置，决定系统如何处理符合文件规则条件的文件。您可以检测特定的文件类型，针对其发出警报，以及阻止这些文件的传输。您还可以针对这些文件类型的子集执行恶意软件云查找，并基于恶意软件性质阻止这些文件的传输。

文件轨迹

请参阅网络文件轨迹。

文件控制

作为访问控制组成部分的一种功能，允许指定和记录可以流经网络的文件的类型。

文件类别

文件类型的一般分类，例如图形文件、可执行文件或存档文件。

文件类型

具体的文件格式类型，例如 PDF、 EXE 或 MP3。

文件列表

请参阅干净列表和自定义检测列表。

文件事件

一个事件，代表由受管设备在网络流量中检测到的文件。

文件性质

请参阅恶意软件性质。

无法识别的主机

一个主机，系统因尚未收集到关于该主机的足够信息而无法识别其操作系统。与未知主机进行比较。

无旁路模式

内联集的一种特性，如果集合内的检测接口由于任何原因出现故障，它会阻止流量。

无人值守管理 (LOM)

一个3 系列 功能，您可以通过此功能使用带外 LAN 上串行 (SOL) 管理连接来远程监控或管理特定设备，而无需登录至设备的 Web 界面。可以执行有限的任务，例如查看机箱序列号或监控风扇转速和温度等情况。

物理接口

代表 NetMod 上物理端口的接口。

系统策略

对于部署中的多个设备来说类似的设置，例如邮件中继主机首选项和时间同步设置等。使用防御中心将系统策略应用到自身及其受管设备上。

相关性

一个功能，您可以用来构建可实时响应您网络上的威胁的关联策略。有相关性的修复组件提供灵活的 API，可以使用此 API 创建和上载自定义补救模块以回应违反策略的情况。

向下钻取页面

一个中间工作流程页面，用于约束事件视图。通常，向下钻取页面会提供约束，您可以选择约束以便前进至更严格约束的页面或表视图。

效率低下

对关联策略的反应，可以是警报或修复。

信誉 (URL)

请参阅URL 信誉。

信誉 （IP 地址）

请参阅安全情报。

性质

请参阅恶意软件性质。

修复

降低系统的潜在攻击的操作。您可以配置补救，并且在关联策略内将其与关联规则和合规性白名单关联，以便在其触发时，防御中心可以启动补救。这不仅可以在您没有时间处理攻击的时候减轻攻击，而且可以确保系统保持符合组织的安全策略。防御中心附带有预定义的补救模块，而且您也可以使用灵活的 API 来创建自定义补救。

虚拟防御中心

可以在虚拟宿主环境中在设备上部署的防御中心。

虚拟交换机

处理通过网络的出站和入站流量的一组交换接口。在第 2 层部署中，可以在受管设备上配置虚拟交换机，用作独立广播域，将网络分为不同逻辑分段。虚拟交换机使用来自主机的媒体访问和控制 (MAC) 地址确定向哪里发送数据包。

虚拟局域网 (VLAN)

VLAN 不是按地理位置而是按其他一些条件映射主机，例如按部门或主要用途。受监控的主机的主机配置文件显示与主机关联的所有 VLAN 信息。最内部的 VLAN 标记信息也包括在各种事件内。系统还可以根据连接的 VLAN 标记执行多种类型的流量处理，包括访问控制。在第 2 层和第 3 层部署中，您可以在受管设备上配置虚拟交换机和虚拟路由器，以便适当地处理带有 VLAN 标记的流量。

虚拟路由器

路由第 3 层流量的一组路由接口。在第 3 层部署中，可以通过依据目标 IP 地址制定数据包转发决策将虚拟路由器配置为路由数据包。可以定义静态路由，配置路由信息协议 (RIP) 和开放最短路径优先 (OSPF) 动态路由协议以及实施网络地址转换 (NAT)。

虚拟设备

可以在虚拟宿主环境中在设备上部署的受管设备。虚拟设备不支持基于硬件的功能，如高可用性、集群、堆栈、 NAT、 VPN 和 Fast-Path 规则，而且您无法将虚拟设备配置为虚拟交换机或虚拟路由器。

