思科 ASA 系列防火墙 CLI 配置指南

软件版本 9.3

发布日期：2014 年 7 月 24 日
更新日期：2014 年 9 月 16 日

Cisco Systems, Inc.
www.cisco.com

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

文本部件号：不适用，仅在线提供

思科 ASA 系列防火墙 CLI 配置指南

目 录

关于本指南 xvii

文档目的 xvii

相关文档 xvii

约定 xvii

获取文档和提交服务请求 xviii

第 1 部分 服务策略和访问控制

第 1 章 使用模块化策略框的服务策略 1-1

关于服务策略 1-1

服务策略的组成部分 1-2

使用服务策略配置的功能 1-3

功能方向性 1-4

服务策略内的功能匹配 1-5

应用多项功能操作的顺序 1-5

某些功能操作的不兼容性 1-6

多项服务策略的功能匹配 1-7

服务策略准则 1-7

服务策略的默认设置 1-8

服务策略默认配置 1-9

默认类映射（流量类） 1-10

配置服务策略 1-10

识别流量（第 3/4 层类映射） 1-12

定义操作（第 3/4 层策略映射） 1-14

将操作应用到接口（服务策略） 1-16

监控服务策略 1-17

服务策略示例（模块化策略框架） 1-17

将检测和 QoS 策略管制应用到 HTTP 流量 1-17

将检测全局应用到 HTTP 流量 1-18

将检测和连接限制应用到流向特定服务器的 HTTP 流量 1-18

通过 NAT 将检测应用到 HTTP 流量 1-19

服务策略历史 1-20

第 2 章 应用检测的特殊操作（检测策略映射） 2-1
检测策略映射有关信息 2-1
准则和限制 2-2
默认检测策略映射 2-3
在检测策略映射中定义操作 2-4
在检测类映射中识别流量 2-5
更多信息指南 2-7
检测策略映射的功能历史 2-7

第 3 章 访问规则 3-1
控制网络访问 3-1
有关规则的一般信息 3-2
扩展访问规则 3-4
以太网类型规则 3-5
访问控制准则 3-6
配置访问控制 3-7
配置访问组 3-7
配置 ICMP 访问规则 3-8
监控访问规则 3-9
评估访问规则的系统日志消息 3-9
允许或拒绝网络访问的配置示例 3-10
访问规则历史记录 3-11

第 2 部分 网络地址转换

第 4 章 网络地址转换 (NAT) 4-1
为何使用 NAT? 4-1
NAT 术语 4-2
NAT 类型 4-2
NAT 类型概述 4-3
静态 NAT 4-3
动态 NAT 4-8
动态 PAT 4-10
身份标识 NAT 4-11
路由和透明模式下的 NAT 4-11
路由模式下的 NAT 4-12
透明模式下的 NAT 4-12

NAT 和 IPv6 4-14
如何实施 NAT 4-14
网络对象 NAT 和两次 NAT 之间的主要差异 4-14
网络对象 NAT 4-15
两次 NAT 4-15
NAT 规则顺序 4-18
NAT 接口 4-20
路由 NAT 数据包 4-20
映射地址和路由 4-20
远程网络的透明模式路由要求 4-23
确定出口接口 4-23
面向 VPN 的 NAT 4-23
NAT 和远程访问 VPN 4-24
NAT 和站点到站点 VPN 4-26
NAT 和 VPN 管理访问 4-28
NAT 和 VPN 故障排除 4-30
DNS 和 NAT 4-30
DNS 回复修改，外部接口上的 DNS 服务器 4-31
独立网络上的 DNS 回复修改、DNS 服务器、主机和服务器 4-32
DNS 回复修改，主机网络上的 DNS 服务器 4-33
使用外部 NAT 进行 DNS64 回复修改 4-34
PTR 修改，主机网络上的 DNS 服务器 4-35
更多信息指南 4-35

第 5 章 网络对象 NAT 5-1
有关网络对象 NAT 的信息 5-1
网络对象 NAT 的许可要求 5-2
网络对象 NAT 的先决条件 5-2
准则和限制 5-2
默认设置 5-3
配置网络对象 NAT 5-3
为映射地址添加网络对象 5-4
使用 PAT 池配置动态 NAT 5-5
配置动态 PAT（隐藏） 5-7
配置静态 NAT 或带有端口转换的静态 NAT 5-10
配置身份标识 NAT 5-12
配置每会话 PAT 规则 5-13
监控网络对象 NAT 5-15

网络对象 NAT 配置示例 5-15
提供到内部网络服务器的访问（静态 NAT） 5-16
面向内部主机的 NAT（动态 NAT）和面向外部网络服务器的 NAT（静态 NAT） 5-17
有多个映射地址的内部负载平衡器（静态 NAT，一对多） 5-18
用于 FTP、HTTP 和 SMTP（带端口转换的静态 NAT）的单一地址 5-19
映射接口上的 DNS 服务器、实际接口上的网络服务器（带 DNS 修改的静态 NAT） 5-20
映射接口上的 DNS 服务器和 FTP 服务器，FTP 服务器已转换（带 DNS 修改的静态 NAT） 5-22
映射接口上的 IPv4 DNS 服务器和 FTP 服务器，实际接口上的 IPv6 主机（带 DNS64 修改的静态 NAT64） 5-23
网络对象 NAT 的功能历史 5-24

第 6 章 两次 NAT 6-1
有关两次 NAT 的信息 6-1
两次 NAT 的许可要求 6-2
两次 NAT 的先决条件 6-2
准则和限制 6-2
默认设置 6-4
配置两次 NAT 6-4
为真实和映射地址添加网络对象 6-4
（可选）为真实和映射端口添加服务对象 6-6
配置动态 NAT 6-7
配置动态 PAT（隐藏） 6-10
配置静态 NAT 或带有端口转换的静态 NAT 6-14
配置身份标识 NAT 6-17
配置每会话 PAT 规则 6-19
监控两次 NAT 6-19
两次 NAT 的配置示例 6-19
取决于目标的不同转换（动态 PAT） 6-20
取决于目标地址和端口的不同转换（动态 PAT） 6-21
两次 NAT 的功能历史记录 6-22

第 3 部分 应用检查

第 7 章 应用层协议检测入门 7-1
应用层协议检测 7-1
检测引擎如何工作 7-1
何时使用应用协议检测 7-2

检测策略映射 7-3
应用检测准则 7-4
应用检测的默认操作 7-5
默认检测和 NAT 限制 7-5
默认检测策略映射 7-8
配置应用层协议检测 7-9
选择要检测的正确流量类 7-12
配置正则表达式 7-13
创建正则表达式 7-13
创建正则表达式类映射 7-16
应用检测历史记录 7-16

第 8 章 基本互联网协议检测 8-1
DNS 检测 8-1
DNS 检测操作 8-2
DNS 检测的默认设置 8-2
配置 DNS 检测 8-2
监控 DNS 检测 8-7
FTP 检测 8-8
FTP 检测概述 8-8
严格 FTP 8-8
配置 FTP 检测 8-9
验证和监控 FTP 检测 8-13
HTTP 检测 8-13
HTTP 检测概述 8-13
配置 HTTP 检测 8-14
ICMP 检测 8-19
ICMP 错误检测 8-19
即时消息检测 8-20
配置即时消息检测策略映射 8-20
配置 IM 检测服务策略 8-22
IP 选项检测 8-24
IP 选项检测概述 8-24
IP 选项检测的默认设置 8-25
配置 IP 选项检测 8-25
监控 IP 选项检测 8-27
IPsec 穿透检测 8-27
IPsec 穿透检测概述 8-27

配置 IPsec 穿透检测 8-28
IPv6 检测 8-30
IPv6 检测的默认设置 8-30
配置 IPv6 检测 8-31
NetBIOS 检测 8-34
为其他检测控制配置 NetBIOS 检测策略映射 8-34
配置 NetBIOS 检测服务策略 8-35
PPTP 检测 8-36
SMTP 检测和扩展 SMTP 检测 8-36
SMTP 检测和 ESMTP 检测概述 8-37
ESMTP 检测的默认设置 8-37
配置 ESMTP 检测 8-38
TFTP 检测 8-42

第 9 章 **语音和视频协议的检测 9-1**
CTIQBE 检测 9-1
CTIQBE 检测的局限性 9-1
验证和监控 CTIQBE 检测 9-2
H.323 检测 9-3
H.323 检测概述 9-3
H.323 如何工作 9-3
H.245 消息中的 H.239 支持 9-4
H.323 检测的局限性 9-5
配置 H.323 检测 9-5
配置 H.323 和 H.225 超时值 9-9
验证和监控 H.323 检测 9-9
MGCP 检测 9-11
MGCP 检测概述 9-11
配置 MGCP 检测 9-12
配置 MGCP 超时值 9-15
验证和监控 MGCP 检测 9-15
RTSP 检测 9-16
RTSP 检测概述 9-16
RealPlayer 配置要求 9-16
RSTP 检测的局限性 9-17
配置 RTSP 检测 9-17
SIP 检测 9-20
SIP 检测概述 9-21

SIP 检测的局限性 9-21
SIP 即时消息 9-22
默认 SIP 检测 9-22
配置 SIP 检测 9-23
配置 SIP 超时值 9-27
验证和监控 SIP 检测 9-27
瘦客户端 (SCCP) 检测 9-28
SCCP 检测概述 9-28
支持思科 IP 电话 9-28
SCCP 检测的局限性 9-29
默认 SCCP 检测 9-29
配置 SCCP（瘦客户端）检测 9-29
验证和监控 SCCP 检测 9-32
语音和视频协议检测的历史记录 9-33

第 10 章 数据库和目录协议的检测 10-1
ILS 检测 10-1
SQL*Net 检测 10-2
Sun RPC 检测 10-3
Sun RPC 检测概述 10-3
管理 Sun RPC 服务 10-3
验证并监控 Sun RPC 检测 10-4

第 11 章 管理应用协议检测 11-1
DCERPC 检测 11-1
DCERPC 概述 11-1
配置 DCERPC 检测 11-2
GTP 检测 11-4
GTP 检测概述 11-5
GTP 检测的默认设置 11-5
配置 GTP 检测 11-6
验证和监控 GTP 检测 11-10
RADIUS 计费检测 11-11
RADIUS 计费检测概述 11-11
配置 RADIUS 计费检测 11-11
RSH 检测 11-14
SNMP 检测 11-14
XDMCP 检测 11-16

第 4 部分 连接设置和服务质量

第 12 章 连接设置 12-1

有关连接设置的信息 12-1
TCP 拦截和限制半开连接 12-2
因无客户端 SSL 兼容性而禁用管理数据包的 TCP 拦截 12-2
死连接检测 (DCD) 12-2
TCP 序列随机化 12-2
TCP 规范化 12-3
TCP 状态旁路 12-3
连接设置的许可要求 12-4
准则和限制 12-4
默认设置 12-5
配置连接设置 12-5
配置连接设置的任务流 12-5
用 TCP 映射自定义 TCP 规范器 12-6
配置连接设置 12-9
监控连接设置 12-12
连接设置的配置示例 12-12
连接限制和超时的配置示例 12-12
TCP 状态旁路的配置示例 12-13
TCP 规范化的配置示例 12-13
连接设置的功能历史 12-13

第 13 章 服务质量 13-1

关于 QoS 13-1
支持的 QoS 功能 13-2
什么是令牌桶？ 13-2
策略管制 13-2
优先级队列 13-2
QoS 功能如何相互作用 13-3
DSCP（区分服务）保留 13-3
QoS 准则 13-3
配置 QoS 13-4
确定优先级队列的队列和传输环路限制 13-4
配置接口的优先级队列 13-5
配置优先级队列和策略管制的服务规则 13-6
监控 QoS 13-8

QoS 策略统计信息 13-9
QoS 优先级统计信息 13-9
QoS 优先级队列统计信息 13-9
优先级队列和策略管制的配置示例 13-10
VPN 流量的类映射示例 13-10
优先级和策略管制示例 13-11
QoS 的历史记录 13-12

第 14 章 连接和资源故障排除 14-1
测试配置 14-1
启用 ICMP 调试消息和系统日志消息 14-1
ping ASA 接口 14-2
通过 ASA 传输流量 14-4
禁用测试配置 14-5
使用 traceroute 功能确定数据包路由 14-5
使用数据包跟踪器跟踪数据包 14-6
监控每个进程的 CPU 使用情况 14-7

第 5 部分 高级网络保护

第 15 章 ASA 和思科云网络安全 15-1
有关思科云网络安全的信息 15-2
网络流量重定向到云网络安全 15-2
用户身份验证和云网络安全 15-2
身份验证密钥 15-2
ScanCenter 策略 15-3
云网络安全操作 15-4
通过白名单绕过扫描 15-5
IPv4 和 IPv6 支持 15-5
从主用代理服务器到备用代理服务器的故障转移 15-5
思科云网络安全的许可证要求 15-6
云网络安全先决条件 15-6
准则和限制 15-6
默认设置 15-7
配置思科云网络安全 15-7
配置与云网络安全代理服务器的通信 15-7
（多情景模式）根据安全情景允许云网络安全 15-8
配置服务策略，将流量发送到云网络安全 15-9

（可选）配置白名单流量 15-13
（可选）配置用户身份监控 15-14
配置云网络安全策略 15-14
监控云网络安全 15-15
思科云网络安全配置示例 15-16
单一模式示例 15-16
多模式示例 15-17
白名单示例 15-17
目录集成示例 15-18
带身份防火墙的云网络安全示例 15-20
相关文档 15-23
功能历史思科云网络安全 15-24

第 16 章 威胁检测 16-1
检测威胁 16-1
基础威胁检测统计信息 16-2
高级威胁检测统计信息 16-2
扫描威胁检测 16-2
威胁检测准则 16-3
威胁检测的默认设置 16-3
配置威胁检测 16-4
配置基础威胁检测统计信息 16-5
配置高级威胁检测统计信息 16-5
配置扫描威胁检测 16-7
监控威胁检测 16-7
监控基础威胁检测统计信息 16-8
监控高级威胁检测统计信息 16-8
评估主机威胁检测统计信息 16-10
监控被避开的主机、攻击者和攻击目标 16-11
威胁检测示例 16-12
威胁检测历史 16-12

第 6 部分 ASA 模块

第 17 章 ASA FirePOWER (SFR) 模块 17-1
ASA FirePOWER 模块 17-1
ASA FirePOWER 模块如何与 ASA 配合使用 17-2
ASA FirePOWER 管理访问权限 17-3

与 ASA 功能的兼容性 17-4
ASA FirePOWER 模块的许可要求 17-5
ASA FirePOWER 的准则 17-5
ASA FirePOWER 的默认设置 17-5
配置 ASA FirePOWER 模块 17-6
连接 ASA FirePOWER 管理接口 17-6
（ASA 5512-X 至 5555-X）安装或重新映像软件模块 17-9
更改 ASA FirePOWER 管理 IP 地址 17-12
在 ASA FirePOWER CLI 处配置基本 ASA FirePOWER 设置 17-13
向 FireSIGHT 管理中心添加 ASA FirePOWER 17-14
在 ASA FirePOWER 模块上配置安全策略 17-15
向 ASA FirePOWER 模块重定向流量 17-15
管理 ASA FirePOWER 模块 17-17
重置密码 17-17
重新加载或重置模块 17-18
关闭模块 17-18
（适用于 ASA 5512-X 至 ASA 5555-X）卸载软件模块映像 17-18
（ASA 5512-X 至 ASA 5555-X）从 ASA 向模块发起会话 17-19
重新映像 5585-X ASA FirePOWER 硬件模块 17-19
升级系统软件 17-21
监控 ASA FirePOWER 模块 17-21
显示模块状态 17-21
显示模块统计信息 17-23
监控模块连接 17-23
ASA FirePOWER 模块的示例 17-24
ASA FirePOWER 模块的历史记录 17-25

第 18 章 **ASA CX 模块** 18-1
ASA CX 模块 18-1
ASA CX 模块如何与 ASA 配合使用 18-2
ASA CX 管理访问 18-4
用于主动活动身份验证的身份验证代理 18-4
与 ASA 功能的兼容性 18-5
ASA CX 模块的许可要求 18-5
ASA CX 的先决条件 18-5
ASA CX 的准则 18-5
ASA CX 的默认设置 18-7
配置 ASA CX 模块 18-7

连接 ASA CX 管理接口 18-7
（适用于 ASA 5512-X 至 ASA 5555-X）安装或重新映像软件模块 18-10
（适用于 ASA 5585-X）更改 ASA CX 管理 IP 地址 18-12
配置 ASA CX 基本设置 18-12
在 ASA CX 模块上配置安全策略 18-14
配置身份验证代理端口 18-14
向 ASA CX 模块重定向流量 18-14
管理 ASA CX 模块 18-17
重置密码 18-17
重新加载或重置模块 18-18
关闭模块 18-18
（ ASA 5512-X 至 ASA 5555-X）卸载软件模块映像 18-18
（ASA 5512-X 至 ASA 5555-X）从 ASA 向模块发起会话 18-19
监控 ASA CX 模块 18-19
显示模块状态 18-19
显示模块统计信息 18-20
监控模块连接 18-20
对身份验证代理进行故障排除 18-21
ASA CX 模块的示例 18-22
ASA CX 模块的历史 18-23

第 19 章 **ASA IPS 模块** 19-1
有关 ASA IPS 模块的信息 19-1
ASA IPS 模块如何与 ASA 配合使用 19-1
操作模式 19-2
使用虚拟传感器 19-3
有关管理访问权的信息 19-4
ASA IPS 模块的许可要求 19-5
准则和限制 19-5
默认设置 19-6
配置 ASA IPS 模块 19-6
ASA IPS 模块的任务流 19-6
连接 ASA IPS 管理接口 19-7
从 ASA 向模块发起会话 19-10
（ASA 5512-X 至 ASA 5555-X）启动软件模块 19-11
配置基本 IPS 模块网络设置 19-11
配置 ASA IPS 模块上的安全策略 19-12
向安全情景分配虚拟传感器 19-13

将流量转移至 ASA IPS 模块 19-14
管理 ASA IPS 模块 19-16
安装并启动模块上的映像 19-16
关闭模块 19-18
卸载软件模块映像 19-18
重置密码 19-19
重新加载或重置模块 19-19
监控 ASA IPS 模块 19-20
ASA IPS 模块的配置示例 19-21
ASA IPS 模块的功能历史记录 19-21

关于本指南

- 文档目的，第 xvii 页
- 相关文档，第 xvii 页
- 约定，第 xvii 页
- 获取文档和提交服务请求，第 xviii 页

文档目的

本指南旨在帮助您使用命令行界面 配置思科 ASA 系列的防火墙功能。本指南仅介绍最常见的一些配置场景，并未涵盖所有功能。

通过使用自适应安全设备管理器 (ASDM) 这个基于网络的 GUI 应用，您也可以配置和监控 ASA。ASDM 提供配置向导指导您完成一些常见配置场景，并提供联机帮助以使您获得不常见场景的信息。

本指南中，术语 “ASA” 一般适用于所支持的型号，除非另有说明。

相关文档

有关详细信息，请参阅《*思科 ASA 系列文档导航*》，网址为 http://www.cisco.com/go/asadocs。

约定

本文档使用下列约定：

约定	说明
粗体	命令和关键字及用户输入的文本以**粗体**显示。
斜体	文档标题、新增或强调的术语以及要为其提供值的参数以*斜体*表示。
[ ]	方括号中的元素是可选项。
{x | y | z }	必选的备选关键字括在大括号内，以**竖线**分隔。
[x | y | z]	可选的备选关键字括在方括号内，以**竖线**分隔。

约定	说明
字符串	不加引号的字符集。请勿将字符串用引号引起来，否则会将字符串和引号视为一个整体。
courier 字体	系统显示的终端会话和信息以 courier 字体显示。
courier 粗体	命令和关键字及用户输入的文本以 **courier 粗体**显示。
courier 斜体	要提供值的参数以 *courier 斜体*显示。
< >	非打印字符（如密码）括在尖括号中。
[ ]	系统提示的默认回复括在方括号中。
!，#	代码行开头的感叹号 (!) 或井号 (#) 表示注释行。

注 *表示读者需要注意的地方。*

提示 *表示以下信息有助于您解决问题。*

注意事项 *表示读者应当小心。*在这种情况下，操作可能会导致设备损坏或数据丢失。

获取文档和提交服务请求

有关获取文档、使用思科漏洞搜索工具 (BST)、提交服务请求和收集附加信息的详细信息，请参阅《*思科产品文档更新*》，网址为：
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html。

通过 RSS 源的方式订阅*思科产品文档更新*（其中包括所有新的和修改过的思科技术文档），并将相关内容通过阅读器应用直接发送至您的桌面。RSS 源是一种免费服务。

第 1 部分

服务策略和访问控制

使用模块化策略框的服务策略

发布日期：2014 年 7 月 24 日
更新日期：2014 年 9 月 16 日

使用模块化策略框的服务策略给 ASA 功能配置提供了一致并灵活的方法。例如，您可以使用服务策略创建特定于某项 TCP 应用而非应用于所有 TCP 应用的超时配置。服务策略由多个应用于某个接口或全局应用的操作或规则组成。

- 第 1-1 页上的关于服务策略
- 第 1-7 页上的服务策略准则
- 第 1-8 页上的服务策略的默认设置
- 第 1-10 页上的配置服务策略
- 第 1-17 页上的监控服务策略
- 第 1-17 页上的服务策略示例（模块化策略框架）
- 第 1-20 页上的服务策略历史

关于服务策略

以下主题介绍服务策略的工作原理。

- 第 1-2 页上的服务策略的组成部分
- 第 1-3 页上的使用服务策略配置的功能
- 第 1-4 页上的功能方向性
- 第 1-5 页上的服务策略内的功能匹配
- 第 1-5 页上的应用多项功能操作的顺序
- 第 1-6 页上的某些功能操作的不兼容性
- 第 1-7 页上的多项服务策略的功能匹配

服务策略的组成部分

服务策略的关键在于将高级服务应用于您允许的流量。任何被访问规则允许的流量都可以应用服务策略，从而接受特殊处理，例如被重定向到服务模块，或者运用应用检测。

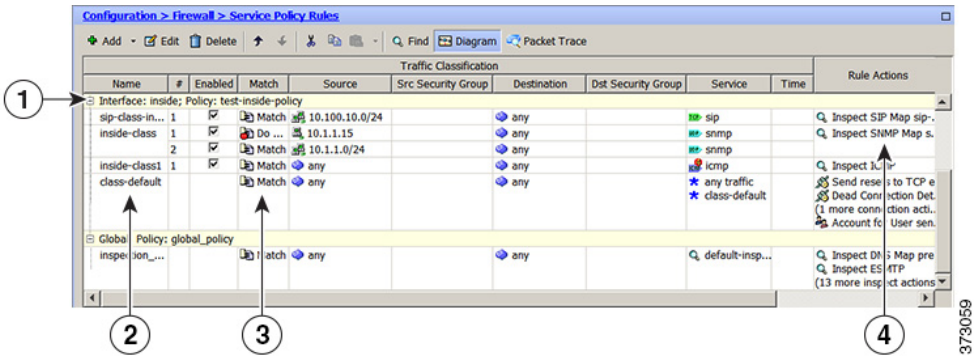
提供以下类型的服务策略：

- 一项应用到所有接口的全局策略。
- 一项应用到单个接口的服务策略。策略可以是一个类组合，适用于流经设备的流量以及在 ASA 接口定向但不流经该设备的管理流量。

每项服务策略都由以下要素组成：

1. 服务策略映射，这是一组按顺序排列的规则集，根据 **service-policy** 命令命名。在 ASDM 中，策略映射表示为 Service Policy Rules 页面上的一个文件夹。
2. 规则，每条规则都是服务策略映射中的 **class** 命令，以及与 **class** 命令相关联的命令。在 ASDM 中，每条规则都显示于不同的行，规则名称为类名称。
   a. **class** 命令定义匹配规则条件的流量。
   b. 与类相关联的命令，例如 **inspect** 和 **set connection timeout**，定义应用于匹配流量的服务和限制。请注意，检测命令可以指向检测策略映射，通过这种方式定义应用于被检测流量的操作。请记住，检测策略映射不同于服务策略映射。

以下示例将服务策略在 CLI 中的显示方式与在 ASDM 中的显示方式进行了对比。请注意，图中编号和 CLI 中的行之间没有一对一映射关系。



以下 CLI 由上图中显示的规则生成。

```
: Access lists used in class maps.
: In ASDM, these map to call-out 3, from the Match to the Time fields.
access-list inside_mpc line 1 extended permit tcp 10.100.10.0 255.255.255.0 any eq sip
access-list inside_mpc_1 line 1 extended deny udp host 10.1.1.15 any eq snmp
access-list inside_mpc_1 line 2 extended permit udp 10.1.1.0 255.255.255.0 any eq snmp
access-list inside_mpc_2 line 1 extended permit icmp any any
: SNMP map for SNMP inspection.Denies all by v3.
: In ASDM, this maps to call-out 4, rule actions, for the class-inside policy.
snmp-map snmp-v3only
  deny version 1
  deny version 2
  deny version 2c
: Inspection policy map to define SIP behavior.
: The sip-high inspection policy map must be referred to by an inspect sip command
: in the service policy map.
: In ASDM, this maps to call-out 4, rule actions, for the sip-class-inside policy.
policy-map type inspect sip sip-high
  parameters
```

```
    rtp-conformance enforce-payloadtype
    no traffic-non-sip
    software-version action mask log
    uri-non-sip action mask log
    state-checking action drop-connection log
    max-forwards-validation action drop log
    strict-header-validation action drop log
: Class map to define traffic matching for the inside-class rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class
  match access-list inside_mpc_1
: Class map to define traffic matching for the sip-class-inside rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map sip-class-inside
  match access-list inside_mpc
: Class map to define traffic matching for the inside-class1 rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class1
  match access-list inside_mpc_2
: Policy map that actually defines the service policy rule set named test-inside-policy.
: In ASDM, this corresponds to the folder at call-out 1.
policy-map test-inside-policy
: First rule in test-inside-policy, named sip-class-inside.Inspects SIP traffic.
: The sip-class-inside rule applies the sip-high inspection policy map to SIP inspection.
: In ASDM, each rule corresponds to call-out 2.
  class sip-class-inside
    inspect sip sip-high
: Second rule, inside-class.Applies SNMP inspection using an SNMP map.
  class inside-class
    inspect snmp snmp-v3only
: Third rule, inside-class1.Applies ICMP inspection.
  class inside-class1
    inspect icmp
: Fourth rule, class-default.Applies connection settings and enables user statistics.
  class class-default
    set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 1:00:00
reset dcd 0:15:00 5
    user-statistics accounting
: The service-policy command applies the policy map rule set to the inside interface.
: This command activates the policies.
service-policy test-inside-policy interface inside
```

使用服务策略配置的功能

下表列出了您使用服务策略配置的功能。

表 1-1　使用服务策略配置的功能

功能	适用于直通流量？	适用于管理流量？	请参阅：
应用类型（多种类型）	**全部**，除 RADIUS 记账以外	**仅 RADIUS** 记账	• 第 7 章，“应用层协议检测入门”。 • 第 8 章，“基本互联网协议检测”。 • 第 9 章，“语音和视频协议的检测”。 • 第 10 章，“数据库和目录协议的检测”。 • 第 11 章，“管理应用协议检测”。 • 第 15 章，“ASA 和思科云网络安全”。

表 1-1　使用服务策略配置的功能（续）

功能	适用于直通流量？	适用于管理流量？	请参阅：
ASA IPS	是	否	第 19 章，“ASA IPS 模块 ”。
ASA CX	是	否	第 18 章，“ASA CX 模块 ”。
ASA FirePOWER (ASA SFR)	是	否	第 17 章，“ASA FirePOWER (SFR) 模块 ”。
NetFlow 安全事件记录过滤	是	是	请参阅常规操作配置指南。
QoS 输入和输出策略管制	是	否	第 13 章，“ 服务质量 ”。
QoS 标准优先级队列	是	否	第 13 章，“ 服务质量 ”。
TCP 和 UDP 连接限制与超时，以及 TCP 序列号随机化	是	是	第 12 章，“ 连接设置 ”。
TCP 规范化	是	否	第 12 章，“ 连接设置 ”。
TCP 状态旁路	是	否	第 12 章，“ 连接设置 ”。
身份防火墙用户统计信息	是	是	请参阅命令参考中的 **user-statistics** 命令

功能方向性

可以将操作双向或单向应用到流量，具体情况视功能而定。对于双向应用的功能，如果流量在两个方向上都匹配类映射，所有进入或退出应用了策略映射的接口的流量都会受到影响。

注　当您使用全局策略时，所有功能都是单向的；通常在应用到单一接口时为双向的功能，在全局应用时仅应用到每个接口的入口。因为策略应用到所有接口，所以策略将在两个方向上应用，因此，在这种情况下，双向性是冗余的。

对于单向应用的功能，例如 QoS 优先级队列，仅进入（或退出，具体取决于功能）应用了策略映射的接口的流量会受到影响。请参见下表，了解每项功能的方向性。

表 1-2　功能方向性

功能	单一接口方向	全局方向
应用类型（多种类型）	双向	入口
ASA CSC	双向	入口
ASA CX	双向	入口
ASA CX 身份验证代理	入口	入口
ASA FirePOWER (ASA SFR)	双向	入口
ASA IPS	双向	入口
NetFlow 安全事件记录过滤	无	入口
QoS 输入策略管制	入口	入口
QoS 输出策略管制	出口	出口
QoS 标准优先级队列	出口	出口
TCP 和 UDP 连接限制与超时，以及 TCP 序列号随机化	双向	入口

表 1-2　　功能方向性（续）

功能	单一接口方向	全局方向
TCP 规范化	双向	入口
TCP 状态旁路	双向	入口
身份防火墙用户统计信息	双向	入口

服务策略内的功能匹配

数据包根据以下规则，匹配策略映射中适用于既定接口的类映射：

1. 对于每种功能类型，数据包仅可以匹配适用于某个接口的策略映射中的一个。
2. 当数据包匹配某种功能类型的某条类映射时，ASA 不会尝试将其与该功能类型的任何后续 类映射进行匹配。
3. 然而，如果数据包匹配另一种功能类型的某条后续类映射，在支持的情况下，ASA 还将为该后续类映射应用操作。请参阅第 1-6 页上的某些功能操作的不兼容性，了解有关不受支持的组合的详细信息。

注　应用检测包括多种检测类型，大部分类型都相互排斥。对于可以组合在一起的检测，每项检测都被视为一项独立功能。

数据包匹配示例

例如：

- 如果数据包不仅匹配连接限制的类映射，还匹配应用检测类映射，则两项操作均会被应用。
- 如果数据包不仅匹配 HTTP 检测的类映射，还匹配另一条包含 HTTP 检测的类映射，则第二条类映射操作不会被应用。
- 如果数据包不仅匹配 HTTP 检测类映射，还匹配另一条包含 FTP 检测的类映射，则第二条类映射操作不会被应用，因为 HTTP 检测和 FTP 检测不能整合在一起。
- 如果数据包不仅匹配 HTTP 检测类映射，还匹配另一条包含 IPv6 检测的类映射，则两项操作均会被应用，因为 IPv6 检测可以与任何其他类型的检测整合在一起。

应用多项功能操作的顺序

不同类型的操作在策略映射中的执行顺序独立于这些操作在策略映射中显示的顺序。

按以下顺序执行操作：

1. QoS 输入策略管制
2. TCP 规范化、TCP and UDP 连接限制与超时、TCP 序列号随机化和 TCP 状态旁路。

注　当 ASA 执行代理服务（例如，AAA 或 CSC）或者修改 TCP 负载（例如，FTP 检测）时，TCP 规化器在双模式下运行，在代理或负载修改服务之前和之后应用。

3. ASA CSC

4. 可以与其他检测整合在一起的应用检测：
   a. IPv6
   b. IP 选项
   c. WAAS
5. 无法与其他检测组合在一起的应用检测。有关详细信息，请参阅第 1-6 页上的某些功能操作的不兼容性。
6. ASA IPS
7. ASA CX
8. ASA FirePOWER (ASA SFR)
9. QoS 输出策略管制
10. QoS 标准优先级队列

注　NetFlow 安全事件记录过滤和身份防火墙用户统计信息不受顺序约束。

某些功能操作的不兼容性

某些功能对于同一流量互不兼容。下表可能不包含所有不兼容性；有关每项功能兼容性的详细信息，请参阅功能对应的章节：

- 您无法为同一组流量配置 QoS 优先级队列和 QoS 策略管制。
- 大部分检测不应与另一项检测整合在一起，因此，如果您为同一流量配置多项检测，ASA 仅应用一项检测。HTTP 检测可以与云网络安全检测整合在一起。其他例外已在第 1-5 页上的应用多项功能操作的顺序中列出。
- 您无法配置即将发送到多个模块（例如 ASA CX 和 ASA IPS）的流量。
- HTTP 检测不兼容 ASA CX 或 ASA FirePOWER。
- 云网络安全不兼容 ASA CX 或 ASA FirePOWER。

注　在默认全局策略中使用的 **match default-inspection-traffic** 命令是一个特殊的 CLI 快捷方式，用以匹配所有检测的默认端口。在策略映射中使用时，该类映射可以根据流量的目标端口确保应用到每个数据包的检测都正确。例如，当端口 69 的 UDP 流量到达 ASA 时，ASA 将应用 TFTP 检测；当端口 21 的 TCP 流量到达时，ASA 将应用 FTP 检测。因此，只有在这种情况下，您才能为同一类映射配置多项检测。通常，ASA 不使用端口号确定应用哪项检测，因此，您可以将检测应用到非标准端口（例如）。

该流量类不包含云网络安全检测的默认端口（80 和 443）。

错误配置示例：您在同一策略映射中配置多个检测，并且不使用 default-inspection-traffic 快捷方式。在示例 1-1 中，错误地为发往端口 21 的流量配置了 FTP 和 HTTP 检测。在示例 1-2 中，错误地为发往端口 80 的流量配置了 FTP 和 HTTP 检测。在这两种错误配置示例的情况下，仅 FTP 检测将会被应用，因为以检查被应用的顺序，FTP 先于 HTTP。

示例 1-1　FTP 数据包的错误配置：也配置了 HTTP 检测

```
class-map ftp
   match port tcp eq 21
class-map http
```

```
   match port tcp eq 21 [ 应为 80]
policy-map test
   class ftp
     inspect ftp
   class http
     inspect http
```

示例 1-2　HTTP 数据包的错误配置：也配置了 FTP 检测

```
class-map ftp
   match port tcp eq 80 [ 应为 21]
class-map http
   match port tcp eq 80
policy-map test
   class ftp
     inspect ftp
   class http
     inspect http
```

多项服务策略的功能匹配

对于 TCP 和 UDP 流量（以及启用状态性 ICMP 检测时的 ICMP），服务策略不仅在单个数据包上运行，还在流量上运行。如果流量为现有连接的一部分且该现有连接匹配一个接口上的策略中的某项功能，那么该流量无法匹配另一个接口上的策略中的同一项功能；仅使用第一项策略。

例如，如果 HTTP 流量匹配内部接口上的检查 HTTP 流量的策略，而且您在 HTTP 检测的外部接口上有独立策略，该流量也不会在外部接口的出口被检测。同样，该连接的返回流量不会被外部接口的入口策略检测，也不会被内部接口的出口策略检测。

对于未被当作流量处理的流量，例如，不启用状态性 ICMP 检测时的 ICMP，返回流量可以匹配返回接口上的另一个策略映射。例如，如果在内部和外部接口上配置 IPS，但内部策略使用虚拟传感器 1，同时外部策略使用虚拟传感器 2，则非状态性 Ping 将匹配出站虚拟传感器 1，以及匹配入站虚拟传感器 2。

服务策略准则

IPv6 准则

支持在以下功能中使用 IPv6：

- DNS、FTP、HTTP、ICMP、ScanSafe、SIP、SMTP、IPsec-pass-thru 和 IPv6 的应用检测。
- ASA IPS
- ASA CX
- ASA FirePOWER
- NetFlow 安全事件记录过滤
- TCP and UDP 连接限制与超时，TCP 系列号随机化
- TCP 规范化
- TCP 状态旁路
- 身份防火墙用户统计信息

类映射（流量类）准则

所有类型的最大类映射（流量类）数量在单一模式下为 255，在多模式下视情景而定。类映射包括以下类型：

- 第 3/4 层类映射（对于直通流量和管理流量）。
- 检测类映射
- 正则表达式类映射
- 直接在检测策略映射下使用的 **match** 命令

该限制还包括所有类型的默认类映射，将用户配置的类映射限制为大约 235 个。请参阅第 1-10 页上的默认类映射（流量类）。

策略映射准则

请参阅下列有关使用策略映射的准则：

- 对于每个接口，您只能为分配一个策略映射。然而，您可以在配置中最多创建 64 个策略映射。
- 您可以将同一策略映射应用到多个接口。
- 您可以在第 3/4 层映射中识别多达 63 个第 3/4 层类映射。
- 对于每个类映射，在支持的情况下，您可以从一种或多种功能类型分配多项操作。请参阅第 1-6 页上的某些功能操作的不兼容性。

服务策略准则

- 对于某个既定功能来说，接口服务策略优先于全局服务策略。例如，如果有 FTP 检测全局策略和 TCP 规范化接口策略，则 FTP 检测和 TCP 规范化都会被应用到接口。然而，如果有 FTP 检测全局策略和 FTP 检测接口策略，则仅接口策略 FTP 检测会被应用到接口。
- 您只能应用一项全局策略。例如，您无法创建一个包含功能集 1 的全局策略和另一个包含功能集 2 的全局策略。所有功能都必须包含在单一策略中。
- 对配置进行服务策略更改时，所有*新的*连接都使用新的服务策略。现有连接继续使用在建立连接时配置的策略。**show** 命令输出不包含有关旧连接的数据。

  例如，如果从某接口移除 QoS 服务策略，然后添加经修改的版本，**show service-policy** 命令仅显示与匹配新服务策略的新连接相关联的 QoS 计数器；旧策略上的现有连接不再在命令输出中显示。

  为确保所有连接都使用新策略，您需要断开当前连接，使其能够使用新策略重新连接。使用 **clear conn** 或 **clear local-host** 命令。

服务策略的默认设置

以下主题介绍服务策略和模块化策略框架的默认设置：

- 第 1-9 页上的服务策略默认配置
- 第 1-10 页上的默认类映射（流量类）

服务策略默认配置

默认情况下，配置包含一项策略（全局策略），该策略匹配所有默认应用检测流量并将某些检测应用到所有接口上的流量。默认情况下，并非所有检测都被启用。您只能应用一项全局策略，因此，如果想要调整全局策略，您需要编辑默认策略，或者将其禁用来应用新策略。（对于某项特定功能，接口策略覆盖全局策略。）

默认策略包括以下应用检测：

- DNS
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP
- IP 选项

默认策略配置包括以下命令：

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
service-policy global_policy global
```

注　请参阅第 1-6 页上的某些功能操作的不兼容性，了解有关在默认类映射中使用的特殊 **match default-inspection-traffic** 命令的详细信息。

默认类映射（流量类）

该配置包含一个默认的第 3/4 层类映射（流量类），ASA 在叫作 default-inspection-traffic 的默认全局策略中使用该类映射；它匹配默认检测流量。该类在默认全局策略中使用，是一个用来匹配所有检测的默认端口的特殊快捷方式。

在策略中使用时，该类可以根据流量的目标端口，确保应用到每个数据包的检测都正确。例如，当端口 69 的 UDP 流量到达 ASA 时，ASA 将应用 TFTP 检测；当端口 21 的 TCP 流量到达时，ASA 将应用 FTP 检测。因此，只有在这种情况下，您才能为同一类映射配置多项检测。通常，ASA 不使用端口号确定应用哪项检测，因此，您可以将检测应用到非标准端口（例如）。

```
class-map inspection_default
 match default-inspection-traffic
```

默认配置中的另一个类映射叫作 class-default，该类映射匹配所有流量。该类映射出现在所有第 3/4 层策略映射的末尾，实质上要求 ASA 不要在所有其他流量上执行任何操作。如果需要，您可以使用 class-default 类，而非使用 Any 流量类的 **match any** 。事实上，有些功能仅对 class-default 可用。

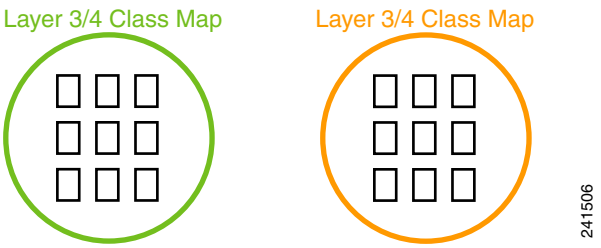
```
class-map class-default
 match any
```

配置服务策略

要使用模块化策略框架配置服务策略，请执行以下步骤：

步骤 1　创建第 3/4 层类映射，识别您想执行操作的**流量**，如第 1-12 页上的识别流量（第 3/4 层类映射）中所述。

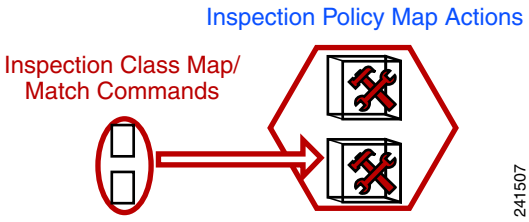
例如，您可能想对所有流经 ASA 的流量执行操作；或者，只想对从 10.1.1.0/24 到任何目标地址的流量执行某些操作。



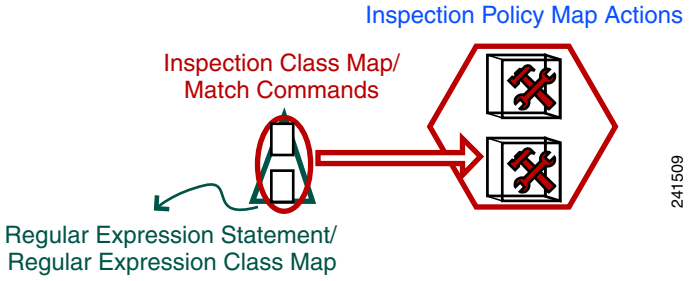
步骤 2　或者，在某些检测流量上执行其他操作。

如果您想执行的操作之一是应用检测，并想在某些上执行附加操作，请创建检测策略映射。检测策略映射可以识别流量并指定对流量执行的操作。

例如，您可能想丢弃所有体长度大于 1000 字节的 HTTP 请求。

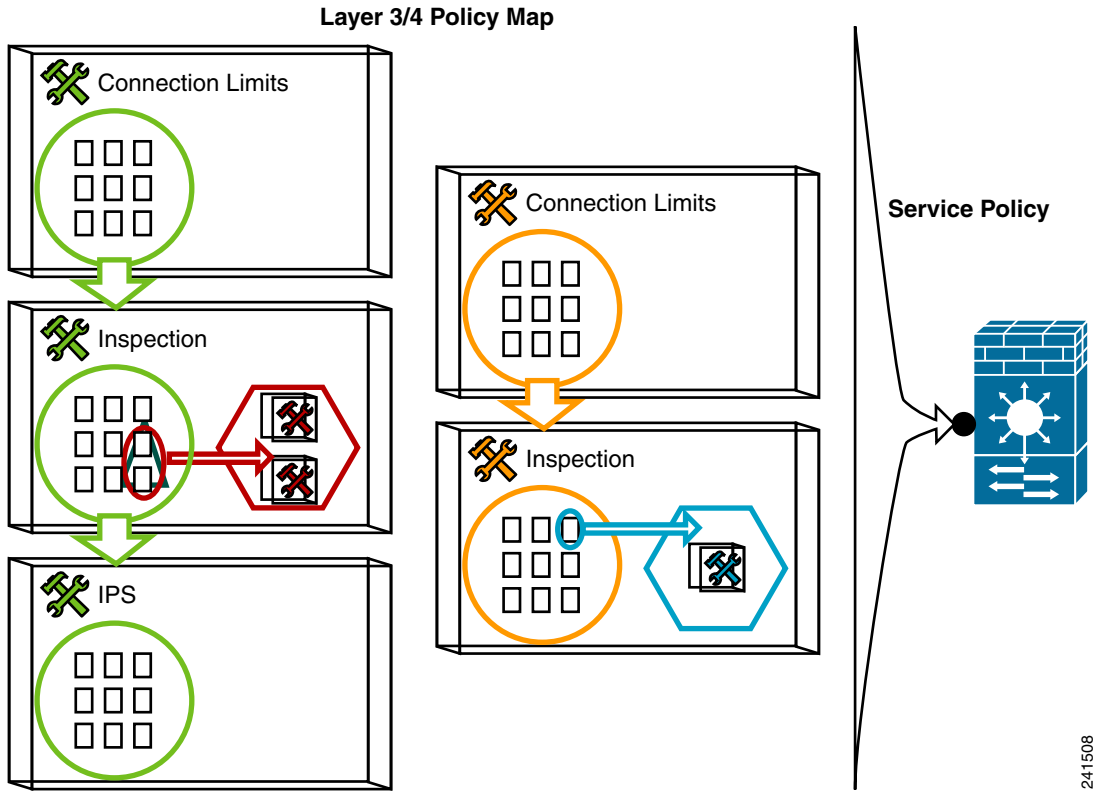


您可以创建一个独立检测策略映射，该映射直接使用 **match** 命令识别流量；或者，创建一个可重用或进行更复杂的匹配的检测类映射。例如，您可以使用一个正则表达式或一组正则表达式（一个正则表达式类映射）匹配被检测数据包中的文本，并基于更小的条件范围指定操作。例如，您可能想丢弃所有 URL 中包含 “example.com” 文本的 HTTP 请求。



请参阅第 2-4 页上的在检测策略映射中定义操作和第 2-5 页上的在检测类映射中识别流量。

步骤 3　创建第 3/4 层策略映射，定义您想在每个第 3/4 层类映射上执行的操作，如第 1-14 页上的定义操作（第 3/4 层策略映射）中所述。



步骤 4　确定您想应用策略映射的接口，或者全局应用策略映射，如第 1-16 页上的将操作应用到接口（服务策略）中所述。

识别流量（第 3/4 层类映射）

第 3/4 层类映射可以识别您想应用操作的第 3 层和第 4 层流量。您可以为每个第 3/4 层策略映射创建多个第 3/4 层类映射。

- 第 1-12 页上的为直通流量创建第 3/4 层类映射
- 第 1-14 页上的 Create a Layer 3/4 Class Map for Management Traffic

为直通流量创建第 3/4 层类映射

第 3/4 层类映射根据协议、端口、IP 地址和其他第 3 或 4 层属性匹配流量。

提示　我们建议您仅检测理应出现应用流量的端口上的流量；如果检测所有流量，例如，使用 **match any**，ASA 性能则将受到影响。

操作步骤

步骤 1　创建第 3/4 层类映射，其中 *class_map_name* 是一个长度最多为 40 个字符的字符串。

class-map *class_map_name*

保留名称 “class-default”。所有类型的类映射都使用同一命名空间，因此，您无法重用已被另一类型的类映射使用的名称。CLI 进入类映射配置模式。

示例：

```
hostname(config)# class-map all_udp
```

步骤 2　（可选）向类映射添加说明。

description *string*

示例：

```
hostname(config-cmap)# description All UDP traffic
```

步骤 3　使用以下某个命令匹配流量。除非另有规定，您仅能将一个 **match** 命令包含在类映射中。

- **match any** - 匹配所有流量。

  ```
  hostname(config-cmap)# match any
  ```

- **match access-list** *access_list_name* - 匹配扩展 ACL 指定的流量。如果 ASA 正在透明防火墙模式下运行，您可以使用以太网类型 ACL。

  ```
  hostname(config-cmap)# match access-list udp
  ```

- **match port** {**tcp** | **udp**} {**eq** *port_num* | **range** *port_num port_num*} - 匹配 TCP 或 UDP 目标端口，为单一端口或一系列连续的端口。对于使用多个非连续端口的应用，请使用 **match access-list** 命令，定义一个匹配每个端口的 ACE。

  ```
  hostname(config-cmap)# match tcp eq 80
  ```

- **match default-inspection-traffic** - 匹配检测的默认流量：ASA 能够检测的所有应用使用的默认 TCP 和 UDP 端口。

  ```
  hostname(config-cmap)# match default-inspection-traffic
  ```

  该命令在默认全局策略中使用，在策略映射中使用时，是一个特殊的 CLI 快捷方式，可以根据流量的目标端口确保应用到每个数据包的检测都正确。例如，当端口 69 的 UDP 流量到达 ASA 时，ASA 将应用 TFTP 检测；当端口 21 的 TCP 流量到达时，ASA 将应用 FTP 检测。因此，仅在这种情况下，您可以为同一类映射配置多个检测（WAAS 检测除外，该检测可以通过其他检测配置）。请参阅第 1-6 页上的某些功能操作的不兼容性，了解有关整合操作的详细信息）。通常，ASA 不使用端口号确定应用的检测，因此，您可以将检测应用到非标准端口（例如）。

  请参阅第 7-5 页上的默认检测和 NAT 限制，查看默认端口列表。默认情况下，不是所有其端口包含在 **match default-inspection-traffic** 命令中的应用都在策略映射中启用。

  您可以指定 **match access-list** 命令以及 **match default-inspection-traffic** 命令，缩小被匹配流量的范围。因为 **match default-inspection-traffic** 命令指定了要匹配的端口和协议，所以 ACL 中的任意端口和协议都将被忽略。

- **match dscp** *value1* [*value2*] [...] [*value8*] - 匹配 IP 标头中的 DSCP 值，最多 8 个 DSCP 值。

  ```
  hostname(config-cmap)# match dscp af43 cs1 ef
  ```

- **match precedence** *value1* [*value2*] [*value3*] [*value4*] - 最多匹配 4 个优先级值，用 IP 标头中的 TOS 字节表示，其中 *value1* 至 *value4* 可以为 0 至 7，对应可能的优先级。

  ```
  hostname(config-cmap)# match precedence 1 4
  ```

- **match rtp** *starting_port range* - 匹配 RTP 流量，其中 *starting_port* 指定介于 2000 和 65534 之间的偶数 UDP 目标端口。*range* 指定要匹配上述 *starting_port* 的额外 UDP 端口的数量，介于 0 和 16383 之间。

  ```
  hostname(config-cmap)# match rtp 4004 100
  ```

- **match tunnel-group** *name* - 匹配您想应用 QoS 的 VPN 隧道组流量。

  您还可以指定另一个 **match** 命令，细化流量匹配。您可以指定上述命令中除 **match any**、**match access-list** 或 **match default-inspection-traffic** 之外的的任意命令。或者，您还可以输入 **match flow ip destination-address** 命令，匹配隧道组中流向每个 IP 地址的流。

  ```
  hostname(config-cmap)# match tunnel-group group1
  hostname(config-cmap)# match flow ip destination-address
  ```

示例

下面是一个 **class-map** 命令示例：

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp
```

```
hostname(config-cmap)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

Create a Layer 3/4 Class Map for Management Traffic

对于流向 ASA 的管理流量，您可能想执行特定于该类流量的操作。您可以指定能够匹配 ACL、TCP 或 UDP 端口的管理类映射。策略映射中管理类映射的可用操作类型专门用于管理流量。请参阅第 1-3 页上的使用服务策略配置的功能。

操作步骤

步骤 1　创建管理类映射，其中 *class_map_name* 是一个长度最多为 40 个字符的字符串。

class-map type management *class_map_name*

保留名称 “class-default”。所有类型的类映射都使用同一命名空间，因此，您无法重用已被另一类型的类映射使用的名称。CLI 进入类映射配置模式。

示例：

```
hostname(config)# class-map all_udp
```

步骤 2　（可选）向类映射添加说明。

description *string*

示例：

```
hostname(config-cmap)# description All UDP traffic
```

步骤 3　使用以下某个命令匹配流量。

- **match access-list** *access_list_name* - 匹配扩展 ACL 指定的流量。如果 ASA 正在透明防火墙模式下运行，您可以使用以太网类型 ACL。

  ```
  hostname(config-cmap)# match access-list udp
  ```

- **match port** {**tcp** | **udp**} {**eq** *port_num* | **range** *port_num port_num*} - 匹配 TCP 或 UDP 目标端口，为单一端口或一系列连续的端口。对于使用多个非连续端口的应用，请使用 **match access-list** 命令，定义一个匹配每个端口的 ACE。

  ```
  hostname(config-cmap)# match tcp eq 80
  ```

定义操作（第 3/4 层策略映射）

配置第 3/4 层类映射识别流量之后，使用第 3/4 层策略映射将操作与这些类关联起来。

提示　策略映射最大数量为 64 个，但每个接口只能应用一个策略映射。

操作步骤

步骤 1　添加策略映射。

policy-map *policy_map_name*

参数 *policy_map_name* 是策略映射名称，长度最多为 40 个字符。所有类型的策略映射都使用同一命名空间，因此，您无法重用已被另一类型的策略映射使用的名称。CLI 将进入策略映射配置模式。

示例：

```
hostname(config)# policy-map global_policy
```

步骤 2　指定先前配置的第 3/4 层类映射，其中 *class_map_name* 是类映射名称。

class *class_map_name*

请参阅第 1-12 页上的识别流量（第 3/4 层类映射），添加类映射。

注　如果类映射中没有 **match default-inspection-traffic** 命令，则最多允许在该类下配置一个 **inspect** 命令。

class *class_map_name*

示例：

```
hostname(config-pmap)# description global policy map
```

步骤 3　为该类映射指定一项或多项操作。

请参阅第 1-3 页上的使用服务策略配置的功能。

步骤 4　为想添加到策略映射中的每个类映射重复此流程。

示例

下面是一个连接策略的 **policy-map** 命令示例。该命令限制允许连到网络服务器 10.1.1.1 的连接的数量。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

以下示例显示多匹配在策略映射中的工作原理：

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout idle 0:10:0
```

以下示例显示流量如何匹配第一个可用的类映射，并且将不会匹配在同一功能域中指定操作的任何后续类映射：

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout idle 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout idle 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout idle 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

当某个 Telnet 连接被发起时，它将匹配 **class telnet_traffic**。同样，如果某个 FTP 连接被发起，它将匹配 **class ftp_traffic**。对于 Telnet 和 FTP 以外的任何 TCP 连接，它将匹配 **class tcp_traffic**。尽管 Telnet 或 FTP 连接可以匹配 **class tcp_traffic**，但 ASA 不会进行这种匹配，因为这些连接之前匹配了其他的类。

将操作应用到接口（服务策略）

要激活第 3/4 层策略映射，请创建一项将其应用到一个或多个接口或将其全局应用到所有接口的服务策略。使用以下命令：

service-policy *policy_map_name* {**global** | **interface** *interface_name*} [**fail-close**]

其中：

- *policy_map_name* 是策略映射名称。
- **global** 可以创建一项应用于所有没有特定策略的接口的服务策略。

  您只能应用一项全局策略，因此，如果想要调整全局策略，您需要编辑默认策略，或者将其禁用来应用新策略。默认情况下，此配置包含一项全局策略，该策略匹配所有默认应用检测流量并将检测全局应用到流量。默认服务策略包含以下命令：**service-policy global_policy global**。
- **interface** *interface_name* 通过将策略映射与接口相关联，创建服务策略。
- **fail-close** 为不支持 IPv6 流量的应用检测丢弃的 IPv6 流量生成系统日志 (767001)。默认情况下，不生成系统日志。有关支持 IPv6 的检测列表的详细信息，请参阅第 1-7 页上的 IPv6 准则。

示例

例如，以下命令可以在外部接口上启用 inbound_policy 策略映射：

```
hostname(config)# service-policy inbound_policy interface outside
```

以下命令在所有其他 ASA 接口上禁用默认全局策略，并启用一个叫作 new_global_policy 的新全局策略。

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

监控服务策略

要监控服务策略，请输入以下命令：

- **show service-policy**

  系统将显示服务策略统计信息。

服务策略示例（模块化策略框架）

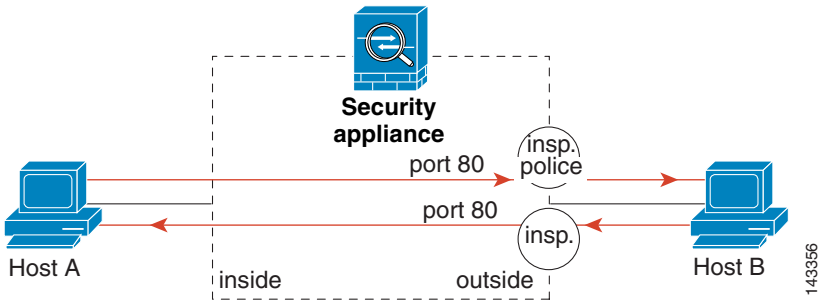
本章节包括若干模块化策略框架示例。

- 第 1-17 页上的将检测和 QoS 策略管制应用到 HTTP 流量
- 第 1-18 页上的将检测全局应用到 HTTP 流量
- 第 1-18 页上的将检测和连接限制应用到流向特定服务器的 HTTP 流量
- 第 1-19 页上的通过 NAT 将检测应用到 HTTP 流量

将检测和 QoS 策略管制应用到 HTTP 流量

在本例中，任何通过外部接口进入或退出 ASA 的 HTTP 连接（端口 80 上的 TCP 流量）都针对 HTTP 检测进行分类。任何退出外部接口的 HTTP 流量针对策略管制进行分类。

图 1-1　　HTTP 检测和 QoS 策略管制



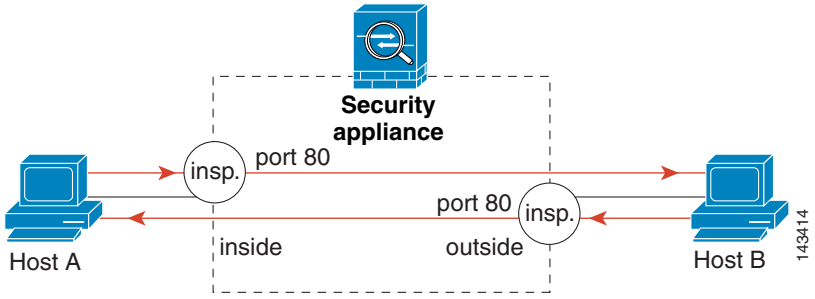
请见以下适用于本示例的命令：

```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# police output 250000
hostname(config)# service-policy http_traffic_policy interface outside
```

将检测全局应用到 HTTP 流量

在本例中，任何通过任何接口进入 ASA 的 HTTP 连接（端口 80 上的 TCP 流量）都针对 HTTP 检测进行分类。因为采用了全局策略，所以检测仅在流量进入每个接口时发生。

图 1-2　全局 HTTP 检测



请见以下适用于本示例的命令：

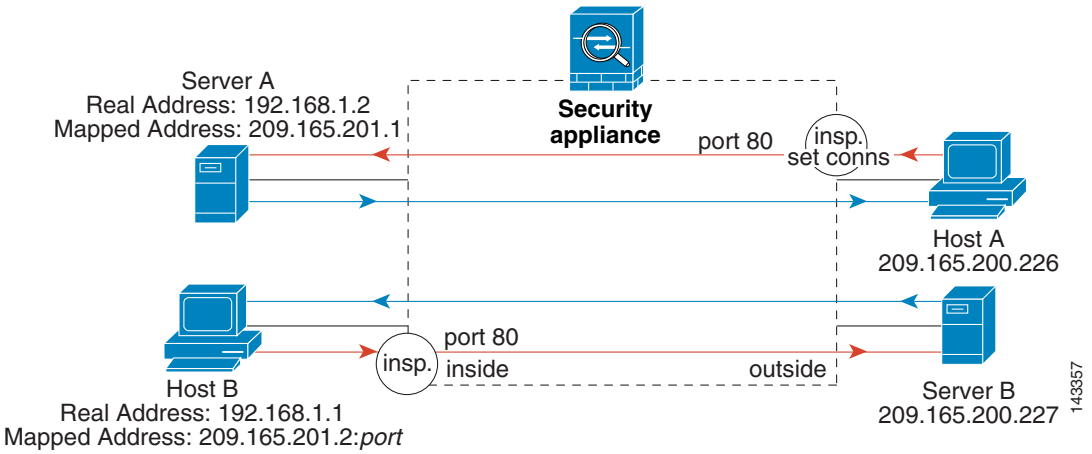
```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config)# service-policy http_traffic_policy global
```

将检测和连接限制应用到流向特定服务器的 HTTP 流量

在本例中，任何以服务器 A 为目标的通过外部端口进入 ASA 的 HTTP 连接（端口 80 上的 TCP 流量）都针对 HTTP 检测和最大连接限制进行分类。从服务器 A 发起到主机 A 的连接不匹配类映射中的 ACL，因此，这些连接不会受到影响。

任何发往服务器 B 并通过内部接口进入 ASA 的 HTTP 连接都针对 HTTP 检测进行分类。从服务器 B 发起到主机 B 的连接不匹配类映射中的 ACL，因此，这些连接不会受到影响。

图 1-3　特定服务器的 HTTP 检测和连接限制



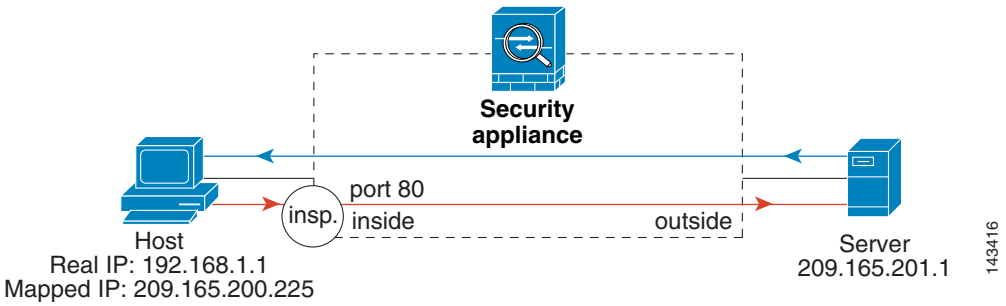
请见以下适用于本示例的命令：

```
hostname(config)# object network obj-192.168.1.2
hostname(config-network-object)# host 192.168.1.2
hostname(config-network-object)# nat (inside,outside) static 209.165.201.1
hostname(config)# object network obj-192.168.1.0
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 209.165.201.2
hostname(config)# access-list serverA extended permit tcp any host 209.165.201.1 eq 80
hostname(config)# access-list ServerB extended permit tcp any host 209.165.200.227 eq 80

hostname(config)# class-map http_serverA
hostname(config-cmap)# match access-list serverA
hostname(config)# class-map http_serverB
hostname(config-cmap)# match access-list serverB

hostname(config)# policy-map policy_serverA
hostname(config-pmap)# class http_serverA
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# set connection conn-max 100
hostname(config)# policy-map policy_serverB
hostname(config-pmap)# class http_serverB
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy policy_serverB interface inside
hostname(config)# service-policy policy_serverA interface outside
```

通过 NAT 将检测应用到 HTTP 流量

在本例中，内部网络上的主机有两个地址：一个是实际地址 192.168.1.1，另一个是在外部网络上使用的映射 IP 地址 209.165.200.225。在类映射中的 ACL 中，必须使用实际 IP 地址。如果已将其应用到外部接口，也可以使用实际地址。

图 1-4　通过 NAT 进行的 HTTP 检测



请见以下适用于本示例的命令：

```
hostname(config)# object network obj-192.168.1.1
hostname(config-network-object)# host 192.168.1.1
hostname(config-network-object)# nat (VM1,outside) static 209.165.200.225

hostname(config)# access-list http_client extended permit tcp host 192.168.1.1 any eq 80

hostname(config)# class-map http_client
hostname(config-cmap)# match access-list http_client
```

```
hostname(config)# policy-map http_client
hostname(config-pmap)# class http_client
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy http_client interface inside
```

服务策略历史

功能名称	版本	说明
模块化策略框架	7.0(1)	引入了模块化策略框架。
与 RADIUS 记账流量一起使用的管理类映射	7.2(1)	引入了管理类映射，与 RADIUS 记账流量一起使用。引入了以下命令：**class-map type management** 和 **inspect radius-accounting**。
检测策略映射	7.2(1)	引入了检测策略映射。引入了以下命令：**class-map type inspect**。
正则表达式和策略映射	7.2(1)	引入了正则表达式和策略映射，在检测策略映射下使用。引入了以下命令：**class-map type regex**、**regex**、**match regex**。
检测策略映射的 match any 命令	8.0(2)	引入了关键字 **match any**，与检测策略映射一起使用：流量可以匹配一个或多个条件以匹配类映射。过去，仅 **match all** 命令可用。

应用检测的特殊操作（检测策略映射）

您可以使用模块化策略框架为许多应用检测配置特殊操作。当您在第 3/4 层策略映射中启用检测引擎时，或者还可以启用在*检测策略映射*中定义的操作。当检测策略映射与第 3/4 层策略映射中定义了检测操作的流量匹配时，将根据指定的操作处理该流量的子集（例如，丢弃或限制速率）。

- 第 2-1 页上的检测策略映射有关信息
- 第 2-2 页上的准则和限制
- 第 2-3 页上的默认检测策略映射
- 第 2-4 页上的在检测策略映射中定义操作
- 第 2-5 页上的在检测类映射中识别流量
- 第 2-7 页上的更多信息指南
- 第 2-7 页上的检测策略映射的功能历史

检测策略映射有关信息

有关支持检测策略映射的应用列表，请参阅第 7-9 页上的配置应用层协议检测。

检测策略映射由下列一个或多个要素组成： 检测策略映射的确切可用选项视应用而定。

- 流量匹配命令 - 您可以直接在检测策略映射中定义流量匹配 命令，将应用流量与应用的特定条件相匹配，例如 URL 字符串，然后为流量启用操作。
  - 某些流量匹配命令可以指定正则表达式，以匹配数据包中的文本。请务必在配置策略映射之前，在正则表达式类映射中单独或集中创建和测试正则表达式。
- 检测类映射 - 检测类映射包括多个流量匹配命令。然后，在策略映射中识别类映射，并针对整个类映射启用操作。创建类映射和直接在检测策略映射中定义流量匹配的差别在于，您可以创建更复杂的匹配条件和重用类映射。然而，您无法为不同的匹配设置不同操作。**请注意，**并非所有检测都支持检测类映射。
- 参数 - 参数会影响检测引擎的行为。

准则和限制

- HTTP 检测策略映射 - 如果修改正在使用的 HTTP 检测策略映射 (**policy-map type inspect http**)，您必须移除并重新应用 **inspect http** *map* 操作，才能使更改生效。例如，如果修改 “http-map” 检测策略映射，您必须移除、，将 **inspect http http-map** 命令：

```
hostname(config)# policy-map test
hostname(config-pmap)# class http
hostname(config-pmap-c)# no inspect http http-map
hostname(config-pmap-c)# inspect http http-map
```

- 所有检测策略映射 - 如果想用正在使用的检测策略映射交换不同的映射名称，必须删除、**inspect** *protocol map* 命令，并通过新映射重新添加。例如：

```
hostname(config)# policy-map test
hostname(config-pmap)# class sip
hostname(config-pmap-c)# no inspect sip sip-map1
hostname(config-pmap-c)# inspect sip sip-map2
```

- 您可以在检测策略映射中指定多个 **class** 或 **match** 命令。

  如果数据包匹配多个不同的 **match** 或 **class** 命令，ASA 应用操作的顺序将由内部 ASA 规则决定，而不是由向检测策略映射添加的顺序决定。内部规则由应用类型和分解数据包的逻辑进展确定，并且不可由用户配置。例如，对于 HTTP 流量，解析 Request Method 字段优先于解析 Header Host Length 字段； Request Method 字段的操作早于 Header Host Length 字段的操作。例如，以下匹配命令可以按任意顺序输入，但首先匹配的是 **match request method get** 命令。

```
match request header host length gt 100
  reset
match request method get
  log
```

  如果操作丢弃数据包，在检测策略映射中将不会执行进一步操作。例如，如果第一个操作是重置连接，它绝不会匹配任何更多 **match** 或 **class** 命令。如果第一个操作是记录数据包，则会发生第二个操作，例如，重置连接。

  如果数据包匹配多个相同的 **match** 或 **class** 命令，它们将会按照在策略映射中出现的顺序进行匹配。例如，对于报头长度为 1001 的数据包，将会首先匹配下面的第一个命令，进行相关记录，然后匹配第二个命令并重置。如果对调两个 **match** 命令的顺序，数据包将被丢弃且连接将被重置，然后才能匹配第二个 **match** 命令；数据包不再会被记录下来。

```
match request header length gt 100
  log
match request header length gt 1000
  reset
```

  会根据类映射中的最低优先级 **match** 命令（优先级基于内部规则）来确定某类映射是与另一类映射同类型还是 **match** 命令。如果某个类映射与另一个类映射有同一类型的最低优先级 **match** 命令，类映射将根据被添加到策略映射中采用的顺序被匹配。如果每个类映射的最低优先级匹配不同，将会首先匹配具有较高优先级 **match** 命令的类映射。例如，以下三个类映射包含两种类型的 **match** 命令：**match request-cmd**（优先级更高）和 **match filename**（优先级更低）。ftp3 类映射包含这两个命令，但它根据最低优先级命令 **match filename** 进行排序。ftp1 类映射包含最高优先级的命令，因此，不管在策略映射中的顺序如何，都会首先对它进行匹配。ftp3 类映射的排列优先级和 ftp2 类映射相同，ftp2 类映射也含有 **match filename** 命令。ftp3 和 ftp2 类映根据在策略映射中的顺序被匹配：首先匹配 ftp3，然后匹配 ftp2。

```
class-map type inspect ftp match-all ftp1
  match request-cmd get
class-map type inspect ftp match-all ftp2
  match filename regex abc
```

```
class-map type inspect ftp match-all ftp3
  match request-cmd get
  match filename regex abc

policy-map type inspect ftp ftp
  class ftp3
    log
  class ftp2
    log
  class ftp1
    log
```

默认检测策略映射

默认情况下，启用 DNS 检测，使用 preset_dns_map 检测类映射：

- 最大 DNS 消息长度为 512 字节。
- 最大客户端 DNS 消息长度是自动设置的，以匹配资源记录。
- DNS 保护已启用，这样，一旦 ASA 转发 DNS 应答，ASA 就会断开与 DNS 查询相关的 DNS 会话。另外，ASA 还监控消息交换，确保 DNS 回复 ID 匹配 DNS 查询 ID。
- 根据 NAT 配置的 DNS 记录转换已启用。
- 协议执行已启用，使得可以进行 DNS 消息格式检查（具体检查内容包括：域名长度不得超过 255 个字符，标签长度不得超过 63 个字符，压缩检查和循环指针检查）。

请参阅以下默认命令：

```
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
```

注　还存在其他默认检测策略映射，例如 **_default_esmtp_map**。例如， **inspect esmtp** 隐式地使用策略映射 “_default_esmtp_map”。可以使用 **show running-config all policy-map** 命令显示所有默认策略映射。

在检测策略映射中定义操作

当您在第 3/4 层策略映射中启用检测引擎时，或者还可以启用在检测策略映射中定义的操作。

详细步骤

	命令	用途
步骤 1	（可选） 创建检测类映射。	请参阅第 2-5 页上的在检测类映射中识别流量。 或者，您可以直接在策略映射中识别流量。
步骤 2	（可选） 创建正则表达式。	对于支持正则表达式的策略映射类型，请参阅常规操作配置指南。
步骤 3	**policy-map type inspect** *application policy_map_name* **示例：** `hostname(config)# policy-map type inspect http http_policy`	创建检测策略映射。有关支持检测策略映射的应用列表，请参阅第 7-9 页上的配置应用层协议检测。 参数 *policy_map_name* 是策略映射的名称，最大长度为 40 个字符。所有类型的策略映射都使用同一命名空间，因此，您无法重用已被另一类型的策略映射使用的名称。CLI 将进入策略映射配置模式。
步骤 4	使用以下其中一种方法指定要对其执行操作的流量：	

	class *class_map_name*
	示例：
	`hostname(config-pmap)# class http_traffic`
	`hostname(config-pmap-c)#`
		指定您在第 2-5 页上的在检测类映射中识别流量中创建的检测类映射。
		并非所有应用都支持检测类映射。

	使用在检测章节为每个应用描述的其中某个 **match** 命令，直接在策略映射中指定流量。
	示例：
	`hostname(config-pmap)# match req-resp content-type mismatch`
	`hostname(config-pmap-c)#`
		如果使用 **match not** 命令，则任何匹配 **match not** 命令中条件的流量都不会应用操作。
		对于支持正则表达式的策略映射类型，请参阅常规操作配置指南。

步骤 5	*action* **示例：** `hostname(config-pmap-c)# drop-connection log`	指定您想对匹配流量执行的操作。操作因检测和匹配类型而异。常见操作包括：**drop**、**log** 和 **drop-connection**。对于每个匹配的可用操作，请参阅相应的检测章节。

步骤 6	**parameters**
	示例：
	`hostname(config-pmap)# parameters`
	`hostname(config-pmap-p)#`
		配置影响检测引擎的参数。CLI 进入参数配置模式。对于每个应用的可用参数，请参阅相应的检测章节。

示例

下面是一个 HTTP 检测策略映射以及相关类映射的示例。此策略映射由服务策略启用的第 3/4 层策略映射激活。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2

hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs

hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# protocol-violation action log

hostname(config-pmap-p)# policy-map test
hostname(config-pmap)# class test（未显示第 3/4 层类映射）
hostname(config-pmap-c)# inspect http http-map1

hostname(config-pmap-c)# service-policy test interface outside
```

在检测类映射中识别流量

此类型的类映射可以让您匹配某个应用特定的条件。例如，对于 DNS 流量，您可以匹配 DNS 查询中的域名。

类映射可以将多个流量匹配聚集在一起（在 match-all 类映射中），或者让您匹配在匹配列表中的任何一个（在 match-any 类映射中）。创建类映射和直接在检测策略映射中定义流量的差别在于，类映射可以让您将多个匹配命令聚集在一起并重用类映射。对于您在类映射中识别的流量，您可以指定操作，例如丢弃、重置和 / 或在检测策略映射中记录连接。如果您想对不同类型的流量执行不同操作，应当直接在策略映射中识别流量。

限制

并非所有应用都支持检测类映射。请参阅 **class-map type inspect** 的 CLI 帮助文件，了解支持的应用列表。

详细步骤

	命令	用途
步骤 1	（可选） 创建正则表达式。	请参阅常规操作配置指南。

步骤 2	**class-map type inspect** *application* [**match-all** | **match-any**] *class_map_name*
	
	示例：
	`hostname(config)# class-map type inspect http http_traffic`
	`hostname(config-cmap)#`
		创建检测类映射，其中 *application* 是您要检测的应用。对于支持的应用，请参阅 CLI 帮助文件，了解支持的应用列表，或者参阅第 7 章，“应用层协议检测入门”。
		参数 *class_map_name* 为类映射名称，最大长度为 40 个字符。
		match-all 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。
		关键字 **match-any** 指定如果流量匹配至少一个条件，则匹配类映射。
		CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

步骤 3	（可选） **description** *string* **示例：** `hostname(config-cmap)# description All UDP traffic`	向类映射添加说明。
步骤 4	输入一个或多个可用于应用的 **match** 命令，定义包含在类中的流量。	要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定字符串 “example.com”，则任何包含 “example.com” 的流量都不匹配类映射。 要查看每个应用可用的 **match** 命令，请参阅相应的检测章节。

示例

以下示例创建一个必须匹配所有条件的 HTTP 类映射：

```
hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs
```

以下示例创建一个可以匹配任意条件的 HTTP 类映射：

```
hostname(config-cmap)# class-map type inspect http match-any monitor-http
hostname(config-cmap)# match request method get
hostname(config-cmap)# match request method put
hostname(config-cmap)# match request method post
```

更多信息指南

要使用检测策略，请参阅第 1 章，“ 使用模块化策略框的服务策略 ”。

检测策略映射的功能历史

表 2-1 列出了此功能的版本历史。

表 2-1　　服务策略的功能历史

功能名称	版本	功能信息
检测策略映射	7.2(1)	引入了检测策略映射。引入了以下命令：**class-map type inspect**。
正则表达式和策略映射	7.2(1)	引入了正则表达式和策略映射，在检测策略映射下使用。引入了以下命令：**class-map type regex**、**regex**、**match regex**。
检测策略映射的 match any 命令	8.0(2)	引入了关键字 **match any**，与检测策略映射一起使用：流量可以匹配一个或多个条件以匹配类映射。过去，仅 **match all** 命令可用。

访问规则

本章描述如何使用访问规则，控制经由或至 ASA 的网络访问。在路由和透明防火墙模式下均可使用访问规则控制网络访问。在透明模式下，可同时使用访问规则（适用于第 3 层流量）和以太网类型规则（适用于第 2 层流量）。

注 要访问用于管理访问的 ASA 接口，也不需要允许主机 IP 地址的访问规则。只需按照常规操作配置指南配置管理访问。

- 第 3-1 页上的控制网络访问
- 第 3-6 页上的访问控制准则
- 第 3-7 页上的配置访问控制
- 第 3-9 页上的监控访问规则
- 第 3-10 页上的允许或拒绝网络访问的配置示例
- 第 3-11 页上的访问规则历史记录

控制网络访问

访问规则确定允许哪些流量通过 ASA。有多个不同的规则层，这些规则层共同实施访问控制策略：

- 分配至接口的扩展访问规则（第 3+ 层流量）- 可于入站和出站方向应用单独的规则集 (ACL)。扩展访问规则根据源和目标流量条件允许或拒绝流量。
- 全局分配的扩展访问规则 - 可创建用作默认访问控制的单个全局规则集。全局规则在接口规则之后应用。
- 管理访问规则（第 3+ 层流量）- 可应用单个规则集以覆盖接口处定向的流量，这通常是管理流量。在 CLI 中，这些是 “ 控制平面 ” 访问组。对于在设备处定向的 ICMP 流量，也可配置 ICMP 规则。
- 分配至接口（仅透明防火墙模式）的以太网类型规则（第 2 层流量）- 可在入站和出站方向应用单独的规则集。以太网类型规则控制针对非 IP 流量的网络访问。以太网类型规则根据以太网类型允许或拒绝流量。

在透明防火墙模式下，可在相同的接口上整合使用扩展访问规则、管理访问规则和以太网类型规则。

- 第 3-2 页上的有关规则的一般信息
- 第 3-4 页上的扩展访问规则
- 第 3-5 页上的以太网类型规则

有关规则的一般信息

本节介绍有关访问规则和以太网类型规则的信息，包含以下主题：

- 第 3-2 页上的接口访问规则和全局访问规则
- 第 3-2 页上的入站和出站规则
- 第 3-3 页上的规则顺序
- 第 3-3 页上的隐式允许
- 第 3-4 页上的隐式拒绝
- 第 3-4 页上的 NAT 和访问规则

接口访问规则和全局访问规则

可将访问规则应用于特定接口，也可将访问规则全局应用于所有接口。可结合接口访问规则配置全局访问规则，在此情况下，特定入站接口访问规则始终在通用全局访问规则之前得以处理。全局访问规则仅适用于入站流量。

入站和出站规则

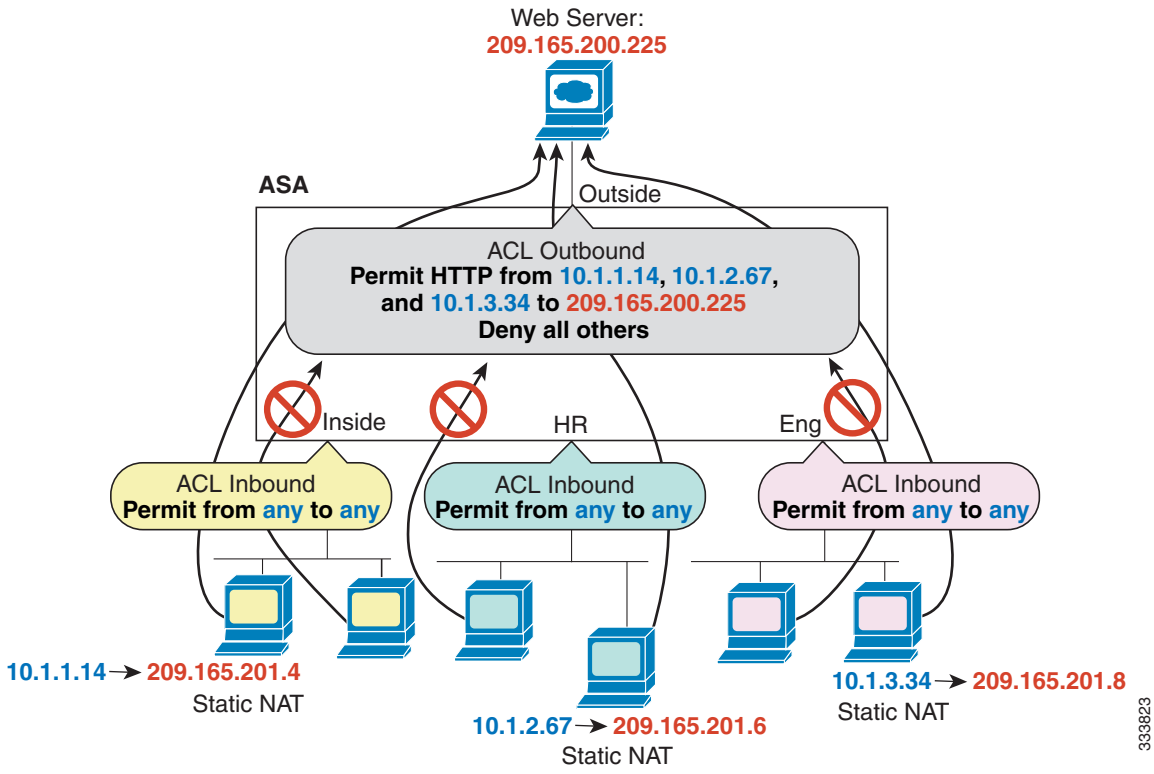
可根据流量的方向配置访问规则：

- 入站 - 入站访问规则在流量进入接口时应用于流量。全局访问规则和管理访问规则始终为入站规则。
- 出站 - 出站规则在流量离开接口时应用于流量。

注　“ 入站 ” 和 “ 出站 ” 是指 ACL 在接口上的应用，针对进入接口上 ASA 上的流量，或者离开接口上的 ASA 的流量。这些术语不是指流量从较低安全性接口至较高安全性接口的移动（通常称为入站），或者流量从较高安全性接口至较低安全性接口的移动（通常称为出站）。

出站 ACL 非常有用，例如，如果您想要仅允许内部网络上的某些主机访问外部网络上的某个网络服务器。可创建仅允许指定主机的单个出站 ACL，而不是创建多个入站 ACL 以限制访问。（请参阅下图。）出站 ACL 防止任何其他主机访问外部网络。

图 3-1　　出站 ACL



请见以下适用于本示例的命令：

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.1.14
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34
host 209.165.200.225 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

规则顺序

规则顺序非常重要。在 ASA 决定是否转发或丢弃数据包时，ASA 将按规则在已应用 ACL 中列出的顺序针对每条规则测试数据包。发现某个匹配后，不再检查其他规则。例如，如果在起始处创建的访问规则显式允许某接口的所有流量，则将不检查更多的规则。

隐式允许

对于路由模式，将默认允许以下类型的流量通过：

- 从较高安全性接口流向较低安全性接口的单播 IPv4 和 IPv6 流量。

对于透明模式，将默认允许以下类型的流量通过：

- 从较高安全性接口流向较低安全性接口的单播 IPv4 和 IPv6 流量。
- 两个方向上的 ARP 流量。（可使用 ARP 检测控制 ARP 流量，但不能通过访问规则控制该流量。）

- 两个方向上的 BPDU 流量。

对于其他流量，需要使用扩展访问规则（IPv4 和 IPv6）或以太网类型规则（非 IP）。

隐式拒绝

ACL 列表的末尾有隐式拒绝，因此，除非您显式允许流量，否则流量无法通过。例如，如果除特定地址外，您想要允许所有用户通过 ASA 访问某个网络，则需要拒绝这些特定地址，然后允许所有其他地址。

对于以太网类型 ACL，ACL 末尾处的隐式拒绝不会影响 IP 流量或 ARP 流量；例如，如果您允许以太网类型 8037，则 ACL 末尾处的隐式拒绝此时将不阻止您先前使用扩展 ACL 允许的任何 IP 流量（或者隐式允许的从较高安全性接口流向较低安全性接口的 IP 流量）。然而，如果您使用以太网类型规则显式拒绝所有流量，则将拒绝 IP 和 ARP 流量，仅物理协议流量（如自动协商流量）仍得以允许。

如果配置全局访问规则，则全局规则*之后*的隐式拒绝得以处理。请参阅以下操作顺序：

1. 接口访问规则。
2. 全局访问规则。
3. 隐式拒绝。

NAT 和访问规则

在确定访问规则匹配时，访问规则始终将使用真实 IP 地址，即使您已配置 NAT。例如，如果已为内部服务器 (10.1.1.5) 配置 NAT，以使该服务器在外部拥有公共可路由的 IP 地址 209.165.201.5，则用于允许外部流量访问内部服务器的访问规则需要引用该服务器的真实 IP 地址 (10.1.1.5)，而非映射地址 (209.165.201.5)。

扩展访问规则

本节介绍有关扩展访问规则的信息。

- 第 3-4 页上的用于返回流量的扩展访问规则
- 第 3-5 页上的使用访问规则允许通过透明防火墙的广播和组播流量
- 第 3-5 页上的管理访问规则

用于返回流量的扩展访问规则

对于路由和透明模式的 TCP 和 UDP 连接，不需要访问规则即可允许返回流量，因为 ASA 允许已建立的双向连接的所有返回流量。

然而，对于诸如 ICMP 的无连接协议，ASA 将建立单向会话，因此，您需要在两个方向访问规则以允许 ICMP（通过将 ACL 应用于源和目标接口），或需要启用 ICMP 检测引擎。ICMP 检测引擎将 ICMP 会话视为双向连接。要控制 ping，可指定**回显回复 (0)**（ASA 至主机）或**回显 (8)**（主机至 ASA）。

使用访问规则允许通过透明防火墙的广播和组播流量

在路由防火墙模式下，包括不受支持的动态路由协议和 DHCP 在内的广播和组播流量均将被阻止，即使已在访问规则中允许该流量（除非配置 DHCP 中继）。透明防火墙模式可允许任何 IP 流量通过。

注　由于这些特定类型的流量是无连接的，因此，您需要将访问规则应用于两个接口，以便允许返回流量通过。

下表列出了允许通过透明防火墙的常见流量类型。

表 3-1　　透明防火墙的特定流量

流量类型	协议或端口	备注
DHCP	UDP 端口 67 和 68	如果启用 DHCP 服务器，则 ASA 将不允许 DHCP 数据包通过。
EIGRP	协议 88	—
OSPF	协议 89	—
组播流	UDP 端口因应用而异。	组播流始终以 D 类地址为目标（224.0.0.0 至 239.x.x.x）。
RIP（v1 或 v2）	UDP 端口 520	—

管理访问规则

可配置控制以 ASA 为目标的管理流量的访问规则。入站管理流量（通过诸如 **http**、**ssh** 或 **telnet** 的命令定义）的访问控制规则拥有的优先级高于使用 **control-plane** 选项应用的管理访问规则。因此，将允许此类管理流量进入，即使其被入站 ACL 显式拒绝。

或者，可使用 ICMP 规则控制流向设备的 ICMP 流量。使用正则扩展访问规则可控制通过设备的 ICMP 流量。

以太网类型规则

本节介绍以太网类型规则。

- 第 3-5 页上的受支持的以太网类型流量和其他流量
- 第 3-6 页上的返回流量的以太网类型规则
- 第 3-6 页上的允许 MPLS

受支持的以太网类型流量和其他流量

以太网类型规则控制以下内容：

- 通过 16 位十六进制数标识的以太网类型，包括常见类型的 IPX 和 MPLS 单播或组播。
- 以太网 V2 帧。
- 默认允许的 BPDU。BPDU 为 SNAP 封装式，ASA 专用于处理 BPDU。

- Trunk 端口（思科专有）BPDU。Trunk BPDU 在负载内拥有 VLAN 信息，因此，如果允许 BPDU，则 ASA 将使用出站 VLAN 修改负载。
- 中间系统至中间系统 (IS-IS)。

以下类型的流量不受支持：

- 802.3 格式化帧 - 规则将不处理这些帧，因为它们使用长度字段而不是类型字段。

返回流量的以太网类型规则

因为以太网类型是无连接的，所以，如果想要在两个方向上允许流量通过，则需要在两个接口上应用规则。

允许 MPLS

如果允许 MPLS，请将连接至 ASA 的两个 MPLS 路由器配置为将 ASA 接口上的 IP 地址用作 LDP 或 TDP 会话的路由器 ID，从而确保标签分发协议和标记分发协议 TCP 连接通过 ASA 建立。（LDP 和 TDP 允许 MPLS 路由器协商用于转发数据包的标签（地址）。）

在 Cisco IOS 路由器上，输入适合您的协议 LDP 或 TDP 的命令。*interface* 为连接至 ASA 的接口。

```
hostname(config)# mpls ldp router-id interface force
```

或

```
hostname(config)# tag-switching tdp router-id interface force
```

访问控制准则

IPv6 准则

支持 IPv6。源和目标地址可能包括 IPv4 和 IPv6 地址的任意混合。

每用户 ACL 准则

- 每用户 ACL 使用 **timeout uauth** 命令中的值，但该值可由 AAA 每用户会话超时值覆盖。
- 如果由于每用户 ACL 而拒绝流量，则将记录系统日志消息 109025。如果允许流量，则将不生成系统日志消息。每用户 ACL 中的 **log** 选项将不产生影响。

附加准则和限制

- 通过启用对象组搜索，可减少搜索访问规则所需的内存，但这将以降低规则查找性能为代价。已启用的对象组搜索将不展开网络对象，而是根据这些组定义搜索匹配的访问规则。可使用 **object-group-search access-control** 命令设置此选项。
- 可使用访问组的事务提交模型，从而提高系统性能和可靠性。请参阅常规操作配置指南中的基本设置章节，了解详细信息。可使用 **asp rule-engine transactional-commit access-group** 命令。
- 在 ASDM 中，规则描述基于出现在 ACL 中规则之前的访问列表注释，对于在 ASDM 中创建的新规则，任何描述均将配置为相关规则之前的注释。然而，ASDM 中的数据包跟踪器匹配在 CLI 中在匹配规则之后配置的注释。

配置访问控制

以下主题解释如何配置访问控制。

- 第 3-7 页上的配置访问组
- 第 3-8 页上的配置 ICMP 访问规则

配置访问组

应先创建 ACL，然后才能创建访问组。有关详细信息，请参阅常规操作配置指南。

要将 ACL 绑定至接口，或将其全局应用，请使用以下命令：

```
access-group access_list {
{in | out} interface interface_name [per-user-override | control-plane] |
global}
```

示例：

```
hostname(config)# access-group outside_access in interface outside
```

对接口特定的访问组：

- 指定扩展或以太网类型 ACL 名称。可为每个 ACL 类型、每个接口、每个方向配置一个 **access-group** 命令，并配置一个控制平面 ACL。控制平面 ACL 必须是扩展 ACL。
- 关键字 **in** 将 ACL 应用于入站流量。关键字 **out** 将 ACL 应用于出站流量。
- 指定 **interface** 名称。
- 关键字 **per-user-override**（仅用于入站 ACL）允许下载后用于用户授权的动态用户 ACL 覆盖已分配至接口的 ACL。例如，如果接口 ACL 拒绝来自 10.0.0.0 的所有流量，但动态 ACL 允许来自 10.0.0.0 的所有流量，则动态 ACL 将覆盖该用户的接口 ACL。

  默认情况下，将不针对接口 ACL 匹配 VPN 远程访问流量。然而，如果使用 **no sysopt connection permit-vpn** 命令关闭此旁路，行为取决于是否在组策略中已应用 **vpn-filter** 以及是否已设置 **per-user-override** 选项：

  - No **per-user-override**, no **vpn-filter** - 针对接口 ACL 匹配流量。
  - No **per-user-override**, **vpn-filter** - 依次针对接口 ACL 和 VPN 过滤器匹配流量。
  - **per-user-override**, **vpn-filter** - 仅针对 VPN 过滤器匹配流量。
- 关键字 **control-plane** 指定规则是否适用于入站流量。

对于全局访问组，指定 **global** 关键字，以将扩展 ACL 应用于所有接口的入站方向流量。

示例

以下示例展示如何使用 **access-group** 命令：

```
hostname(config)# access-list outside_access permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group outside_access interface outside
```

access-list 命令可使任何主机使用端口 80 访问主机地址。**access-group** 命令指定 **access-list** 命令应用于进入外部接口的流量。

配置 ICMP 访问规则

默认情况下，可使用 IPv4 或 IPv6 向任何 ASA 接口发送 ICMP 数据包，以下情况例外：

- ASA 不响应定向至广播地址的 ICMP 回显请求。
- ASA 仅响应发送至流量进入的接口的 ICMP 流量；不能通过某个接口将 ICMP 流量发送至远端接口。

要保护设备免受攻击，可使用 ICMP 规则将对 ASA 接口的 ICMP 访问限制为特定主机、网络或 ICMP 类型。ICMP 规则的工作原理与访问规则类似，将对规则进行排序，与数据包匹配的第一条规则将定义操作。

如为某个接口配置任何 ICMP 规则，则将隐式拒绝 ICMP 规则添加至 ICMP 规则列表的末尾，从而更改默认行为。因此，如果想要仅拒绝几种消息类型，则须在 ICMP 规则列表的末尾纳入一条允许任何消息类型的规则，以便允许剩余的消息类型。

我们建议，始终为 ICMP 不可到达消息类型（类型 3）授予权限。拒绝 ICMP 不可到达消息将禁用 ICMP 路径 MTU 发现，这可能停止 IPsec 和 PPTP 流量。此外，IPv6 中的 ICMP 数据包用于 IPv6 邻居发现进程。请参阅 RFC 1195 和 RFC 1435，了解有关路径 MTU 发现的详细信息。

操作步骤

步骤 1　创建适用于 ICMP 流量的规则。

```
icmp {permit | deny} {host ip_address | ip_address mask | any}
[icmp_type] interface_name
```

如未指定 *icmp_type*，则规则将应用于所有类型。可输入编号或名称。要控制 ping，请指定回显回复 (0)（ASA 至主机）或回显 (8)（主机至 ASA）

对于地址，可将规则应用于 **any** 地址、单个 **host** 或某个网络 (*ip_address mask*)。

步骤 2　创建适用于 ICMPv6 (IPv6) 流量的规则。

```
ipv6 icmp {permit | deny} {host ipv6_address | ipv6-network/prefix-length | any}
[icmp_type] interface_name
```

如未指定 *icmp_type*，则规则将应用于所有类型。

对于地址，可将规则应用于 **any** 地址、单个 **host** 或某个网络 (*ipv6-network/prefix-length*)。

步骤 3　（可选）对 ICMP 不可到达消息设置速率限制，以使 ASA 显示在跟踪路由输出上。

```
icmp unreachable rate-limit rate burst-size size
```

示例

```
hostname(config)# icmp unreachable rate-limit 50 burst-size 1
```

速率限制可能为 1-100，1 为默认值。突发大小无意义，但必须为 1-10。

要允许将 ASA 显示为跃点之一的跟踪路由通过 ASA，需要在服务策略中提高速率限制，并启用 **set connection decrement-ttl** 命令。例如，以下策略将降低通过 ASA 的所有流量的生存时间 (TTL) 值。

```
class-map global-class
  match any
policy-map global_policy
  class global-class
  set connection decrement-ttl
```

示例

以下示例展示，如何允许除处于 10.1.1.15 的主机之外的所有主机使用 ICMP 流量侦测内部接口：

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

以下示例展示，如何允许处于 10.1.1.15 的主机仅使用 ping 来侦测内部接口：

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

以下示例展示，如何拒绝所有外部接口的 ping 请求，并允许所有外部接口的 packet-too-big 消息（以便支持路径 MTU 发现）：

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

以下示例展示，如何允许主机 2000:0:0:4::2 或前缀 2001::/64 上的主机 ping 外部接口：

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

监控访问规则

要监控网络访问，请输入以下命令：

- **clear access-list** *id* **counters**

  清除访问列表的命中计数。

- **show access-list** [*name*]

  显示访问列表，包括每个 ACE 的行号和命中计数。纳入 ACL 名称，否则您将看到所有访问列表。

- **show running-config access-group**

  显示已绑定至接口的当前 ACL。

评估访问规则的系统日志消息

使用系统日志事件查看器，如 ASDM 中的查看器，查看与访问规则相关的消息。

如果使用默认日志记录，则只会看到与显式拒绝的流对应的系统日志消息 106023。将不记录与规则列表末尾的 “ 隐式拒绝 ” 条目匹配的流量。

如果 ASA 受到攻击，则表明已拒绝数据包的系统日志消息数量可能十分庞大。我们建议您转而启用使用系统日志消息 106100 的日志记录，该记录提供每条规则（包括允许规则）的统计信息，且可使您限制所生成的系统日志消息的数量。或者，您可禁用给定规则的所有日志记录。

为消息 106100 启用日志记录时，如果数据包与 ACE 匹配，则 ASA 将创建流条目以跟踪特定间隔内收到的数据包的数量。ASA 将在首次命中以及在每个间隔结束时生成系统日志消息，从而确定间隔期间总命中数量和最后一个命中的时间戳。在每个间隔结束时，ASA 将命中计数重置为 0。如在间隔期间没有与 ACE 匹配的数据包，则 ASA 将删除流条目。为规则配置日志记录时，可控制间隔，甚至可控制每条规则的日志消息的严重性级别。

流是按源与目标 IP 地址、协议和端口定义的。由于对于相同两台主机之间的新连接而言源端口可能不同，且为该连接创建了新的流，因此，可能看不到相同的流递增。

不需要针对 ACL 检查属于已建立连接的已允许数据包；仅初始数据包将得以记录并纳入命中计数中。对于无连接的协议（如 ICMP），所有数据包均得以记录，即使它们是被允许的数据包，且所有已拒绝数据包均得以记录。

有关这些消息的详细信息，请参阅*系统日志消息指南*。

提示 为消息 106100 启用日志记录时，如果数据包与 ACE 匹配，则 ASA 将创建流条目以跟踪特定间隔内收到的数据包的数量。对于 ACE，ASA 拥有最大为 32 K 的日志记录流。在任何时间点，都可能有大量的流同时存在。为防止无限制地消耗内存和 CPU 资源，ASA 将限制并发*拒绝*流的数量，仅对拒绝流施加该限制（不施加于允许流），因为它们可能是潜在攻击。达到限制时，ASA 将不为日志记录创建新的拒绝流，直至现有流到期，并且发布消息 106101。可使用 **access-list alert-interval** *secs* 命令控制该消息的频率，并可以使用 **access-list deny-flow-max** *number* 命令控制缓存的拒绝流的最大数量。

允许或拒绝网络访问的配置示例

本小节包含允许或拒绝网络访问的典型配置示例。

以下示例为内部服务器 1 添加网络对象，为服务器执行静态 NAT 以及为内部服务器 1 启用来自外部的访问。

```
hostname(config)# object network inside-server1
hostname(config)# host 10.1.1.1
hostname(config)# nat (inside,outside) static 209.165.201.12

hostname(config)# access-list outside_access extended permit tcp any object inside-server1
eq www
hostname(config)# access-group outside_access in interface outside
```

以下示例允许所有主机在 **inside** 和 **hr** 网络之间进行通信，但仅允许特定主机访问外部网络：

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any

hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

例如，以下示例 ACL 允许源自内部接口的常见以太网类型流量：

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

以下示例允许通过 ASA 的一些以太网类型流量，但其将拒绝所有其他流量：

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

以下示例将拒绝以太网类型 0x1256 的流量，但允许两个接口上的所有其他流量：

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

以下示例使用对象组来允许内部接口上的特定流量：

```
!
hostname (config)# object-group service myaclog
hostname (config-service)# service-object tcp source range 2000 3000
hostname (config-service)# service-object tcp source range 3000 3010 destinatio$
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo

hostname(config)# access-list outsideacl extended permit object-group myaclog interface
inside any
```

访问规则历史记录

功能名称	平台版本	说明
接口访问规则	7.0(1)	使用 ACL 控制经由 ASA 的网络访问。 我们引入了以下命令：**access-group**。
全局访问规则	8.3(1)	引入了全局访问规则。 我们修改了以下命令：**access-group**。
标识防火墙的支持	8.4(2)	现可将标识防火墙用户和组用于源和目标。可将标识防火墙 ACL 与访问规则、AAA 规则组合使用，及用于 VPN 身份验证。 我们修改了以下命令：**access-list extended**。
IS-IS 流量的以太网类型 ACL 支持	8.4(5)、9.1(2)	在透明防火墙模式下，ASA 现可使用以太网类型 ACL 允许 IS-IS 流量通过。 我们修改了以下命令：**access-list ethertype** {**permit** | **deny**} **isis**。
对 TrustSec 的支持	9.0(1)	现可将 TrustSec 安全组用于源和目标。可将标识防火墙 ACL 与访问规则组合使用。 我们修改了以下命令：**access-list extended**。

功能名称	平台版本	说明
适用于 IPv4 和 IPv6 的统一 ACL	9.0(1)	ACL 现支持 IPv4 和 IPv6 地址。甚至可为源和目标指定 IPv4 和 IPv6 地址的混合。已将 **any** 关键字更改为代表 IPv4 和 IPv6 流量。已添加 **any4** 和 **any6** 关键字，分别用于代表纯 IPv4 和纯 IPv6 流量。IPv6 特定 ACL 已弃用。现有 IPv6 ACL 已迁移至扩展 ACL。有关迁移的详细信息，请参阅版本说明。 我们修改了以下命令：**access-list extended**、**access-list webtype**。 我们移除了以下命令：**ipv6 access-list**、**ipv6 access-list webtype**、**ipv6-vpn-filter**
用于按 ICMP 代码过滤 ICMP 流量的扩展 ACL 和对象增强	9.0(1)	现可根据 ICMP 代码允许 / 拒绝 ICMP 流量。 我们引入或修改了以下命令：**access-list extended**、**service-object**、**service**。
基于访问组规则引擎的事务提交模型	9.1(5)	启用时，规则更新将在规则编译完成后应用，而不影响规则匹配性能。 我们引入了以下命令：**asp rule-engine transactional-commit**、**show running-config asp rule-engine transactional-commit**、**clear configure asp rule-engine transactional-commit**。

第 2 部分

网络地址转换

网络地址转换 (NAT)

本章概述网络地址转换 (NAT) 在 ASA 上的工作原理。

- 第 4-1 页上的为何使用 NAT?
- 第 4-2 页上的 NAT 术语
- 第 4-2 页上的 NAT 类型
- 第 4-11 页上的路由和透明模式下的 NAT
- 第 4-14 页上的 NAT 和 IPv6
- 第 4-14 页上的如何实施 NAT
- 第 4-18 页上的 NAT 规则顺序
- 第 4-20 页上的 NAT 接口
- 第 4-20 页上的路由 NAT 数据包
- 第 4-23 页上的面向 VPN 的 NAT
- 第 4-30 页上的 DNS 和 NAT
- 第 4-35 页上的更多信息指南

注 要开始配置 NAT，请参阅第 5 章，“网络对象 NAT”， 或第 6 章，“两次 NAT”。

为何使用 NAT?

IP 网络中的每台计算机和设备都分配了标识主机的唯一 IP 地址。因为缺乏公用 IPv4 地址，所以这些 IP 地址中的大多数都是专用地址，在专用公司网络以外的任何地方都不可路由。RFC 1918 定义可以在内部使用但不应通告的专用 IP 地址：

- 10.0.0.0 到 10.255.255.255
- 172.16.0.0 到 172.31.255.255
- 192.168.0.0 到 192.168.255.255

NAT 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的合法的可路由地址。NAT 以此方式保存公用地址，因为它可配置为至少仅将整个网络的一个公用地址向外界通告。

NAT 的其他功能包括：

- 安全 - 隐藏内部 IP 地址可以阻止直接攻击。
- IP 路由解决方案 - 使用 NAT 时不会出现重叠 IP 地址。
- 灵活性 - 可以更改内部 IP 寻址方案，而不影响外部的可用公用地址；例如，对于可以访问互联网的服务器，您可以维护供互联网使用的固定 IP 地址，但在内部，您可以更改服务器地址。
- 在 IPv4 和 IPv6 之间转换（仅路由模式）- 如果想将 IPv6 网络连接到 IPv4 网络，可以利用 NAT 在两种类型的地址之间转换。

注　不需要 NAT。如果不为一组给定流量配置 NAT，将不转换这些流量，但会正常应用所有安全策略。

NAT 术语

本文档使用以下术语：

- 实际地址 / 主机 / 网络 / 接口 - 实际地址是指在主机上定义的转换前地址。在内部网络访问外部网络时，您想转换内部网络的典型 NAT 场景中，内部网络会成为“实际”网络。请注意，您可以转换任何连接到 ASA 的网络，不仅仅是内部网络。因此，如果配置 NAT 以转换外部地址，“实际”指的是访问内部网络时的外部网络。
- 映射地址 / 主机 / 网络 / 接口 - 映射地址是指实际地址转换而成的地址。在内部网络访问外部网络时，您想转换内部网络的典型 NAT 场景中，外部网络会成为“映射”网络。

注　在地址转换过程中，不会转换驻留在 ASA 的接口上的 IP 地址。

- 双向发起 - 静态 NAT 允许*双向*发起连接，意味着发起到主机和从主机发起。
- 源 NAT 和目标 NAT - 对于任何给定数据包，将源 IP 地址和目标 IP 地址与 NAT 规则进行比较，转换 / 不转换一个或两个地址。对于静态 NAT，规则是双向的，因此，请注意，整个本指南中命令和描述中使用的“源”和“目标”，即便是给定的连接，也可能源自“目标”地址。

NAT 类型

以下主题介绍各种类型的 NAT。

- 第 4-3 页上的 NAT 类型概述
- 第 4-3 页上的静态 NAT
- 第 4-8 页上的动态 NAT
- 第 4-10 页上的动态 PAT
- 第 4-11 页上的身份标识 NAT

NAT 类型概述

可以使用以下方法实施 NAT：

- 静态 NAT - 实际 IP 地址和映射 IP 地址之间的一致映射。允许双向流量发起。请参阅第 4-3 页上的静态 NAT。
- 动态 NAT - 按先到先得的方式，将一组实际 IP 地址映射到一组映射 IP 地址（通常较小）。仅实际主机可以发起流量。请参阅第 4-8 页上的动态 NAT。
- 动态端口地址转换 (PAT) - 使用 IP 地址的唯一源端口，将一组实际 IP 地址映射到单一 IP 地址。请参阅第 4-10 页上的动态 PAT。
- 身份标识 NAT - 系统将实际地址静态转换为其本身，基本绕过 NAT。当您想转换一大组地址，但又想免除一个较小的地址子集时，可能想这样配置 NAT。请参阅第 4-11 页上的身份标识 NAT。

静态 NAT

以下主题介绍静态 NAT。

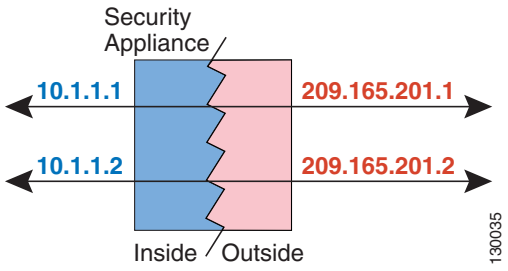
- 第 4-3 页上的关于静态 NAT
- 第 4-4 页上的带端口转换的静态 NAT
- 第 4-5 页上的一对多静态 NAT
- 第 4-7 页上的其他映射场景（不推荐）

关于静态 NAT

静态 NAT 创建实际地址到映射地址的固定转换。因为映射地址对于每个连续连接都是相同的，所以静态 NAT 允许双向连接发起，即到主机发起和从主机发起（如果有允许这样做的访问规则）。另一方面，通过动态 NAT 和 PAT，每台主机为每次后续转换使用不同的地址或端口，因此，不支持双向发起。

下图显示了典型的静态 NAT 场景。转换始终处于活动状态，所以，实际主机和远程主机可以发起连接。

图 4-1　　静态 NAT



注　如果需要，可以禁用双向性。

带端口转换的静态 NAT

通过带端口转换的静态 NAT，您可以指定实际和映射协议（TCP 或 UDP）及端口。

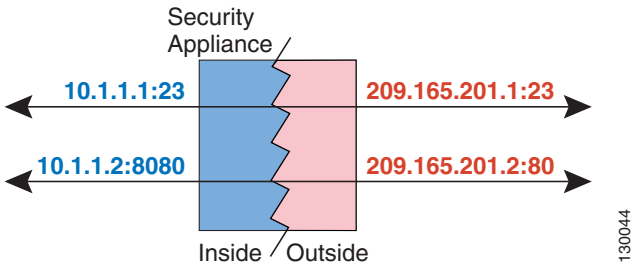
- 第 4-4 页上的关于带端口地址转换的静态 NAT
- 第 4-4 页上的带身份端口转换的静态 NAT
- 第 4-5 页上的面向非标准端口的带端口转换的静态 NAT
- 第 4-5 页上的带端口转换的静态接口 NAT

关于带端口地址转换的静态 NAT

指定带静态 NAT 的端口时，可以选择将端口和 / 或 IP 地址映射到同一值或不同值。

下图显示带端口转换的静态 NAT 场景，其中显示映射到本身的端口和映射到不同值的端口；在这两种情况下，IP 地址映射到不同值。转换始终处于活动状态，因此，转换主机和映射主机都能发起连接。

图 4-2　带端口转换的典型静态 NAT 场景

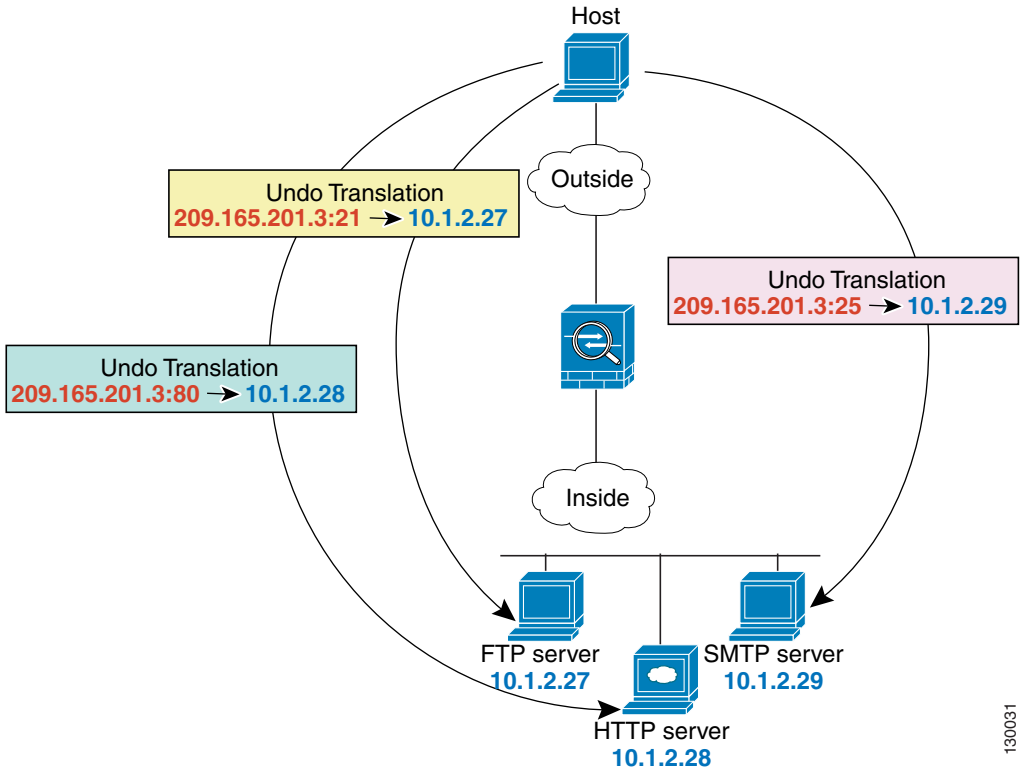


注　对于需要应用检测以寻找辅助信道的应用（例如，FTP 或 VOIP），ASA 会自动转换辅助端口。

带身份端口转换的静态 NAT

以下带端口转换的静态 NAT 示例为远程用户访问 FTP、HTTP 和 SMTP 提供单一地址。实际上，这些服务器是实际网络上的不同设备，但对于每台服务器，可以指定采用端口转换规则的静态 NAT，这些规则使用同一映射 IP 地址和不同端口。有关如何配置此示例的详细信息，请参阅第 5-19 页上的用于 FTP、HTTP 和 SMTP（带端口转换的静态 NAT）的单一地址。

图 4-3　带端口转换的静态 NAT



面向非标准端口的带端口转换的静态 NAT

还可以利用带端口转换的静态 NAT 将一个已知端口转换为一个非标准端口，反之亦然。例如，如果内部网络服务器使用端口 8080，您可以允许外部用户连接到端口 80，然后取消转换到原始端口 8080。同样，要提供额外安全性，您可以告知网络用户连接到非标准端口 6785，然后取消转换到端口 80。

带端口转换的静态接口 NAT

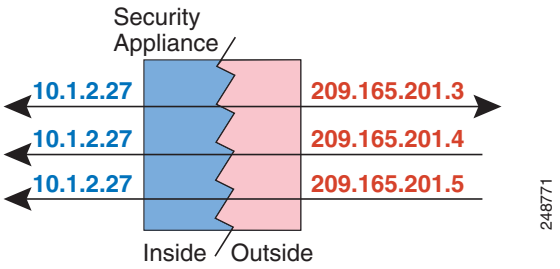
可以配置静态 NAT，以将一个实际地址映射到一个接口地址 / 端口组合。例如，如果要将 ASA 外部接口的 Telnet 访问重新定向到内部主机，可以将内部主机 IP 地址 / 端口 23 映射到 ASA 接口地址 / 端口 23。（请注意，尽管不允许到 ASA 的 Telnet 连接到安全性最低的接口，但带接口端口转换的静态 NAT 可以重新定向 Telnet 会话，而不是拒绝它）。

一对多静态 NAT

通常，配置带一对一映射的静态 NAT。然而，在某些情况下，您可能想要将单一实际地址配置到多个映射地址（一对多）。配置一对多静态 NAT 时，当实际主机发起流量时，它始终使用第一个映射地址。然而，对于发起到主机的流量，您可以发起到任何映射地址的流量，并且不将它们转换为单一实际地址。

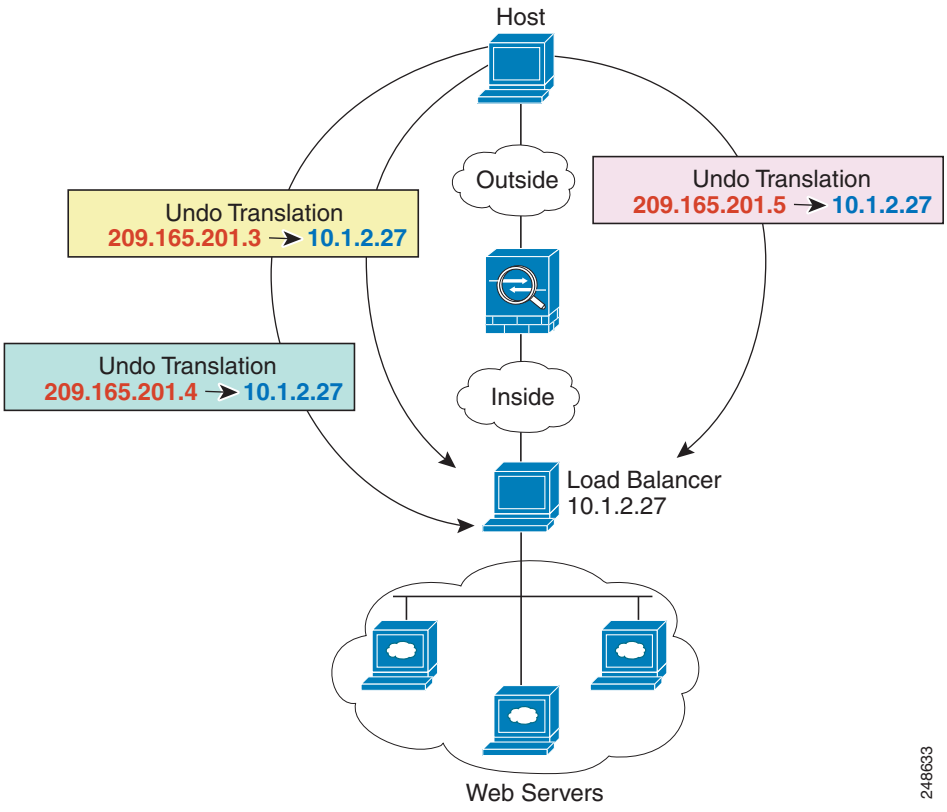
图 4-4 显示了典型的一对多静态 NAT 场景。因为实际主机做出的发起始终使用第一个映射地址，所以实际主机 IP/ 第一个映射 IP 的转换在技术上只能是双向转换。

图 4-4　　一对多静态 NAT



例如，在 10.1.2.27 上有一个负载平衡器。根据请求的 URL，它会将流量重新定向到正确的网络服务器。有关如何配置此示例的详细信息，请参阅第 5-18 页上的有多个映射地址的内部负载平衡器（静态 NAT，一对多）。

图 4-5　　一对多静态 NAT 示例



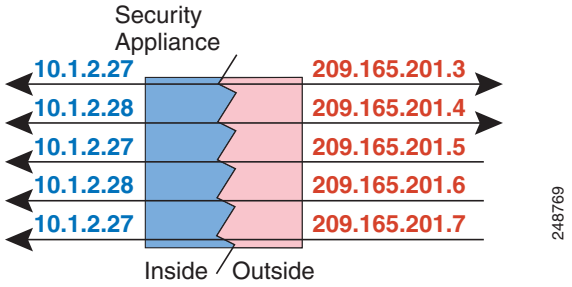
其他映射场景（不推荐）

ASA 可以灵活地允许任何类别的静态映射场景：一对一、一对多、少对多、多对少、多对一映射。我们推荐仅使用一对一或一对多映射。其他映射选项可能会导致意外后果。

在功能上，少对多与一对多相同；但是，因为此配置更加复杂，而且实际映射可能不会一目了然，所以我们建议为每个需要一对多配置的实际地址创建该配置。例如，对于少对多场景，少量的实际地址会按顺序映射到多个映射地址（A 到 1、B 到 2、C 到 3）。当映射所有实际地址时，下一个映射地址会映射到第一个实际地址，等等，直到映射了所有映射地址为止（A 到 4、B 到 5、C 到 6）。这将导致每个实际地址有多个映射地址。就像一对多配置一样，仅第一个映射是双向的；后续映射可以将流量发起*到*实际主机，但所有*从*实际主机发起的流量仅将第一个映射地址用于源。

下图显示了一个典型的少对多静态 NAT 场景。

图 4-6　　少对多静态 NAT

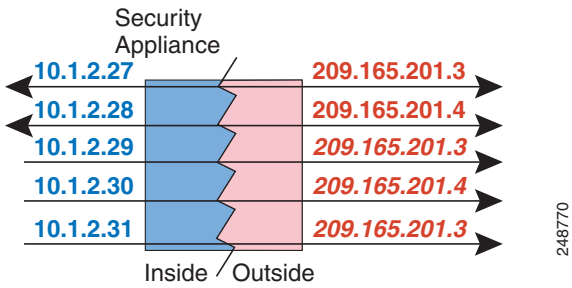


对于实际地址多于映射地址的多对少或多对一配置，映射地址会在实际地址用尽之前先用尽。仅最低实际 IP 地址和映射池之间的映射可以导致双向发起。剩余的更高的实际地址可以发起流量，但不能将流量发起到这些地址（由于唯一五元组 [源 IP、目标 IP、源端口、目标端口、协议]，连接的返回流量会定向到正确的实际地址）。

注　多对少或多对一 NAT 不是 PAT。如果两台实际主机使用同一源端口号，连接到同一外部服务器和同一 TCP 目标端口，并且两台主机转换到同一 IP 地址，那么由于地址冲突（五元组不是唯一的），将重置两个连接。

下图显示一个典型的多对少静态 NAT 场景。

图 4-7　　多对少静态 NAT



我们建议不要这样使用静态规则，而是为需要双向发起的流量创建一对一规则，为其他地址创建动态规则。

动态 NAT

以下主题介绍动态 NAT。

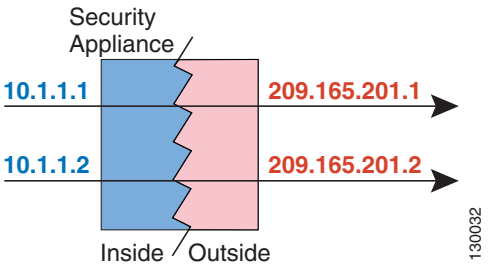
- 第 4-8 页上的关于动态 NAT
- 第 4-9 页上的动态 NAT 的缺点和优点

关于动态 NAT

动态 NAT 将一个实际地址组转换为一个可在目标网络上路由的映射地址池。映射池通常包含少于实际地址组的地址。当您要转换的主机访问目标网络时，ASA 从映射池为主机分配一个 IP 地址。仅在实际主机发起连接时创建转换。转换仅在连接期间发生，而且转换超时后，给定用户不保存同一 IP 地址。因此，目标网络上的用户不能向使用动态 NAT 的主机发起可靠连接，即使访问规则允许该连接。

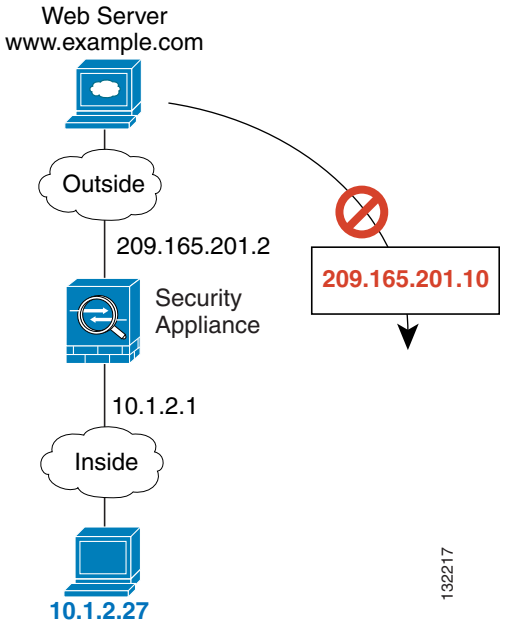
下图显示典型的动态 NAT 场景。仅实际主机可以创建 NAT 会话，允许响应流量返回。

图 4-8　　动态 NAT



下图显示一台远程主机尝试发起到映射地址的连接。此地址当前不在转换表中；因此，ASA 丢弃该数据包。

图 4-9　　远程主机尝试向映射地址发起连接



注　在转换期间，如果访问规则允许到转换主机的连接，远程主机可以发起该连接。因为地址不可预测，所以到主机的连接不可能发生。然而，在这种情况下，您可以依靠访问规则的安全性。

动态 NAT 的缺点和优点

动态 NAT 有以下缺点：

- 如果映射池的地址少于实际组，并且流量数量大于预期，可能会用尽地址。

  如果此事件经常发生，请使用 PAT 或 PAT 退回方法，因为 PAT 可以使用单一地址的端口提供超过 64,000 次转换。
- 您不得不利用映射池中的大量可路由地址，而且可能没有大量的可路由地址可用。

动态 NAT 的优点在于，某些协议不能使用 PAT。PAT 不作用于以下各项：

- 没有超载端口的 IP 协议，例如 GRE 0 版本。
- 某些多媒体应用，它们在一个端口上有数据流，在另一个端口上有控制路径，并且不是开放标准。

有关 NAT 和 PAT 支持的详细信息，请参阅第 7-5 页上的默认检测和 NAT 限制。

动态 PAT

以下主题介绍动态 PAT。

- 第 4-10 页上的有关动态 PAT
- 第 4-10 页上的每会话 PAT 与多会话 PAT
- 第 4-11 页上的动态 PAT 缺点和优点

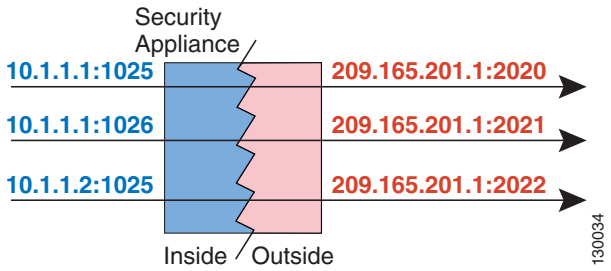
有关动态 PAT

通过将实际地址和源端口转换为映射地址和唯一端口，动态 PAT 可以将多个实际地址转换为单一映射地址。如果可用，真实源端口号将用于映射端口。然而，如果真实端口*不*可用，将默认从与真实端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，低于 1024 的端口仅拥有很小的可用 PAT 池。如果您有大量使用较低端口范围的流量，可以指定一个要使用的单一端口范围，而不是三个大小不等的层。

每个连接都需要单独的转换会话，因为每个连接的源端口都不同。例如，10.1.1.1:1025 需要来自 10.1.1.1:1026 的单独的转换。

下图显示一个典型的动态 PAT 场景。仅实际主机可以创建 NAT 会话，允许响应流量返回。映射地址对于每次转换都是相同的，但端口需要动态分配。

图 4-10　　动态 PAT



在连接过期后，端口转换也将过期。对于多会话 PAT，使用 PAT 超时，默认情况下为 30 秒。对于每会话 PAT，立即删除 xlate。目标网络上的用户不能可靠地发起到使用 PAT 的主机的连接（即使访问规则允许该连接）。

注　在转换期间，如果访问规则允许到转换主机的连接，远程主机可以发起该连接。因为端口地址（实际和映射）不可预测，所以到该主机的连接不可能发生。然而，在这种情况下，您可以依靠访问规则的安全性。

每会话 PAT 与多会话 PAT

每会话 PAT 可以提高 PAT 的可扩展性，对于集群，允许每个成员单元拥有自己的 PAT 连接；多会话 PAT 连接必须转发到主单元并且归主单元所有。每会话 PAT 会话结束时，ASA 将发送重置，并立即移除转换。此重置将导致结束节点立即释放连接，从而避免 TIME_WAIT 状态。另一方面，多会话 PAT 使用 PAT 超时，默认情况下为 30 秒。

对于“肇事逃逸”流量，例如 HTTP 或 HTTPS，每会话 PAT 可以显著增加一个地址支持的连接速率。不使用每会话 PAT，IP 协议的一个地址的最大连接速率大约为每秒 2000。使用每会话 PAT，IP 协议的一个地址的连接速率为 65535/ *平均生命周期*。

默认情况下，所有 TCP 流量和 UDP DNS 流量均使用每会话 PAT 转换。对于可以受益于多会话 PAT 的流量，例如 H.323、SIP 或 Skinny，您可以创建每会话拒绝规则，以禁用每会话 PAT。请参阅第 5-13 页上的配置每会话 PAT 规则。

动态 PAT 缺点和优点

通过动态 PAT，可以使用单一映射地址，从而保存可路由地址。您甚至可以将 ASA 接口 IP 地址用作 PAT 地址。

动态 PAT 不作用于某些数据流不同于控制路径的多媒体应用。有关 NAT 和 PAT 支持的详细信息，请参阅第 7-5 页上的默认检测和 NAT 限制。

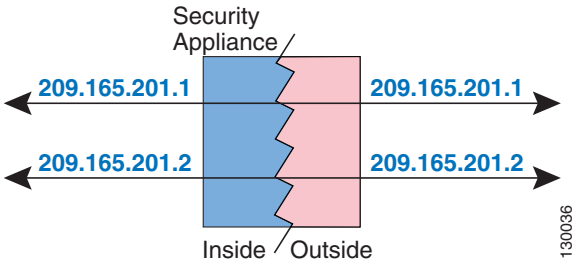
动态 PAT 还可以创建大量显示为来自单一 IP 地址的连接，服务器可以将流量解释为 DoS 攻击。您可以配置一个 PAT 地址池，使用 PAT 地址轮询分配减少这种情况。

身份标识 NAT

您可能有一个 NAT 配置，在其中需要将 IP 地址转换为其本身。例如，如果创建一条将 NAT 应用于每个网络的大体的规则，但想使一个网络免于 NAT，则可以创建一条静态 NAT 规则，以将地址转换为其本身。身份标识 NAT 是远程访问 VPN 所必需的，您需要使客户端流量免于 NAT。

下图显示一个典型的身份标识 NAT 场景。

图 4-11　身份标识 NAT



路由和透明模式下的 NAT

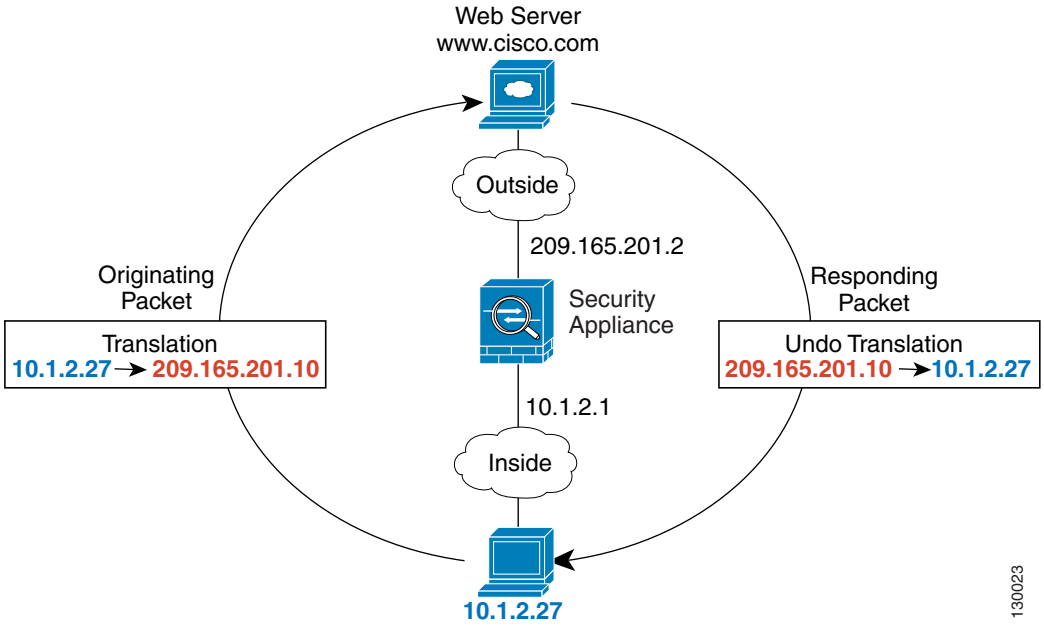
您可以在路由和透明防火墙模式下配置 NAT。本节介绍每个防火墙模式的典型用途。

- 第 4-12 页上的路由模式下的 NAT
- 第 4-12 页上的透明模式下的 NAT

路由模式下的 NAT

下图显示路由模式下的一个典型 NAT 示例，专用网络位于内部。

图 4-12　NAT 示例：路由模式



1. 当位于 10.1.2.27 的内部主机将数据包发送到网络服务器时，数据包的实际源地址 10.1.2.27 被更改为映射地址 209.165.201.10。
2. 当服务器响应时，它会将响应发送到映射地址 209.165.201.10，ASA 接收数据包，因为 ASA 执行代理 ARP 以认领数据包。
3. 接下来，ASA 变更从映射地址 209.165.201.10 回到实际地址 10.1.2.27 的转换，然后再发送到主机。

透明模式下的 NAT

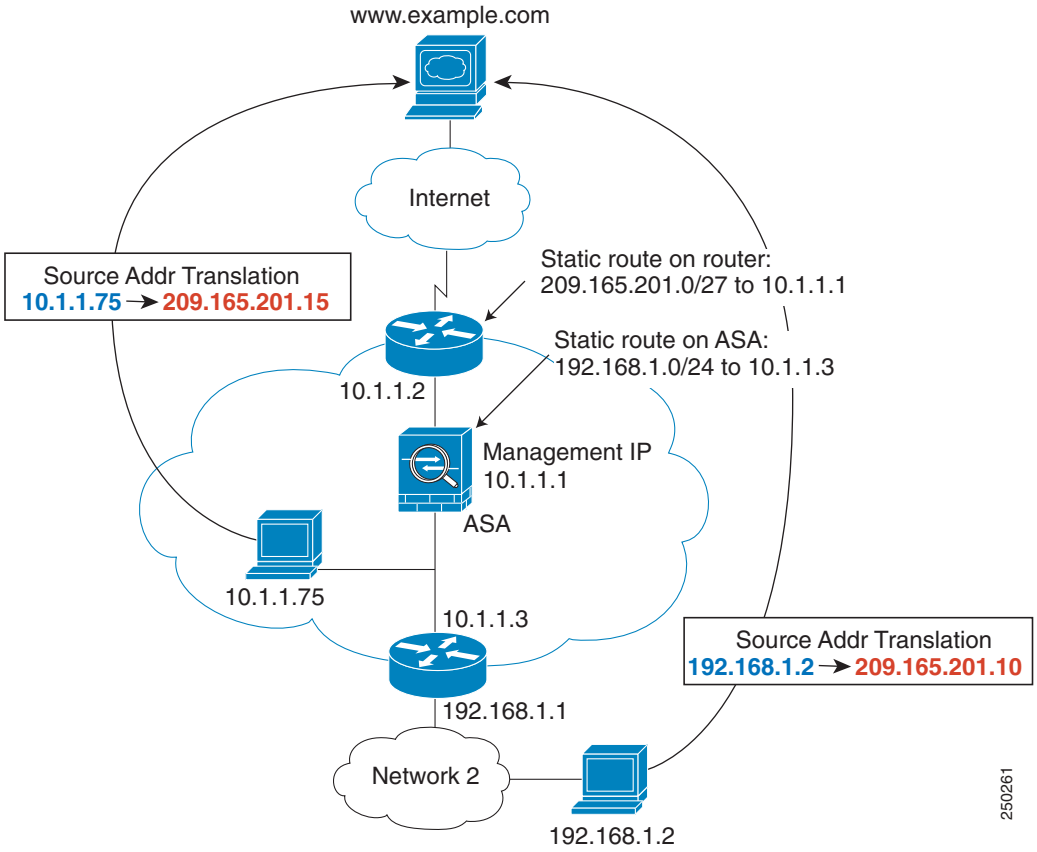
在透明模式下使用 NAT 可以消除上游或下游路由器为它们的网络执行 NAT 的需求。

透明模式下的 NAT 有以下要求和限制：

- 因为透明防火墙没有任何接口 IP 地址，所以不能使用接口 PAT。
- 不支持 ARP 检测。此外，如果由于某种原因，ASA 一端的主机向 ASA 另一端的主机发送 ARP 请求，而且发起主机实际地址被映射到同一子网的不同地址，那么实际地址在 ARP 请求中依然可见。
- 不支持在 IPv4 和 IPv6 网络之间进行转换。支持在两个 IPv6 网络之间或两个 IPv4 网络之间进行转换。

下图显示透明模式下的典型 NAT 场景，内部接口和外部接口上的网络相同。在此场景中，透明防火墙执行 NAT 服务，因此，上游路由器不必执行 NAT。

图 4-13　　NAT 示例：透明模式



1. 当位于 10.1.1.75 的内部主机向网络服务器发送数据包时，数据包的实际源地址 10.1.1.75 被更改为映射地址 209.165.201.15。
2. 当服务器响应时，它将响应发送到映射地址 209.165.201.15，ASA 接收数据包，因为上游路由器将此映射网络包含在定向到 ASA 管理 IP 地址的静态路由中。有关所需路由的详细信息，请参阅第 4-20 页上的映射地址和路由。
3. 然后，ASA 取消映射地址 209.165.201.15 回到实际地址 10.1.1.1.75 的转换。因为实际地址是直接连接的，所以 ASA 将实际地址直接发送到主机。
4. 对于主机 192.168.1.2，发生相同流程，但返回流量除外，ASA 在其路由表中查询路由，根据 192.168.1.0/24 的 ASA 静态路由，将数据包发送到位于 10.1.1.3 的下游路由器。有关所需路由的详细信息，请参阅第 4-23 页上的远程网络的透明模式路由要求。

NAT 和 IPv6

您可以使用 NAT 在 IPv6 网络之间转换，以及在 IPv4 和 IPv6 网络之间转换（仅路由模式）。我们推荐以下最佳实践：

- NAT66（IPv6 对 IPv6）- 我们建议使用静态 NAT。尽管您可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此您不必使用动态 NAT。如果不想允许返回流量，可以使静态 NAT 规则成为单向的（仅两次 NAT）。
- NAT46（IPv4 对 IPv6）- 我们建议使用静态 NAT。因为 IPv6 地址空间远远大于 IPv4 地址空间，所以可以轻松满足静态转换需求。如果不想允许返回流量，可以使静态 NAT 规则成为单向的（仅两次 NAT） 转换为 IPv6 子网（/96 或更低）时，默认情况下，生成的映射地址为有嵌入 IPv4 的 IPv6 地址，其中 32 位 IPv4 地址嵌入在 IPv6 前缀后面。例如，如果 IPv6 前缀为 /96 前缀，则 IPv4 地址附在最后的 32 位地址中。例如，如果将 192.168.1.0/24 映射到 201b::0/96，则 192.168.1.4 将被映射到 201b::0.192.168.1.4（通过混合表示法显示）。如果前缀较小（例如 /64），则 IPv4 地址附在前缀的后面，后缀 0 附在 IPv4 地址后面。或者，您还能够以网络对网络的方式转换地址，其中第一个 IPv4 地址映射到第一个 IPv6 地址，第二个 IPv4 地址映射到第二个 IPv6，依次类推。
- NAT64（IPv6 到 IPv4）- 您可能没有足够的 IPv4 地址来容纳大量的 IPv6 地址。我们建议使用动态 PAT 池提供大量的 IPv4 转换。

有关特定的实施准则和限制，请参阅配置章节。

如何实施 NAT

ASA 可以通过两种方法实施地址转换：*网络对象 NAT* 和*两次 NAT*。

- 第 4-14 页上的网络对象 NAT 和两次 NAT 之间的主要差异
- 第 4-15 页上的网络对象 NAT
- 第 4-15 页上的两次 NAT

网络对象 NAT 和两次 NAT 之间的主要差异

这两类 NAT 之间的主要差异是：

- 定义实际地址的方法。
  - 网络对象 NAT - 将 NAT 定义为网络对象的参数。网络对象命名 IP 主机、范围或子网，以便您能在 NAT 配置中使用对象，而不是实际 IP 地址。网络对象 IP 地址用作实际地址。通过此方法，您可以轻松将 NAT 添加到可能已在配置的其他部分使用的网络对象。
  - 两次 NAT - 识别实际地址和映射地址的网络对象或网络对象组。在这种情况下，NAT 不是网络对象的参数；网络对象或组是 NAT 配置的参数。可以使用实际地址的网络对象*组*意味着两次 NAT 更具可扩展性。
- 实施源和目标 NAT 的方法。
  - 网络对象 NAT - 每条规则都能应用于数据包的源或目标。因此，可能使用两条规则，一条用于源 IP 地址，一条用于目标 IP 地址。这两条规则不能绑在一起以对源 / 目标组合实施特定转换。
  - 两次 NAT - 单一规则可以转换源和目标。匹配数据包仅匹配一条规则，不检查更多规则。即使不为两次 NAT 配置可选的目标地址，匹配数据包依然仅匹配一条两次 NAT 规则。源和目标绑在一起，使您可以根据源 / 目标组合实施不同的转换。例如，源 A/ 目标 A 可以有不同于源 A/ 目标 B 的转换。

- NAT 规则顺序。
  - 网络对象 NAT - 在 NAT 表中自动排序。
  - 两次 NAT - 在 NAT 表中手动排序（在网络对象 NAT 规则之前或之后）。

  有关详细信息，请参阅第 4-18 页上的 NAT 规则顺序。

我们建议使用网络对象 NAT，除非您需要两次 NAT 提供的额外功能。网络对象 NAT 更容易配置，而且可能对应用（例如 Voice over IP (VoIP)）更加可靠。（对于 VoIP，因为两次 NAT 仅在两个对象之间适用，所以您可能会看到不属于任何一个对象的间接地址转换失败。）

网络对象 NAT

配置为网络对象的参数的所有 NAT 规则都被视为*网络对象 NAT* 规则。网络对象 NAT 是一种为网络对象配置 NAT 的快捷方便的方法，网络对象可以是单一 IP 地址、地址范围或子网。

配置网络对象之后，您可以接着将该对象的映射地址识别为内联地址或者另一个网络对象或网络对象组。

当数据包进入 ASA 时，根据网络对象 NAT 规则检查源 IP 地址和目标 IP 地址。如果进行独立匹配，可根据独立规则转换数据包中的源地址和目标地址。这些规则互不牵连，可以根据流量使用不同的规则组合。

因为规则从未配对，所以您不能指定源 A/ 目标 A 应当有不同于源 A/ 目标 B 的转换。将两次 NAT 用于此类功能（两次 NAT 可以让您识别单一规则中的源地址和目标地址）。

要开始配置网络对象 NAT，请参阅第 5 章，“ 网络对象 NAT”。

两次 NAT

两次 NAT 可供您在单一规则中同时确定源和目标地址。指定源地址和目标地址，可以让您指定源 A/ 目标 A 有不同于源 A/ 目标 B 的转换。

目标地址是可选的。如果指定目标地址，可以将它映射到其本身（身份标识 NAT），或者将它映射到不同的地址。目标映射始终是静态映射。

两次 NAT 还可以让您将服务对象用于带端口转换的静态 NAT ；网络对象 NAT 仅接受内联定义。

要开始配置两次 NAT，请参阅第 6 章，“ 两次 NAT”。

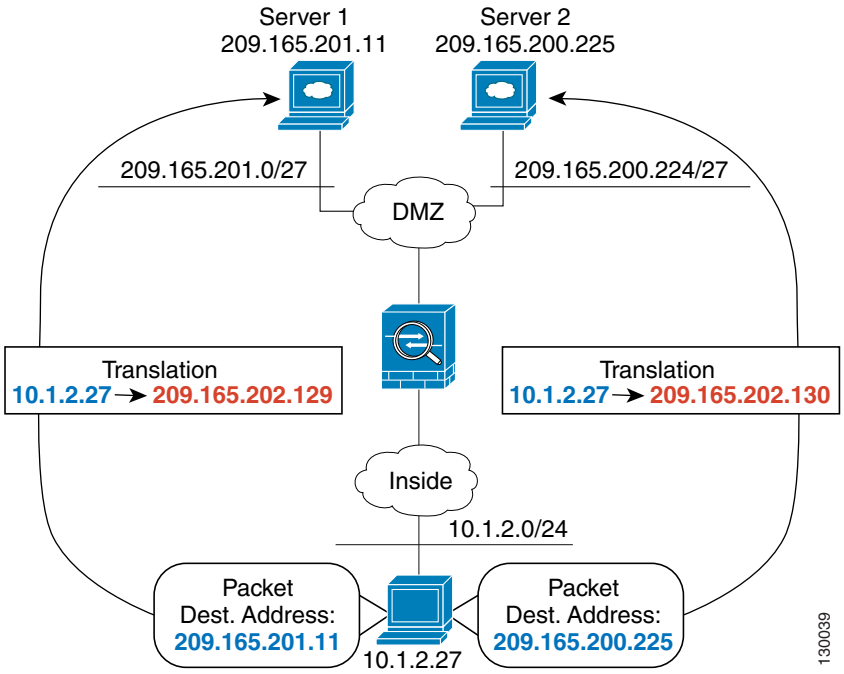
以下主题提供一些两次 NAT 的示例。

- 第 4-16 页上的示例：使用不同目标地址的两次 NAT
- 第 4-17 页上的示例：使用不同目标端口的两次 NAT
- 第 4-18 页上的示例：带目标地址转换的两次 NAT

示例：使用不同目标地址的两次 NAT

下图显示 10.1.2.0/24 网络上的一台主机正在访问两台不同的服务器。当主机访问位于 209.165.201.11 的服务器时，实际地址被转换为 209.165.202.129。当主机访问位于 209.165.200.225 的服务器时，实际地址被转换为 209.165.202.130。有关如何配置此示例的详细信息，请参阅第 5-19 页上的用于 FTP、HTTP 和 SMTP（带端口转换的静态 NAT）的单一地址。

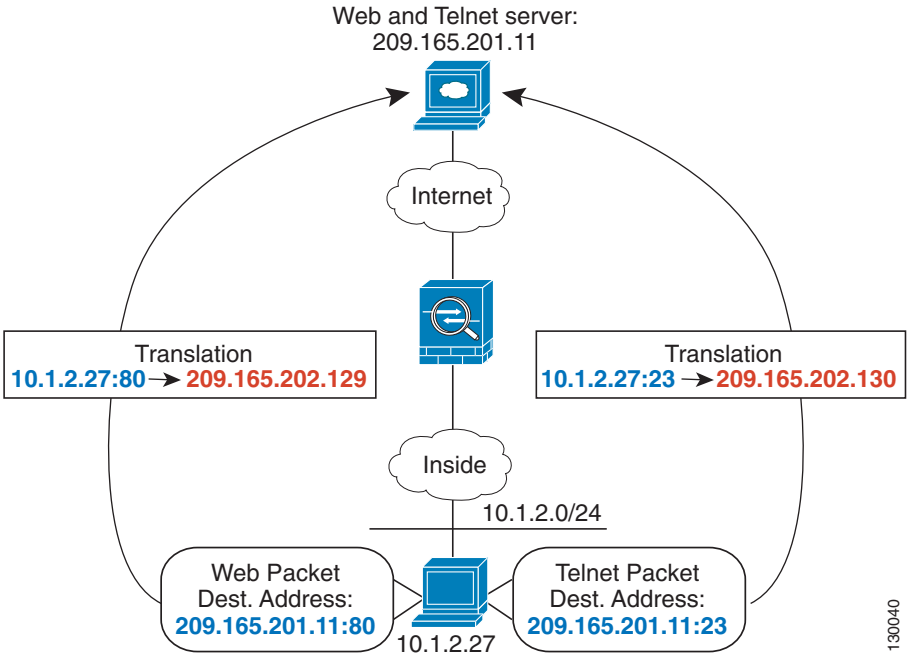
图 4-14　使用不同目标地址的两次 NAT



示例：使用不同目标端口的两次 NAT

下图显示源端口和目标端口的使用情况。10.1.2.0/24 网络上的主机同时因为网络服务和 Telnet 服务访问单个主机。当主机访问服务器以获取网络服务时，实际地址被转换为 209.165.202.129。当主机访问同一服务器以获取 Telnet 服务时，实际地址被转换为 209.165.202.130。

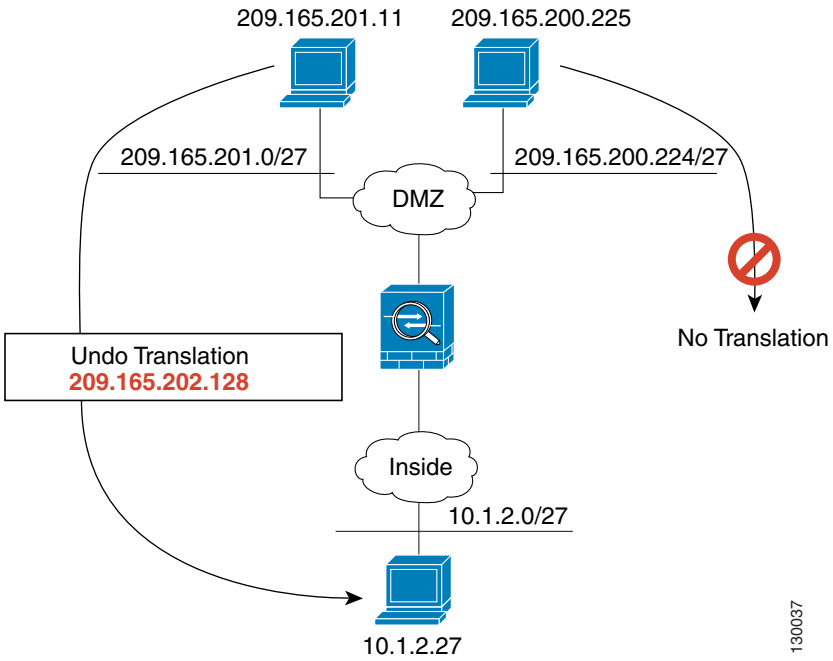
图 4-15　使用不同目标端口的两次 NAT



示例：带目标地址转换的两次 NAT

下图显示一台连接到映射主机的远程主机。映射主机有一个两次静态 NAT 转换，将仅面向流量的实际地址转换到 209.165.201.0/27 网络或从 209.165.201.0/27 网络转换。不存在面向 209.165.200.224/27 网络的转换，因此，转换主机不能连接到该网络，该网络上的主机也不能连接到转换主机。

图 4-16　带目标地址转换的两次静态 NAT



NAT 规则顺序

网络对象 NAT 规则和两次 NAT 规则存储在划分为三部分的单个表中。首先应用第一部分规则，其次是第二部分，最后是第三部分，直到找到匹配项为止。例如，如果在第一部分找到匹配项，则不评估第二部分和第三部分。下表显示每个部分的规则顺序。

表 4-1　NAT 规则表

表部分	规则类型	部分中的规则顺序
第一部分	两次 NAT	在第一个匹配的基础上，按照在配置中出现的顺序应用。因为应用了第一个匹配，必须确保特定规则位于更加通用的规则前面，否则不能按预期应用特定规则。默认情况下，两次 NAT 规则添加到第一部分。 **注**　如果配置 EasyVPN Remote，ASA 动态地将不可见 NAT 规则添加到此部分的末尾。确保勿在此部分配置可能匹配 VPN 流量而不匹配不可见规则的两次 NAT 规则。如果 VPN 由于 NAT 故障而无法工作，请考虑将两次 NAT 规则添加到第三部分。

表 4-1　NAT 规则表

表部分	规则类型	部分中的规则顺序
第二部分	网络对象 NAT	如果在第一部分没有找到匹配项，则按 ASA 自动确定的以下顺序应用第二部分规则： 1. 静态规则。 2. 动态规则。 **在每个规则类型中，使用以下排序准则：** 1. 实际 IP 地址数量 - 从最小到最大。例如，带一个地址的对象将在带 10 个地址的对象之前进行评估。 2. 如果数量相同，则按从最低到最高的顺序使用 IP 地址编号。例如，10.1.1.0 在 11.1.1.0 之前进行评估。 3. 如果使用同一 IP 地址，则按字母数字顺序使用网络对象名称。例如，abracadabra 在 catwoman 之前进行评估。
第三部分	两次 NAT	如果仍未找到匹配项，则按照在配置中出现的顺序，在第一个匹配的基础上应用第三部分规则。此部分应当包含最通用的规则。您还必须确保此部分的任何特定规则在以其他方式应用通用规则之前进行。添加规则时，可以指定是否将两次 NAT 规则添加到第三部分。

例如，对于第二部分规则，在网络对象中已定义以下 IP 地址：

192.168.1.0/24（静态）

192.168.1.0/24（动态）

10.1.1.0/24（静态）

192.168.1.1/32（静态）

172.16.1.0/24（动态）（对象 def）

172.16.1.0/24（动态）（对象 abc）

结果排序可能是：

192.168.1.1/32（静态）

10.1.1.0/24（静态）

192.168.1.0/24（静态）

172.16.1.0/24（动态）（对象 abc）

172.16.1.0/24（动态）（对象 def）

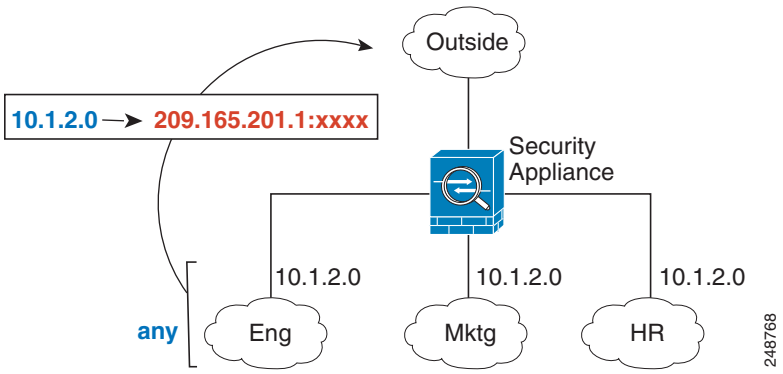
192.168.1.0/24（动态）

NAT 接口

您可以将 NAT 规则配置为应用到任何接口（换句话说，所有接口），或者可以识别特定的实际接口和映射接口。还可以为实际地址指定任何接口，为映射地址指定特定接口，反之亦然。

例如，如果在多个接口上使用相同的专用地址，并且在访问外部接口时要将这些地址全部转换到同一全局池，则您可能想为实际地址指定任何接口，并且为映射地址指定外部接口。

图 4-17　　指定任何接口



注　对于透明模式，必须选择特定源接口和目标接口。

路由 NAT 数据包

ASA 需要成为发送到映射地址的任何数据包的目标。此外，ASA 还需要为它收到的以映射地址为目标的数据包确定出口接口。本节介绍 ASA 如何处理通过 NAT 接受和交付数据包。

- 第 4-20 页上的映射地址和路由
- 第 4-23 页上的远程网络的透明模式路由要求
- 第 4-23 页上的确定出口接口

映射地址和路由

当您将实际地址转换为映射地址时，如果需要，您选择的映射地址将确定如何为映射地址配置路由。

请参阅第 5 章，“ 网络对象 NAT” 和第 6 章，“ 两次 NAT”，了解有关映射 IP 地址的其他指南

以下主题解释映射地址类型：

- 第 4-21 页上的与映射接口位于同一网络中的地址
- 第 4-21 页上的唯一网络上的地址
- 第 4-21 页上的与实际地址相同的地址（身份标识 NAT）

与映射接口位于同一网络中的地址

如果使用与映射接口位于同一网络中的地址，ASA 使用代理 ARP 响应任何对映射地址的 ARP 请求，从而解释以映射地址为目标的流量。此解决方案可以简化路由，因为 ASA 不必成为任何其他网络的网关。如果外部网络包含足够多的空闲地址，并且您正在使用 1:1 转换（例如动态 NAT 或静态 NAT），此解决方案是理想选择。动态 PAT 可以显著增加您可以通过少量地址实现的转换数量，因此，即使外部网络中的可用地址较少，依然可以使用此方法。对于 PAT，您甚至可以使用映射接口的 IP 地址。

注　如果将映射接口配置为任何接口，而且在与其中一个映射接口相同的网络中指定映射地址，那么如果对此映射地址的 ARP 请求在*不同*接口上进入，则需要为入口接口上的该网络手动配置 ARP 条目，指定其 MAC 地址（请参阅 **arp** 命令）。通常，如果该映射接口指定任何接口，则将唯一网络用于此映射地址，避免此类情况发生。

唯一网络上的地址

如果您需要的地址数量多于映射接口网络上的可用地址数量，则可以识别不同子网上的地址。上游路由器需要对指向 ASA 的映射地址进行静态路由。或者，对于路由模式，您可以将目标网络上的任何 IP 地址用作网关，为映射地址配置 ASA 上的静态路由，然后使用路由协议重新分配路由。例如，如果将 NAT 用于内部网络 (10.1.1.0/24)，并且使用映射 IP 地址 209.165.201.5，则可以配置以下可以重新分配的静态路由：

```
209.165.201.5 255.255.255.255 10.1.1.99 中的路由
```

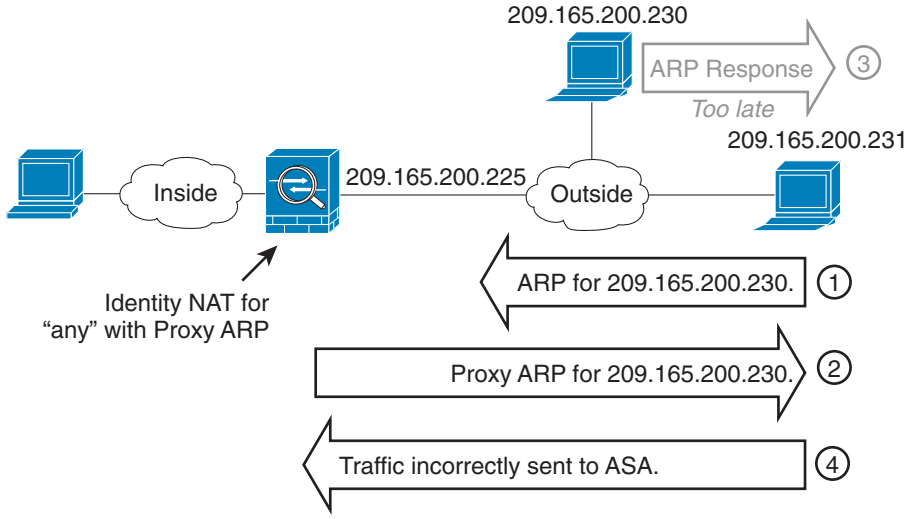
对于透明模式，如果直接连接实际主机，则将上游路由器的静态路由配置为指向 ASA：，指定桥接组 IP 地址。对于透明模式下的远程主机，在上游路由器上的静态路由中，还可以指定下游路由器 IP 地址。

与实际地址相同的地址（身份标识 NAT）

用于身份标识 NAT 的默认行为已启用代理 ARP，匹配其他静态 NAT 规则。如果需要，可以禁用代理 ARP。如果需要，还可以为常规静态 NAT 禁用代理 ARP，在这种情况下，需要确保上游路由器上有适当的路由。

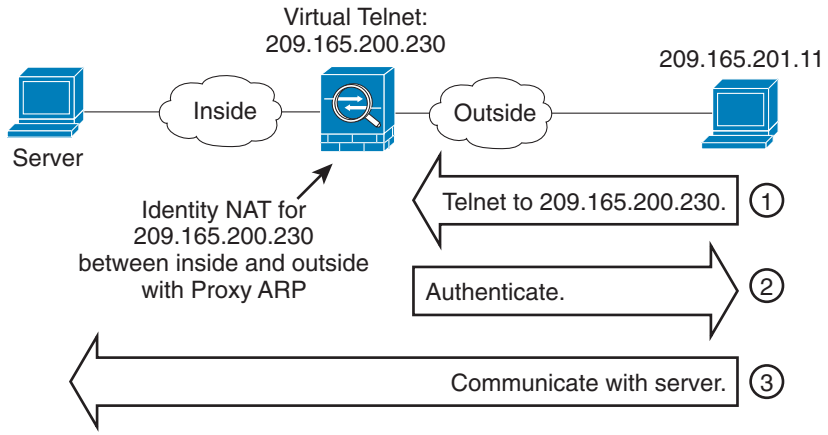
通常，对于身份标识 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。例如，如果为“任何”IP 地址配置一条大体的身份标识 NAT 规则，则使代理 ARP 保持启用状态会给直接连接到映射接口的网络上的主机造成问题。在这种情况下，当映射网络上的主机要与同一网络上的其他主机通信时，ARP 请求中的地址匹配 NAT 规则（匹配“任何”地址）。然后，ASA 将代理地址的 ARP，即使数据包实际上不以 ASA 为目标。（请注意，此问题甚至会在您有两次 NAT 规则时发生；尽管 NAT 规则必须匹配源地址和目标地址，但代理 ARP 决策仅在“源”地址上做出）。如果 ASA ARP 响应在实际主机 ARP 响应之前收到，则流量将被错误地发送到 ASA（请参阅图 4-18）。

图 4-18　身份标识 NAT 的代理 ARP 问题



在极少数情况下，需要面向身份标识 NAT 的代理 ARP；例如，对于虚拟 Telnet。将 AAA 用于网络访问时，主机需要先利用 Telnet 等服务对 ASA 进行身份验证，然后才能让任何其他流量通过。您可以在 ASA 上配置虚拟 Telnet 服务器，以提供必需的登录。从外部访问虚拟 Telnet 地址时，必需为此地址配置身份标识 NAT，尤其是对于代理 ARP 功能而言。由于虚拟 Telnet 的内部流程，代理 ARP 可以让 ASA 保存以虚拟 Telnet 地址为目标的流量，而不是根据 NAT 规则将流量向外发送到源接口。（请参阅图 4-19）。

图 4-19　代理 ARP 和虚拟 Telnet



远程网络的透明模式路由要求

当您在透明模式下使用 NAT 时，某些类型的流量要求静态路由。有关详细信息，请参阅常规操作配置指南。

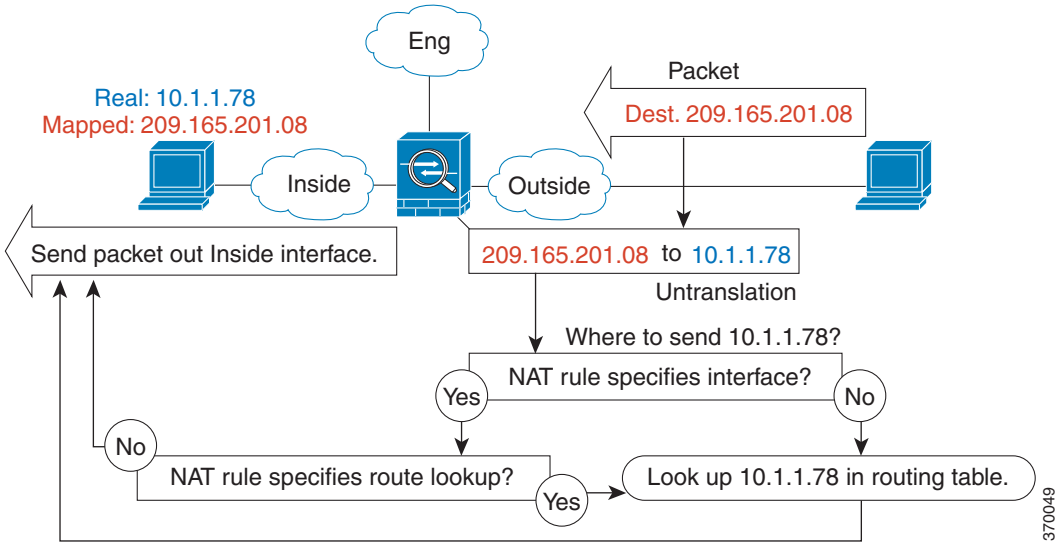
确定出口接口

当 ASA 接收用于映射地址的流量时，ASA 根据 NAT 规则取消转换目标地址，然后将数据包发送到实际地址。ASA 按照以下方式为数据包确定出口接口：

- 透明模式 - ASA 使用 NAT 规则，为实际地址确定出口接口；必须指定源接口和目标接口，作为 NAT 规则的一部分。
- 路由模式 - ASA 按照以下方式之一确定出口接口：
  - 在 NAT 规则中配置接口 - ASA 使用 NAT 规则确定出口接口。然而，您可以选择始终使用路由查询。在某些场景下，路由查询覆盖是必需的；例如，请参阅第 4-28 页上的 NAT 和 VPN 管理访问。
  - 不在 NAT 规则中配置接口 - ASA 使用路由查询确定出口接口。

下图显示路由模式下的出口接口选择方法。几乎在所有情况下，路由查询都等同于 NAT 规则接口，但在某些配置中，这两种方法可能不同。

图 4-20　　路由模式出口接口选择



面向 VPN 的 NAT

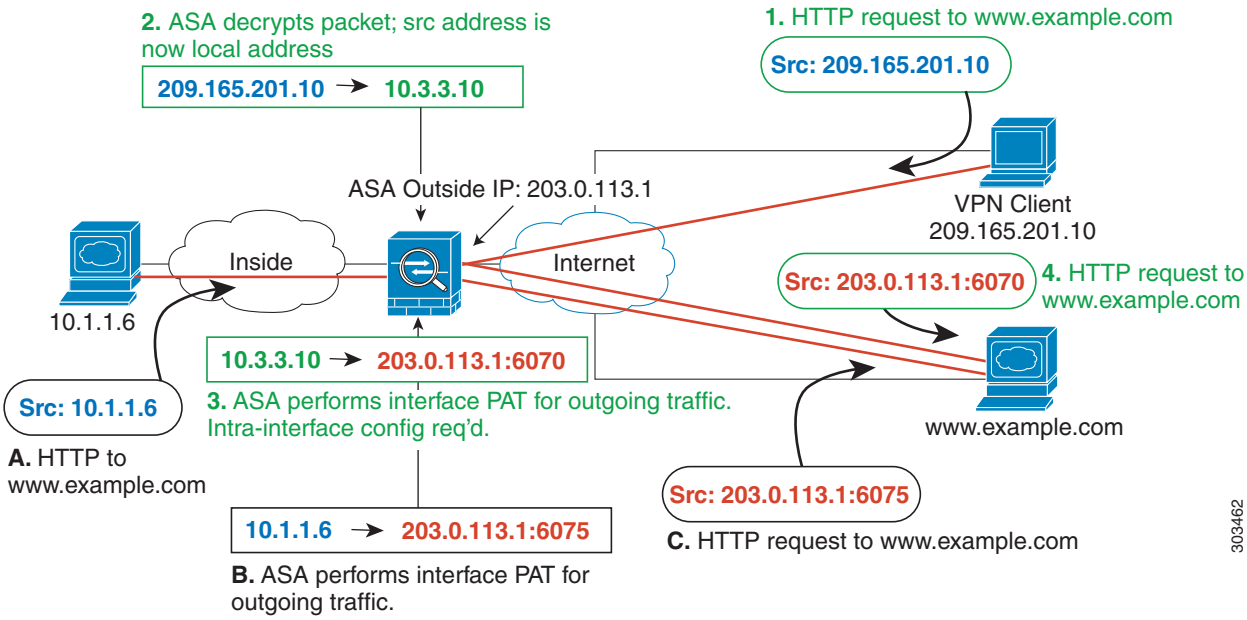
以下主题借助各种类型的 VPN 来解释 NAT 用途。

- 第 4-24 页上的 NAT 和远程访问 VPN
- 第 4-26 页上的 NAT 和站点到站点 VPN
- 第 4-28 页上的 NAT 和 VPN 管理访问
- 第 4-30 页上的 NAT 和 VPN 故障排除

NAT 和远程访问 VPN

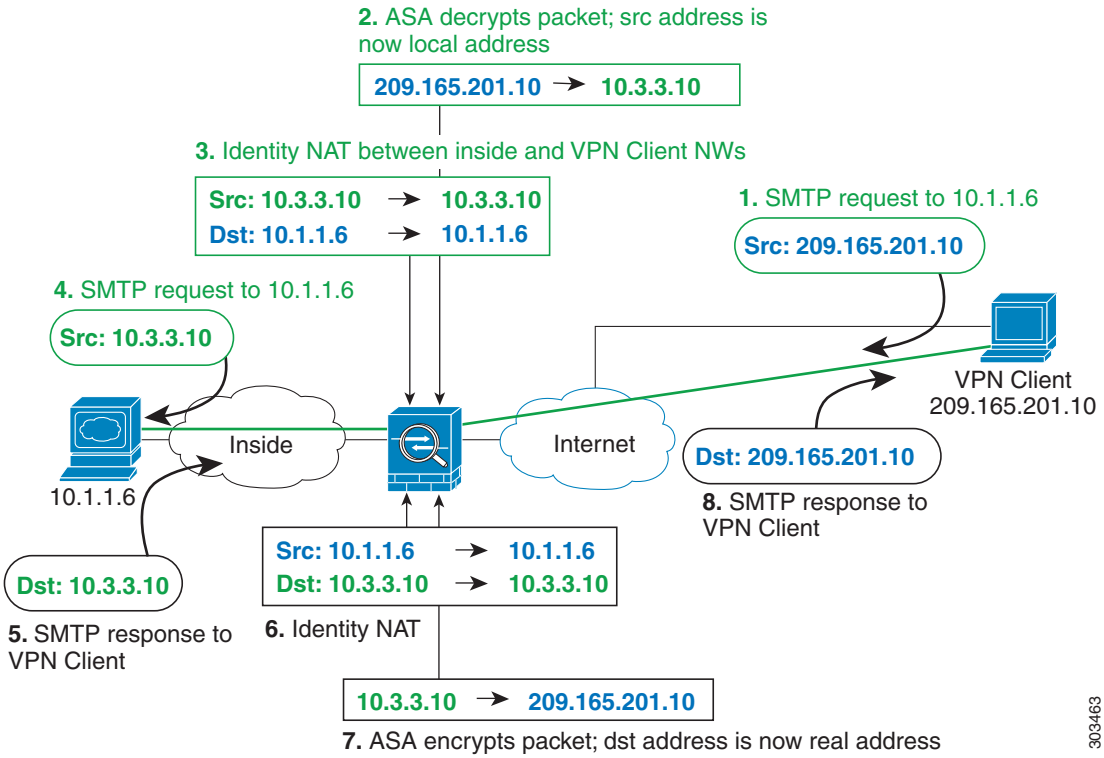
下图显示访问互联网的内部服务器 (10.1.1.6) 和 VPN 客户端 (209.165.201.10)。除非为 VPN 客户端配置拆分隧道（其中，仅指定流量穿过 VPN 隧道），否则互联网绑定 VPN 流量也必须穿过 ASA。当 VPN 流量进入 ASA 时，ASA 解密数据包；产生的数据包包含作为源地址的 VPN 客户端本地地址 (10.3.3.10)。对于内部和 VPN 客户端本地网络，您需要使用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口 PAT 规则。为使 VPN 流量可以退出其已进入的相同接口，您还需要启用接口内通信（也称为“发夹”网络）。

图 4-21　面向互联网绑定 VPN 流量的接口 PAT（接口内）



下图显示要访问内部邮件服务器的 VPN 客户端。因为 ASA 希望内部网络和任何外部网络之间的流量匹配您为互联网访问建立的接口 PAT 规则，所以从 VPN 客户端 (10.3.3.10) 到 SMTP 服务器 (10.1.1.6) 的流量将会因为逆向路径故障而被丢弃：从 10.3.3.10 到 10.1.1.6 的流量不匹配 NAT 规则，但从 10.1.1.6 到 10.3.3.10 的返回流量*应当*匹配用于传出流量的接口 PAT 规则。因为正向流量和逆向流量不匹配，所以 ASA 会在收到数据包后丢弃数据包。为避免这种故障，您需要在那些网络之间使用身份标识 NAT 规则，使内部到 VPN 客户端流量免于应用接口 PAT 规则。身份标识 NAT 只能将地址转换为其相同的地址。

图 4-22　面向 VPN 客户端的身份标识 NAT



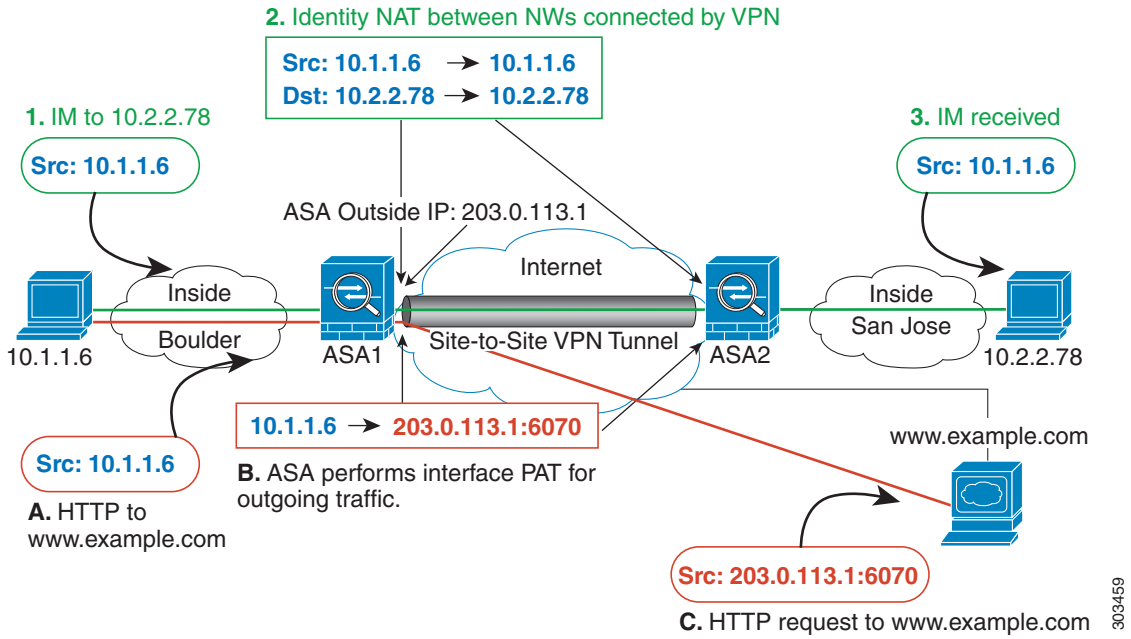
请参阅以下用于上述网络的 NAT 配置示例：

```
!Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

!Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0
    nat (outside,outside) dynamic interface

!Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
    subnet 10.1.1.0 255.255.255.0
    nat (inside,outside) dynamic interface

!Use twice NAT to pass traffic between the inside network and the VPN client without
!address translation (identity NAT):
nat (inside,outside) source static inside_nw inside_nw destination static vpn_local
vpn_local
```

NAT 和站点到站点 VPN

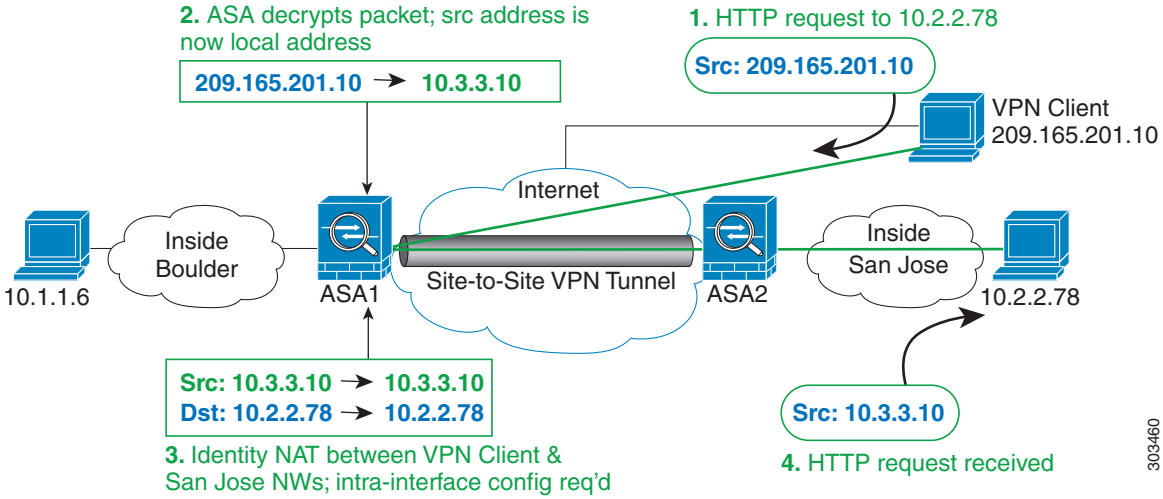
下图显示连接博尔德办公室和圣荷西办公室的站点到站点隧道。对于要发送到互联网的流量（例如，从博尔德办公室中的 10.1.1.6 到 www.example.com），您需要利用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口 PAT 规则。然而，对于要穿过 VPN 隧道的流量（例如，从博尔德办公室中的 10.1.1.6 到圣荷西办公室中的 10.2.2.78），您不想执行 NAT；您需要通过创建身份标识 NAT 规则来豁免此流量。身份标识 NAT 只能将地址转换为其相同的地址。

图 4-23　用于站点到站点 VPN 的接口 PAT 和身份标识 NAT



下图显示连接到 ASA1（博尔德）的 VPN 客户端，以及可通过 ASA1 和 ASA2（圣荷西）之间的站点到站点隧道访问的服务器 (10.2.2.78) 的 Telnet 请求。因为这是一种发夹连接，所以您需要启用接口内通信，这也是来自 VPN 客户端的非拆分隧道互联网绑定流量所必需的。您还需要在 VPN 客户端以及博尔德和圣荷西网络之间配置身份标识 NAT，就像在 VPN 连接的任何网络之间一样配置，使此流量免于应用出站 NAT 规则。

图 4-24　　VPN 客户端访问站点到站点 VPN



请参阅以下用于 ASA1（博尔德）的 NAT 配置示例：

```
!Enable hairpin for VPN client traffic:
same-security-traffic permit intra-interface

!Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0
    nat (outside,outside) dynamic interface

!Identify inside Boulder network, & perform object interface PAT when going to Internet:
object network boulder_inside
    subnet 10.1.1.0 255.255.255.0
    nat (inside,outside) dynamic interface