业务相关性

应用被用于组织的企业运营中 （而不是被用于娱乐目的）的可能性。应用的业务相关性的取值范围为极低到极高。

移动设备

在 FireSIGHT 系统中是指被发现功能识别为移动、手持设备的主机 （例如手机或平板电脑）。系统通常可以检测移动设备是否被越狱。

抑制

请参阅事件抑制。

应用标记

其应用类别未涵盖的应用相关信息。例如，视频流网络应用通常带有标记“高带宽”和“显示广告”，应用可能拥有任意数量的标记，包括无标记。

应用风险

应用的使用可能会违反组织的安全策略的可能性。应用风险的取值范围为极低到极高。

应用过滤器

按照与应用风险、业务相关性、类型、类别和标记关联的条件分组的一个或多个应用。您可以在对象管理器中创建应用过滤器。

应用

检测到的网络资产、通信方法或 HTTP 内容。系统可检测三种类型的应用：应用协议、客户端应用和网络应用。

应用检测器

系统用于识别您网络上的应用的工具。应用检测器通过数据包包头中的 ASCII 或十六进制模式、流量使用的端口或者二者来识别应用。思科可能会通过系统更新、漏洞数据库更新或者导入/导出功能提供其他的检测器。您也可以创建您自己的应用协议检测器。

应用控制

一种功能，是访问控制的组成部分，允许指定哪些应用流量可以流经网络。

应用类别

应用的一般分类，描述其最基本的功能。每个应用都至少归属于一个类别。

应用类型

应用是应用协议、客户端应用，还是网络应用。

应用

使策略或对该策略的更改生效所采取的操作。可以将防御中心的大多数策略应用到其受管设备上；但是，可以激活和停用相关性策略，因为它们不涉及对受管设备的配置的更改。

应用协议

一种应用，描述服务器与主机上的客户端应用通信期间检测到的应用协议流量；例如 SSH 或 HTTP。

应用业务相关性

请参阅业务相关性。

影响

针对入侵事件，入侵数据、发现数据和漏洞信息之间的关联的编号指标。影响级别 1（红色影响图标）表示目标主机 *容易遭受*入侵事件所代表的攻击，影响级别 2（橙色影响图标）表示该主机 *可能容易遭受攻击*，诸如此类。针对未受网络发现策略监控的网络上的主机的攻击为影响级别 0（灰色影响图标），指示防御中心无法确定事件的影响。

用户标识

请参阅用户。

用户层

入侵策略中的一个 层，您可以在其中修改该策略中的设置。

用户代理

在服务器上安装的代理，用于在用户登录网络或出于任何其他原因按照 Active Directory 凭据进行身份验证时监控用户。访问受控用户的活动只有在用户代理报告该活动时才会用于访问控制。

用户感知

一个功能，该功能允许组织将威胁、终端和网络情报与用户标识信息关联，这使得您可以执行用户控制。

用户感知对象

一系列设置，通过这些设置可以连接到 LDAP 服务器，对在网络流量中检测到其活动或被用户代理检测到其活动的用户检索其元数据。如果贵组织使用 Microsoft Active Directory，用户感知对象还可以指定访问受控用户。

用户活动

当系统检测到有用户登录或注销 （或者，包括某些失败的登录尝试）或者有用户记录被添加到防御中心数据库或从其中删除时生成的事件。

用户角色

对 FireSIGHT 系统的用户授予的访问级别。例如，对于事件分析师、管理 FireSIGHT 系统的管理员、使用第三方工具访问防御中心数据库的用户等等，可以授予不同的 Web 界面访问权限。还可以创建具备特殊访问权限的自定义用户角色。

用户角色升级

您可以赋予自定义用户角色的一个权限，该权限允许用户在登录会话期间，输入密码来获得另一用户角色的权限。

用户控制

作为访问控制组成部分的一种功能，允许指定和记录可以流经网络的用户关联流量。

用户历史记录

主机过去二十四小时的用户活动的图形表示。您可以在主机的主机配置文件中查看的用户历史记录，会显示检测到登入主机的用户的用户名，以及以条形图表示的登录和注销的近似次数。