!Identify inside San Jose network for use in twice NAT rule:
object network sanjose_inside
    subnet 10.2.2.0 255.255.255.0

!Use twice NAT to pass traffic between the Boulder network and the VPN client without
!address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside destination static
vpn_local vpn_local

!Use twice NAT to pass traffic between the Boulder network and San Jose without
!address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside destination static
sanjose_inside sanjose_inside

!Use twice NAT to pass traffic between the VPN client and San Jose without
!address translation (identity NAT):
nat (outside,outside) source static vpn_local vpn_local destination static sanjose_inside
sanjose_inside
```

请参阅以下用于 ASA2（圣荷西）的 NAT 配置示例：

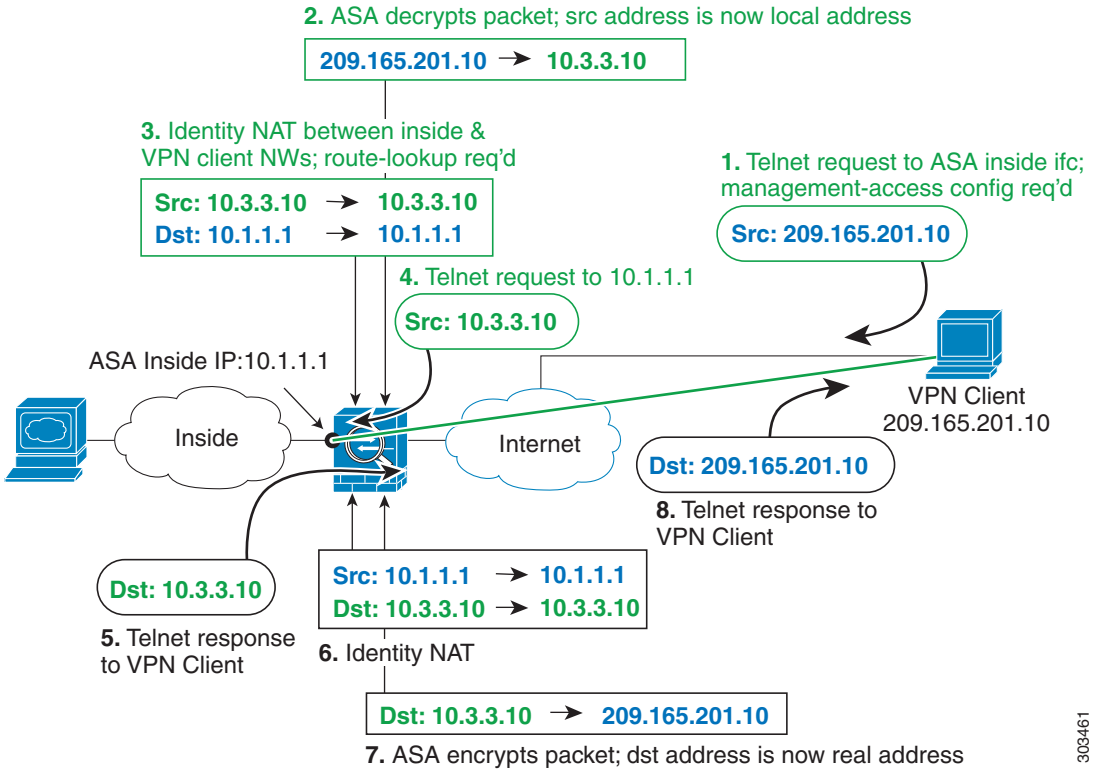
```
!Identify inside San Jose network, & perform object interface PAT when going to Internet:
object network sanjose_inside
    subnet 10.2.2.0 255.255.255.0
    nat (inside,outside) dynamic interface

!Identify inside Boulder network for use in twice NAT rule:
object network boulder_inside
    subnet 10.1.1.0 255.255.255.0

!Identify local VPN network for use in twice NAT rule:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0

!Use twice NAT to pass traffic between the San Jose network and Boulder without
!address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside destination static
boulder_inside boulder_inside

!Use twice NAT to pass traffic between the San Jose network and the VPN client without
!address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside destination static
vpn_local vpn_local
```

NAT 和 VPN 管理访问

使用 VPN 时，您可以对进入 ASA（请参阅**管理访问**命令）所通过的接口以外的接口进行管理访问。例如，如果您从外部接口进入 ASA，管理访问功能可以让您使用 ASDM、SSH、Telnet 或 SNMP 连接到内部接口；或者您可以 ping 内部接口。

下图显示通过 Telnet 连接到 ASA 内部接口的 VPN 客户端。当您使用管理访问接口，并且根据第 4-24 页上的 NAT 和远程访问 VPN或第 4-26 页上的 NAT 和站点到站点 VPN配置身份标识 NAT 时，必须为 NAT 配置路由查询选项。如果没有路由查询，ASA 会将流量向外发送到在 NAT 命令中指定的接口，无论路由表显示什么；在以下示例中，出口接口为内部接口。您不希望 ASA 将管理流量向外发送到内部网络；它永远不会返回到内部接口 IP 地址。路由查询选项可以让 ASA 将流量直接发送到内部接口 IP 地址，而不是内部网络。对于从 VPN 客户端到内部网络上的主机的流量，路由查询选项仍将导致正确的出口接口（内部），因此，正常业务流不会受到影响。有关路由查询选项的详细信息，请参阅第 4-23 页上的确定出口接口。

图 4-25　VPN 管理访问



请参阅以下用于上述网络的 NAT 配置示例：

```
!Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

!Enable management access on inside ifc:
management-access inside

!Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0
    nat (outside,outside) dynamic interface

!Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
    subnet 10.1.1.0 255.255.255.0
    nat (inside,outside) dynamic interface

!Use twice NAT to pass traffic between the inside network and the VPN client without
!address translation (identity NAT), w/route-lookup:
nat (outside,inside) source static vpn_local vpn_local destination static inside_nw
inside_nw route-lookup
```

NAT 和 VPN 故障排除

请参阅以下用于排除 VPN 中 NAT 问题的监控工具：

- 数据包跟踪器 - 正确使用时，数据包跟踪器显示数据包命中了哪些 NAT 规则。
- **show nat detail** - 显示给定 NAT 规则的命中数和未转换流量。
- **show conn all** - 让您查看活动连接，包括流向设备的流量和通过设备的流量。

要让自己熟悉非工作配置和工作配置，您可以执行以下步骤：

1. 配置无身份标识 NAT 的 VPN。
2. 输入 **show nat detail** 和 **show conn all**。
3. 添加身份标识 NAT 配置。
4. 重复 **show nat detail** 和 **show conn all**。

DNS 和 NAT

您可能需要配置 ASA 以修改 DNS 回复，方法是用匹配 NAT 配置的地址替换回复中的地址。配置每条转换规则时，您可以配置 DNS 修改。

此功能可以重写匹配 NAT 规则的 DNS 查询和回复中的地址（例如，适用于 IPv4 的 A 记录；适用于 IPv6 的 AAAA 记录；或者，适用于逆向 DNS 查询的 PTR 记录）。对于从映射接口穿越到任何其他接口的 DNS 回复，记录会从映射值被重写为实际值。相反，对于从任何接口穿越到映射接口的 DNS 回复，记录会从实际值被重写为映射值。

以下是 DNS 重写的某些限制：

- DNS 重写不适用于 PAT，因为多条 PAT 规则适用于每个 A 记录，而且要使用的 PAT 规则不确定。
- 如果配置了两次 NAT 规则，并且指定了源地址和目标地址，则不能配置 DNS 修改。或者，这种规则发送到 A 和 B 时， 对单一地址可能有不同的转换。因此，ASA 不能精确匹配 DNS 回复中的 IP 地址和正确的两次 NAT 规则； DNS 回复不包含有关哪个源地址 / 目标地址组合位于提示 DNS 请求的数据包中的信息。
- DNS 重写要求启用 DNS 应用检测，默认情况下 DNS 应用检测处于启用状态。有关详细信息，请参阅第 8-1 页上的 DNS 检测。
- 实际上，DNS 重写在 xlate 条目而非 NAT 规则上完成。因此，如果没有面向动态规则的 xlate，则不能正确完成重写。静态 NAT 也会出现相同的问题。

以下主题提供 DNS 重写示例：

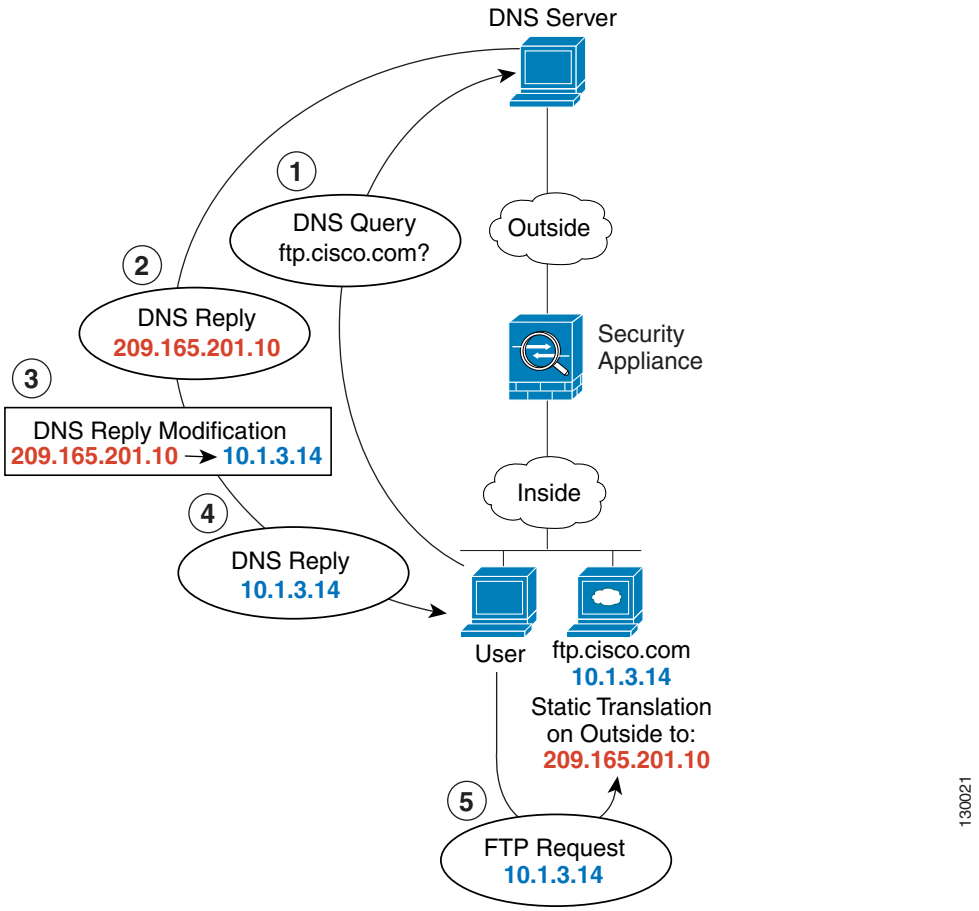
- 第 4-31 页上的 DNS 回复修改，外部接口上的 DNS 服务器
- 第 4-32 页上的独立网络上的 DNS 回复修改、DNS 服务器、主机和服务器
- 第 4-33 页上的 DNS 回复修改，主机网络上的 DNS 服务器
- 第 4-34 页上的使用外部 NAT 进行 DNS64 回复修改
- 第 4-35 页上的 PTR 修改，主机网络上的 DNS 服务器

DNS 回复修改，外部接口上的 DNS 服务器

下图显示可从外部接口访问的 DNS 服务器。服务器 ftp.cisco.com 在内部接口上。将 ASA 配置为静态地将 ftp.cisco.com 实际地址 (10.1.3.14) 转换为在外部网络上可见的映射地址 (209.165.201.10)。

在这种情况下，您要在此静态规则上启用 DNS 回复修改，以便使用实际地址访问 ftp.cisco.com 的内部用户可以接收来自 DNS 服务器的实际地址，而不是映射地址。当内部主机发送对 ftp.cisco.com 的地址的 DNS 请求时，DNS 服务器将以映射地址 (209.165.201.10) 作为回复。ASA 是指内部服务器的静态规则，并且将 DNS 回复中的地址转换为 10.1.3.14。如果不启用 DNS 回复修改，则内部主机尝试将流量发送到 209.165.201.10，而不是直接访问 ftp.cisco.com。

图 4-26　　DNS 回复修改，外部接口上的 DNS 服务器

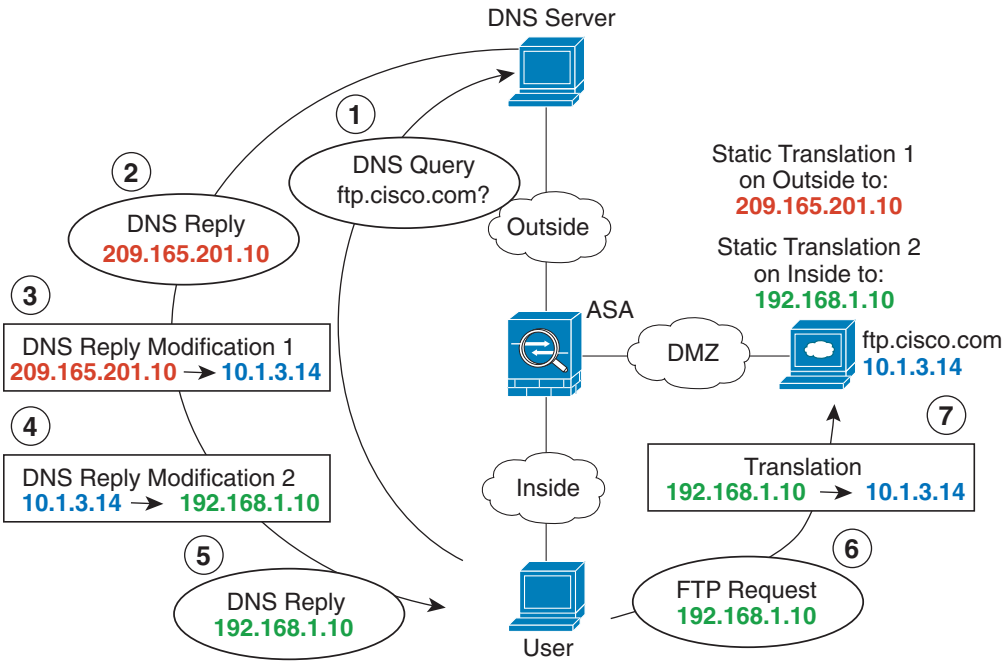


独立网络上的 DNS 回复修改、DNS 服务器、主机和服务器

下图显示一个内部网络的用户正在从外部 DNS 服务器请求 DMZ 网络上的 ftp.cisco.com 的 IP 地址。DNS 服务器根据外部网络和 DMZ 网络之间的静态规则，以映射地址 (209.165.201.10) 作为回复，即使该用户不在 DMZ 网络中。ASA 将 DNS 回复中的地址转换为 10.1.3.14。

如果用户需要使用实际地址访问 ftp.cisco.com，则无需更多配置。如果内部网络和 DMZ 网络之间也有静态规则，您还需要在此规则上启用 DNS 回复修改。然后，DNS 回复将被修改两次。在这种情况下，ASA 会根据内部网络和 DMZ 网络之间的静态规则，再次将 DNS 回复中的地址转换为 192.168.1.10。

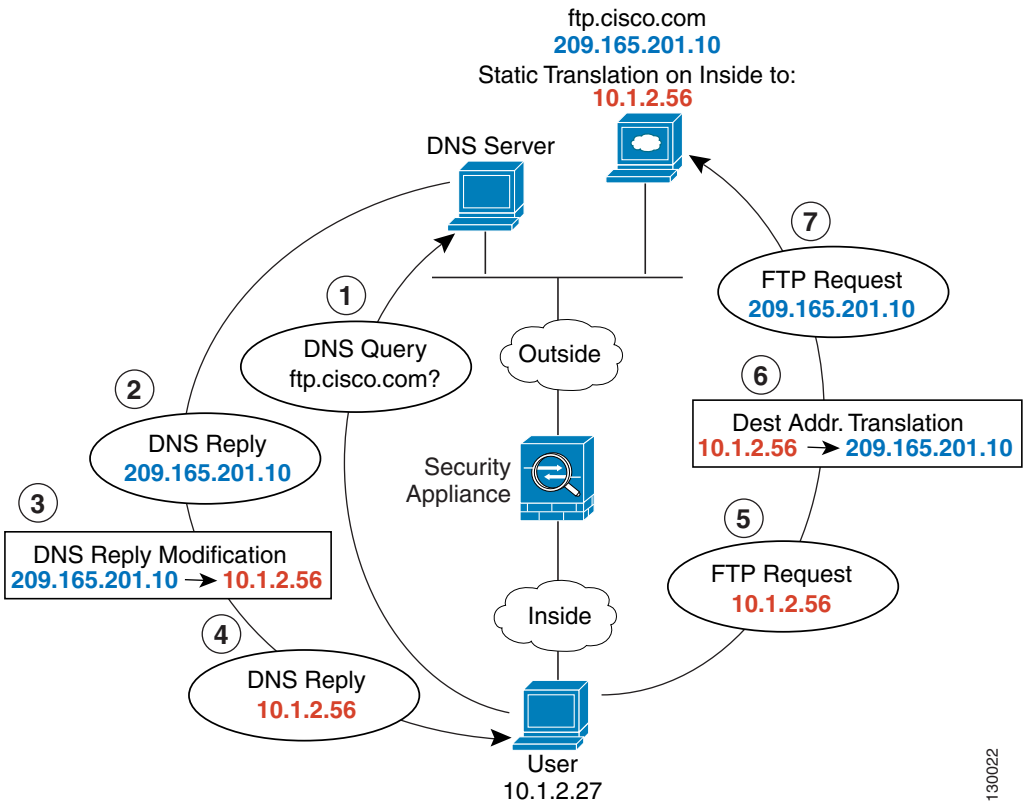
图 4-27　独立网络上的 DNS 回复修改、DNS 服务器、主机和服务器



DNS 回复修改，主机网络上的 DNS 服务器

下图显示外部网络上的 FTP 服务器和 DNS 服务器。ASA 有面向外部服务器的静态转换。在这种情况下，当内部用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.20.10 作为响应。因为您想让内部用户使用 ftp.cisco.com 的映射地址 (10.1.2.56)，所以您需要配置 DNS 回复修改以进行静态转换。

图 4-28　　DNS 回复修改，主机网络上的 DNS 服务器

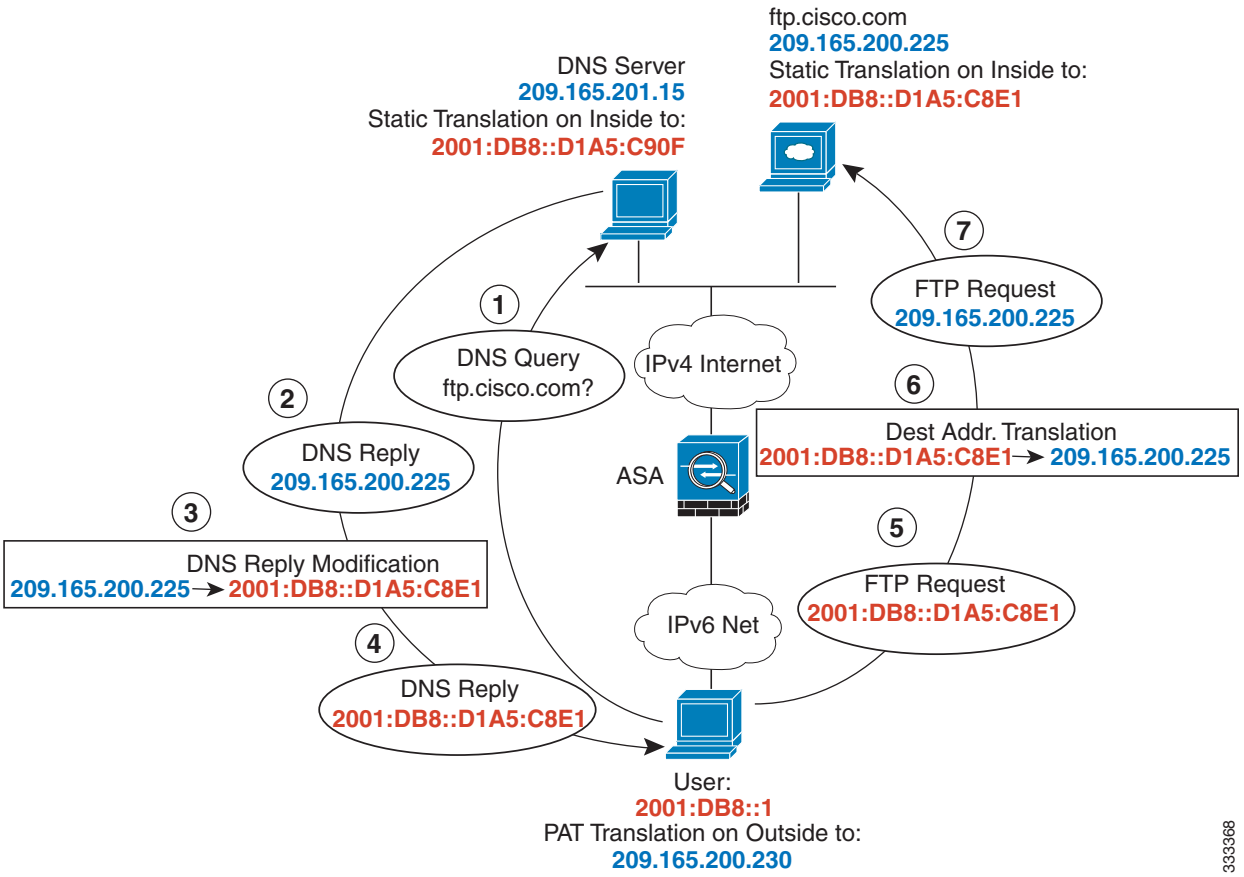


使用外部 NAT 进行 DNS64 回复修改

下图显示外部 IPv4 网络上的 FTP 服务器和 DNS 服务器。ASA 有面向外部服务器的静态转换。在这种情况下，当内部 IPv6 用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.200.225 作为响应。

因为您想让内部用户使用 ftp.cisco.com 的映射地址 (2001:DB8::D1A5:C8E1)，所以您需要配置 DNS 回复修改以进行静态转换。本示例还包括面向 DNS 服务器的静态 NAT 转换和面向内部 IPv6 主机的 PAT 规则。

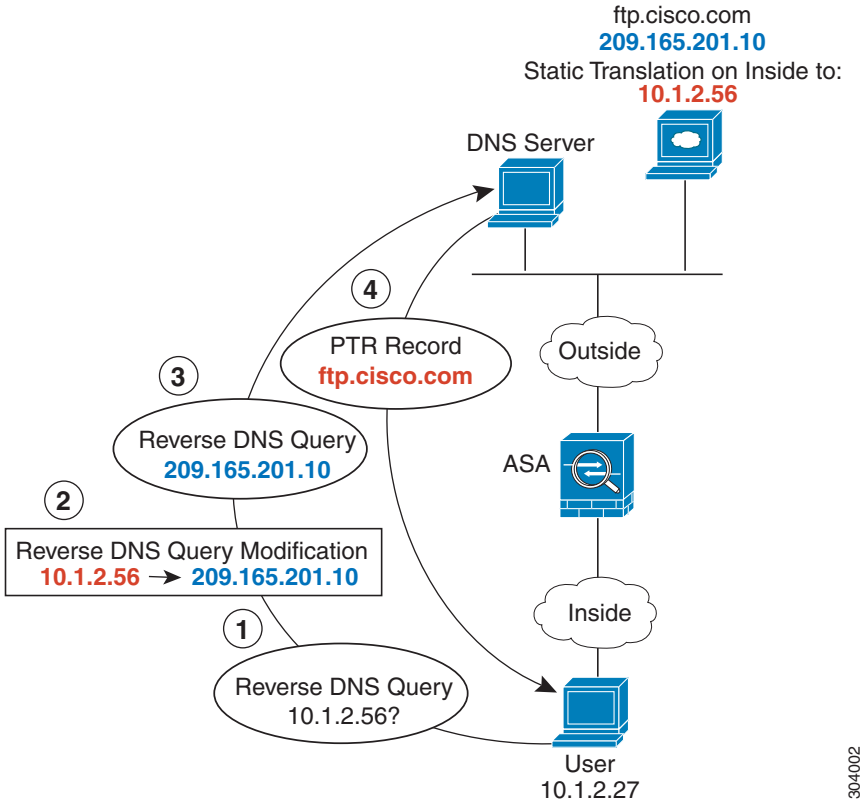
图 4-29　使用外部 NAT 进行 DNS64 回复修改



PTR 修改，主机网络上的 DNS 服务器

下图显示外部网络上的 FTP 服务器和 DNS 服务器。ASA 有面向外部服务器的静态转换。在这种情况下，当内部用户执行逆向 DNS 查询以获取 10.1.2.56 时，ASA 将通过实际地址修改逆向 DNS 查询，DNS 服务器将以服务器名称 ftp.cisco.com 作为响应。

图 4-30　PTR 修改，主机网络上的 DNS 服务器



更多信息指南

要配置网络对象 NAT，请参阅第 5 章，“ 网络对象 NAT”。

要配置两次 NAT，请参阅第 6 章，“ 两次 NAT”。

网络对象 NAT

配置为网络对象的参数的所有 NAT 规则都被视为*网络对象 NAT* 规则。网络对象 NAT 是一种为单一 IP 地址、地址范围或子网配置 NAT 的快速便捷方法。配置网络对象后，随后可以识别该对象的映射地址。

本章介绍如何配置网络对象 NAT，其中包含以下各节：

- 第 5-1 页上的有关网络对象 NAT 的信息
- 第 5-2 页上的网络对象 NAT 的许可要求
- 第 5-2 页上的网络对象 NAT 的先决条件
- 第 5-2 页上的准则和限制
- 第 5-3 页上的默认设置
- 第 5-3 页上的配置网络对象 NAT
- 第 5-15 页上的监控网络对象 NAT
- 第 5-15 页上的网络对象 NAT 配置示例
- 第 5-24 页上的网络对象 NAT 的功能历史

注 有关 NAT 工作原理的详细信息，请参阅第 4 章，“ 网络地址转换 (NAT)”。

有关网络对象 NAT 的信息

当数据包进入 ASA 时，根据网络对象 NAT 规则检查源 IP 地址和目标 IP 地址。如果进行独立匹配，可根据独立规则转换数据包中的源地址和目标地址。这些规则互不牵连，可以根据流量使用不同的规则组合。

因为从未对规则进行配对，所以无法指定源地址在转到目标 X 时应被转换为 A，但是，在转到目标 Y 时应被转换为 B。将两次 NAT 用于此类功能（两次 NAT 可以让您识别单一规则中的源地址和目标地址）。

有关两次 NAT 和网络对象 NAT 之间的差异的详细信息，请参阅第 4-14 页上的如何实施 NAT。

网络对象 NAT 已添加到 NAT 规则表中的第 2 部分。有关 NAT 排序的详细信息，请参阅第 4-18 页上的 NAT 规则顺序。

网络对象 NAT 的许可要求

下表显示此功能的许可要求：

型号	许可证要求
ASAv	标准或高级许可证。
所有其他型号	基础许可证。

网络对象 NAT 的先决条件

根据此配置，如果需要，您可以配置映射地址内联，或者可以为映射地址创建独立网络对象或网络对象组（**对象网络**或**对象组网络**命令）。网络对象组对于使用不连续的 IP 地址范围或多台主机或多个子网创建映射地址池尤其有用。要创建网络对象或组，请参阅常规操作配置指南。

有关对象和组的特定准则，请参阅与您想要配置的 NAT 类型对应的配置部分。另请参阅第 5-2 页上的准则和限制小节。

准则和限制

情景模式准则

在单一和多情景模式下受支持。

防火墙模式准则

- 在路由和透明防火墙模式下受支持。
- 在透明模式下，必须指定实际接口和映射接口；不能使用 **any**。
- 在透明模式下，不能配置接口 PAT，因为透明模式接口没有 IP 地址。也不能将管理 IP 地址用作映射地址。
- 在透明模式下，不支持在 IPv4 和 IPv6 网络之间进行转换。支持在两个 IPv6 网络之间或两个 IPv4 网络之间进行转换。

IPv6 准则

- 支持 IPv6。另请参阅第 4-14 页上的 NAT 和 IPv6。
- 对于路由模式，还可以在 IPv4 和 IPv6 之间进行转换。
- 对于透明模式，不支持在 IPv4 和 IPv6 网络之间进行转换。支持在两个 IPv6 网络之间或两个 IPv4 网络之间进行转换。
- 对于透明模式，对于 IPv6 来说不支持 PAT 池。
- 对于静态 NAT，可以指定一个多达 /64 的 IPv6 子网。不支持更大的子网。
- 将 FTP 和 NAT46 配合使用时，当 IPv4 FTP 客户端连接到 IPv6 FTP 服务器时，客户端必须使用扩展被动模式 (EPSV) 或扩展端口模式 (EPRT)；在使用 IPv6 时，PASV 和 PORT 命令不受支持。

其他准则

- 只能为给定对象定义单一 NAT 规则；如果想为对象配置多条 NAT 规则，需要使用指定同一 IP 地址的不同名称创建对个对象，例如，**object network obj-10.10.10.1-01**、**object network obj-10.10.10.1-02** 等等。
- 如果更改 NAT 配置，而且在使用新 NAT 配置之前不想等待现有转换超时，则可以使用 **clear xlate** 命令清除转换表。然而，清除转换表将断开使用转换的当前所有连接。

> **注**　如果移除动态 NAT 或 PAT 规则，然后使用与已移除规则中地址重叠的映射地址添加新规则，则将不使用新规则，直至与已移除规则关联的所有连接超时，或已使用 **clear xlate** 命令将这些连接清除。此保护措施确保相同的地址将不分配至多个主机。

- NAT 中使用的对象和对象组不能是未定义的，它们必须包含 IP 地址。
- 不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。
- 可以在多条 NAT 规则中使用同一映射对象或组。
- 已映射 IP 地址池不能包括：
  - 已映射接口的 IP 地址。如果为规则指定 **any 接口**，那么所有接口 IP 地址将不被允许。对于接口 PAT（仅路由模式），请使用 **interface** 关键字，而非 IP 地址。
  - （透明模式）管理 IP 地址。
  - （动态 NAT）启用 VPN 时，备用接口 IP 地址。
  - 现有的 VPN 池地址。
- 避免在静态和动态 NAT 策略中使用重叠地址。例如，使用重叠地址，如果 PPTP 的辅助连接命中静态而非动态 xlate，将无法建立 PPTP 连接。
- 有关 NAT 或 PAT 的应用检测限制，请参阅第 7 章，“应用层协议检测入门”中的第 7-5 页上的默认检测和 NAT 限制。

默认设置

- （路由模式）默认实际接口和映射接口为 Any，可将规则应用于所有接口。
- 用于身份标识 NAT 的默认行为已启用代理 ARP，匹配其他静态 NAT 规则。如果需要，可以禁用代理 ARP。有关详细信息，请参阅第 4-20 页上的路由 NAT 数据包。
- 如果指定可选接口，则 ASA 将使用 NAT 配置确定出口接口，但您可以选择始终使用路由查询。有关详细信息，请参阅第 4-20 页上的路由 NAT 数据包。

配置网络对象 NAT

本节介绍如何配置网络对象 NAT。

- 第 5-4 页上的为映射地址添加网络对象
- 第 5-5 页上的使用 PAT 池配置动态 NAT
- 第 5-7 页上的配置动态 PAT（隐藏）
- 第 5-10 页上的配置静态 NAT 或带有端口转换的静态 NAT
- 第 5-12 页上的配置身份标识 NAT
- 第 5-13 页上的配置每会话 PAT 规则

为映射地址添加网络对象

对于动态 NAT，必须为映射地址使用一个对象或组。其他 NAT 类型可以选择使用内联地址，或者您可以根据本节创建一个对象或组。有关配置网络对象或组的详细信息，请参阅常规操作配置指南。

准则

- 网络对象组可以包含多个对象和 / 或 IPv4 或 IPv6 地址的内联地址。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。
- 有关不允许的映射 IP 地址的详细信息，请参阅第 5-2 页上的准则和限制。
- 动态 NAT：
  - 不能使用内联地址；必须配置一个网络对象或组。
  - 对象或组不能包含子网；对象必须定义一个范围；组可以包含主机和范围。
  - 如果映射网络对象包含范围和主机 IP 地址，则范围可用于动态 NAT，主机 IP 地址可用作 PAT 退回。
- 动态 PAT（隐藏）：
  - 如果不使用对象，或者可以配置内联主机地址或指定接口地址。
  - 如果使用对象，对象或组不能包含子网；对象必须定义主机，或者对于 PAT 池，必须定义范围；组（对于 PAT 池）可以包含主机和范围。
- 静态 NAT 或带端口转换的静态 NAT：
  - 如果不使用对象，可以配置内联地址，或者指定接口地址（对于带端口转换的静态 NAT）。
  - 如果使用对象，对象或组可以包含主机、范围或子网。
- 身份标识 NAT
  - 如果不使用对象，可以配置内联地址。
  - 如果使用对象，对象必须匹配要转换的实际地址。

详细步骤

命令	用途

object network *obj_name*
{**host** *ip_address* | **range** *ip_address_1 ip_address_2* | **subnet** *subnet_address netmask*}
 	
示例：
`hostname(config)# object network TEST`
`hostname(config-network-object)# range 10.1.1.1 10.1.1.70`
	添加网络对象，IPv4 或 IPv6。

命令	用途
object-group network *grp_name* {**network-object** {**object** *net_obj_name* | *subnet_address netmask* | **host** *ip_address*} | **group-object** *grp_obj_name*} **示例：** hostname(config)# object network TEST hostname(config-network-object)# range 10.1.1.1 10.1.1.70 hostname(config)# object network TEST2 hostname(config-network-object)# range 10.1.2.1 10.1.2.70 hostname(config-network-object)# object-group network MAPPED_IPS hostname(config-network)# network-object object TEST hostname(config-network)# network-object object TEST2 hostname(config-network)# network-object host 10.1.2.79	添加网络对象组，IPv4 或 IPv6。

使用 PAT 池配置动态 NAT

本节介绍如何使用 PAT 池为配置网络对象 NAT。有关详细信息，请参阅第 4-8 页上的动态 NAT。

详细步骤

	命令	用途
步骤 1	为映射地址创建网络对象或组。	请参阅第 5-4 页上的为映射地址添加网络对象。
步骤 2	**object network** *obj_name* **示例：** hostname(config)# object network my-host-obj1	配置一个要为其配置 NAT 的网络对象，或者进入一个现有网络对象的对象网络配置模式。
步骤 3	{**host** *ip_address* | **subnet** *subnet_address* *netmask* | **range** *ip_address_1 ip_address_2*} **示例：** hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0	如果正在创建新网络对象，则定义要转换的**实际** IP 地址（IPv4 或 IPv6）。

	命令	用途
步骤 4	**nat** [(*real_ifc*,*mapped_ifc*)] **dynamic** *mapped_obj* [**interface** [**ipv6**]] [**dns**] **示例：** hostname(config-network-object)# nat (inside,outside) dynamic MAPPED_IPS interface	为对象 IP 地址配置**动态 NAT**。 **注**　只能为给定对象定义单一 NAT 规则。请参阅第 5-3 页上的其他准则。 请参阅以下准则： • Interfaces -（透明模式必需）指定真实和映射接口。确保命令中包含圆括号。在路由模式下，如不指定真实和映射接口，则将使用所有接口；还可为一个或两个接口指定关键字 **any**。 • Mapped IP address - 将映射 IP 地址指定为： – 现有网络对象（请参阅步骤 1）。 – 现有网络对象组（请参阅步骤 1）。 • Interface PAT fallback -（可选）**interface** 关键字启用接口 PAT 退回。映射 IP 地址用尽后和映射接口的 IP 地址。如果指定 **ipv6**，则将使用接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置特定接口。（不能在透明模式下指定**接口**）。 • DNS -（可选）**dns** 关键字可以转换 DNS 回复。确保启用 DNS 检测（默认情况下启用）。有关详细信息，请参阅第 4-30 页上的 DNS 和 NAT。

示例

以下示例配置动态 NAT，将 192.168.2.0 网络隐藏在地址 10.2.2.1 到 10.2.2.10 以外的范围后面。

```
hostname(config)# object network my-range-obj
hostname(config-network-object)# range 10.2.2.1 10.2.2.10
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

以下示例使用动态 PAT 备份配置动态 NAT。内部网络 10.76.11.0 中的主机首先映射到 nat-range 1 池 (10.10.10.10-10.10.10.20)。分配 nat-range1 池中的所有地址之后，使用 pat-ip1 地址 (10.10.10.21) 执行动态 PAT。PAT 转换也用尽的可能性不大，即使发生这种情况，也可以使用外部接口地址执行动态 PAT。

```
hostname(config)# object network nat-range1
hostname(config-network-object)# range 10.10.10.10 10.10.10.20

hostname(config-network-object)# object network pat-ip1
hostname(config-network-object)# host 10.10.10.21

hostname(config-network-object)# object-group network nat-pat-grp
hostname(config-network-object)# network-object object nat-range1
hostname(config-network-object)# network-object object pat-ip1

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 10.76.11.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

以下示例使用动态 PAT 备份配置动态 NAT，将 IPv6 主机转换为 IPv4 主机。内部网络 2001:DB8::/96 上的主机首先映射到 IPv4_NAT_RANGE 池（209.165.201.1 到 209.165.201.30）。分配 IPv4_NAT_RANGE 池中的所有地址之后，使用 IPv4_PAT 地址 (209.165.201.31) 执行动态 PAT。在 PAT 转换也用尽的情况下，使用外部接口地址执行动态 PAT。

```
hostname(config)# object network IPv4_NAT_RANGE
hostname(config-network-object)# range 209.165.201.1 209.165.201.30

hostname(config-network-object)# object network IPv4_PAT
hostname(config-network-object)# host 209.165.201.31

hostname(config-network-object)# object-group network IPv4_GROUP
hostname(config-network-object)# network-object object IPv4_NAT_RANGE
hostname(config-network-object)# network-object object IPv4_PAT

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

配置动态 PAT（隐藏）

本节介绍如何为动态 PAT（隐藏）配置网络对象 NAT。有关详细信息，请参阅第 4-10 页上的动态 PAT。

准则

对于 PAT 池：

- 如果可用，真实源端口号将用于映射端口。然而，如果真实端口不可用，将默认从与真实端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，低于 1024 的端口仅拥有很小的可用 PAT 池。（8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)）如果您有大量使用较低端口范围的流量，现在可以指定一个要使用的单一端口范围，而不是三个大小不等的层：1024 到 65535 或 1 到 65535。
- 如在两个不同的规则中使用相同的 PAT 池对象，则请确保为每条规则指定相同的选项。例如，如果一条规则指定扩展 PAT 和无层次的范围，则另一条规则也必须指定扩展 PAT 和无层次的范围。

对于用于 PAT 池的扩展 PAT：

- 许多应用检测不支持扩展 PAT。有关不支持的检测的完整列表，请参阅第 7 章，“应用层协议检测入门”中的第 7-5 页上的默认检测和 NAT 限制。
- 如为动态 PAT 规则启用扩展 PAT，则无法也在不同的带有端口转换规则的静态 NAT 中使用 PAT 池中的地址作为 PAT 地址。例如，如果 PAT 池包括 10.1.1.1，则无法创建一个将 10.1.1.1 用作 PAT 地址的采用端口转换规则的静态 NAT。
- 如使用 PAT 池，并为回退指定接口，则无法指定扩展 PAT。
- 对于使用 ICE 或 TURN 的 VoIP 部署，请勿使用扩展 PAT。ICE 和 TURN 依赖于 PAT 绑定才能对所有目标均保持相同。

对于 PAT 池的轮询调度：

- 如果主机拥有现有连接，并且端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。**注意**：此“粘性”在故障转移后将不复存在。如果 ASA 进行故障转移，则来自某个主机的后续连接可能将不使用初始 IP 地址。
- 轮询调度可能会消耗大量的内存，在与扩展 PAT 组合使用时尤其如此。由于将为每一个映射协议 /IP 地址 / 端口范围创建 NAT 池，因此，轮询调度会导致大量并发 NAT 池，从而消耗内存。扩展 PAT 将导致甚至更多数量的并发 NAT 池。

详细步骤

	命令	用途
步骤 1	（可选）为映射地址创建网络对象或组。	请参阅第 5-4 页上的为映射地址添加网络对象。
步骤 2	**object network** *obj_name* **示例：** `hostname(config)# object network my-host-obj1`	配置一个要为其配置 NAT 的网络对象，或者进入一个现有网络对象的对象网络配置模式。
步骤 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **示例：** `hostname(config-network-object)# range 10.1.1.1 10.1.1.90`	如果正在创建新网络对象，则定义要转换的**实际** IP 地址（IPv4 或 IPv6）。
步骤 4	**nat** [**(***real_ifc***,***mapped_ifc***)**] **dynamic** {*mapped_inline_host_ip* | *mapped_obj* | **pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] | **interface** [**ipv6**]} [**interface** [**ipv6**]] [**dns**] **示例：** `hostname(config-network-object)# nat (any,outside) dynamic interface`	为对象 IP 地址配置**动态 PAT**。只能为给定对象定义单一 NAT 规则。请参阅第 5-3 页上的其他准则。 请参阅以下准则： • Interfaces -（透明模式必需）指定真实和映射接口。确保命令中包含圆括号。在路由模式下，如不指定真实和映射接口，则将使用所有接口；还可为一个或两个接口指定关键字 **any**。 • Mapped IP address - 可以将映射 IP 地址指定为： – 内联主机地址。 – 被定义为主机地址的现有网络对象（请参阅步骤 1）。 – **pat-pool** - 包含多个地址的现有网络对象或组。 – **interface** -（仅路由模式）用作映射地址的映射接口 IP 地址。如果指定 **ipv6**，则将使用接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置特定接口。要使用接口 IP 地址时，必须使用此关键字；不能内联输入或作为对象输入。 • 对于 PAT 池，可以指定以下一个或多个选项： – Round robin - **round-robin** 关键字使轮询地址分配能够用于 PAT 池。不使用轮询调度时，默认情况下，在使用下一个 PAT 地址前，将分配 PAT 地址的所有端口。轮询调度方法分配来自池中每个 PAT 地址的地址 / 端口，然后才返回再次使用第一个地址，然后是第二个地址，以此类推。 （续）

命令	用途
	（续） – Extended PAT - **extended** 关键字支持扩展 PAT。通过将目标地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按*服务*使用 65535 个端口。通常，创建 PAT 转换时，将不考虑目标端口和地址，因此，限定您按 PAT 地址使用 65535 个端口。例如，借助于扩展 PAT，可创建进入 192.168.1.7:23 时的 10.1.1.1:1027 转换，以及进入 192.168.1.7:80 时的 10.1.1.1:1027 转换。 – Flat range - 分配端口时，**flat** 关键字支持使用 1024 到 65535 的整个端口范围。为转换选择映射端口号时，ASA 将使用真实源端口号（如可用）。然而，如不使用此选项，则当真实端口*不*可用时，将默认从与真实端口号相同的端口范围选择映射端口：1 至 511、512 至 1023 以及 1024 至 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用整个范围 1 至 65535，请也指定 **include-reserve** 关键字。 • Interface PAT fallback -（可选）在主要 PAT 地址之后输入时，**interface** 关键字支持接口 PAT 退回。主要 PAT 地址用尽之后，则使用映射接口的 IP 地址。如果指定 **ipv6**，则将使用接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置特定接口。（不能在透明模式下指定**接口**）。 • DNS -（可选）**dns** 关键字可以转换 DNS 回复。确保启用 DNS 检测（默认情况下启用）。有关详细信息，请参阅第 4-30 页上的 DNS 和 NAT。

示例

以下示例配置动态 PAT，将 192.168.2.0 网络隐藏在地址 10.2.2.2 后面：

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 10.2.2.2
```

以下示例配置动态 PAT，将 192.168.2.0 网络隐藏在外部接口地址后面：

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic interface
```

以下示例使用 PAT 池配置动态 PAT，将内部 IPv6 网络转换为外部 IPv4 网络：

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

配置静态 NAT 或带有端口转换的静态 NAT

本节介绍如何使用网络对象 NAT 配置静态 NAT 规则。有关详细信息，请参阅第 4-3 页上的静态 NAT。

详细步骤

	命令	用途
步骤 1	（可选）为映射地址创建网络对象或组。	请参阅第 5-4 页上的为映射地址添加网络对象。
步骤 2	**object network** *obj_name* **示例：** `hostname(config)# object network my-host-obj1`	配置一个要为其配置 NAT 的网络对象，或者进入一个现有网络对象的对象网络配置模式。
步骤 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **示例：** `hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0`	如果正在创建新的网络对象，则定义要转换的**实际** IP 地址（IPv4 或 IPv6）。

	命令	用途
步骤 4	**nat** [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj* | **interface** [**ipv6**]} [**net-to-net**] [**dns** | **service** {**tcp** | **udp**} *real_port mapped_port*] [**no-proxy-arp**] **示例：** `hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS service tcp 80 8080`	为对象 IP 地址创建**静态 NAT**。只能为给定对象定义单一 NAT 规则。 • Interfaces -（透明模式必需）指定真实和映射接口。确保命令中包含圆括号。在路由模式下，如不指定真实和映射接口，则将使用所有接口；还可为一个或两个接口指定关键字 **any**。 • Mapped IP Addresses - 可以将映射 IP 地址指定为： – 内联 IP 地址。映射网络的网络掩码或范围与实际网络的相同。例如，如果实际网络为主机，则该地址将是主机地址。如果是范围，则映射地址包含的地址数量与实际范围的相同。例如，如果实际地址定义为 10.1.1.1 到 10.1.1.6 的范围，并且将 172.20.1.1 指定为映射地址，则映射范围将包括 172.20.1.1 到 172.20.1.6。 – 现有网络对象或组（请参阅步骤 1）。 – **interface** -（仅带端口转换的静态 NAT；路由模式）对于此选项，必须为 *mapped_ifc* 配置特定接口。如果指定 **ipv6**，则将使用接口的 IPv6 地址。另请确保配置 **service** 关键字。 通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。请参阅第 4-3 页上的静态 NAT。 • Net-to-net -（可选）对于 NAT 46，指定 **net-to-net** 以便将第一个 IPv4 地址转换为第一个 IPv6 地址，将第二个 IPv4 地址转换为第二个 IPv6 地址，以此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此关键字。 • DNS -（可选）**dns** 关键字可以转换 DNS 回复。确保启用 DNS 检测（默认情况下启用）。请参阅第 4-30 页上的 DNS 和 NAT。如果指定 **service** 关键字，此选项不可用。 • Port translation -（仅带端口转换的静态 NAT）指定 **tcp** 或 **udp** 以及实际和映射端口。可以输入端口号或已知端口名称（例如 **ftp**）。 • No Proxy ARP -（可选）指定 **no-proxy-arp**，以便为流向映射 IP 地址的传入数据包禁用代理 ARP。有关详细信息，请参阅第 4-20 页上的映射地址和路由。

示例

以下示例为内部的实际主机 10.1.1.1 到外部的 10.2.2.2 配置静态 NAT，启用 DNS 重写。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.2.2.2 dns
```

以下示例使用映射对象为内部实际主机 10.1.1.1 到外部 10.2.2.2 配置静态 NAT。

```
hostname(config)# object network my-mapped-obj
hostname(config-network-object)# host 10.2.2.2
```

```
hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-mapped-obj
```

以下示例为位于 TCP 端口 21 的 10.1.1.1 到位于端口 2121 的外部接口配置带端口转换的静态 NAT。

```
hostname(config)# object network my-ftp-server
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static interface service tcp 21 2121
```

以下示例将内部 IPv4 网络映射到外部 IPv6 网络。

```
hostname(config)# object network inside_v4_v6
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

以下示例将内部 IPv6 网络映射到外部 IPv6 网络。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96
hostname(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

配置身份标识 NAT

本节介绍如何使用网络对象 NAT 配置身份标识 NAT 规则。有关详细信息，请参阅第 4-11 页上的身份标识 NAT。

详细步骤

	命令	用途
步骤 1	（可选）为映射地址创建网络对象。	对象必须包含要转换的相同地址。请参阅第 5-4 页上的为映射地址添加网络对象。
步骤 2	**object network** *obj_name* **示例：** `hostname(config)# object network my-host-obj1`	配置一个要为其执行身份标识 NAT 的网络对象，或者进入一个现有网络对象的对象网络配置模式。此网络对象的名称不同于映射网络对象的名称（请参阅步骤 1），即使它们都包含相同的 IP 地址。
步骤 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **示例：** `hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0`	如果正在创建新的网络对象，定义要向其执行身份标识 NAT 的实际 IP 地址（IPv4 或 IPv6）。如果为步骤 1 中的映射地址配置了网络对象，则这些地址必须匹配。

	命令	用途
步骤 4	**nat** [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj*} [**no-proxy-arp**] [**route-lookup**] **示例：** hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS	为对象 IP 地址配置**身份标识 NAT**。 **注**　只能为给定对象定义单一 NAT 规则。请参阅第 5-3 页上的其他准则。 请参阅以下准则： • Interfaces -（透明模式必需）指定真实和映射接口。确保命令中包含圆括号。在路由模式下，如不指定真实和映射接口，则将使用所有接口；还可为一个或两个接口指定关键字 **any**。 • Mapped IP addresses - 确保为映射地址和实际地址配置相同的 IP 地址。使用以下方法之一： – Network object - 包含与实际对象相同的 IP 地址（请参阅步骤 1）。 – Inline IP address - 映射网络的网络掩码或范围与实际网络的相同。例如，如果实际网络为主机，则该地址将是主机地址。如果是范围，则映射地址包含的地址数量与实际范围的相同。例如，如果实际地址定义为 10.1.1.1 到 10.1.1.6 的范围，并且将 10.1.1.1 指定为映射地址，则映射范围将包括 10.1.1.1 到 10.1.1.6。 • No Proxy ARP - 指定 **no-proxy-arp**，为映射 IP 地址的传入数据包禁用代理 ARP。有关详细信息，请参阅第 4-20 页上的映射地址和路由。 • Route lookup -（仅路由模式；接口已指定）指定 **route-lookup**，以使用路由查询而非在 NAT 命令中指定的接口确定出口接口。有关详细信息，请参阅第 4-23 页上的确定出口接口。

示例

以下示例使用内联映射地址将主机地址映射到它本身：

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.1.1.1
```

以下示例使用网络对象将主机地址映射到它本身：

```
hostname(config)# object network my-host-obj1-identity
hostname(config-network-object)# host 10.1.1.1

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

配置每会话 PAT 规则

默认情况下，所有 TCP PAT 流量和所有 UDP DNS 流量均使用每会话 PAT。要将多会话 PAT 用于流量，可配置每会话 PAT 规则：一条允许规则使用每会话 PAT，一条拒绝规则使用多会话 PAT。有关每会话 PAT 和 多会话 PAT 的详细信息，请参阅第 4-10 页上的每会话 PAT 与多会话 PAT。

默认值

默认情况下，安装以下规则：

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

注　无法移除这些规则，它们始终存在于任何手动创建的规则后面。因为按顺序评估规则，所以您可以忽略默认规则。例如，要完全忽略这些规则，您可以添加以下规则：

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

详细步骤

命令	用途
xlate per-session {**permit** | **deny**} {**tcp** | **udp**} *source_ip* [*operator src_port*] *destination_ip operator dest_port* **示例：** `hostname(config)# xlate per-session deny tcp any4 209.165.201.3 eq 1720`	创建允许或拒绝规则。此规则置于默认规则上方，但在任何其他手动创建的规则下方。确保按应用顺序创建规则。 对于源 IP 地址和目标 IP 地址，可以配置以下选项： • **host** *ip_address* - 指定 IPv4 主机地址。 • *ip_address mask* - 指定 IPv4 网络地址和子网掩码。 • *ipv6-address/prefix-length* - 指定 IPv6 主机或网络地址和前缀。 • **any4** 和 **any6** - **any4** 仅指定 IPv4 流量； **any6** 指定 any6 流量。 *运算符*与源或目标使用的端口号相匹配。允许的运算符如下所示： • lt - 小于 • gt - 大于 • eq - 等于 • neq - 不等于 • range - 包含的值范围。使用此运算符时，指定两个端口号，例如： `范围 100 200`

示例

以下示例为 H.323 流量创建拒绝规则，以便其能够使用多会话 PAT：

```
hostname(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
hostname(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

监控网络对象 NAT

要监控对象 NAT，请输入以下命令之一：

命令	用途
show nat	显示 NAT 统计信息，包括每条 NAT 规则的命中信息。
show nat pool	显示 NAT 池统计信息，包括已分配的地址和端口，及其分配次数。

show running-config nat	显示 NAT 配置。
	注　不能使用 **show running-config object** 命令查看 NAT 配置。不能引用尚未**在 nat** 命令中创建的对象或对象组。为避免在 **show** 命令输出中向前引用或循环引用，**show running-config** 命令显示两次 **object** 命令：首先，定义 IP 地址；稍后，定义 **nat** 命令。此命令输出保证首先定义对象，然后定义对象组，最后定义 NAT。例如：
	`hostname# show running-config`
	`...`
	`object network obj1`
	`  range 192.168.49.1 192.150.49.100`
	`object network obj2`
	`  object 192.168.49.100`
	`object network network-1`
	`  subnet <network-1>`
	`object network network-2`
	`  subnet <network-2>`
	`object-group network pool`
	`  network-object object obj1`
	`  network-object object obj2`
	`...`
	`object network network-1`
	`  nat (inside,outside) dynamic pool`
	`object network network-2`
	`  nat (inside,outside) dynamic pool`

show xlate	显示当前 NAT 会话信息。

网络对象 NAT 配置示例

本节包括以下配置示例：

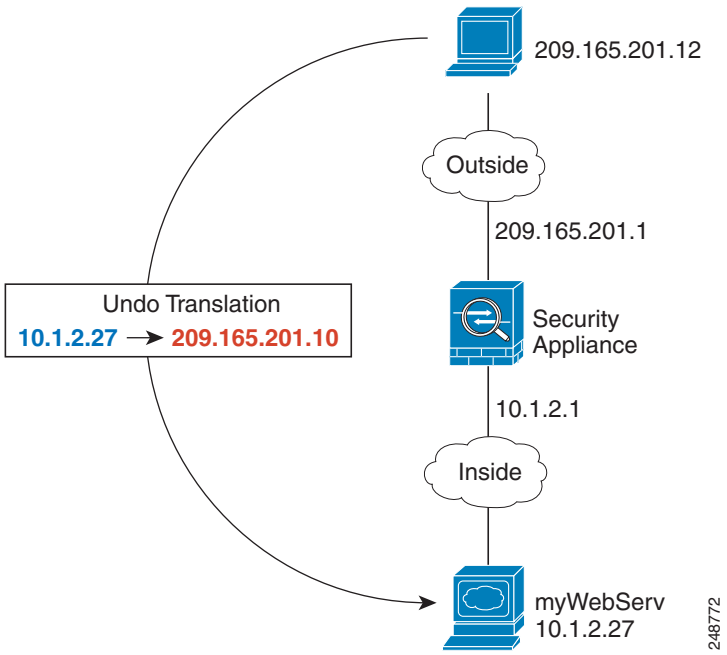
- 第 5-16 页上的提供到内部网络服务器的访问（静态 NAT）
- 第 5-17 页上的面向内部主机的 NAT（动态 NAT）和面向外部网络服务器的 NAT（静态 NAT）
- 第 5-18 页上的有多个映射地址的内部负载平衡器（静态 NAT，一对多）

- 第 5-19 页上的用于 FTP、HTTP 和 SMTP（带端口转换的静态 NAT）的单一地址
- 第 5-20 页上的映射接口上的 DNS 服务器、实际接口上的网络服务器（带 DNS 修改的静态 NAT）
- 第 5-22 页上的映射接口上的 DNS 服务器和 FTP 服务器，FTP 服务器已转换（带 DNS 修改的静态 NAT）
- 第 5-23 页上的映射接口上的 IPv4 DNS 服务器和 FTP 服务器，实际接口上的 IPv6 主机（带 DNS64 修改的静态 NAT64）

提供到内部网络服务器的访问（静态 NAT）

以下示例为内部网络服务器执行静态 NAT。实际地址位于专用网络上，因此，公共地址是必需的。静态 NAT 是必需的，因此，主机能够在固定地址发起到网络服务器的流量。（请参阅图 5-1）。

图 5-1　内部网络服务器的静态 NAT



步骤 1　为内部网络服务器创建网络对象：

```
hostname(config)# object network myWebServ
```

步骤 2　定义网络服务器地址：

```
hostname(config-network-object)# host 10.1.2.27
```

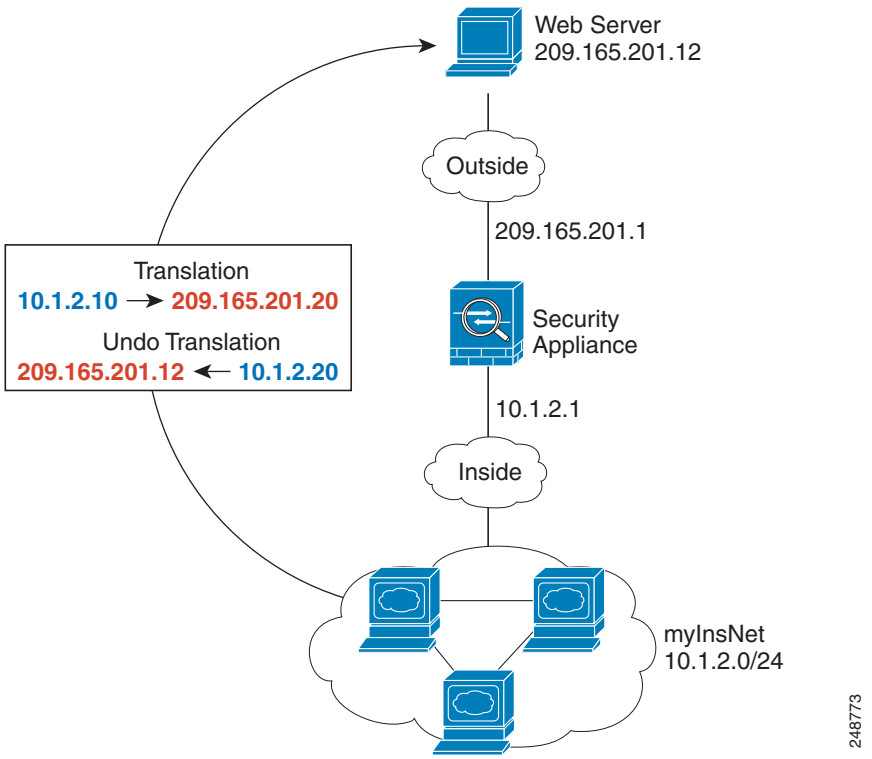
步骤 3　配置对象的静态 NAT：

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

面向内部主机的 NAT（动态 NAT）和面向外部网络服务器的 NAT（静态 NAT）

当专用网络上的内部用户访问外部网络服务器时，以下示例为他们配置动态 NAT。此外，当内部用户连接到外部网络服务器时，该网络服务器地址被转换为显示在内部网络上的地址。（请参阅图 5-2）。

图 5-2　面向内部网络的动态 NAT，面向外部网络服务器的静态 NAT



步骤 1　为要向其转换内部地址的动态 NAT 池创建一个网络对象：

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 209.165.201.20 209.165.201.30
```

步骤 2　为内部网络创建网络对象：

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

步骤 3　为内部网络启用动态 NAT：

```
hostname(config-network-object)# nat (inside,outside) dynamic myNatPool
```

步骤 4　为外部网络服务器创建网络对象：

```
hostname(config)# object network myWebServ
```

步骤 5　定义网络服务器地址：

```
hostname(config-network-object)# host 209.165.201.12
```

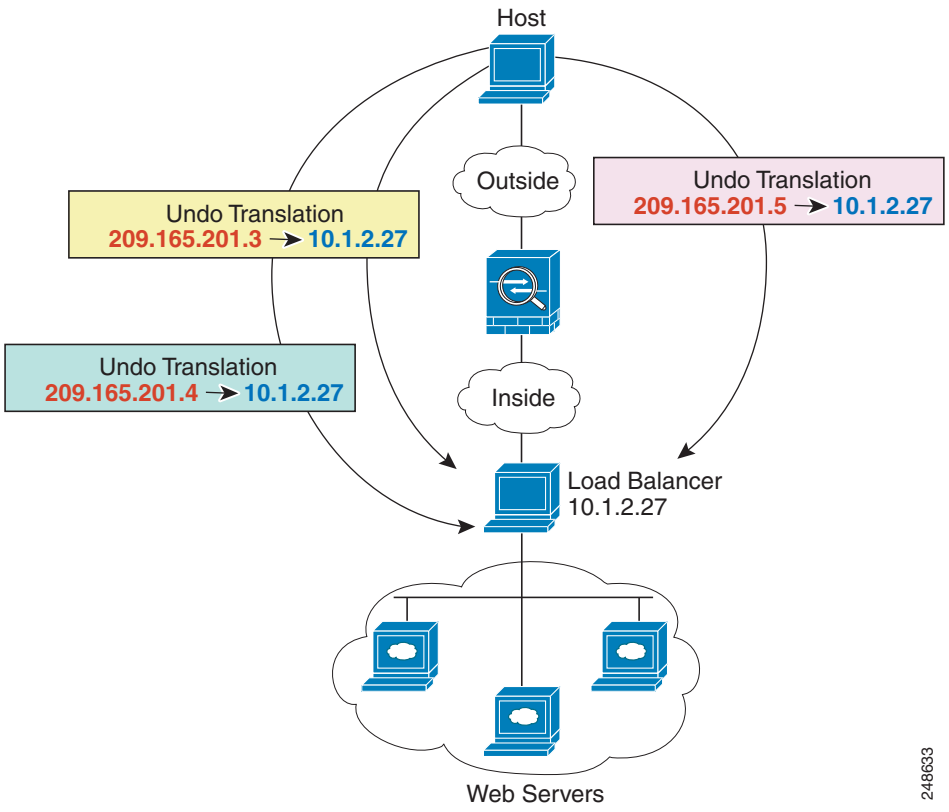
步骤 6　为网络服务器配置静态 NAT：

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.20
```

有多个映射地址的内部负载平衡器（静态 NAT，一对多）

以下示例显示转换为多个 IP 地址的内部负载平衡器。当外部主机访问其中一个映射 IP 地址时，将该地址反向转换为单一负载平衡器地址。根据请求的 URL，它会将流量重新定向到正确的网络服务器。（请参阅图 5-3）。

图 5-3　　内部负载平衡器的一对多静态 NAT



步骤 1　为要向其映射负载平衡器的地址创建网络对象：

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 209.165.201.3 209.265.201.8
```

步骤 2　为负载平衡器创建网络对象：

```
hostname(config)# object network myLBHost
```

步骤 3　定义负载平衡器地址：

```
hostname(config-network-object)# host 10.1.2.27
```

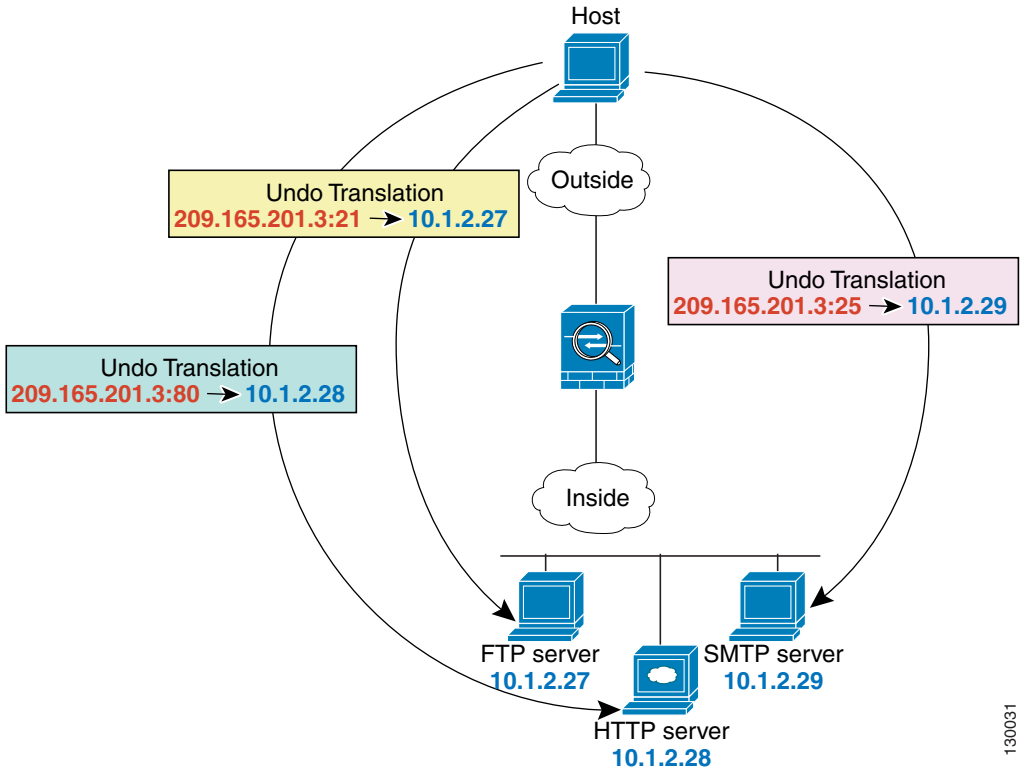
步骤 4　为负载平衡器配置静态 NAT：

```
hostname(config-network-object)# nat (inside,outside) static myPublicIPs
```

用于 FTP、HTTP 和 SMTP（带端口转换的静态 NAT）的单一地址

以下带端口转换的静态 NAT 示例为远程用户访问 FTP、HTTP 和 SMTP 提供单一地址。实际上，这些服务器是实际网络上的不同设备，但对于每台服务器，可以指定采用端口转换规则的静态 NAT，这些规则使用同一映射 IP 地址和不同端口。（请参阅图 5-4。）

图 5-4　　带端口转换的静态 NAT



步骤 1　为 FTP 服务器地址创建网络对象：

```
hostname(config)# object network FTP_SERVER
```

步骤 2　定义 FTP 服务器地址，为 FTP 服务器配置带身份端口转换的静态 NAT：

```
hostname(config-network-object)# host 10.1.2.27
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp ftp
ftp
```

步骤 3　为 HTTP 服务器地址创建网络对象：

```
hostname(config)# object network HTTP_SERVER
```

步骤 4　定义 HTTP 服务器地址，为 HTTP 服务器配置带身份端口转换的静态 NAT：

```
hostname(config-network-object)# host 10.1.2.28
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
http http
```

步骤 5　为 SMTP 服务器地址创建网络对象：

```
hostname(config)# object network SMTP_SERVER
```

步骤 6　定义 SMTP 服务器地址，为 SMTP 服务器配置带身份端口转换的静态 NAT：

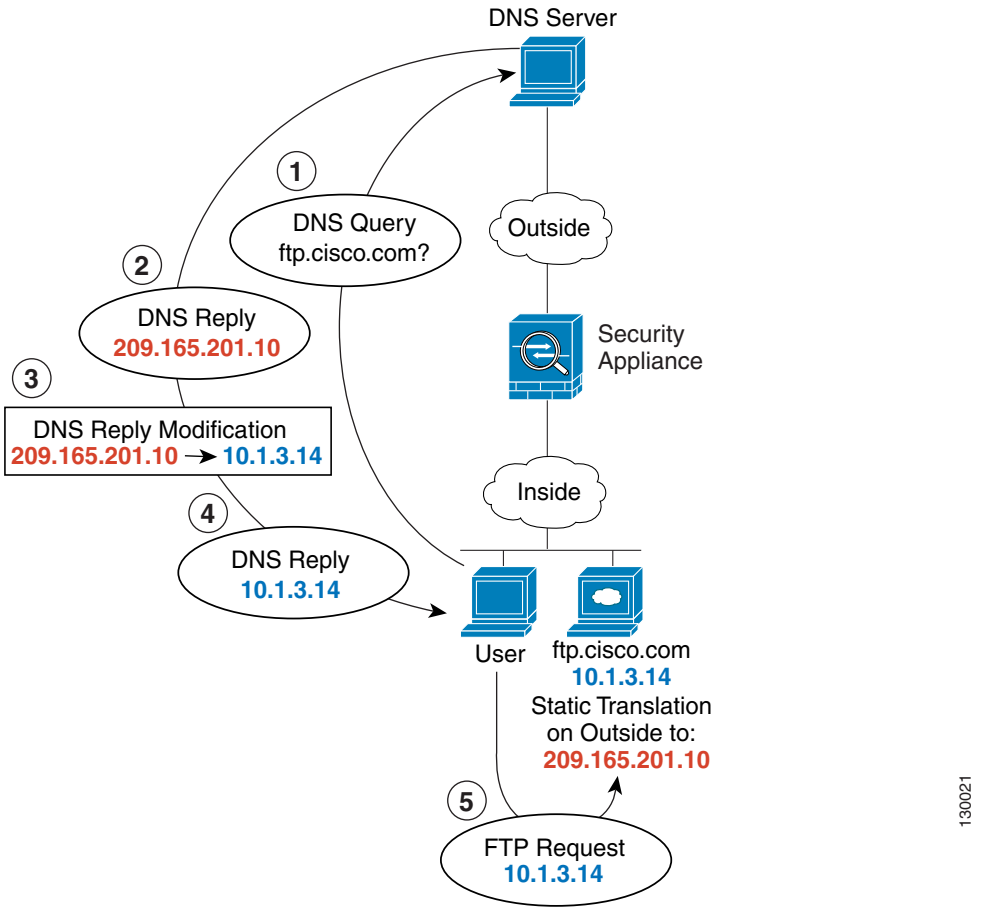
```
hostname(config-network-object)# host 10.1.2.29
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
smtp smtp
```

映射接口上的 DNS 服务器、实际接口上的网络服务器（带 DNS 修改的静态 NAT）

例如，可以从外部接口访问 DNS 服务器。服务器 ftp.cisco.com 在内部接口上。将 ASA 配置为静态地将 ftp.cisco.com 实际地址 (10.1.3.14) 转换为在外部网络上可见的映射地址 (209.165.201.10)。（请参阅图 5-5。）在这种情况下，您要在此静态规则上启用 DNS 回复修改，以便使用实际地址访问 ftp.cisco.com 的内部用户可以接收来自 DNS 服务器的实际地址，而不是映射地址。

当内部主机发送对 ftp.cisco.com 的地址的 DNS 请求时，DNS 服务器将以映射地址 (209.165.201.10) 作为回复。ASA 是指内部服务器的静态规则，并且将 DNS 回复中的地址转换为 10.1.3.14。如果不启用 DNS 回复修改，则内部主机尝试将流量发送到 209.165.201.10，而不是直接访问 ftp.cisco.com。

图 5-5　DNS 回复修改



步骤 1　为 FTP 服务器地址创建网络对象：

```
hostname(config)# object network FTP_SERVER
```

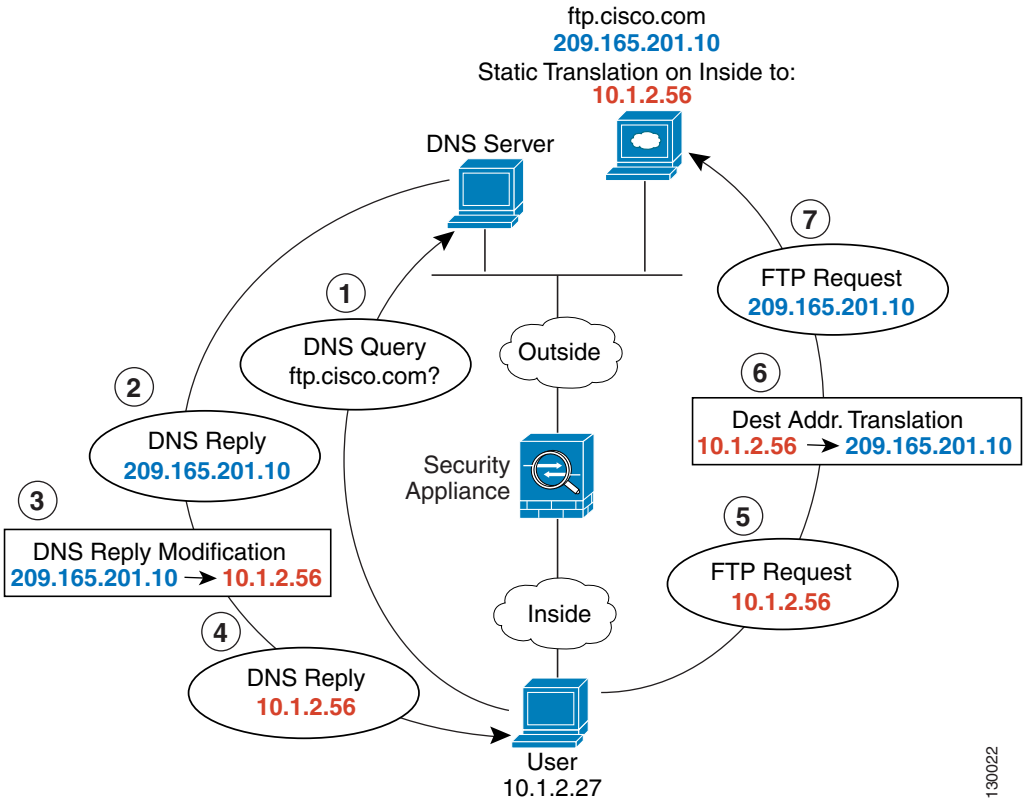
步骤 2　定义 FTP 服务器地址，并且配置带 DNS 修改的静态 NAT：

```
hostname(config-network-object)# host 10.1.3.14
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10 dns
```

映射接口上的 DNS 服务器和 FTP 服务器，FTP 服务器已转换（带 DNS 修改的静态 NAT）

图 5-6 显示外部网络上的 FTP 服务器和 DNS 服务器。ASA 有面向外部服务器的静态转换。在这种情况下，当内部用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.201.10 作为响应。因为您想让内部用户使用 ftp.cisco.com 的映射地址 (10.1.2.56)，所以您需要配置 DNS 回复修改以进行静态转换。

图 5-6　使用外部 NAT 的 DNS 回复修改



步骤 1　为 FTP 服务器地址创建网络对象：

```
hostname(config)# object network FTP_SERVER
```

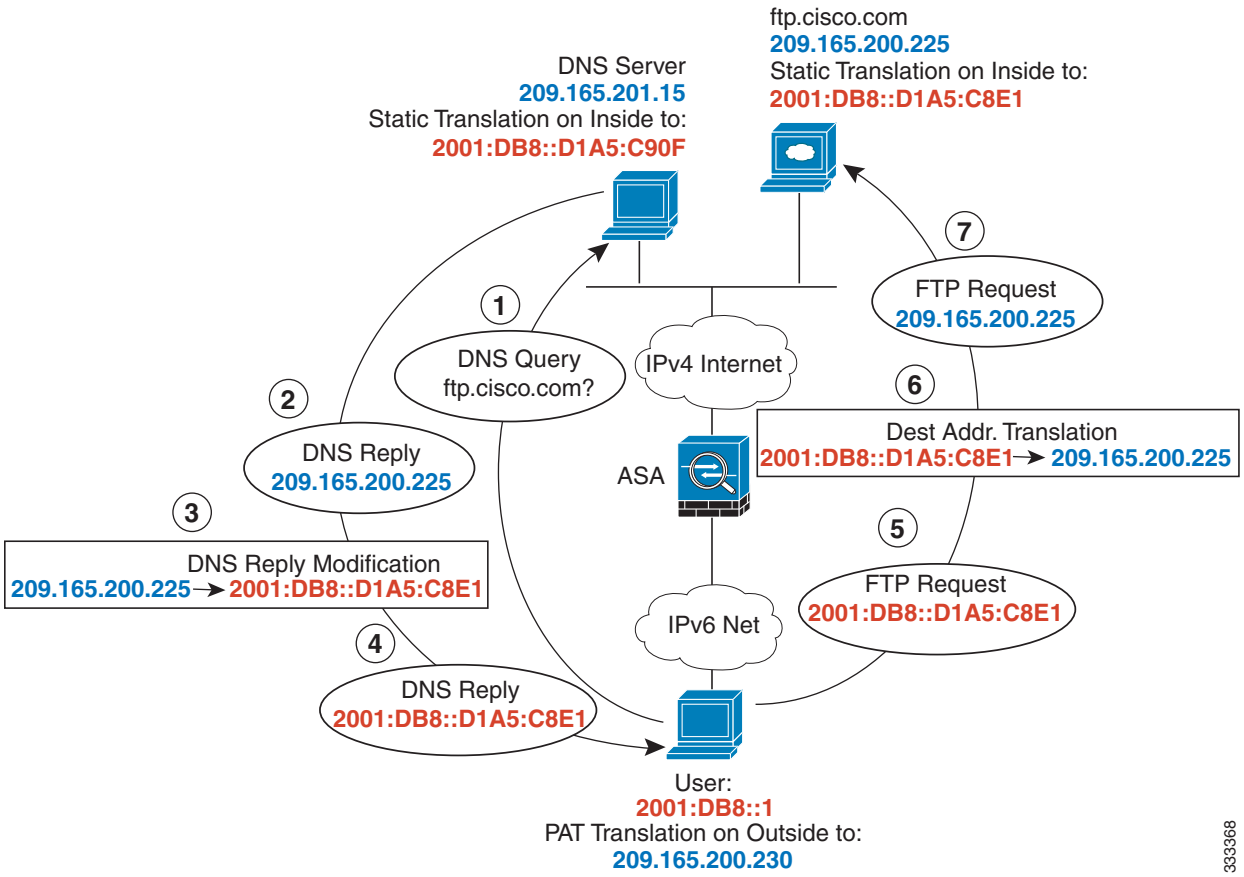
步骤 2　定义 FTP 服务器地址，并且配置带 DNS 修改的静态 NAT：

```
hostname(config-network-object)# host 209.165.201.10
hostname(config-network-object)# nat (outside,inside) static 10.1.2.56 dns
```

映射接口上的 IPv4 DNS 服务器和 FTP 服务器，实际接口上的 IPv6 主机（带 DNS64 修改的静态 NAT64）

图 5-6 显示外部 IPv4 网络上的 FTP 服务器和 DNS 服务器。ASA 有面向外部服务器的静态转换。在这种情况下，当内部 IPv6 用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.200.225 作为响应。因为您想让内部用户使用 ftp.cisco.com 的映射地址 (2001:DB8::D1A5:C8E1)，所以您需要配置 DNS 回复修改以进行静态转换。本示例还包括面向 DNS 服务器的静态 NAT 转换和面向内部 IPv6 主机的 PAT 规则。

图 5-7　使用外部 NAT 的 DNS 回复修改



步骤 1　为 FTP 服务器配置带 DNS 修改的静态 NAT。

a. 为 FTP 服务器地址创建网络对象。

```
hostname(config)# object network FTP_SERVER
```

b. 定义 FTP 服务器地址，配置带 DNS 修改的静态 NAT，因为这是一对一转换，所以请为 NAT46 网络对网络一对一方法。

```
hostname(config-network-object)# host 209.165.200.225
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C8E1/128
net-to-net dns
```

步骤 2　为 DNS 服务器配置 NAT。

a. 为 DNS 服务器地址创建网络对象。

```
hostname(config)# object network DNS_SERVER
```

b. 定义 DNS 服务器地址，并且使用网络对网络方法配置静态 NAT。

```
hostname(config-network-object)# host 209.165.201.15
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C90F/128
net-to-net
```

步骤 3　配置 IPv4 PAT 池，以转换内部 IPv6 网络。

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
```

步骤 4　为内部 IPv6 网络配置 PAT。

a. 为内部 IPv6 网络创建网络对象。

```
hostname(config)# object network IPv6_INSIDE
```

b. 定义 IPv6 网络地址，并且使用 PAT 池配置动态 NAT。

```
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

网络对象 NAT 的功能历史

表 5-1 列出了各项功能变更以及实施了该变更的平台版本。

表 5-1　网络对象 NAT 的功能历史

功能名称	平台版本	功能信息
网络对象 NAT	8.3(1)	为网络对象 IP 地址配置 NAT。 我们引入或修改了以下命令：**nat**（对象网络配置模式）、**show nat**、**show xlate**、**show nat pool**。
身份标识 NAT 可配置代理 ARP 和路由查询	8.4(2)/8.5(1)	在身份标识 NAT 的更早版本中，代理 ARP 被禁用，路由查询始终用于确定出口接口。无法配置这些设置。在 8.4(2) 及更高版本中，身份标识 NAT 的默认行为已更改为匹配其他静态 NAT 配置的行为：在默认情况下，代理 ARP 已启用，并且 NAT 配置确定出口接口（如果已指定）。您可以原样保留这些设置，或者单独启用或禁用这些设置。请注意，现在您也可以为常规静态 NAT 禁用代理 ARP。 从 8.3(1)、8.3(2) 和 8.4(1) 升级至 8.4(2) 时，所有标识 NAT 配置现包含 **no-proxy-arp** 和 **route-lookup** 关键字，以便维持现有功能。 我们修改了以下命令：**nat static** [**no-proxy-arp**] [**route-lookup**]。

表 5-1　网络对象 NAT 的功能历史（续）

功能名称	平台版本	功能信息
PAT 池和轮询调度地址分配	8.4(2)/8.5(1)	现在，您可以指定 PAT 地址池，而不是单一地址。或者还可以启用 PAT 地址的轮询调度分配，而不是先使用 PAT 地址上的所有端口，然后再使用池中的下一个地址。这些功能有助于防止来自单一 PAT 地址的大量连接显示为 DoS 攻击的一部分，并使大量 PAT 地址的配置过程变轻松。 我们修改了以下命令：**nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]]。
轮询调度 PAT 池分配使用现有主机的相同 IP 地址	8.4(3)	组合使用 PAT 池与轮询调度分配时，如果主机拥有现有连接，且有端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。 我们未修改任何命令。 *此功能在 8.5(1) 或 8.6(1) 中不可用。*
用于 PAT 池的无层次的 PAT 端口范围	8.4(3)	如果可用，真实源端口号将用于映射端口。然而，如果真实端口*不*可用，将默认从与真实端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，1024 以下的端口只有一个小 PAT 池。 如您拥有的大量流量使用较低端口范围，在使用 PAT 池时，现可指定将要使用的无层次的端口范围，而不是三个不同大小的层：1024 至 65535，或 1 至 65535。 我们修改了以下命令：**nat dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]]。 *此功能在 8.5(1) 或 8.6(1) 中不可用。*
用于 PAT 池的扩展 PAT	8.4(3)	每个 PAT IP 地址允许最多 65535 个端口。如果 65535 个端口不能提供足够的转换，则现可启用适合 PAT 池的扩展 PAT。通过将目标地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按*服务*使用 65535 个端口。 我们修改了以下命令：**nat dynamic** [**pat-pool** *mapped_object* [**extended**]]。 *此功能在 8.5(1) 或 8.6(1) 中不可用。*

表 5-1　网络对象 NAT 的功能历史（续）

功能名称	平台版本	功能信息
自动 NAT 规则，这些规则可以将 VPN 对等设备的本地 IP 地址转换回对等设备的真实 IP 地址	8.4(3)	在极少数情况下，您可能想要使用 VPN 对等设备在内部网络上的真实 IP 地址，而非已分配的本地 IP 地址。通常在使用 VPN 的情况下，会给定对等体分配的本地 IP 地址来访问内部网络。但是，在例如内部服务器和网络安全基于对等体的真实 IP 地址的情况下，可能要将本地 IP 地址重新转换为对等体的真实公有 IP 地址。 可以在每个隧道组一个接口的基础上启用此功能。当 VPN 会话已建立或断开连接时，动态添加或删除对象 NAT 规则。可使用 **show nat** 命令查看这些规则。 **注**　由于路由问题，我们不建议使用此功能，除非您知道您需要此功能；请联系思科 TAC 确认网络的功能兼容性。请参阅以下限制： • 仅支持 Cisco IPsec 和 AnyConnect Client。 • 流向公共 IP 地址的返回流量必须路由回 ASA，因此，可应用 NAT 策略和 VPN 策略。 • 不支持负载平衡（由于路由问题）。 • 不支持漫游（公共 IP 更改）。 我们引入了以下命令：**nat-assigned-to-public-ip** *interface*（tunnel-group general-attributes 配置模式）。
对 IPv6 的 NAT 支持	9.0(1)	NAT 现在支持 IPv6 流量，以及 IPv4 和 IPv6 之间的转换。在透明模式下，不支持 IPv4 和 IPv6 之间的转换。 我们修改了以下命令：**nat**（对象网络配置模式）、**show nat**、 **show nat pool**、**show xlate**。
反向 DNS 查找的 NAT 支持	9.0(1)	在为 NAT 规则启用了 DNS 检测的情况下使用 IPv4 NAT、IPv6 NAT 和 NAT64 时，NAT 现支持为反向 DNS 查找转换 DNS PTR 记录。

表 5-1　网络对象 NAT 的功能历史（续）

功能名称	平台版本	功能信息
每会话 PAT	9.0(1)	每会话 PAT 功能可以提高 PAT 的可扩展性，而且对于集群，允许每个成员单元拥有自己的 PAT 连接；多会话 PAT 连接必须转发到主单元并归主单元所有。每会话 PAT 会话结束时，ASA 将发送重置，并立即移除转换。此重置将导致结束节点立即释放连接，从而避免 TIME_WAIT 状态。另一方面，多会话 PAT 使用 PAT 超时，默认情况下为 30 秒。对于“游击”流量，如 HTTP 或 HTTPS，每会话功能可以显著提高一个地址支持的连接速率。在不使用每会话功能的情况下，对于 IP 协议，一个地址的最大连接速率约为每秒 2000。在使用每会话功能的情况下，对于 IP 协议，一个地址的连接速率为 65535/*average-lifetime*。 默认情况下，所有 TCP 流量和 UDP DNS 流量均使用每会话 PAT 转换。对于需要多会话 PAT 的流量，如 H.323、SIP 或 Skinny，可通过创建每会话拒绝规则来禁用每会话 PAT。 我们引入了以下命令：**xlate per-session**、**show nat pool**。

两次 NAT

两次 NAT 可供您在单一规则中同时确定源和目标地址。本章向您展示如何配置两次 NAT。

- 第 6-1 页上的有关两次 NAT 的信息
- 第 6-2 页上的两次 NAT 的许可要求
- 第 6-2 页上的两次 NAT 的先决条件
- 第 6-2 页上的准则和限制
- 第 6-4 页上的默认设置
- 第 6-4 页上的配置两次 NAT
- 第 6-19 页上的监控两次 NAT
- 第 6-19 页上的两次 NAT 的配置示例
- 第 6-22 页上的两次 NAT 的功能历史记录

注 有关 NAT 工作原理的详细信息，请参阅第 4 章，“ 网络地址转换 (NAT)”。

有关两次 NAT 的信息

两次 NAT 可供您在单一规则中同时确定源和目标地址。如果同时指定源和目标地址，则可指定以下情况：例如，在进入目标 X 时源地址应转换为 A，但在进入目标 Y 时转换为 B。

注 对于静态 NAT，规则是双向的，因此，请注意，整个本指南中命令和描述中使用的“ 源 ”和“ 目标 ”，即便是给定的连接，也可能源自“ 目标 ”地址。例如，如果使用端口地址转换配置静态 NAT，将源地址指定为 Telnet 服务器，且您想要进入该 Telnet 服务器的所有流量将端口从 2323 转换为 23，则在命令中，必须指定将要转换的 *source* 端口（real: 23，mapped: 2323）。您指定源端口是因为您将 Telnet 服务器地址指定为源地址。

目标地址是可选的。如果指定目标地址，可以将它映射到其本身（身份标识 NAT），或者将它映射到不同的地址。目标映射始终是静态映射。

两次 NAT 还可供您将服务对象用于带有端口转换的静态 NAT ；网络对象 NAT 仅接受内联定义。

有关两次 NAT 和网络对象 NAT 之间的差异的详细信息，请参阅第 4-14 页上的如何实施 NAT。

两次 NAT 规则将添加至 NAT 规则表的第 1 部分，或如已指定，也将添加至第 3 部分。有关 NAT 排序的详细信息，请参阅第 4-18 页上的 NAT 规则顺序。

两次 NAT 的许可要求

型号	许可证要求
ASAv	标准或高级许可证。
所有其他型号	基础许可证。

两次 NAT 的先决条件

- 对于真实和映射地址，请配置网络对象或网络对象组（**object network** 或 **object-group network** 命令）。在使用不连续的 IP 地址范围、多个主机或子网创建映射地址池时，网络对象组特别有用。要创建网络对象或组，请参阅常规操作配置指南。
- 对于带有端口转换的静态 NAT，请配置 TCP 或 UDP 服务对象（**object service** 命令）。要创建服务对象，请参阅常规操作配置指南。

有关对象和组的特定准则，请参阅与您想要配置的 NAT 类型对应的配置部分。另请参阅第 6-2 页上的准则和限制小节。

准则和限制

此节包括该功能的指导原则和限制。

情景模式准则

在单一和多情景模式下受支持。

防火墙模式准则

- 在路由和透明防火墙模式下受支持。
- 在透明模式下，必须指定实际接口和映射接口；不能使用 **any**。
- 在透明模式下，不能配置接口 PAT，因为透明模式接口没有 IP 地址。也不能将管理 IP 地址用作映射地址。
- 在透明模式下，不支持在 IPv4 和 IPv6 网络之间进行转换。支持在两个 IPv6 网络之间或两个 IPv4 网络之间进行转换。

IPv6 准则

- 支持 IPv6。
- 对于路由模式，还可以在 IPv4 和 IPv6 之间进行转换。
- 对于透明模式，不支持在 IPv4 和 IPv6 网络之间进行转换。支持在两个 IPv6 网络之间或两个 IPv4 网络之间进行转换。
- 对于透明模式，对于 IPv6 来说不支持 PAT 池。
- 对于静态 NAT，可以指定一个多达 /64 的 IPv6 子网。不支持更大的子网。
- 将 FTP 和 NAT46 配合使用时，当 IPv4 FTP 客户端连接到 IPv6 FTP 服务器时，客户端必须使用扩展被动模式 (EPSV) 或扩展端口模式 (EPRT)；在使用 IPv6 时，PASV 和 PORT 命令不受支持。

其他准则

- 当源 IP 地址为子网（或使用辅助连接的任何其他应用）时，无法配置 FTP 目标端口转换；FTP 数据信道的建立将不成功。例如，以下配置不起作用：

```
object network MyInsNet
 subnet 10.1.2.0 255.255.255.0
object network MapInsNet
 subnet 209.165.202.128 255.255.255.224
object network Server1
 host 209.165.200.225
object network Server1_mapped
 host 10.1.2.67
object service REAL_ftp
 service tcp destination eq ftp
object service MAPPED_ftp
 service tcp destination eq 2021
object network MyOutNet
 subnet 209.165.201.0 255.255.255.224

nat (inside,outside) source static MyInsNet MapInsNet destination static
Server1_mapped Server1 service MAPPED_ftp REAL_ftp
```

- 如果更改 NAT 配置，且不想要在使用新 NAT 信息之前等待现有转换超时，则可使用 **clear xlate** 命令清除转换表。然而，清除转换表将断开使用转换的当前所有连接。

  注　如果移除动态 NAT 或 PAT 规则，然后使用与已移除规则中地址重叠的映射地址添加新规则，则将不使用新规则，直至与已移除规则关联的所有连接超时，或已使用 **clear xlate** 命令将这些连接清除。此保护措施确保相同的地址将不分配至多个主机。

- 不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。
- 在 NAT 规则中使用 **any** 关键字时，“any” 流量（IPv4 与 IPv6）的定义取决于规则。只有数据包为 IPv6 至 IPv6 或 IPv4 至 IPv4，ASA 才能对数据包执行 NAT；借助此先决条件，ASA 可确定 NAT 规则中的 **any** 的值。例如，如果配置一条从 “any” 到 IPv6 服务器的规则，且该服务器映射自 IPv4 地址，则 **any** 意味着 “ 任何 IPv6 流量 ”。如果配置一条从 “any” 到 “any” 的规则，且将源映射至接口的 IPv4 地址，则 **any** 意味着 “ 任何 IPv4 流量 ”，因为映射接口地址暗示目标也是 IPv4。
- NAT 中使用的对象和对象组不能是未定义的，它们必须包含 IP 地址。
- 可在多个规则中使用相同的对象。
- 已映射 IP 地址池不能包括：
  - 已映射接口的 IP 地址。如果为规则指定 **any 接口**，那么所有接口 IP 地址将不被允许。对于接口 PAT（仅路由模式），请使用 **interface** 关键字，而非 IP 地址。
  - （透明模式）管理 IP 地址。
  - （动态 NAT）启用 VPN 时，备用接口 IP 地址。
  - 现有的 VPN 池地址。
- 避免在静态和动态 NAT 策略中使用重叠地址。例如，使用重叠地址，如果 PPTP 的辅助连接命中静态而非动态 xlate，将无法建立 PPTP 连接。
- 可使用 NAT 的事务提交模型提高系统性能和可靠性。请参阅常规操作配置指南中的基本设置章节，了解详细信息。使用 **asp rule-engine transactional-commit nat** 命令。

默认设置

- 默认情况下，规则将添加至 NAT 表的第 1 部分的末尾。
- （路由模式）默认实际接口和映射接口为 Any，可将规则应用于所有接口。
- 如果指定可选接口，则 ASA 将使用 NAT 配置确定出口接口，但您可以选择始终使用路由查询。

配置两次 NAT

本节描述如何配置两次 NAT。

- 第 6-4 页上的为真实和映射地址添加网络对象
- 第 6-6 页上的（可选）为真实和映射端口添加服务对象
- 第 6-7 页上的配置动态 NAT
- 第 6-10 页上的配置动态 PAT（隐藏）
- 第 6-14 页上的配置静态 NAT 或带有端口转换的静态 NAT
- 第 6-17 页上的配置身份标识 NAT
- 第 6-19 页上的配置每会话 PAT 规则

为真实和映射地址添加网络对象

对于每条 NAT 规则，均可为以下地址配置最多四个网络对象或组：

- **源真实地址**
- **源映射地址**
- **目标真实地址**
- **目标映射地址**

除非您以内联方式指定 **any** 关键字来代表所有流量，或对于某些类型的 NAT，指定 **interface** 关键字来代表接口地址，否则需要配置对象。有关配置网络对象或组的详细信息，请参阅常规操作配置指南。

准则

- 网络对象组可以包含多个对象和 / 或 IPv4 或 IPv6 地址的内联地址。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。
- 有关不允许的映射 IP 地址的详细信息，请参阅第 6-2 页上的准则和限制。
- 源动态 NAT：
  - 您通常会配置将要映射至较小组的较大真实地址组。
  - 已映射对象或分组不能包含子网；对象必须定义范围；分组可能包括主机和范围。
  - 如果已映射网络对象同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。

- 源动态 PAT（隐藏）：
  - 已映射对象或组不能包含子网；网络对象必须定义主机或为 PAT 池定义范围；网络对象组（用于 PAT 池）可能包含主机和范围。
- 源静态 NAT 或带有端口转换的静态 NAT：
  - 已映射对象或组可能包含主机、范围或子网。
  - 静态映射通常为一对一，因此真实地址的数量与映射地址相同。然而，如果需要，您可拥有不同的数量。有关详细信息，请参阅第 4-3 页上的静态 NAT。
- 源标识 NAT
  - 真实对象和映射对象必须匹配；可将相同的对象用于二者，也可创建包含相同 IP 地址的不同对象。
- 目标静态 NAT 或带有端口转换的静态 NAT（目标转换始终为静态）：
  - 尽管两次 NAT 的主要功能是纳入目标 IP 地址，但目标地址是可选的。如果您确实指定目标地址，则可为该地址配置静态转换，或只需将标识 NAT 用于该地址。您可能想要配置没有目标地址的两次 NAT，以利用两次 NAT 的一些其他特性，包括使用真实地址的网络对象组或对规则手动排序。有关详细信息，请参阅第 4-14 页上的网络对象 NAT 和两次 NAT 之间的主要差异。
  - 对于标识 NAT，真实对象和映射对象必须匹配；可将相同的对象用于二者，也可创建包含相同 IP 地址的不同对象。
  - 静态映射通常为一对一，因此真实地址的数量与映射地址相同。然而，如果需要，您可拥有不同的数量。有关详细信息，请参阅第 4-3 页上的静态 NAT。
  - 对于带有端口转换的静态接口 NAT（仅路由模式），可指定 **interface** 关键字，而不是映射地址的网络对象 / 组。有关详细信息，请参阅第 4-5 页上的带端口转换的静态接口 NAT。

详细步骤

命令	用途

object network *obj_name*
{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
 	
示例：
`hostname(config)# object network MyInsNet`
`hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0`
	添加网络对象，IPv4 或 IPv6。

命令	用途
object-group network *grp_name* {**network-object** {**object** *net_obj_name* | *subnet_address netmask* | **host** *ip_address*} | **group-object** *grp_obj_name*} **示例：** hostname(config)# object network TEST hostname(config-network-object)# range 10.1.1.1 10.1.1.70 hostname(config)# object network TEST2 hostname(config-network-object)# range 10.1.2.1 10.1.2.70 hostname(config-network-object)# object-group network MAPPED_IPS hostname(config-network)# network-object object TEST hostname(config-network)# network-object object TEST2 hostname(config-network)# network-object host 10.1.2.79	添加网络对象组，IPv4 或 IPv6。

（可选）为真实和映射端口添加服务对象

为以下端口配置服务对象：

- **源真实端口（仅静态）***或***目标真实端口**
- **源映射端口（仅静态）***或***目标映射端口**

有关配置服务对象的详细信息，请参阅常规操作配置指南。

准则

- NAT 仅支持 TCP 或 UDP。转换端口时，请确保真实和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。
- “ 不等于 ”**(neq)** 运算符不受支持。
- 对于标识端口转换，可将相同的服务对象同时用于真实和映射端口。
- 源动态 NAT - 源动态 NAT 不支持端口转换。
- 源动态 PAT（隐藏）- 源动态 PAT 不支持端口转换。
- 源静态 NAT 或带有端口转换的静态 NAT - 服务对象可能同时包含源和目标端口；然而，应为两个服务对象指*定*源*或*目标端口。如果您的应用使用固定的源端口（如某些 DNS 服务器），则您只能*同时*指定源和目标端口；然而，很少使用固定源端口。例如，如果您想要转换源主机的端口，则请配置源服务。
- 源标识 NAT - 服务对象可能同时包含源和目标端口；然而您应为两个服务对象指*定*源*或*目标端口。如果您的应用使用固定的源端口（如某些 DNS 服务器），则您只能*同时*指定源和目标端口；然而，很少使用固定源端口。例如，如果您想要转换源主机的端口，则请配置源服务。
- 目标静态 NAT 或带有端口转换的静态 NAT（目标转换始终为静态）- 对于非静态源 NAT，只能对目标执行端口转换。服务对象可能同时包含源和目标端口，但在此情况下，将仅使用目标端口。将忽略您指定的源端口。

详细步骤

	命令	用途

步骤 1	**object service** *obj_name*
	service {**tcp** | **udp**} [**source** *operator port*] [**destination** *operator port*]
	
	示例：
	`hostname(config)# object service REAL_SRC_SVC`
	`hostname(config-service-object)# service tcp source eq 80`
	
	`hostname(config)# object service MAPPED_SRC_SVC`
	`hostname(config-service-object)# service tcp source eq 8080`
		添加服务对象。

配置动态 NAT

本节描述如何为动态 NAT 配置两次 NAT。有关详细信息，请参阅第 4-8 页上的动态 NAT。

详细步骤

	命令	用途
步骤 1	为以下地址创建网络对象或组： • 源真实地址 • 源映射地址 • 目标真实地址 • 目标映射地址	请参阅第 6-4 页上的为真实和映射地址添加网络对象。 如果想要转换所有源流量，则跳过为源真实地址添加对象，转而在 **nat** 命令中指定 **any** 关键字。 如果想要配置仅带有端口转换的目标静态接口 NAT，则可跳过为目标映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。
步骤 2	（可选）为以下端口创建服务对象： • 目标真实端口 • 目标映射端口	请参阅第 6-6 页上的（可选）为真实和映射端口添加服务对象。

命令	用途
步骤 3 **nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-auto** [*line*]}] **source dynamic** {*real_obj* | **any**} {*mapped_obj* [**interface** [**ipv6**]]} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*] **示例：** hostname(config)# nat (inside,outside) source dynamic MyInsNet NAT_POOL destination static Server1_mapped Server1 service MAPPED_SVC REAL_SVC	配置**动态 NAT**。请参阅以下准则： • Interfaces -（透明模式必需）指定真实和映射接口。确保命令中包含圆括号。在路由模式下，如不指定真实和映射接口，则将使用所有接口；还可为一个或两个接口指定关键字 **any**。 • Section and Line -（可选）默认情况下，NAT 规则将添加至 NAT 表第 1 部分的末尾（请参阅第 4-18 页上的 NAT 规则顺序）。如果想要转而将规则添加至第 3 部分（位于网络对象 NAT 规则之后），则可使用 **after-auto** 关键字。借助于 *line* 参数，可将规则插入适用部分中的任何位置。 • 源地址： – Real - 指定网络对象、组或 **any** 关键字。 – Mapped - 指定不同的网络对象或组。或者您可以配置以下回退方法： 接口 PAT 回退 -（仅路由模式）**interface** 关键字可启用接口 PAT 回退。如果指定 **ipv6**，则将使用接口的 IPv6 地址。映射 IP 地址用尽后和映射接口的 IP 地址。对于此选项，必须为 *mapped_ifc* 配置特定接口。 • 目标地址（可选）： – Mapped - 指定网络对象或组，或对于仅带有端口转换的静态接口 NAT，指定 **interface** 关键字。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如指定 **interface**，请务必也配置 **service** 关键字。对于此选项，必须为 *real_ifc* 配置特定接口。有关详细信息，请参阅第 4-5 页上的带端口转换的静态接口 NAT。 – Real - 指定网络对象或组。对于标识 NAT，只需将相同的对象或组同时用于真实和映射地址。 • 目标端口 -（可选）指定 **service** 关键字以及映射和真实服务对象。对于标识端口转换，只需将相同的服务对象同时用于真实和映射端口。 • DNS -（可选；对于源专用规则）**dns** 关键字可转换 DNS 回复。确保启用 DNS 检测（默认情况下启用）。如配置 **destination** 地址，则无法配置 **dns** 关键字。有关详细信息，请参阅第 4-30 页上的 DNS 和 NAT。 • Unidirectional -（可选）请指定 **unidirectional**，以使目标地址无法发起流向源地址的流量。 • Inactive -（可选）要使该规则处于非活动状态，而无需移除此命令，请使用 **inactive** 关键字。要将其重新激活，请重新输入没有 **inactive** 关键字的整个命令。 • 描述 -（可选）使用 **description** 关键字提供最多 200 个字符的描述。

示例

以下示例在访问 209.165.201.1/27 网络上的服务器以及 203.0.113.0/24 网络上的服务器时为内部网络 10.1.1.0/24 配置动态 NAT。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1 destination
static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2 destination
static SERVERS_2 SERVERS_2
```

以下示例在访问 IPv4 209.165.201.1/27 网络上的服务器以及 203.0.113.0/24 网络上的服务器时为 IPv6 内部网络 2001:DB8:AAAA::/96 配置动态 NAT。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1 destination
static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2 destination
static SERVERS_2 SERVERS_2
```

配置动态 PAT（隐藏）

本节描述如何为动态 PAT（隐藏）配置两次 NAT。有关详细信息，请参阅第 4-10 页上的动态 PAT。

准则

对于 PAT 池：

- 如果可用，真实源端口号将用于映射端口。然而，如果真实端口不可用，将默认从与真实端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，低于 1024 的端口仅拥有很小的可用 PAT 池。（8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)）如果您拥有的大量流量使用较低端口范围，则现可指定将要使用的无层次的端口范围，而不是三个不同大小的层：1024 至 65535，或 1 至 65535。
- 如在两个不同的规则中使用相同的 PAT 池对象，则请确保为每条规则指定相同的选项。例如，如果一条规则指定扩展 PAT 和无层次的范围，则另一条规则也必须指定扩展 PAT 和无层次的范围。

对于用于 PAT 池的扩展 PAT：

- 许多应用检测不支持扩展 PAT。有关不支持的检测的完整列表，请参阅第 7 章，“应用层协议检测入门”中的第 7-5 页上的默认检测和 NAT 限制。
- 如为动态 PAT 规则启用扩展 PAT，则无法也在不同的带有端口转换规则的静态 NAT 中使用 PAT 池中的地址作为 PAT 地址。例如，如果 PAT 池包括 10.1.1.1，则无法创建一个将 10.1.1.1 用作 PAT 地址的采用端口转换规则的静态 NAT。
- 如使用 PAT 池，并为回退指定接口，则无法指定扩展 PAT。
- 对于使用 ICE 或 TURN 的 VoIP 部署，请勿使用扩展 PAT。ICE 和 TURN 依赖于 PAT 绑定才能对所有目标均保持相同。

对于 PAT 池的轮询调度：

- 如果主机拥有现有连接，并且端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。**注意**：此“粘性”在故障转移后将不复存在。如果 ASA 进行故障转移，则来自某个主机的后续连接可能将不使用初始 IP 地址。
- 轮询调度可能会消耗大量的内存，在与扩展 PAT 组合使用时尤其如此。由于将为每一个映射协议 /IP 地址 / 端口范围创建 NAT 池，因此，轮询调度会导致大量并发 NAT 池，从而消耗内存。扩展 PAT 将导致甚至更多数量的并发 NAT 池。

详细步骤

	命令	用途
步骤 1	为以下地址创建网络对象或组： • 源真实地址 • 源映射地址 • 目标真实地址 • 目标映射地址	请参阅第 6-4 页上的为真实和映射地址添加网络对象。 如果想要转换所有源流量，则跳过为源真实地址添加对象，转而在 **nat** 命令中指定 **any** 关键字。 如果您想将接口地址用作映射地址，则可跳过为源映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。 如果想要配置仅带有端口转换的目标静态接口 NAT，则可跳过为目标映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。

	命令	用途
步骤 2	（可选）为以下端口创建服务对象： • 目标真实端口 • 目标映射端口	请参阅第 6-6 页上的（可选）为真实和映射端口添加服务对象。
步骤 3	**nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-auto** [*line*]}] **source dynamic** {*real-obj* | **any**} {*mapped_obj* [**interface** [**ipv6**]] | [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] [**interface** [**ipv6**]] | **interface** [**ipv6**]} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*] **示例：** `hostname(config)# nat (inside,outside) source dynamic MyInsNet interface destination static Server1 Server1 description Interface PAT for inside addresses when going to server 1`	配置**动态 PAT（隐藏）**。请参阅以下准则： • Interfaces -（透明模式必需）指定真实和映射接口。确保命令中包含圆括号。在路由模式下，如不指定真实和映射接口，则将使用所有接口；还可为一个或两个接口指定关键字 **any**。 • Section and Line -（可选）默认情况下，NAT 规则将添加至 NAT 表第 1 部分的末尾（请参阅第 4-18 页上的 NAT 规则顺序）。如果想要转而将规则添加至第 3 部分（位于网络对象 NAT 规则之后），则可使用 **after-auto** 关键字。借助于 *line* 参数，可将规则插入适用部分中的任何位置。 • 源地址： – Real - 指定网络对象、组或 **any** 关键字。如果想要转换从真实接口到映射接口的所有流量，请使用 **any** 关键字。 – Mapped - 配置以下其中一项： - 网络对象 - 指定包含主机地址的网络对象。 - **pat-pool** - 指定 **pat-pool** 关键字及包含多个地址的网络对象或组。 - **interface** -（仅路由模式）只指定 **interface** 关键字，以仅使用接口 PAT。如果指定 **ipv6**，则将使用接口的 IPv6 地址。通过 PAT 池或网络对象进行指定时，**interface** 关键字将启用接口 PAT 反馈。PAT IP 地址用尽后，接着将使用映射接口的 IP 地址。对于此选项，必须为 *mapped_ifc* 配置特定接口。 （续）

命令	用途
	（续） 对于 PAT 池，可以指定以下一个或多个选项： -- Round robin - **round-robin** 关键字可以为 PAT 池启用轮询调度地址分配。不使用轮询调度时，默认情况下，在使用下一个 PAT 地址前，将分配 PAT 地址的所有端口。轮询调度方法分配来自池中每个 PAT 地址的地址 / 端口，然后才返回再次使用第一个地址，然后是第二个地址，以此类推。 -- Extended PAT - **extended** 关键字可启用扩展 PAT。通过将目标地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按*服务*使用 65535 个端口。通常，创建 PAT 转换时，将不考虑目标端口和地址，因此，限定您按 PAT 地址使用 65535 个端口。例如，借助于扩展 PAT，可创建进入 192.168.1.7:23 时的 10.1.1.1:1027 转换，以及进入 192.168.1.7:80 时的 10.1.1.1:1027 转换。 -- Flat range - **flat** 关键字允许在分配端口时使用整个端口范围 1024 至 65535。为转换选择映射端口号时，ASA 将使用真实源端口号（如可用）。然而，如不使用此选项，则当真实端口*不*可用时，将默认从与真实端口号相同的端口范围选择映射端口：1 至 511、512 至 1023 以及 1024 至 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用整个范围 1 至 65535，请也指定 **include-reserve** 关键字。 • 目标地址（可选）： – Mapped - 指定网络对象或组，或对于仅带有端口转换的静态接口 NAT（路由模式），指定 **interface** 关键字。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如指定 **interface**，请务必也配置 **service** 关键字。对于此选项，必须为 *real_ifc* 配置特定接口。 有关详细信息，请参阅第 4-5 页上的带端口转换的静态接口 NAT。 – Real - 指定网络对象或组。对于标识 NAT，只需将相同的对象或组同时用于真实和映射地址。 • Destination port -（可选）指定 **service** 关键字以及真实和映射服务对象。对于标识端口转换，只需将相同的服务对象同时用于真实和映射端口。 • DNS -（可选；对于源专用规则）**dns** 关键字可转换 DNS 回复。确保启用 DNS 检测（默认情况下启用）。如配置 **destination** 地址，则无法配置 **dns** 关键字。有关详细信息，请参阅第 4-30 页上的 DNS 和 NAT。 • Unidirectional -（可选）请指定 **unidirectional**，以使目标地址无法发起流向源地址的流量。 • Inactive -（可选）要使该规则处于非活动状态，而无需移除此命令，请使用 **inactive** 关键字。要将其重新激活，请重新输入没有 **inactive** 关键字的整个命令。 • Description -（可选）使用 **description** 关键字提供最多 200 个字符的描述。

示例

以下示例为内部网络 192.168.1.0/24 配置访问外部 Telnet 服务器 209.165.201.23 时的接口 PAT，以及访问 203.0.113.0/24 网络上任何服务器时的使用 PAT 池的动态 PAT。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 209.165.201.23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface destination
static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

以下示例为内部网络 192.168.1.0/24 配置访问外部 IPv6 Telnet 服务器 2001:DB8::23 时的接口 PAT，以及访问 2001:DB8:AAAA::/96 网络上任何服务器时的使用 PAT 池的动态 PAT。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 2001:DB8::23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6 destination
static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

配置静态 NAT 或带有端口转换的静态 NAT

本节描述如何使用两次 NAT 配置静态 NAT 规则。有关静态 NAT 的详细信息，请参阅第 4-3 页上的静态 NAT。

详细步骤

	命令	用途
步骤 1	为以下地址创建网络对象或组： • 源真实地址 • 源映射地址 • 目标真实地址 • 目标映射地址	请参阅第 6-4 页上的为真实和映射地址添加网络对象。 如果想要配置仅带有端口转换的源静态接口 NAT，则可跳过为源映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。 如果想要配置仅带有端口转换的目标静态接口 NAT，则可跳过为目标映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。
步骤 2	（可选）为以下端口创建服务对象： • 源*或*目标真实端口 • 源*或*目标映射端口	请参阅第 6-6 页上的（可选）为真实和映射端口添加服务对象。

命令	用途
步骤 3 **nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-object** [*line*]}] **source static** *real_ob* [*mapped_obj* | **interface** [**ipv6**]] [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj*] [**net-to-net**] [**dns**] [**unidirectional** | **no-proxy-arp**] [**inactive**] [**description** *desc*] **示例：** `hostname(config)# nat (inside,dmz) source static MyInsNet MyInsNet_mapped destination static Server1 Server1 service REAL_SRC_SVC MAPPED_SRC_SVC`	配置**静态 NAT**。请参阅以下准则： • Interfaces -（透明模式必需）指定真实和映射接口。确保命令中包含圆括号。在路由模式下，如不指定真实和映射接口，则将使用所有接口；还可为一个或两个接口指定关键字 **any**。 • Section and Line -（可选）默认情况下，NAT 规则将添加至 NAT 表第 1 部分的末尾。请参阅第 4-18 页上的 NAT 规则顺序，了解有关这些小节的详细信息。如果想要转而将规则添加至第 3 部分（位于网络对象 NAT 规则之后），则可使用 **after-auto** 关键字。借助于 *line* 参数，可将规则插入适用部分中的任何位置。 • 源地址： – Real - 指定网络对象或组。 – Mapped - 指定不同的网络对象或组。对于仅带有端口转换的静态接口 NAT，可指定 **interface** 关键字（仅路由模式）。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如果指定 **interface**，请务必也配置 **service** 关键字（在此情况下，服务对象应仅包括源端口）。对于此选项，必须为 *mapped_ifc* 配置特定接口。有关详细信息，请参阅第 4-5 页上的带端口转换的静态接口 NAT。 • 目标地址（可选）： – Mapped - 指定网络对象或组，或对于仅带有端口转换的静态接口 NAT，指定 **interface** 关键字。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如果指定 **interface**，务必也配置 **service** 关键字（在此情况下，服务对象应仅包括目标端口）。对于此选项，必须为 *real_ifc* 配置特定接口。 – Real - 指定网络对象或组。对于标识 NAT，只需将相同的对象或组同时用于真实和映射地址。

命令	用途
	（续） • Ports -（可选）指定 **service** 关键字以及真实和映射服务对象。对于源端口转换，对象必须指定源服务。对于源端口转换，命令中服务对象的顺序为 **service** *real_obj mapped_obj*。对于目标端口转换，对象必须指定目标服务。对于目标端口转换，服务对象的顺序为 **service** *mapped_obj real_obj*。在极少数的情况下，您会在对象中同时指定源和目标端口，第一个服务对象包含真实源端口 / 映射目标端口；第二个服务对象包含映射源端口 / 真实目标端口。对于标识端口转换，只需将相同的服务对象同时用于真实和映射端口（源和 / 或目标端口，具体取决于您的配置）。 • Net-to-net -（可选）对于 NAT 46，指定 **net-to-net** 以便将第一个 IPv4 地址转换为第一个 IPv6 地址，将第二个 IPv4 地址转换为第二个 IPv6 地址，以此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此关键字。 • DNS -（可选；对于源专用规则）**dns** 关键字可转换 DNS 回复。确保启用 DNS 检测（默认情况下启用）。如配置 **destination** 地址，则无法配置 **dns** 关键字。有关详细信息，请参阅第 4-30 页上的 DNS 和 NAT。 • Unidirectional -（可选）请指定 **unidirectional**，以使目标地址无法发起流向源地址的流量。 • No Proxy ARP -（可选）指定 **no-proxy-arp**，以便为流向映射 IP 地址的传入数据包禁用代理 ARP。有关详细信息，请参阅第 4-20 页上的映射地址和路由。 • Inactive -（可选）要使该规则处于非活动状态，而无需移除此命令，请使用 **inactive** 关键字。要将其重新激活，请重新输入没有 **inactive** 关键字的整个命令。 • Description -（可选）使用 **description** 关键字提供最多 200 个字符的描述。

示例

以下示例展示带有端口转换的静态接口 NAT 的用途。外部主机通过目标端口 65000 至 65004 连接至外部接口 IP 地址，从而访问内部 FTP 服务器。流量通过 :65004 未经转换地发送至位于 192.168.10.100:6500 的内部 FTP 服务器。请注意，因为您想要转换命令中确定的源地址和端口，您会在服务对象中指定源端口范围（不指定目标端口）；目标端口为 “any”。因为静态 NAT 是双向的，“source” 和 “destination” 主要是指命令关键字；数据包中实际的源和目标地址与端口决于是哪一个主机发送数据包。在此示例中，连接源自外部，通向内部，因此，FTP 服务器的 “ 源 ” 地址和端口实际是源数据包中的目标地址和端口。

```
hostname(config)# object service FTP_PASV_PORT_RANGE
hostname(config-service-object)# service tcp source range 65000 65004

hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100

hostname(config)# nat (inside,outside) source static HOST_FTP_SERVER interface service
FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

以下示例展示了，访问 IPv6 网络时的一个 IPv6 网络至另一个 IPv6 网络的静态转换，以及访问 IPv4 网络时的至 IPv4 PAT 池的动态 PAT 转换。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:BBBB::/96

hostname(config)# object network OUTSIDE_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:CCCC::/96

hostname(config)# object network OUTSIDE_IPv4_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_IPv4_POOL
hostname(config-network-object)# range 10.1.2.1 10.1.2.254

hostname(config)# nat (inside,outside) source static INSIDE_NW MAPPED_IPv6_NW destination
static OUTSIDE_IPv6_NW OUTSIDE_IPv6_NW
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool MAPPED_IPv4_POOL
destination static OUTSIDE_IPv4_NW OUTSIDE_IPv4_NW
```

配置身份标识 NAT

本节描述如何使用两次 NAT 配置标识 NAT 规则。有关标识 NAT 的详细信息，请参阅第 4-11 页上的身份标识 NAT。

详细步骤

	命令	用途
步骤 1	为以下地址创建网络对象或组： • 源真实地址（您通常会将相同的对象用于源映射地址） • 目标真实地址 • 目标映射地址	请参阅第 6-4 页上的为真实和映射地址添加网络对象。 如果想要为所有地址执行标识 NAT，则可跳过为源真实地址创建对象，转而在 **nat** 命令中使用关键字 **any any**。 如果想要配置仅带有端口转换的目标静态接口 NAT，则可跳过为目标映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。
步骤 2	（可选）为以下端口创建服务对象： • 源*或*目标真实端口 • 源*或*目标映射端口	请参阅第 6-6 页上的（可选）为真实和映射端口添加服务对象。

命令	用途
步骤 3 **nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-object** [*line*]}] **source static** {*nw_obj nw_obj* | **any any**} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj*] [**no-proxy-arp**] [**route-lookup**] [**inactive**] [**description** *desc*] **示例：** hostname(config)# nat (inside,outside) source static MyInsNet MyInsNet destination static Server1 Server1	配置**标识 NAT**。请参阅以下准则： • Interfaces -（透明模式必需）指定真实和映射接口。确保命令中包含圆括号。在路由模式下，如不指定真实和映射接口，则将使用所有接口；还可为一个或两个接口指定关键字 **any**。 • Section and Line -（可选）默认情况下，NAT 规则将添加至 NAT 表第 1 部分的末尾。请参阅第 4-18 页上的 NAT 规则顺序，了解有关这些小节的详细信息。如果想要转而将规则添加至第 3 部分（位于网络对象 NAT 规则之后），则可使用 **after-auto** 关键字。借助于 *line* 参数，可将规则插入适用部分中的任何位置。 • Source addresses - 同时为真实和映射地址指定网络对象、组或 **any** 关键字。 • 目标地址（可选）： – Mapped - 指定网络对象或组，或者，对于仅带有端口转换的静态接口 NAT，指定 **interface** 关键字（仅路由模式）。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如果指定 **interface**，务必也配置 **service** 关键字（在此情况下，服务对象应仅包括目标端口）。对于此选项，必须为 *real_ifc* 配置特定接口。有关详细信息，请参阅第 4-5 页上的带端口转换的静态接口 NAT。 – Real - 指定网络对象或组。对于标识 NAT，只需将相同的对象或组同时用于真实和映射地址。 • Port -（可选）指定 **service** 关键字以及真实和映射服务对象。对于源端口转换，对象必须指定源服务。对于源端口转换，命令中服务对象的顺序为 **service** *real_obj mapped_obj*。对于目标端口转换，对象必须指定目标服务。对于目标端口转换，服务对象的顺序为 **service** *mapped_obj real_obj*。在极少数的情况下，您会在对象中同时指定源和目标端口，第一个服务对象包含真实源端口 / 映射目标端口；第二个服务对象包含映射源端口 / 真实目标端口。对于标识端口转换，只需将相同的服务对象同时用于真实和映射端口（源和 / 或目标端口，具体取决于您的配置）。 • No Proxy ARP -（可选）指定 **no-proxy-arp**，以便为流向映射 IP 地址的传入数据包禁用代理 ARP。有关详细信息，请参阅第 4-20 页上的映射地址和路由。 • Route lookup -（可选；仅路由模式；指定接口）指定 **route-lookup**，以便使用路由查找而不是 NAT 命令中指定的接口来确定出口接口。有关详细信息，请参阅第 4-23 页上的确定出口接口。 • Inactive -（可选）要使该规则处于非活动状态，而无需移除此命令，请使用 **inactive** 关键字。要将其重新激活，请重新输入没有 **inactive** 关键字的整个命令。 • Description -（可选）使用 **description** 关键字提供最多 200 个字符的描述。

配置每会话 PAT 规则

默认情况下，所有 TCP PAT 流量和所有 UDP DNS 流量均使用每会话 PAT。要将多会话 PAT 用于流量，可配置每会话 PAT 规则：一条允许规则使用每会话 PAT，一条拒绝规则使用多会话 PAT。有关每会话 PAT 和 多会话 PAT 的详细信息，请参阅第 4-10 页上的每会话 PAT 与多会话 PAT。

详细步骤

要配置每会话 PAT 规则，请参阅第 5-13 页上的配置每会话 PAT 规则。

监控两次 NAT

要监控两次 NAT，请输入以下命令之一：

命令	用途
show nat	显示 NAT 统计信息，包括每条 NAT 规则的命中信息。
show nat pool	显示 NAT 池统计信息，包括已分配的地址和端口，及其分配次数。
show xlate	显示当前 NAT 会话信息。
show nat divert-table	所有 NAT 规则均将在 NAT 转移表中生成条目。如果在匹配的规则上，NAT 转移字段设置为 ignore=yes NAT，则 ASA 将停止查找，并根据目标 IP 执行路由查找，以确定出口接口。如果在匹配的规则上，NAT 转移字段设置为 ignore=no，则将根据找到的 input_ifc 和 output_ifc 遍历 NAT 表，并执行必要的转换。出口接口将为 output_ifc。

两次 NAT 的配置示例

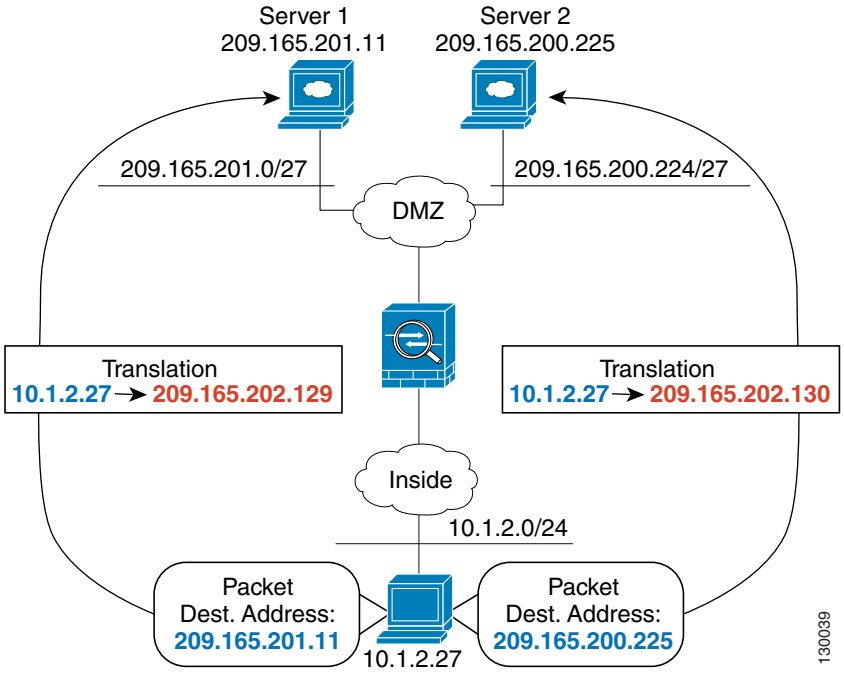
本节包括以下配置示例：

- 第 6-20 页上的取决于目标的不同转换（动态 PAT）
- 第 6-21 页上的取决于目标地址和端口的不同转换（动态 PAT）

取决于目标的不同转换（动态 PAT）

图 6-1 展示了 10.1.2.0/24 网络上的主机访问两个不同的服务器。当主机访问处于 209.165.201.11 的服务器时，真实地址将转换为 209.165.202.129:*port*。当主机访问处于 209.165.200.225 的服务器时，真实地址将转换为 209.165.202.130:*port*。

图 6-1　使用不同目标地址的两次 NAT



步骤 1　为内部网络添加网络对象：

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

步骤 2　为 DMZ 网络 1 添加网络对象：

```
hostname(config)# object network DMZnetwork1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224
```

步骤 3　为 PAT 地址添加网络对象：

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

步骤 4　配置第一条两次 NAT 规则：

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1 destination
static DMZnetwork1 DMZnetwork1
```

由于您不想转换目标地址，因此，需要为其配置标识 NAT，只需为真实和映射目标地址指定相同的地址。

默认情况下，NAT 规则将添加至 NAT 表第 1 部分的末尾，请参阅第 6-10 页上的配置动态 PAT（隐藏）了解有关如何为 NAT 规则指定部分和行号的详细信息。

步骤 5　为 DMZ 网络 2 添加网络对象：

```
hostname(config)# object network DMZnetwork2
hostname(config-network-object)# subnet 209.165.200.224 255.255.255.224
```

步骤 6　为 PAT 地址添加网络对象：

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

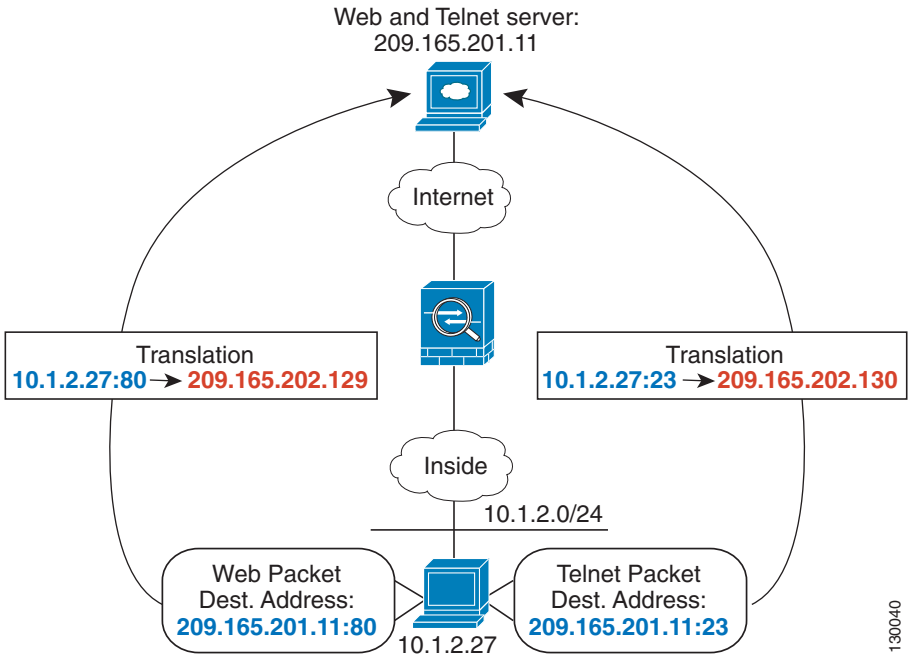
步骤 7　配置第二条两次 NAT 规则：

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2 destination
static DMZnetwork2 DMZnetwork2
```

取决于目标地址和端口的不同转换（动态 PAT）

图 6-2 展示了源和目标端口的使用。10.1.2.0/24 网络上的主机同时因为网络服务和 Telnet 服务访问单个主机。当主机因为 Telnet 服务访问服务器时，真实地址将转换为 209.165.202.129:*port*。当主机因为网络服务访问相同服务器时，真实地址将转换为 209.165.202.130:*port*。

图 6-2　使用不同目标端口的两次 NAT



步骤 1　为内部网络添加网络对象：

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

步骤 2　为 Telnet/ 网络服务器添加网络对象：

```
hostname(config)# object network TelnetWebServer
hostname(config-network-object)# host 209.165.201.11
```

步骤 3　使用 Telnet 时为 PAT 地址添加网络对象：

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

步骤 4　为 Telnet 添加服务对象：

```
hostname(config)# object service TelnetObj
hostname(config-network-object)# service tcp destination eq telnet
```

步骤 5　配置第一条两次 NAT 规则：

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
```

由于您不想要转换目标地址或端口，因此需要为其配置标识 NAT，只需为真实和映射目标地址指定相同的地址，为真实和映射服务指定相同的端口。

默认情况下，NAT 规则将添加至 NAT 表第 1 部分的末尾，请参阅第 6-10 页上的配置动态 PAT（隐藏）了解有关如何为 NAT 规则指定部分和行号的详细信息。

步骤 6　使用 HTTP 时为 PAT 地址添加网络对象：

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

步骤 7　为 HTTP 添加服务对象：

```
hostname(config)# object service HTTPObj
hostname(config-network-object)# service tcp destination eq http
```

步骤 8　配置第二条两次 NAT 规则：

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

两次 NAT 的功能历史记录

表 6-1 列出了各项功能变更以及实施了该变更的平台版本。

表 6-1　两次 NAT 的功能历史记录

功能名称	平台版本	功能信息
两次 NAT	8.3(1)	两次 NAT 可供您在单一规则中同时确定源和目标地址。 我们修改或引入了以下命令：**nat**、**show nat**、**show xlate**、**show nat pool**。

表 6-1　两次 NAT 的功能历史记录（续）

功能名称	平台版本	功能信息
身份标识 NAT 可配置代理 ARP 和路由查询	8.4(2)/8.5(1)	在身份标识 NAT 的更早版本中，代理 ARP 被禁用，路由查询始终用于确定出口接口。无法配置这些设置。在 8.4(2) 及更高版本中，身份标识 NAT 的默认行为已更改为匹配其他静态 NAT 配置的行为：在默认情况下，代理 ARP 已启用，并且 NAT 配置确定出口接口（如果已指定）。您可以原样保留这些设置，或者单独启用或禁用这些设置。请注意，现在您也可以为常规静态 NAT 禁用代理 ARP。 对于 8.3 之前版本的配置，NAT 免除规则（**nat 0 access-list** 命令）至 8.4(2) 及更高版本的迁移现包含以下关键字，以禁用代理 ARP 并使用路由查找：**no-proxy-arp** 和 **route-lookup**。用于迁移至 8.3(2) 和 8.4(1) 的 **unidirectional** 关键字不再用于迁移。从 8.3(1)、8.3(2) 和 8.4(1) 升级至 8.4(2) 时，所有标识 NAT 配置现包含 **no-proxy-arp** 和 **route-lookup** 关键字，以便维持现有功能。**unidirectional** 关键字已移除。 我们修改了以下命令：**nat source static** [**no-proxy-arp**] [**route-lookup**]。
PAT 池和轮询调度地址分配	8.4(2)/8.5(1)	现在，您可以指定 PAT 地址池，而不是单一地址。或者还可以启用 PAT 地址的轮询调度分配，而不是先使用 PAT 地址上的所有端口，然后再使用池中的下一个地址。这些功能有助于防止来自单一 PAT 地址的大量连接显示为 DoS 攻击的一部分，并使大量 PAT 地址的配置过程变轻松。 我们修改了以下命令：**nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]]。
轮询调度 PAT 池分配使用现有主机的相同 IP 地址	8.4(3)	组合使用 PAT 池与轮询调度分配时，如果主机拥有现有连接，且有端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。 我们未修改任何命令。 *此功能在 8.5(1) 或 8.6(1) 中不可用。*
用于 PAT 池的无层次的 PAT 端口范围	8.4(3)	如果可用，真实源端口号将用于映射端口。然而，如果真实端口*不*可用，将默认从与真实端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，1024 以下的端口只有一个小 PAT 池。 如您拥有的大量流量使用较低端口范围，在使用 PAT 池时，现可指定将要使用的无层次的端口范围，而不是三个不同大小的层：1024 至 65535，或 1 至 65535。 我们修改了以下命令：**nat source dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]]。 *此功能在 8.5(1) 或 8.6(1) 中不可用。*

表 6-1　两次 NAT 的功能历史记录（续）

功能名称	平台版本	功能信息
用于 PAT 池的扩展 PAT	8.4(3)	每个 PAT IP 地址允许最多 65535 个端口。如果 65535 个端口不能提供足够的转换，则现可启用适合 PAT 池的扩展 PAT。通过将目标地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按*服务*使用 65535 个端口。 我们修改了以下命令：**nat source dynamic** [**pat-pool** *mapped_object* [**extended**]]。 *此功能在 8.5(1) 或 8.6(1) 中不可用。*
自动 NAT 规则，这些规则可以将 VPN 对等设备的本地 IP 地址转换回对等设备的真实 IP 地址	8.4(3)	在极少数情况下，您可能想要使用 VPN 对等设备在内部网络上的真实 IP 地址，而非已分配的本地 IP 地址。通常在使用 VPN 的情况下，会给定对等体分配的本地 IP 地址来访问内部网络。但是，在例如内部服务器和网络安全基于对等体的真实 IP 地址的情况下，可能要将本地 IP 地址重新转换为对等体的真实公有 IP 地址。 可以在每个隧道组一个接口的基础上启用此功能。当 VPN 会话已建立或断开连接时，动态添加或删除对象 NAT 规则。可使用 **show nat** 命令查看这些规则。 **注**　由于路由问题，我们不建议使用此功能，除非您知道您需要此功能；请联系思科 TAC 确认网络的功能兼容性。请参阅以下限制： • 仅支持 Cisco IPsec 和 AnyConnect Client。 • 流向公共 IP 地址的返回流量必须路由回 ASA，因此，可应用 NAT 策略和 VPN 策略。 • 不支持负载平衡（由于路由问题）。 • 不支持漫游（公共 IP 更改）。 我们引入了以下命令：**nat-assigned-to-public-ip** *interface*（tunnel-group general-attributes 配置模式）。
对 IPv6 的 NAT 支持	9.0(1)	NAT 现在支持 IPv6 流量，以及 IPv4 和 IPv6 之间的转换。在透明模式下，不支持 IPv4 和 IPv6 之间的转换。 我们修改了以下命令：**nat**（全局配置模式）、**show nat**、 **show nat pool**、**show xlate**。
反向 DNS 查找的 NAT 支持	9.0(1)	在为 NAT 规则启用了 DNS 检测的情况下使用 IPv4 NAT、IPv6 NAT 和 NAT64 时，NAT 现支持为反向 DNS 查找转换 DNS PTR 记录。

表 6-1　两次 NAT 的功能历史记录（续）

功能名称	平台版本	功能信息
每会话 PAT	9.0(1)	每会话 PAT 功能可以提高 PAT 的可扩展性，而且对于集群，允许每个成员单元拥有自己的 PAT 连接；多会话 PAT 连接必须转发到主单元并归主单元所有。每会话 PAT 会话结束时，ASA 将发送重置，并立即移除转换。此重置将导致结束节点立即释放连接，从而避免 TIME_WAIT 状态。另一方面，多会话 PAT 使用 PAT 超时，默认情况下为 30 秒。对于“游击”流量，如 HTTP 或 HTTPS，每会话功能可以显著提高一个地址支持的连接速率。在不使用每会话功能的情况下，对于 IP 协议，一个地址的最大连接速率约为每秒 2000。在使用每会话功能的情况下，对于 IP 协议，一个地址的连接速率为 65535/*average-lifetime*。 默认情况下，所有 TCP 流量和 UDP DNS 流量均使用每会话 PAT 转换。对于需要多会话 PAT 的流量，如 H.323、SIP 或 Skinny，可通过创建每会话拒绝规则来禁用每会话 PAT。 我们引入了以下命令：**xlate per-session**、**show nat pool**。
NAT 规则引擎上的事务提交模型	9.3(1)	启用时，NAT 规则更新将在规则编译完成后应用，而不影响规则匹配性能。 我们已将 **nat** 关键字添加至以下命令：**asp rule-engine transactional-commit**、**show running-config asp rule-engine transactional-commit**、**clear configure asp rule-engine transactional-commit**。

第 3 部分

应用检查

应用层协议检测入门

以下主题介绍如何配置应用层协议检测。

- 第 7-1 页上的应用层协议检测
- 第 7-4 页上的应用检测准则
- 第 7-5 页上的应用检测的默认操作
- 第 7-9 页上的配置应用层协议检测
- 第 7-13 页上的配置正则表达式
- 第 7-16 页上的应用检测历史记录

应用层协议检测

对于在用户数据包嵌入 IP 寻址信息的服务或在动态分配端口上打开辅助信道的服务，需要使用检测引擎。这些协议需要 ASA 执行深度数据包检测，而不是通过快速路径传递数据包（有关快速路径的详细信息，请参阅常规操作配置指南）。因此，检测引擎可能会影响整体吞吐量。ASA 默认启用几个常见检测引擎，但可能需要根据网络启用其他检测引擎。

以下主题详细说明应用检测。

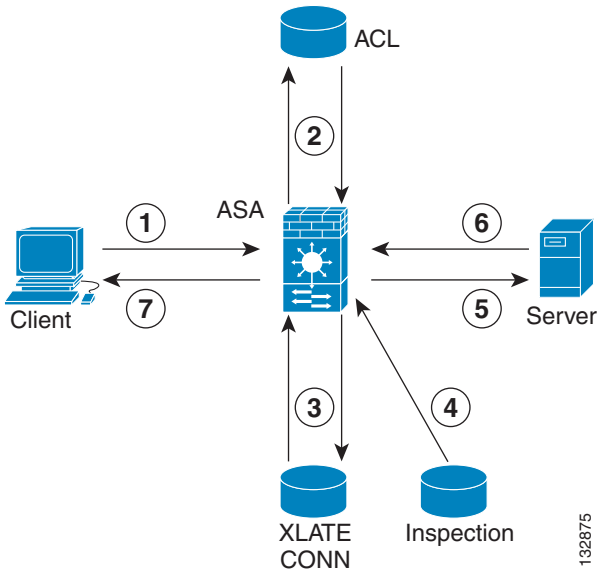
- 第 7-1 页上的检测引擎如何工作
- 第 7-2 页上的何时使用应用协议检测
- 第 7-3 页上的检测策略映射

检测引擎如何工作

如下图所示，ASA 使用三个数据库来执行基本操作：

- ACL - 用于对基于特定网络、主机和服务（TCP/UDP 端口号）的连接进行身份验证和授权。
- 检测 - 包含一组应用级别的预定义的静态检测功能。
- 连接（XLATE 和 CONN 表）- 维护关于每个已建立连接的状态和其他信息。自适应安全算法和直通代理使用这些信息在已建立的会话中高效地转发流量。

图 7-1　　检测引擎如何工作



在此图中，操作按发生的顺序进行编号：

1. TCP SYN 数据包到达 ASA 以建立新连接。
2. ASA 检查 ACL 数据库以确定是否允许连接。
3. ASA 在连接数据库（XLATE 和 CONN 表）中创建新条目。
4. ASA 检查测数据库，以确定连接是否需要应用级别检测。
5. 在应用检测引擎对数据包完成所有需要的操作后，ASA 将数据包转发到目标系统。
6. 目标系统响应初始请求。
7. ASA 接收应答数据包，在连接数据库中查找连接，并转发数据包，因为数据包属于已建立的会话。

ASA 的默认配置包括一组应用检测条目，这些条目将受支持的协议与特定 TCP 或 UDP 端口号关联并识别所需的任何特殊处理。

何时使用应用协议检测

当用户建立连接时，ASA 会根据 ACL 检查数据包，创建地址转换，并在快速路径中创建会话条目，以便后续数据包可以绕过耗时的检查。但是，快速路径依赖于可预测的端口号，且不在数据包内执行地址转换。

许多协议开放辅助 TCP 或 UDP 端口。已知端口上的初始会话用于协商动态分配的端口号。

其他应用在需要匹配源地址的数据包中嵌入 IP 地址，源地址通常在通过 ASA 时进行转换。

如果使用类似的应用，需要启用应用检测。

如果对嵌入 IP 地址的服务启用应用检测，ASA 将会转换嵌入式地址，并更新受转换影响的所有校验和或其他字段。

如果对使用动态分配的端口的服务启用应用检测，ASA 将会监控会话，识别动态端口分配，并允许特定会话期间在这些端口上进行数据交换。

检测策略映射

可以使用*检测策略映射*为许多应用检测配置特殊操作。这些映射是可选的：无需配置映射，就可以为支持检测策略映射的协议启用检测。仅在需要执行非默认检测操作的情况下，才需要这些映射。

有关支持检测策略映射的应用列表，请参阅第 7-9 页上的配置应用层协议检测。

检测策略映射由下列一个或多个要素组成： 检测策略映射的确切可用选项视应用而定。

- 流量匹配条件 - 将应用流量与特定于应用的条件进行匹配（例如 URL 字符串，随后可以对这些条件启用操作）。

  对于某些流量匹配条件，可使用正则表达式来匹配数据包中的文本。请务必在配置策略映射之前，在正则表达式类映射中单独或集中创建和测试正则表达式。

- 检测类映射 - 某些检测策略映射可以实现使用检测类映射包含多个流量匹配条件。然后，可以在检测策略映射中识别检测类映射，并整体启用用于类的操作。创建类映射和直接在检测策略映射中定义流量匹配的差别在于，您可以创建更复杂的匹配条件和重用类映射。然而，您无法为不同的匹配设置不同操作。
- 参数 - 参数会影响检测引擎的行为。

以下主题提供了有关详细信息：

- 第 7-3 页上的替换使用中的检测策略映射
- 第 7-3 页上的如何处理多个流量类

替换使用中的检测策略映射

如果需要替换已在服务策略中使用的检测策略映射，可使用以下方法：

- 所有检测策略映射 - 如果要将使用中的检测策略映射替换为不同的映射名称，必须移除 **inspect** *protocol map* 命令，并将其与新映射一起重新添加回去。例如：

```
hostname(config)# policy-map test
hostname(config-pmap)# class sip
hostname(config-pmap-c)# no inspect sip sip-map1
hostname(config-pmap-c)# inspect sip sip-map2
```

- HTTP 检测策略映射 - 如果修改了使用中的 HTTP 检测策略映射 (**policy-map type inspect http**)，必须移除并重新应用 **inspect http** *map* 操作，所做的更改才会生效。例如，如果修改了“http-map” 检测策略映射，必须从第 3/4 层策略移除再重新添加 **inspect http http-map** 命令：

```
hostname(config)# policy-map test
hostname(config-pmap)# class http
hostname(config-pmap-c)# no inspect http http-map
hostname(config-pmap-c)# inspect http http-map
```

如何处理多个流量类

在检测策略映射中可以指定多个检测类映射或直接匹配。

如果数据包匹配多个不同的 **match** 或 **class** 命令，ASA 应用操作的顺序将由内部 ASA 规则决定，而不是由向检测策略映射添加的顺序决定。内部规则由应用类型和分解数据包的逻辑进展确定，并且不可由用户配置。例如，对于 HTTP 流量，解析 Request Method 字段优先于解析 Header Host Length 字段； Request Method 字段的操作早于 Header Host Length 字段的操作。例如，以下匹配命令可以按任意顺序输入，但首先匹配的是 **match request method get** 命令。

```
match request header host length gt 100
  reset
match request method get
  log
```

如果操作丢弃数据包，在检测策略映射中将不会执行进一步操作。例如，如果第一个操作是重置连接，将不会匹配任何进一步的匹配条件。如果第一个操作是记录数据包，则会发生第二个操作，例如，重置连接。

如果数据包匹配多个相同的 **match** 或 **class** 命令，它们将会按照在策略映射中出现的顺序进行匹配。例如，对于报头长度为 1001 的数据包，将会首先匹配下面的第一个命令，进行相关记录，然后匹配第二个命令并重置。如果对调两个 **match** 命令的顺序，数据包将被丢弃且连接将被重置，然后才能匹配第二个 **match** 命令；数据包不再会被记录下来。

```
match request header length gt 100
  log
match request header length gt 1000
  reset
```

会根据类映射中的最低优先级 **match** 命令（优先级基于内部规则）来确定某类映射是与另一类映射同类型还是 **match** 命令。如果某个类映射与另一个类映射有同一类型的最低优先级 **match** 命令，类映射将根据被添加到策略映射中采用的顺序被匹配。如果每个类映射的最低优先级匹配不同，将会首先匹配具有较高优先级 **match** 命令的类映射。例如，以下三个类映射包含两种类型的 **match** 命令：**match request-cmd**（较高优先级）和 **match filename**（较低优先级）。ftp3 类映射包含这两个命令，但它根据最低优先级命令 **match filename** 进行排序。ftp1 类映射包含最高优先级的命令，因此，不管在策略映射中的顺序如何，都会首先对它进行匹配。ftp3 类映射的排列优先级和 ftp2 类映射相同，ftp2 类映射也含有 **match filename** 命令。ftp3 和 ftp2 类映根据在策略映射中的顺序被匹配：首先匹配 ftp3，然后匹配 ftp2。

```
class-map type inspect ftp match-all ftp1
  match request-cmd get
class-map type inspect ftp match-all ftp2
  match filename regex abc
class-map type inspect ftp match-all ftp3
  match request-cmd get
  match filename regex abc

policy-map type inspect ftp ftp
  class ftp3
    log
  class ftp2
    log
  class ftp1
    log
```

应用检测准则

故障转移准则

需要检测的多媒体会话的状态信息不通过用于状态故障转移的状态链路进行传递。但 GTP 和 SIP 是例外，它们在状态链路上复制。

IPv6 准则

以下检测中支持 IPv6：

- DNS
- FTP

- HTTP
- ICMP
- SCCP（瘦客户端）
- SIP
- SMTP
- IPsec 穿透
- IPv6

以下检测中支持 NAT64：

- DNS
- FTP
- HTTP
- ICMP

附加准则和限制

- 某些检测引擎不支持 PAT、NAT、外部 NAT 或相同安全接口之间的 NAT。有关 NAT 支持的详细信息，请参阅第 7-5 页上的默认检测和 NAT 限制。
- 对于所有应用检测，ASA 将同时活动的数据连接数限制为 200。例如，如果 FTP 客户端打开多个辅助连接，FTP 检测引擎只允许 200 个活动连接，第 201 个连接将被丢弃，并且自适应安全设备将生成系统错误消息。
- 检测的协议受制于高级 TCP 状态跟踪，这些连接的 TCP 状态不会自动复制。如果这些连接复制到备用设备，将会尽力尝试重新建立 TCP 状态。
- 默认情况下，会检测流向 ASA（到接口）的 TCP/UDP 流量。但是，即使启用 ICMP 检测，也不会检测流向接口的 ICMP 流量。因此，到接口的 ping（回应请求）可能会在特定情况下失败，例如，如果回应请求来自 ASA 可以通过备用默认路由到达的源。

应用检测的默认操作

以下主题介绍应用检测的默认操作。

- 第 7-5 页上的默认检测和 NAT 限制
- 第 7-8 页上的默认检测策略映射

默认检测和 NAT 限制

默认情况下，配置包括会匹配所有默认应用检测流量并对所有接口的流量应用检测的策略（全局策略）。默认应用检测流量包括流向各个协议的默认端口的流量。只能应用一个全局策略，因此，如果要改变全局策略（例如，要对非标准端口应用检测，或者要添加默认情况下未启用的检测），需要编辑默认策略或者禁用默认策略并应用新策略。

下表列出了所有支持的检测、用于默认类映射的默认端口和默认打开的检测引擎（以粗体显示）。该表中还对任何 NAT 限制作了备注。在该表中：

- 默认情况下为默认端口启用的检测引擎以粗体显示。
- ASA 符合指示的标准，但它不会对正接受检测的数据包执行合规性。例如，FTP 命令应该按照特定的顺序，但 ASA 不执行该顺序。

表 7-1　支持的应用检测引擎

应用	默认端口	NAT 限制	标准	备注
CTIQBE	TCP/2748	无扩展 PAT。 无 NAT64。 （集群）无静态 PAT。	—	—
DCERPC	TCP/135	无 NAT64。	—	—
使用 UDP 的 **DNS**	UDP/53	无可用于通过 WINS 进行名称解析的 NAT 支持。	RFC 1123	—
FTP	TCP/21	（集群）无静态 PAT。	RFC 959	—
GTP	UDP/3386 UDP/2123	无扩展 PAT。 无 NAT。	—	需要特殊许可证。
H.323 H.225 和 **RAS**	TCP/1720 UDP/1718 UDP (RAS) 1718 - 1719	无动态 NAT 或 PAT。 静态 PAT 可能不起作用。 （集群）无静态 PAT。 无扩展 PAT。 不支持对每个会话执行 PAT。 不支持对同类安全接口执行 NAT。 无 NAT64。	ITU-T H.323、H.245、H225.0、Q.931、Q.932	—
HTTP	TCP/80	—	RFC 2616	请注意，MTU 限制会去除 ActiveX 和 Java。如果 MTU 因为太小而不允许在数据包中包含 Java 或 ActiveX 标记，可能不会出现去除操作。
ICMP	—	—	—	不会检测流向 ASA 接口的 ICMP 流量。
ICMP 错误	—	—	—	—
ILS (LDAP)	TCP/389	无扩展 PAT。 无 NAT64。	—	—
即时消息 (IM)	因客户端而异	无扩展 PAT。 无 NAT64。	RFC 3860	—
IP 选项	—	无 NAT64。	RFC 791、RFC 2113	—
IPsec 穿透	UDP/500	无 PAT。 无 NAT64。	—	—
IPv6	—	无 NAT64。	RFC 2460	—
MGCP	UDP/2427、2727	无扩展 PAT。 无 NAT64。 （集群）无静态 PAT。	RFC 2705bis-05	—
MMP	TCP 5443	无扩展 PAT。 无 NAT64。	—	—

表 7-1　　支持的应用检测引擎（续）

应用	默认端口	NAT 限制	标准	备注
使用 IP 的 **NetBIOS 域名服务器**	UDP/137、138（源端口）	无扩展 PAT。 无 NAT64。	—	通过执行 NBNS UDP 端口 137 和 NBDS UDP 端口 138 的数据包 NAT 来支持 NetBIOS。
PPTP	TCP/1723	无 NAT64。 （集群）无静态 PAT。	RFC 2637	—
RADIUS 计费	1646	无 NAT64。	RFC 2865	—
RSH	TCP/514	无 PAT。 无 NAT64。 （集群）无静态 PAT。	Berkeley UNIX	—
RTSP	TCP/554	无扩展 PAT。 无 NAT64。 （集群）无静态 PAT。	RFC 2326、2327、1889	无 HTTP 掩蔽处理。
ScanSafe（云网络安全）	TCP/80 TCP/413	—	—	这些端口未包含在适用于 ScanSafe 检测的 default-inspection-traffic 类中。
SIP	TCP/5060 UDP/5060	不支持对同类安全接口执行 NAT。 无扩展 PAT。 不支持对每个会话执行 PAT。 无 NAT64 或 NAT46。 （集群）无静态 PAT。	RFC 2543	某些情况下不处理 TFTP 上传的思科 IP 电话配置。
瘦客户端 (SCCP)	TCP/2000	不支持对同类安全接口执行 NAT。 无扩展 PAT。 不支持对每个会话执行 PAT。 无 NAT64、NAT46 或 NAT66。 （集群）无静态 PAT。	—	某些情况下不处理 TFTP 上传的思科 IP 电话配置。
SMTP 和 **ESMTP**	TCP/25	无 NAT64。	RFC 821、1123	—
SNMP	UDP/161、162	无 NAT 或 PAT。	RFC 1155、1157、1212、1213、1215	v.2 RFC 1902 - 1908； v.3 RFC 2570 - 2580。
SQL*Net	TCP/1521	无扩展 PAT。 无 NAT64。 （集群）无静态 PAT。	—	v.1 和 v.2。
使用 UDP 和 TCP 的 Sun RPC	UDP/111	无扩展 PAT。 无 NAT64。	—	默认规则包括 UDP 端口 111；如果要对 TCP 端口 111 启用 Sun RPC 检测，需要创建匹配 TCP 端口 111 并执行 Sun RPC 检测的新规则。

表 7-1　支持的应用检测引擎（续）

应用	默认端口	NAT 限制	标准	备注
TFTP	UDP/69	无 NAT64。 （集群）无静态 PAT。	RFC 1350	不转换负载 IP 地址。
WAAS	TCP/1 - 65535	无扩展 PAT。 无 NAT64。	—	—
XDMCP	UDP/177	无扩展 PAT。 无 NAT64。 （集群）无静态 PAT。	—	—

默认策略配置包括以下命令：

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

默认检测策略映射

某些检测类型使用隐藏的默认策略映射。例如，如果启用 ESMTP 检测但不指定映射，将会使用 _default_esmtp_map。

说明每种检测类型的各节中介绍了默认检测。可以使用 **show running-config all policy-map** 命令 查看这些默认映射。

DNS 检测是唯一一种采用明确配置的默认映射 preset_dns_map 的检测。

配置应用层协议检测

应用检测在服务策略中进行配置。服务策略提供一致且灵活的方式来配置 ASA 功能。例如，您可以使用服务策略创建特定于某项 TCP 应用而非应用于所有 TCP 应用的超时配置。对于某些应用，可以在启用检测后执行特殊操作。关于服务策略的一般信息，请参阅第 1 章，“ 使用模块化策略框的服务策略 ”。

默认情况下，某些应用的检测已启用。有关详细信息，请参阅第 7-5 页上的默认检测和 NAT 限制。可按照本节所述的步骤修改检测策略。

操作步骤

步骤 1　确定要在第 3/4 层类映射中应用检测的流量是直通流量还是管理流量（如果是要向现有类映射添加检测，请忽略这一步）。

有关详细信息，请参阅第 1-12 页上的为直通流量创建第 3/4 层类映射和第 1-14 页上的 Create a Layer 3/4 Class Map for Management Traffic。第 3/4 层管理类映射仅可使用 RADIUS 计费检测。

所选的类映射有重要含义。只有 inspection_default 类可以有多项检测，而且可能需要简单地编辑应用检测默认操作的现有全局策略。有关选择哪种类映射的详细信息，请参阅第 7-12 页上的选择要检测的正确流量类。

步骤 2　（可选）某些检测引擎允许您在对流量应用检测时控制其他参数。下面的表显示了哪些协议允许检测策略映射，还提供了指向相关配置说明的链接。

步骤 3　添加或编辑第 3/4 层策略映射，以用于设置要对类映射流量执行的操作。

```
hostname(config)# policy-map name
hostname(config-pmap)#
```

默认策略映射称为 “global_policy”。第 7-5 页上的默认检测和 NAT 限制中列出了此策略映射包括的默认检测。如果要修改默认策略（例如，要添加或删除检测，或者要识别用于操作的其他类映射），请输入 **global_policy** 作为名称。

步骤 4　识别要向其分配操作的类映射。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

如果正在编辑默认策略映射，则默认策略映射包括 inspection_default 类映射。可以通过输入 **inspection_default** 作为名称来编辑用于该类的操作。要向此策略映射添加其他类映射，请识别不同的名称。

必要时可以将多个类映射整合在同一策略中，因此，可以创建一个类映射来匹配特定流量，创建另一个类映射来匹配不同流量。但是，如果流量匹配包含检测命令的某个类映射，然后匹配也包含检测命令的另一个类映射，将会仅使用第一个匹配的类。例如，SNMP 匹配 inspection_default 类映射。要启用 SNMP 检测，请启用默认类的 SNMP 检测。请勿添加另一个匹配 SNMP 的类。

步骤 5　启用应用检测。

```
hostname(config-pmap-c)# inspect protocol
```

protocol 是以下其中一个值：

表 7-2　　协议关键字

关键字	备注
ctiqbe	请参阅第 9-1 页上的 CTIQBE 检测。
dcerpc [*map_name*]	请参阅第 11-1 页上的 DCERPC 检测。 如果已按照第 11-2 页上的配置 DCERPC 检测策略映射中所述添加了 DCERPC 检测策略映射，请在此命令中识别映射名称。
dns [*map_name*] [**dynamic-filter-snoop**]	请参阅第 8-1 页上的 DNS 检测。 如果已按照第 8-3 页上的配置 DNS 检测策略映射中所述添加了 DNS 检测策略映射，请在此命令中识别映射名称。默认 DNS 检测策略映射名称为 “preset_dns_map”。 要启用适用于僵尸网络流量过滤器的 DNS 监听，请输入 **dynamic-filter-snoop** 关键字。
esmtp [*map_name*]	请参阅第 8-36 页上的 SMTP 检测和扩展 SMTP 检测。 如果已按照第 8-38 页上的配置 ESMTP 检测策略映射中所述添加了 ESMTP 检测策略映射，请在此命令中识别映射名称。
ftp [**strict** [*map_name*]]	请参阅第 8-8 页上的 FTP 检测。 使用 **strict** 关键字防止网络浏览器在 FTP 请求中发送嵌入式命令，从而提高受保护网络的安全。有关详细信息，请参阅第 8-8 页上的严格 FTP。 如果已按照第 8-9 页上的配置 FTP 检测策略映射中所述添加了 FTP 检测策略映射，请在此命令中识别映射名称。
gtp [*map_name*]	请参阅第 11-4 页上的 GTP 检测。 如果已按照第 11-6 页上的配置 GTP 检测策略映射中所述添加了 GTP 检测策略映射，请在此命令中识别映射名称。
h323 h225 [*map_name*]	请参阅第 9-3 页上的 H.323 检测。 如果已按照第 9-5 页上的配置 H.323 检测策略映射中所述添加了 H323 检测策略映射，请在此命令中识别映射名称。
h323 ras [*map_name*]	请参阅第 9-3 页上的 H.323 检测。 如果已按照第 9-5 页上的配置 H.323 检测策略映射中所述添加了 H323 检测策略映射，请在此命令中识别映射名称。
http [*map_name*]	请参阅第 8-13 页上的 HTTP 检测。 如果已按照第 8-14 页上的配置 HTTP 检测策略映射中所述添加了 HTTP 检测策略映射，请在此命令中识别映射名称。
icmp	请参阅第 8-19 页上的 ICMP 检测。

表 7-2　协议关键字

关键字	备注
icmp error	请参阅第 8-19 页上的 ICMP 错误检测。
ils	请参阅第 10-1 页上的 ILS 检测。
im [*map_name*]	请参阅第 8-20 页上的即时消息检测。 如果已按照第 8-20 页上的配置即时消息检测策略映射中所述添加了即时消息检测策略映射，请在此命令中识别映射名称。
ip-options [*map_name*]	请参阅第 8-24 页上的 IP 选项检测。 如果已按照第 8-25 页上的配置 IP 选项检测策略映射中所述添加了 IP 选项检测策略映射，请在此命令中识别映射名称。
ipsec-pass-thru [*map_name*]	请参阅第 8-27 页上的 IPsec 穿透检测。 如果已按照第 8-27 页上的 IPsec 穿透检测中所述添加了 IPsec 穿透检测策略映射，请在此命令中识别映射名称。
ipv6 [*map_name*]	请参阅第 8-30 页上的 IPv6 检测。 如果已按照第 8-31 页上的配置 IPv6 检测策略映射中所述添加了 IPv6 检测策略映射，请在此命令中识别映射名称。
mgcp [*map_name*]	请参阅第 9-11 页上的 MGCP 检测。 如果已按照第 9-13 页上的为其他检测控制配置 MGCP 检测策略映射中所述添加了 MGCP 检测策略映射，请在此命令中识别映射名称。
netbios [*map_name*]	请参阅第 8-34 页上的 NetBIOS 检测。 如果已按照第 8-34 页上的为其他检测控制配置 NetBIOS 检测策略映射中所述添加了 NetBIOS 检测策略映射，请在此命令中识别映射名称。
pptp	请参阅第 8-36 页上的 PPTP 检测。
radius-accounting *map_name*	请参阅第 11-11 页上的 RADIUS 计费检测。 **radius-accounting** 关键字仅适用于管理类映射。必须指定 RADIUS 计费检测策略映射；请参阅第 11-12 页上的配置 RADIUS 计费检测策略映射。
rsh	请参阅第 11-14 页上的 RSH 检测。
rtsp [*map_name*]	请参阅第 9-16 页上的 RTSP 检测。 如果已按照第 9-17 页上的配置 RTSP 检测策略映射中所述添加了 RTSP 检测策略映射，请在此命令中识别映射名称。
scansafe [*map_name*] [**fail-open** | **fail-closed**]	如果要启用 ScanSafe（云网络安全），请执行以下主题中介绍的操作步骤而不要执行此步骤：第 15-9 页上的配置服务策略，将流量发送到云网络安全。该操作步骤说明了全面策略配置，包括如何配置检测策略映射。

表 7-2　协议关键字

关键字	备注
sip [*map_name*] [**tls-proxy** *proxy_name*]	请参阅第 9-20 页上的 SIP 检测。 如果已按照第 9-23 页上的配置 SIP 检测策略映射中所述添加了 SIP 检测策略映射，请在此命令中识别映射名称。指定 TLS 代理以启用加密流量检测。
skinny [*map_name*] [**tls-proxy** *proxy_name*]	请参阅第 9-28 页上的瘦客户端 (SCCP) 检测。 如果已按照第 9-29 页上的为其他检测控制配置瘦客户端 (SCCP) 检测策略映射中所述添加了瘦客户端检测策略映射，请在此命令中识别映射名称。指定 TLS 代理以启用加密流量检测。
snmp [*map_name*]	请参阅第 11-14 页上的 SNMP 检测。 如果添加了 SNMP 检测策略映射，请在此命令中识别映射名称。
sqlnet	请参阅第 10-2 页上的 SQL*Net 检测。
sunrpc	请参阅第 10-3 页上的 Sun RPC 检测。 默认类组映射包括 UDP 端口 111；如果要对 TCP 端口 111 启用 Sun RPC 检测，需要创建匹配 TCP 端口 111 的新的类映射，将该类添加到策略，然后对该类应用 **inspect sunrpc** 命令。
tftp	请参阅第 8-42 页上的 TFTP 检测。
waas	启用 TCP 选项 33 解析。部署思科广域应用服务产品时使用。
xdmcp	请参阅第 11-16 页上的 XDMCP 检测。

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的检测策略映射，必须使用 **no inspect** *protocol* 命令移除旧的检测，然后为其提供新的检测策略映射名称并重新添加这项检测。

步骤 6　在一个或多个接口上激活策略映射，请输入以下命令：

```
hostname(config)# service-policy policymap_name {global | interface interface_name}
```

其中，**global** 将策略映射应用于所有接口，**interface** 将策略应用于一个接口。默认情况下，会全局应用默认策略映射 “global_policy”。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

选择要检测的正确流量类

直通流量的第 3/4 层默认类映射称为 “inspection_default”。此类使用特殊的 **match** 命令 **match default-inspection-traffic** 来匹配流量，以匹配每个应用协议的默认端口。此流量类（以及通常不用于检测的 **match any**）匹配支持 IPv6 检测的 IPv4 和 IPv6 流量。有关支持 IPv6 的检测的列表，请参阅第 7-4 页上的应用检测准则。

可以指定 **match access-list** 命令以及 **match default-inspection-traffic** 命令将流量匹配范围缩窄为特定 IP 地址。由于 **match default - inspection - traffic** 命令指定要匹配的端口，因此，将忽略 ACL 中的任何端口。

提示　我们建议您仅检测理应出现应用流量的端口上的流量；如果检测所有流量，例如，使用 **match any**，ASA 性能则将受到影响。

如果要匹配非标准端口，请创建适用于非标准端口的新的类映射。有关每个检测引擎的标准端口，请参阅第 7-5 页上的默认检测和 NAT 限制。必要时可以将多个类映射整合在同一策略中，因此，可以创建一个类映射来匹配特定流量，创建另一个类映射来匹配不同流量。但是，如果流量匹配包含检测命令的某个类映射，然后匹配也包含检测命令的另一个类映射，将会仅使用第一个匹配的类。例如，SNMP 匹配 inspection_default 类。要启用 SNMP 检测，请启用默认类的 SNMP 检测。请勿添加另一个匹配 SNMP 的类。

例如，要使用默认类映射将检测限制为针对从 10.1.1.0 - 192.168.1.0 的流量，请输入以下命令：

```
hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
hostname(config)# class-map inspection_default
hostname(config-cmap)# match access-list inspect
```

使用以下命令可查看整个类映射：

```
hostname(config-cmap)# show running-config class-map inspection_default
!
class-map inspection_default
 match default-inspection-traffic
 match access-list inspect
!
```

要检测端口 21 和 1056（非标准端口）上的 FTP 流量，请创建指定端口的 ACL，并将其分配给一个新的类映射：

```
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 21
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 1056
hostname(config)# class-map new_inspection
hostname(config-cmap)# match access-list ftp_inspect
```

配置正则表达式

正则表达式定义文本字符串的模式匹配。可以在某些协议检测映射中使用这些表达式根据字符串（例如，URL 或特定报头字段的内容）来匹配数据包。

- 第 7-13 页上的创建正则表达式
- 第 7-16 页上的创建正则表达式类映射

创建正则表达式

正则表达式可逐字地完全匹配文本字符串，或者，可以使用 *metacharacters* 来匹配文本字符串的多个变体。可以使用正则表达式匹配某些应用流量的内容，例如，可以匹配 HTTP 数据包中的 URL 字符串。

准备工作

使用 **Ctrl+V** 对 CLI 中的所有特殊字符进行转义，例如问号 (?) 或制表符。例如，键入 **d[Ctrl+V]?g** 将会在配置中输入 **d?g**。

有关将正则表达式与数据包进行匹配会造成的性能影响的信息，请参阅命令参考中的 **regex** 命令。一般来说，匹配长输入字符串或尝试匹配大量的正则表达式将会降低系统性能。

注　作为一种优化手段，ASA 会在进行了去模糊化处理的 URL 进行搜索。去模糊化处理将多个正斜杠 (/) 压缩为一个斜杠。对于通常使用双斜杠的字符串（例如 “http://”），请务必搜索 “http:/”。

下表列出了有特殊意义的元字符。

表 7-3　正则表达式元字符

字符	说明	备注
。	点	匹配任何单个字符。例如，**d.g** 匹配 dog、dag、dtg 以及任何含有这些字符的单词，如 doggonnit。
(*exp*)	子表达式	子表达式将字符与其周围的字符分隔开，从而可以在子表达式上使用其他元字符。例如，**d(o|a)g** 匹配 dog 和 dag，但是，**do|ag** 匹配 do 和 ag。子表达式还可以与重复限定符配合使用，以区分意味着重复的字符。例如，**ab(xy){3}z** 匹配 abxyxyxyz。
|	交替	匹配其分隔的任意一个表达式。例如，**dog|cat** 匹配 dog 或 cat。
?	问号	一个限定符，表示前面有 0 个或 1 个表达式。例如，**lo?se** 匹配 lse 或 lose。
*	星号	一个限定符，表示前面有 0 个、1 个或任意数量的表达式。例如，**lo*se** 匹配 lse、lose、loose 等等。
+	加号	一个限定符，表示前面至少有 1 个表达式。例如，**lo+se** 匹配 lose 和 loose，但不匹配 lse。
{*x*} 或 {*x*,}	最小重复限定符	至少重复 *x* 次。例如，**ab(xy){2,}z** 匹配 abxyxyz、abxyxyxyz 等等。
[*abc*]	字符类	匹配方括号中的任意字符。例如，**[abc]** 匹配 a、b 或 c。
[^*abc*]	求反字符类	匹配不包含在方括号中的单个字符。例如，**[^abc]** 匹配 a、b 或 c 以外的任意字符。**[^A-Z]** 匹配非大写形式的任意单个字符。
[*a-c*]	字符范围类	匹配范围内的任意字符。**[a-z]** 匹配任意小写字母。可以混合使用字符和字符范围：**[abcq-z]** 匹配 a、b、c、q、r、s、t、u、v、w、x、y 和 z，**[a-cq-z]** 也是匹配这些字符。 破折号 (-) 字符仅在是括号中的最后一个或第一个字符时，才是原义字符：例如，**[abc-]** 或 **[-abc]**。

表 7-3　　正则表达式元字符（续）

字符	说明	备注
“”	引号	保留字符串中的尾随空格或前导空格。例如，**“ test”** 在查找匹配时会保留前导空格。
^	脱字号	指定行首。
\	转义字符	当与元字符一起使用时，可以匹配原义字符。例如，**\[** 匹配左方括号。
char	字符	当字符不是元字符时，匹配原义字符。
\r	回车符	匹配回车符 0x0d。
\n	换行符	匹配换行符 0x0a。
\t	制表符	匹配制表符 0x09。
\f	换页符	匹配换页符 0x0c。
\x*NN*	转义的十六进制数字	匹配十六进制的 ASCII 字符（必须是两位数）。
NNN	转义的八进制数字	匹配八进制的 ASCII 字符（必须是三位数）。例如，字符 040 代表空格。

操作步骤

步骤 1　测试正则表达式，确保它匹配预期的内容。

```
hostname(config)# test regex input_text regular_expression
```

其中，*input_text* 参数是要使用正则表达式匹配的字符串，最多可包含 201 个字符。

regular_expression 参数最多可包含 100 个字符。

使用 **Ctrl+V** 对 CLI 中的所有特殊字符进行转义。例如，要在 **test regex** 命令的输入文本中输入制表符，必须输入 **test regex “test[Ctrl+V Tab]” “test\t”**。

如果正则表达式与输入文本相匹配，将显示以下消息：

```
INFO: Regular expression match succeeded.
```

如果正则表达式与输入文本不匹配，将显示以下消息：

```
INFO: Regular expression match failed.
```

步骤 2　要在测试正则表达式后添加正则表达式，请输入以下命令：

```
hostname(config)# regex name regular_expression
```

其中的 *name* 参数最多可包含 40 个字符。

regular_expression 参数最多可包含 100 个字符。

示例

以下示例创建两个用于检测策略映射的正则表达式：

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

创建正则表达式类映射

正则表达式类映射识别一个或多个正则表达式， 是正则表达式对象的集合。在很多情况下，可以使用正则表达式类映射代替正则表达式对象。

操作步骤

步骤 1　创建正则表达式类映射。

```
hostname(config)# class-map type regex match-any class_map_name
hostname(config-cmap)#
```

其中，*class_map_name* 是最多可包含 40 个字符的字符串。保留名称 “class-default”。所有类型的类映射都使用同一命名空间，因此，您无法重用已被另一类型的类映射使用的名称。

match-any 关键字指明如果流量至少匹配类映射中的一个正则表达式，那么它匹配类映射。

步骤 2　（可选）向类映射添加描述：

```
hostname(config-cmap)# description string
```

步骤 3　为每个正则表达式输入以下命令，以识别要包括的正则表达式：

```
hostname(config-cmap)# match regex regex_name
```

示例

以下示例创建两个正则表达式，并将其添加到正则表达式类映射。如果流量包含字符串 “example.com” 或 “example2.com”，那么它匹配类映射。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2
```

应用检测历史记录

功能名称	版本	说明
检测策略映射	7.2(1)	引入了检测策略映射。引入了以下命令：**class-map type inspect**。
正则表达式和策略映射	7.2(1)	引入了正则表达式和策略映射，在检测策略映射下使用。引入了以下命令：**class-map type regex**、**regex**、**match regex**。
检测策略映射的 match any 命令	8.0(2)	引入了关键字 **match any**，与检测策略映射一起使用：流量可以匹配一个或多个条件以匹配类映射。过去，仅 **match all** 命令可用。

基本互联网协议检测

以下主题介绍基本互联网协议的应用检测。有关为何需要对某些协议进行检测以及应用检测的总体方法的信息，请参阅第 7-1 页上的应用层协议检测入门。

- 第 8-1 页上的 DNS 检测
- 第 8-8 页上的 FTP 检测
- 第 8-13 页上的 HTTP 检测
- 第 8-19 页上的 ICMP 检测
- 第 8-19 页上的 ICMP 错误检测
- 第 8-20 页上的即时消息检测
- 第 8-24 页上的 IP 选项检测
- 第 8-27 页上的 IPsec 穿透检测
- 第 8-30 页上的 IPv6 检测
- 第 8-34 页上的 NetBIOS 检测
- 第 8-36 页上的 PPTP 检测
- 第 8-36 页上的 SMTP 检测和扩展 SMTP 检测
- 第 8-42 页上的 TFTP 检测

DNS 检测

以下各节介绍 DNS 应用检测。

- 第 8-2 页上的 DNS 检测操作
- 第 8-2 页上的 DNS 检测的默认设置
- 第 8-2 页上的配置 DNS 检测
- 第 8-7 页上的监控 DNS 检测

DNS 检测操作

默认情况下，DNS 检测已启用。可以自定义 DNS 检测来执行许多任务：

- 根据 NAT 配置转换 DNS 记录。有关详细信息，请参阅第 4-30 页上的 DNS 和 NAT。
- 强制消息长度、域名长度和标签长度。
- 如果在 DNS 消息中遇到压缩指针，应验证指针所引用的域名的完整性。
- 检查是否存在压缩指针循环。
- 根据 DNS 报头、类型、类别等检测数据包。

DNS 检测的默认设置

默认情况下，启用 DNS 检测，使用 preset_dns_map 检测类映射：

- 最大 DNS 消息长度为 512 字节。
- 最大客户端 DNS 消息长度是自动设置的，以匹配资源记录。
- DNS 保护已启用，这样，一旦 ASA 转发 DNS 应答，ASA 就会断开与 DNS 查询相关的 DNS 会话。另外，ASA 还监控消息交换，确保 DNS 回复 ID 匹配 DNS 查询 ID。
- 根据 NAT 配置的 DNS 记录转换已启用。
- 协议执行已启用，使得可以进行 DNS 消息格式检查（具体检查内容包括：域名长度不得超过 255 个字符，标签长度不得超过 63 个字符，压缩检查和循环指针检查）。

请参阅以下默认 DNS 检测命令：

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
!...
service-policy global_policy global
```

配置 DNS 检测

默认情况下，DNS 检测已启用。仅在需要非默认处理的情况下，才需要配置这项检测。如果要自定义 DNS 检测，请按照以下流程进行操作。

操作步骤

步骤 1　第 8-3 页上的配置 DNS 检测策略映射。

步骤 2　第 8-6 页上的配置 DNS 检测服务策略。

配置 DNS 检测策略映射

如果默认检测行为不能满足网络要求，可以创建 DNS 检测策略映射来自定义 DNS 检测操作。

在定义流量匹配条件时，可以创建类映射或者直接在策略映射中包括匹配语句。以下操作步骤说明这两种方法。

准备工作

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

操作步骤

步骤 1　（可选）执行以下步骤创建 DNS 检测类映射。

类映射对多个流量匹配进行分组。或者，可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定字符串 “example.com”，则任何包含 “example.com” 的流量都不匹配类映射。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a. 输入以下命令创建类映射：

```
hostname(config)# class-map type inspect dns [match-all | match-any] class_map_name
hostname(config-cmap)#
```

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。match-any 关键字指明如果流量至少与一个 **match** 语句匹配，即为与类映射匹配。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b. （可选）要向类映射添加描述，请输入以下命令：