用户

网络活动已被受管设备或用户代理检测到的用户。

用户详细信息

用户标识和用户活动工作流程的最终页面。连同关于用户的一般信息，用户详细信息页面还会显示主机历史记录，此历史记录是过去二十四小时的用户活动的图形表示。

用户证书

一份加密证书，向 FireSIGHT 系统网络服务器提供用户浏览器标识信息，从而允许服务器对用户标识进行二次验证。该证书必须由为设备颁发服务器证书的相同证书颁发机构颁发。

用于 Blue Coat X-系列的思科 NGIPS

基于软件的应用，建立在 Blue Coat的基于机架的可扩展系统之上，该系统提供虚拟设备的大多数功能。

预处理器规则

与预处理器或端口扫描流量探测器关联的入侵规则。如果想要预处理器规则生成事件，必须启用预处理器规则。预处理器规则有预处理器特定的生成器 ID (GID)。

预处理器事件

一种类型的入侵事件，数据包触发指定预处理器选项时生成。预处理器事件可以帮助您检测异常协议攻击。

预处理器

准备流量以便进行进一步入侵和漏洞检查的系统组件。预处理器规范化流量并通过识别不适当的报头选项、分片重组 IP 数据报、提供 TCP 状态检查和数据流重组以及验证校验和，帮助识别网络层和传输层协议异常。预处理器可以用系统可以分析的格式直接显示特定类型的数据包数据；这些预处理器叫做数据规范化预处理器或应用层协议预处理器。系统可通过规范化应用层协议编码有效地将相同的与内容相关的入侵规则应用于采用不同数据表示形式的数据包并获取有意义的结果。每当数据包触发配置的预处理器选项时，预处理器都会生成预处理器事件。预处理器要求具备特定专业知识才能进行配置，通常只需要很少修改或无需修改，并且不是每个部署都通用。

阈值

请参阅事件阈值。

源

请参阅安全情报源。

云服务

请参阅综合安全智能云。

运行状况监控

持续监控部署中的设备性能的一种功能。运行状况监控功能在应用的健康策略内使用运行状况模块来测试设备。

运行状况监控黑名单

一个配置，可以临时禁用运行状况监控的某些方面，以便防止生成不必要的运行状况事件。您可以禁用设备组、单台设备或特定运行状况模块的监控。

运行状况模块

对部署中的设备的 CPU 使用情况或可用磁盘空间等特定性能进行的一种测试。您在健康策略中启用的运行状况模块在它们监控的性能方面达到特定水平时，会生成运行状况事件。

运行状况事件

一个事件，您的部署中的某个设备满足 （或未能满足）运行状况模块中指定的性能条件时生成。运行状况事件还可以生成警报。

暂停期

一个以秒、分钟或小时为单位指定的间隔，关联规则触发后，在该间隔内，系统停止触发该规则，即便在该间隔内该规则被再次违反。暂停期结束后，该规则可以再次触发 （然后开始一个新的暂停期）。另请参阅非活动期。

证书颁发机构

用于创建服务器证书或用户公共密钥证书的证书颁发者。服务器和用户证书提供服务器或用户标识的额外确认。

证书撤销列表 (CRL)

为您的设备发行用户证书的证书颁发机构已撤销证书的列表。这使得您可以使用客户端浏览器证书检查来限制对 FireSIGHT 系统 Web 界面的访问。如果用户选择在 CRL 中列为已撤销证书的证书，浏览器将无法加载 Web 界面。在SSL 检查期间，设备可以检测到 CRL 上的公共密钥证书，并且不会信任已加密的流量。

终端

计算机或移动设备，其中用户在上面安装了 FireAMP 连接器，作为组织高级恶意软件防护战略的一部分。

主动检测

使用主动源发现主机、应用和用户信息。主动源包括诸如 Nmap 的扫描器、至系统 Web 界面的用户输入或者使用使用命令行或第三方应用 API 调用的至网络映射的主机输入。与被动检测进行比较。

主机历史记录

过去 24 小时内的用户活动的图形表示。您可以在用户的用户详细信息中查看的主机历史记录会显示用户登入的主机的 IP 地址，以及以条形图表示的登录和注销的近似次数。