```
hostname(config-cmap)# description string
```

其中，*string* 是对类映射的描述（最多可包含 200 个字符）。

c. 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match** [**not**] **header-flag** [**eq**] {*f_name* [*f_name...*] | *f_value*} - 匹配 DNS 标志。*f_name* 参数是以下 DNS 标志名称之一：**AA**（授权应答）、**QR**（查询）、**RA**（可用递归）、**RD**（所需递归）、**TC**（截断）。*f_value* 参数是以 0x 开头的十六进制的 16 位值，范围是 0x0 到 0xffff。**eq** 关键字指定完全匹配（匹配所有）；如果不使用 **eq** 关键字，则数据包只需要匹配指定的报头之一（匹配任意）。例如，**match header-flag AA QR**。
- **match** [**not**] **dns-type** {**eq** {*t_name* | *t_value*} | **range** *t_value1 t_value2*} - 匹配 DNS 类型。*t_name* 参数是以下 DNS 类型名称之一：**A**（IPv4 地址）、**AXFR**（完整区域传送）、**CNAME**（规范名称）、**IXFR**（增量区域传输）、**NS**（授权域名服务器）、**SOA**（授权区域起始）或 **TSIG**（事务数字签名）。*t_value* 参数是 DNS Type 字段中的任意值（0 至 65535）。**range** 关键字指定范围，**eq** 关键字指定完全匹配。例如：**match dns-type eq A**。
- **match** [**not**] **dns-class** {**eq** {**in** | *c_value*} | **range** *c_value1 c_value2*} - 匹配 DNS 类。DNS 类是 **in**（代表互联网）或 *c_value*（DNS Class 字段中 0 到 65535 之间的任意值）。**range** 关键字指定范围，**eq** 关键字指定完全匹配。例如：**match dns-class eq in**。

- **match** [**not**] {**question** | **resource-record** {**answer** | **authority** | **additional**}} - 匹配 DNS 问题或资源记录。**question** 关键字指定 DNS 消息的问题部分。**resource-record** 关键字指定资源记录的如下部分之一：**answer**、**authority** 或 **additional**。例如：**match resource-record answer**。
- **match** [**not**] **domain-name regex** {*regex_name* | **class** *class_name*} - 根据指定的正则表达式或正则表达式类匹配 DNS 消息域名列表。

d. 输入 **exit** 退出类映射配置模式。

步骤 2　创建 DNS 检测策略映射，然后输入以下命令：

```
hostname(config)# policy-map type inspect dns policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 4　要对匹配的流量应用操作，请执行以下步骤。

a. 使用以下其中一种方法指定要对其执行操作的流量：

- 如果已创建 DNS 类映射，请输入以下命令指定该类映射：

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- 要直接在策略映射中指定流量，请对 DNS 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b. 输入下列命令，以指定要对匹配流量执行的操作：

```
hostname(config-pmap-c)# {drop [log] | drop-connection [log] |
enforce-tsig {[drop] [log]} | mask [log] | log}
```

并非所有选项对于每个 **match** 或 **class** 命令都可用。有关可用的确切选项，请参阅 CLI 帮助或命令参考。

drop 关键字丢弃所有匹配的数据包。

drop-connection 关键字丢弃数据包并关闭连接。

mask 关键字掩蔽数据包的匹配部分。此操作仅适用于报头标志匹配项。

关键字 **log**（可以单独使用，也可以与其他关键字之一结合使用）用于发送系统日志消息。

enforce-tsig {[**drop**] [**log**]} 关键字强制消息中必须有 TSIG 资源记录。可以丢弃数据包但不丢弃 TSIG 资源记录，可以记录数据包，也可以丢弃并记录数据包。可以将此选项与针对报头标志匹配项的掩蔽操作结合使用；否则，此操作与其他操作相互排斥。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅第 2-4 页上的在检测策略映射中定义操作。

例如：

```
hostname(config)# policy-map type inspect dns dns-map
hostname(config-pmap)# class dns-class-map
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match header-flag eq aa
hostname(config-pmap-c)# drop log
```

步骤 5　要配置影响检测引擎的参数，请执行以下步骤：

a. 要进入参数配置模式，请输入以下命令：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **dns-guard** - 启用 DNS 保护。一旦 ASA 转发 DNS 应答，ASA 就会断开与 DNS 查询相关的 DNS 会话。另外，ASA 还监控消息交换，确保 DNS 回复 ID 匹配 DNS 查询 ID。
- **id-mismatch count** *number* **duration** *seconds* **action log** - 允许记录过多的 DNS ID 不匹配项，其中，**count** *number* **duration** *seconds* 参数指定在发送系统消息日志之前每秒的最大不匹配实例数。
- **id-randomization** - 随机化 DNS 查询的 DNS 标识符。
- **message-length maximum** {*length* | **client** {*length* | **auto**} | **server** {*length* | **auto**}} - 设置最大 DNS 消息长度（512 至 65535 字节）。还可以设置客户端或服务器消息的最大长度。**auto** 关键字将最大长度设置为资源记录中的值。
- **nat-rewrite** - 根据 NAT 配置转换 DNS 记录。
- **protocol-enforcement** - 启用 DNS 消息格式检查（具体检查内容包括：域名长度不得超过 255 个字符，标签长度不得超过 63 个字符，压缩检查和循环指针检查）。
- **tsig enforced action** {[**drop**] [**log**]} - 要求必须有 TSIG 资源记录。可以**丢弃**和 / 或**记录**不符合要求的数据包。

例如：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)# dns-guard
hostname(config-pmap-p)# message-length maximum 1024
hostname(config-pmap-p)# nat-rewrite
hostname(config-pmap-p)# protocol-enforcement
```

示例

以下示例显示如何定义 DNS 检测策略映射。

```
regex domain_example "example\.com"
regex domain_foo "foo\.com"

!define the domain names that the server serves
class-map type inspect regex match-any my_domains
    match regex domain_example
    match regex domain_foo

!Define a DNS map for query only
class-map type inspect dns match-all pub_server_map
    match not header-flag QR
    match question
    match not domain-name regex class my_domains

policy-map type inspect dns new_dns_map
    class pub_server_map
        drop log
    match header-flag RD
        mask log
```

```
parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
```

配置 DNS 检测服务策略

默认 ASA 配置包括对默认端口的 DNS 检测（这项检测全局应用于所有接口）。自定义检测配置的一种常用方法是自定义默认全局策略。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map dns_class_map
hostname(config-cmap)# match access-list dns
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 DNS 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 DNS 检测。

inspect dns [*dns_policy_map*] [**dynamic-filter-snoop**]

其中：

- *dns_policy_map* 是可选的 DNS 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建 DNS 检测策略映射的信息，请参阅第 8-3 页上的配置 DNS 检测策略映射。

- **dynamic-filter-snoop** 启用动态过滤器监听（仅适用于僵尸网络流量过滤器）。应仅在使用僵尸网络流量过滤时包含此关键字。我们建议仅在有外部 DNS 请求经过的接口上启用 DNS 监听。如果对所有 UDP DNS 流量（包括流向内部 DNS 服务器的流量）启用 DNS 监听，将会对 ASA 造成不必要的负载。

示例：

```
hostname(config-class)# no inspect dns
hostname(config-class)# inspect dns dns-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 DNS 检测策略映射（例如，要替换默认 preset_dns_map），必须使用 **no inspect dns** 命令移除 DNS 检测，然后为其提供新的 DNS 检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

示例

以下示例显示如何在全局默认配置中使用新的检测策略映射：

```
policy-map global_policy
 class inspection_default
  no inspect dns preset_dns_map
  inspect dns new_dns_map
service-policy global_policy global
```

监控 DNS 检测

要查看有关当前 DNS 连接的信息，请在 或 Monitoring > Properties > Connections 中输入以下命令：

```
hostname# show conn
```

对于使用 DNS 服务器的连接，可以用 show conn 命令输出中的 DNS 服务器的 IP 地址替换连接的源端口。

可以为多个 DNS 会话创建单一连接，前提是，这些会话都在同两台主机之间且具有相同的五元组（源 / 目标 IP 地址、源 / 目标端口和协议）。可通过 app_id 跟踪 DNS 标识，且每个 app_id 的空闲计时器独立运行。

由于 app_id 的期限是独立，因此，合法的 DNS 应答只能在有限的时间段内通过安全设备，而且不会累积资源。但是，输入 **show conn** 命令时，将会看到新的 DNS 会话正在重置 DNS 连接的空闲计时器。这是由共享 DNS 连接的性质决定的，也是如此设计的。

要显示 DNS 应用检测的统计信息，请输入 **show service-policy** 命令。以下是 **show service-policy** 命令的输出示例：

```
hostname# show service-policy
Interface outside:
Service-policy: sample_policy
    Class-map: dns_port
      Inspect: dns maximum-length 1500, packet 0, drop 0, reset-drop 0
```

FTP 检测

以下各节介绍 FTP 检测引擎。

- 第 8-8 页上的 FTP 检测概述
- 第 8-8 页上的严格 FTP
- 第 8-9 页上的配置 FTP 检测
- 第 8-13 页上的验证和监控 FTP 检测

FTP 检测概述

FTP 应用检测检查 FTP 会话并执行以下四项任务：

- 准备动态辅助数据连接
- 跟踪 FTP 命令 - 响应序列
- 生成审核线索
- 转换嵌入式 IP 地址

FTP 应用检测为 FTP 数据传输准备辅助信道。这些信道的端口是通过 PORT 或 PASV 命令协商的。这些信道根据文件上传、文件下载或目录列表事件进行分配。

注　如果您使用 **no inspect ftp** 命令禁用 FTP 检测引擎，出站用户只能在被动模式下启动连接，且所有入站 FTP 都将被禁用。

严格 FTP

严格 FTP 可防止网络浏览器在 FTP 请求中发送嵌入式命令，从而提高受保护网络的安全。要启用严格 FTP，请使用 **inspect ftp** 命令将 **strict** 选项包含在内。

如果使用严格 FTP，或者还可以指定 FTP 检测策略映射，以指定不允许通过 ASA 的 FTP 命令。

对接口启用 **strict** 选项后，FTP 检测将强制执行以下行为：

- ASA 在 FTP 命令得到确认后才允许新的命令。
- ASA 断开发送嵌入式命令的连接。
- 检查 227 命令和 PORT 命令，以确保这些命令不显示在错误字符串中。

注意事项　使用 **strict** 选项可能会导致不完全符合 FTP RFC 要求的客户端发生故障。

如果启用 **strict** 选项，将会跟踪每个 FTP 命令 - 响应序列，以确定是否存在以下异常活动：

- 截断命令 - 检查 PORT 和 PASV 应答命令中逗号的数量是否是五个。如果不是五个，将会截断 PORT 命令并关闭 TCP 连接。
- 错误命令 - 检查 FTP 命令以确定它是否以 <CR><LF> 字符结尾（如 RFC 所要求）。如果不是，将会关闭连接。
- RETR 和 STOR 命令的大小 - 根据某个固定常数检查这些命令的大小。如果命令大小大于该固定常数，将会记录错误消息并关闭连接。
- 命令欺骗 - PORT 命令应始终从客户端发送。如果 PORT 命令是从服务器发送，将会拒绝 TCP 连接。
- 应答欺骗 - PASV 应答命令 (227) 应始终从服务器发送。如果 PASV 应答命令是从客户端发送，将会拒绝 TCP 连接。这样可防止用户执行 “227 xxxxx a1, a2, a3, a4, p1, p2.” 时出现安全漏洞
- TCP 数据流编辑 - 如果 ASA 检测到 TCP 数据流编辑，它会关闭连接。
- 无效的端口协商 - 检查协商的动态端口值是否小于 1024。由于 1 至 1024 范围内的端口号是为已知连接保留的，因此，如果协商的端口在这个范围内，将会释放 TCP 连接。
- 命令管道 - 将 PORT 和 PASV 应答命令中在端口号后显示的字符数与常数值 8 进行比较。如果该字符数大于 8，将会关闭 TCP 连接。
- ASA 用一系列 X 替换 FTP 服务器对 SYST 命令的响应， 以防止服务器向 FTP 客户端显示其系统类型。要覆盖此默认行为，请在 FTP 映射中使用 **no mask-syst-reply** 命令。

配置 FTP 检测

默认情况下，FTP 检测已启用。仅在需要非默认处理的情况下，才需要配置这项检测。如果要自定义 FTP 检测，请按照以下流程进行操作。

操作步骤

步骤 1　第 8-9 页上的配置 FTP 检测策略映射。

步骤 2　第 8-12 页上的配置 FTP 检测服务策略。

配置 FTP 检测策略映射

使用严格 FTP 检测可进行 FTP 命令过滤和安全检查，从而提高安全和加强控制。协议符合性包括数据包长度检查、分隔符和数据包格式检查、命令终止符检查以及命令验证。

也支持根据用户值阻止 FTP，这样，FTP 站点可以发布供下载的文件，但仅允许某些用户访问。可以根据文件类型、服务器名称及其他属性阻止 FTP 连接。如果进行检测后 FTP 连接被拒绝，将会生成系统消息日志。

如果您希望 FTP 检测允许 FTP 服务器向 FTP 客户端显示其系统类型，并限制允许的 FTP 命令，可以创建并配置 FTP 检测策略映射。然后，可以在启用 FTP 检测时应用所创建的映射。

准备工作

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

操作步骤

步骤 1　（可选）执行以下步骤创建 FTP 检测类映射。

类映射对多个流量匹配进行分组。或者，可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定字符串 “example.com”，则任何包含 “example.com” 的流量都不匹配类映射。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a. 输入以下命令创建类映射：

```
hostname(config)# class-map type inspect ftp [match-all | match-any] class_map_name
hostname(config-cmap)#
```

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。match-any 关键字指明如果流量至少与一个 **match** 语句匹配，即为与类映射匹配。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b. （可选）要向类映射添加描述，请输入以下命令：

```
hostname(config-cmap)# description string
```

其中，*string* 是对类映射的描述（最多可包含 200 个字符）。

c. 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match** [**not**] **filename regex** {*regex_name* | **class** *class_name*} - 将 FTP 传输中的文件名与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **filetype regex** {*regex_name* | **class** *class_name*} - 将 FTP 传输中的文件类型与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **request-command** *ftp_command* [*ftp_command...*] - 匹配以下一个或多个 FTP 命令：

  APPE - 附加到文件。

  CDUP - 更改为当前工作目录的父目录。

  DELE - 删除服务器上的文件。

  GET - 从服务器获取文件。

  HELP - 提供帮助信息。

  MKD - 在服务器上创建目录。

  PUT - 向服务器发送文件。

  RMD - 在服务器上删除目录。

  RNFR - 指定 “rename-from” 文件名

  RNTO - 指定 “rename-to” 文件名

  SITE - 用于指定服务器特定命令。此命令通常用于远程管理。

  STOU - 用唯一文件名存储文件。

- **match** [**not**] **server regex** {*regex_name* | **class** *class_name*} - 将 FTP 服务器名称与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **username regex** {*regex_name* | **class** *class_name*} - 将 FTP 用户名与指定的正则表达式或正则表达式类进行匹配。

d. 输入 **exit** 退出类映射配置模式。

步骤 2　创建 FTP 检测策略映射：

```
hostname(config)# policy-map type inspect ftp policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 4　要对匹配的流量应用操作，请执行以下步骤。

a. 使用以下其中一种方法指定要对其执行操作的流量：

- 如果已创建 FTP 类映射，请输入以下命令指定该类映射：

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- 要直接在策略映射中指定流量，请对 FTP 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b. 输入下列命令，以指定要对匹配流量执行的操作：

```
hostname(config-pmap-c)# reset [log]
```

reset 关键字丢弃数据包、关闭连接并向服务器或客户端发送 TCP 重置。添加 **log** 关键字以发送系统日志消息。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅第 2-4 页上的在检测策略映射中定义操作。

步骤 5　要配置影响检测引擎的参数，请执行以下步骤：

a. 要进入参数配置模式，请输入以下命令：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **mask-banner** - 掩蔽来自 FTP 服务器的问候横幅。
- **mask-syst-reply** - 掩蔽对 **syst** 命令的应答。

示例

提交用户名和密码之前，所有 FTP 用户均可以看到问候横幅。默认情况下，该横幅包含对于试图发现系统缺陷的黑客来说很有用的版本信息。以下示例显示如何掩蔽该横幅：

```
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner

hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp
```

```
hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap

hostname(config)# service-policy ftp-policy interface inside
```

配置 FTP 检测服务策略

默认 ASA 配置包括对默认端口的 FTP 检测（这项检测全局应用于所有接口）。自定义检测配置的一种常用方法是自定义默认全局策略。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map ftp_class_map
hostname(config-cmap)# match access-list ftp
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 FTP 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 FTP 检测。

inspect ftp [**strict** [*ftp_policy_map*]]

其中：

- **strict** 执行严格 FTP。必须使用严格 FTP 来指定 FTP 检测策略映射。
- *ftp_policy_map* 是可选的 FTP 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建 FTP 检测策略映射的信息，请参阅第 8-9 页上的配置 FTP 检测策略映射。

示例：

```
hostname(config-class)# no inspect ftp
hostname(config-class)# inspect ftp strict ftp-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 FTP 检测策略映射，必须使用 **no inspect ftp** 命令移除 FTP 检测，然后为其提供新的 FTP 检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

验证和监控 FTP 检测

FTP 应用检测生成以下日志消息：

- 为检索或上传的每个文件生成审核记录 303002。
- 检查 FTP 命令以确定它是否是 RETR 或 STOR 命令，并记录检索命令和存储命令。
- 通过查找提供了 IP 地址的表格获取用户名。
- 记录用户名、源 IP 地址、目标 IP 地址、NAT 地址和文件操作。
- 如果辅助动态信道准备因内存不足而失败，将会生成审核记录 201005。

如果与 NAT 配合使用，FTP 应用检测可转换应用负载中的 IP 地址。RFC 959 中对此进行了说明。

HTTP 检测

以下各节介绍 HTTP 检测引擎。

- 第 8-13 页上的 HTTP 检测概述
- 第 8-14 页上的配置 HTTP 检测

HTTP 检测概述

提示　可以安装执行应用过滤和 URL 过滤（包括 HTTP 检测）的服务模块，例如 ASA CX 或 ASA FirePOWER。ASA 上运行的 HTTP 检测与这些模块不兼容。请注意，使用专用模块配置应用过滤比在 ASA 上使用 HTTP 检测策略映射手动配置应用过滤要容易得多。

使用 HTTP 检测引擎可防御特定攻击以及与 HTTP 流量相关的其他威胁。

HTTP 应用检测扫描 HTTP 报头和正文，并对数据执行各种检查。这些检查可防止各种 HTTP 构造、内容类型、隧道协议和消息传送协议通过安全设备。

增强型 HTTP 检测功能（又称为应用防火墙，在配置 HTTP 检测策略映射时可使用此功能）有助于防止攻击者使用 HTTP 消息来避开网络安全策略。

HTTP 应用检测可阻止通过隧道传送的应用以及 HTTP 请求和响应中的非 ASCII 字符，从而防止恶意内容到达网络服务器。还支持对 HTTP 请求和响应报头中的各个元素进行大小限制、URL 拦截以及 HTTP 服务器报头类型欺骗。

增强型 HTTP 检测验证所有 HTTP 消息是否满足以下条件：

- 符合 RFC 2616 的要求
- 仅使用 RFC 定义的方法。
- 符合其他条件。

配置 HTTP 检测

默认情况下，HTTP 检测未启用。如果 HTTP 检测和应用过滤未使用专用模块（例如 ASA CX 或 ASA FirePOWER），可以按照以下步骤在 ASA 上手动配置 HTTP 检测。

提示　请勿在服务模块和 ASA 上都配置 HTTP 检测，因为这两者上的检测是不兼容的。

操作步骤

步骤 1　第 8-14 页上的配置 HTTP 检测策略映射。

步骤 2　第 8-18 页上的配置 HTTP 检测服务策略。

配置 HTTP 检测策略映射

要指定消息违反参数时要执行的操作，请创建 HTTP 检测策略映射。然后，可以在启用 HTTP 检测时应用所创建的检测策略映射。

准备工作

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

操作步骤

步骤 1　（可选）执行以下步骤创建 HTTP 检测类映射。

类映射对多个流量匹配进行分组。或者，可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定字符串 “example.com”，则任何包含 “example.com” 的流量都不匹配类映射。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a. 输入以下命令创建类映射：

```
hostname(config)# class-map type inspect http [match-all | match-any] class_map_name
hostname(config-cmap)#
```

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。match-any 关键字指明如果流量至少与一个 **match** 语句匹配，即为与类映射匹配。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b. （可选）要向类映射添加描述，请输入以下命令：

```
hostname(config-cmap)# description string
```

其中，*string* 是对类映射的描述（最多可包含 200 个字符）。

c. 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match** [**not**] **req-resp content-type mismatch** - 匹配 HTTP 响应中的 content-type 字段与相应 HTTP 请求消息中的接受字段不匹配的流量。
- **match** [**not**] **request args regex** {*regex_name* | **class** *class_name*} - 将在 HTTP 请求消息参数中找到的文本与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **request body** {**regex** {*regex_name* | **class** *class_name*} | **length gt** *bytes*} - 将在 HTTP 请求消息正文中找到的文本与指定的正则表达式或正则表达式类进行匹配，或者匹配请求正文长度大于指定长度的消息。
- **match** [**not**] **request header** {*field* | **regex** *regex_name*} **regex** {*regex_name* | **class** *class_name*} - 将 HTTP 请求消息报头中字段的内容与指定的正则表达式或正则表达式类进行匹配。可以明确指定字段名称，或者将字段名称与正则表达式进行匹配。字段名称包括：accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。
- **match** [**not**] **request header** {*field* | **regex** {*regex_name* | **class** *class_name*}} {**length gt** *bytes* | **count gt** *number*} - 匹配 HTTP 请求消息报头中指定字段的长度或报头中的字段总数。可以明确指定字段名称，或者将字段名称与正则表达式或正则表达式类进行匹配。上一要点中列出了字段名称。
- **match** [**not**] **request header** {**length gt** *bytes* | **count gt** *number* | **non-ascii**} - 匹配 HTTP 请求消息报头的总长度、报头中的字段总数或包含非 ASCII 字符的报头。
- **match** [**not**] **request method** {*method* | **regex** {*regex_name* | **class** *class_name*}} - 匹配 HTTP 请求方法。可以明确指定方法，或者将方法与正则表达式进行匹配。方法包括：bcopy、bdelete、bmove、bpropfind、bproppatch、connect、copy、delete、edit、get、getattribute、getattributenames、getproperties、head、index、lock、mkcol、mkdir、move、notify、options、poll、post、propfind、proppatch、put、revadd、revlabel、revlog、revnum、save、search、setattribute、startrev、stoprev、subscribe、trace、unedit、unlock、unsubscribe。
- **match** [**not**] **request uri** {**regex** {*regex_name* | **class** *class_name*} | **length gt** *bytes*} - 将在 HTTP 请求消息 URI 中找到的文本与指定的正则表达式或正则表达式类进行匹配，或者匹配请求 URI 长度大于指定长度的消息。

- **match** [**not**] **response body** {**active-x** | **java-applet** | **regex** {*regex_name* | **class** *class_name*}} - 将 HTTP 响应消息正文中找到的文本与指定的正则表达式或正则表达式类进行匹配，或者注释掉 Java 小程序和 Active X 对象标签以便对其进行过滤。
- **match** [**not**] **response body length gt** *bytes* - 匹配正文长度大于指定长度的 HTTP 响应消息。
- **match** [**not**] **response header** {*field* | **regex** *regex_name*} **regex** {*regex_name* | **class** *class_name*}- 将 HTTP 响应消息报头中字段的内容与指定的正则表达式或正则表达式类进行匹配。可以明确指定字段名称，或者将字段名称与正则表达式进行匹配。字段名称包括：accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。
- **match** [**not**] **response header** {*field* | **regex** {*regex_name* | **class** *class_name*}} {**length gt** *bytes* | **count gt** *number*} - 匹配 HTTP 响应消息报头中指定字段的长度或报头中的字段总数。可以明确指定字段名称，或者将字段名称与正则表达式或正则表达式类进行匹配。上一要点中列出了字段名称。
- **match** [**not**] **response header** {**length gt** *bytes* | **count gt** *number* | **non-ascii**} - 匹配 HTTP 响应消息报头的总长度、报头中的字段总数或包含非 ASCII 字符的报头。
- **match** [**not**] **response status-line regex** {*regex_name* | **class** *class_name*} - 将 HTTP 响应消息状态行中找到的文本与指定的正则表达式或正则表达式类进行匹配。

d. 输入 **exit** 退出类映射配置模式。

步骤 2　创建 HTTP 检测策略映射：

```
hostname(config)# policy-map type inspect http policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 4　要对匹配的流量应用操作，请执行以下步骤。

a. 使用以下其中一种方法指定要对其执行操作的流量：

- 如果已创建 HTTP 类映射，请输入以下命令指定该类映射：

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- 要直接在策略映射中指定流量，请对 HTTP 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b. 输入下列命令，以指定要对匹配流量执行的操作：

```
hostname(config-pmap-c)# {drop-connection [log]| reset [log] | log}
```

drop-connection 关键字丢弃数据包并关闭连接。

reset 关键字丢弃数据包、关闭连接并向服务器或客户端发送 TCP 重置。

关键字 **log**（可以单独使用，也可以与其他关键字之一结合使用）用于发送系统日志消息。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅第 2-4 页上的在检测策略映射中定义操作。

步骤 5　要配置影响检测引擎的参数，请执行以下步骤：

a. 要进入参数配置模式，请输入以下命令：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **body-match-maximum** *number* - 设置应在正文匹配中搜索的 HTTP 消息正文中的最大字符数。默认值为 200 字节。字符数量大将会对性能造成明显影响。
- **protocol-violation action** {**drop-connection [log] | reset [log] | log**} - 设置应在正文匹配中搜索的 HTTP 消息正文中的最大字符数。默认值为 200 字节。字符数量大将会明显影响针对 HTTP 协议违规的 performance.xxxChecks。必须选择要对违规情况执行的操作（断开连接、重置连接或记录连接）以及是否启用或禁用日志记录。
- **spoof-server** *string* - 用字符串替换服务器报头字段，WebVPN 数据流不受 **spoof-server** 命令影响。

示例

以下示例显示如何定义这样的 HTTP 检测策略映射：允许并记录使用 “GET” 或 “PUT” 方法尝试访问 “www\.xyz.com/.*\.asp” 或 “www\.xyz[0-9][0-9]\.com” 的任何 HTTP 连接。默认允许 URL 与方法的所有其他组合。

```
hostname(config)# regex url1 "www\.xyz.com/.*\.asp"
hostname(config)# regex url2 "www\.xyz[0-9][0-9]\.com"
hostname(config)# regex get "GET"
hostname(config)# regex put "PUT"

hostname(config)# class-map type regex match-any url_to_log
hostname(config-cmap)# match regex url1
hostname(config-cmap)# match regex url2
hostname(config-cmap)# exit

hostname(config)# class-map type regex match-any methods_to_log
hostname(config-cmap)# match regex get
hostname(config-cmap)# match regex put
hostname(config-cmap)# exit

hostname(config)# class-map type inspect http http_url_policy
hostname(config-cmap)# match request uri regex class url_to_log
hostname(config-cmap)# match request method regex class methods_to_log
hostname(config-cmap)# exit

hostname(config)# policy-map type inspect http http_policy
hostname(config-pmap)# class http_url_policy
hostname(config-pmap-c)# log
```

配置 HTTP 检测服务策略

HTTP 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。但是，默认检测类包括默认 HTTP 端口，因此，只需简单地编辑默认全局检测策略即可添加 HTTP 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map http_class_map
hostname(config-cmap)# match access-list http
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 HTTP 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 HTTP 检测。

inspect http [*http_policy_map*]

其中，*http_policy_map* 是可选的 HTTP 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建 HTTP 检测策略映射的信息，请参阅第 8-14 页上的配置 HTTP 检测策略映射。

示例：

```
hostname(config-class)# no inspect http
hostname(config-class)# inspect http http-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 HTTP 检测策略映射，必须使用 **no inspect http** 命令移除 HTTP 检测，然后为其提供新的 HTTP 检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

ICMP 检测

ICMP 检测引擎允许 ICMP 流量具有“会话”，这样可以像对 TCP 和 UDP 流量那样对这种流量进行检测。如果没有 ICMP 检测引擎，我们建议不要允许 ICMP 通过 ACL 中的 ASA。如果不进行状态检测，ICMP 可能被用于攻击网络。ICMP 检测引擎确保每个请求只有一个响应，并确保序列号是正确的。

但是，即使启用 ICMP 检测，也不会检测流向 ASA 接口的 ICMP 流量。因此，到接口的 ping（回应请求）可能会在特定情况下失败，例如，如果回应请求来自 ASA 可以通过备用默认路由到达的源。

有关启用 ICMP 检测的信息，请参阅第 7-9 页上的配置应用层协议检测。

ICMP 错误检测

如果启用了 ICMP 错误检测，ASA 会根据 NAT 配置为发送 ICMP 错误消息的中间跃点创建转换会话。ASA 用转换后的 IP 地址覆盖数据包。

如果这项检测被禁用，ASA 不会为生成 ICMP 错误消息的中间节点创建转换会话。内部主机与 ASA 之间的中间节点生成的 ICMP 错误消息可在不占用任何额外 NAT 资源的情况下到达外部主机。如果外部主机使用路由跟踪命令跟踪到达 ASA 内部目标的跃点，不需要执行此操作。如果 ASA 不转换中间跃点时，所有中间跃点都将与映射的目标 IP 地址一起显示。

会扫描 ICMP 负载，以从原始数据包检索五元组。然后，会使用检索到的五元组进行查找，以确定客户端的原始地址。ICMP 错误检测引擎会对 ICMP 数据包进行以下更改：

- 在 IP 报头中，映射 IP 更改为实际 IP（目标地址）并修改 IP 校验和。
- 在 ICMP 报头中，会根据 ICMP 数据包的变化修改 ICMP 校验和。
- 在负载中，会进行以下更改：
  - 原始数据包映射 IP 更改为实际 IP
  - 原始数据包映射端口更改为实际端口
  - 重新计算原始数据包 IP 校验和

有关启用 ICMP 错误检测的信息，请参阅第 7-9 页上的配置应用层协议检测。

即时消息检测

使用即时消息 (IM) 检测引擎可以控制 IM 的网络使用情况，以及阻止机密数据泄露、蠕虫传播和针对公司网络的其他威胁。

默认情况下，IM 检测未启用。如果需要 IM 检测，必须对其进行配置。

操作步骤

步骤 1　第 8-20 页上的配置即时消息检测策略映射。

步骤 2　第 8-22 页上的配置 IM 检测服务策略。

配置即时消息检测策略映射

要指定消息违反参数时要执行的操作，请创建 IM 检测策略映射。然后，可以在启用 IM 检测时应用所创建的检测策略映射。

准备工作

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

操作步骤

步骤 1　（可选）执行以下步骤创建 IM 检测类映射。

类映射对多个流量匹配进行分组。或者，可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定字符串 “example.com”，则任何包含 “example.com” 的流量都不匹配类映射。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a.　输入以下命令创建类映射：

```
hostname(config)# class-map type inspect im [match-all | match-any] class_map_name
hostname(config-cmap)#
```

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。match-any 关键字指明如果流量至少与一个 **match** 语句匹配，即为与类映射匹配。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b.　（可选）要向类映射添加描述，请输入以下命令：

```
hostname(config-cmap)# description string
```

其中，*string* 是对类映射的描述（最多可包含 200 个字符）。

c. 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match** [**not**] **protocol {im-yahoo | im-msn}** - 匹配特定 IM 协议（Yahoo 或 MSN）。
- **match** [**not**] **service {chat | file-transfer | webcam | voice-chat | conference | games}** - 匹配特定 IM 服务。
- **match** [**not**] **login-name regex** {*regex_name* | **class** *class_name*} - 将 IM 消息的源客户端登录名与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **peer-login-name regex** {*regex_name* | **class** *class_name*} - 将 IM 消息的目标对等体登录名与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **ip-address** *ip_address mask*} - 匹配 IM 消息的源 IP 地址和掩码。
- **match** [**not**] **peer-ip-address** *ip_address mask*} - 匹配 IM 消息的目标 IP 地址和掩码。
- **match** [**not**] **version regex** {*regex_name* | **class** *class_name*} - 将 IM 消息的版本与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **filename regex** {*regex_name* | **class** *class_name*} - 将 IM 消息的文件名与指定的正则表达式或正则表达式类进行匹配。MSN IM 协议不支持这种匹配。

d. 输入 **exit** 退出类映射配置模式。

步骤 2　创建 IM 检测策略映射：

```
hostname(config)# policy-map type inspect im policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 4　要对匹配的流量应用操作，请执行以下步骤。

a. 使用以下其中一种方法指定要对其执行操作的流量：

- 如果已创建 IM 类映射，请输入以下命令指定该类映射：

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- 要直接在策略映射中指定流量，请对 IM 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b. 输入下列命令，以指定要对匹配流量执行的操作：

```
hostname(config-pmap-c)# {drop-connection [log]| reset [log] | log}
```

drop-connection 关键字丢弃数据包并关闭连接。

reset 关键字丢弃数据包、关闭连接并向服务器或客户端发送 TCP 重置。

关键字 **log**（可以单独使用，也可以与其他关键字之一结合使用）用于发送系统日志消息。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅第 2-4 页上的在检测策略映射中定义操作。

示例

以下示例显示如何定义 IM 检测策略映射。

```
hostname(config)# regex loginname1 "ying\@yahoo.com"
hostname(config)# regex loginname2 "Kevin\@yahoo.com"
hostname(config)# regex loginname3 "rahul\@yahoo.com"
hostname(config)# regex loginname4 "darshant\@yahoo.com"
hostname(config)# regex yahoo_version_regex "1\.0"
hostname(config)# regex gif_files ".*\.gif"
hostname(config)# regex exe_files ".*\.exe"

hostname(config)# class-map type regex match-any yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-any yahoo_dst_login_name_regex
hostname(config-cmap)# match regex loginname3
hostname(config-cmap)# match regex loginname4

hostname(config)# class-map type inspect im match-any yahoo_file_block_list
hostname(config-cmap)# match filename regex gif_files
hostname(config-cmap)# match filename regex exe_files

hostname(config)# class-map type inspect im match-all yahoo_im_policy
hostname(config-cmap)# match login-name regex class yahoo_src_login_name_regex
hostname(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex

hostname(config)# class-map type inspect im match-all yahoo_im_policy2
hostname(config-cmap)# match version regex yahoo_version_regex

hostname(config)# class-map im_inspect_class_map
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map type inspect im im_policy_all
hostname(config-pmap)# class yahoo_file_block_list
hostname(config-pmap-c)# match service file-transfer
hostname(config-pmap)# class yahoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yahoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspect_class_map
hostname(config-pmap-c)# inspect im im_policy_all
```

配置 IM 检测服务策略

IM 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。但是，默认检测类包括默认 IM 端口，因此，只需简单地编辑默认全局检测策略即可添加 IM 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map im_class_map
hostname(config-cmap)# match access-list im
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 IM 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 IM 检测。

inspect im [*im_policy_map*]

其中，*im_policy_map* 是可选的 IM 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建 IM 检测策略映射的信息，请参阅第 8-20 页上的配置即时消息检测策略映射。

示例：

```
hostname(config-class)# no inspect im
hostname(config-class)# inspect im im-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 IM 检测策略映射，必须使用 **no inspect im** 命令移除 IM 检测，然后为其提供新的 IM 检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

IP 选项检测

可以配置 IP 选项检测来控制具有特定 IP 选项的哪些 IP 数据包可以通过 ASA。可以通过配置这项检测来指示 ASA 采取以下行动：允许数据包通过；或者清除指定的 IP 选项，然后允许数据包通过。

以下各节介绍 IP 选项检测引擎。

- 第 8-24 页上的 IP 选项检测概述
- 第 8-25 页上的 IP 选项检测的默认设置
- 第 8-25 页上的配置 IP 选项检测
- 第 8-27 页上的监控 IP 选项检测

IP 选项检测概述

每个 IP 数据包都包含一个带有 Options 字段的 IP 报头。Options 字段（通常称为 IP 选项）提供了某些情况下需要使用的控制功能，但这些功能在大多数常见通信中是不必要的。具体来说，IP 选项提供了时间戳、安全性和特殊路由。并非必须使用 IP 选项，此字段可能包括零个、一个或多个选项。

有关 IP 选项的列表以及相关 RFC 的引用，请参阅 IANA 页面 http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml。

可以配置 IP 选项检测来控制具有特定 IP 选项的哪些 IP 数据包可以通过 ASA。可以通过配置这项检测来指示 ASA 采取以下行动：允许数据包通过；或者清除指定的 IP 选项，然后允许数据包通过。

清除选项时会发生的情况

配置 IP 选项检测策略映射时，可以指定是否要允许或清除每种选项类型。如果不指定某个选项类型，包含该选项的数据包将被丢弃。

如果仅允许一个选项，包含该选项的数据包将会在不发生变化的情况下通过。

如果指定了要从 IP 报头中清除的选项，IP 报头会发生如下变化：

- 将会从报头中移除该选项。
- 将会填充 Options 字段，以使该字段以 32 位边界结尾。
- 数据包中的互联网报头长度 (IHL) 将会发生变化。
- 数据包的总长度将会发生变化。
- 将会重新计算校验和。

支持检测的 IP 选项

IP 选项检测可以检查数据包中的以下 IP 选项。如果 IP 报头包含除这些选项外的其他选项，那么，无论 ASA 是否配置为允许这些选项，ASA 都会丢弃数据包。

- End of Options List (EOOL) 或 IP 选项 0 - 此选项仅包含一个零字节，显示在所有选项的末尾，用于标记选项列表的末尾。根据报头长度，这可能与报头末尾不一致。
- No Operation (NOP) 或 IP 选项 1 - IP 报头中的 Options 字段可能包括零个、一个或多个选项，这些选项共同构成此字段变量的总长度。但是，IP 报头必须是 32 位的倍数。如果所有选项的位数不是 32 位的倍数，NOP 选项将被作为 “ 内部填充 ”，用于对齐 32 位边界上的选项。

- Router Alert (RTRALT) 或 IP 选项 20 - 此选项通知中转路由器应检测数据包的内容，即使数据包不是发送给该路由器。实施 RSVP 以及实施需要路由器沿着数据包传送路径进行相对复杂的处理的类似协议时，这项检查很有用。丢弃包含 Router Alert 选项的 RSVP 数据包可能会导致 VoIP 的实施出现问题。

IP 选项检测的默认设置

默认情况下，IP 选项检测已使用 _default_ip_options_map 检测策略映射启用。

- 允许使用 Router Alert 选项。
- 包含任何其他选项（包括不受支持的选项）的数据包将被丢弃。

以下是策略映射配置：

```
policy-map type inspect ip-options _default_ip_options_map
 description Default IP-OPTIONS policy-map
 parameters
  router-alert action allow
```

配置 IP 选项检测

默认情况下，IP 选项检测已启用。仅在要允许默认映射允许的选项以外的其他选项时，才需要配置这项检测。

操作步骤

步骤 1　第 8-25 页上的配置 IP 选项检测策略映射。

步骤 2　第 8-26 页上的配置 IP 选项检测服务策略。

配置 IP 选项检测策略映射

如果要执行非默认 IP 选项检测，请创建 IP 选项检测策略映射，以指定要如何处理每种受支持的选项类型。

操作步骤

步骤 1　创建 IP 选项检测策略映射：

```
hostname(config)# policy-map type inspect ip-options policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 3　要配置影响检测引擎的参数，请执行以下步骤：

a. 要进入参数配置模式，请输入以下命令：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项。在所有情况下，**allow** 操作允许包含指定选项且未经过修改的数据包； **clear** 操作允许包含指定选项的数据包，但会从报头中移除该选项。包含映射中未包括的选项的任何数据包将被丢弃。有关选项的说明，请参阅第 8-24 页上的支持检测的 IP 选项。

- **eool action** {**allow** | **clear**} - 允许或清除 End of Options List 选项。
- **nop action** {**allow** | **clear**} - 允许或清除 No Operation 选项。
- **router-alert action** {**allow** | **clear**} - 允许或清除 Router Alert (RTRALT) 选项。

配置 IP 选项检测服务策略

默认 ASA 配置包括全局应用于所有接口的 IP 选项检测。自定义检测配置的一种常用方法是自定义默认全局策略。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map ip_options_class_map
hostname(config-cmap)# match access-list ipoptions
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 IP 选项检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 IP 选项检测。

inspect ip-options [*ip_options_policy_map*]

其中，*ip_options_policy_map* 是可选的 IP 选项检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建 IP 选项检测策略映射的信息，请参阅第 8-25 页上的配置 IP 选项检测策略映射。

示例：

```
hostname(config-class)# no inspect ip-options
hostname(config-class)# inspect ip-options ip-options-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 IP 选项检测策略映射，必须使用 **no inspect ip-options** 命令移除 IP 选项检测，然后为其提供新的 IP 选项检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

监控 IP 选项检测

可以使用以下方法来监控 IP 选项检测的结果：

- 每次数据包因检测而被丢弃时，都会发出系统日志 106012。该消息会显示是哪个选项导致数据包被丢弃。
- 使用 **show service-policy inspect ip-options** 命令可查看每个选项的统计信息。

IPsec 穿透检测

以下各节介绍 IPsec 穿透检测引擎。

- 第 8-27 页上的 IPsec 穿透检测概述
- 第 8-28 页上的配置 IPsec 穿透检测

IPsec 穿透检测概述

互联网协议安全 (IPsec) 是一个协议集，用于通过验证和加密数据流的每个 IP 数据包来保护 IP 通信。IPsec 还包括用于会话开始时在代理之间建立相互身份验证以及用于协商将在会话期间使用的加密密钥的协议。IPsec 可用于保护一对主机之间（例如，计算机用户或服务器）、一对安全网关之间（例如，路由器或防火墙）或安全网关与主机之间的数据流。

IPSec 穿透应用检测使得与 IKE UDP 端口 500 连接相关的 ESP（IP 协议 50）和 AH（IP 协议 51）流量可以轻松地通过。这项检测避免了为允许 ESP 和 AH 流量而需要进行冗长的 ACL 配置，并使用超时和最大连接数实现安全性。

可以为 IPsec 穿透检测配置策略映射，以指定 ESP 或 AH 流量的限制。可以为每个客户端设置最大连接数和空闲超时。

允许 NAT 流量和非 NAT 流量。但是，不支持 PAT。

配置 IPsec 穿透检测

默认情况下，IPSec 穿透检测未启用。如果需要 IPsec 穿透检测，必须对其进行配置。

操作步骤

步骤 1　第 8-28 页上的配置 IPsec 穿透检测策略映射。

步骤 2　第 8-29 页上的配置 IPSec 穿透检测服务策略。

配置 IPsec 穿透检测策略映射

通过 IPsec 穿透映射可以更改用于 IPSec 穿透应用检测的默认配置值。借助 IPsec 穿透映射，无需使用 ACL 即可允许某些数据流。

配置包括默认映射 _default_ipsec_passthru_map，该默认映射设置每个客户端的最大 ESP 连接数，并将 ESP 空闲超时设置为 10 分钟。仅在需要非默认值或者需要设置 AH 值的情况下，才需要配置检测策略映射。

操作步骤

步骤 1　创建 IPsec 穿透检测策略映射：

```
hostname(config)# policy-map type inspect ipsec-pass-thru policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 3　要配置影响检测引擎的参数，请执行以下步骤：

a.　要进入参数配置模式，请输入以下命令：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b.　设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **esp per-client-max** *number* **timeout** *time* - 允许 ESP 隧道并设置每个客户端的最大允许连接数和空闲超时（格式为 hh:mm:ss）。要允许无限连接数，请指定 0。
- **ah per-client-max** *number* **timeout** *time* - 允许 AH 隧道。这些参数的含义与 esp 命令的含义相同。

示例

以下示例显示如何使用 ACL 来标识 IKE 流量、定义 IPsec 穿透参数映射、定义策略以及将策略应用于外部接口：

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
hostname(config-pmap-c)# inspect ipsec-pass-thru iptmap
hostname(config)# service-policy inspection_policy interface outside
```

配置 IPSec 穿透检测服务策略

IPsec 穿透检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。但是，默认检测类包括默认 IPsec 端口，因此，只需简单地编辑默认全局检测策略即可添加 IPsec 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map ipsec_class_map
hostname(config-cmap)# match access-list ipsec
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 IPsec 穿透检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 IPsec 穿透检测。

inspect ipsec-pass-thru [*ipsec_policy_map*]

其中，*ipsec_policy_map* 是可选的 IPsec 穿透检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建检测策略映射的信息，请参阅第 8-28 页上的配置 IPsec 穿透检测策略映射。

示例：

```
hostname(config-class)# no inspect ipsec-pass-thru
hostname(config-class)# inspect ipsec-pass-thru ipsec-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 IPsec 穿透检测策略映射，必须使用 **no inspect ipsec-pass-thru** 命令移除 IPsec 穿透检测，然后为其提供新的 IPsec 穿透检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

IPv6 检测

IPv6 检测根据扩展报头有选择性地记录或丢弃 IPv6 流量。此外，IPv6 检测可以检查 IPv6 数据包中扩展报头的类型和顺序是否符合 RFC 2460 的要求。

- 第 8-30 页上的 IPv6 检测的默认设置
- 第 8-31 页上的配置 IPv6 检测

IPv6 检测的默认设置

如果启用 IPv6 检测但不指定检测策略映射，将会使用默认 IPv6 检测策略映射并执行以下操作：

- 仅允许已知的 IPv6 扩展报头。丢弃并记录不符合要求的数据包。
- 按照 RFC 2460 规范的规定实施 IPv6 扩展报头顺序。丢弃并记录不符合要求的数据包。
- 丢弃带有路由类型报头的任何数据包。

以下是策略映射配置：

```
policy-map type inspect ipv6 _default_ipv6_map
 description Default IPV6 policy-map
 parameters
  verify-header type
  verify-header order
 match header routing-type range 0 255
  drop log
```

配置 IPv6 检测

默认情况下，IPv6 检测未启用。如果需要 IPv6 检测，必须对其进行配置。

操作步骤

步骤 1　第 8-31 页上的配置 IPv6 检测策略映射。

步骤 2　第 8-32 页上的配置 IPv6 检测服务策略。

配置 IPv6 检测策略映射

要标识要丢弃或记录的扩展报头，或者要禁用数据包验证，请创建 IPv6 检测策略映射以用于服务策略。

操作步骤

步骤 1　创建 IPv6 检测策略映射。

```
hostname(config)# policy-map type inspect ipv6 policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2　（可选）向策略映射添加描述。

```
hostname(config-pmap)# description string
```

步骤 3　（可选）根据 IPv6 消息中的报头丢弃或记录流量。

a. 根据 IPv6 报头标识流量。

```
hostname(config-pmap)# match header type
```

其中，type 是以下其中一项：

- **ah** - 匹配 IPv6 身份验证扩展报头。
- **count gt** *number* - 指定 IPv6 扩展报头的最大数量（0 至 255）。
- **destination-option** - 匹配 IPv6 目标选项扩展报头。
- **esp** - 匹配 IPv6 封装安全负载 (ESP) 扩展报头。
- **fragment** - 匹配 IPv6 分片扩展报头。
- **hop-by-hop** - 匹配 IPv6 逐跳扩展报头。
- **routing-address count gt** *number* - 设置 IPv6 路由报头类型 0 地址的最大数量（大于 0 至 255 之间的值）。
- **routing-type** {**eq** | **range**} *number* - 匹配 IPv6 路由报头类型（0 至 255）。对于范围，请用空格将各个值隔开，例如，**30 40**。

b. 指定要对匹配的数据包执行的操作。可以丢弃数据包和（可选）记录数据包，或者只记录数据包。如果未输入操作，将会记录数据包。

```
hostname(config-pmap)# {drop [log] | log}
```

c. 重复以上步骤，直至标识出所有要丢弃或记录的报头。

步骤 4　配置影响检测引擎的参数。

a. 进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **verify-header type** - 仅允许已知的 IPv6 扩展报头。
- **verify-header order** - 按照 RFC 2460 的规定实施 IPv6 扩展报头顺序。

示例

以下示例创建将会丢弃并记录带有逐跳报头、目标选项报头、路由地址报头和路由类型 0 报头的所有 IPv6 数据包。此示例还强制报头顺序和类型。

```
policy-map type inspect ipv6 ipv6-pm
 parameters
  verify-header type
  verify-header order
 match header hop-by-hop
  drop log
 match header destination-option
  drop log
 match header routing-address count gt 0
  drop log
 match header routing-type eq 0
  drop log

policy-map global_policy
 class class-default
  inspect ipv6 ipv6-pm
!
service-policy global_policy global
```

配置 IPv6 检测服务策略

IPv6 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。可以简单地编辑默认全局检测策略来添加 IPv6 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map ipv6_class_map
hostname(config-cmap)# match access-list ipv6
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 IPv6 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 IPv6 检测。

inspect ipv6 [*ipv6_policy_map*]

其中，*ipv6_policy_map* 是可选的 IPv6 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建检测策略映射的信息，请参阅第 8-31 页上的配置 IPv6 检测策略映射。

示例：

```
hostname(config-class)# no inspect ipv6
hostname(config-class)# inspect ipv6 ipv6-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 IPv6 检测策略映射，必须使用 **no inspect ipv6** 命令移除 IPv6 检测，然后为其提供新的 IPv6 检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

NetBIOS 检测

默认情况下，NetBIOS 检测已启用。NetBIOS 检测引擎根据 ASA NAT 配置转换 NetBIOS 名称服务 (NBNS) 数据包中的 IP 地址。或者可以创建策略映射以便丢弃或记录 NetBIOS 协议违规情况。

操作步骤

步骤 1　第 8-34 页上的为其他检测控制配置 NetBIOS 检测策略映射。

步骤 2　第 8-35 页上的配置 NetBIOS 检测服务策略。

为其他检测控制配置 NetBIOS 检测策略映射

要指定出现协议违规时应执行的操作，请创建 NETBIOS 检测策略映射。然后，可以在启用 NETBIOS 检测时应用所创建的检测策略映射。

操作步骤

步骤 1　创建 NetBIOS 检测策略映射。

```
hostname(config)# policy-map type inspect netbios policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 3　进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

步骤 4　指定出现 NetBIOS 协议违规时应执行的操作。

```
hostname(config-pmap-p)# protocol-violation action {drop [log] | log}
```

其中，**drop** 操作丢弃数据包。如果策略映射与流量匹配，**log** 操作将会发送系统日志消息。

示例

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation drop log

hostname(config)# policy-map netbios_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect netbios netbios_map
```

配置 NetBIOS 检测服务策略

NetBIOS 应用检测为 NetBIOS 名称服务数据包和 NetBIOS 数据报服务数据包中的嵌入式 IP 地址执行 NAT。这项检测还会检查各个数量字段和长度字段的一致性，从而强制执行协议符合性。

默认 ASA 配置包括对默认端口的 NetBIOS 检测（这项检测全局应用于所有接口）。自定义检测配置的一种常用方法是自定义默认全局策略。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map netbios_class_map
hostname(config-cmap)# match access-list netbios
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射（**match default-inspection-traffic**）。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 NetBIOS 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 NetBIOS 检测。

inspect netbios [*netbios_policy_map*]

其中，*netbios_policy_map* 是可选的 NetBIOS 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建 NetBIOS 检测策略映射的信息，请参阅第 8-34 页上的为其他检测控制配置 NetBIOS 检测策略映射。

示例：

```
hostname(config-class)# no inspect netbios
hostname(config-class)# inspect netbios netbios-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 NetBIOS 检测策略映射，必须使用 **no inspect skinny** 命令移除 NetBIOS 检测，然后为其提供新的 NetBIOS 检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

PPTP 检测

PPTP 是用于对 PPP 流量进行隧道传送的协议。PPTP 会话通常包括一个 TCP 信道和两个 PPTP GRE 隧道。TCP 信道是用于协商和管理 PPTP GRE 隧道的控制信道。GRE 隧道在两台主机之间传送 PPP 会话。

启用后，PPTP 应用检测会检查 PPTP 协议数据包，并动态创建允许 PPTP 流量所需的 GRE 连接和转换。

具体来说，ASA 检查 PPTP 版本公告和传出呼叫的请求 - 响应序列。如 RFC 2637 所要求，仅检测 PPTP 版本 1。如果任一端公布的版本不是版本 1，将会禁用对 TCP 控制信道的进一步检测。此外，会跟踪传出呼叫的请求 - 应答序列。会根据需要动态分配连接和转换，以允许后续辅助 GRE 数据流量。

要以 PAT 方式转换 PPTP 流量，必须启用 PPTP 检测引擎。此外，仅对符合如下条件的 GRE 版本执行 PAT：经过修改的（如 RFC2637 所要求）；且是通过 TCP 控制信道协商的。不会对未经修改的 GRE 版本执行 PAT（如 RFC 1701 和 RFC 1702 所要求）。

有关启用 PPTP 检测的信息，请参阅第 7-9 页上的配置应用层协议检测。

SMTP 检测和扩展 SMTP 检测

ESMTP 检测检查各种攻击，包括垃圾邮件、网络钓鱼、畸形消息攻击、缓冲区溢出 / 下溢攻击。这项检测还支持应用安全和协议符合性检查，即，会对 ESMTP 消息执行健全性检查，检测若干种攻击，阻止发件人 / 收件人，以及阻止邮件转发。

以下各节介绍 ESMTP 检测引擎。

- 第 8-37 页上的 SMTP 检测和 ESMTP 检测概述
- 第 8-37 页上的 ESMTP 检测的默认设置
- 第 8-38 页上的配置 ESMTP 检测

SMTP 检测和 ESMTP 检测概述

ESMTP 应用检测能够限制可通过 ASA 的 SMTP 命令类型以及添加监控功能，从而加强针对基于 SMTP 的攻击的防御。

ESMTP 是增强型 SMTP 协议，在大多数方面和 SMTP 类似。为方便起见，本文档中用 SMTP 来同时指代 SMTP 和 ESMTP。扩展 SMTP 的应用检测流程类似于 SMTP 应用检测，这项检测支持 SMTP 会话。扩展 SMTP 会话中使用的大多数命令与 SMTP 会话中使用的命令相同，但 ESMTP 会话的速度快很多，而且提供了更多与可靠性和安全性相关的选项，例如，传送状态通知。

扩展 SMTP 应用检测增加了对如下扩展 SMTP 命令的支持：AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS 和 VRFY。ASA 另外还支持七个 RFC 821 命令（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET），也就是说，总共支持十五个 SMTP 命令。

不支持其他扩展 SMTP 命令（例如 ATRN、ONEX、VERB、CHUNKING）和专用扩展。不受支持的命令将被转换为 X（内部服务器会拒绝这些命令）。这将会生成消息，例如 “500 Command unknown: 'XXX'.”。不完整的命令将被丢弃。

ESMTP 检测引擎将服务器 SMTP 横幅中的字符更改为星号，但对 “2”、“0”、“0” 字符除外。会忽略回车符 (CR) 和换行符 (LF)。

在 SMTP 检测启用的情况下，如果不遵守以下规则，用于交互式 SMTP 的 Telnet 会话可能会挂起：SMTP 命令长度必须至少为四个字符；必须以回车符和换行符终止；且必须在获得响应后才能发出下一个应答。

SMTP 服务器使用数字应答代码和（可选）人可读字符串来响应客户端请求。SMTP 应用检测控制和减少用户可使用的命令以及服务器返回的消息。SMTP 检测主要执行以下三项任务：

- 将 SMTP 请求限制为七个基本 SMTP 命令和八个扩展命令。
- 监控 SMTP 命令 - 响应序列。
- 生成审核线索 - 邮件地址中嵌入的无效字符被替换时，会生成审核记录 108002。有关详细信息，请参阅 RFC 821。

SMTP 检测监控以下异常签名的命令 - 响应序列：

- 截断的命令。
- 命令终止错误（不是以 <CR><LR> 终止）。
- MAIL 和 RCPT 命令指定邮件的发件人和收件人。会扫描邮件地址以检测异常字符。竖线 (|) 将被删除（更改为空格）； “<” 和 “>” 只能用于定义邮件地址（“>” 前面必须有 “<”）。
- SMTP 服务器执行的意外转换。
- 对于未知命令，ASA 会将数据包中的所有字符更改为 X。在这种情况下，服务器会对客户端生成错误代码。由于数据包发生了变化，因此必须重新计算或调整 TCP 校验和。
- TCP 数据流编辑。
- 命令管道。

ESMTP 检测的默认设置

默认情况下，ESMTP 选项检测已使用 _default_esmtp_map 检测策略映射启用。

- 会掩蔽服务器横幅。
- 会检测加密流量。
- 不会查找发件人和收件人地址中的特殊字符，不会执行任何操作。
- 会丢弃并记录命令行长度大于 512 的连接。

- 会丢弃并记录有多于 100 个收件人的连接。
- 会记录正文长度超过 998 字节的消息。
- 会丢弃并记录报头行长度大于 998 的连接。
- 会丢弃并记录 MIME 文件名超过 255 个字符的消息。
- 会掩蔽匹配 “others” 的 EHLO 应答参数。

以下是策略映射配置：

```
policy-map type inspect esmtp _default_esmtp_map
 description Default ESMTP policy-map
 parameters
  mask-banner
  no mail-relay
  no special-character
  no allow-tls
 match cmd line length gt 512
  drop-connection log
 match cmd RCPT count gt 100
  drop-connection log
 match body line length gt 998
  log
 match header line length gt 998
  drop-connection log
 match sender-address length gt 320
  drop-connection log
 match MIME filename length gt 255
  drop-connection log
 match ehlo-reply-parameter others
  mask
```

配置 ESMTP 检测

默认情况下，ESMTP 检测已启用。仅在要执行非默认检测映射流程的情况下，才需要配置这项检测。

操作步骤

步骤 1　第 8-38 页上的配置 ESMTP 检测策略映射。

步骤 2　第 8-41 页上的配置 ESMTP 检测服务策略。

配置 ESMTP 检测策略映射

要指定消息违反参数时要执行的操作，请创建 ESMTP 检测策略映射。然后，可以在启用 ESMTP 检测时应用所创建的检测策略映射。

准备工作

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

操作步骤

步骤 1　创建 ESMTP 检测策略映射，然后输入以下命令：

```
hostname(config)# policy-map type inspect esmtp policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 3　要对匹配的流量应用操作，请执行以下步骤。

a. 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match** [**not**] **body** {**length** | **line length**} **gt** *bytes* - 匹配 ESMTP 消息正文长度或其行长度大于指定字节数的消息。
- **match** [**not**] **cmd verb** *verb1* [*verb2*...] - 匹配消息中的命令谓词。可以指定以下一个或多个命令：auth、data、ehlo、etrn、helo、help、mail、noop、quit、rcpt、rset、saml、soml、vrfy。
- **match** [**not**] **cmd line length gt** *bytes* - 匹配命令谓词中行长度大于指定字节数的消息。
- **match** [**not**] **cmd rcpt count gt** *count* - 匹配收件人数量大于指定数量的消息。
- **match** [**not**] **ehlo-reply-parameter** *parameter* [*parameter2*...] - 匹配 ESMTP EHLO 应答参数。可以指定以下一个或多个参数：8bitmime、auth、binaryname、checkpoint、dsn、etrn、others、pipelining、size、vrfy。
- **match** [**not**] **header** {**length** | **line length**} **gt** *bytes* - 匹配 ESMTP 报头长度或其行长度大于指定字节数的消息。
- **match** [**not**] **header to-fields count gt** *count* - 匹配报头中 To 字段数量大于指定数量的消息。
- **match** [**not**] **invalid-recipients count gt** *number* - 匹配无效收件人数量大于指定数量的消息。
- **match** [**not**] **mime filetype regex** {*regex_name* | **class** *class_name*} - 将 MIME 或媒体文件类型与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **mime filename length gt** *bytes* - 匹配文件名长度大于指定字节数的消息。
- **match** [**not**] **mime encoding** *type* [*type2*...] - 匹配 MIME 编码类型。可以指定以下一个或多个类型：7bit、8bit、base64、binary、others、quoted-printable。
- **match** [**not**] **sender-address regex** {*regex_name* | **class** *class_name*} - 将发件人邮件地址与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **sender-address length gt** *bytes* - 匹配发件人地址长度大于指定字节数的消息。

b. 输入下列命令，以指定要对匹配流量执行的操作：

```
hostname(config-pmap-c)# {drop-connection [log] | mask [log] | reset [log] | log |
rate-limit message_rate}
```

并非所有选项对于每个 **match** 命令都可用。有关可用的确切选项，请参阅 CLI 帮助或命令参考。

- **drop-connection** 关键字丢弃数据包并关闭连接。
- **mask** 关键字掩蔽数据包的匹配部分。此操作仅适用于 **ehlo-reply-parameter** 和 **cmd verb**。

- **reset** 关键字丢弃数据包、关闭连接并向服务器和 / 或客户端发送 TCP 重置。
- 关键字 **log**（可以单独使用，也可以与其他关键字之一结合使用）用于发送系统日志消息。
- **rate-limit** *message_rate* 参数限制消息速率。此选项仅适用于 **cmd verb**（可以将其用作唯一操作，也可以将其与 **mask** 操作结合使用）。

可以在策略映射中指定多个 **match** 命令。有关 **match** 命令顺序的信息，请参阅第 2-4 页上的在检测策略映射中定义操作。

步骤 4　要配置影响检测引擎的参数，请执行以下步骤：

a. 要进入参数配置模式，请输入以下命令：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **mail-relay** *domain-name* **action** {**drop-connection** [**log**] | **log**} - 标识用于邮件转发的域名。可以断开连接和（可选）记录连接，或者只记录连接。
- **mask-banner** - 掩蔽来自 ESMTP 服务器的横幅。
- **special-character action** {**drop-connection** [**log**] | **log**} - 标识要对发件人或收件人邮件地址中包含特殊字符（竖线 (|)、反引号和空字符）的消息执行的操作。可以断开连接和（可选）记录连接，或者只记录连接。
- **allow-tls** [**action log**] - 是否允许 ESMTP 在未经检测的情况下通过 TLS（加密连接）。如有需要，可以记录加密连接。

示例

以下示例显示如何定义 ESMTP 检测策略映射。

```
hostname(config)# regex user1 "user1@cisco.com"
hostname(config)# regex user2 "user2@cisco.com"
hostname(config)# regex user3 "user3@cisco.com"
hostname(config)# class-map type regex senders_black_list
hostname(config-cmap)# description "Regular expressions to filter out undesired senders"
hostname(config-cmap)# match regex user1
hostname(config-cmap)# match regex user2
hostname(config-cmap)# match regex user3

hostname(config)# policy-map type inspect esmtp advanced_esmtp_map
hostname(config-pmap)# match sender-address regex class senders_black_list
hostname(config-pmap-c)# drop-connection log

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect esmtp advanced_esmtp_map

hostname(config)# service-policy outside_policy interface outside
```

配置 ESMTP 检测服务策略

默认 ASA 配置包括全局应用于所有接口的 ESMTP 检测。自定义检测配置的一种常用方法是自定义默认全局策略。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map esmtp_class_map
hostname(config-cmap)# match access-list esmtp
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 IP 选项检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 ESMTP 检测。

inspect esmtp [*esmtp_policy_map*]

其中，*esmtp_policy_map* 是可选的 ESMTP 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建 ESMTP 检测策略映射的信息，请参阅第 8-41 页上的配置 ESMTP 检测服务策略。

示例：

```
hostname(config-class)# no inspect esmtp
hostname(config-class)# inspect esmtp esmtp-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的检测策略映射，必须使用 **no inspect esmtp** 命令移除 ESMTP 检测，然后为其提供新的检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

TFTP 检测

默认情况下，TFTP 检测已启用。

如 RFC 1350 中所述，TFTP 是用于在 TFTP 服务器与客户端之间读取和写入文件的简单协议。

ASA 会检查 TFTP 流量，并在必要时动态创建连接和转换，以允许 TFTP 客户端与服务器之间进行文件传输。具体来说，此检测引擎检查 TFTP 读取请求 (RRQ)、写入请求 (WRQ) 和错误通知 (ERROR)。

如有必要，在接收有效的读取 (RRQ) 或写入 (WRQ) 请求时会分配动态辅助信道和 PAT 转换。随后，TFTP 会使用该辅助信道进行文件传输或错误通知。

只有 TFTP 服务器可以通过辅助信道发起流量；此外，TFTP 客户端与服务器之间最多只能有一个不完整的辅助信道。服务器发出的错误通知会致使辅助信道关闭。

如果静态 PAT 用于重定向 TFTP 流量，必须启用 TFTP 检查检测。

有关启用 TFTP 检测的信息，请参阅第 7-9 页上的配置应用层协议检测。

语音和视频协议的检测

以下主题介绍针对语音和视频协议的应用检测。有关为何需要对某些协议进行检测以及应用检测的总体方法的基本信息，请参阅第 7-1 页上的应用层协议检测入门。

- 第 9-1 页上的 CTIQBE 检测
- 第 9-3 页上的 H.323 检测
- 第 9-11 页上的 MGCP 检测
- 第 9-16 页上的 RTSP 检测
- 第 9-20 页上的 SIP 检测
- 第 9-28 页上的瘦客户端 (SCCP) 检测
- 第 9-33 页上的语音和视频协议检测的历史记录

CTIQBE 检测

CTIQBE 协议检测支持 NAT、PAT 和双向 NAT。这使得 Cisco IP SoftPhone 和其他思科 TAPI/JTAPI 应用可与 Cisco CallManager 配合使用，从而能够越过 ASA 建立呼叫。

许多思科 VoIP 应用都使用 TAPI 和 JTAPI。思科 TSP 通过 CTIQBE 与 Cisco CallManager 通信。

有关启用 CTIQBE 检测的信息，请参阅第 7-9 页上的配置应用层协议检测。

- 第 9-1 页上的 CTIQBE 检测的局限性
- 第 9-2 页上的验证和监控 CTIQBE 检测

CTIQBE 检测的局限性

下面总结了 CTIQBE 应用检测的局限性：

- CTIQBE 应用检测不支持使用 **alias** 命令的配置。
- 不支持 CTIQBE 呼叫状态故障转移。
- 输入 **debug ctiqbe** 命令可能会延迟消息传输，这在实时环境中可能会造成性能影响。如果您启用了这种调试或日志记录，但 Cisco IP SoftPhone 似乎无法通过 ASA 完成呼叫建立，请在运行 Cisco IP SoftPhone 的系统上增大思科 TSP 设置中的超时值。

下面总结了在特定情况下使用 CTIQBE 应用检测时的特殊注意事项：

- 如果两个 Cisco IP SoftPhone 注册到不同的 Cisco CallManager，而这些 Cisco CallManager 连接到 ASA 的不同接口，那么这两部电话之间的呼叫将会失败。

- 当 Cisco CallManager 位于安全性高于 Cisco IP SoftPhone 的接口上时，如果 Cisco CallManager IP 地址需要 NAT 或外部 NAT，则映射必须是静态的，因为 Cisco IP SoftPhone 要求在 PC 上的思科 TSP 配置中明确指定 Cisco CallManager IP 地址。
- 当使用 PAT 或外部 PAT 时，如果 Cisco CallManager IP 地址将被转换，它的 TCP 端口 2748 必须静态映射到 PAT（接口）地址的同一端口，这样 Cisco IP SoftPhone 注册才能成功。CTIQBE 侦听端口 (TCP 2748) 是固定的，用户不可在 Cisco CallManager、Cisco IP SoftPhone 或思科 TSP 上配置该端口。

验证和监控 CTIQBE 检测

show ctiqbe 命令显示有关越过 ASA 建立的 CTIQBE 会话的信息。此命令显示有关 CTIQBE 检测引擎分配的媒体连接的信息。

下面是 **show ctiqbe** 命令在以下条件下的输出示例。越过 ASA 仅建立了一个活动的 CTIQBE 会话。该会话建立在本地地址 10.0.0.99 的内部 CTI 设备（例如，Cisco IP SoftPhone）与地址 172.29.1.77 的外部 Cisco CallManager 之间，其中 TCP 端口 2748 是 Cisco CallManager。会话的心跳间隔为 120 秒。

```
hostname# # show ctiqbe

Total: 1
        LOCAL            FOREIGN          STATE   HEARTBEAT
-----------------------------------------------------------------
1       10.0.0.99/1117  172.29.1.77/2748        1       120
        ------------------------------------------------
        RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
        ------------------------------------------------
        MEDIA: Device ID 27     Call ID 0
               Foreign 172.29.1.99      (1028 - 1029)
               Local   172.29.1.88      (26822 - 26823)
        ------------------------------------------------
```

在本示例中，CTI 设备已注册到 CallManager。该设备的内部地址和 RTP 侦听端口通过 PAT 方式转换到 172.29.1.99 UDP 端口 1028。该设备的 RTCP 侦听端口通过 PAT 方式转换到 UDP 1029。

以 `RTP/RTCP: PAT xlates:` 开头的行仅在满足如下条件时显示：内部 CTI 设备已注册到外部 CallManager，且 CTI 设备地址和端口已通过 PAT 方式转换到该外部接口。如果 CallManager 位于内部接口上，或者，如果内部 CTI 设备地址和端口转换到 CallManager 使用的外部接口上，此行将不会显示。

该输出表示已在此 CTI 设备与位于 172.29.1.88 的另一个电话之间建立呼叫。另一个电话的 RTP 和 RTCP 侦听端口分别是 UDP 26822 和 26823。由于 ASA 不保留与第二个电话和 CallManager 相关的 CTIQBE 会话记录，因此，另一部电话和 CallManager 位于同一接口。在 CTI 设备端的活动呼叫分支可以用设备 ID 27 和呼叫 ID 0 来标识。

以下是 **show xlate debug** 命令针对这些 CTIBQE 连接的输出示例：

```
hostname# show xlate debug
3 in use, 3 most used
Flags:  D - DNS, d - dump, I - identity, i - inside, n - no random,
        r - portmap, s - static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
```

show conn state ctiqbe 命令显示 CTIQBE 连接的状态。在输出中，CTIQBE 检测引擎分配的媒体连接以 “C” 标志表示。以下是 **show conn state ctiqbe** 命令的输出示例：

```
hostname# show conn state ctiqbe
1 in use, 10 most used
hostname# show conn state ctiqbe detail
1 in use, 10 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, k - Skinny media,
       M - SMTP data, m - SIP media, O - outbound data, P - inside back connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
```

H.323 检测

以下部分介绍 H.323 应用检测。

- 第 9-3 页上的 H.323 检测概述
- 第 9-3 页上的 H.323 如何工作
- 第 9-4 页上的 H.245 消息中的 H.239 支持
- 第 9-5 页上的 H.323 检测的局限性
- 第 9-5 页上的配置 H.323 检测
- 第 9-9 页上的配置 H.323 和 H.225 超时值
- 第 9-9 页上的验证和监控 H.323 检测

H.323 检测概述

H.323 检测为符合 H.323 的应用（例如 Cisco CallManager 和 VocalTec Gatekeeper）提供支持。H.323 是国际电信联盟制定的一套协议，用于通过 LAN 进行多媒体会议。ASA 最高支持 H.323 v6，其中包括 H.323 v3 的 “ 支持在一个呼叫信令信道上进行多个呼叫 ” 功能。

启用 H.323 检测后，ASA 支持在同一呼叫信令信道上进行多个呼叫（此功能在 H.323 v3 中引入）。此功能可缩短呼叫建立时间并减少 ASA 上端口的使用。

H.323 检测具有如下两个主要功能：

- 对 H.225 和 H.245 消息中必要的嵌入式 IPv4 地址进行 NAT 转换。由于 H.323 消以 PER 编码格式进行编码，因此，ASA 使用 ASN.1 解码器来解码 H.323 消息。
- 动态分配协商的 H.245 和 RTP/RTCP 连接。使用 RAS 时，也可以动态分配 H.225 连接。

H.323 如何工作

H.323 协议集合总共最多可以使用两个 TCP 连接和四到八个 UDP 连接。FastConnect 仅使用一个 TCP 连接，且 RAS 使用单个 UDP 连接用于注册、准入和状态。

首先，H.323 客户端可以使用 TCP 端口 1720 建立与 H.323 服务器之间的 TCP 连接，以请求 Q.931 呼叫建立。作为呼叫建立流程的一部分，H.323 终端会向客户端提供用于 H.245 TCP 连接的端口号。在使用 H.323 网守的环境中，初始数据包通过 UDP 进行传输。

H.323 检测会监控 Q.931 TCP 连接，以确定 H.245 端口号。如果 H.323 终端不使用 FastConnect，ASA 会根据 H.225 消息的检测情况动态分配 H.245 连接。

注　使用 RAS 时，也可以动态分配 H.225 连接。

在每个 H.245 消息中，H.323 终端交换用于后续 UDP 数据流的端口号。H.323 检测会检测 H.245 消息来标识这些端口，并动态创建用于媒体交换的连接。RTP 使用协商的端口号，而 RTCP 使用下一个更高的端口号。

H.323 控制信道处理 H.225、H.245 和 H.323 RAS。H.323 检测使用以下端口。

- 1718 - 网守发现 UDP 端口
- 1719 - RAS UDP 端口
- 1720 - TCP 控制端口

要实现 RAS 信令，必须允许已知 H.323 端口 1719 的流量。此外，要实现 H.225 呼叫信令，必须允许已知 H.323 端口 1720 的流量；但是，H.245 信令端口在 H.225 信令中的终端之间协商。如果有使用 H.323 网守，ASA 会根据 ACF 和 RCF 消息的检测情况打开 H.225 连接。

检测 H.225 消息后，ASA 会打开 H.245 信道，然后检测通过 H.245 信道发送的流量。所有通过 ASA 的 H.245 消息都要接受 H.245 应用检测，这项检测会转换嵌入式 IP 地址并打开 H.245 消息中协商的媒体信道。

H.323 ITU 标准要求，定义消息长度的 TPKT 报头在传递到可靠连接之前应先于 H.225 和 H.245。由于 TPKT 报头不一定要在 H.225 和 H.245 消息所在的 TCP 数据包中发送，因此，ASA 必须记住 TPKT 长度，以便正确处理和解码消息。对于每个连接，ASA 会保留包含下一个预期消息的 TPKT 长度的记录。

如果 ASA 需要对消息中的 IP 地址执行 NAT，它会更改校验和、UUIE 长度和 TPKT（如果 TPKT 和 H.225 消息位于同一个 TCP 数据包中）。如果 TPKT 在单独的 TCP 数据包中发送，ASA 代理会确认该 TPKT，并将具有新长度的新 TPKT 附加到 H.245 消息。

注　在针对 TPKT 的代理确认中，ASA 不支持 TCP 选项。

每个具有通过 H.323 检测的数据包的 UDP 连接将被标记为 H.323 连接，每个这些连接的超时为 **timeout** 命令配置的 H.323 超时。

注　如果网守在网络内部，可以在 H.323 终端之间启用呼叫建立。ASA 包含用于根据 RegistrationRequest/RegistrationConfirm (RRQ/RCF) 消息为呼叫打开针孔的选项。由于这些 RRQ/RCF 消息在终端与网守之间来回发送，因此，呼叫终端的 IP 地址是未知的，ASA 则会通过源 IP 地址 / 端口 0/0 打开针孔。默认情况下，此选项已禁用。要在 H.323 终端之间启用呼叫建立，请在创建 H.323 检测策略映射时，在参数配置模式期间输入 **ras-rcf-pinholes enable** 命令。请参阅第 9-5 页上的配置 H.323 检测策略映射。

H.245 消息中的 H.239 支持

ASA 位于两个 H.323 终端之间。两个 H.323 终端建立电话演示会话并可以相互之间发送和接收数据演示（例如电子表格数据）后，ASA 会确保这些终端之间可实现成功 H.239 协商。

H.239 是一项标准，使 H.300 系列终端能够在单个呼叫中打开另外一个视频信道。在呼叫中，终端（例如视频电话）会发送视频信道和数据演示信道。H.239 协商在 H.245 信道上发生。

ASA 打开用于另外一个媒体信道和媒体控制信道的针孔。终端使用开放逻辑信道 (OLC) 消息来发出有关新信道创建的信息。消息扩展是 H.245 v13 的一部分。

默认情况下，电话演示会话的解码和编码已启用。H.239 的编码和解码由 ASN.1 编码器执行。

H.323 检测的局限性

H.323 检测已经过测试，受 Cisco Unified Communications Manager (CUCM) 7.0 支持。CUCM 8.0 及更高版本不支持这项检测。H.323 检测可能适用于其他版本和产品。

以下是 H.323 应用检测的一些已知问题和局限性：

- 仅完全支持静态 NAT。静态 PAT 可能无法正确转换 H.323 消息内嵌入到可选字段中的 IP 地址。如果遇到这种问题，请勿对 H.323 使用静态 PAT。
- 不支持动态 NAT 或 PAT。
- 不支持扩展 PAT。
- 不支持同一安全级别接口之间的 NAT。
- 不支持外部 NAT。
- 不支持 NAT64。
- 如果 NetMeeting 客户端已注册到 H.323 网守，并尝试呼叫也已注册到 H.323 网守的 H.323 网关，将会建立连接，但两端都不会听到语音。这个问题与 ASA 无关。
- 如果将网络静态地址配置为与第三方子网掩码和地址相同，任何出站 H.323 连接都将失败。

配置 H.323 检测

H.323 检测支持 RAS、H.225 和 H.245，这项检测会转换所有嵌入式 IP 地址和端口。它执行状态跟踪和过滤，并且可以级联检测功能激活。H.323 检测支持电话号码过滤、动态 T.120 控制、H.245 隧道控制、HSI 组、协议状态跟踪、H.323 呼叫持续时间实施和音频 / 视频控制。

默认情况下，H.323 检测已启用。仅在需要非默认处理的情况下，才需要配置这项检测。如果要自定义 H.323 检测，请按照以下流程进行操作。

操作步骤

步骤 1　第 9-5 页上的配置 H.323 检测策略映射

步骤 2　第 9-8 页上的配置 H.323 检测服务策略

配置 H.323 检测策略映射

如果默认检测行为不能满足网络要求，可以创建 H.323 检测策略映射来自定义 H.323 检测操作。

在定义流量匹配条件时，可以创建类映射或者直接在策略映射中包括匹配语句。以下操作步骤说明这两种方法。

准备工作

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

操作步骤

步骤 1　（可选）执行以下步骤创建 H.323 检测类映射。

类映射对多个流量匹配进行分组。或者，可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定字符串 “example.com”，则任何包含 “example.com” 的流量都不匹配类映射。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a. 输入以下命令创建类映射：

```
hostname(config)# class-map type inspect h323 [match-all | match-any] class_map_name
hostname(config-cmap)#
```

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。关键字 **match-any** 指定如果流量匹配至少一个条件，则匹配类映射。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b. （可选）要向类映射添加描述，请输入以下命令：

```
hostname(config-cmap)# description string
```

其中，*string* 是对类映射的描述（最多可包含 200 个字符）。

c. 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*} - 将被叫方与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*} - 将主叫方与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **media-type** {**audio** | **data** | **video**} - 匹配媒体类型。

步骤 2　创建 H.323 检测策略映射：

```
hostname(config)# policy-map type inspect h323 policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 4　要对匹配的流量应用操作，请执行以下步骤。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅第 2-4 页上的在检测策略映射中定义操作。

a. 使用以下其中一种方法指定要对其执行操作的流量：

- 如果已创建 H.323 类映射，请输入以下命令指定该类映射：

  ```
  hostname(config-pmap)# class class_map_name
  hostname(config-pmap-c)#
  ```

- 要直接在策略映射中指定流量，请对 H.323 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b. 输入下列命令，以指定要对匹配流量执行的操作：

```
hostname(config-pmap-c)# {drop [log] | drop-connection | reset}
```

drop 关键字丢弃数据包。对于媒体类型匹配，可以包括 **log** 关键字以发送系统日志消息。

drop-connection 关键字丢弃数据包并关闭连接。此选项适用于被叫方匹配或主叫方匹配。

reset 关键字丢弃数据包、关闭连接并向服务器和 / 或客户端发送 TCP 重置。此选项适用于被叫方匹配或主叫方匹配。

步骤 5　要配置影响检测引擎的参数，请执行以下步骤：

a. 要进入参数配置模式，请输入以下命令：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **ras-rcf-pinholes enable** - 启用 H.323 终端之间的呼叫建立。如果网守在网络内部，可以在 H.323 终端之间启用呼叫建立。使用此选项可根据 RegistrationRequest/RegistrationConfirm (RRQ/RCF) 消息为呼叫打开针孔。由于这些 RRQ/RCF 消息在终端与网守之间来回发送，因此，呼叫终端的 IP 地址是未知的，ASA 则会通过源 IP 地址 / 端口 0/0 打开针孔。默认情况下，此选项已禁用。
- **timeout users** *time* - 设置 H.323 呼叫持续时间限制（格式为 hh:mm:ss）。如果不想设置超时，请指定 00:00:00。超时范围是 0:0:0 到 1193:0:0。
- **call-party-number** - 在呼叫建立过程中强制发送主叫方号码。
- **h245-tunnel-block action** {**drop-connection** | **log**} - 强制阻止 H.245 隧道。指定是要断开连接还是仅记录连接。
- **rtp-conformance** [**enforce-payloadtype**] - 检查流经针孔的 RTP 数据包的协议符合性。可选的 **enforce-payloadtype** 关键字根据信令交换将负载类型强制为音频或视频。
- **state-checking** {**h225** | **ras**} - 启用状态检查验证。可以分别为 H.225 和 RAS 输入此命令来启用状态检查。

步骤 6　可以在仍处于参数配置模式下时配置 HSI 组。

a. 定义 HSI 组并进入 HSI 组配置模式。

```
hostname(config-pmap-p)# hsi-group id
```

其中，*id* 是 HSI 组的 ID。ID 范围是 0 到 2147483647。

b. 使用 IP 地址向 HSI 组添加 HSI。每个 HSI 组最多可以添加 5 台主机。

```
hostname(config-h225-map-hsi-grp)# hsi ip_address
```

c. 向 HSI 组添加终端。

```
hostname(config-h225-map-hsi-grp)# endpoint ip_address if_name
```

其中，*ip_address* 是要添加的终端，*if_name* 是该终端连接到 ASA 所通过的接口。每个 HSI 组最多可以添加 10 个终端。

示例

以下示例显示如何配置电话号码过滤：

```
hostname(config)# regex caller 1 "5551234567"
hostname(config)# regex caller 2 "5552345678"
hostname(config)# regex caller 3 "5553456789"

hostname(config)# class-map type inspect h323 match-all h323_traffic
hostname(config-pmap-c)# match called-party regex caller1
hostname(config-pmap-c)# match calling-party regex caller2

hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# class h323_traffic
hostname(config-pmap-c)# drop
```

配置 H.323 检测服务策略

默认 ASA 配置包括对默认端口的 H.323 H.255 和 RAS 检测（这两项检测全局应用于所有接口）。自定义检测配置的一种常用方法是自定义默认全局策略。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map h323_class_map
hostname(config-cmap)# match access-list h323
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 H.323 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 H.323 检测

inspect h323 {**h255** | **ras**} [*h323_policy_map*]

其中，*h323_policy_map* 是可选的 H.323 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建 H.323 检测策略映射的信息，请参阅第 9-5 页上的配置 H.323 检测策略映射。

示例：

```
hostname(config-class)# no inspect h323 h225
hostname(config-class)# no inspect h323 ras
hostname(config-class)# inspect h255 h323-map
hostname(config-class)# inspect ras h323-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 H.323 检测策略映射，必须使用 **no inspect h323** 命令移除 H.323 检测，然后为其提供新的 H.323 检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

配置 H.323 和 H.225 超时值

可以在 **Configuration > Firewall > Advanced > Global Timeouts** 页面上配置 H.323/H.255 全局超时值。可以设置 H.255 信令连接关闭前的非活动时间间隔（默认值为 1 小时）或 H.323 控制连接关闭前的非活动时间间隔（默认为 5 分钟）。

要配置 H.225 信令连接关闭前的空闲时间，请使用 **timeout h225** 命令。H.225 超时默认值为 1 小时。

要配置 H.323 控制连接关闭之前允许的空闲时间，请使用 **timeout h323** 命令。默认值为 5 分钟。

验证和监控 H.323 检测

以下各节介绍如何显示有关 H.323 会话的信息。

- 第 9-10 页上的监控 H.225 会话
- 第 9-10 页上的监控 H.245 会话
- 第 9-11 页上的监控 H.323 RAS 会话

监控 H.225 会话

show h225 命令显示有关越过 ASA 建立的 H.225 会话的信息。与 **debug h323 h225 event**、**debug h323 h245 event** 和 **show local-host** 命令一样，此命令也用于排解 H.323 检测引擎问题。

如果存在异常大量的连接，请根据默认超时值或设置的超时值检查会话是否超时。如果会话未超时，则表示存在需要调查的问题。

以下是 **show h225** 命令的输出示例：

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
    1. CRV 9861
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
    Local:   10.130.56.4/1050   Foreign: 172.30.254.205/1720
```

此输出表示目前有 1 个活动 H.323 呼叫正通过本地终端 10.130.56.3 与外部主机 172.30.254.203 之间的 ASA，而且对于这些特定终端，在它们之间有 1 个并发呼叫，该呼叫的 CRV 为 9861。

对于本地终端 10.130.56.4 和外部主机 172.30.254.205，有 0 个并发呼叫。这意味着即使 H.225 会话仍然存在，终端之间也不会有活动呼叫。如果在输入 **show h225** 命令时呼叫已结束，但 H.225 会话仍未删除，可能会发生这种情况。或者，这可能意味着，这两个终端之间仍存在打开的 TCP 连接，因为它们将 “maintainConnection” 设置为 TRUE，所以，会话一直保持打开，直至它们重新将 “maintainConnection” 设为 FALSE，或者直至会话根据配置中的 H.225 超时值超时。

监控 H.245 会话

show h245 命令显示有关终端使用慢启动越过 ASA 建立的 H.245 会话的信息。当呼叫的两个终端打开 H.245 的另一 TCP 控制信道，即为慢启动。当 H.245 消息作为 H.225 消息的一部分在 H.225 控制信道上交换，即为快启动。

以下是 **show h245** 命令的输出示例：

```
hostname# show h245
Total: 1
        LOCAL            TPKT    FOREIGN          TPKT
1       10.130.56.3/1041         0       172.30.254.203/1245    0
        MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
                       Local   10.130.56.3 RTP 49608 RTCP 49609
        MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
                       Local   10.130.56.3 RTP 49606 RTCP 49607
```

在此示例中，当前只有一个越过 ASA 的处于活动状态的 H.245 控制会话。本地终端是 10.130.56.3，来自此终端的下一个数据包预计将会包含 TPKT 报头，因为 TPKT 值为 0。TKTP 报头是位于每条 H.225/H.245 消息之前的 4 字节报头。TKTP 报头提供消息长度（包括 4 字节报头在内）。外部主机终端是 172.30.254.203，来自此终端的下一个数据包预计将会包含 TPKT 报头，因为 TPKT 值为 0。

在这些终端之间协商的媒体的 LCN 为 258，该 LCN 的外部 RTP IP 地址 / 端口对为 172.30.254.203/49608，RTCP IP 地址 / 端口对为 172.30.254.203/49609，本地 RTP IP 地址 / 端口对为 10.130.56.3/49608，RTCP 端口为 49609。

第二个 LCN 为 259，该 LCN 的外部 RTP IP 地址 / 端口对为 172.30.254.203/49606，RTCP IP 地址 / 端口对为 172.30.254.203/49607，本地 RTP IP 地址 / 端口对为 10.130.56.3/49606，RTCP 端口为 49607。

监控 H.323 RAS 会话

show h323-ras 命令显示有关越过 ASA 在网守与其 H.323 终端之间建立的 H.323 RAS 会话的连接信息。与 **debug h323 ras event** 和 **show local-host** 命令一样，此命令也用于排解 H.323 RAS 检测引擎问题。

以下是 **show h323-ras** 命令的输出示例：

```
hostname# show h323-ras
Total: 1
        GK                      Caller
        172.30.254.214 10.130.56.14
```

此输出显示网守 172.30.254.214 与其客户端 10.130.56.14 之间有一个活动注册。

MGCP 检测

以下各节介绍 MGCP 应用检测。

- 第 9-11 页上的 MGCP 检测概述
- 第 9-12 页上的配置 MGCP 检测
- 第 9-15 页上的配置 MGCP 超时值
- 第 9-15 页上的验证和监控 MGCP 检测

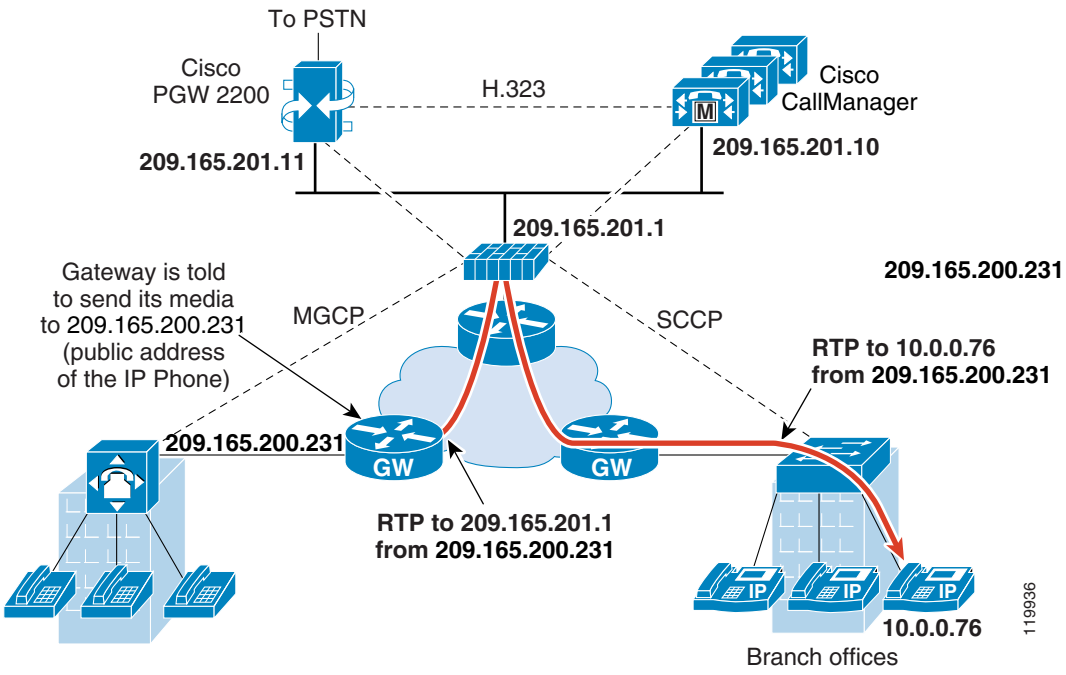
MGCP 检测概述

MGCP 是一个主 / 从协议，用于控制来自称为媒体网关控制器或呼叫代理的外部呼叫控制元件的媒体网关。媒体网关通常是一个网络元素，用于在电话电路上传送的音频信号和互联网上或其他数据包网络上传送的数据包之间提供转换。借助具有 MGCP 的 NAT 和 PAT，可以使用一组有限的外部（全局）地址来支持内部网络中的大量设备。下面列举了一些媒体网关：

- 中继网关：用于在电话网络和 IP 语音网络之间建立连接。这种网关通常管理大量的数字电路。
- 家庭网关：提供用于连接到 IP 语音网络的传统模拟 (RJ11) 接口。电缆调制解调器 / 电缆机顶盒、xDSL 设备、宽带无线设备都是家庭网关。
- 企业网关：提供用于连接到 IP 语音网络的传统数字 PBX 接口或集成 soft PBX 接口。

MGCP 消息通过 UDP 传输。响应发回到命令的源地址（IP 地址和 UDP 端口号），但是响应可能不来自命令发送到的那个地址。如果在同一故障转移配置中使用多个呼叫代理，且接收命令的呼叫代理已经将控制转交给备用呼叫代理，由备用呼叫代理来发送响应，可能会发生这种情况。下图说明如何配合使用 NAT 与 MGCP。

图 9-1　　配合使用 NAT 与 MGCP



MGCP 终端是数据的物理或虚拟源及目标。媒体网关包含终端，呼叫代理可以在这些终端上创建、修改和删除连接，从而建立并控制与其他多媒体终端之间的媒体会话。此外，呼叫代理可以指示终端检测特定事件和生成信号。终端会自动将服务状态变化情况告知呼叫代理。

- 网关通常会侦听 UDP 端口 2427 以接收来自呼叫代理的命令。
- 呼叫代理所在的端口接收来自网关的命令。呼叫代理通常会侦听 UDP 端口 2727 以接收来自网关的命令。

注　MGCP 检测不支持对 MGCP 信令和 RTP 数据使用不同的 IP 地址。建议的常见做法是，从弹性 IP 地址（例如，环回或虚拟 IP 地址）发送 RTP 数据；但是，ASA 要求 RTP 数据来自与 MGCP 信令相同的地址。

配置 MGCP 检测

可按照以下过程启用 MGCP 检测。

操作步骤

步骤 1　第 9-13 页上的为其他检测控制配置 MGCP 检测策略映射。

步骤 2　第 9-14 页上的配置 MGCP 检测服务策略。

为其他检测控制配置 MGCP 检测策略映射

如果网络有 ASA 必须为其打开针孔的多个呼叫代理和网关，应创建 MGCP 映射。然后，可以在启用 MGCP 检测时应用所创建的 MGCP 映射。

操作步骤

步骤 1　要创建 MGCP 检测策略映射，请输入以下命令：

```
hostname(config)# policy-map type inspect mgcp map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 3　进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

步骤 4　设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项。

- **call-agent** *ip_address group_id* - 配置可以管理一个或多个网关的呼叫代理组。呼叫代理组信息用于为组内的呼叫代理打开连接（而不是只为网关向其发送命令的那个呼叫代理打开连接），以使任何呼叫代理都可以发送响应。具有相同 *group_id* 的呼叫代理属于同一组。一个呼叫代理可以同时属于多个组。*group_id* 选项是介于 0 到 4294967295 之间的数字。*ip_address* 选项指定呼叫代理的 IP 地址。

  注　MGCP 呼叫代理发送 AUEP 消息以确定 MGCP 终端是否存在。这将建立通过 ASA 的流量并允许 MGCP 终端注册到呼叫代理。

- **gateway** *ip_address group_id* - 标识哪个呼叫代理组在管理特定网关。*ip_address* 选项指定网关的 IP 地址。*group_id* 选项是介于 0 到 4294967295 之间的数字，而且必须对应于管理网关的呼叫代理的 *group_id*。一个网关只能属于一个组。
- **command-queue** *command_limit* - 设置 MGCP 命令队列允许的最大命令数，范围是 1 到 2147483647。默认值为 200。

示例

以下示例显示如何定义 MGCP 映射：

```
hostname(config)# policy-map type inspect mgcp sample_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-agent 10.10.11.5 101
hostname(config-pmap-p)# call-agent 10.10.11.6 101
hostname(config-pmap-p)# call-agent 10.10.11.7 102
hostname(config-pmap-p)# call-agent 10.10.11.8 102
hostname(config-pmap-p)# gateway 10.10.10.115 101
hostname(config-pmap-p)# gateway 10.10.10.116 102
hostname(config-pmap-p)# gateway 10.10.10.117 102
hostname(config-pmap-p)# command-queue 150
```

配置 MGCP 检测服务策略

MGCP 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。但是，默认检测类包括默认 MGCP 端口，因此，只需简单地编辑默认全局检测策略即可添加 MGCP 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map mgcp_class_map
hostname(config-cmap)# match access-list mgcp
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 MGCP 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 MGCP 检测。

inspect mgcp [*mgcp_policy_map*]

其中，*mgcp_policy_map* 是可选的 MGCP 检测策略映射。有关创建 MGCP 检测策略映射的信息，请参阅第 9-13 页上的为其他检测控制配置 MGCP 检测策略映射。

示例：

```
hostname(config-class)# no inspect mgcp
hostname(config-class)# inspect mgcp mgcp-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 MGCP 检测策略映射，必须使用 **no inspect mgcp** 命令移除 MGCP 检测，然后为其提供新的 MGCP 检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

配置 MGCP 超时值

可以在 **Configuration > Firewall > Advanced > Global Timeouts** 页面上配置多个 MGCP 全局超时值。可以设置 MGCP 媒体连接关闭前的非活动时间间隔（默认值为 5 分钟）。还可以设置 PAT 转换的超时（30 秒）。

timeout mgcp 命令可用于设置 MGCP 媒体连接关闭前的非活动时间间隔。默认值为 5 分钟。

timeout mgcp-pat 命令可用于设置 PAT 转换的超时。由于 MGCP 没有保持连接机制，因此，如果使用非思科 MGCP 网关（呼叫代理），PAT 转换将会在默认超时间隔（30 秒）后断开。

验证和监控 MGCP 检测

show mgcp commands 命令列出命令队列中的 MGCP 命令数。**show mgcp sessions** 命令列出现有的 MGCP 会话数。**detail** 选项包括有关输出中每个命令（或会话）的额外信息。以下是 **show mgcp commands** 命令的输出示例：

```
hostname# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
```

以下是 **show mgcp detail** 命令的输出示例。

```
hostname# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
       Gateway IP      host-pc-2
       Transaction ID  2052
       Endpoint name   aaln/1
       Call ID         9876543210abcdef
       Connection ID
       Media IP        192.168.5.7
       Media port      6058
```

以下是 **show mgcp sessions** 命令的输出示例。

```
hostname# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
```

以下是 **show mgcp sessions detail** 命令的输出示例。

```
hostname# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
```

```
Gateway IP      host-pc-2
Call ID         9876543210abcdef
Connection ID   6789af54c9
Endpoint name   aaln/1
Media lcl port  6166
Media rmt IP    192.168.5.7
Media rmt port  6058
```

RTSP 检测

以下各节介绍 RTSP 应用检测。

- 第 9-16 页上的 RTSP 检测概述
- 第 9-16 页上的 RealPlayer 配置要求
- 第 9-17 页上的 RSTP 检测的局限性
- 第 9-17 页上的配置 RTSP 检测

RTSP 检测概述

RTSP 检测引擎使 ASA 可以传递 RTSP 数据包。RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer 和思科 IP/TV 连接都使用 RTSP。

注　对于思科 IP/TV，请使用 RTSP TCP 端口 554 和 8554。

RTSP 应用使用已知 TCP 端口 554（很少用 UDP）作为控制信道。ASA 仅支持 TCP（这符合 RFC 2326 的要求）。该 TCP 控制信道用于根据客户端配置的传输模式协商用于传输音频 / 视频流量的数据信道。

支持如下 RDT 传输：rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp 和 x-pn-tng/udp。

ASA 解析状态代码为 200 的 Setup 响应消息。如果响应消息为入站消息，服务器相对于 ASA 为外部设备，则需要为来自服务器的入站连接打开动态信道。如果响应消息为出站消息，ASA 将无需打开动态信道。

由于 RFC 2326 不要求客户端和服务器端口必须处于 SETUP 响应消息中，因此，ASA 会保持状态并记住 SETUP 消息中的客户端端口。QuickTime 将客户端端口置于 SETUP 消息中，这样，服务器仅会使用服务器端口作出响应。

RTSP 检测不支持 PAT 或双 NAT。此外，ASA 无法识别 HTTP 掩蔽（即，RTSP 消息隐藏在 HTTP 消息中）。

RealPlayer 配置要求

使用 RealPlayer 时，正确配置传输模式非常重要。对于 ASA，应从服务器向客户端添加 **access-list** 命令；反之亦然。对于 RealPlayer，可点击 **Options>Preferences>Transport>RTSP Settings** 更改传输模式。

如果 RealPlayer 使用 TCP 模式，请选择 **Use TCP to Connect to Server** 和 **Attempt to use TCP for all content** 复选框。在 ASA 中，无需配置检测引擎。

如果 RealPlayer 使用 UDP 模式，请选择 **Use TCP to Connect to Server** 和 **Attempt to use UDP for static content** 复选框，而且直播内容不可进行组播。在 ASA 中，应添加 **inspect rtsp** *port* 命令。

RSTP 检测的局限性

RSTP 检测有以下局限性。

- ASA 不支持通过 UDP 组播 RTSP 或 RTSP 消息。
- ASA 不能识别 HTTP 掩蔽（即，RTSP 消息隐藏在 HTTP 消息中）。
- 由于嵌入式 IP 地址作为 HTTP 或 RTSP 消息的一部分包含在 SDP 文件中，因此，ASA 无法对 RTSP 消息执行 NAT。数据包可以分片，但 ASA 无法对分片数据包执行 NAT。
- 对于思科 IP/TV，ASA 在消息的 SDP 部分上转换的数量与内容管理器中的节目列表数成正比（每个节目列表可至少有六个嵌入式 IP 地址）。
- 可以为 Apple QuickTime 4 或 RealPlayer 配置 NAT。如果查看器和内容管理器位于外部网络，而服务器位于内部网络，则思科 IP/TV 只能采用 NAT。

配置 RTSP 检测

默认情况下，RTSP 检测已启用。仅在需要非默认处理的情况下，才需要配置这项检测。如果要自定义 RTSP 检测，请按照以下流程进行操作。

操作步骤

步骤 1　第 9-17 页上的配置 RTSP 检测策略映射

步骤 2　第 9-19 页上的配置 RTSP 检测服务策略

配置 RTSP 检测策略映射

如果默认检测行为不能满足网络要求，可以创建 RTSP 检测策略映射来自定义 RTSP 检测操作。

在定义流量匹配条件时，可以创建类映射或者直接在策略映射中包括匹配语句。以下操作步骤说明这两种方法。

准备工作

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

操作步骤

步骤 1　（可选）执行以下步骤创建 RTSP 检测类映射。

类映射对多个流量匹配进行分组。或者，可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定字符串 “example.com”，则任何包含 “example.com” 的流量都不匹配类映射。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a. 输入以下命令创建类映射：

```
hostname(config)# class-map type inspect rtsp [match-all | match-any] class_map_name
hostname(config-cmap)#
```

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。关键字 **match-any** 指定如果流量匹配至少一个条件，则匹配类映射。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b. （可选）要向类映射添加描述，请输入以下命令：

```
hostname(config-cmap)# description string
```

c. 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match** [**not**] **request-method** *method* - 匹配 RTSP 请求方法。这些方法包括：announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameter、teardown。
- **match** [**not**] **url-filter regex** {*regex_name* | **class** *class_name*} - 将 URL 与指定的正则表达式或正则表达式类进行匹配。

步骤 2　要创建 RTSP 检测策略映射，请输入以下命令：

```
hostname(config)# policy-map type inspect rtsp policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 4　要对匹配的流量应用操作，请执行以下步骤。

a. 使用以下其中一种方法指定要对其执行操作的流量：

- 如果已创建 RTSP 类映射，请输入以下命令指定该类映射：

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- 要直接在策略映射中指定流量，请对 RTSP 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b. 输入下列命令，以指定要对匹配流量执行的操作：

```
hostname(config-pmap-c)# {drop-connection [log] | log | rate-limit message_rate}
```

drop-connection 关键字丢弃数据包并关闭连接。此选项适用于 URL 匹配。

log 关键字（可以单独使用，也可以与 **drop-connection** 关键字结合使用）发送系统日志消息。

rate-limit *message_rate* 参数限制每秒消息速率。此选项适用于请求方法匹配。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅第 2-4 页上的在检测策略映射中定义操作。

步骤 5　要配置影响检测引擎的参数，请执行以下步骤：

a. 要进入参数配置模式，请输入以下命令：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **reserve-port-protect** - 在媒体协商期间限制保留端口的使用。
- **url-length-limit** *bytes* - 设置消息中使用的 URL 的长度限制（0 到 6000 字节）。

示例

以下示例显示如何定义 RTSP 检测策略映射。

```
hostname(config)# regex badurl1 www.url1.com/rtsp.avi
hostname(config)# regex badurl2 www.url2.com/rtsp.rm
hostname(config)# regex badurl3 www.url3.com/rtsp.asp

hostname(config)# class-map type regex match-any badurl-list
hostname(config-cmap)# match regex badurl1
hostname(config-cmap)# match regex badurl2
hostname(config-cmap)# match regex badurl3

hostname(config)# policy-map type inspect rtsp rtsp-filter-map
hostname(config-pmap)# match url-filter regex class badurl-list
hostname(config-pmap-p)# drop-connection

hostname(config)# class-map rtsp-traffic-class
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map rtsp-traffic-policy
hostname(config-pmap)# class rtsp-traffic-class
hostname(config-pmap-c)# inspect rtsp rtsp-filter-map

hostname(config)# service-policy rtsp-traffic-policy global
```

配置 RTSP 检测服务策略

默认 ASA 配置包括对默认端口的 RTSP 检测（这项检测全局应用于所有接口）。自定义检测配置的一种常用方法是自定义默认全局策略。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map rtsp_class_map
hostname(config-cmap)# match access-list rtsp
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 RTSP 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 RTSP 检测。

inspect rtsp [*rtsp_policy_map*]

其中，*rtsp_policy_map* 是可选的 RTSP 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建 RTSP 检测策略映射的信息，请参阅第 9-17 页上的配置 RTSP 检测策略映射。

示例：

```
hostname(config-class)# no inspect rtsp
hostname(config-class)# inspect rtsp rtsp-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 RTSP 检测策略映射，必须使用 **no inspect rtsp** 命令移除 RTSP 检测，然后为其提供新的 RTSP 检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

SIP 检测

SIP 是一种广泛用于网络会议、电话、展示、事件通知和即时消息的协议。由于 SIP 本质上是文本协议，而且具有灵活性，因此，SIP 网络面临大量安全威胁。

SIP 应用检测会在消息报头和正文中提供地址转换，会动态打开端口，还会执行基本健全性检查。它还支持应用安全和协议符合性（此功能强制对 SIP 消息进行健全性检查，以及检测基于 SIP 的攻击）。

默认情况下，SIP 检测已启用。只有需要非默认处理时，或者要标识 TLS 代理来启用加密流量检测时，才需要配置这项检测。以下主题详细说明 SIP 检测。

- 第 9-21 页上的 SIP 检测概述
- 第 9-21 页上的 SIP 检测的局限性
- 第 9-22 页上的 SIP 即时消息
- 第 9-22 页上的默认 SIP 检测
- 第 9-23 页上的配置 SIP 检测
- 第 9-27 页上的配置 SIP 超时值
- 第 9-27 页上的验证和监控 SIP 检测

SIP 检测概述

如 IETF 所定义，SIP 能够实现呼叫处理会话，特别是双方音频会议（又称为“通话”）。SIP 可与 SDP 配合使用来实现呼叫信令。SDP 指定用于媒体流的端口。借助 SIP，ASA 可以支持任何 SIP VoIP 网关和 VoIP 代理服务器。SIP 和 SDP 在以下 RFC 中定义：

- SIP：会话初始协议，RFC 3261
- SDP：会话描述协议，RFC 2327

要支持通过 ASA 的 SIP 呼叫，必须检测媒体连接地址的信令消息、媒体端口和媒体的初期连接，因为发送信令到已知目标端口 (UDP/TCP 5060) 的同时，也会动态分配媒体流。此外，SIP 还会在 IP 数据包的用户数据部分嵌入 IP 地址。请注意，ASA 支持的 SIP 请求 URI 的最大长度为 255。

SIP 检测的局限性

SIP 检测适用于嵌入式 IP 地址的 NAT。但是，如果配置 NAT 来转换源地址和目标地址，将不会重写外部地址（“trying” 响应消息的 SIP 报头中的 “from”）。因此，在处理 SIP 流量时应使用对象 NAT，从而避免转换目标地址。

对 SIP 使用 PAT 时，有以下限制：

- 如果远程终端尝试注册到受 ASA 保护的网络中的 SIP 代理，在某些非常特定的情况下，注册会失败，如下所示：
  - 对远程终端配置了 PAT。
  - SIP 注册服务器位于外部网络。
  - 终端发送到代理服务器的 REGISTER 消息中的联系人字段缺少端口。
- 如果 SIP 设备传输的数据包中 SDP 部分在所有者 / 创建者字段 (o=) 中有一个 IP 地址，且该 IP 地址不同于在连接字段 (c=) 中的 IP 地址，则在 o= 字段中的 IP 地址可能无法正确转换。这是 SIP 协议的如下局限性造成的：不在 o= 字段中提供端口值。
- 使用 PAT 时，任何包含无端口的内部 IP 地址的 SIP 报头字段可能不会转换，因此，内部 IP 地址将向外泄漏。如果要避免这种泄漏，请配置 NAT 来代替 PAT。

SIP 即时消息

即时消息 (IM) 是指消息在用户之间以近实时的方式传输。SIP 仅支持 Windows XP 上使用 Windows Messenger RTC Client v4.7.0105 的聊天功能。MESSAGE/INFO 方法和 202 Accept 响应用于支持 IM，如以下 RFC 所定义：

- 会话初始协议 (SIP) - 特定事件通知，RFC 3265
- 会话初始协议 (SIP) 即时消息扩展，RFC 3428

MESSAGE/INFO 请求可以在注册 / 订用后随时进入。例如，两个用户可以随时在线，但几个小时都不聊天。因此，SIP 检测引擎会根据配置的 SIP 超时值打开超时的针孔。该值必须配置为比订用持续时间至少长 5 分钟。订用持续时间在 Contact Expires 值中定义，通常是 30 分钟。

由于 MESSAGE/INFO 请求通常使用动态分配的端口（而不是端口 5060）发送，因此，这些请求必须通过 SIP 检测引擎。

注　仅支持聊天功能。不支持白板、文件传输和应用共享。不支持 RTC Client 5.0。

SIP 检测转换基于文本的 SIP 消息，重新计算消息的 SDP 部分的内容长度，并重新计算数据包长度和校验和。对于在 SIP 消息的 SDP 部分中被指定为终端应对其进行侦听的地址 / 端口，该检测会动态打开这些端口的媒体连接。

SIP 检测带有一个数据库，该数据库的索引 CALL_ID/FROM/TO 来自 SIP 负载。这些索引标识呼叫、源和目标。该数据库包含在 SDP 媒体信息字段中发现的媒体地址和媒体端口以及媒体类型。一个会话可以有多个媒体地址和端口。ASA 会打开使用这些媒体地址 / 端口的两个终端之间的 RTP/RTCP 连接。

初始呼叫建立 (INVITE) 消息必须使用已知端口 5060；但是，后续消息可能没有此端口号。SIP 检测引擎会打开信令连接针孔，并将这些连接标记为 SIP 连接。会对要到达 SIP 应用并进行转换的消息执行此操作。

呼叫建立后，SIP 会话将处于 “ 临时 ” 状态，直至在响应消息中收到来自被叫终端的媒体地址和媒体端口（该消息指明被叫终端侦听的 RTP 端口）。如果未能在一分钟内收到响应消息，将会断开信令连接。

完成最终握手后，呼叫将变为活动状态，信令连接将保持，直至收到 BYE 消息。

如果内部终端向外部终端发起呼叫，将会对外部接口打开媒体孔，以允许 RTP/RTCP UDP 数据包流向来自内部终端的 INVITE 消息中指定的内部终端媒体地址和媒体端口。流向内部接口的主动提供的 RTP/RTCP UDP 数据包不会流经 ASA，除非 ASA 配置特别允许。

默认 SIP 检测

默认情况下，SIP 检测已通过默认检测映射启用，具体以下：

- SIP 即时消息 (IM) 扩展：已启用。
- SIP 端口的非 SIP 流量：允许。
- 隐藏服务器和终端的 IP 地址：已禁用。
- 掩蔽软件版本和非 SIP URI：已禁用。
- 确保到目标的跳数大于 0：已启用。
- RTP 符合性：未执行。
- SIP 符合性：请勿执行状态检查和报头验证。

另请注意，加密流量检测未启用。要检测加密流量，必须配置 TLS 代理。

配置 SIP 检测

SIP 应用检测会在消息报头和正文中提供地址转换，会动态打开端口，还会执行基本健全性检查。它还支持应用安全和协议符合性（此功能强制对 SIP 消息进行健全性检查，以及检测基于 SIP 的攻击）。

默认情况下，SIP 检测已启用。只有需要非默认处理时，或者要标识 TLS 代理来启用加密流量检测时，才需要配置这项检测。如果要自定义 SIP 检测，请按照以下流程进行操作。

操作步骤

步骤 1　第 9-23 页上的配置 SIP 检测策略映射

步骤 2　第 9-26 页上的配置 SIP 检测服务策略

配置 SIP 检测策略映射

如果默认检测行为不能满足网络要求，可以创建 SIP 检测策略映射来自定义 SIP 检测操作。

在定义流量匹配条件时，可以创建类映射或者直接在策略映射中包括匹配语句。以下操作步骤说明这两种方法。

准备工作

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

操作步骤

步骤 1　（可选）执行以下步骤创建 SIP 检测类映射。

类映射对多个流量匹配进行分组。或者，可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定字符串 “example.com”，则任何包含 “example.com” 的流量都不匹配类映射。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a.　输入以下命令创建类映射：

```
hostname(config)# class-map type inspect sip [match-all | match-any] class_map_name
hostname(config-cmap)#
```

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。match-any 关键字指明如果流量至少与一个 **match** 语句匹配，即为与类映射匹配。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b.　（可选）要向类映射添加描述，请输入以下命令：

```
hostname(config-cmap)# description string
```

其中，*string* 是对类映射的描述（最多可包含 200 个字符）。

c. 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*} - 将 To 报头中指定的被叫方与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*} - 将 From 报头中指定的主叫方与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **content length gt** *bytes* - 匹配在 SIP 报头中的内容长度大于指定字节数（0 到 65536）的消息。
- **match** [**not**] **content type** {**sdp** | **regex** {*regex_name* | **class** *class_name*} - 将内容类型匹配为 SDP 或者与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **im-subscriber regex** {*regex_name* | **class** *class_name*} - 将 SIP IM 用户与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **message-path regex** {*regex_name* | **class** *class_name*} - 将 SIP Via 报头与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **request-method** *method* - 匹配 SIP 请求方法：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。
- **match** [**not**] **third-party-registration regex** {*regex_name* | **class** *class_name*} - 将第三方注册的请求方与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **uri {sip | tel} length gt** *bytes* - 匹配长度大于指定长度（0 到 65536 字节）的选定类型（SIP 或 TEL）的 SIP 报头 URI。

d. 输入 **exit** 退出类映射配置模式。

步骤 2　创建 SIP 检测策略映射，然后输入以下命令：

```
hostname(config)# policy-map type inspect sip policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 4　要对匹配的流量应用操作，请执行以下步骤。

a. 使用以下其中一种方法指定要对其执行操作的流量：

- 如果已创建 SIP 类映射，请输入以下命令指定该类映射：

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- 要直接在策略映射中指定流量，请对 SIP 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b. 输入下列命令，以指定要对匹配流量执行的操作：

```
hostname(config-pmap-c)# {[drop | drop-connection | reset] [log] |
rate-limit message_rate}
```

并非所有选项对于每个 **match** 或 **class** 命令都可用。有关可用的确切选项，请参阅 CLI 帮助或命令参考。

drop 关键字丢弃所有匹配的数据包。

drop-connection 关键字丢弃数据包并关闭连接。

reset 关键字丢弃数据包、关闭连接并向服务器和 / 或客户端发送 TCP 重置。

关键字 **log**（可以单独使用，也可以与其他关键字之一结合使用）用于发送系统日志消息。

rate-limit *message_rate* 参数限制消息速率。速率限制仅适用于匹配 “invite” 和 “register” 的请求方法。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅第 2-4 页上的在检测策略映射中定义操作。

步骤 5　要配置影响检测引擎的参数，请执行以下步骤：

a. 要进入参数配置模式，请输入以下命令：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **im** - 启用即时消息。
- **ip-address-privacy** - 启用 IP 地址隐私（即，隐藏服务器和终端的 IP 地址）。
- **max-forwards-validation action {drop | drop-connection | reset | log} [log]** - 检查 Max-Forwards 报头值（在到达目标之前，此值不能为 0）。必须选择要对不符合要求的流量执行的操作（丢弃数据包、断开连接、重置连接或记录连接）以及是否启用或禁用日志记录。
- **rtp-conformance [enforce-payloadtype]** - 检查流经针孔的 RTP 数据包的协议符合性。可选的 **enforce-payloadtype** 关键字根据信令交换将负载类型强制为音频或视频。
- **software-version action {mask [log] | log}** - 使用 Server 和 User-Agent（终端）报头字段标识软件版本。可以在 SIP 消息中掩蔽软件版本以及（可选）进行有关记录，或者仅进行有关记录。
- **state-checking action {drop | drop-connection | reset | log} [log]** - 启用状态转换检查。必须选择要对不符合要求的流量执行的操作（丢弃数据包、断开连接、重置连接或记录连接）以及是否启用或禁用日志记录。
- **strict-header-validation action {drop | drop-connection | reset | log} [log]** - 根据 RFC 3261 对 SIP 消息中的报头字段启用严格验证。必须选择要对不符合要求的流量执行的操作（丢弃数据包、断开连接、重置连接或记录连接）以及是否启用或禁用日志记录。
- **traffic-non-sip** - 允许已知 SIP 信令端口上出现非 SIP 流量。
- **uri-non-sip action {mask [log] | log}** - 标识在 Alert-Info 和 Call-Info 报头字段中出现的非 SIP URI。可以在 SIP 消息中掩蔽这部分信息以及（可选）进行有关记录，或者仅进行有关记录。

示例

以下示例显示如何禁用采用 SIP 的即时消息：

```
hostname(config)# policy-map type inspect sip mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# no im

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect sip mymap

hostname(config)# service-policy global_policy global
```

配置 SIP 检测服务策略

默认 ASA 配置包括对默认端口的 SIP 检测（这项检测全局应用于所有接口）。自定义检测配置的一种常用方法是自定义默认全局策略。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map sip_class_map
hostname(config-cmap)# match access-list sip
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 SIP 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 SIP 检测。

inspect sip [*sip_policy_map*] [**tls-proxy** *proxy_name*]

其中：

- *sip_policy_map* 是可选的 SIP 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建 SIP 检测策略映射的信息，请参阅第 9-23 页上的配置 SIP 检测策略映射。
- **tls-proxy** *proxy_name* 标识用于这项检测的 TLS 代理。仅在要启用加密流量检测时，才需要 TLS 代理。

示例：

```
hostname(config-class)# no inspect sip
hostname(config-class)# inspect sip sip-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 SIP 检测策略映射，必须使用 **no inspect sip** 命令移除 SIP 检测，然后为其提供新的 SIP 检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

配置 SIP 超时值

连接变为空闲状态后两分钟内，媒体连接将会断开。但是，此超时是可配置的，可以设置为更短或更长时间。

可以在 **Configuration > Firewall > Advanced > Global Timeouts** 页面上配置多个 SIP 全局超时值。

要配置 SIP 控制连接的超时，请输入以下命令：

```
hostname(config)# timeout sip hh:mm:ss
```

此命令配置 SIP 控制连接关闭之前允许的空闲时间。

要配置 SIP 媒体连接的超时，请输入以下命令：

```
hostname(config)# timeout sip_media hh:mm:ss
```

此命令配置 SIP 媒体连接关闭之前允许的空闲时间。

验证和监控 SIP 检测

show sip 命令显示有关越过 ASA 建立的 SIP 会话的信息。与 **debug sip** 和 **show local-host** 命令一样，此命令也用于排解 SIP 检测引擎问题。

以下是 **show sip** 命令的输出示例：

```
hostname# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
    state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
    state Active, idle 0:00:06
```

此示例显示 ASA 中的两个活动 SIP 会话（如 Total 字段中所示）。每个呼叫 ID 代表一个呼叫。

第一个会话（其呼叫 ID 为 c3943000-960ca-2e43-228f@10.130.56.44）处于 Call Init 状态，这意味着会话仍处于呼叫建立阶段。收到对呼叫的最终响应后，即表示呼叫建立完成。例如，主叫方已发送 INVITE 并可能收到 100 Response，但没有看到 200 OK ），因此，呼叫建立还未完成。任何非 1xx 响应消息都被视为最终响应。该会话已空闲 1 秒。

第二个会话处于 Active 状态，这表示呼叫建立已完成，且终端正在交换媒体。该会话已空闲 6 秒。

瘦客户端 (SCCP) 检测

以下各节介绍 SCCP 应用检测。

- 第 9-28 页上的 SCCP 检测概述
- 第 9-28 页上的支持思科 IP 电话
- 第 9-29 页上的 SCCP 检测的局限性
- 第 9-29 页上的默认 SCCP 检测
- 第 9-29 页上的配置 SCCP（瘦客户端）检测
- 第 9-27 页上的验证和监控 SIP 检测

SCCP 检测概述

瘦客户端 (SCCP) 是用于 VoIP 网络的简化协议。使用 SCCP 的思科 IP 电话可共存于 H.323 环境中。与 Cisco CallManager 一起使用时，SCCP 客户端可以与兼容 H.323 的终端进行互操作。

ASA 支持对 SCCP 执行 PAT 和 NAT。如果要使用的 IP 电话多于 IP 电话可使用的全局 IP 地址，必须进行 PAT。通过支持对 SCCP 信令数据包执行 NAT 和 PAT，瘦客户端应用检测确保所有 SCCP 信令和媒体数据包都可流经 ASA。

Cisco CallManager 与思科 IP 电话之间的正常流量使用 SCCP，这些流量由 SCCP 检测处理，无需任何特殊配置。ASA 还支持 DHCP 选项 150 和 66；它通过向思科 IP 电话及其他 DHCP 客户端发送 TFTP 服务器的位置来实现这种支持。思科 IP 电话可能在请求中还包含 DHCP 选项 3（该选项用于设置默认路由）。

注　ASA 支持检测来自运行 SCCP 协议 v22 及更低版本的思科 IP 电话的流量。

支持思科 IP 电话

在 Cisco CallManager 位于安全性高于 Cisco IP SoftPhone 的接口的拓扑中，如果 Cisco CallManager IP 地址需要进行 NAT，则映射必须是**静态的**，因为思科 IP 电话要求在其配置中明确指定 Cisco CallManager IP 地址。静态标识条目使位于安全性较高的接口的 Cisco CallManager 可以接受来自思科 IP 电话的注册。

思科 IP 电话需要访问 TFTP 服务器，以下载它们连接到 Cisco CallManager 服务器所需要的配置信息。

如果思科 IP 电话位于安全性*高于* TFTP 服务器和 Cisco CallManager 的接口，思科 IP 电话无需 ACL 或静态条目即可发起连接。

SCCP 检测的局限性

如果将内部 Cisco CallManager 的地址配置为要通过 NAT 或 PAT 方式转换到另一个 IP 地址或端口，外部思科 IP 电话的注册将会失败，因为 ASA 目前不支持对通过 TFTP 传输的文件内容进行 NAT 或 PAT。尽管 ASA 支持对 TFTP 消息进行 NAT 并会打开用于 TFTP 文件的针孔，但 ASA 无法转换嵌入到在电话注册期间通过 TFTP 传输的思科 IP 电话配置文件中的 Cisco CallManager IP 地址和端口。

注　ASA 支持 SCCP 呼叫的状态故障转移，但处于建立过程中的呼叫除外。

默认 SCCP 检测

默认情况下，SCCP 检测已启用，默认设置如下：

- 注册：未执行。
- 最大消息 ID：0x181。
- 最小前缀长度：4
- 媒体超时：00:05:00
- 信令超时：01:00:00
- RTP 符合性：未执行。

另请注意，加密流量检测未启用。要检测加密流量，必须配置 TLS 代理。

配置 SCCP（瘦客户端）检测

SCCP（瘦客户端）应用检测对数据包数据中的嵌入式 IP 地址和端口号执行转换，并会动态打开针孔。它还执行其他协议符合性检查和基本状态跟踪。

默认情况下，SCCP 检测已启用。只有需要非默认处理时，或者要标识 TLS 代理来启用加密流量检测时，才需要配置这项检测。如果要自定义 SCCP 检测，请按照以下流程进行操作。

操作步骤

步骤 1　第 9-29 页上的为其他检测控制配置瘦客户端 (SCCP) 检测策略映射。

步骤 2　第 9-31 页上的配置 SCCP 检测服务策略。

为其他检测控制配置瘦客户端 (SCCP) 检测策略映射

要指定消息违反参数时要执行的操作，请创建 SCCP 检测策略映射。然后，可以在启用 SCCP 检测时应用所创建的检测策略映射。

操作步骤

步骤 1　创建 SCCP 检测策略映射。

```
hostname(config)# policy-map type inspect skinny policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2　（可选）向策略映射添加描述。

```
hostname(config-pmap)# description string
```

步骤 3　（可选）根据 SCCP 消息的站消息 ID 字段丢弃流量。

a. 根据十六进制的站消息 ID 值（0x0 到 0xffff）标识流量。使用 **match** [**not**] **message-id** 命令可以指定单个 ID 或 ID 范围。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

```
hostname(config-pmap)# match message-id value
hostname(config-pmap)# match message-id range start_value end_value
```

示例：

```
hostname(config-pmap)# match message-id 0x181

hostname(config-pmap)# match message-id range 0x200 0xffff
```

b. 指定要对匹配的数据包执行的操作。可以丢弃数据包和或者记录数据包。

```
hostname(config-pmap)# drop [log]
```

c. 重复以上步骤，直至标识出所有要丢弃的消息 ID。

步骤 4　配置影响检测引擎的参数。

a. 进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **enforce-registration** - 要求必须进行注册才能发出呼叫。
- **message-ID max** *hex_value* - 设置允许的最大 SCCP 站消息 ID。消息 ID 采用十六进制，默认最大值是 0x181。
- **rtp-conformance** [**enforce-payloadtype**] - 检查流经针孔的 RTP 数据包的协议符合性。可选的 **enforce-payloadtype** 关键字根据信令交换将负载类型强制为音频或视频。
- **sccp-prefix-len** {**max** | **min**} *length* - 设置允许的最大或最小 SCCP 前缀长度值。请输入此命令两次，以设置最小值和最大值。默认最小值是 4，没有默认最大值。
- **timeout** {**media** | **signaling**} *time* - 设置媒体和信令连接的超时（格式为 hh:mm:ss）。如果不想设置超时，请指定数字 0。默认的媒体超时是 5 分钟，默认的信令超时是 1 小时。

示例

以下示例显示如何定义 SCCP 检测策略映射。

```
hostname(config)# policy-map type inspect skinny skinny-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enforce-registration
hostname(config-pmap-p)# match message-id range 200 300
hostname(config-pmap-p)# drop log
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect skinny skinny-map
hostname(config)# service-policy global_policy global
```

配置 SCCP 检测服务策略

默认 ASA 配置包括对默认端口的 SCCP 检测（这项检测全局应用于所有接口）。自定义检测配置的一种常用方法是自定义默认全局策略。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map sccp_class_map
hostname(config-cmap)# match access-list sccp
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 SCCP 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 SCCP 检测。

inspect skinny [*sccp_policy_map*] [**tls-proxy** *proxy_name*]

其中：

- *sccp_policy_map* 是可选的 SCCP 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建 SCCP 检测策略映射的信息，请参阅第 9-29 页上的为其他检测控制配置瘦客户端 (SCCP) 检测策略映射。
- **tls-proxy** *proxy_name* 标识用于这项检测的 TLS 代理。仅在要启用加密流量检测时，才需要 TLS 代理。

示例：

```
hostname(config-class)# no inspect skinny
hostname(config-class)# inspect skinny sccp-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的 SCCP 检测策略映射，必须使用 **no inspect skinny** 命令移除 SCCP 检测，然后为其提供新的 SCCP 检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

验证和监控 SCCP 检测

show skinny 命令帮助排解 SCCP（瘦客户端）检测引擎问题。下面是 **show skinny** 命令在以下条件下的输出示例。在此示例中，越过 ASA 建立了两个活动瘦客户端会话。第一个会话是建立在本地地址 10.0.0.11 的一个内部思科 IP 电话与地址 172.18.1.33 的外部 Cisco CallManager 之间。TCP 端口 2000 是 CallManager。第二个会话是建立在本地地址 10.0.0.22 的另一个内部思科 IP 电话与第一个会话的那个 Cisco CallManager 之间。

```
hostname# show skinny
        LOCAL                   FOREIGN                 STATE
--------------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000                1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000                1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

输出表明已在两个内部思科 IP 电话之间建立呼叫。第一个和第二个电话的 RTP 侦听端口分别是 UDP 22948 和 20798。

以下是 **show xlate debug** 命令针对这些瘦客户端连接的输出示例：

```
hostname# show xlate debug
2 in use, 2 most used
Flags:  D - DNS, d - dump, I - identity, i - inside, n - no random,
        r - portmap, s - static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

语音和视频协议检测的历史记录

功能名称	版本	功能信息
适用于 IPv6 的 SIP、SCCP 和 TLS 代理支持	9.3(1)	现在，使用 SIP、SCCP 和 TLS 代理时，可以检测 IPv6 流量（使用 SIP 或 SCCP）。 我们未修改任何命令。

数据库和目录协议的检测

以下主题说明数据库和目录协议的应用检测。有关为何需要对某些协议进行检测以及应用检测的总体方法的信息，请参阅第 7-1 页上的应用层协议检测入门。

- 第 10-1 页上的 ILS 检测
- 第 10-2 页上的 SQL*Net 检测
- 第 10-3 页上的 Sun RPC 检测

ILS 检测

ILS 检测引擎可为 Microsoft NetMeeting、SiteServer 以及使用 LDAP 与 ILS 服务器交换目录信息的 Active Directory 产品提供 NAT 支持。

ASA 支持对 ILS 使用 NAT，其用于在 ILS 或 SiteServer Directory 中注册和查找端点。因为 LDAP 数据库仅存储 IP 地址，所以，无法支持 PAT。

对于搜索响应，当 LDAP 服务器位于外部时，应考虑 NAT，以允许内部对等设备在注册到外部 LDAP 服务器时进行本地通信。对于此类搜索响应，会先搜索 xlate，然后搜索 DNAT 条目以获得正确地址。如果上述两种搜索都失败，则地址未更改。对于使用 NAT 0（无 NAT）且不期望 DNAT 交互的站点，建议关闭检测引擎以提供更佳性能。

当 ILS 服务器位于 ASA 边界内部时，可能需要进行其他配置。这需要一个孔，可供外部客户端访问指定端口（通常是 TCP 389）上的 LDAP 服务器。

注 由于 ILS 流量（H225 呼叫信号）仅出现在辅助 UDP 信道上，因此，过了 TCP 非活动间隔后，TCP 连接将断开。默认情况下，此间隔为 60 分钟，且可使用 TCP **timeout** 命令进行调整。在 ASDM 中，可在 **Configuration > Firewall > Advanced > Global Timeouts** 窗格上完成此操作。

ILS/LDAP 遵循客户端 / 服务器模型，通过单一 TCP 连接处理会话。根据客户端的操作，将可能创建多个上述会话。

在连接协商期间，BIND PDU 从客户端发送至服务器。一旦收到来自服务器的成功 BIND RESPONSE，就可能交换其他操作消息（例如 ADD、DEL、SEARCH 或 MODIFY），以对 ILS 目录执行多项操作。ADD REQUEST 和 SEARCH RESPONSE PDU 可能包含 NetMeeting 对等设备的 IP 地址，供 H.323 （SETUP 和 CONNECT 消息）用于建立 NetMeeting 会话。Microsoft NetMeeting v2.X 和 v3.X 提供 ILS 支持。

ILS 检测将执行以下操作：

- 使用 BER 解码功能解码 REQUEST/RESPONSE PDU。
- 解析 LDAP 数据包。
- 提取 IP 地址。
- 根据需要转换 IP 地址。
- 使用 BER 编码功能，用已转换地址对 PDU 进行编码。
- 将新编码的 PDU 复制回 TCP 数据包。
- 执行递增 TCP 校验和与序列号调整。

ILS 检测存在如下限制：

- 推荐请求和响应不受支持。
- 多个目录中的用户不统一。
- NAT 无法识别在多个目录中有多个标识的单一用户。

有关启用 ILS 检测的信息，请参阅第 7-9 页上的配置应用层协议检测。

SQL*Net 检测

系统已默认启用 SQL*Net 检测。

SQL*Net 协议包括不同类型的数据包，ASA 将处理这些数据包，以使数据流对 ASA 任一侧的 Oracle 应用显示为一致。

SQL*Net 的默认端口赋值为 1521。这是 Oracle 用于 SQL*Net 的值，但是，该值与结构化查询语言 (SQL) 的 IANA 端口赋值不符。使用 **class - map** 命令将 SQL*Net 检测应用于一系列端口号。

注　当与 SQL 控制 TCP 端口 1521 相同的端口上发生 SQL 数据传输时，请禁用 SQL*Net 检测。安全设备在启用 SQL*Net 检测之后充当代理，且将客户端窗口大小从 65000 缩小至大约 16000，从而导致数据传输问题。

ASA 将转换所有地址，并在数据包中查找要为 SQL*Net 第 1 版打开的所有嵌入式端口。

对于 SQL*Net 第 2 版，将修复紧跟 REDIRECT 数据包且数据长度为零的所有 DATA 或 REDIRECT 数据包。

需要修复的数据包包含以下格式的嵌入式主机 / 端口地址：

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

将不在 SQL*Net 第 2 版 TNSFrame 类型（连接、接受、拒绝、重新发送和标记）中扫描 NAT 地址，检测也将不为数据包中的任何嵌入式端口打开动态连接。

如果负载前面是数据长度为零的 REDIRECT TNSFrame 类型，则将在 SQL*Net 第 2 版 TNSFrames、Redirect 和 Data 数据包中扫描要打开的端口和 NAT 地址。当数据长度为零的 Redirect 消息通过 ASA 时，将会在连接数据结构中设置标志，以期转换后续的 Data 或 Redirect 消息并动态打开端口。如果上一个段落中的其中一个 TNS 帧在 Redirect 消息后到达，则将重置该标志。

SQL*Net 检测引擎将使用新旧消息的长度差异，重新计算校验和，更改 IP、TCP 长度，并重新调整序列号和确认号。

针对所有其他情况对 SQL*Net 第 1 进行假设。将在 TNSFrame 类型（连接、接受、拒绝、重新发送、标记、重定向和数据）和所有数据包中扫描端口和地址。系统将转换地址并打开端口连接。

有关启用 SQL*Net 检测的信息，请参阅第 7-9 页上的配置应用层协议检测。

Sun RPC 检测

本节介绍 Sun RPC 应用检测。

- 第 10-3 页上的 Sun RPC 检测概述
- 第 10-3 页上的管理 Sun RPC 服务
- 第 10-4 页上的验证并监控 Sun RPC 检测

Sun RPC 检测概述

Sun RPC 检测引擎为 Sun RPC 协议启用或禁用应用检测。Sun RPC 可供 NFS 和 NIS 使用。Sun RPC 服务可在任何端口上运行。当客户端尝试访问服务器上的 Sun RPC 服务时，必须获悉服务运行所在的端口。它通过查询端口映射程序进程执行此操作，通常为 rpcbind，位于公认端口 111。

客户端将发送服务的 Sun RPC 程序号，而端口映射程序进程将用服务的端口号进行响应。客户端发送其 Sun RPC 查询至服务器，指定端口映射程序进程识别的端口。服务器回复后，ASA 会截取此数据包，并打开该端口上的初始化 TCP 和 UDP 连接。

提示　系统将默认启用 Sun RPC 检测。您只需管理 Sun RPC 服务器表，即可确定允许穿越防火墙的服务。有关启用 Sun RPC 检测的信息，请参阅第 7-9 页上的配置应用层协议检测。

以下限制适用于 SUN RPC 检测：

- 不支持 Sun RPC 负载信息的 NAT 或 PAT。
- Sun RPC 检测仅支持入站 ACL。由于检测引擎使用动态 ACL 而不是辅助连接，因此，Sun RPC 检测不支持出站 ACL。由于始终在入口方向而不是出口方向添加动态 ACL；因此，此检测引擎不支持出站 ACL。要查看为 ASA 配置的动态 ACL，请使用 **show asp table classify domain permit** 命令。

管理 Sun RPC 服务

使用 Sun RPC 服务表，根据已建立的 Sun RPC 会话控制通过 ASA 的 Sun RPC 流量。要在 Sun RPC 服务表中创建条目，请在全局配置模式下使用 **sunrpc-server** 命令：

```
hostname(config)# sunrpc-server interface_name ip_address mask service service_type
protocol {tcp | udp} port[-port] timeout hh:mm:ss
```

可以使用此命令指定超时，过了此时间，就会关闭 Sun RPC 应用检测打开的针孔。例如，要为 IP 地址为 192.168.100.2 的 Sun RPC 服务器创建 30 分钟的超时，请输入以下命令：

```
hostname(config)# sunrpc-server inside 192.168.100.2 255.255.255.255 service 100003
protocol tcp 111 timeout 00:30:00
```

此命令指定 Sun RPC 应用检测打开的针孔将在 30 分钟后关闭。在此示例中，Sun RPC 服务器位于使用 TCP 端口 111 的内部接口上。还可指定 UDP、不同的端口号或端口范围。要指定端口范围，请使用连字符分隔范围中起始端口号和结束端口号（例如，111-113）。

服务类型可确定特定服务类型与用于该服务的端口号之间的映射。要确定服务类型（在此示例中为 100003），请在 Sun RPC 服务器计算机上的 UNIX 或 Linux 命令行处使用 **sunrpcinfo** 命令。

要清除 Sun RPC 配置，请输入以下命令。

```
hostname(config)# clear configure sunrpc-server
```

此操作将移除使用 **sunrpc-server** 命令执行的配置。**sunrpc-server** 命令可用于创建具有指定超时的针孔。

要清除活动 Sun RPC 服务，请输入以下命令：

```
hostname(config)# clear sunrpc-server active
```

这将清除 Sun RPC 应用检测为特定服务（如 NFS 或 NIS）打开的针孔。

验证并监控 Sun RPC 检测

本小节中的输出示例是针对内部接口上 IP 地址为 192.168.100.2 的 Sun RPC 服务器和外部接口上 IP 地址为 209.168.200.5 的 Sun RPC 客户端。

要查看有关当前 Sun RPC 连接的信息，请输入 **show conn** 命令。以下是 **show conn** 命令的输出示例。

```
hostname# show conn
15 in use, 21 most used
UDP out 209.165.200.5:800 in 192.168.100.2:2049 idle 0:00:04 flags -
UDP out 209.165.200.5:714 in 192.168.100.2:111 idle 0:00:04 flags -
UDP out 209.165.200.5:712 in 192.168.100.2:647 idle 0:00:05 flags -
UDP out 192.168.100.2:0 in 209.165.200.5:714 idle 0:00:05 flags i
hostname(config)#
```

要显示有关 Sun RPC 服务表配置的信息，请输入 **show running-config sunrpc-server** 命令。以下是 **show running-config sunrpc-server** 命令的输出示例。

```
hostname(config)# show running-config sunrpc-server
sunrpc-server inside 192.168.100.2 255.255.255.255 service 100003 protocol UDP port 111
timeout 0:30:00
sunrpc-server inside 192.168.100.2 255.255.255.255 service 100005 protocol UDP port 111
timeout 0:30:00
```

此输出显示，UDP 端口 111 上已针对内部接口上 IP 地址为 192.168.100.2 的 Sun RPC 服务器配置 30 分钟的超时间隔。

要显示为 Sun RPC 服务打开的针孔，请输入 **show sunrpc-server active** 命令。以下是 **show sunrpc-server active** 命令的输出示例：

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
-----------------------------------------------
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

LOCAL 列中的条目显示内部接口上客户端或服务器的 IP 地址，而 FOREIGN 列中的值则显示外部接口上客户端或服务器的 IP 地址。

要查看有关 Sun RPC 服务器上运行的 Sun RPC 服务的信息，请从 Linux 或 UNIX 服务器的命令行输入 **rpcinfo -p** 命令。以下是 **rpcinfo -p** 命令的输出示例：

```
sunrpcserver:~ # rpcinfo -p
program vers proto port
100000 2 tcp 111 portmapper
100000 2 udp 111 portmapper
100024 1 udp 632 status
100024 1 tcp 635 status
100003 2 udp 2049 nfs
100003 3 udp 2049 nfs
```

```
100003 2 tcp 2049 nfs
100003 3 tcp 2049 nfs
100021 1 udp 32771 nlockmgr
100021 3 udp 32771 nlockmgr
100021 4 udp 32771 nlockmgr
100021 1 tcp 32852 nlockmgr
100021 3 tcp 32852 nlockmgr
100021 4 tcp 32852 nlockmgr
100005 1 udp 647 mountd
100005 1 tcp 650 mountd
100005 2 udp 647 mountd
100005 2 tcp 650 mountd
100005 3 udp 647 mountd
100005 3 tcp 650 mountd
```

在此输出中，端口 647 对应于通过 UDP 运行的 mountd 守护程序。mountd 进程通常更多地使用端口 32780。在此示例中，通过 UDP 运行的 mountd 进程使用端口 650。

管理应用协议检测

以下主题介绍管理应用协议的应用检测。有关为何需要对某些协议进行检测以及应用检测的总体方法的信息，请参阅第 7-1 页上的应用层协议检测入门。

ASA 默认启用几个常见检测引擎，但可能需要根据网络启用其他检测引擎。

- 第 11-1 页上的 DCERPC 检测
- 第 11-4 页上的 GTP 检测
- 第 11-11 页上的 RADIUS 计费检测
- 第 11-14 页上的 RSH 检测
- 第 11-14 页上的 SNMP 检测
- 第 11-16 页上的 XDMCP 检测

DCERPC 检测

以下各节介绍 DCERPC 检测引擎。

- 第 11-1 页上的 DCERPC 概述
- 第 11-2 页上的配置 DCERPC 检测

DCERPC 概述

DCERPC 是由 Microsoft 分布式客户端和服务器应用广泛使用的、允许软件客户端在服务器远程执行程序的协议。

这通常涉及查询称为终端映射器的服务器（用于侦听已知端口号，以获取所需服务的动态分配网络信息）的客户端。然后，客户端建立与提供服务的服务器实例之间的辅助连接。安全设备允许相应的端口号以及网络地址，如有必要，还会为辅助连接应用 NAT。

DCERPC 检测映射检测已知 TCP 端口 135 上 EPM 与客户端之间的本地 TCP 通信。支持客户端的 EPM 映射和查找操作。客户端和服务器可位于任何安全区域。从适用的 EPM 响应消息接收嵌入式服务器 IP 地址和端口号。由于客户端可能尝试多次连接到 EPM 返回的服务器端口，因此，允许使用可配置超时的多个针孔。

注 DCERPC 检测仅支持 EPM 与客户端之间的通信通过 ASA 打开针孔。如果客户端进行不使用 EPM 的 RPC 通信，则不支持 DCERPC 检测。

配置 DCERPC 检测

默认情况下，DCERPC 检测未启用。如果需要 DCERPC 检测，必须对其进行配置。

操作步骤

步骤 1　第 11-2 页上的配置 DCERPC 检测策略映射。

步骤 2　第 11-3 页上的配置 DCERPC 检测服务策略。

配置 DCERPC 检测策略映射

要指定其他 DCERPC 检测参数，请创建 DCERPC 检测策略映射。然后，可以在启用 DCERPC 检测时应用所创建的检测策略映射。

准备工作

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

操作步骤

步骤 1　创建 DCERPC 检测策略映射，然后输入以下命令：

```
hostname(config)# policy-map type inspect dcerpc policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 3　要配置影响检测引擎的参数，请执行以下步骤：

a.　要进入参数配置模式，请输入以下命令：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b.　设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **timeout pinhole** *hh:mm:ss* - 配置 DCERPC 针孔超时，并覆盖两分钟的全局系统针孔超时。超时可以是 00:00:01 到 119:00:00。
- **endpoint-mapper** [**epm-service-only**] [**lookup-operation** [**timeout** *hh:mm:ss*]] - 配置终端映射器流量选项。**epm-service-only** 关键字在绑定期间执行终端映射器服务，从而仅处理其服务流量。**lookup-operation** 关键字启用终端映射器服务的查找操作。可以配置查找操作生成的针孔超时。如果没有为查找操作配置超时，将会使用针孔超时命令或默认值。

示例

以下示例显示如何使用为 DCERPC 针孔配置的超时定义 DCERPC 检测策略映射。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc-map

hostname(config)# service-policy global-policy global
```

配置 DCERPC 检测服务策略

DCERPC 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。可以简单地编辑默认全局检测策略来添加 DCERPC 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map dcerpc_class_map
hostname(config-cmap)# match access-list dcerpc
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 DCERPC 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 DCERPC 检测。

inspect dcerpc [*dcerpc_policy_map*]

其中，*dcerpc_policy_map* 是可选的 DCERPC 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建检测策略映射的信息，请参阅第 11-2 页上的配置 DCERPC 检测策略映射。

示例：

```
hostname(config-class)# no inspect dcerpc
hostname(config-class)# inspect dcerpc dcerpc-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的检测策略映射，必须使用 **no inspect dcerpc** 命令移除 DCERPC 检测，然后为其提供新的检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

GTP 检测

以下各节介绍 GTP 检测引擎。

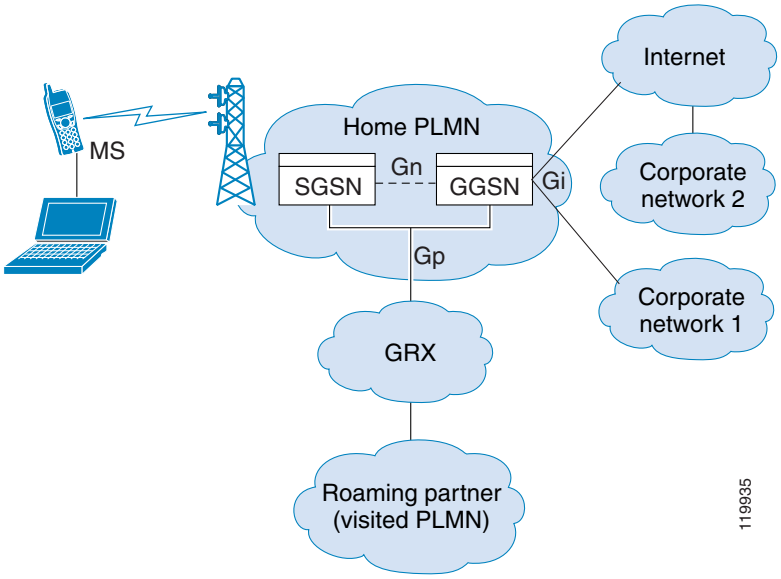
注　GTP 检测需要特殊许可证。

- 第 11-5 页上的 GTP 检测概述
- 第 11-5 页上的 GTP 检测的默认设置
- 第 11-6 页上的配置 GTP 检测
- 第 11-10 页上的验证和监控 GTP 检测

GTP 检测概述

GPRS 为移动用户提供 GSM 网络与公司网络或互联网之间的不间断连接。GGSN 是 GPRS 无线数据网络与其他网络之间的接口。SGSN 执行移动管理、数据会话管理和数据压缩。

图 11-1　GPRS 隧道协议



UMTS 是固定线路电话、移动电话、互联网和计算机技术的商业融合。UTRAN 是在系统中实施无线网络所使用的网络协议。GTP 使多协议数据包可通过 GGSN、SGSN 和 UTRAN 之间的 UMTS/GPRS 主干进行隧道传输。

GTP 不包含用户数据的任何固有安全或加密，但是，使用具有 ASA 的 GTP 有助于保护网络免受这些风险。

SGSN 逻辑上连接到使用 GTP 的 GGSN。GTP 允许多协议数据包通过 GSN 之间的 GPRS 主干进行隧道传输。GTP 提供隧道控制和管理协议，使 SGSN 可通过创建、修改和删除隧道为移动站提供 GPRS 网络访问。GTP 使用隧道机制提供用户数据包传输服务。

注　使用具有故障转移的 GTP 时，如果 GTP 连接已建立，而主用设备在数据通过隧道传输之前发生故障，则 GTP 数据连接（设置了 “j” 标志）不会复制到备用设备。这是因为主用设备不会将半开连接复制到备用设备。

GTP 检测的默认设置

默认情况下，GTP 检测未启用。但是，如果在未指定检测映射的情况下启用 GTP 检测，将会使用默认映射（默认映射提供以下处理）。仅在需要不同值的情况下，才需要配置映射。

- 不允许错误。
- 最大请求数为 200。
- 最大隧道数为 500。
- GSN 超时为 30 分钟。

- PDP 情景超时为 30 分钟。
- 请求超时为 1 分钟。
- 信令超时为 30 分钟。
- 隧道超时为 1 小时。
- T3 响应超时为 20 秒。
- 未知消息 ID 已被丢弃并作了记录。

配置 GTP 检测

默认情况下，GTP 检测未启用。如果需要 GTP 检测，必须对其进行配置。

操作步骤

步骤 1　第 11-6 页上的配置 GTP 检测策略映射。

步骤 2　第 11-8 页上的配置 GTP 检测服务策略。

步骤 3　（可选）配置 RADIUS 计费检测，以防止过度计费攻击。请参阅第 11-11 页上的 RADIUS 计费检测。

配置 GTP 检测策略映射

如果要对 GTP 流量执行其他参数，而默认映射不能满足需求，则可以创建并配置 GTP 映射。

准备工作

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

操作步骤

步骤 1　创建 GTP 检测策略映射：

```
hostname(config)# policy-map type inspect gtp policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2　（可选）要向策略映射添加描述，请输入以下命令：

```
hostname(config-pmap)# description string
```

步骤 3　要对匹配的流量应用操作，请执行以下步骤。

a. 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match** [**not**] **apn regex** {*regex_name* | **class** *class_name*} - 根据指定的正则表达式或正则表达式类匹配接入点名称 (APN)。
- **match** [**not**] **message id** {*message_id* | **range** *message_id_1 message_id_2*} - 匹配消息 ID（ID 范围可以是 1 到 255）。可以指定单个 ID 或 ID 范围。

- **match** [**not**] **message length min** *bytes* **max** *bytes* - 匹配 UDP 负载长度（GTP 报头长度加上消息的其余部分）介于最小值与最大值（1 到 65536）之间的消息。
- **match** [**not**] **version** {*version_id* | **range** *version_id_1 version_id_2*} - 匹配 GTP 版本（版本范围是可以是 0 到 255）。可以指定单个版本或版本范围。

b. 输入下列命令，以指定要对匹配流量执行的操作：

```
hostname(config-pmap-c)# {drop [log]| log | rate-limit message_rate}
```

并非所有选项对于每个 **match** 命令都可用。

- **drop** 关键字丢弃数据包。
- **log** 关键字（可以单独使用，也可以与 **drop** 关键字结合使用）发送系统日志消息。
- **rate-limit** *message_rate* 参数限制消息速率。此选项仅对 **message id** 可用。

可以在策略映射中指定多个 **match** 命令。有关 **match** 命令顺序的信息，请参阅第 2-4 页上的在检测策略映射中定义操作。

步骤 4　要配置影响检测引擎的参数，请执行以下步骤：

a. 要进入参数配置模式，请输入以下命令：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **permit errors** - 允许无效 GTP 数据包或者那些无法解析并将被丢弃的数据包。
- **request-queue** *max_requests* - 设置排队等待响应的最大 GTP 请求数。默认值为 200。达到限制后，如果有新请求到达，将会移除队列中等待时间最长的请求。错误提示、不支持的版本和 SGSN 情景确认消息不被视为请求，且不会进入请求队列中等待响应。
- **tunnel-limit** *max_tunnels* - 设置 ASA 上允许处于活动状态的最大 GTP 隧道数。默认值为 500。一旦达到此命令指定的隧道数，将丢弃新请求。
- **timeout** {**gsn** | **pdp-context** | **request** | **signaling** | **tunnel**} *time* - 设置指定服务的空闲超时（格式为 hh:mm:ss）。如果不想设置超时，请指定数字 0。为每个超时分别输入此命令。

  gsn 关键字指定在移除 GSN 之前允许处于非活动状态的时间段。

  pdp-context 关键字指定开始接收 PDP 情景之前所允许的最大时间段。

  request 关键字指定开始接收 GTP 消息之前所允许的最大时间段。

  gsn 关键字指定在移除 GTP 信令之前允许处于非活动状态的时间段。

  tunnel 关键字指定断开 GTP 隧道之前允许处于非活动状态的时间段。

步骤 5　如有需要，可以在仍处于参数配置模式下时配置 IMSI 前缀过滤。

```
hostname(config-pmap-p)# mcc country_code mnc network_code
```

默认情况下，安全设备不检查有效的移动设备国家 / 地区代码 (MCC)/ 移动网络代码 (MNC) 组合。如果配置 IMSI 前缀过滤，接收到的数据包 IMSI 中的 MCC 和 MNC 将会与配置的 MCC/MNC 组合进行比较，如果不匹配，数据包将被丢弃。

移动设备国家 / 地区代码是非零的三位数值；应在一位或两位数值前添加零作为前缀。移动网络代码是两位或三位数值。

可添加所有允许的 MCC 和 MNC 组合。默认情况下，ASA 不检查 MNC 和 MCC 组合有效性，因此，必须验证所配置组合的有效性。有关 MCC 和 MNC 代码的详细信息，请参阅 ITU E.212 建议《*Identification Plan for Land Mobile Stations*》（陆地移动站识别计划）。

步骤 6　如有需要，可以在仍处于参数配置模式下时配置 GSN 池。

```
hostname(config-pmap-p)# permit response to-object-group SGSN_name
from-object-group GSN_pool
```

ASA 执行 GTP 检测时，默认情况下，ASA 会丢弃来自未在 GTP 请求中指定的 GSN 的 GTP 响应。如果在 GSN 池中使用负载平衡来实现 GPRS 的效率和可扩展性，将会出现这种情况。

要配置 GSN 池并支持负载平衡，请创建指定 GSN 的网络对象组，并在 **from-object-group** 参数中指定该对象组。同样，请为 SGSN 创建一个网络对象组，并在 **to-object-group** 参数中选择该对象组。如果 GSN 响应与 GTP 请求所发送到的 GSN 属于同一个对象组，且 SGSN 所在的对象组允许响应 GSN 向其发送 GTP 响应，则 ASA 允许响应。

网络对象组可以通过主机地址或包含主机地址的子网来标识 GSN 或 SGSN。

示例

以下示例显示如何通过为 GSN 池和 SGSN 定义网络对象来支持 GSN 池。在此示例中，整个 C 类网络被定义为 GSN 池，但您可以标识多个单独的 IP 地址（一个 **network-object** 命令用于标识一个地址），而不是标识整个网络。然后，此示例修改 GTP 检测映射，以允许响应从 GSN 池传输到 SGSN。

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.100.0 255.255.255.0
hostname(config)# object-group network sgsn32
hostname(config-network)# network-object host 192.168.50.100

hostname(config)# policy-map type inspect gtp gtp-policy
hostname(config)# gtp-map gtp-policy
hostname(config-pmap)# parameters
hostname(config-pmap-p)# permit response to-object-group sgsn32
from-object-group gsnpool32
```

示例

以下示例显示如何限制网络中的隧道数：

```
hostname(config)# policy-map type inspect gtp gmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tunnel-limit 3000

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect gtp gmap

hostname(config)# service-policy global_policy global
```

配置 GTP 检测服务策略

GTP 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。可以简单地编辑默认全局检测策略来添加 GTP 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

```
class-map name
match parameter
```

示例：

```
hostname(config)# class-map gtp_class_map
hostname(config-cmap)# match access-list gtp
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 GTP 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 4　配置 GTP 检测。

inspect gtp [*gtp_policy_map*]

其中，*gtp_policy_map* 是可选的 GTP 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。有关创建检测策略映射的信息，请参阅第 11-6 页上的配置 GTP 检测策略映射。

示例：

```
hostname(config-class)# no inspect gtp
hostname(config-class)# inspect gtp gtp-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的检测策略映射，必须使用 **no inspect gtp** 命令移除 GTP 检测，然后为其提供新的检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

验证和监控 GTP 检测

要显示 GTP 配置，请在特权 EXEC 模式下输入 **show service-policy inspect gtp** 命令。

使用 **show service - policy inspect gtp statistics** 命令显示 GTP 检测的统计信息。以下是 **show service-policy inspect gtp statistics** 命令的输出示例：

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                   0     total_dropped             0
  signalling_msg_dropped            0     data_msg_dropped          0
  signalling_msg_forwarded          0     data_msg_forwarded        0
  total created_pdp                 0     total deleted_pdp         0
  total created_pdpmcb              0     total deleted_pdpmcb      0
  pdp_non_existent                  0
```

以下是 **show service-policy inspect gtp statistics gsn** 命令的 GSN 输出示例：

```
hostname# show service-policy inspect gtp statistics gsn 10.9.9.9
1 in use, 1 most used, timeout 0:00:00

GTP GSN Statistics for 10.9.9.9, Idle 0:00:00, restart counter 0
    Tunnels Active 0Tunnels Created 0
    Tunnels Destroyed 0
    Total Messages Received 2
    Signaling Messages Data Messages
    total received 2 0
    dropped 0 0
    forwarded 2 0
```

可使用 **show service-policy inspect gtp pdp-context** 命令显示 PDP 情景相关信息。例如：

```
hostname# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used, timeout 0:00:00

Version TID                 MS Addr        SGSN Addr    Idle      APN
v1      1234567890123425        10.0.1.1       10.0.0.2 0:00:13  gprs.cisco.com

    user_name (IMSI): 214365870921435    MS address:         1.1.1.1
    primary pdp: Y                       nsapi: 2
    sgsn_addr_signal:        10.0.0.2    sgsn_addr_data:          10.0.0.2
    ggsn_addr_signal:        10.1.1.1    ggsn_addr_data:          10.1.1.1
    sgsn control teid:     0x000001d1    sgsn data teid:        0x000001d3
    ggsn control teid:     0x6306ffa0    ggsn data teid:        0x6305f9fc
    seq_tpdu_up:                  0      seq_tpdu_down:                0
    signal_sequence:              0
    upstream_signal_flow:         0      upstream_data_flow:           0
    downstream_signal_flow:       0      downstream_data_flow:         0
    RAupdate_flow:                0
```

PDP 情景通过隧道 ID（IMSI 和 NSAPI 值的组合）标识。GTP 隧道由不同 GSN 节点中的两个关联 PDP 情景来定义，并通过隧道 ID 标识。要在外部数据包数据网络与 MS 用户之间转发数据包，必须有 GTP 隧道。

RADIUS 计费检测

以下各节介绍 RADIUS 计费检测引擎。

- 第 11-11 页上的 RADIUS 计费检测概述
- 第 11-11 页上的配置 RADIUS 计费检测

RADIUS 计费检测概述

RADIUS 计费检测是为了防止使用 RADIUS 服务器的 GPRS 网络上出现过度计费攻击。尽管实施 RADIUS 计费检测不需要 GTP/GPRS 许可证，但如果不实施 GTP 检测并设置 GPRS，实施 RADIUS 计费检测将毫无意义。

GPRS 网络上的过度计费攻击会导致消费者为他们未使用的服务付费。在这种情况下，恶意攻击者会建立与服务器之间的连接，并从 SGSN 获取 IP 地址。即使攻击者结束呼叫，恶意服务器仍会向其发送数据包；虽然 GGSN 会丢弃这些数据包，但来自服务器的连接仍会保持活动状态。分配给恶意攻击者的 IP 地址将被释放，并重新分配给某个合法用户（该用户将需要为攻击者将会使用的服务付费）。

RADIUS 计费检测可确保流经 GGSN 的流量都是合法流量，从而防止此类攻击。通过正确配置的 RADIUS 计费功能，ASA 可根据 Radius Accounting Request Start 消息和 Radius Accounting Request Stop 消息中的 Framed IP 属性匹配情况来断开连接。如果 Framed IP 属性中显示有关匹配的 IP 地址的 Stop 消息，ASA 将会查找具有与该 IP 地址匹配的源的所有连接。

可以选择对 RADIUS 服务器配置预共享密钥，以便 ASA 能够验证消息。如果没有配置共享密钥，ASA 仅会检查源 IP 地址是否是其中一个已配置为可以传输 RADIUS 信息的地址。

注　如果在启用了 GPRS 的情况下使用 RADIUS 计费检测，ASA 会检查 Accounting Request STOP 消息中的 3GPP-Session-Stop-Indicator，以便正确处理辅助 PDP 情景。具体而言，ASA 要求 Accounting Request STOP 消息必须包含 3GPP-SGSN-Address 属性，它才会终止用户会话及所有相关连接。默认情况下，某些第三方 GGSN 可能不发送此属性。

配置 RADIUS 计费检测

默认情况下，RADIUS 计费检测未启用。如果需要 RADIUS 计费检测，必须对其进行配置。

操作步骤

步骤 1　第 11-12 页上的配置 RADIUS 计费检测策略映射。

步骤 2　第 11-13 页上的配置 RADIUS 计费检测服务策略。

配置 RADIUS 计费检测策略映射

要配置 RADIUS 计费检测所需的属性，必须创建 RADIUS 计费检测策略映射。

操作步骤

步骤 1　配置 RADIUS 计费检测策略映射：

```
hostname(config)# policy-map type inspect radius-accounting policy_map_name
hostname(config-pmap)#
```

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2　（可选）向策略映射添加描述。

```
hostname(config-pmap)# description string
```

步骤 3　进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

步骤 4　设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项。

- **send response** - 指示 ASA 将 Accounting-Request Start 和 Stop 消息发送到这些消息的发送方（在 **host** 命令中标识）。
- **enable gprs** - 实施 GPRS 过度计费防护。ASA 会在 Accounting-Request Stop 和 Disconnect 消息中检查 3GPP VSA 26-10415 属性，以便正确处理辅助 PDP 情景。如果该属性存在，ASA 会断开源 IP 地址与已配置端口上的用户 IP 地址相匹配的所有连接。
- **validate-attribute** *number* - 接收 Accounting-Request Start 消息时用于构建用户帐户表的其他条件。这些属性有助于 ASA 决定是否断开连接。

  如果没有指定要验证的其他属性，ASA 将会以 Framed IP Address 属性中的 IP 地址作为唯一依据作出决定。如果您配置了其他属性，且 ASA 接收到包含当前正被跟踪的地址的开始计费消息，但是其他要验证的属性不同，那么将断开所有用原来属性开始的连接（假设 IP 地址已重新分配给新用户）。

  值范围是 1 到 191，而且可以多次输入命令。有关属性编号及其描述的列表，请访问 http://www.iana.org/assignments/radius-types。
- **host** *ip_address* [**key** *secret*] - RADIUS 服务器或 GGSN 的 IP 地址。或者，可以包括密钥，以便 ASA 可以验证消息。如果没有密钥，则只检查 IP 地址。可以重复使用此命令来标识多个 RADIUS 和 GGSN 主机。ASA 收到来自这些主机的 RADIUS 计费消息的副本。
- **timeout users** *time* - 设置用户空闲时间（格式为 hh:mm:ss）。如果不想设置超时，请指定 00:00:00。默认值为 1 小时。

示例

```
policy-map type inspect radius-accounting radius-acct-pmap
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345
class-map type management radius-class
  match port udp eq radius-acct
```

```
policy-map global_policy
  class radius-class
    inspect radius-accounting radius-acct-pmap
```

配置 RADIUS 计费检测服务策略

RADIUS 计费检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。由于 RADIUS 计费检测适用于流向 ASA 的流量，因此，必须将这项检测配置为管理检测规则而不是标准规则。

操作步骤

步骤 1　创建 L3/L4 管理类映射，以标识要应用检测的流量并确定匹配流量。

class-map type management *name*
match {port | access-list} *parameter*

示例：

```
hostname(config)# class-map type management radius-class-map
hostname(config-cmap)# match port udp eq radius-acct
```

在本示例中，匹配 radius-acct UDP 端口，即端口 1646。可以指定其他端口或端口范围 (**match port udp range** *number1 number2*)，也可以使用 **match access-list** *acl_name* 和 ACL。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　标识正用于 RADIUS 记帐检测的 L3/L4 管理类映射。

class *name*

示例：

```
hostname(config-pmap)# class radius-class-map
```

步骤 4　配置 RADIUS 计费检测。

inspect radius-accounting *radius_accounting_policy_map*

其中，*radius_accounting_policy_map* 是在第 11-12 页上的配置 RADIUS 计费检测策略映射中创建的 RADIUS 计费检测策略映射。

示例：

```
hostname(config-class)# no inspect radius-accounting
hostname(config-class)# inspect radius-accounting radius-class-map
```

注　如果要编辑使用中的策略来使用不同的检测策略映射，必须使用 **no inspect radius-accounting** 命令移除 RADIUS 计费检测，然后为其提供新的检测策略映射名称并重新添加这项检测。

步骤 5　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

RSH 检测

默认情况下，RSH 检测已启用。RSH 协议在 TCP 端口 514 上使用从 RSH 客户端到 TCP RSH 服务器的连接。客户端和服务器协商用于客户端会侦听 STDERR 输出流的 TCP 端口号。如有必要，RSH 检测支持协商端口号的 NAT。

有关启用 RSH 检测的信息，请参阅第 7-9 页上的配置应用层协议检测。

SNMP 检测

通过 SNMP 应用检测可以将 SNMP 流量限制于特定 SNMP 版本。SNMP 早期版本的安全性较低；因此，安全策略可能要求拒绝使用某些 SNMP 版本。ASA 可能会拒绝 SNMP 1、2、2c 或 3 版本。可以创建 SNMP 映射来控制允许的版本。

SNMP 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。可以简单地编辑默认全局检测策略来添加 SNMP 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

操作步骤

步骤 1　创建 SNMP 映射。

使用 **snmp-map** *map_name* 命令创建映射，进入 SNMP 映射配置模式，然后使用 **deny version** *version* 命令标识不允许的版本。版本可能是 1、2、2c 或 3。

示例：

以下示例拒绝 SNMP 1 和 2 版本：

```
hostname(config)# snmp-map sample_map
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# deny version 2
```

步骤 2　如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

class-map *name*
match *parameter*

示例：

```
hostname(config)# class-map snmp_class_map
hostname(config-cmap)# match access-list snmp
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 3　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

policy-map *name*

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 4　标识正用于 SNMP 检测的 L3/L4 类映射。

class *name*

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的步骤中创建的类。

步骤 5　配置 SNMP 检测。

inspect snmp [*snmp_map*]

其中，*snmp_map* 是可选的 SNMP 检测策略映射。仅在需要非默认检测处理的情况下，才需要映射。

示例：

```
hostname(config-class)# no inspect snmp
hostname(config-class)# inspect snmp snmp-map
```

注　如果要编辑默认全局策略（或任何使用中的策略）来使用不同的检测策略映射，必须使用 **no inspect snmp** 命令移除 SNMP 检测，然后为其提供新的检测策略映射名称并重新添加这项检测。

步骤 6　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

XDMCP 检测

默认情况下，XDMCP 已启用；但是，XDMCP 检测引擎取决于 **established** 命令的正确配置。

XDMCP 是使用 UDP 端口 177 来协商 X 会话（建立后使用 TCP）的协议。

为了成功协商和启动 XWindows 会话，ASA 必须允许来自 Xhosted 计算机的 TCP 向后连接。要允许向后连接，请在 ASA 上使用 **established** 命令。一旦 XDMCP 协商端口发送显示，**established** 命令将接受咨询，以验证是否应允许此向后连接。

在 XWindows 会话期间，管理器与已知端口 6000 | n 上的显示 Xserver 进行通信。由于以下终端设置，每个显示都具有与 Xserver 的单独连接。

```
setenv DISPLAY Xserver:n
```

其中，*n* 是显示编号。

如果使用 XDMCP，将会使用 IP 地址对显示进行协商（如有必要，ASA 可以对这些 IP 地址进行 NAT）。XDCMP 检测不支持 PAT。

有关启用 XDMCP 检测的信息，请参阅第 7-9 页上的配置应用层协议检测。

第 4 部分

连接设置和服务质量

连接设置

本章介绍如何为通过 ASA 的连接或指向 ASA 的管理连接配置连接设置。连接设置包括：

- 最大连接数（TCP 和 UDP 连接、半开连接、每客户端连接）
- 连接超时
- 死连接检测
- TCP 序列随机化
- TCP 规范化自定义
- TCP 状态旁路
- 全局超时
- 第 12-1 页上的有关连接设置的信息
- 第 12-4 页上的连接设置的许可要求
- 第 12-4 页上的准则和限制
- 第 12-5 页上的默认设置
- 第 12-5 页上的配置连接设置
- 第 12-12 页上的监控连接设置
- 第 12-12 页上的连接设置的配置示例
- 第 12-13 页上的连接设置的功能历史

有关连接设置的信息

本节介绍了您可能需要限制连接的原因。

- 第 12-2 页上的 TCP 拦截和限制半开连接
- 第 12-2 页上的因无客户端 SSL 兼容性而禁用管理数据包的 TCP 拦截
- 第 12-2 页上的死连接检测 (DCD)
- 第 12-2 页上的 TCP 序列随机化
- 第 12-3 页上的 TCP 规范化
- 第 12-3 页上的 TCP 状态旁路

TCP 拦截和限制半开连接

限制半开连接数可保护系统免受 DoS 攻击。ASA 使用每客户端限制和半开连接限制触发 TCP 拦截，保护内部系统免受对具有 TCP SYN 数据包的接口以泛洪方式发起的 DoS 攻击。半开连接是指在源和目标之间尚未完成必要的握手的连接请求。TCP 拦截使用 SYN cookie 算法防止 TCP SYN 泛洪攻击。SYN 泛洪攻击包括通常由伪装 IP 地址发起的一系列 SYN 数据包。SYN 数据包的持续泛洪使服务器 SYN 队列保持已满的状态，从而阻止它处理连接请求。当超过某个连接的半开连接阈值时，ASA 作为服务器代理对客户端 SYN 请求产生 SYN-ACK 响应。当 ASA 收到客户端返回的 ACK 时，它可以对客户端进行身份验证并允许连接到服务器。

注　当您使用 TCP SYN Cookie 保护以防止服务器遭受 SYN 攻击时，您必须设置半开连接限制，使之低于您想要保护的服务器上的 TCP SYN 缓冲区队列。否则，在 SYN 攻击期间，有效客户端将无法访问服务器。

要查看 TCP 拦截的统计信息，包括遭受攻击的前 10 名服务器，请参阅第 16 章，“威胁检测”。

因无客户端 SSL 兼容性而禁用管理数据包的 TCP 拦截

默认情况下，TCP 管理连接会始终启用 TCP 拦截。启用 TCP 拦截时，它会拦截三次 TCP 连接建立握手数据包并阻止 ASA 为无客户端 SSL 处理数据包。无客户端 SSL 要求能够处理三次握手数据包，以便为无客户端 SSL 连接提供选择性 ACK 和其他 TCP 选项。要禁用管理流量的 TCP 拦截，您可以设置半开连接限制；只有达到半开连接限制后，TCP 拦截才会启用。

死连接检测 (DCD)

DCD 检测死连接并允许其过期，无需使仍然可以处理流量的连接过期。如果希望存留空闲但有效的连接，您可以配置 DCD。

如果启用 DCD，空闲超时行为会发生变化。当发生空闲超时时，DCD 探测器会被发送至两个终端主机以确定连接的有效性。如果终端主机未能在探测器按配置的时间间隔被发送后作出响应，连接即被释放，而且重设值（如果已配置的话）将被发送到每个终端主机。如果两个终端主机均响应连接有效，活动超时更新到当前时间，而系统会相应地重新安排空闲超时。

启用 DCD 会更改 TCP 规范器中的空闲超时处理行为。DCD 探测器重置在 **show conn** 命令中看到的连接上的空闲超时。为了确定连接在什么时候超出 timeout 命令中配置的超时值但因 DCD 探测器而保持运行，**show service-policy** 命令包括显示来自 DCD 的活动数量的计数器。

TCP 序列随机化

每个 TCP 连接都有两个 ISN：一个由客户端生成，另一个由服务器生成。ASA 将通过入站和出站方向的 TCP SYN 的 ISN 随机化。

随机化受保护主机的 ISN 可以防止攻击者预测新连接的下一个 ISN 并可能对新会话进行拦截。

如果需要的话，您可以禁用 TCP 初始序列号随机化。例如：

- 如果另一个在线防火墙也执行初始序列号随机化，尽管此操作不会影响流量，但无需两个防火墙同时执行此操作。
- 如果您使用 eBGP 多跳通过 ASA，并且 eBGP 的对等体在使用 MD5。随机化会中断 MD5 校验和。
- 您使用一台要求 ASA 不对连接序列号进行随机化的 WAAS 设备。

TCP 规范化

TCP 规范化功能可识别异常数据包，检测到该等数据包时，ASA 可对其进行操作；例如，ASA 可允许、丢弃或清除数据包。TCP 规范化有助于保护 ASA 免受攻击。TCP 规范化始终启用，但是，您可以自定义某些功能的行为方式。

TCP 规范器包括不可配置操作和可配置操作。通常，丢弃或清除连接的不可配置操作适用于始终不良的数据包。可配置操作（有关详细信息，请参阅第 12-6 页上的用 TCP 映射自定义 TCP 规范器）可能需要根据网络需求自定义。

有关 TCP 规范化的信息，请参阅以下准则：

- 规范器无法防止 SYN 泛洪。ASA 包括其他方式的 SYN 泛洪保护。
- 除非 ASA 因故障转移而处于松散模式，否则规范器始终将 SYN 数据包视为流量中的第一个数据包。

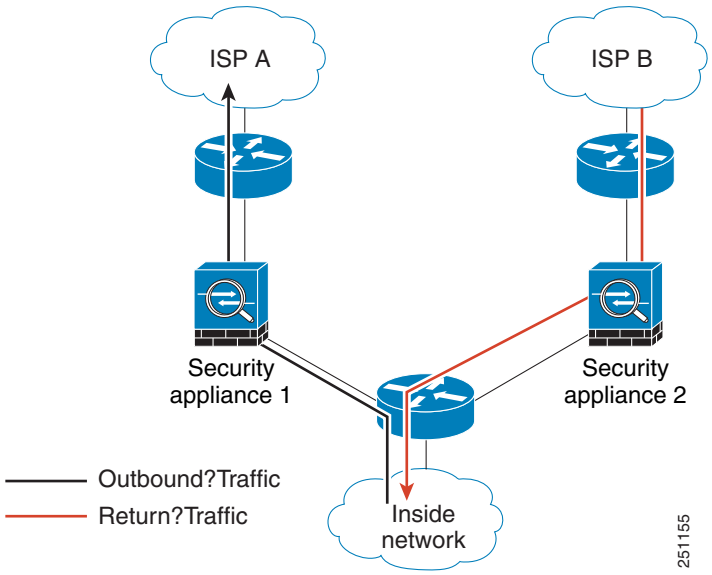
TCP 状态旁路

默认情况下，系统对通过 ASA 的所有流量均使用自适应安全算法进行检查并根据安全策略允许通过或丢弃。ASA 通过检查每个数据包的状态（是新连接还是已建立连接？）并将其分配到会话管理路径（新连接 SYN 数据包）、快速路径（已建立连接），或控制层面路径（高级检测）来实现防火墙性能的最大化。有关状态防火墙的详细信息，请参阅常规操作配置指南。

与快速路径中现有连接的相匹配的 TCP 数据包可以通过 ASA，而无需重新检查安全策略的各个方面。此功能可最大限度地提高性能。但是，使用 SYN 数据包在快速路径中建立会话的方法以及快速路径中发生的检查（如 TCP 序列号），可能会阻碍非对称路由解决方案：连接的出站和入站流量必须通过同一个 ASA。

例如，新连接指向 ASA 1。SYN 数据包通过会话管理路径，而后连接条目成功添加至快速路径表。如果此连接的后续数据包通过 ASA 1，则数据包将与快速路径中的条目相匹配并通过。但是，如果后续数据包到达 ASA 2，其中不存在经过管理会话路径的 SYN 数据包，则连接的快速路径中没有条目，导致数据包会被丢弃。图 12-1 显示一个非对称路由示例，其中，出站流量通过一个与入站流量不同的 ASA：

图 12-1　　非对称路由：



如果上游路由器配置了非对称路由，而且流量在两个 ASA 之间交替，则可为特定流量配置 TCP 状态旁路。TCP 状态旁路修改在快速路径中建立会话的方式并禁用快速路径检查。此功能将 TCP 流量视作 UDP 连接处理：如果一个与指定网络相匹配的非 SYN 数据包进入 ASA，而且不存在快速路径条目，则该数据包通过会话管理路径以在快速路径中建立连接。一旦进入快速路径，流量就会绕过快速路径检查。

连接设置的许可要求

型号	许可证要求
ASAv	标准或高级许可证。
所有其他型号	基础许可证。

准则和限制

情景模式准则

在单一和多情景模式下受支持。

防火墙模式准则

在路由和透明模式中支持。

故障转移准则

支持故障转移。

TCP 状态旁路不支持的功能

使用 TCP 状态旁路时，系统不支持以下功能：

- 应用检测 - 应用检测要求入站和出站流量通过同一个 ASA，因此，TCP 状态旁路不支持应用检测。
- AAA 身份验证会话 - 当用户与一个 ASA 进行身份验证，通过其他 ASA 返回的流量会被拒绝，因为用户未与该 ASA 进行身份验证。
- TCP 拦截、最大半开连接限制及 TCP 序列号随机化 - ASA 不记录连接状态，因此，这些功能无法应用。
- TCP 规范化 - TCP 规范器被禁用。
- SSM 和 SSC 功能 - 无法使用 SSM 或 SSC 上运行的 TCP 状态旁路和任何应用，例如 IPS 或 CSC。