主机配置文件

收集到的特定已检测到的主机的相关信息。这包括一般主机信息 （例如主机名和操作系统）以及在主机上运行的协议和应用。主机配置文件可能还包括该主机的用户历史记录、主机属性、虚拟局域网 (VLAN) 信息、适用的白名单违规、检测到的漏洞、威胁表现 (IOC) 以及扫描结果。

主机配置文件限定条件

对流量变曲线或关联规则施加的约束。关联规则内的主机配置文件限定条件指定防御中心应仅当涉及的主机满足特定条件时才生成关联事件。流量配置文件中的主机配置文件限定条件可以限制会被配置的主机。

主机视图

工作流程中显示发现事件或网络资产的最终页面。主机视图显示您正在查看的事件或资产涉及的主机的 主机配置文件。

主机输入

一种功能，您可以通过此功能使用脚本或命令行文件从第三方来源导入数据，以便补充网络映射中的信息。 Web 界面也提供一些主机输入功能；可以修改操作系统或应用协议标识、验证或阻止漏洞以及从网络映射删除各种项目，包括客户端和服务器端口。

主机输入事件

一种发现事件，您使用主机输入功能时生成。通常，系统会以相同方式处理主机输入和被动发现事件，尽管在构建关联规则时，它们会被区分开来。

主机属性

一个您可用于提供系统检测到的主机的相关信息的工具，该工具可将这些信息以对您网络环境而言十分重要的方式进行分类。系统拥有两个预定义的主机属性，主机重要性与注释，以及指示每个主机对于每个活动合规性白名单的合规性的主机属性。您也可以创建自己的主机属性。

主机

与网络连接并且具有独一无二 IP 地址的一种设备。对于 FireSIGHT 系统，主机是指未被分类为移动设备、网桥、路由器、 NAT 设备或负载均衡器的任何已识别的主机。

主机重要性

一个主机属性，指示系统检测到的任意给定主机的业务重要性。

状态共享

一个功能，允许集群设备或堆叠进行同步，以便在设备或堆栈发生故障时，对等设备可以在不中断流量的情况下接管工作。状态共享可以确保严格 TCP 强制、单向访问控制规则、阻止暂留以及动态 NAT 可以正确地故障转移。

追溯性恶意软件事件

基于网络的恶意事件，先前检测到的文件的恶意软件性质变化时生成。发生这种情况时，系统还会更新共享追溯性事件的 SHA-256 哈希值的文件性质和恶意软件。

子服务器

被相同主机上的另一服务器调用的服务器。

自定义表

您可以构造的表，该表可以结合来自 FireSIGHT 系统附带的两个或更多预定义表的字段。例如，您可以将来自主机属性表的主机重要性信息与来自连接数据表的信息结合起来，以便在新的上下文中检查连接数据。

自定义工作流程

为满足组织的独特需求而创建的工作流程。

自定义检测列表

由其 SHA-256 哈希值所代表的文件的列表。当系统检测到列表中的某个文件时，不会执行恶意软件云查找，将该文件视为恶意软件，即便综合安全智能云中该文件的性质是干净文件也是如此。

自定义拓扑

一个功能，允许您有意地组织和标识主机、移动设备和网络设备网络映射中的子网。

自定义用户角色

具有专用访问权限的用户角色。自定义用户角色可以具有任何基于菜单的权限和系统权限，并且可以是完全原创的或基于预定义的用户角色。

自定义指纹

请参阅 fingerprint。

自动应用旁路 (AAB)

一个高级设备设置，该设置限制允许用于处理通过接口的数据包的时间，如果超过该时间，将允许数据包绕过处理。

自适应配置文件

建议用于被动部署，这是一种访问控制策略高级设置，其使用发现数据确定数据包的目标主机的操作系统。确定网络分析策略内的配置文件目标，然后以目标主机上操作系统相同的方式分片重组 IP 数据包并重组数据流。然后，入侵策略分析与目标主机所使用格式相同格式的数据。

综合安全智能云

有时称为*云服务*或*思科云*，是一种 思科托管服务器，防御中心可从中获得最新的相关信息，包括恶意软件、安全情报和 URL 过滤数据。另请参阅恶意软件云查找和 FireAMP 私有云。