TCP 状态旁路 NAT 准则

由于每个 ASA 的转换会话是分别建立的，需确保在两个 ASA 上为 TCP 状态旁路流量配置静态 NAT ；如果使用动态 NAT，为 ASA 1 上会话选择的地址与为 ASA 2 上会话选择的地址将会不同。

最大并发和半开连接准则

根据 ASA 型号的 CPU 内核数量，由于每个内核管理连接的方式不同，最大并发和半开连接可能超出配置的数量。在最坏的情况下，ASA 允许高达 *n*-1 个额外连接和半开连接，其中，*n* 为内核的数量。例如，如果设备型号有 4 个内核，如果配置了 6 个并发连接和 4 个半开连接，每个类型可额外配置 3 个连接。要确定型号的内核数量，请输入 **show cpu core** 命令。

默认设置

TCP 状态旁路

TCP 状态旁路默认为禁用。

TCP 规范器

默认配置包括以下设置：

```
no check-retransmission
no checksum-verification
exceed-mss allow
queue-limit 0 timeout 4
reserved-bits allow
syn-data allow
synack-data drop
invalid-ack drop
seq-past-window drop
tcp-options range 6 7 clear
tcp-options range 9 255 clear
tcp-options selective-ack allow
tcp-options timestamp allow
tcp-options window-scale allow
ttl-evasion-protection
urgent-flag clear
window-variation allow-connection
```

配置连接设置

- 第 12-6 页上的用 TCP 映射自定义 TCP 规范器
- 第 12-9 页上的配置连接设置

配置连接设置的任务流

步骤 1　对于 TCP 规范化自定义，根据第 12-6 页上的用 TCP 映射自定义 TCP 规范器创建一个 TCP 映射。

步骤 2　对于的所有连接设置，根据第 1 章，“ 使用模块化策略框的服务策略 ”。配置服务策略。

步骤 3　根据第 12-9 页上的配置连接设置配置连接设置。

用 TCP 映射自定义 TCP 规范器

要自定义 TCP 规范器，首先使用 TCP 映射定义设置。

详细步骤

步骤 1　要指定希望查找的 TCP 规范化条件，通过输入下列命令创建一个 TCP 映射：

```
hostname(config)# |tcp-map tcp-map-name
```

对于每个 TCP 映射，可自定义一项或多项设置。

步骤 2　（可选）通过输入下列一条或多条命令配置 TCP 映射条件。（请参阅表 12-1）。如果希望自定义某些设置，系统则对未输入的所有命令使用默认设置。

表 12-1　tcp-map 命令

命令	备注
check-retransmission	防止不一致的 TCP 重传。
checksum-verification	验证校验和。
exceed-mss {**allow** | **drop**}	为数据长度超过 TCP 最大分段大小的数据包设置操作。 （默认）关键字 **allow** 允许数据长度超过 TCP 最大分段大小的数据包。 （默认）关键字 **drop** 丢弃数据长度超过 TCP 最大分段大小的数据包。
invalid-ack {**allow** | **drop**}	为具有无效 ACK 的数据包设置操作。您可能会在下列情况下看到无效 ACK ： • 在 SYN-ACK 已收到的 TCP 连接状态下，如果已收到 TCP 数据包的 ACK 号码与发送的下一个 TCP 数据包的序列号不完全相同，则为无效 ACK。 • 如果已收到 TCP 数据包的 ACK 号码大于发送的下一个 TCP 数据包的序列号，则为无效 ACK。 关键字 **allow** 允许具有无效 ACK 的数据包。 （默认）关键字 **drop** 丢弃具有无效 ACK 的数据包。 **注**　对于 WAAS 连接，具有无效 ACK 的 TCP 数据包自动被允许。

表 12-1　tcp-map 命令（续）

命令	备注
queue-limit *pkt_num* [**timeout** *seconds*]	设置 TCP 连接可缓冲并可按顺序排列的最大无序数据包数量，介于 1 至 250 之间。默认值为 0，表示禁用此设置，而且使用的默认系统队列限制取决于流量类型： • 对于用于应用检测（**inspect** 命令）、IPS（**ips** 命令）和 TCP 检查重传（TCP 映射 **check-retransmission** 命令）的连接，队列限制为 3 个数据包。如果 ASA 收到一个具有不同窗口大小的 TCP 数据包，则队列限制可动态变更以匹配通告的设置。 • 对于其他 TCP 连接，无序数据包保留原样通过。 如果将 **queue-limit** 命令设置为 1 或以上，则允许用于所有 TCP 流量的无序数据包的数量与此设置匹配。例如，对于应用检测、IPS 和 TCP 检查重发流量，来自 TCP 数据包的所有通告设置将被忽略，以支持 **queue-limit** 设置。对于其他 TCP 流量，无序数据包现在可进行缓冲并按顺序排列而非保留原样通过。 **timeout** *seconds* 参数设置无序数据包可停留在缓冲区的最长时间，介于 1 至 20 秒之间；如果这些数据包在超时期间内未按顺序排列并通过，则将被丢弃。默认值为 4 秒。如果 *pkt_num* 参数设置为 0，则无法为任何流量更改超时；您需将 limit 设置为 1 或以上，以便使关键字 **timeout** 生效。
reserved-bits {**allow** | **clear** | **drop**}	为 TCP 报头保留位设置操作。 （默认）关键字 **allow** 允许在 TCP 报头中具有保留位的数据包。 关键字 **clear** 清除在 TCP 报头中的保留位并允许数据包。 关键字 **drop** 丢弃在 TCP 报头中具有保留位的数据包。
seq-past-window {**allow** | **drop**}	为具有超出窗口序列号的数据包设置操作，即已收到 TCP 数据包的序列号超出 TCP 接收窗口的右边。 关键字 **allow** 允许具有超出窗口序列号的数据包。仅在 **queue-limit** 命令设置为 0（禁用）时，此操作才被允许。 （默认）关键字 **drop** 丢弃具有超出窗口序列号的数据包。
synack-data {**allow** | **drop**}	为包含数据的 TCP SYNACK 数据包设置操作。 关键字 **allow** 允许包含数据的 TCP SYNACK 数据包。 （默认）关键字 **drop** 丢弃包含数据的 TCP SYNACK 数据包。
syn-data {**allow** | **drop**}	为具有数据的 SYN 数据包设置操作。 （默认）关键字 **allow** 允许具有数据的 SYN 数据包。 关键字 **drop** 丢弃具有数据的 SYN 数据包。

表 12-1　tcp-map 命令（续）

命令	备注
tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**} 或 **tcp-options range** *lower upper* {**allow** | **clear** | **drop**}	为具有 TCP 选项的数据包设置操作，包括 selective-ack、timestamp 或 window-scale TCP 选项。 （默认）关键字 **allow** 允许具有指定选项的数据包。 （对于 **range** 默认）关键字 **clear** 清除选项并允许数据包。 关键字 **drop** 丢弃具有指定选项的数据包。 关键字 **selective-ack** 为 SACK 选项设置操作。 关键字 **timestamp** 为时间戳选项设置操作。清除时间戳选项将禁用 PAWS 和 RTT。 关键字 **widow-scale** 为窗口扩展机制选项设置操作。 关键字 **range** 指定选项范围。*lower* 参数将范围的低端设置为 6、7 或 9 - 255。 *upper* 参数将范围的高端设置为 6、7 或 9 - 255。
ttl-evasion-protection	禁用 TTL 规避保护。如果要阻止尝试规避安全策略的攻击，请勿输入此命令。 例如，攻击者可能发送一个使用极短 TTL 通过策略的数据包。如果 TTL 变为 零，ASA 与终端之间的路由器将丢弃数据包。此时攻击者可发送一个具有较长 TTL 的恶意数据包，该数据包对 ASA 显示为重传并获得通过。但是，在终端主机，它是攻击者收到的第一个数据包。在这种情况下，没有安全防止攻击，攻击者便可达到目的。
urgent-flag {**allow** | **clear**}	为具有 URG 标记的数据包设置操作。URG 标记用于表示数据包包含优先级高于数据流内其他数据的信息。TCP RFC 对 URG 标记的确切解释比较模糊，因此终端系统以不同的方式处理紧急偏移，这可能使终端系统容易受到攻击。 关键字 **allow** 允许具有 URG 标记的数据包。 （默认）关键字 **clear** 清除 URG 标记并允许数据包。
window-variation {**allow** | **drop**}	为意外更改其窗口大小的连接设置操作。窗口大小机制允许 TCP 通告一个大窗口，随后通告一个不接受过多数据的较小窗口。根据 TCP 规范，强烈反对“缩小窗口”。检测到这种情况时，可以丢弃该连接。 （默认）关键字 **allow** 允许窗口变体的连接。 关键字 **drop** 丢弃窗口变体的连接。

配置连接设置

要设置连接设置，请执行以下步骤。

详细步骤

	命令	用途
步骤 1	**class-map** *name* **示例：** `hostname(config)# class-map bypass_traffic`	创建一个类映射，以识别您要禁用状态性防火墙检测的流量。
步骤 2	**match** *parameter* **示例：** `hostname(config-cmap)# match access-list bypass`	指定类映射中的流量。有关详细信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。
步骤 3	**policy-map** *name* **示例：** `hostname(config)# policy-map tcp_bypass_policy`	添加或编辑策略映射，以设置要对类映射流量执行的操作。
步骤 4	**class** *name* **示例：** `hostname(config-pmap)# class bypass_traffic`	识别步骤 1 中创建的类映射

命令	用途
步骤 5 执行以下一项或多项操作：	
set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]} **示例：** `hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable`	设置最大连接限制或是否启用 TCP 序列随机化。 **conn-max** *n* 参数设置允许的最大同步 TCP 和 / 或 UDP 连接数，介于 0 至 2000000 之间。默认值为 0，即允许无限制连接。 如果两个服务器配置为允许同步 TCP 和 / 或 UDP 连接，连接限制分别应用于每个配置的服务器。 如果在一个类别下配置，此参数限制整个类别允许的最大同步连接数。在这种情况下，一台攻击主机可占用所有连接而且使其余所有主机无法在该类别的 ACL 中匹配。 **embryonic-conn-max** *n* 参数设置允许的最大同步半开连接数，介于 0 至 2000000 之间。默认值为 0，即允许无限制连接。 **per-client-embryonic-max** *n* 参数设置每个客户端允许的最大同步半开连接数，介于 0 至 2000000 之间。默认值为 0，即允许无限制连接。 **per-client-max** *n* 参数设置每个客户端允许的最大同步连接数，介于 0 至 2000000 之间。默认值为 0，即允许无限制连接。如果在一个类别下配置，此参数限制通过该类别下某 ACL 匹配的每台主机所允许的最大同步连接数。 关键字 **random-sequence-number** {**enable** | **disable**} 启用或禁用 TCP 序列号随机化。有关详细信息，请参阅第 12-2 页上的 TCP 序列随机化。 您可以将该命令（按任何顺序）输入在同一行中，也可以将每个属性作为单独的命令输入。ASA 在运行的配置中，会将该命令组合为一行。 **注**　对于管理流量，您只能设置关键字 **conn-max** 和 **embryonic-conn-max**。

命令	用途
set connection timeout {[**embryonic** *hh*:*mm*:*ss*] {**idle** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [dcd *hh*:*mm*:*ss* [*max_retries*]]} **示例：** hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 half-closed 0:20:0 dcd	设置连接超时。有关全局超时的信息，请参阅命令参考中的 **timout** 命令。下述默认设置假设您未更改这些行为的全局默认值；全局默认设置覆盖此处所述的设置。 关键字 **embryonic** *hh*:*mm*:*ss* 设置 TCP 半开连接关闭之前的超时期间，介于 0:0:5 至 1193:00:00 之间。默认值为 0:0:30。该值也可以设置为 0，表示连接永不会超时。 关键字 **idle** *hh*:*mm*:*ss* 设置空闲超时时间，介于 0:0:1 至 1193:0:0 之间。在此时间之后，系统会关闭任何协议的已建立连接。默认值为 1:0:0。该值也可以设置为 0，表示连接永不会超时。对于 TCP 流量，如果连接超时，关键字 **reset** 向 TCP 终端发送重置命令。 关键字 **half-closed** *hh*:*mm*:*ss* 设置半关闭连接关闭之前的空闲超时时间，介于 0:5:0（用于 9.1(1) 及以前版本）或 0:0:30（用于 9.1(2) 及以后版本）至 1193:0:0 之间。默认值为 0:10:0。半关闭连接不受 DCD 的影响。此外，如果取消半关闭连接，ASA 将不发送重置消息。 关键字 **dcd** 启用了 DCD。DCD 检测死连接并允许其过期，无需使仍然可以处理流量的连接过期。如果希望存留空闲但有效的连接，您可以配置 DCD。TCP 连接超时后，ASA 发送 DCD 探测器到终端主机以确定连接的有效性。如果其中一台终端主机在最大尝试次数用完后未作出响应，ASA 将会释放连接。如果两台终端主机均响应连接有效，ASA 会更新活动超时到当前时间，而系统会相应地重新安排空闲超时。*retry-interval* 以 *hh*:*mm*:*ss* 格式设置每个 DCD 探测器无响应之后发送另一个探测器之前的等待时间，介于 0:0:1 至 24:0:0 之间。默认值为 0:0:15。*max-retries* 设置宣告连接为死连接之前 DCD 的连续失败重试次数。最小值为 1，最大值为 255。默认值为 5。 默认 **udp** 空闲超时为 2 分钟。 默认 **icmp** 空闲超时为 2 秒。 默认 **esp** 和 **ha** 空闲超时为 30 秒。 对于其他所有协议，默认空闲超时为 2 分钟。 要设置为永不超时，请输入 0:0:0。 您可以将该命令（按任何顺序）输入在同一行中，也可以将每个属性作为单独的命令输入。该命令在运行的配置中将会合并为一行。该命令在管理流量中不可用。
set connection advanced-options *tcp-map-name* **示例：** hostname(config-pmap-c)# set connection advanced-options tcp_map1	自定义 TCP 规范器。参阅第 12-6 页上的用 TCP 映射自定义 TCP 规范器，创建 TCP 映射。

	命令	用途
	set connection advanced-options tcp-state-bypass **示例：** hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass	启用 TCP 状态旁路。
步骤 6	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **示例：** hostname(config)# service-policy tcp_bypass_policy outside	在一个或多个接口上激活策略映射。**global** 可以将策略映射应用到所有接口，**interface** 可以将策略应用到某个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

监控连接设置

要监控 TCP 状态旁路，请执行以下操作之一：

命令	用途
show conn	如果您使用 **show conn** 命令，则使用 TCP 状态旁路的连接显示包含标记 “b”。

连接设置的配置示例

- 第 12-12 页上的连接限制和超时的配置示例
- 第 12-13 页上的 TCP 状态旁路的配置示例
- 第 12-13 页上的 TCP 规范化的配置示例

连接限制和超时的配置示例

以下示例设置所有流量的连接限制和超时：

```
hostname(config)# class-map CONNS
hostname (config-cmap)# match any
hostname (config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname (config-pmap-c)# set connection conn-max 1000 embryonic-conn-max 3000
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
hostname (config-pmap-c)# service-policy CONNS interface outside
```

您可以输入带多个参数 **set connection** 命令，也可以使用单独的命令输入每个参数。ASA 在运行的配置中，会将该命令组合为一行。例如，如果在类配置模式中输入以下两个命令：

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

show running-config policy-map 命令的输出将以单条的组合命令形式显示两个命令的结果：

```
set connection conn-max 600 embryonic-conn-max 50
```

TCP 状态旁路的配置示例

以下是 TCP 状态旁路的示例配置

```
hostname(config)# |access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any

hostname(config)# class-map tcp_bypass
hostname(config-cmap)# description "TCP traffic that bypasses stateful firewall"
hostname(config-cmap)# match access-list tcp_bypass

hostname(config-cmap)# policy-map tcp_bypass_policy
hostname(config-pmap)# class tcp_bypass
hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass

hostname(config-pmap-c)# service-policy tcp_bypass_policy outside

hostname(config-pmap-c)# |static (inside,outside) 209.165.200.224 10.1.1.0 netmask
255.255.255.224
```

TCP 规范化的配置示例

例如，对于发送到公认 FTP 数据端口与 Telnet 端口之间的 TCP 端口范围内的所有流量，要允许该等流量的紧急标记和紧急偏移数据包，请输入以下命令：

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet
hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap
hostname(config-pmap-c)# service-policy pmap global
```

连接设置的功能历史

表 12-2 列出了各项功能变更以及实施了该变更的平台版本。

表 12-2　　连接设置的功能历史

功能名称	平台版本	功能信息
TCP 状态旁路	8.2(1)	引入了此功能。以下命令已引入：**set connection advanced-options tcp-state-bypass**。
所有协议的连接超时	8.2(2)	空闲超时已被更改为应用于所有协议，而不仅是 TCP 协议。 以下命令已被修改：**set connection timeout**

表 12-2　连接设置的功能历史（续）

功能名称	平台版本	功能信息
使用备份静态路由的连接超时	8.2(5)/8.4(2)	如果存在多条静态路由连至具有不同度量的网络，ASA 在创建连接时使用具有最佳度量的网络。如果有更好的路由可用，则此超时会关闭连接，因而可以使用更好的路由重新建立连接。默认值为 0（连接永不会超时）。要利用此功能，请更改超时值。 我们修改了以下命令：**timeout floating-conn**。
PAT 转换可配置超时	8.4(3)	如果 PAT 转换超时（默认情况下在 30 秒之后），而且 ASA 重复使用该端口进行新的转换，一些上游路由器可能因为先前的连接可能仍在上游设备上打开而拒绝新连接。PAT 转换超时现在可配置为一个介于 30 秒至 5 分钟之间的值。 以下命令已被引入：**timeout pat-xlate**。 *此功能在 8.5(1) 或 8.6(1) 中不可用。*
服务策略规则增加的最大连接数限制	9.0(1)	服务策略规则的最大连接数从 65535 增加至 2000000。 我们修改了以下命令：**set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max**、**set connection per-client-max**。
半关闭超时最小值减小至 30 秒	9.1(2)	全局超时和连接超时的半关闭超时最小值从 5 分钟缩短至 30 秒，以提供更好的 DoS 保护。 我们修改了以下命令：**set connection timeout half-closed**、**timeout half-closed**。

服务质量

您是否曾用过使用卫星连接的长途电话？对话可能会不定期中断，出现短暂但可察觉的间隙。这些短暂间隙是在网络上传输的数据包到达之间的时间，即延迟。某些网络流量，例如语音和视频，无法容忍较长的延迟时间。服务质量 (QoS) 功能使您能够优先考虑关键流量，防止带宽占用和管理网络瓶颈以防止丢包。

注 对于 ASASM，我们建议在交换机上而非 ASASM 上运行 QoS。交换机在此领域具有更多功能。一般来说，网络中 QoS 在路由器和交换机上运行最佳，往往比 ASA 更具广泛的功能。

本章介绍如何应用 QoS 策略。

- 第 13-1 页上的关于 QoS
- 第 13-3 页上的 QoS 准则
- 第 13-4 页上的配置 QoS
- 第 13-8 页上的监控 QoS
- 第 13-10 页上的优先级队列和策略管制的配置示例
- 第 13-12 页上的 QoS 的历史记录

关于 QoS

应考虑到在不断变化的网络环境中，QoS 不是一次性部署，而是网络设计的持续必要的部分。

本章节介绍 ASA 上可用的 QoS 功能。

- 第 13-2 页上的支持的 QoS 功能
- 第 13-2 页上的什么是令牌桶？
- 第 13-2 页上的策略管制
- 第 13-2 页上的优先级队列
- 第 13-3 页上的 DSCP（区分服务）保留

支持的 QoS 功能

ASA 也支持下列 QoS 功能：

- 策略管制 - 要防止分类流量占用网络带宽，可以限制每个类别使用的最大带宽。有关详细信息，请参阅第 13-2 页上的策略管制。
- 优先级队列 - 对于无法容忍延迟的关键流量，例如 IP 语音 (VoIP)，您可以将此流量标记为低延迟队列的 (LLQ) 流量，以便其始终在其他流量之前传输。请参阅第 13-2 页上的优先级队列。

什么是令牌桶？

令牌桶用于管理对流量中的数据进行管制的设备，例如流量监管器。令牌桶本身不具有丢弃或优先级策略。相反，如果流量超过管制器，令牌桶会丢弃令牌，并将管理传输队列的问题留给流量。

令牌桶是传输速率的正式定义。它包含三个组成部分：突发大小、平均速率和时间间隔。虽然平均速率通常表示为位 / 秒，但任意两个值可以通过以下关系从第三个值中推出：

平均速率 = 突发大小 / 时间间隔

以下是这些术语的部分定义：

- 平均速率 - 亦称承诺信息速率 (CIR)，指定单位时间平均发送或转发的数据量。
- 突发大小 - 亦称承诺突发 (Bc) 大小，以每次突发的字节为单位指定在给定的单位时间内可以发送而不引起调度问题的流量大小。
- 时间间隔 - 亦称测量间隔，以每次突发的秒为单位指定时间量。

在令牌桶比喻中，以一定速率将令牌添加到桶中。令牌桶本身有指定的容量。如果令牌桶容量已满，新到达的令牌会被丢弃。每个令牌允许源将一定数量的位发送到网络中。要发送数据包，管制器必须从令牌桶中移除与所代表的数据包大小相等的若干令牌。

如果令牌桶内没有足够的令牌来发送数据包，数据包会一直等，直到数据包被丢弃或被降级。如果令牌桶的令牌已满，传入的令牌会溢出而不能用于后续数据包。因此，在任何时刻，源能够发送到网络中的最大突发流量都大致与令牌桶的大小成正比。

策略管制

策略管制是一种通过确保流量不超过配置的最大速率（以位 / 秒为单位）以保证任何一个流量类都不会沿用全部资源的方式。如果流量超出最大速率，ASA 会丢弃超额流量。策略管制还设定了允许的单次最大突发流量。

优先级队列

LLQ 优先级队列使您可以在处理其他流量之前优先处理特定流量（例如，像语音和视频之类的延迟敏感型流量）。优先级队列使用接口上的一个 LLQ 优先级队列（请参阅第 13-5 页上的配置接口的优先级队列），而其他流量进入“尽力而为”队列。由于大小有限制，队列可以填装和溢出。当队列已满时，任何额外的数据包都无法进入队列并将被丢弃。这称为*尾部丢弃*。要避免队列被填满，您可以增加队列缓冲区的大小。还可以优化允许进入传输队列的数据包的最大数。这些选项使您能够控制优先级队列的延迟和稳健性。在 LLQ 队列中的数据包始终在“尽力而为”队列中的数据包之前传输。

QoS 功能如何相互作用

如果 ASA 需要，您可以单独配置各 QoS 功能。但是，通常您要在 ASA 上配置多个 QoS 功能，以允许更多操作，例如，可以优先处理某些流量，并防止其它流量引起带宽问题。您可以配置：

优先级队列（用于特定流量）+ 策略管制（用于其余流量）。

您无法对同一组的流量配置优先级队列和策略管制。

DSCP（区分服务）保留

DSCP (DiffServ) 标记保留在所有通过 ASA 的流量上。ASA 不对任何分类流量做本地标记 / 注释。例如，可以解密每个数据包的加速转发 (EF) DSCP 位以确定其是否需要 " 优先级 " 处理并让 ASA 将这些数据包送到 LLQ。

QoS 准则

情景模式准则

仅支持单一情景模式。不支持多情景模式。

防火墙模式准则

仅支持路由防火墙模式。不支持透明防火墙模式。

IPv6 准则

不支持 IPv6。

型号准则

- (ASA 5512-X 到 ASA 5555-X) 管理 0/0 接口不支持优先级队列。
- (ASASM) 仅支持策略管制。

附加准则和限制

- QoS 只能单向应用；只有进入（或退出，根据 QoS 功能而定）应用了策略映射的接口的流量才会受到影响。有关详细信息，请参阅第 1-4 页上的功能方向性。
- 对于优先级流量，您无法使用 **class-default** 类映射。
- 对于优先级队列，优先级队列必须是为某个物理接口或为 ASASM（一个 VLAN）配置的。
- 策略管制不支持流向设备的流量。
- 对于策略管制，往返 VPN 隧道的流量会绕过接口策略管制。
- 对于策略管制，匹配隧道组类映射时，仅支持出站策略管制。

配置 QoS

采用以下顺序在 ASA 上执行 QoS。

步骤 1　第 13-4 页上的确定优先级队列的队列和传输环路限制。

步骤 2　第 13-5 页上的配置接口的优先级队列

步骤 3　第 13-6 页上的配置优先级队列和策略管制的服务规则。

确定优先级队列的队列和传输环路限制

使用下列工作表确定优先级队列和传输环路限制。

- 第 13-4 页上的队列限制工作表
- 第 13-5 页上的传输环路限制工作表

队列限制工作表

下列工作表显示如何计算优先级队列大小。由于大小有限制，队列可以填装和溢出。当队列已满时，任何额外的数据包都无法进入队列并将被丢弃（称为*尾部丢弃*）。要避免队列被填满，您可以根据第 13-5 页上的配置接口的优先级队列调整队列缓冲区大小。

关于工作表的小提示：

- 出站带宽 - 例如，DSL 的上行链路速度可能为 768 Kbps。请与供应商核对。
- 平均数据包大小 - 通过编码解码器或样本量确定此值。例如，对于 VPN 上 的 VoIP，可以使用 160 字节。如果不知道使用哪种大小，我们建议使用 256 字节。
- 延迟 - 延迟取决于应用程序。例如，VoIP 建议的最大延迟是 200 毫秒。如果您不知道使用哪种延迟，我们建议使用 500 字节。

表 13-1　队列限制工作表

1	_____ *出站带宽（单位为Mbps 或Kbps）*	Mbps	**x 125**	**=**	_____ *# 字节 / 毫秒*		
		kbps	**x .125**	**=**	_____ *# 字节 / 毫秒*		
2	_____ *来自第 1 步的 # 字节 / 毫秒*	**÷**	_____ *平均数据包大小（字节）*	**x**	_____ *延迟（毫秒）*	**=**	_____ *队列限制（# 数据包）*

传输环路限制工作表

下列工作表显示如何计算 传输环路限制。此限制确定在以太网传输驱动器推回到接口的队列之前允许进入驱动器的数据包的最大数量以便缓冲数据包，直到堵塞消除为止。该设置确保基于硬件的传输环路对高优先级数据包施加有限数量的额外延迟。

关于工作表的小提示：

- 出站带宽 - 例如，DSL 的上行链路速度可能为 768 Kbps。请与供应商核对。
- 最大数据包 - 通常，最大数据包为 1538 字节（标记的以太网为 1542 字节）。如果允许超巨型帧（如果平台支持），则该数据包可能更大。
- 延迟 - 延迟取决于应用程序。例如，要控制 VoIP 的抖动，应使用 20 毫秒。

表 13-2　　传输环路限制工作表

1	_____ *出站带宽（单位为Mbps 或Kbps）*	Mbps	**x 125**	**=**	_____ *# 字节 / 毫秒*		
		kbps	**x 0.125**	**=**	_____ *# 字节 / 毫秒*		
2	_____ *来自第 1 步的 # 字节 / 毫秒*		**÷** _____ *最大数据包大小（字节）*	**x**	_____ *延迟（毫秒）*	**=**	_____ *传输环路限制（# 数据包）*

配置接口的优先级队列

如果启用物理接口上流量的优先级队列，您还需要在每个接口上创建优先级队列。每个物理接口使用两个队列：一个用于优先级流量和另一个用于所有其他的流量。对于其他流量，您或者可以配置策略管制。

准备工作

- (ASASM) ASASM 不支持优先级队列。
- (ASA 5512-X 到 ASA 5555-X) 管理 0/0 接口不支持优先级队列。

操作步骤

步骤 1　创建接口的优先级队列。

priority-queue *interface_name*

示例：

```
hostname(config) # priority-queue inside
```

interface_name 参数指定要启用优先级队列的物理接口名称，或对于 ASASM，指定 VLAN 接口名称。

步骤 2　更改优先级队列的大小。

queue-limit *number_of_packets*

示例：

```
hostname(config-priority-queue)# queue-limit 260
```

默认队列限制为 1024 个数据包。由于大小有限制，队列可以填装和溢出。当队列已满时，任何额外的数据包都无法进入队列并将被丢弃（称为*尾部丢弃*）。要避免队列被填满，您可以使用 **queue-limit** 命令增加队列缓冲区大小。

queue-limit 命令的数值范围的上限在运行时动态确定。要查看此限制，请在命令行上输入 **queue-limit?** 命令。关键决定因素是支持队列所需的内存和设备上的可用内存。

指定的 **queue-limit** 对更高优先级的低延迟队列和 “ 尽力而为 ” 队列都有影响。

步骤 3　指定优先级队列的深度。

tx-ring-limit *number_of_packets*

示例：

```
hostname(config-priority-queue)# tx-ring-limit 3
```

默认 tx-ring-limit 是 128 个数据包。此命令设定在以太网传输驱动器推回到接口上的队列之前允许进入驱动器的低延迟或正常优先级数据包的最大数量以便缓冲数据包，直到堵塞消除为止。该设置确保基于硬件的传输环路对高优先级数据包施加有限数量的额外延迟。

tx-ring-limit 命令的数值范围的上限在运行时动态确定。要查看此限制，请在命令行上输入 **tx-ring-limit?** 命令。关键决定因素是支持队列所需的内存和设备上的可用内存。

指定的 **tx-ring-limit** 对更高优先级的低延迟队列和 “ 尽力而为 ” 队列都有影响。

示例

以下示例在接口 “outside”（GigabitEthernet0/1 接口）建立优先级队列，默认值为 queue-limit 和 tx-ring-limit：

```
hostname(config) # priority-queue outside
```

以下示例在接口 “outside”（GigabitEthernet0/1 接口）建立优先级队列，queue-limit 设置为 260 个数据包，tx-ring-limit 设置为 3：

```
hostname(config) # priority-queue outside
hostname(config-priority-queue)# queue-limit 260
hostname(config-priority-queue)# tx-ring-limit 3
```

配置优先级队列和策略管制的服务规则

您可以为同一策略映射中不同类映射配置优先级队列和策略管制。关于有效 QoS 配置的详细信息，请参阅第 13-3 页上的 QoS 功能如何相互作用。

准备工作

- 无法为优先级流量使用 **class - default** 类映射。
- (ASASM) ASASM 仅支持策略管制。
- 策略管制不支持流向设备的流量。
- 对于策略管制，往返 VPN 隧道的流量会绕过接口策略管制。

- 对于策略管制，匹配隧道组类映射时，仅支持出站策略管制。
- 优先级流量仅识别延迟敏感型流量。
- 关于策略管制流量，可以选择对其他流量进行策略管制，也可以将流量限制到特定类型。

操作步骤

步骤 1　创建一个类映射以识别要执行优先级队列的流量。

class-map *priority_map_name*

示例：

```
hostname(config)# class-map priority_traffic
```

步骤 2　指定类映射中的流量。

match *parameter*

示例：

```
hostname(config-cmap)# match access-list priority
```

有关详细信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 3　创建一个类映射以识别要执行策略管制的流量。

class-map *policing_map_name*

示例：

```
hostname(config)# class-map policing_traffic
```

步骤 4　指定类映射中的流量。

match *parameter*

示例：

```
hostname(config-cmap)# match access-list policing
```

有关详细信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

提示　如果使用 ACL 进行流量匹配，仅在 ACL 指定的方向上应用策略管制。即从源到目标的流量受到策略管制，但是从目标到源的流量则不受策略管制。

步骤 5　添加或编辑策略映射。

policy-map *name*

示例：

```
hostname(config)# policy-map QoS_policy
```

步骤 6　识别已为优先流量创建的类映射。

class *priority_map_name*

示例：

```
hostname(config-pmap)# class priority_class
```

步骤 7　配置类的优先级队列。

优先级

示例：

```
hostname(config-pmap-c)# priority
```

步骤 8　识别已为管制流量创建的类映射。

class *policing_map_name*

示例：

```
hostname(config-pmap)# class policing_class
```

步骤 9　配置类的策略管制。

police {**output** | **input**} *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**]] [**exceed-action** [**drop** | **transmit**]]

示例：

```
hostname(config-pmap-c)# police output 56000 10500
```

选项有：

- *conform-burst 参数* - 指定在减速到合格速率值之前连续突发中允许的短暂字节的最大数量，在 1000 和 512000000 字节之间。
- **conform-action** - 设置在速率低于 *conform_burst* 值时待采取的操作。
- *conform-rate* - 设置此流量类的速率限制；在 8000 和 2000000000 位 / 秒之间。]
- **drop** - 丢弃数据包。
- **exceed-action** - 设置当速率在 *conform-rate* 和 *conform-burst* 值之间时待采取的操作
- **input** - 在输入方向启用流量的策略管制。
- **output** - 在输出方向启用流量的策略管制。
- **transmit** - 发送数据包。

步骤 10　激活一个或多个接口上的策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy QoS_policy interface inside
```

global 选项将策略映射应用于所有接口，而 **interface** 选项将策略应用于某个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

监控 QoS

- 第 13-9 页上的 QoS 策略统计信息
- 第 13-9 页上的 QoS 优先级统计信息
- 第 13-9 页上的 QoS 优先级队列统计信息

QoS 策略统计信息

要查看流量策略管制的 QoS 统计信息，请使用 **show service-policy police** 命令。

```
hostname# show service-policy police

Global policy:
    Service-policy: global_fw_policy

Interface outside:
    Service-policy: qos
        Class-map: browse
            police Interface outside:
                cir 56000 bps, bc 10500 bytes
                conformed 10065 packets, 12621510 bytes; actions: transmit
                exceeded 499 packets, 625146 bytes; actions: drop
                conformed 5600 bps, exceed 5016 bps
        Class-map: cmap2
            police Interface outside:
                cir 200000 bps, bc 37500 bytes
                conformed 17179 packets, 20614800 bytes; actions: transmit
                exceeded 617 packets, 770718 bytes; actions: drop
                conformed 198785 bps, exceed 2303 bps
```

QoS 优先级统计信息

要查看执行 **priority** 命令的服务策略的统计信息，请使用 **show service-policy priority** 命令。

```
hostname# show service-policy priority
Global policy:
    Service-policy: global_fw_policy
Interface outside:
    Service-policy: qos
        Class-map: TG1-voice
            Priority:
                Interface outside: aggregate drop 0, aggregate transmit 9383
```

“Aggregate drop” 表示此接口中的汇聚丢弃； “Aggregate transmit” 表示此接口中已传输数据包的汇聚数量。

QoS 优先级队列统计信息

要显示接口的优先级队列统计信息，请使用 **show priority-queue statistics** 命令。结果将显示尽力而为 (BE) 队列和低延迟队列 (LLQ) 的统计信息。以下示例显示使用 **show priority-queue statistics** 命令进行接口命名测试。

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type         = BE
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0
```

```
Queue Type         = LLQ
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0
hostname#
```

在此统计报告中：

- “Packets Dropped” 表示此队列中已丢弃数据包的总数量。
- “Packets Transmit” 表示此队列中已传输数据包的总数量。
- “Packets Enqueued” 表示此队列中排队数据包的总数量。
- “Current Q Length” 表示此队列当前的深度。
- “Max Q Length” 表示此队列曾发生过的最大深度。

优先级队列和策略管制的配置示例

以下各节提供配置优先级队列和策略管制的示例。

VPN 流量的类映射示例

在以下示例中，**class-map** 命令采用一个名为 tcp_traffic 的 ACL 对所有不通过隧道传输的 TCP 流量进行分类：

```
hostname(config)# access-list tcp_traffic permit tcp any any09
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic
```

在以下示例中，采用其他更具体的匹配标准为特定安全相关隧道组进行流量分类。这些具体匹配标准规定隧道组（在本示例中指，先前定义的隧道组 1 ）上的匹配需要作为第一个匹配特征以对特定隧道的流量进行分类，并且此匹配允许一个附加匹配线对流量进行分类（IP 差分服务代码点，加速转发）。

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef
```

在以下示例中，**class-map** 命令根据流量类型对通过隧道传输的流量和不通过隧道传输的流量进行分类：

```
hostnameconfig)# access-list tunneled extended permit ip 10.10.34.0 255.255.255.0
192.168.10.0 255.255.255.0
hostname(config)# access-list non-tunneled extended permit tcp any any
hostname(config)# tunnel-group tunnel-grp1 type IPsec_L2L

hostname(config)# class-map browse
hostname(config-cmap)# description "This class-map matches all non-tunneled tcp traffic."
hostname(config-cmap)# match access-list non-tunneled

hostname(config-cmap)# class-map TG1-voice
hostname(config-cmap)# description "This class-map matches all dscp ef traffic for
tunnel-grp 1."
hostname(config-cmap)# match dscp ef
hostname(config-cmap)# match tunnel-group tunnel-grp1
```

```
hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# description "This class-map matches all best-effort traffic for
tunnel-grp1."
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address
```

以下示例显示一种在隧道内对流量进行策略管制的方式，前提是分类的流量未被指定为隧道，而是*通过*隧道。在本示例中，192.168.10.10 是远程隧道的专用端上的主机地址，且 ACL 命名为 “host-over-l2l”。通过创建类映射（命名为 " 主机特定 " ），您可以在 LAN 对 LAN 连接管制隧道之前对 " 主机特定 " 类进行策略管制。在本示例中，“ 主机特定 ” 流量先被限制速率，随后隧道被限制速率。

```
hostname(config)# access-list host-over-l2l extended permit ip any host 192.168.10.10
hostname(config)# class-map host-specific
hostname(config-cmap)# match access-list host-over-l2l
```

优先级和策略管制示例

以下示例基于上节中开发的配置。在上述示例中，有两个命名的类映射 : tcp_traffic 和 TG1-voice。

```
hostname(config)# class-map TG1-best-effort
hostname(config-cmap)# match tunnel-group Tunnel-Group-1
hostname(config-cmap)# match flow ip destination-address
```

添加第三个类映射，为定义通过隧道传输和不通过隧道传输的 QoS 策略提供依据，如下，为通过隧道传输的流量和不通过隧道传输的流量创建一个简单的 QoS 策略，从而将 TG1-voice 类的数据包分配到低延迟队列并对 tcp_traffic 和 TG1-best-effort 流量设置速率限制。

在本示例中，tcp_traffic 类流量的最大速率为 56,000 位 / 秒，最大突发大小为 10,500 字节 / 秒。TC1-BestEffort 类的最大速率为 200,000 位 / 秒，最大突发大小为 37,500 字节 / 秒。因为 TC1-voice 类属于优先级类，所以 TC1-voice 类的流量最大速率和突发速率没有受管制。

```
hostname(config)# access-list tcp_traffic permit tcp any any09
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic

hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address

hostname(config)# policy-map qos
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# police output 56000 10500

hostname(config-pmap-c)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# class TG1-best-effort
hostname(config-pmap-c)# police output 200000 37500

hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# police output 1000000 37500

hostname(config-pmap-c)# service-policy qos global
```

QoS 的历史记录

功能名称	平台版本	说明
优先级队列和策略管制	7.0(1)	我们引入了 QoS 优先级队列和策略管制。 我们引入了以下命令：**priority-queue**, **queue-limit**, **tx-ring-limit**, **priority, police, show priority-queue statistics, show service-policy police, show service-policy priority, show running-config priority-queue, clear configure priority-queue**。
整形和分级式优先级队列	7.2(4)/8.0(4)	我们引入了 QoS 整形和分级式优先级队列。 我们引入了以下命令：**shape**, **show service-policy shape**。
ASA 5585-X 标准优先级队列支持万兆以太网	8.2(3)/8.4(1)	我们为 ASA 5585-X 支持万兆以太网接口上的标准优先级队列。

连接和资源故障排除

本章介绍如何对 ASA 进行故障排除。

- 第 14-1 页上的测试配置
- 第 14-7 页上的监控每个进程的 CPU 使用情况

测试配置

此章节介绍如何为单模式 ASA 或每个安全情景测试连接，如何 ping ASA 接口，以及如何让一个接口上的主机 ping 到另一个接口的主机上。

我们建议您在故障排除期间只启用 ping 和调试消息功能。当您完成 ASA 测试后，请执行第 14-5 页上的禁用测试配置中的步骤。

- 第 14-1 页上的启用 ICMP 调试消息和系统日志消息
- 第 14-2 页上的 ping ASA 接口
- 第 14-4 页上的通过 ASA 传输流量
- 第 14-5 页上的禁用测试配置
- 第 14-5 页上的使用 traceroute 功能确定数据包路由
- 第 14-6 页上的使用数据包跟踪器跟踪数据包

启用 ICMP 调试消息和系统日志消息

调试消息和系统日志消息可帮助您解决 ping 无法成功的问题。ASA 仅显示 ping 到 ASA 接口的 ICMP 调试消息，而不会显示通过 ASA ping 到其他主机的消息。

要启用调试和系统日志消息，请执行以下步骤：

	命令	用途
步骤 1	**debug icmp trace** **示例：** `hostname(config)# debug icmp trace`	显示 ping 到 ASA 接口的 ICMP 数据包信息。

步骤 2	**logging monitor debug** **示例：** `hostname(config)# logging monitor debug`	设置要发送到 Telnet 或 SSH 会话的系统日志消息。 **注**　您也可以使用 **logging buffer debug** 命令将日志消息发送到缓冲区，稍后使用 **show logging** 命令进行查看。
步骤 3	**terminal monitor** **示例：** `hostname(config)# terminal monitor`	将系统日志消息发送到 Telnet 或 SSH 会话。
步骤 4	**logging on** **示例：** `hostname(config)# logging on`	启用系统日志消息生成。

示例

以下为从外部主机 (209.165.201.2) 成功 ping 到 ASA 外部接口 (209.165.201.1) 的示例：

```
hostname(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

输出显示 ICMP 数据包长度（32 字节），ICMP 数据包的标识符 (1) 和 ICMP 序列号（ICMP 序列号从 0 起计，每次发送请求后序列号增加）。

ping ASA 接口

要测试 ASA 接口是否打开并正常运行，以及 ASA 和相连的路由器是否正常运行，您可以 ping ASA 接口。

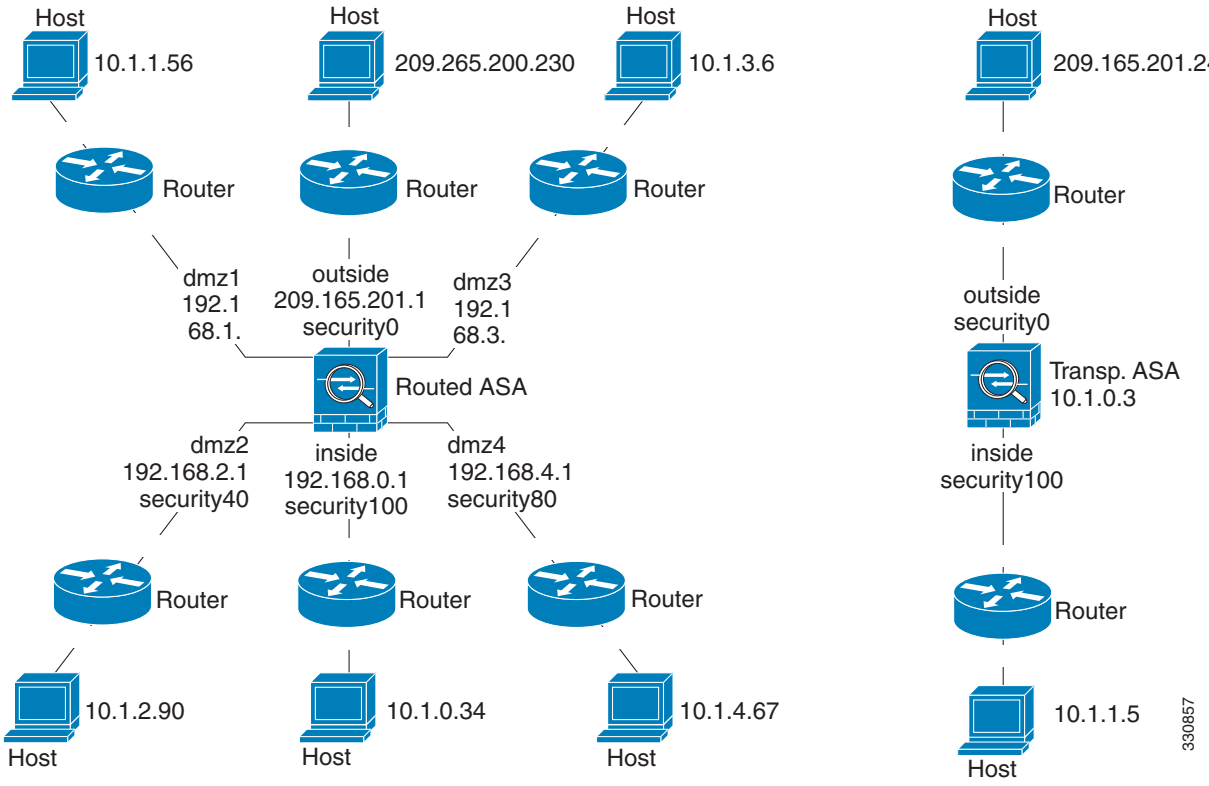
要 ping ASA 接口，请执行以下步骤：

步骤 1　绘制显示接口名称、安全级别和 IP 地址的单模式 ASA 或安全情景的示意图。

注　虽然此操作步骤使用 IP 地址，但是 **ping** 命令也支持 DNS 名称以及通过 **name** 命令分配到本地 IP 地址的名称。

示意图也应该包括所有直接连接的路由器和一台主机，该主机位于用于 ping ASA 的路由器的另一端。在此操作步骤中以及第 14-4 页上的通过 ASA 传输流量的操作步骤中您将使用此信息。（请参阅图 14-1。）

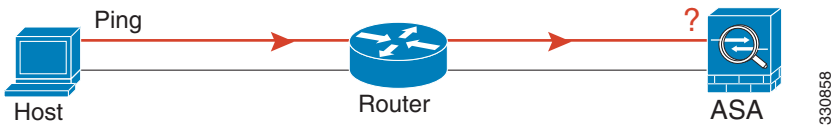
图 14-1　　接口、路由器和主机的网络图



步骤 2　从*直*接相连的路由器 ping 每个 ASA 接口。在透明模式中，ping 管理 IP 地址。此测试旨在确保 ASA 接口处于活动状态，并且接口配置正确。

如果 ASA 接口处于非活动状态、接口配置不正确，或如果 ASA 与路由器之间的交换机关闭（请参阅图 14-2），ping 操作可能会失败。在这种情况下，数据包不能到达 ASA，因此调试消息或系统日志消息不会显示。

图 14-2　　ASA 接口 ping 故障

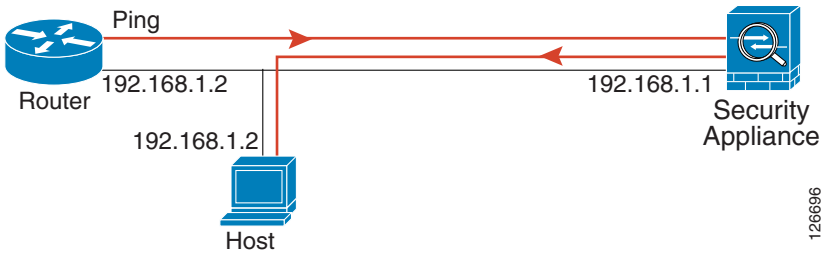


如果 ping 到达 ASA 并且得到响应，调试消息显示类似的以下内容：

```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

如果 ping 回复没有返回路由器，则可能存在一个交换机环路或冗余 IP 地址（请参阅图 14-3）。

图 14-3　IP 编址问题引发的 ping 故障



步骤 3　从一台远程主机上 ping 每个 ASA 接口。在透明模式中，ping 管理 IP 地址。此测试检查直接连接的路由器是否能在主机和 ASA 之间路由数据包，以及 ASA 是否可以正确地将数据包路由回主机。

如果 ASA 没有通过中间路由器返回路由到主机，ping 操作可能失败（请参阅图 14-4）。在这种情况下，调试消息显示 ping 成功，但是系统日志消息 110001 显示，提示出现路由故障。

图 14-4　ASA 没有返回路由引发的 ping 故障

通过 ASA 传输流量

在成功 ping 到 ASA 接口后，确保流量可以成功通过 ASA。默认情况下，您可以从安全性高的端口 ping 安全性低的端口。您只需要启用 ICMP 检测以允许回程流量通行即可。要想从高到低进行 ping，您需要应用 ACL 来允许流量。如果使用 NAT，测试显示 NAT 运行正常。

从一个源接口的主机或路由器 ping 另一个接口上的主机或路由器。无论您想要检查多少接口对，都可以重复此步骤。

如果 ping 成功，系统将显示系统日志消息确认路由模式的地址转换（305009 或 305011），并确认已创建一个 ICMP 连接（302020）。您还可以输入 **show xlate** 或 **show conns** 命令查看此信息。

如果 NAT 配置错误，ping 操作可能会失败。在这种情况下，系统会显示系统日志消息，表示 NAT 失败（305005 或 305006）。如果在没有静态转换的情况下从外部主机 ping 内部主机，系统将会显示以下系统日志消息：

```
%ASA-3-106010: deny inbound icmp.
```

注　ASA 仅显示 ping 到 ASA 接口的 ICMP 调试消息，而不会显示通过 ASA ping 到其他主机的消息。

图 14-5　ASA 未进行地址转换引发的 ping 故障

详细步骤

	命令	用途
步骤 1	`policy-map global_policy`	编辑默认全局策略并输入策略映射配置模式。
步骤 2	`class inspection_default`	编辑默认类映射，与标准协议和端口的应用流量匹配。对于 ICMP，此类匹配所有 ICMP 流量。
步骤 3	`inspect icmp`	启用 ICMP 检测引擎并确保 ICMP 响应可以返回到源主机。
步骤 4	（对于低安全性接口可选） `access-list ICMPACL extended permit icmp any any`	添加一个 ACL 以允许来自任意源主机的 ICMP 流量。
步骤 5	`access-group ICMPACL in interface outside`	将 ACL 分配到外部接口。如果名称不同，使用您的接口名称替换 " outside " 。为每个想要允许从高安全性到低安全性 ICMP 流量的接口重复该命令。 **注**　在将此 ACL 应用到一个非最低安全性的接口后，仅允许 ICMP 流量；移除高安全性到低安全性的隐式许可。例如，要允许 DMZ 接口（第 50 级）ping 内部接口（第 100 级），您需要应用此 ACL。然而，由于目前从 DMZ 到外部（级别 0 ）的流量仅限 ICMP 流量，而非之前隐式许可允许的所有流量。测试 ping 后，请务必从您的接口删除此 ACL，尤其是要恢复隐式许可 (**no access-list ICMPACL**) 的接口。

禁用测试配置

在您完成测试后，请禁用会允许 ICMP 到达及通过 ASA 的测试配置以及会打印调试消息的测试配置。如果您对此配置不作更改，它可能会带来严重的安全隐患。调试消息会阻碍 ASA 性能。

要禁用测试配置，请执行以下步骤：

	命令	用途
步骤 1	`no debug icmp trace`	禁用 ICMP 调试消息。
步骤 2	`no logging on`	禁用日志记录。
步骤 3	`no access-list ICMPACL`	移除 ICMPACL ACL，然后删除相关 **access-group** 命令。

步骤 4	`policy-map global_policy`
	`  class inspection_default`
	`  no inspect icmp`
		（可选）禁用 ICMP 检测引擎。

使用 traceroute 功能确定数据包路由

您可以使用 traceroute 功能跟踪数据包的路由，使用 **traceroute** 命令访问。将 UDP 数据包发送到一个无效端口上的目标地址，traceroute 即可启用。由于端口无效，到达目标地址过程中的路由器回应的是一个 ICMP Time Exceeded 消息，并将该错误报告给 ASA。

使用数据包跟踪器跟踪数据包

数据包跟踪器工具为数据包嗅探和网络故障隔离提供数据包跟踪服务，也可以提供数据包的详细信息以及 ASA 如何处理数据包。如果配置命令没有导致数据包被丢弃，数据包跟踪器工具会以便于读取的方式提供其原因的相关信息。

您可以使用数据包跟踪器工具进行以下操作：

- 通过 ASA 跟踪数据包的使用期限，查看数据包是否正常运行。
- 在生产网络中调试所有数据包丢失。
- 验证配置是否按预期运行。
- 显示适用于数据包的所有规则，同时也显示引发规则增加的 CLI 命令。
- 在数据路径显示数据包变更的时间线。
- 在数据路径中注入跟踪器数据包。
- 基于用户身份和 FQDN 搜索 IPv4 或 IPv6 地址。
- 调试允许或拒绝特定会话的原因。
- 确定正在使用哪种安全组标记 (SGT) 值（即来自数据包中的 SGT、IP-SGT 管理器，或接口上配置的 **policy static sgt** 命令）。
- 确定应用了哪些基于安全组的安全政策。

要跟踪数据包，请输入以下命令：

命令	用途
packet-tracer input [*ifc_name*] [**icmp** [**inline-tag** *tag*] [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*]| **fqdn** *fqdn-string*] *type code ident* [*dip* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*]] | [**tcp** [**inline-tag** *tag*] [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] *sport* [*dip* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] *dport*] | [**udp** [**inline-tag** *tag*] [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] *sport* [*dip* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] *dport*] | [**rawip** [**inline-tag** *tag*] [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] [*dip* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] | **security-group** [**name** *name* | **tag** *tag*] [**detailed**] [**xml**] **示例：** `hostname# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed`	提供数据包的详细信息以及 ASA 如何处理这些数据包。示例显示如何从启用从内部主机 10.2.25.3 到外部主机 209.165.202.158 的数据包跟踪并提供详细信息。

监控每个进程的 CPU 使用情况

您可以监控 CPU 上运行的进程。可以获得某个进程的 CPU 使用百分比信息。CPU 使用情况统计信息以降序排序显示，占比最高的进程排在顶部。也包括每个进程的 CPU 负载信息，显示日志时间之前 5 秒、1 分钟和 5 分钟的数据。此信息每 5 秒自动更新一次，提供实时的统计信息。

您可以使用 **show process cpu-usage sorted** 命令查看进程相关的任何已配置上下文消耗的 CPU 负载分解数据。

第 5 部分

高级网络保护

ASA 和思科云网络安全

思科云网络安全通过软件即服务 (SaaS) 模式提供网络安全和网络过滤服务。如果在网络中已部署 ASA，企业无需安装附加硬件即可使用云网络安全服务。

当云网络安全在 ASA 上启用时，ASA 会将选择的 HTTP 和 HTTPS 流量透明地重定向到云网络安全代理服务器。然后，云网络安全代理服务器扫描内容，根据在思科 ScanCenter 中配置的策略，允许、阻止或发送有关流量的警告，以执行可接受的使用并保护用户不受恶意软件攻击。

或者，ASA 可以利用身份防火墙 (IDFW) 和 AAA 规则进行身份验证以识别用户。ASA 对用户凭证（包括用户名和 / 或用户组）进行加密，将其包含在被重定向到云网络安全的流量中。然后，云网络安全服务使用这些用户凭证使流量与策略匹配。此外，还将这些凭证用于基于用户的报告。如果没有用户身份验证，ASA 能够提供（可选）默认用户名和 / 或组，尽管云网络安全服务应用策略并不要求用户和组。

创建服务策略规则时，您可以自定义想要发送到云网络安全的流量。此外，您还可以配置一份“ 白名单 ”，使匹配服务策略规则的网络流量子集不经云网络安全扫描便直接流向最初请求的网络服务器。

您可以配置一台主用云网络安全代理服务器和一台备用云网络安全代理服务器，ASA 会定期轮询每台服务器，以检查可用性。

注 此功能也叫作 “ScanSafe”，因此，ScanSafe 名称出现在一些命令中。

- 第 15-2 页上的有关思科云网络安全的信息
- 第 15-6 页上的思科云网络安全的许可证要求
- 第 15-6 页上的云网络安全先决条件
- 第 15-6 页上的准则和限制
- 第 15-7 页上的默认设置
- 第 15-7 页上的配置思科云网络安全
- 第 15-15 页上的监控云网络安全
- 第 15-16 页上的思科云网络安全配置示例
- 第 15-23 页上的相关文档
- 第 15-24 页上的功能历史思科云网络安全

有关思科云网络安全的信息

- 第 15-2 页上的网络流量重定向到云网络安全
- 第 15-2 页上的用户身份验证和云网络安全
- 第 15-2 页上的身份验证密钥
- 第 15-3 页上的 ScanCenter 策略
- 第 15-4 页上的云网络安全操作
- 第 15-5 页上的通过白名单绕过扫描
- 第 15-5 页上的 IPv4 和 IPv6 支持
- 第 15-5 页上的从主用代理服务器到备用代理服务器的故障转移

网络流量重定向到云网络安全

当最终用户发送 HTTP 或 HTTPS 请求时，ASA 接收请求，并或者检索用户和 / 或组信息。如果流量匹配 ASA 云网络安全服务策略，ASA 会将请求重定向到云网络安全代理服务器。通过将连接重定向到代理服务器，ASA 充当最终用户和云网络安全代理服务器之间的媒介。ASA 改变客户请求中的目标 IP 地址和端口，添加云网络安全特定 HTTP 标头，然后将修改的请求发送到云网络安全代理服务器。这些云网络安全 HTTP 标头包括各种信息，包括用户名和用户组（如果可用）。

用户身份验证和云网络安全

用户身份可用于在云网络安全中应用策略。此外，用户身份对于云网络安全报告也非常有用。使用云网络安全并不要求用户身份。还存在其他为云网络安全策略识别流量的方法。

ASA 支持以下确定用户身份或提供默认身份的方法：

- AAA 规则 - 当 ASA 使用 AAA 规则执行用户身份验证时，从 AAA 服务器或本地数据库检索用户名。来自 AAA 规则的身份不包含组信息。如果已配置默认组，则使用默认组。有关配置 AAA 规则的详细信息，请参阅旧版功能指南。
- IDFW - 当 ASA 使用带 Active Directory (AD) 的 IDFW 时，在您通过在访问规则等功能或服务策略中使用 ACL，或者通过配置用户身份监控直接下载用户身份信息激活用户和 / 或组时，从 AD 代理检索用户名和组。

  有关配置 IDFW 的详细信息，请参阅常规操作配置指南。
- 默认用户名和组 - 如果没有用户身份验证， ASA 会将可选的默认用户名和 / 组用于所有匹配云网络安全服务策略的用户。

身份验证密钥

每个 ASA 必须使用您从云网络安全获取的身份验证密钥。身份验证密钥可以让云网络安全识别与网络请求相关联的公司，确保 ASA 与有效的客户相关联。

您可以将两种身份验证密钥的其中一种用于 ASA：公司密钥和组密钥。

- 第 15-3 页上的公司身份验证密钥
- 第 15-3 页上的组身份验证密钥

公司身份验证密钥

公司身份验证密钥可以在同一公司内的多个 ASA 上使用。此密钥可以为 ASA 启用云网络安全服务。管理员在 ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp) 中生成此密钥；您可以通过邮件发送此密钥，以备后续使用。您后续无法在 ScanCenter 中查找此密钥； ScanCenter 中仅显示最后 4 位数。有关详细信息，请参阅云网络安全文档：http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html。

组身份验证密钥

组身份验证密钥是一个特殊密钥，对于每个执行两项功能的 ASA 具有唯一性：

- 为一个 ASA 启用云网络安全服务。
- 识别所有来自 ASA 的流量，因此，您能够为每个 ASA 创建 ScanCenter 策略。

有关将组身份验证密钥用于策略的详细信息，请参阅第 15-3 页上的 ScanCenter 策略。

管理员在 ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp) 中生成此密钥；您可以通过邮件发送此密钥，以备后续使用。您后续无法在 ScanCenter 中查找此密钥； ScanCenter 中仅显示最后 4 位数。有关详细信息，请参阅云网络安全文档：http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html。

ScanCenter 策略

在 ScanCenter 中，流量按顺序匹配策略规则，直到某个规则被匹配。然后，云网络安全应用已配置的规则操作。用户流量可以根据组关联在 ScanCenter 中匹配策略规则：*directory group* 或 *custom group*。

- 第 15-3 页上的目录组
- 第 15-4 页上的自定义组
- 第 15-4 页上的组和身份验证密钥如何进行互操作

目录组

目录组定义流量所属的组。如果有的话，组包含在客户端请求的 HTTP 标头中。当您配置 IDFW 时，ASA 将组包含在 HTTP 标头中。如果不使用 IDFW，您可以为匹配 ASA 云网络安全检测规则的流量配置默认组。

当您配置目录组时，必须正确输入组名。

- IDFW 组名按以下格式发送：

  *domain-name**group-name*

  当 ASA 获悉 IDFW 组名时，ASA 上的格式为 *domain-name**group-name*。然而，ASA 会修改此名称，仅使用一个反斜线符号 (\) 以符合典型的 ScanCenter 表示法。

- 默认组名按以下格式发送：

  [*domain*\]*group-name*

  在 ASA 上，您需要配置可选域名，使选域名后跟 2 个反斜线符号 (\\)；然而，ASA 会修改此名称，仅使用一个反斜线符号 (\) 以符合典型的 ScanCenter 表示法。例如，如果您指定 “Cisco\\Boulder1”， ASA 会在将组名发送到云网络安全时，将组名修改为 “Cisco\Boulder1”，仅使用一个反斜线符号 (\)。

自定义组

使用以下一个或多个条件定义自定义组：

- ScanCenter 组身份验证密钥 - 您可以为自定义组生成一个组身份验证密钥。然后，如果在配置 ASA 时识别此组密钥，所有来自 ASA 的流量都将使用此组密钥标记。
- 源 IP 地址 - 您可以在自定义组中识别源 IP 地址。请注意，ASA 服务策略基于源 IP 地址，因此，您可能会想在 ASA 上配置任何基于 IP 地址的策略。
- 用户名 - 您可以在自定义组中识别用户名。
  - IDFW 用户名按以下格式发送：

    domain-name\username
  - 使用 RADIUS 或 TACACS+ 时，AAA 用户名按以下格式发送：

    LOCAL*username*
  - 使用 LDAP 时，AAA 用户名按以下格式发送：

    domain-name\username
  - 默认用户名按以下格式发送：

    [*domain-name*\]*username*

    例如，如果您将默认用户名配置为 “Guest”，ASA 则发送 “Guest”。如果您将默认用户名配置为 “Cisco\Guest”，ASA 则发送 “Cisco\Guest”。

组和身份验证密钥如何进行互操作

除非您需要自定义 group+group 密钥提供的每 ASA 策略，否则您可能将使用公司密钥。请注意，并非所有的自定义组都与组密钥相关联。未加密的自定义组可用于识别 IP 地址或用户名，并且可在策略以及使用目录组的规则中使用。

即使您的确需要每 ASA 策略并且正在使用组密钥，您也可以使用目录组和非加密自定义组提供的匹配功能。在这种情况下，您可能需要基于 ASA 的策略，但有一些基于组成员身份、 IP 地址或用户名的策略除外。例如，如果您想免除所有 ASA 上 America/Management 组中的用户：

1. 为 America/Management 添加目录组。
2. 为此组添加免除规则。
3. 在免除规则的后面，为每个自定义 group+group 密钥添加规则，以按 ASA 应用策略。
4. 来自 America\Management 中的用户的流量将匹配免除规则，而所有其他流量将匹配其来源 ASA 的规则。

您可以将诸多密钥、组和策略规则进行组合。

云网络安全操作

在应用已配置的策略之后，云网络安全阻止、允许或发送有关用户请求的警告：

- 允许 - 当云网络安全允许客户端请求时，会联系最初请求的服务器并检索数据。云网络安全将服务器响应转发给 ASA，然后再转发给用户。
- 阻止 - 当云网络安全阻止客户端请求时，会通知用户访问已被阻止。云网络安全发送 HTTP 302 “Moved Temporarily” 响应，将客户端应用重定向到云网络安全代理服务器托管的网页，该网页显示被阻止的错误消息。 ASA 将 302 响应转发给客户端。

- 警告 - 当云网络安全代理服务器确定网站可能违反了可接受的使用策略时，会显示有关网站的警告页面。您可以选择听从警告并丢弃连接请求，也可以点击浏览警告，转到请求的站点。

此外，您还可以选择 ASA 对无法到达主或备云网络安全代理服务器的网络流量的处理方式。可以阻止或允许所有网络流量。默认情况下，阻止网络流量。

通过白名单绕过扫描

如果您使用 AAA 规则或 IDFW，您可以配置 ASA，使来自特定用户或组的匹配服务策略规则的网络流量不被重定向到云网络安全代理服务器进行扫描。当您绕过云网络安全扫描时， ASA 不会联系代理服务器，而直接从最初请求的网络服务器检索内容。当 ASA 收到来自网络服务器的响应时，会将数据发送到客户端。此过程被称作 “ 白名单 ” 流量。

尽管在使用 ACL 配置流量类以发送到云网络安全时，实现的结果与根据用户或组免除流量实现的结果相同，但您可能发现，使用白名单更加简单。请注意，白名单功能仅基于用户和组，不基于 IP 地址。

IPv4 和 IPv6 支持

云网络安全目前仅支持 IPv4 地址。如果您在内部使用 IPv6，必须对任何需要发送到云网络安全的 IPv6 流量执行 NAT 64。

下表显示了云网络安全重定向支持的类映射流量：

类映射流量	云网络安全检测
从 IPv4 到 IPv4	受支持的
从 IPv6 到 IPv4（使用 NAT64）	受支持的
从 IPv4 到 IPv6	不支持
从 IPv6 到 IPv6	不支持

从主用代理服务器到备用代理服务器的故障转移

当您订用思科云网络安全服务时，您将被分配一台主用云网络安全代理服务器和一台备用代理服务器。

如果任何客户端都无法到达主用服务器，则 ASA 开始轮询塔式服务器，以确定可用性。（如果没有客户端活动，则 ASA 每 15 分钟轮询一次。）如果代理服务器在配置的重试次数 （默认为 5 次，此设置可以配置）之后不可用，该服务器将被宣布为无法访问，进而备用代理服务器进入活动状态。

如果在达到重试计数之前，客户端或 ASA 至少能够连续两次到达该服务器，轮询将停止，而且塔式服务器被确定可以访问。

在故障转移到备用服务器后， ASA 继续轮询主用服务器。如果主用服务器恢复为可以访问，则 ASA 重新使用主用服务器。

思科云网络安全的许可证要求

型号	许可证要求
ASAv	标准或高级许可证。
所有其他型号	基础许可证。

在云网络安全端，您必须购买思科云网络安全许可证，并识别 ASA 处理的用户数量。然后，登录 ScanCenter，生成身份验证密钥。

云网络安全先决条件

（可选）用户身份验证先决条件

要将用户身份信息发送到云网络安全，请在 ASA 上配置以下项目之一：

- AAA 规则（仅用户名）- 请参阅旧版功能指南。
- IDFW（用户名和组）- 请参阅常规操作配置指南。

（可选）完全限定域名先决条件

如果您将 ACL 中的 FQDN 用于服务策略规则或云网络安全服务器，您必须根据常规操作配置指南为 ASA 配置 DNS 服务器。

准则和限制

情景模式准则

支持单一和多情景模式。

在多情景模式中，仅允许在系统中进行服务器配置，并且仅允许在安全情景中进行服务器策略规则配置。

如果需要的话，每个情景都可以拥有各自的身份验证密钥。

防火墙模式准则

仅支持路由防火墙模式。不支持透明防火墙模式。

IPv6 准则

不支持 IPv6。请参阅第 15-5 页上的 IPv4 和 IPv6 支持。

其他准则

- 云网络安全不支持 ASA 集群。
- 无客户端 SSL VPN 不支持云网络安全，请务必将任何无客户端 SSL VPN 流量从 ASA 云网络安全服务策略中免除。
- 当指向云网络安全代理服务器的接口发生故障时，**show scansafe server** 命令输出要花大约 15-25 分钟才能显示出两台服务器。发生这种情况的原因是，轮询机制基于活动连接，而且接口发生故障，显示零连接，所以采用了轮询时间最长的方法。

- 云网络安全不支持 ASA CX 模块。如果为同一流量配置 ASA CX 操作和云网络安全检测，则 ASA 仅执行 ASA CX 操作。
- 对于同一流量，云网络安全检测兼容 HTTP 检测。 HTTP 检测作为默认全局策略的一部分默认被启用。
- 云网络安全不支持扩展 PAT 或任何可能使用同一源端口和 IP 地址进行不同连接的应用。例如，如果两个不同连接（以不同服务器为目标）使用扩展 PAT，ASA 可能将同一源 IP 和源端口重用于两个连接转换，因为对于不同目标来说它们是有区别的。当 ASA 将这些连接重定向到云网络安全服务器时，会用云网络安全服务器 IP 地址和端口（默认为 8080）替换目标。结果，两个连接现在看起来属于同一流量（相同源 IP/ 端口和目标 IP/ 端口），导致返回流量无法被适当地反向转换。
- **match default-inspection-traffic** 命令 流量类不包含云网络安全检测的默认端口（80 和 443）。

默认设置

默认情况下，不启用思科云网络安全。

配置思科云网络安全

- 第 15-7 页上的配置与云网络安全代理服务器的通信
- 第 15-8 页上的 （多情景模式）根据安全情景允许云网络安全
- 第 15-9 页上的配置服务策略，将流量发送到云网络安全
- 第 15-13 页上的 （可选）配置白名单流量
- 第 15-14 页上的配置云网络安全策略

配置与云网络安全代理服务器的通信

准则

公钥嵌入在 ASA 软件中，因此，您无需配置。

详细步骤

	命令	用途
步骤 1	**scansafe general-options** **示例：** `hostname(config)# scansafe general-options`	进入 scansafe general-options 配置模式。
步骤 2	**server primary** {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*] **示例：** `hostname(cfg-scansafe)# server primary ip 192.168.43.10`	配置主用云网络安全代理服务器的完全限定域名或 IP 地址。 默认情况下，云网络安全代理服务器将端口 8080 用于 HTTP 和 HTTPS 流量；除非您被要求更改，否则请勿更改此值。

	命令	用途
步骤 3	**server backup** {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*] **示例：** `hostname(cfg-scansafe)# server backup fqdn server.example.com`	（可选）配置备用云网络安全代理服务器的完全限定域名或 IP 地址。 默认情况下，云网络安全代理服务器将端口 8080 用于 HTTP 和 HTTPS 流量；除非您被要求更改，否则请勿更改此值。
步骤 4	**retry-count** *value* **示例：** `hostname(cfg-scansafe)# retry-count 2`	（可选）在确定云网络安全代理服务器无法访问之前，输入服务器连续轮询失败的次数。每 30 秒执行一次轮询。有效值介于 2 和 100 之间，默认为 5。 请参阅第 15-5 页上的从主用代理服务器到备用代理服务器的故障转移。
步骤 5	**license** *hex_key* **示例：** `hostname(cfg-scansafe)# license F12A588FE5A0A4AE86C10D222FC658F3`	配置 ASA 发送到云网络安全代理服务器的身份验证密钥，指明请求来自哪个公司。身份验证密钥是一个 16 字节的十六进制数字。 请参阅第 15-2 页上的身份验证密钥。

示例

以下示例配置主用和备用服务器：

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server primary ip 10.10.0.7 port 8080
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

（多情景模式）根据安全情景允许云网络安全

在多情景模式下，您必须根据情景允许云网络安全。有关详细信息，请参阅常规操作配置指南。

注　必须在管理员情景和特定情景中指定一个指向 Scansafe 塔式服务器的路由。这可以确保 Scansafe 塔式服务器不会在主动 / 主动故障转移情境中变得无法访问。

以下示例配置在采用默认许可证的情景 1 和采用许可证密钥覆盖的情景 2 中启用了云网络安全：

```
!System Context
!
scansafe general-options
server primary ip 180.24.0.62 port 8080
retry-count 5
license 366C1D3F5CE67D33D3E9ACEC265261E5
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
```

```
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC26789534
 config-url disk0:/two_ctx.cfg
!
```

配置服务策略，将流量发送到云网络安全

有关服务策略规则的详细信息，请参阅第 1 章，“使用模块化策略框的服务策略”，。

先决条件

（可选）如果您需要使用白名单，使某些流量免于被发送到云网络安全，则首先根据第 15-13 页上的 （可选）配置白名单流量创建白名单，以便在服务策略规则中参照此白名单。

详细步骤

	命令	用途
步骤 1	**policy-map type inspect scansafe** *name1* **示例：** `hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1`	创建检测策略映射，以便能够为规则配置基本参数，并且或者识别白名单。对于您想发送到云网络安全的每个流量类，都要求检测策略映射。 参数 *policy_map_name* 最大长度为 40 个字符。 进入策略映射配置模式。
步骤 2	parameters **示例：** `hostname(config-pmap)# parameters`	通过这些参数，您可以配置协议和默认用户或组。进入参数配置模式。
步骤 3	**{http | https}** **示例：** `hostname(config-pmap-p)# http`	您只能为该检测策略映射指定一个服务类型， **http** 或 **https**。
步骤 4	（可选） **default** {**[user** *username*] [**group** *groupname*]} **示例：** `hostname(config-pmap-p)# default group default_group`	指定如果 ASA 无法确定进入 ASA 的用户的身份，则默认用户和 / 或组将包含在 HTTP 标头中。
步骤 5	（可选，对于白名单） **class** *whitelist_name* **示例：** `hostname(config-pmap-p)# class whitelist1`	识别您在第 15-13 页上的 （可选）配置白名单流量中创建的白名单类映射名称。

	命令	用途
步骤 6	whitelist **示例：** hostname(config-pmap-p)# class whitelist1 hostname(config-pmap-c)# whitelist	对流量类执行白名单操作。
步骤 7	**policy-map type inspect scansafe** *name2* parameters **default** {**[user** *user*] [**group** *group*]} **class** *whitelist_name2* whitelist **示例：** hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2 hostname(config-pmap)# parameters hostname(config-pmap-p)# default group2 default_group2 hostname(config-pmap-p)# class whitelist2 hostname(config-pmap-c)# whitelist	重复步骤 1 至步骤 6，为 HTTP 流量 （例如）创建单独的类映射。您可以为想发送到云网络安全的每个流量类创建检测类映射。如果需要的话，您可以将一个检测类别重用于多个流量类。
步骤 8	**access-list** *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} **tcp** [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] *dest_address_argument* [*port_argument*] **示例：** hostname(config)# object network cisco1 hostname(config-object-network)# fqdn www.cisco.com hostname(config)# object network cisco2 hostname(config-object-network)# fqdn tools.cisco.com hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80 hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80 hostname(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80	识别您想发送到云网络安全的流量类。创建包含一个或多个访问控制条目 (ACE) 的 ACL。有关 ACL 的详细信息，请参阅常规操作配置指南。 云网络安全只能在 HTTP 和 HTTPS 流量上运行。每种类型的流量都被 ASA 单独处理。因此，您需要创建仅 HTTP ACL 和仅 HTTPS ACL。根据策略需求创建多个 ACL。 **permit** ACE 将匹配流量发送到云网络安全。 **deny** ACE 使流量免受服务策略规则的约束，因此，流量不会被发送到云网络安全。 创建 ACL 时，请考虑如何匹配以互联网为目标的相应流量，但不匹配以其他内部网络为目标的流量。例如，当目标为 DMZ 上的内部服务器时，为阻止内部流量被发送到云网络安全，请务必将 deny ACE 添加到 ACL，使流量免于被发送到 DMZ。 对于使流量免于被发送到特定服务器， FQDN 网络对象可能比较有用。 您可以使用 *user_argument* 指定 IDFW 用户名或组，采用内联或参考对象组。 您可以使用 *security_group_argument* 指定 TrustSec 安全组，采用内联或参考对象组。请注意，尽管您可以按安全组匹配要发送到云网络安全的流量，但 ASA 不会在 HTTP 标头中将安全组信息发送到云网络安全；云网络安全无法根据安全组创建策略。
步骤 9	**class-map** *name1* **示例：** hostname(config)# class-map cws_class1	创建类映射，识别您想为其启用云网络安全过滤的流量。

	命令	用途
步骤 10	**match access-list** *acl1* **示例：** hostname(config-cmap)# match access-list SCANSAFE_HTTP	指定在步骤 8 中创建的 ACL。 尽管您可以使用此规则的其他匹配语句，但我们建议您使用 **match access-list** 命令，因为对于识别仅 HTTP 或仅 HTTPS 流量来说，该命令功能最齐全。有关详细信息，请参阅第 1-12 页上的识别流量 （第 3/4 层类映射）。
步骤 11	**class-map** *name2* **match access-list** *acl2* **示例：** hostname(config)# class-map cws_class2 hostname(config-cmap)# match access-list SCANSAFE_HTTPS	（可选）创建附加的类映射 （例如，为 HTTPS 流量创建）。您可以按需为该服务策略规则创建多个类。
步骤 12	**policy-map** *name* **示例：** hostname(config)# policy-map cws_policy	添加或编辑策略映射，以设置要对类映射流量执行的操作。此策略映射在默认全局策略中被称作 global_policy。您可以编辑该策略，或者创建新策略。您只能将一项策略应用到每个接口或全局应用。
步骤 13	**class** *name1* **示例：** hostname(config-pmap)# class cws_class1	识别在步骤 9 中创建的类映射。
步骤 14	**inspect scansafe** *scansafe_policy_name1* [**fail-open** | **fail-close**] **示例：** hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open	为该类中的流量启用云网络安全检测。指定您在步骤 1 中创建的检测类映射名称。 指定 **fail-open** 的话，如果云网络安全服务器不可用，将会允许流量穿过 ASA。 指定 **fail-close** 的话，如果云网络安全服务器不可用，将会丢弃所有流量。默认设置为 **fail-close**。
步骤 15	**class** *name2* **inspect scansafe** *scansafe_policy_name2* [**fail-open** | **fail-close**] **示例：** hostname(config-pmap)# class cws_class2 hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open	（可选）识别您在步骤 11 中创建的第二个类映射，并为其启用云网络安全检测。 您可以按需配置多个类映射。
步骤 16	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **示例：** hostname(config)# service-policy cws_policy inside	在一个或多个接口上激活策略映射。 **global** 可以将策略映射应用到所有接口， **interface** 可以将策略应用到某个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。有关详细信息，请参阅第 1-16 页上的将操作应用到接口 （服务策略）。

示例

以下示例配置两个类：一个是 HTTP 流量类，一个是 HTTPS 流量类。每个 ACL 都可以使 HTTP 和 HTTPS 流量免于被发送到 www.cisco.com 和 tools.cisco.com，以及 DMZ 网络。所有其他流量将被发送到云网络安全，但来自若干白名单用户和组的流量除外。然后，策略将被应用到内部接口。

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
hostname(config-cmap)# match user user1 group cisco
hostname(config-cmap)# match user user2
hostname(config-cmap)# match group group1
hostname(config-cmap)# match user user3 group group3

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
hostname(config-pmap-p)# default group default_group
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
hostname(config-pmap)# parameters
hostname(config-pmap-p)# https
hostname(config-pmap-p)# default group2 default_group2
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# object network cisco1
hostname(config-object-network)# fqdn www.cisco.com
hostname(config)# object network cisco2
hostname(config-object-network)# fqdn tools.cisco.com
hostname(config)# object network dmz_network
hostname(config-object-network)# subnet 10.1.1.0 255.255.255.0

hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
80
hostname(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80

hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco1 eq 443
hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco2 eq 443
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
443
hostname(config)# access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443

hostname(config)# class-map cws_class1
hostname(config-cmap)# match access-list SCANSAFE_HTTP
hostname(config)# class-map cws_class2
hostname(config-cmap)# match access-list SCANSAFE_HTTPS

hostname(config)# policy-map cws_policy
hostname(config-pmap)# class cws_class1
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
hostname(config-pmap)# class cws_class2
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
hostname(config)# service-policy cws_policy inside
```

（可选）配置白名单流量

如果您使用用户身份验证，可以根据用户名和 / 或组名，使某些流量免于被云网络安全过滤。配置云网络安全服务策略规则时，您可以参考白名单检测类映射。 IDFW 和 AAA 用户凭证均可以与此功能一起使用。

尽管配置服务策略规则时实现的结果与根据用户或组免除流量实现的结果相同，但您可能发现，使用白名单更简单。请注意，白名单功能仅基于用户和组，不基于 IP 地址。

详细步骤

	命令	用途
步骤 1	**class-map type inspect scansafe** [**match-all** | **match-any**] *name* **示例：** `hostname(config)# class-map type inspect scansafe match-any whitelist1`	为白名单用户和组创建检测类映射。 参数 *class_map_name* 为类映射名称，最大长度为 40 个字符。 **match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。 关键字 **match-any** 指定如果流量匹配至少一个条件，则匹配类映射。 CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。
步骤 2	**match** [**not**] {[**user** *username*] [**group** *groupname*]} **示例：** `hostname(config-cmap)# match`	关键字 **match** 后跟一个特定用户名或组名，向白名单指定某个用户或组。 关键字 **match not** 指定用户和 / 或组应当使用云网络安全过滤。例如，如果将组 “cisco” 列入白名单，但想扫描来自用户 “johncrichton” 和 “aerynsun” 的流量，您可以为这些用户指定 **match not**。重复此命令，按需添加多个用户和组。

示例

以下示例将 HTTP 和 HTTPS 检测策略映射的相同用户和组列入白名单：

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
hostname(config-cmap)# match user user1 group cisco
hostname(config-cmap)# match user user2
hostname(config-cmap)# match group group1
hostname(config-cmap)# match user user3 group group3

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
hostname(config-pmap-p)# default group default_group
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
hostname(config-pmap)# parameters
hostname(config-pmap-p)# https
hostname(config-pmap-p)# default group2 default_group2
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist
```

（可选）配置用户身份监控

使用 IDFW 时， ASA 仅为包含在活动 ACL 中的用户和组从 AD 服务器下载用户身份信息；该 ACL 必须在访问规则、 AAA 规则、服务、策略规则等功能或者被视为活动的其他功能中使用。因为云网络安全可以使其策略以用户身份为基础，所以您可能需要下载不包含在活动 ACL 中的组，使 IDFW 覆盖所有用户。例如，尽管您可以配置云网络安全服务策略规则使用带用户和组的 ACL，从而激活任何相关组，但这不是必需的；您可以使用完全基于 IP 地址的 ACL。通过用户身份监控功能，您可以让直接从 AD 代理下载组信息。

限制

ASA 最多只能监控 512 个组，包括为用户身份监控配置的组和通过活动 ACL 监控的组。

详细步骤

命令	用途
user-identity monitor {**user-group** [*domain-name*\\]*group-name* | **object-group-user** *object-group-name*} **示例：** `hostname(config)# user-identity monitor user-group CISCO\\Engineering`	从 AD 代理下载指定的用户或组信息。 • **user-group** - 指定内联组名。尽管您在域和组之间指定 2 个反斜线符号 (\\)，但 ASA 会在将名称发送到云网络安全时修改名称，使其仅包含 1 个反斜线符号，以符合云网络安全表示法约定。 • **object-group-user** - 指定 **对象组用户** 名。此组可以包含多个组。

配置云网络安全策略

配置 ASA 服务策略规则后，启动 ScanCenter Portal，配置网络内容扫描、过滤、恶意软件检查服务和报告。

详细步骤

转至：https://scancenter.scansafe.com/portal/admin/login.jsp。

有关详细信息，请参阅 《思科 ScanSafe 云网络安全配置指南》：

http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

监控云网络安全

命令	用途
show scansafe server	显示服务器状态，无论是当前的活动服务器、备用服务器，还是无法访问的服务器。
show scansafe statistics	显示全部和当前 HTTP(S) 连接。
show conn scansafe	显示所有云网络安全连接，如大写字母 Z 标记所示。
show service policy inspect scansafe	显示被特定策略重定向或列入白名单的连接的数量。
请参见以下 URL： http://Whoami.scansafe.net	从客户端访问此网站，确定流量是否流向到云网络安全服务器。

show scansafe server 命令显示云网络安全代理服务器是否可以访问。

```
hostname# show scansafe server
hostname# Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
hostname# Backup: proxy137.scansafe.net (80.254.152.99)
```

show scansafe statistics 命令显示有关云网络安全活动的信息，例如重定向到代理服务器的连接的数量，当前正在被重定向的连接的数量，以及被列入白名单的连接的数量：

```
hostname# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 0
Total HTTPS Sessions : 0
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 0 Bytes
Total Bytes Out : 0 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 0/0/0
HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

show service policy inspect scansafe 命令显示被特定策略重定向或列入白名单的连接的数量：

```
hostname(config)# show service-policy inspect scansafe
Global policy:
Service-policy: global_policy
    Class-map: inspection_default
Interface inside:
Service-policy: scansafe-pmap
    Class-map: scansafe-cmap
      Inspect: scansafe p-scansafe fail-open, packet 0, drop 0, reset-drop 0,
v6-fail-close 0
Number of whitelisted connections: 0
Number of connections allowed without scansafe inspection because of "fail-open" config: 0
Number of connections dropped because of "fail-close" config: 0
Number of HTTP connections inspected: 0
Number of HTTPS connections inspected: 0
Number of HTTP connections dropped because of errors: 0
Number of HTTPS connections dropped because of errors: 0
```

思科云网络安全配置示例

- 第 15-16 页上的单一模式示例
- 第 15-17 页上的多模式示例
- 第 15-17 页上的白名单示例
- 第 15-18 页上的目录集成示例
- 第 15-20 页上的带身份防火墙的云网络安全示例

单一模式示例

以下示例显示了思科云网络安全的完整配置：

配置 ACL

我们建议您创建单独的 HTTP 和 HTTPS 类映射来拆分流量，以便知道有多少个 HTTP 和 HTTPS 数据包已通过。

然后，如果您需要进行故障排除，您可以运行调试命令，判断有多少个数据包已穿越每个类映射，确定您正在推送更多 HTTP 流量还是 HTTPS 流量：

```
hostname(config)# access-list web extended permit tcp any any eq www
hostname(config)# access-list https extended permit tcp any any eq https
```

配置类映射

```
hostname(config)# class-map cmap-http
hostname(config-cmap)# match access-list web

hostname(config)# class-map cmap-https
hostname(config-cmap)# match access-list https
```

配置检测策略映射

```
hostname(config)# policy-map type inspect scansafe http-pmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# default group httptraffic
hostname(config-pmap-p)# http

hostname(config)# policy-map type inspect scansafe https-pmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# default group httpstraffic
hostname(config-pmap-p)# https
```

配置策略映射

```
hostname(config)# policy-map pmap-webtraffic
hostname(config-pmap)# class cmap-http
hostname(config-pmap-c)# inspect scansafe http-pmap fail-close

hostname(config-pmap)# class cmap-https
hostname(config-pmap-c)# inspect scansafe https-pmap fail-close
```

配置服务策略

```
hostname(config)# service-policy pmap-webtraffic interface inside
```

在 ASA 上配置云网络安全

```
hostname(config)# scansafe general-options
hostname(cfg-scansafe)# server primary ip 192.168.115.225 web 8080
hostname(cfg-scansafe)# retry-count 5
hostname(cfg-scansafe)# license 366C1D3F5CE67D33D3E9ACEC265261E5
```

多模式示例

以下示例在采用默认许可的情景 1 和采用身份验证密钥覆盖的情景 2 中启用了云网络安全：

```
!System Context
!
hostname(config)#scansafe general-options
hostname(cfg-scansafe)#server primary ip 180.24.0.62 port 8080
hostname(cfg-scansafe)#retry-count 5
hostname(cfg-scansafe)#license FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
hostname(cfg-scansafe)#publickey <path to public key>
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC265261E5
!
config-url disk0:/two_ctx.cfg
!
```

白名单示例

配置哪些访问列表流量应当被发送到云网络安全：

```
access-list 101 extended permit tcp any4 any4 eq www
access-list 102 extended permit tcp any4 any4 eq https

class-map web
 match access-list 101
class-map https
 match access-list 102
```

要配置白名单，确保用户 1 在此访问列表范围内，以绕过云网络安全：

```
class-map type inspect scansafe match-any whiteListCmap
 match user LOCAL\user1
```

要将类映射附加到云网络安全策略映射中，执行以下命令：

```
policy-map type inspect scansafe ss
 parameters
  default user user1 group group1
  http
 class whiteListCmap
  whitelist
```

```
policy-map type inspect scansafe ss2
 parameters
  default user user1 group group1
  https
 class whiteListCmap
  whitelist
```

创建此检测策略后，将其附加在策略映射中，以分配给服务组：

```
policy-map pmap
 class web
  inspect scansafe ss fail-close
class https
  inspect scansafe ss2 fail-close
```

然后，将策略映射附加到服务策略中，使其全局生效或按 ASA 接口生效：

```
service-policy pmap interface inside
```

目录集成示例

本章节包含各种目录集成配置示例。

- 第 15-18 页上的使用 LDAP 配置 Active Directory 服务器
- 第 15-19 页上的使用 RADIUS 配置 Active Directory 代理
- 第 15-19 页上的在 AD 代理服务器上创建 ASA 作为客户端
- 第 15-19 页上的在 AD 代理和 DC 之间创建链接
- 第 15-19 页上的测试 AD 代理
- 第 15-19 页上的在 ASA 上配置身份选项
- 第 15-19 页上的配置用户身份选项并启用精细报告
- 第 15-20 页上的监控 Active Directory 组
- 第 15-20 页上的从 Active Directory 服务器下载整个活动用户数据库
- 第 15-20 页上的从 AD 代理下载数据库
- 第 15-20 页上的显示活动用户列表

使用 LDAP 配置 Active Directory 服务器

以下示例显示如何使用 LDAP 在 ASA 上配置 Active Directory 服务器：

```
hostname(config)# aaa-server AD protocol ldap
hostname(config-aaa-server-group)# aaa-server AD (inside) host 192.168.116.220
hostname(config-aaa-server-host)# ldap-base-dn DC=ASASCANLAB,DC=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# server-type microsoft
hostname(config-aaa-server-host)# server-port 389
hostname(config-aaa-server-host)# ldap-login-dn
cn=administrator,cn=Users,dc=asascanlab,dc=local
hostname(config-aaa-server-host)# ldap-login-password Password1
```

使用 RADIUS 配置 Active Directory 代理

以下示例显示如何使用 RADIUS 在 ASA 上配置 Active Directory 代理：

```
hostname(config)# aaa-server adagent protocol radius
hostname(config-aaa-server-group)# ad-agent-mode
hostname(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.116.220
hostname(config-aaa-server-host)# key cisco123
hostname(config-aaa-server-host)# user-identity ad-agent aaa-server adagent
```

在 AD 代理服务器上创建 ASA 作为客户端

以下示例显示如何在 Active Directory 代理服务器上创建 ASA 作为客户端：

```
c:\IBF\CLI\adacfg client create -name ASA5520DEVICE -ip 192.168.116.90 -secret cisco123
```

在 AD 代理和 DC 之间创建链接

以下示例显示如何在 Active Directory 代理和您想监控登录 / 注销事件的所有 DC 之间创建链接：

```
c:\IBF\CLI\adacfg.exe dc create -name DCSERVER1 -host W2K3DC -domain
W2K3DC.asascanlab.local -user administrator -password Password1
c:\IBF\CLI\adacfg.exe dc list
```

运行最后一个命令应当将状态显示为 “UP”。

为了让 AD_Agent 监控登录 / 注销事件，您需要确保在目前正在被监控的所有 DC 上记录这些事件。为此，请选择：

Start > Administrative Tools > Domain Controller Security Policy

Local policies > Audit Policy > Audit account logon events (success and failure)

测试 AD 代理

以下示例显示如何配置测试 Active Directory 代理，以便它能够与 ASA 通信：

```
hostname# test aaa-server ad-agent adagent
Server IP Address or name: 192.168.116.220
INFO: Attempting Ad-agent test to IP address <192.168.116.220> (timeout: 12 seconds)
INFO: Ad-agent Successful
```

另请参见以下命令：**show user-identity ad-agent**。

在 ASA 上配置身份选项

以下示例显示如何在 ASA 上配置身份选项：

```
hostname(config)# user-identity domain ASASCANLAB aaa-server AD
hostname(config)# user-identity default-domain ASASCANLAB
```

配置用户身份选项并启用精细报告

以下示例显示如何配置用户身份选项，将用户凭证发送到 ASA，并从代理服务器启用精细用户报告：

```
hostname(config)# user-identity inactive-user-timer minutes 60
hostname(config)# user-identity action netbios-response-fail remove-user-ip
hostname(config)# user-identity user-not-found enable
```

```
hostname(config)# user-identity action mac-address-mismatch remove-user-ip
hostname(config)# user-identity ad-agent active-user-database full-download
```

如果您正在使用多个域，请输入以下命令：

```
hostname(config)# user-identity domain OTHERDOMAINNAME
```

监控 Active Directory 组

以下示例显示如何配置要受监控的 Active Directory 组：

```
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME1
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME2
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME3
```

注意事项　切记，完成上述操作后，请立即保存配置。

从 Active Directory 服务器下载整个活动用户数据库

以下命令无需等待 poll-import-user-group-timer 过期即可立即查询 Active Directory 服务器，以更新指定的导入用户组数据库：

```
hostname(config)# user-identity update import-user
```

从 AD 代理下载数据库

以下示例显示如何手动开始从 Active Directory 代理下载数据库 （如果您认为用户数据库与 Active Directory 不同步的话）：

```
hostname(config)# user-identity update active-user-database
```

显示活动用户列表

以下示例显示如何显示活动用户：

```
hostname# show user-identity user active list detail
```

有两种带身份防火墙的下载模式：完全下载和按需下载。

- 完全下载 - 无论用户何时登录网络， IDFW 都会立即将用户身份告知 ASA （建议在 ASA 5512-X 及更高版本上进行）。
- 按需下载 - 无论用户何时登录网络， ASA 都会从 AD (ADHOC) 请求用户身份。

带身份防火墙的云网络安全示例

以下示例显示了如何在 ASA 上配置带身份防火墙的云网络安全：

```
hostname# sh run
ASA Version 100.8(24)32
!
hostname QFW-201-QASS
domain-name uk.scansafe.net
enable password liqhNWIOSfzvir2g encrypted
passwd liqhNWIOSfzvir2g encrypted
names
!
```

```
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.116.90 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 192.168.114.90 255.255.254.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa100824-32-k8.bin
ftp mode passive
dns server-group DefaultDNS
 domain-name uk.scansafe.net
object network obj0192.168.116.x
 subnet 192.168.116.0 255.255.255.0
access-list 101 extended permit tcp any any eq www
access-list 101 extended permit tcp any any eq https
access-list web extended permit tcp any any eq www
access-list icmp extended permit icmp any any
access-list https extended permit tcp any any eq https
!
scansafe general-options
 server primary ip 192.168.115.225 web 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC26789534f
!
pager lines 24
logging buffered debugging
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
!
object network obj0192.168.116.x
 nat (inside,outside) dynamic interface
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.114.19 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
```

```
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AD protocol ldap
aaa-server AD (inside) host 192.168.116.220
 server-port 389
 ldap-base-dn DC=ASASCANLAB,DC=local
 ldap-scope subtree
 ldap-login-password *****
 ldap-login-dn cn=administrator,cn=Users,dc=asascanlab,dc=local
 server-type microsoft
aaa-server adagent protocol radius
 ad-agent-mode
aaa-server adagent (inside) host 192.168.116.220
 key *****
user-identity domain ASASCANLAB aaa-server AD
user-identity default-domain ASASCANLAB
user-identity action netbios-response-fail remove-user-ip
user-identity poll-import-user-group-timer hours 1
user-identity ad-agent aaa-server adagent
user-identity user-not-found enable
user-identity monitor user-group ASASCANLAB\\GROUP1
user-identity monitor user-group ASASCANLAB\\GROUPNAME
no snmp-server location
no snmp-server contact
crypto ca trustpool policy
telnet timeout 5
ssh 192.168.0.0 255.255.255.0 inside
ssh 192.168.21.0 255.255.255.0 inside
ssh timeout 30
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map cmap-https
 match access-list https
class-map inspection_default
 match default-inspection-traffic
class-map cmap-http
 match access-list web
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map type inspect scansafe ss
 parameters
  default user john group qa
  http
policy-map type inspect scansafe https-pmap
 parameters
  https
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
```

```
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
policy-map type inspect scansafe http-pmap
 parameters
  default group http-scansafe
  http
policy-map pmap-http
 class cmap-http
  inspect scansafe http-pmap fail-open
 class cmap-https
  inspect scansafe https-pmap fail-open
!
service-policy pmap-http global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:667ba936945b370c394806a63548e7a0
: end
QFW-201-QASS#
```

相关文档

相关文档	URL
思科 ScanSafe 云网络安全配置指南	http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

功能历史思科云网络安全

表 15-1 列出了各项功能变更以及实施了该变更的平台版本。

表 15-1　功能历史云网络安全

功能名称	平台版本	功能信息
云网络安全	9.0(1)	引入了此功能。 思科云网络安全为网络流量提供内容扫描和其他恶意软件防护服务。还能够根据用户身份重定向网络流量和提交相关报告。 我们引入了以下命令：**class-map type inspect scansafe**、**default user group**、 **http**[**s**] (parameters)、 **inspect scansafe**、 **license**, **match user group**、 **policy-map type inspect scansafe**、 **retry-count**、 **scansafe**、 **scansafe general-options**、 **server** {**primary** | **backup**}、 **show conn scansafe**、 **show scansafe server**、 **show scansafe statistics**、 **user-identity monitor**、 **whitelist**。

威胁检测

本章介绍如何配置威胁检测统计信息和扫描威胁检测。

- 第 16-1 页上的检测威胁
- 第 16-3 页上的威胁检测准则
- 第 16-3 页上的威胁检测的默认设置
- 第 16-4 页上的配置威胁检测
- 第 16-7 页上的监控威胁检测
- 第 16-12 页上的威胁检测示例
- 第 16-12 页上的威胁检测历史

检测威胁

ASA 上的威胁检测可以针对威胁提供第一道防御。威胁检测在第 3 层和第 4 层上工作，为设备上的流量制定基准，基于流量模式分析丢包统计信息，并累计“前面的”报告。相比之下，提供 IPS 或下一代 IPS 服务的模块可以在 ASA 允许的流量上识别和减少高达第 7 层的攻击媒介，并且无法看到已被 ASA 丢弃的流量。因此，威胁检测和 IPS 能够协同工作，以提供更加全面的威胁防御。

威胁检测由以下要素组成：

- 为各种威胁收集的不同级别统计信息。

  威胁检测统计信息可以帮助您管理 ASA 遭遇的威胁；例如，如果启用扫描威胁检测，则查看统计信息有助于分析威胁。您可以配置两种类型的威胁检测统计信息：

  - 基础威胁检测统计信息 - 包括有关针对整个系统的攻击活动的信息。默认情况下启用基础威胁检测统计信息，并且不会对性能产生影响。
  - 高级威胁检测统计信息 - 跟踪对象级活动，因此，ASA 能够报告针对单个主机、端口、协议或 ACL 的活动。高级威胁检测统计信息会对性能产生重要影响，具体情况视收集的统计信息而定，因此，在默认情况下，仅启用 ACL 统计信息。
- 扫描威胁检测，其确定主机何时执行扫描。或者，您可以避开任何被确定为扫描威胁的主机。

基础威胁检测统计信息

使用基础威胁检测统计信息，ASA 监控由以下原因造成的丢包和安全事件比率：

- 被 ACL 拒绝。
- 数据包格式不对（例如，invalid-ip-header 或 invalid-tcp-hdr-length）。
- 超出连接限制（系统范围的资源限制和在配置中设定的限制）。
- 检测到 DoS 攻击（例如，无效 SPI、状态防火墙检查故障）。
- 基础防火墙检查失败。此选项是一个组合比率，包含此列表中所有与防火墙有关的丢包。它不包含与防火墙无关的丢包，例如接口过载、应用检测失败的数据包以及检测到的扫描攻击。
- 检测到可疑的 ICMP 数据包。
- 数据包未通过应用检测。
- 接口过载。
- 检测到扫描攻击。此选项监控扫描攻击；例如，第一个 TCP 数据包不是 SYN 数据包，或者 TCP 连接在三次握手时失败。例如，完整扫描威胁检测采用此扫描攻击比率信息，通过将主机分类为攻击者并自动避开它们，从而对此信息发挥作用。
- 检测到不完整会话，例如，检测到 TCP SYN 攻击或未检测到数据 UDP 会话攻击。

当 ASA 检测威胁时，它会立即发送系统日志消息 (733100)。ASA 跟踪两种类型的比率：间隔期间的平均事件比率和较短爆发间隔期间的突发事件比率。突发率间隔为三十分之一平均率间隔或 10 秒，以较大者为准。对于收到的每个事件，ASA 检查平均和突发率限制；如果超出了两个比率，ASA 会发送两条独立的系统消息，每突发时期每比率类型最多一条消息。

基础威胁检测仅在有丢包或潜在威胁时影响性能；甚至在这种情况下，性能影响也微乎其微。

高级威胁检测统计信息

高级威胁检测统计信息显示单个对象（例如，主机、端口、协议或 ACL）允许和丢弃的流量比率。

注意事项　启用高级统计信息会影响 ASA 性能，具体情况视启用的统计信息类型而定。threat-**detection statistics host** 命令会显著影响性能；如果有高流量负载，您可能会考虑临时启用此类型的统计信息。 **threat-detection statistics port** 命令然而，会产生轻微影响。

扫描威胁检测

典型的扫描攻击包括测试子网中每个 IP 地址的可访问性的主机（通过扫描子网中的多台主机，或者扫描主机或子网中的多个端口）。扫描威胁检测功能可以确定主机何时执行扫描。与基于流量签名的 IPS 扫描检测不同，ASA 威胁检测扫描可以维护一个庞大的数据库，其中包含可面向扫描活动进行分析的主机统计信息。

主机数据库跟踪可疑活动，例如无返回活动的连接、已关闭访问端口的访问、易受攻击的 TCP 行为（例如，非随机 IPID）和更多行为。

如果超出扫描威胁比率，则 ASA 发送系统日志消息 (733101)，并且或者避开攻击者。ASA 跟踪两种类型的比率：间隔期间的平均事件比率和较短爆发间隔期间的突发事件比率。突发事件比率为三十分之一平均率间隔或 10 秒，以较大者为准。对于每个已检测到的被视为扫描攻击的一部分的事件，ASA 检查平均和突发率限制。如果从主机发送的流量超出了其中任意一个比率，则该主机被视为攻击者。如果主机接收的流量超出了其中任意一个比率，则该主机被视为攻击目标。

下表列出了扫描威胁检测的默认比率限制。

表 16-1　扫描威胁检测的默认比率限制

平均率	突发率
在最后 600 秒内，每秒丢弃 5 次。	在最后 20 秒内，每秒丢弃 10 次。
在最后 3600 秒内，每秒丢弃 5 次。	在最后 120 秒内，每秒丢弃 10 次。

注意事项　扫描威胁检测功能可以显著影响 ASA 性能和内存，同时创建和收集基于主机和子网的数据结构和信息。

威胁检测准则

安全情景准则

除了高级威胁统计信息，仅支持单一模式的威胁检测。在多模式下，仅支持 TCP 拦截统计信息。

防火墙模式准则

在路由和透明防火墙模式下受支持。

监控的流量类型

- 仅监控通过设备的流量；流向设备的流量不包含在威胁检测中。
- ACL 拒绝的流量不触发扫描威胁检测；仅允许通过 ASA 并且创建流的流量才会受扫描威胁检测的影响。

威胁检测的默认设置

默认情况下，启用基础威胁检测统计信息。

下表列出了默认的设置。您可以使用 中的 **show running-config all threat-detection** 命令查看所有这些默认设置。

对于高级统计信息，默认情况下，启用 ACL 统计信息。

表 16-2　基础威胁检测默认设置

	触发设置	
丢包原因	平均率	突发率
• 检测到 DoS 攻击 • 数据包格式不对 • 超出连接限制 • 检测到可疑的 ICMP 数据包	在最后 600 秒内，每秒丢弃 100 次。	在最后 20 秒内，每秒丢弃 400 次。
	在最后 3600 秒内，每秒丢弃 80 次。	在最后 120 秒内，每秒丢弃 320 次。

表 16-2　基础威胁检测默认设置（续）

丢包原因	触发设置	
	平均率	突发率
检测到扫描攻击	在最后 600 秒内，每秒丢弃 5 次。	在最后 20 秒内，每秒丢弃 10 次。
	在最后 3600 秒内，每秒丢弃 4 次。	在最后 120 秒内，每秒丢弃 8 次。
检测到不完整会话，例如，检测到 TCP SYN 攻击或未检测到数据 UDP 会话攻击（组合）	在最后 600 秒内，每秒丢弃 100 次。	在最后 20 秒内，每秒丢弃 200 次。
	在最后 3600 秒内，每秒丢弃 80 次。	在最后 120 秒内，每秒丢弃 160 次。
被 ACL 拒绝	在最后 600 秒内，每秒丢弃 400 次。	在最后 20 秒内，每秒丢弃 800 次。
	在最后 3600 秒内，每秒丢弃 320 次。	在最后 120 秒内，每秒丢弃 640 次。
• 基础防火墙检查失败 • 数据包未通过应用检测	在最后 600 秒内，每秒丢弃 400 次。	在最后 20 秒内，每秒丢弃 1600 次。
	在最后 3600 秒内，每秒丢弃 320 次。	在最后 120 秒内，每秒丢弃 1280 次。
接口过载	在最后 600 秒内，每秒丢弃 2000 次。	在最后 20 秒内，每秒丢弃 8000 次。
	在最后 3600 秒内，每秒丢弃 1600 次。	在最后 120 秒内，每秒丢弃 6400 次。

配置威胁检测

默认情况下，启用基础威胁检测统计信息，而且您可能只需要威胁检测服务。如果要实施其他威胁检测服务，请使用以下操作步骤。

操作步骤

步骤 1　第 16-5 页上的配置基础威胁检测统计信息。

基础威胁检测统计信息包括可能与攻击（例如，DoS 攻击）有关的活动。

步骤 2　第 16-5 页上的配置高级威胁检测统计信息。

步骤 3　第 16-7 页上的配置扫描威胁检测。

配置基础威胁检测统计信息

默认情况下，启用基础威胁检测统计信息。您可以禁用此功能，或者，如果已禁用，可以再次启用。

操作步骤

步骤 1　启用基础威胁检测统计信息（如果以前已禁用）。

threat-detection basic-threat

示例：

```
hostname(config)# threat-detection basic-threat
```

默认情况下，启用基础威胁检测。使用 **no threat-detection basic-threat** 禁用此功能。

步骤 2　（可选）更改一种或多种事件类型的默认设置。

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

示例：

```
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

有关每种事件类型的描述，请参阅第 16-2 页上的基础威胁检测统计信息。

当您将此命令与 **scanning-threat** 关键字配合使用时，还可以在扫描威胁检测中使用此命令。如果不配置基础威胁检测，依然可以将此命令与 **scanning-threat** 关键字配合使用，以配置扫描威胁检测的比率限制。

可以为每种事件类型配置最多三个不同的比率间隔。

配置高级威胁检测统计信息

您可以将 ASA 配置为收集大量的统计信息。默认情况下，启用 ACL 统计信息。要启用其他统计信息，请执行以下步骤。

操作步骤

步骤 1　（可选）启用*全部*统计信息。

threat-detection statistics

示例：

```
hostname(config)# threat-detection statistics
```

要仅启用某些统计信息，请为每种统计信息类型（该表中所示）输入此命令，不要输入无任何选项的命令。您可以输入 **threat-detection statistics**（无任何选项），然后通过输入带统计信息特定选项（例如，**threat-detection statistics host number-of-rate 2**）的命令，来自定义某些统计信息。如果输入 **threat-detection statistics**（无任何选项），然后为特定统计信息输入命令，但无任何统计信息特定选项，则此命令无任何影响，因为已启用该命令。

如果输入**无**形式的此命令，它将移除所有**威胁检测统计信息**命令，包括在默认情况下启用的 **threat-detection statistics access-list** 命令。

步骤 2　（可选）启用 ACL 统计信息（如果以前被禁用）。

```
threat-detection statistics access-list
```

示例：

```
hostname(config)# threat-detection statistics access-list
```

默认情况下，启用 ACL 统计信息。ACL 统计信息只能使用 **show threat-detection top access-list** 命令禁用。默认情况下，启用此命令。

步骤 3　（可选）为主机（**host** 关键字）、TCP 和 UDP 端口（**port** 关键字）或者非 TCP/UDP IP 协议（**protocol** 关键字）配置统计信息。

```
threat-detection statistics {host | port | protocol} [number-of-rate {1 | 2 | 3}]
```

示例：

```
hostname(config)# threat-detection statistics host number-of-rate 2

hostname(config)# threat-detection statistics port number-of-rate 2

hostname(config)# threat-detection statistics protocol number-of-rate 3
```

number-of-rate 关键字设置为统计信息维护的比率间隔数量。默认的比率间隔数量为 **1**，使内存使用率保持较低水平。要查看更多比率间隔，请将该值设为 **2** 或 **3**。例如，如果将该值设为 **3**，则可以查看过去 1 小时、8 小时和 24 小时的数据。如果将此关键字设为 **1**（默认值），则仅维护最短比率间隔统计信息。如果将该值设为 **2**，则维护两个最短间隔。

只要主机处于活动状态并且位于扫描威胁主机数据库内，主机统计信息就会累计。非活动时间超过 10 分钟后，将从数据库中删除主机（并且统计信息被清除）。

步骤 4　（可选）为 TCP 拦截而拦截的攻击配置统计信息（请参阅第 12 章，“连接设置”，来启用 TCP 拦截）。

```
threat-detection statistics tcp-intercept [rate-interval minutes]
[burst-rate attacks_per_sec] [average-rate attacks_per_sec]
```

示例：

```
hostname(config)# threat-detection statistics tcp-intercept rate-interval 60 burst-rate
800 average-rate 600
```

rate-interval 关键字设置历史监控窗口的大小，该值位于 1 和 1440 分钟之间。默认值为 30 分钟。在此间隔内，ASA 抽取攻击数量样本 30 次。

burst-rate 关键字为系统日志消息生成设置阈值，该值在 25 和 2147483647 之间。默认值为每秒 400。超出突发率时，生成系统日志消息 733104。

average-rate 关键字为系统日志消息生成设置平均率阈值，该值在 25 和 2147483647 之间。默认值为每秒 200。超出平均率时，生成系统日志消息 733105。

注　此命令在多情景模式下可用，不同于其他威胁检测命令。

配置扫描威胁检测

您可以配置扫描威胁检测，以识别攻击者，并或者避开它们。

操作步骤

步骤 1　启用扫描威胁检测。

threat-detection scanning-threat [**shun** [**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*}]]

示例：

```
hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
```

默认情况下，当主机被识别为攻击者时，生成系统日志消息 733101。多次输入此命令，以将多个 IP 地址或网络对象组识别为免于避开。

步骤 2　（可选）为攻击主机设置避开持续时间。

threat-detection scanning-threat shun duration *seconds*

示例：

```
hostname(config)# threat-detection scanning-threat shun duration 2000
```

步骤 3　（可选）当 ASA 将主机识别为攻击者或攻击目标时，更改默认事件限制：

threat-detection rate scanning-threat rate-interval *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

示例：

```
hostname(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10
burst-rate 20

hostname(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10
burst-rate 20
```

如果在基础威胁检测配置过程中已配置了此命令，则那些设置将与扫描威胁检测功能共享；不能为基础和扫描威胁检测配置独立比率。如果不使用此命令设置比率，则将默认值用于扫描威胁检测功能和基础威胁检测功能。通过输入独立命令，可以配置最多三个不同的比率间隔。

监控威胁检测

以下主题解释如何监控威胁检测和查看流量统计信息。

- 第 16-8 页上的监控基础威胁检测统计信息
- 第 16-8 页上的监控高级威胁检测统计信息
- 第 16-10 页上的评估主机威胁检测统计信息
- 第 16-11 页上的监控被避开的主机、攻击者和攻击目标

监控基础威胁检测统计信息

要显示基础威胁检测统计信息，请使用以下命令：

show threat-detection rate [**min-display-rate** *min_display_rate*]
[**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** |
icmp-drop | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

min-display-rate *min_display_rate* 参数将显示内容限制为超出每秒最低事件显示比率的统计信息。您可以将 *min_display_rate* 设置为介于 0 和 2147483647 之间。

其他参数可以让您将显示内容限制为特定类别。有关每种事件类型的描述，请参阅第 16-2 页上的基础威胁检测统计信息。

输出显示两个固定时间段中的平均率（单位：事件 / 秒）：最后 10 分钟和最后 1 小时。它还显示：最后完成的突发间隔（三十分之一平均率间隔或 10 秒，以较大者为准）内当前突发率（单位：事件 / 秒）；超出（被触发）比率的次数；以及时间段中的事件总数。

ASA 在每个突发时段结束时，为共计 30 个已完成突发间隔存储计数。目前正在发生的未完成突发间隔不包含在平均率中。例如，如果平均率间隔为 20 分钟，则突发间隔为 20 秒。如果最后突发间隔从 3:00:00 到 3:00:20，并且在 3:00:25 使用 **show** 命令，则最后 5 秒则不包含在输出中。

此规则的唯一例外是，当计算事件总数时，如果未完成突发间隔中的事件数量已超出最早突发间隔（三十分之一）中的事件数量。在这种情况下，ASA 把事件总数计算为最后 29 个完成间隔加上到目前为止未完成突发间隔中的事件数量。此例外使您可以实时监控大幅度事件增加情况。

您可以使用 **clear threat-detection rate** 命令清除统计信息。

以下是 **show threat-detection rate** 命令的样本输出：

```
hostname# show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0               0       0                   16
  1-hour ACL  drop:                0               0       0                  112
  1-hour SYN attck:                5               0       2                21438
  10-min  Scanning:                0               0      29                  193
  1-hour  Scanning:              106               0      10               384776
  1-hour Bad  pkts:               76               0       2               274690
  10-min  Firewall:                0               0       3                   22
  1-hour  Firewall:               76               0       2               274844
  10-min DoS attck:                0               0       0                    6
  1-hour DoS attck:                0               0       0                   42
  10-min Interface:                0               0       0                  204
  1-hour Interface:               88               0       0               318225
```

监控高级威胁检测统计信息

要监控高级威胁检测统计信息，请使用下表中显示的命令。显示内容输出显示以下内容：

- 固定时间段内平均率（单位：事件 / 秒）。
- 最后完成突发间隔中的当前突发率（单位：事件 / 秒），其为三十分之一平均率间隔或 10 秒，以较大者为准
- 超出比率的次数（仅限于丢弃的流量统计信息）
- 固定时间段内的事件总数。

ASA 在每个突发时段结束时，为共计 30 个已完成突发间隔存储计数。目前正在发生的未完成突发间隔不包含在平均率中。例如，如果平均率间隔为 20 分钟，则突发间隔为 20 秒。如果最后突发间隔从 3:00:00 到 3:00:20，并且在 3:00:25 使用 **show** 命令，则最后 5 秒则不包含在输出中。

此规则的唯一例外是，当计算事件总数时，如果未完成突发间隔中的事件数量已超出最早突发间隔（三十分之一）中的事件数量。在这种情况下，ASA 把事件总数计算为最后 29 个完成间隔加上到目前为止未完成突发间隔中的事件数量。此例外使您可以实时监控大幅度事件增加情况。

命令	用途
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] **detail**]]	显示前 10 条统计信息。如果不输入任何选项，将显示所有类别的前 10 条统计信息。 **min-display-rate** *min_display_rate* 参数将显示内容限制为超出每秒最低事件显示比率的统计信息。您可以将 *min_display_rate* 设置为介于 0 和 2147483647 之间。 以下行将解释可选关键字。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top access-list** [**rate-1** | **rate-2** | **rate-3**]	要查看匹配数据包的前 10 个 ACE（包括允许和拒绝 ACE），请使用 **access-list** 关键字。在此显示中，不区分被允许和被拒绝的流量。如果使用 **threat-detection basic-threat** 命令启用基础威胁检测，则可以使用 **show threat-detection rate acl-drop** 命令跟踪 ACL 拒绝。 **rate-1** 关键字显示在显示内容中可用的最小固定比率间隔的统计信息；**rate-2** 显示第二大比率间隔；如果定义了三个间隔，**rate-3 显示**最大比率间隔。例如，显示内容显示最后 1 小时、8 小时和 24 小时的统计信息。如果设置 **rate-1** 关键字，ASA 仅显示 1 小时时间间隔。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top host** [**rate-1** | **rate-2** | **rate-3**]	要仅查看主机统计信息，请使用 **host** 关键字。**请注意**：由于威胁检测算法，用作组合故障转移和状态链接的接口会在前 10 台主机中显示；这是预期行为，而且您可以在显示内容中忽略此 IP 地址。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top port-protocol** [**rate-1** | **rate-2** | **rate-3**]	要查看端口和协议统计信息，请使用 **port-protocol** 关键字。**port-protocol** 关键字显示端口和协议统计信息（必须为显示内容启用两者），并且显示 TCP/UDP 端口和 IP 协议类型的组合统计信息。TCP（协议 6）和 UDP（协议 17）不包含在 IP 协议显示内容中；然而，TCP 和 UDP 端口包含在端口显示内容中。如果仅启用这些类型中一个类型（端口或协议）的统计信息，则只能查看启用的统计信息。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top tcp-intercept** [**all**] **detail**]]	要查看 TCP 拦截统计信息，请使用 **tcp-intercept** 关键字。显示内容包含受到攻击的前 10 台受保护服务器。**all** 关键字显示所有被跟踪服务器的历史数据。**detail** 关键字显示历史取样数据。在比率间隔内，ASA 抽取攻击数量样本 30 次，因此，在默认的 30 分钟内，每 60 秒收集一次统计信息。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]	显示所有主机或特定主机或子网的统计信息。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[**-***end_port*]]	显示所有端口或特定端口或端口范围的统计信息。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | **ah** | **eigrp** | **esp** | **gre** | **icmp** | **icmp6** | **igmp** | **igrp** | **ip** | **ipinip** | **ipsec** | **nos** | **ospf** | **pcp** | **pim** | **pptp** | **snp** | **tcp** | **udp**]	显示所有 IP 协议或特定协议的统计信息。 *protocol_number* 参数是介于 0 和 255 之间的整数。

评估主机威胁检测统计信息

以下是 **show threat-detection statistics host** 命令的样本输出：

```
hostname# show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:              2938               0       0             10580308
  8-hour Sent byte:               367               0       0             10580308
 24-hour Sent byte:               122               0       0             10580308
  1-hour Sent pkts:                28               0       0               104043
  8-hour Sent pkts:                 3               0       0               104043
 24-hour Sent pkts:                 1               0       0               104043
  20-min Sent drop:                 9               0       1                10851
  1-hour Sent drop:                 3               0       1                10851
  1-hour Recv byte:              2697               0       0              9712670
  8-hour Recv byte:               337               0       0              9712670
 24-hour Recv byte:               112               0       0              9712670
  1-hour Recv pkts:                29               0       0               104846
  8-hour Recv pkts:                 3               0       0               104846
 24-hour Recv pkts:                 1               0       0               104846
  20-min Recv drop:                42               0       3                50567
  1-hour Recv drop:                14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                 0               0       0                  614
  8-hour Sent byte:                 0               0       0                  614
 24-hour Sent byte:                 0               0       0                  614
  1-hour Sent pkts:                 0               0       0                    6
  8-hour Sent pkts:                 0               0       0                    6
 24-hour Sent pkts:                 0               0       0                    6
  20-min Sent drop:                 0               0       0                    4
  1-hour Sent drop:                 0               0       0                    4
  1-hour Recv byte:                 0               0       0                  706
  8-hour Recv byte:                 0               0       0                  706
 24-hour Recv byte:                 0               0       0                  706
  1-hour Recv pkts:                 0               0       0                    7
```

下表对输出进行了解释。

表 16-3　show threat-detection statistics host

字段	说明
Host	主机 IP 地址。
tot-ses	自主机添加到数据库后的该主机会话总数。
act-ses	主机当前参与的活动会话总数。
fw-drop	防火墙丢包数量。防火墙丢包是一个组合比率，其中包括在基础威胁检测中跟踪的与防火墙有关的所有丢包，包括 ACL 拒绝的数据包、坏数据包、超出连接限制的数据包、DoS 攻击数据包、可疑 ICMP 数据包、TCP SYN 攻击数据包以及无数据 UDP 攻击数据包。它不包含与防火墙无关的丢包，例如接口过载、应用检测失败的数据包以及检测到的扫描攻击。
insp-drop	因为数据包未通过应用检测而被丢弃的数据包的数量。
null-ses	空会话数量，空会话是指在 3 秒超时内未完成的 TCP SYN 会话，以及在会话开始后 3 秒内没有其服务器发送的任何数据的 UDP 会话。

表 16-3　show threat-detection statistics host（续）

字段	说明
bad-acc	对处于关闭状态的主机端口的不良访问尝试次数。当确定端口处于空会话中（请参阅 null-ses 字段说明）时，主机的端口状态被设为 HOST_PORT_CLOSE。访问此主机端口的任何客户端都会被立即分类为不良访问，而无需等待超时。
Average(eps)	每个时间段内的平均率（单位：事件 / 秒）。 ASA 在每个突发时段结束时，为共计 30 个已完成突发间隔存储计数。目前正在发生的未完成突发间隔不包含在平均率中。例如，如果平均率间隔为 20 分钟，则突发间隔为 20 秒。如果最后突发间隔从 3:00:00 到 3:00:20，并且在 3:00:25 使用 **show** 命令，则最后 5 秒则不包含在输出中。 此规则的唯一例外是，当计算事件总数时，如果未完成突发间隔中的事件数量已超出最早突发间隔（三十分之一）中的事件数量。在这种情况下，ASA 把事件总数计算为最后 29 个完成间隔加上到目前为止未完成突发间隔中的事件数量。此例外使您可以实时监控大幅度事件增加情况。
Current(eps)	最后完成突发间隔中的当前突发率（单位：事件 / 秒），其为三十分之一平均率间隔或 10 秒，以较大者为准。对于 Average(eps) 说明中指定的示例，当前比率为从 3:19:30 到 3:20:00 的比率。
Trigger	超出丢包比率限制的次数。对于按已发送和已接收字节和数据包行识别的有效流量，该值始终为 0，因为有效流量没有触发比率限制。
Total events	每个比率间隔内的事件总数。目前正在发生的未完成突发间隔未包含在事件总数中。此规则的唯一例外是，当计算事件总数时，如果未完成突发间隔中的事件数量已超出最早突发间隔（三十分之一）中的事件数量。在这种情况下，ASA 把事件总数计算为最后 29 个完成间隔加上到目前为止未完成突发间隔中的事件数量。此例外使您可以实时监控大幅度事件增加情况。
20 分钟、1 小时、8 小时和 24 小时	这些固定比率间隔的统计信息。对于每个间隔： • Sent byte - 从主机成功发送的字节数。 • Sent pkts - 从主机成功发送的数据包数。 • Sent drop - 已从主机发送但因为是扫描攻击的一部分而被丢弃的数据包数。 • Recv byte - 主机成功接收的字节数。 • Recv pkts - 主机成功接收的数据包数。 • Recv drop - 主机已接收但因为是扫描攻击的一部分而被丢弃的数据包数。

监控被避开的主机、攻击者和攻击目标

要监控和管理被避开的主机以及攻击者和攻击目标，请使用以下命令：

- **show threat-detection shun**

  显示当前避开的主机。例如：

```
hostname# show threat-detection shun
Shunned Host List:
10.1.1.6
192.168.6.7
```

- **clear threat-detection shun** [*ip_address* [*mask*]]

  使主机免于被避开。如果不指定 IP 地址，所有主机都将从避开列表清除。

  例如，要释放位于 10.1.1.6 的主机，请输入以下命令：

  ```
  hostname# clear threat-detection shun 10.1.1.6
  ```

- **show threat-detection scanning-threat** [**attacker** | **target**]

  显示 ASA 确定为攻击者的主机（包括避开列表上的主机），并且显示成为攻击目标的主机。如果不输入选项，将显示攻击者和攻击目标主机。例如：

  ```
  hostname# show threat-detection scanning-threat attacker
  10.1.2.3
  10.8.3.6
  209.165.200.225
  ```

威胁检测示例

以下示例配置基础威胁检测统计信息，并且更改 DoS 攻击比率设置。启用所有高级威胁检测统计信息，比率间隔的主机统计信息数量低至 2。还自定义 TCP 拦截比率间隔。启用扫描威胁检测，自动避开除了 10.1.1.0/24 以外的所有地址。自定义扫描威胁比率间隔。

```
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100
threat-detection statistics
threat-detection statistics host number-of-rate 2
threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate 600
threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20
```

威胁检测历史

功能名称	平台版本	说明
基础和高级威胁检测统计信息、扫描威胁检测	8.0(2)	引入了基础和高级威胁检测统计信息、扫描威胁检测。 引入了以下命令：**threat-detection basic-threat**、**threat-detection rate**、**show threat-detection rate**、**clear threat-detection rate**、 **threat-detection statistics**、**show threat-detection statistics**、**threat-detection scanning-threat**、**threat-detection rate scanning-threat**、**show threat-detection scanning-threat**、**show threat-detection shun**、**clear threat-detection shun**。
避开持续时间	8.0(4)/8.1(2)	您现在可以设置避开持续时间。 引入了以下命令：**threat-detection scanning-threat shun duration**。

功能名称	平台版本	说明
TCP 拦截统计信息	8.0(4)/8.1(2)	引入了 TCP 拦截统计信息。 引入或修改了以下命令：**threat-detection statistics tcp-intercept**、**show threat-detection statistics top tcp-intercept**、**clear threat-detection statistics**。
自定义主机统计信息比率间隔	8.1(2)	现在，您可以自定义收集统计信息的比率间隔数。默认比率数已从 3 更改为 1。 修改了以下命令：**threat-detection statistics host number-of-rates**。
突发率间隔已更改为三十分之一平均率。	8.2(1)	在早期版本中，突发率间隔为六十分之一平均率。为最大限度利用内存，取样间隔已在平均率中减少到 30 次。
自定义端口和协议统计信息比率间隔	8.3(1)	现在，您可以自定义收集统计信息的比率间隔数。默认比率数已从 3 更改为 1。 修改了以下命令：**threat-detection statistics port number-of-rates**、**threat-detection statistics protocol number-of-rates**。
提高内存使用率	8.3(1)	提高了威胁检测的内存使用率。 引入了以下命令：**show threat-detection memory**。

第 6 部分

ASA 模块

ASA FirePOWER (SFR) 模块

本章介绍如何配置在 ASA 上运行的 ASA FirePOWER 模块。

- 第 17-1 页上的 ASA FirePOWER 模块
- 第 17-5 页上的 ASA FirePOWER 模块的许可要求
- 第 17-5 页上的 ASA FirePOWER 的准则
- 第 17-5 页上的 ASA FirePOWER 的默认设置
- 第 17-6 页上的配置 ASA FirePOWER 模块
- 第 17-17 页上的管理 ASA FirePOWER 模块
- 第 17-21 页上的监控 ASA FirePOWER 模块
- 第 17-24 页上的 ASA FirePOWER 模块的示例
- 第 17-25 页上的 ASA FirePOWER 模块的历史记录

ASA FirePOWER 模块

ASA FirePOWER 模块提供下一代防火墙服务，包括下一代 IPS (NGIPS)、应用可视性与控制 (AVC)、URL 过滤以及高级恶意软件防护 (AMP)。该模块既可在单情景模式或多情景模式下使用，也可在路由模式或透明模式下使用。

该模块也称为 ASA SFR。

虽然该模块提供用于初始配置和故障排除的基本命令行界面 (CLI)，但可使用独立的应用 FireSIGHT 管理中心配置设备上的安全策略，该应用可托管在独立的 FireSIGHT 管理中心设备上，也可作为在 VMware 服务器上运行的虚拟设备进行托管。（FireSIGHT 管理中心也称为防御中心。）

- 第 17-2 页上的 ASA FirePOWER 模块如何与 ASA 配合使用
- 第 17-3 页上的 ASA FirePOWER 管理访问权限
- 第 17-4 页上的与 ASA 功能的兼容性

ASA FirePOWER 模块如何与 ASA 配合使用

ASA FirePOWER 模块从 ASA 运行独立的应用。本模块可以是一个硬件模块（适用于 ASA 5585-X），也可以是一个软件模块（适用于 5512-X 至 5555-X）。作为硬件模块，设备包括独立的管理和控制台端口，以及由 ASA 直接使用（而非由模块本身使用）的额外数据接口。

可在被动（“仅监控”）或内联部署中配置设备。

- 在被动部署中，流量的副本发送至设备，但不返回至 ASA。在被动模式，可在不影响网络的情况下查看设备本来会对流量执行的操作，并对流量的内容进行评估。
- 在内联部署中，实际流量发送至设备，并且设备的策略会影响将对流量执行的操作。在丢弃不需要的流量并执行由策略应用的任何其他操作后，流量返回至 ASA，以供进一步处理和最终传输。

以下各节对这些模式进行了更详细地说明。

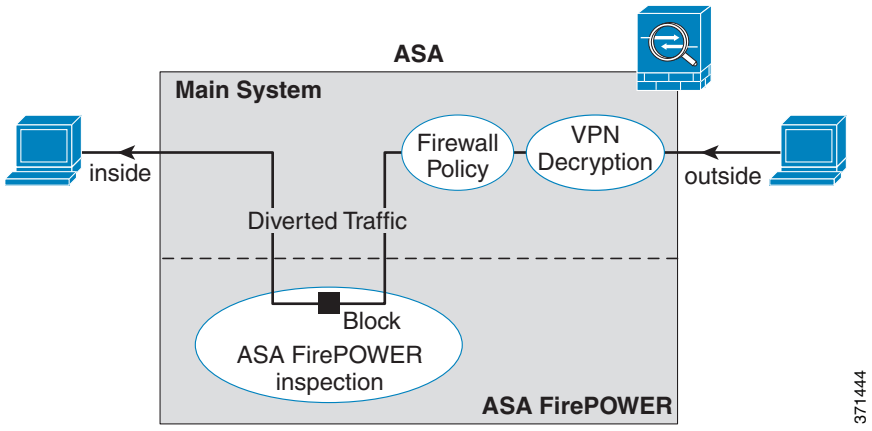
ASA FirePOWER 内联模式

在内联模式下，流量先接受防火墙检查，然后再转发至 ASA FirePOWER 模块。在确定了要在 ASA 上接受 ASA FirePOWER 检测的流量之后，这些流量将按以下方式流经 ASA 和模块：

1. 流量进入 ASA。
2. 对传入的 VPN 流量解密。
3. 应用防火墙策略。
4. 流量发送至 ASA FirePOWER 模块。
5. ASA FirePOWER 模块向流量应用其安全策略，并执行相应的操作。
6. 有效流量发回 ASA； ASA FirePOWER 模块可能根据其安全策略阻止某些流量，被阻止的流量将不传递下去。
7. 对传出的 VPN 流量加密。
8. 流量退出 ASA。

下图显示在内联模式下使用 ASA FirePOWER 模块时的流量流。在此示例中，模块阻止不允许某个应用使用的流量。所有其他流量均通过 ASA 转发。

图 17-1　ASA 中的 ASA FirePOWER 模块流量流



注　如果在两个 ASA 接口上有一个主机间的连接，且仅为其中一个接口配置了 ASA FirePOWER 服务策略，则这些主机间的所有流量均发送至 ASA FirePOWER 模块，包括来自非 ASA FirePOWER 接口的流量（因为该功能是双向的）。

ASA FirePOWER 被动（仅监控）模式

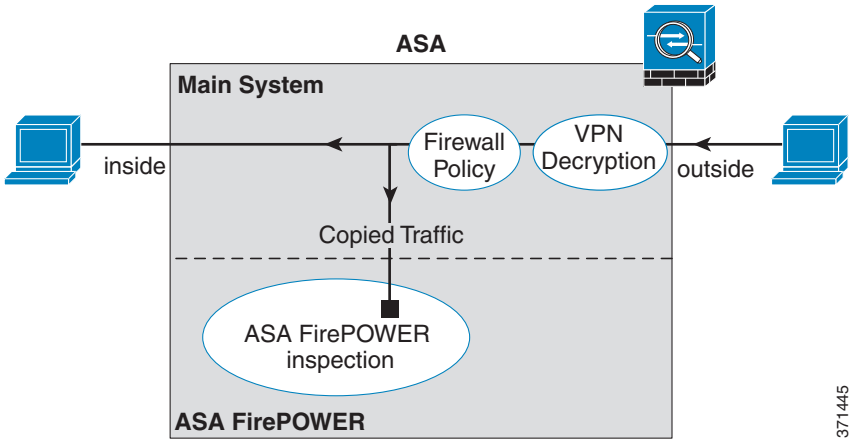
仅监控模式下的流量流与内联模式下的流量流一样。唯一的差异在于 ASA FirePOWER 模块不将流量传回 ASA。相反，模块向流量应用安全策略，并告知您其在内联模式下运行时将会完成的操作，例如，流量可能会在事件中被标记为“可能已丢弃”。您可使用此信息进行流量分析并帮助您决定是否需要内联模式。

要配置被动模式，请在将流量重定向至模块的服务策略中包括仅监控指示。

注　无法在 ASA 上同时配置仅监控模式和正常内联模式。仅允许使用一种安全策略类型。在多情景模式下，无法为某些情景配置仅监控模式，并同时为其他情景配置常规内联模式。

下图显示在被动模式下运行时的流量流。

图 17-2　ASA FirePOWER 被动，仅监控模式



ASA FirePOWER 管理访问权限

有两个用于管理 ASA FirePOWER 模块的独立访问层：初始配置（以及后续故障排除）和策略管理。

- 第 17-4 页上的初始配置
- 第 17-4 页上的策略配置和管理

初始配置

为了执行初始配置，必须使用 ASA FirePOWER 模块上的 CLI。有关默认管理地址的信息，请参阅第 17-5 页上的 ASA FirePOWER 的默认设置。

要访问 CLI，您可以使用以下方法：

- ASA 5585-X：
  - ASA FirePOWER 控制台端口 - 模块上的控制台端口是一个独立的外部控制台端口。
  - ASA FirePOWER 管理 1/0 接口（使用 SSH）- 可连接至默认 IP 地址或使用 ASDM 更改管理 IP 地址，然后使用 SSH 进行连接。模块上的管理接口是一个独立的外部千兆以太网接口。

注　无法使用 **session** 命令访问 ASA 背板上的 ASA FirePOWER 硬件模块 CLI。

- ASA 5512-X 至 ASA 5555-X：
  - 背板上的 ASA 的会话 - 如对 ASA 有 CLI 访问权，则可向模块发起会话并访问模块 CLI。
  - ASA FirePOWER 管理 0/0 接口（使用 SSH）- 可连接至默认 IP 地址或使用 ASDM 更改管理 IP 地址，然后使用 SSH 进行连接。这些模式将 ASA FirePOWER 模块作为软件模块运行。ASA FirePOWER 管理接口与 ASA 共用管理 0/0 接口。ASA 和 ASA FirePOWER 模块分别支持不同的 MAC 地址和 IP 地址。ASA FirePOWER IP 地址的配置必须在 ASA FirePOWER 操作系统内进行（使用 CLI 或 ASDM）。但是，物理特性（例如启用接口）在 ASA 上配置。可移除 ASA 接口配置（特别是接口名称），以便将此接口专门用作纯 ASA FirePOWER 接口。此接口仅用于管理。

策略配置和管理

在执行初始配置后，请使用 FireSIGHT 管理中心配置 ASA FirePOWER 安全策略。然后，使用 ASDM 或思科安全管理器配置用于将流量发送至 ASA FirePOWER 模块的 ASA 策略。

与 ASA 功能的兼容性

ASA 提供许多高级应用检测功能，包括 HTTP 检测。但是，ASA FirePOWER 模块提供的 HTTP 检测比 ASA 提供的更高级 检测，该模块还提供适用于其他应用的附加功能，包括监控和控制应用使用情况。

要充分利用 ASA FirePOWER 模块功能，请参阅以下适用于发送至 ASA FirePOWER 模块的流量的准则：

- 请勿对 HTTP 流量配置 ASA 检测。
- 请勿配置云网络安全 (ScanSafe) 检测。如果为同一流量配置 ASA FirePOWER 检测和云网络安全检测，则 ASA 仅执行 ASA FirePOWER 检测。
- ASA 上的其他应用检测与 ASA FirePOWER 模块兼容，包括默认检测。
- 请勿启用移动用户安全 (MUS) 服务器；它不与 ASA FirePOWER 模块兼容。
- 如果启用故障转移，则当 ASA 进行故障转移时，任何现有 ASA FirePOWER 流均传输至新 ASA。新 ASA 中的 ASA FirePOWER 模块自此开始向前检测流量；将不传输旧检测状态。

ASA FirePOWER 模块的许可要求

ASA FirePOWER 模块和 FireSIGHT 管理中心需要附加许可证，这些许可证需要安装在模块中，而不是安装在 ASA 情景中。ASA 本身不需要附加许可证。

请参阅《*FireSIGHT 系统用户指南*》的“许可”章节或 FireSIGHT 管理中心中的在线帮助，了解详细信息。

ASA FirePOWER 的准则

故障转移准则

不支持直接故障转移；当 ASA 进行故障转移时，任何现有 ASA FirePOWER 流均传输至新的 ASA。新 ASA 中的 ASA FirePOWER 模块自此开始向前检测流量；将不传输旧检测状态。

您负责在高可用性 ASA 对中的 ASA FirePOWER 模块上维护一致的策略（使用 FireSIGHT 管理中心），以确保一致的故障转移行为。

ASA 集群准则

不支持直接集群，但可在集群中使用这些模块。您负责使用 FireSIGHT 管理中心在集群中的 ASA FirePOWER 模块上维护一致的策略。请勿对集群中的设备使用不同的基于 ASA 接口的区域定义。

型号准则

- 在 ASA 5585-X（作为硬件模块）和 5512-X 至 ASA 5555-X（作为软件模块）上受到支持。有关详细信息，请参阅《*思科 ASA 兼容性矩阵*》：

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- 对于 5512-X 至 ASA 5555-X，必须安装思科固态硬盘 (SSD)。有关详细信息，请参阅《ASA 5500-X 硬件指南》。

附加准则和限制

- 请参阅第 17-4 页上的与 ASA 功能的兼容性。
- 无法更改安装在硬件模块上的软件类型；如果购买 ASA FirePOWER 模块，则以后无法在该模块上安装其他软件。
- 无法在 ASA 上同时配置仅监控模式和正常内联模式。仅允许使用一种安全策略类型。在多情景模式下，无法为某些情景配置仅监控模式，并同时为其他情景配置常规内联模式。

ASA FirePOWER 的默认设置

下表列出 ASA FirePOWER 模块的默认设置。

表 17-1　ASA FirePOWER 默认网络参数

参数	默认
管理 IP 地址	• 系统软件映像：192.168.45.45/24 • 启动映像： – ASA 5585-X：管理 1/0 192.168.8.8/24 – ASA 5512-X 至 ASA 5555-X：管理 0/0 192.168.1.2/24

表 17-1　ASA FirePOWER 默认网络参数（续）

参数	默认
网关	• 系统软件映像：无 • 启动映像： – ASA 5585-X：192.168.8.1/24 – ASA 5512-X 至 ASA 5555-X：192.168.1.1/24
SSH 或会话用户名	admin
密码	• 系统软件映像：**Sourcefire** • 启动映像：**Admin123**

配置 ASA FirePOWER 模块

配置 ASA FirePOWER 模块这个过程包括：先在 ASA FirePOWER 模块上配置 ASA FirePOWER 安全策略，然后配置 ASA 以发送流量至 ASA FirePOWER 模块。要配置 ASA FirePOWER 模块，请执行以下步骤：

步骤 1　第 17-6 页上的连接 ASA FirePOWER 管理接口。为 ASA FirePOWER 管理接口和或者控制台接口布线。

步骤 2　第 17-9 页上的（ASA 5512-X 至 5555-X）安装或重新映像软件模块。

步骤 3　如有必要，请参阅第 17-12 页上的更改 ASA FirePOWER 管理 IP 地址。初次 SSH 访问可能要求此操作。

步骤 4　第 17-13 页上的在 ASA FirePOWER CLI 处配置基本 ASA FirePOWER 设置。您在 ASA FirePOWER 模块中执行此操作。

步骤 5　第 17-14 页上的向 FireSIGHT 管理中心添加 ASA FirePOWER。这将确定将管理设备的 FireSIGHT 管理中心。

步骤 6　第 17-15 页上的在 ASA FirePOWER 模块上配置安全策略。

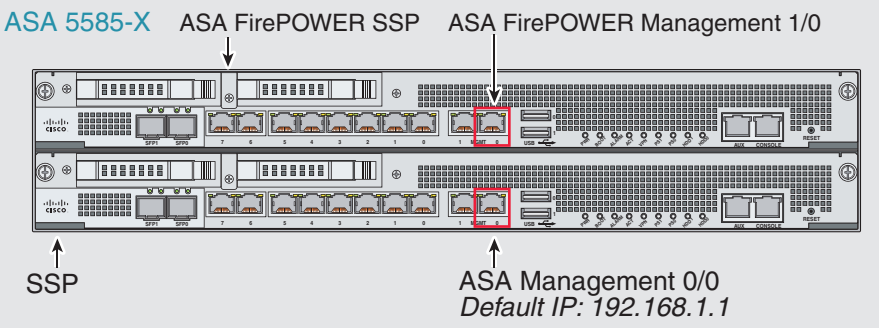
步骤 7　第 17-15 页上的向 ASA FirePOWER 模块重定向流量。

连接 ASA FirePOWER 管理接口

除了提供对 ASA FirePOWER 模块的管理访问权限外，ASA FirePOWER 管理接口还需要访问 HTTP 代理服务器或 DNS 服务器和互联网，以便进行签名更新等操作。本节描述推荐的网络配置。您的网络可能不同。

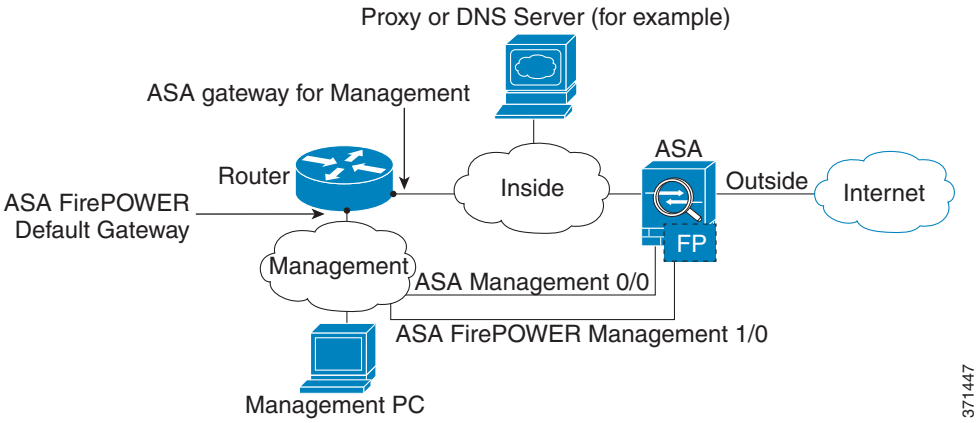
ASA 5585-X（硬件模块）

ASA FirePOWER 模块包括一个独立于 ASA 的管理接口和控制台接口。为了执行初始设置，可通过 SSH 使用默认 IP 地址连接至 ASA FirePOWER 管理 1/0 接口。如果无法使用默认 IP 地址，则可使用控制台端口，或使用 ASDM 来更改管理 IP 地址，以便使用 SSH。（请参阅第 17-12 页上的更改 ASA FirePOWER 管理 IP 地址。）



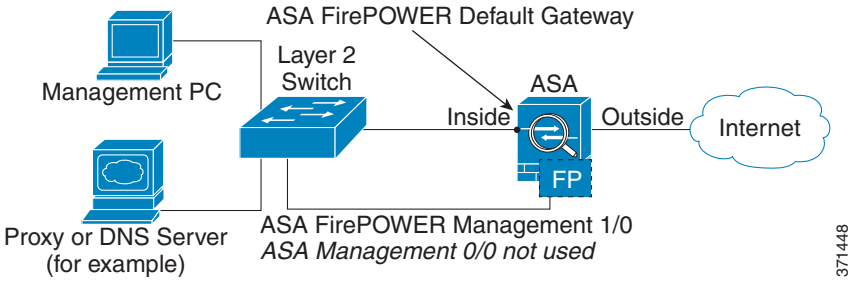
如果有内部路由器

如果有内部路由器，则可在管理网络（可能同时包括 ASA 管理 0/0 接口和 ASA FirePOWER 管理 1/0 接口）与 ASA 内部网络之间路由，以访问互联网。另外，务必在 ASA 上添加一个路由，以便通过内部路由器访问管理网络。



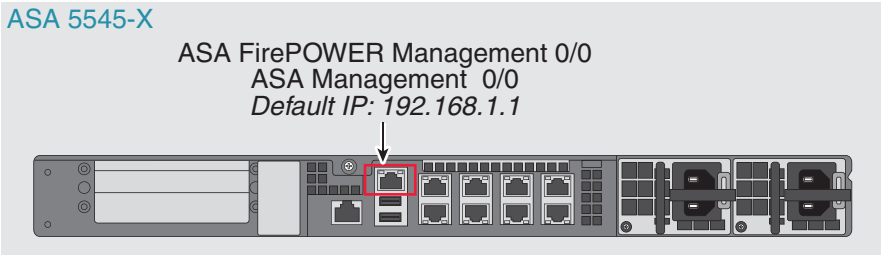
如果没有内部路由器

如果只有一个内部网络，您就无法拥有一个单独管理网络，这需要内部路由器实现网络之间的路由。在这种情况下，可从内部接口而非管理 0/0 接口管理 ASA。由于 ASA FirePOWER 模块是独立于 ASA 的设备，因此，可将 ASA FirePOWER 管理 1/0 地址配置为位于内部接口所在的网络上。



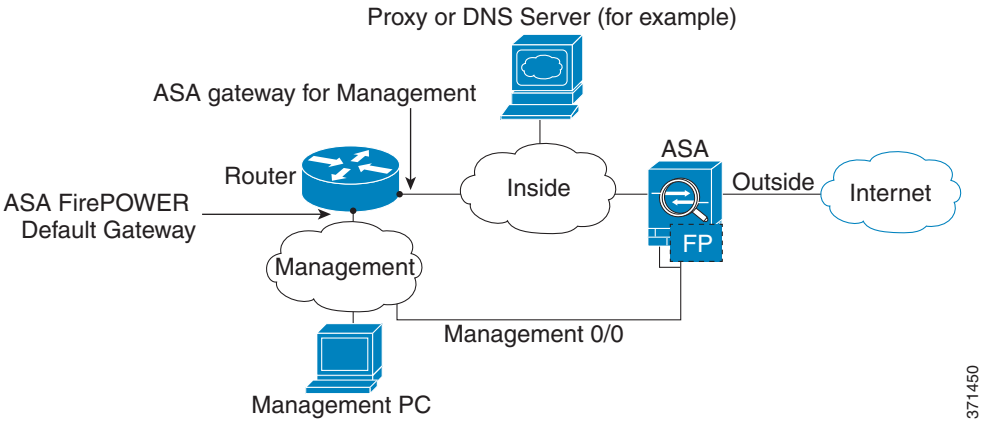
ASA 5512-X 至 ASA 5555-X（软件模块）

这些型号将 ASA FirePOWER 模块作为软件模块运行，并且 ASA FirePOWER 管理接口与 ASA 共用管理 0/0 接口。为了执行初始设置，可使用 SSH 连接至 ASA FirePOWER 默认 IP 地址。如果无法使用默认 IP 地址，则可向背板上的 ASA FirePOWER 发起会话，或使用 ASDM 来更改管理 IP 地址，以便使用 SSH。



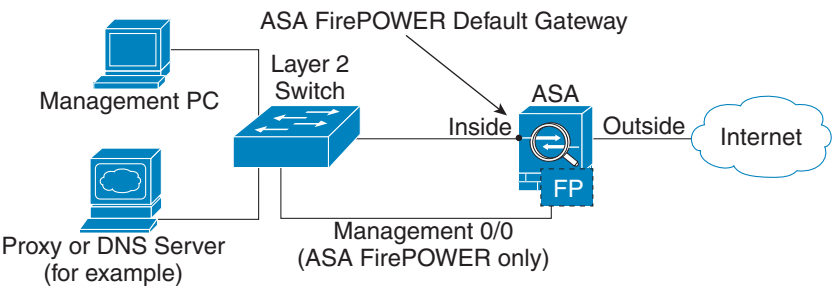
如果有内部路由器

如果有内部路由器，则可在管理 0/0 网络（同时包括 ASA 和 ASA FirePOWER 管理 IP 地址）和内部网络之间路由，以便访问互联网。另外，务必在 ASA 上添加一个路由，以便通过内部路由器访问管理网络。



如果没有内部路由器

如果只有一个内部网络，您就无法拥有一个单独的管理网络。在这种情况下，可从内部接口而非管理 0/0 接口管理 ASA。即使从管理 0/0 接口移除 ASA 配置的名称，也仍可配置该接口的 ASA FirePOWER IP 地址。由于 ASA FirePOWER 模块本质上是独立于 ASA 的设备，因此，*可*将 ASA FirePOWER 管理地址配置为位于内部接口所在的网络上。



注　必须为管理 0/0 接口移除 ASA 配置的名称；如果该名称是在 ASA 上配置的，则 ASA FirePOWER 地址必须位于 ASA 所在的网络上，这其中不包括已在其他 ASA 接口上配置的任何网络。如未配置名称，则 ASA FirePOWER 地址可位于任何网络上，例如，ASA 内部网络。

（ASA 5512-X 至 5555-X）安装或重新映像软件模块

如果购买具有 ASA FirePOWER 模块的 ASA，则模块软件和所需的固态硬盘 (SSD) 已预装好且可供配置。如果想要将 ASA FirePOWER 软件模块添加至现有 ASA，或需要更换 SSD，则需要安装 ASA FirePOWER 启动软件，对 SSD 进行分区，并根据此操作步骤安装系统软件。

重新映像模块的操作步骤相同，但应首先卸载 ASA FirePOWER 模块。如果更换 SSD，需要重新映像系统。

有关如何实际安装 SSD 的信息，请参阅《ASA 硬件指南》。

准备工作

- 除去启动软件所占空间外，闪存 (disk0) 上的可用空间至少应为 3GB。
- 在多情景模式下，请在系统执行空间中执行此操作步骤。
- 必须先关闭可能正在运行的任何其他软件模块；设备一次可运行一个软件模块。必须从 ASA CLI 执行此操作。例如，以下命令关闭并卸载 IPS 软件模块，然后重新加载 ASA；用于移除 CX 模块的命令是一样的，除非使用 **cxsc** 关键字代替 **ips**。

```
hostname# sw-module module ips shutdown
hostname# sw-module module ips uninstall
hostname# reload
```

注　如有活动服务策略将流量重定向至 IPS 或 CX 模块，则必须移除该策略。例如，如果策略为全局策略，则将使用 **no service-policy** *ips_policy* **global**。可以使用 CLI 或 ASDM 移除策略。

- 如果重新映像模块，请使用相同关闭和卸载命令来移除旧映像。例如，**sw-module module sfr uninstall**。
- 从 Cisco.com 获取 ASA FirePOWER 启动映像和系统软件包。

操作步骤

步骤 1　下载启动映像至设备。请勿传输系统软件；稍后会将其下载至 SSD。您有以下选项：

- ASDM - 首先，下载启动映像至工作站，或将其放在 FTP、TFTP、HTTP、HTTPS、SMB 或 SCP 服务器上。然后，在 ASDM 中，选择 **Tools > File Management**，然后选择适当的 **File Transfer** 命令，**Between Local PC and Flash** 或 **Between Remote Server and Flash**。传输启动软件至 ASA 上的 disk0。
- ASA CLI - 首先，将启动映像放在 TFTP、FTP、HTTP 或 HTTPS 服务器上，然后使用 **copy** 命令将其下载至闪存。以下示例使用 TFTP；请使用服务器的 IP 地址或主机名替换 <TFTP Server>。

```
ciscoasa# copy tftp://<TFTP SERVER>/asasfr-5500x-boot-5.3.1-58.img
disk0:/asasfr-5500x-boot-5.3.1-58.img
```

步骤 2　从 Cisco.com 将 ASA FirePOWER 系统软件下载至可从 ASA FirePOWER 管理接口访问的 HTTP、HTTPS 或 FTP 服务器。

步骤 3　通过输入以下命令在 ASA disk0 中设置 ASA FirePOWER 模块启动映像的位置：

```
hostname# sw-module module sfr recover configure image disk0:file_path
```

注　如果收到类似 “ERROR: Another service (cxsc) is running, only one service is allowed to run at any time,” 的消息，则表明已配置了另一个软件模块。必须将其关闭并移除，以安装以上 “ 先决条件 ” 一节所述的新模块。

示例：

```
hostname# sw-module module sfr recover configure image
disk0:asasfr-5500x-boot-5.3.1-58.img
```

步骤 4　通过输入以下命令加载 ASA FirePOWER 启动映像：

```
hostname# sw-module module sfr recover boot
```

步骤 5　等待约 5-15 分钟，以便 ASA FirePOWER 模块启动，然后向现在正在运行的 ASA FirePOWER 启动映像发起控制台会话。可能需要在打开会话后按 Enter 键以进入登录提示符。默认用户名是 **admin**，默认密码是 **Admin123**。

```
hostname# session sfr console
Opening console session with module sfr.
Connected to module sfr.Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

提示　如果模块启动未完成，则 **session** 命令将失败，并显示有关无法通过 ttyS1 连接的消息。请稍后重试。

步骤 6　使用 **setup** 命令配置系统，以便安装系统软件包。

```
asasfr-boot> setup


                Welcome to SFR Setup
                 [hit Ctrl-C to abort]
               Default values are inside []
```

系统将提示输入以下信息。请注意，管理地址和网关，以及 DNS 信息是要配置的关键设置。

- 主机名 - 最多可达 65 个字母数字字符，不能包含空格。允许使用连字符。
- 网络地址 - 可设置静态 IPv4 或 IPv6 地址，或使用 DHCP（适用于 IPv4）或 IPv6 无状态自动配置。
- DNS 信息 - 必须至少确定一个 DNS 服务器，还可设置域名和搜索域。
- NTP 信息 - 可启用 NTP 并配置 NTP 服务器，以便设置系统时间。

步骤 7　使用 **system install** 命令安装系统软件映像：

system install [**noconfirm**] *url*

如果不想回复确认消息，请在命令中添加 **noconfirm** 选项。使用 HTTP、HTTPS 或 FTP URL ；如果需要用户名和密码，系统将提示您提供这些信息。

安装完成后，系统将重新启动。等待 10 分钟或更长时间，以便安装应用组件及启动 ASA FirePOWER 服务。（**show module sfr** 输出应将所有进程状态显示为 Up。）

例如：

```
asasfr-boot> system install http://asasfr-sys-5.3.1-44.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FirePOWER 5.3.1-44 System Install
        Requires reboot:                Yes

Do you want to continue with upgrade?[y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade.Press 'Enter' to reboot the system.
(press Enter)
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2014):

The system is going down for reboot NOW!
Console session with module sfr terminated.
```

步骤 8　向 ASA FirePOWER 模块发起会话。您看到的登录提示符将有所不同，因为您登录的是功能完备的模块。

```
asa3# session sfr
Opening command session with module sfr.
Connected to module sfr.Escape character sequence is 'CTRL-^X'.

Sourcefire ASA5555 v5.3.1 (build 44)
Sourcefire3D login:
```

步骤 9　使用用户名 **admin** 和密码 **Sourcefire** 登录。

步骤 10　根据提示完成系统配置。

必须先阅读并接受最终用户许可协议 (EULA)。然后根据提示依次更改管理员密码，配置管理地址和 DNS 设置。可同时配置 IPv4 和 IPv6 管理地址。例如：

```
System initialization in progress.Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <new password>
Confirm new password: <repeat password>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4?(y/n) [y]: y
Do you want to configure IPv6?(y/n) [n]:
Configure IPv4 via DHCP or manually?(dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.86.118.3
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
```

```
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(Wait for the system to reconfigure itself.)

This sensor must be managed by a Defense Center.A unique alphanumeric
registration key is always required.In most cases, to register a sensor
to a Defense Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.
```

步骤 11　使用 **configure manager add** 命令确定将管理此设备的 FireSIGHT 管理中心设备。

由您提供一个注册密钥，随后将设备添加至 FireSIGHT 管理中心目录时，您将在其中使用该注册密钥。以下示例显示了简单情况。如果存在 NAT 边界，则命令不同；请参阅第 17-14 页上的向 FireSIGHT 管理中心添加 ASA FirePOWER。

```
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

步骤 12　使用浏览器中的 HTTPS 连接登录 FireSIGHT 管理中心，使用以上输入的主机或地址。例如，https://DC.example.com。

使用 Device Management (**Devices > Device Management**) 页面添加设备。有关详细信息，请参阅在机帮助或《*FireSIGHT 系统用户指南*》中的“管理设备”章节。

提示　还可通过 FireSIGHT 管理中心配置 NTP 和时间设置。从 **System > Local > System Policy** 页面编辑本地策略时，使用 Time Synchronization 设置。

更改 ASA FirePOWER 管理 IP 地址

如果无法使用默认管理 IP 地址，则可从 ASA 设置管理 IP 地址。设置管理 IP 地址后，可使用 SSH 访问 ASA FirePOWER 模块，以执行附加设置。

如在初始系统设置期间通过 ASA FirePOWER CLI 已配置管理地址，如第 17-13 页上的在 ASA FirePOWER CLI 处配置基本 ASA FirePOWER 设置中所述，则不需要通过 ASA CLI 或 ASDM 对其进行配置。

注　对于软件模块，可通过从 ASA CLI 发起会话来访问 ASA FirePOWER CLI 以执行设置；然后，在设置过程中，可设置 ASA FirePOWER 管理 IP 地址。对于硬件模块，可通过控制台端口完成初始设置。

要通过 ASA 更改管理 IP 地址，请执行以下操作之一。在多情景模式下，请在系统执行空间中执行此操作步骤。

- 在 CLI 中，使用以下命令设置 ASA FirePOWER 管理 IP 地址、掩码和网关。对硬件模块使用 **1**，对软件模块使用 **sfr**。

  session {1 | sfr} do setup host ip *ip_address*/*mask*,*gateway_ip*

  例如，**session 1 do setup host ip 10.1.1.2/24,10.1.1.1**。
- 在 ASDM 中，选择 **Wizards > Startup Wizard**，并通过向导前进至 ASA FirePOWER Basic Configuration，在其中可设置 IP 地址、掩码和默认网关。

在 ASA FirePOWER CLI 处配置基本 ASA FirePOWER 设置

必须先在 ASA FirePOWER 模块上配置基本网络设置和其他参数，然后才能配置安全策略。此操作步骤假设已安装完整的系统软件（而不仅仅是启动映像），无论是在直接安装它之后，还是因为其已经安装在硬件模块上。

提示　此操作步骤还假设您在执行初始配置。在初始配置期间，系统将提示进行这些设置。如果稍后需要更改这些设置，请使用各种 **configure network** 命令来更改各项设置。有关 **configure network** 命令的详细信息，请使用 **?** 命令获取帮助，并参阅《*FireSIGHT 系统用户指南*》或 FireSIGHT 管理中心中的在线帮助。

操作步骤

步骤 1　执行以下操作之一：

- （所有型号）使用 SSH 连接至 ASA FirePOWER 管理 IP 地址。
- （ASA 5512-X 至 ASA 5555-X）从 ASA CLI 向模块发起会话（请参阅常规操作配置指南中的“入门指南”章节，以访问 ASA CLI）。在多情景模式下，从系统执行空间发起会话。

  ```
  hostname# session sfr
  ```

步骤 2　使用用户名 **admin** 和密码 **Sourcefire** 登录。

步骤 3　根据提示完成系统配置。

必须先阅读并接受最终用户许可协议 (EULA)。然后根据提示依次更改管理员密码，配置管理地址和 DNS 设置。可同时配置 IPv4 和 IPv6 管理地址。看到表示必须通过 FireSIGHT 管理中心管理传感器的消息时，系统已完成配置。

例如：

```
System initialization in progress.Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <new password>
Confirm new password: <repeat password>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4?(y/n) [y]: y
Do you want to configure IPv6?(y/n) [n]:
Configure IPv4 via DHCP or manually?(dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.86.118.3
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
```

```
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(Wait for the system to reconfigure itself.)

This sensor must be managed by a Defense Center.A unique alphanumeric
registration key is always required.In most cases, to register a sensor
to a Defense Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.
```

步骤 4　现在必须确定将管理此设备的 FireSIGHT 管理中心，如第 17-14 页上的向 FireSIGHT 管理中心添加 ASA FirePOWER 中所述。

向 FireSIGHT 管理中心添加 ASA FirePOWER

必须向 FireSIGHT 管理中心（此应用用于在模块上配置策略）注册 ASA FirePOWER 模块。FireSIGHT 管理中心也称为防御中心。

要注册设备，请使用 **configure manager add** 命令。向 FireSIGHT 管理中心注册设备始终需要一个唯一的字母数字注册密钥。这是由您指定的简单密钥，不同于许可密钥。

在大多数情况下，必须随注册密钥一起提供 FireSIGHT 管理中心的主机名或 IP 地址，例如：

```
configure manager add DC.example.com my_reg_key
```

然而，如果设备和 FireSIGHT 管理中心被 NAT 设备分隔，请随注册密钥一起输入一个唯一的 NAT ID，并指定 DONTRESOLVE 替代主机名，例如：

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

操作步骤

步骤 1　执行以下操作之一：

- （所有型号）使用 SSH 连接至 ASA FirePOWER 管理 IP 地址。
- （ASA 5512-X 至 ASA 5555-X）从 ASA CLI 向模块发起会话（请参阅常规操作配置指南中的“入门指南”章节，以访问 ASA CLI）。在多情景模式下，从系统执行空间发起会话。

  ```
  hostname# session sfr
  ```

步骤 2　使用用户名 **admin** 或拥有 CLI 配置（管理员）访问级别的的另一用户名登录。

步骤 3　系统提示符下，使用 **configure manager add** 命令向 FireSIGHT 管理中心注册设备，该命令使用以下语法：

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

其中：

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} 指定 FireSIGHT 管理中心的完全限定主机名或 IP 地址。如果 FireSIGHT 管理中心非直接可寻址，请使用 DONTRESOLVE。
- *reg_key* 是将设备注册到 FireSIGHT 管理中心所需的唯一字母数字注册密钥。
- *nat_id* 是在 FireSIGHT 管理中心与设备之间的注册期间使用的可选字母数字字符串。当主机名设置为 DONTRESOLVE 时需要它。

步骤 4　使用浏览器中的 HTTPS 连接登录 FireSIGHT 管理中心，使用以上输入的主机或地址。例如，https://DC.example.com。

使用 Device Management (**Devices > Device Management**) 页面添加设备。有关详细信息，请参阅在机帮助或《*FireSIGHT 系统用户指南*》中的“管理设备”章节。

在 ASA FirePOWER 模块上配置安全策略

使用 FireSIGHT 管理中心在 ASA FirePOWER 模块上配置安全策略。安全策略控制模块提供的服务，如下一代 IPS 过滤和应用过滤。无法通过 ASA FirePOWER CLI、ASA CLI 或 ASDM 配置策略。

要打开 FireSIGHT 管理中心，请使用网络浏览器打开以下 URL：

https://*DC_address*

其中 *DC_address* 是在第 17-14 页上的向 FireSIGHT 管理中心添加 ASA FirePOWER 中定义的管理器的 DNS 名称或 IP 地址。例如，https://dc.example.com。

有关如何配置安全策略的信息，请参阅《*FireSIGHT 系统用户指南*》或 FireSIGHT 管理中心中的在线帮助。

提示　也可从 ASDM 中的 ASA FirePOWER Status 控制面板打开 FireSIGHT 管理中心。选择 **Home > ASA FirePOWER Status**，并点击控制面板底部的链接。

向 ASA FirePOWER 模块重定向流量

可将流量重定向至 ASA FirePOWER 模块，只需创建可确定特定流量的服务策略。

可在被动（“仅监控”）或内联部署中配置设备。

- 在被动部署中，流量的副本发送至设备，但不返回至 ASA。在被动模式，可在不影响网络的情况下查看设备本来会对流量执行的操作，并对流量的内容进行评估。
- 在内联部署中，实际流量发送至设备，并且设备的策略会影响将对流量执行的操作。在丢弃不需要的流量并执行由策略应用的任何其他操作后，流量返回至 ASA，以供进一步处理和最终传输。

注　无法在 ASA 上同时配置仅监控模式和正常内联模式。仅允许使用一种安全策略类型。在多情景模式下，无法为某些情景配置仅监控模式，并同时为其他情景配置常规内联模式。

准备工作

- 如有活动服务策略将流量重定向至 IPS 或 CX 模块（替换为 ASA FirePOWER），则必须先移除该策略，然后再配置 ASA FirePOWER 服务策略。
- 务必在 ASA 和 ASA FirePOWER 上配置一致的策略（通过 FireSIGHT 管理中心）。所有策略均应反映流量的被动或内联模式。
- 在多情景模式下，请在每个安全情景中执行此操作步骤。

操作步骤

步骤 1　创建 L3/L4 类映射以确定要发送至模块的流量。

```
class-map name
match parameter
```

示例：

```
hostname(config)# class-map firepower_class_map
hostname(config-cmap)# match access-list firepower
```

如果要将多个流量类发送至模块，则可创建多个类映射以用于安全策略。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

```
policy-map name
```

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　确定在此操作步骤开始时创建的类映射。

```
class name
```

示例：

```
hostname(config-pmap)# class firepower_class_map
```

步骤 4　将流量发送至 ASA FirePOWER 模块。

```
sfr {fail-close | fail-open} [monitor-only]
```

其中：

- **fail-close** 关键字将 ASA 设置为在 ASA FirePOWER 模块不可用时阻止所有流量。
- **fail-open** 关键字将 ASA 设置为在模块不可用时允许所有流量未经检查即可通过。
- 指定 **monitor-only** 以将流量的只读副本发送至模块，即被动模式。如未纳入关键字，则流量在内联模式下发送。有关详细信息，请参阅第 17-3 页上的 ASA FirePOWER 被动（仅监控）模式。

示例：

```
hostname(config-pmap-c)# sfr fail-close
```

步骤 5　如果为 ASA FirePOWER 流量创建了多个类映射，则可为策略指定另一个类，并应用 **sfr** 重定向操作。

有关策略映射内类顺序的重要性的详细信息，请参阅第 1-5 页上的服务策略内的功能匹配。对于同一操作类型，流量无法匹配多个类映射。

步骤 6　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

管理 ASA FirePOWER 模块

本节包括用于管理模块的操作步骤。

- 第 17-17 页上的重置密码
- 第 17-18 页上的重新加载或重置模块
- 第 17-18 页上的关闭模块
- 第 17-18 页上的（适用于 ASA 5512-X 至 ASA 5555-X）卸载软件模块映像
- 第 17-19 页上的（ASA 5512-X 至 ASA 5555-X）从 ASA 向模块发起会话
- 第 17-19 页上的重新映像 5585-X ASA FirePOWER 硬件模块
- 第 17-21 页上的升级系统软件

重置密码

如果忘记管理员用户的密码，则拥有 CLI 配置权限的另一个用户可登录并更改该密码。

如果没有拥有所需权限的其他用户，则可使用 **session do** 命令从 ASA 重置管理员密码。

提示　ASA hw-module 和 sw-module 命令中的 password-reset 选项不与 ASA FirePOWER 配合使用。

要将用户 **admin** 的模块密码重置为默认值 **Sourcefire**，请使用以下命令。对硬件模块使用 **1**，对软件模块使用 **sfr**。在多情景模式下，请在系统执行空间中执行此操作步骤。

session {1 | sfr} do password-reset

例如，**session sfr do password-reset**。

重新加载或重置模块

要重新加载，或重置并重新加载模块，请在 ASA CLI 处输入以下命令之一。在多情景模式下，请在系统执行空间中执行此操作步骤。

- 硬件模块 (ASA 5585-X)：

  hw-module module 1 {**reload** | **reset**}

- 软件模块（ASA 5512-X 至 ASA 5555-X）：

  sw-module module sfr {**reload** | **reset**}

关闭模块

通过关闭模块软件，可让模块做好准备，在不丢失配置数据的情况下安全断电。要正确关闭模块，请在 ASA CLI 处输入以下命令之一。在多情景模式下，请在系统执行空间中执行此操作步骤。

注　如果重新加载 ASA，模块将不自动关闭，因此，我们建议先关闭模块，再重新加载 ASA。

- 硬件模块 (ASA 5585-X)：

  hw-module module 1 shutdown

- 软件模块（ASA 5512-X 至 ASA 5555-X）：

  sw-module module sfr shutdown

（适用于 ASA 5512-X 至 ASA 5555-X）卸载软件模块映像

可卸载软件模块映像及其关联配置。在多情景模式下，请在系统执行空间中执行此操作步骤。

操作步骤

步骤 1　卸载软件模块映像以及关联配置。

```
hostname# sw-module module sfr uninstall

Module sfr will be uninstalled.This will completely remove the disk image
associated with the sw-module including any configuration that existed within it.

Uninstall module sfr?[confirm]
```

步骤 2　重新加载 ASA。必须先重新加载 ASA，然后才能安装新模块。

```
hostname# reload
```

（ASA 5512-X 至 ASA 5555-X）从 ASA 向模块发起会话

使用 ASA FirePOWER CLI 配置基本网络设置并对模块进行故障排除。

要从 ASA 访问 ASA FirePOWER 软件模块 CLI，可从 ASA 发起会话。可向模块发起会话（使用 Telnet），也可创建虚拟控制台会话。如果控制面板已关闭且无法建立 Telnet 会话，则控制台会话可能有用。在多情景模式下，从系统执行空间发起会话。

在 Telnet 或控制台会话中，会提示您输入用户名和密码。可使用 ASA FirePOWER 上配置的任何用户名登录。最初，**admin** 用户名是已配置的唯一用户名（且始终可用）。完整映像的初始默认用户名为 **Sourcefire**，启动映像的初始默认用户名为 **Admin123**。

- Telnet 会话：

  ```
  session sfr
  ```

  在 ASA FirePOWER CLI 中时，要退出并返回 ASA CLI，请输入会将您从模块注销的任何命令，如 **logout** 或 **exit**，或按 **Ctrl-Shift-6, x**。

- 控制台会话：

  ```
  session sfr console
  ```

  退出控制台会话的唯一途径为同时按下 **Ctrl-Shift-6, x**。从模块注销后，您将回到模块登录提示符处。

注　请勿将 **session sfr console** 命令与终端服务器结合使用，其中 **Ctrl-Shift-6, x** 是用于返回到终端服务器提示符的转义序列。**Ctrl-Shift-6, x** 序列也用于对 ASA FirePOWER 控制台转义并返回至 ASA 提示符。因此，如果在这种情况下尝试退出 ASA FirePOWER 控制台，反而会一直退回到终端服务器提示符。如将终端服务器重新连接至 ASA，ASA FirePOWER 控制台会话仍将处于活动状态；您将永远无法退回至 ASA 提示符。必须使用直接串行连接才能将控制台返回至 ASA 提示符。出现此情况时，请使用 **session sfr** 命令，而不要使用控制台命令。

重新映像 5585-X ASA FirePOWER 硬件模块

如果出于任何原因需要重新映像 ASA 5585-X 设备中的 ASA FirePOWER 硬件模块，则需要依次安装启动映像和系统软件包。必须安装两个软件包，系统才能正常运行。在正常情况下，不需要重新映像系统即可安装升级软件包。

要安装启动映像，需要通过登录模块的控制台端口来从 ASA FirePOWER SSP 上的管理 0 端口对映像执行 TFTP 启动。因为管理 0 端口位于第一个插槽的一个 SSP 上，所以，也称为管理 1/0，但是，rommon 将其识别为管理 0 或管理 0/1。

要完成 TFTP 启动，必须执行以下操作：

- 将软件映像放在可通过 ASA FirePOWER 上的管理 1/0 接口访问的 TFTP 服务器上。
- 将管理 1/0 连接至网络。必须使用此接口对启动映像执行 TFTP 启动。
- 配置 rommon 变量。按 Esc 键中断自动启动进程，以便配置 rommon 变量。

安装启动映像后，请安装系统软件包。必须将软件包放在可从 ASA FirePOWER 访问的 HTTP、HTTPS 或 FTP 服务器上。

以下操作步骤说明如何依次安装启动映像和系统软件包。

操作步骤

步骤 1　连接至控制台端口。借助于设置为 9600 波特、8 数据位、无奇偶校验、1 停止位、无流控制的终端仿真器，使用 ASA 产品随附的控制台电缆将 PC 连接至控制台。请参阅 ASA 硬件指南，了解有关控制台电缆的详细信息。

步骤 2　输入 **system reboot** 命令以重新加载系统。

步骤 3　系统提示时，按 Esc 键中断启动。如果看到引导程序开始启动系统，则表明您已等得太久。

这将让您进入 rommon 提示符。

步骤 4　在 rommon 提示符处，输入 **set** 并配置以下参数：

- ADDRESS - 模块的管理 IP 地址。
- SERVER - TFTP 服务器的 IP 地址。
- GATEWAY - TFTP 服务器的网关地址 如果 TFTP 服务器直接连接至管理 1/0，请使用 TFTP 服务器的 IP 地址。如果 TFTP 服务器和管理地址位于同一子网，则请勿配置网关，否则 TFTP 启动将失败。
- IMAGE - TFTP 服务器上的启动映像路径和映像名称。例如，如在 TFTP 服务器上将文件放在 tftpboot/images/filename.img 中，则 IMAGE 值为 images/filename.img。

例如：

```
ADDRESS=10.5.190.199
SERVER=10.5.11.170
GATEWAY=10.5.1.1
IMAGE=asasfr-boot-5.3.1-26-54.img
```

步骤 5　输入 **sync** 以保存设置。

步骤 6　输入 **tftp** 以启动下载和启动进程。

您将看到表示进度的 ! 标记。几分钟后启动完成时，将看到登录提示符。

步骤 7　以 **admin** 身份登录并使用密码 **Admin123**。

步骤 8　使用 **setup** 命令配置系统，以便安装系统软件包。

系统将提示输入以下信息。请注意，管理地址和网关，以及 DNS 信息是要配置的关键设置。

- 主机名 - 最多可达 65 个字母数字字符，不能包含空格。允许使用连字符。
- 网络地址 - 可设置静态 IPv4 或 IPv6 地址，或使用 DHCP（适用于 IPv4）或 IPv6 无状态自动配置。
- DNS 信息 - 必须至少确定一个 DNS 服务器，还可设置域名和搜索域。
- NTP 信息 - 可启用 NTP 并配置 NTP 服务器，以便设置系统时间。

步骤 9　使用 **system install** 命令安装系统软件映像：

system install [**noconfirm**] *url*

如果不想回复确认消息，请在命令中添加 **noconfirm** 选项。

安装完成后，系统将重新启动。等待 10 分钟或更长时间，以便安装应用组件及启动 ASA FirePOWER 服务。

例如：

```
asasfr-boot> system install http://asasfr-sys-5.3.1-54.pkg
```

步骤 10　启动完成后，以 **admin** 身份登录，并使用密码 **Sourcefire**。

根据提示完成系统配置。

必须先阅读并接受最终用户许可协议 (EULA)。然后根据提示依次更改管理员密码，配置管理地址和 DNS 设置。可同时配置 IPv4 和 IPv6 管理地址。

步骤 11　使用 **configure manager add** 命令确定将管理此设备的 FireSIGHT 管理中心设备。

由您提供一个注册密钥，随后将设备添加至 FireSIGHT 管理中心目录时，您将在其中使用该注册密钥。以下示例显示了简单情况。如果存在 NAT 边界，则命令不同；请参阅第 17-14 页上的向 FireSIGHT 管理中心添加 ASA FirePOWER。

```
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

步骤 12　使用浏览器中的 HTTPS 连接登录 FireSIGHT 管理中心，使用以上输入的主机或地址。例如，https://DC.example.com。

使用 Device Management (**Devices > Device Management**) 页面添加设备。有关详细信息，请参阅《*FireSIGHT 系统用户指南*》中的“管理设备”章节或 FireSIGHT 管理中心中的在线帮助。

升级系统软件

使用 FireSIGHT 管理中心将升级映象应用于 ASA FirePOWER 模块。在应用升级之前，请确保 ASA 运行的是新版本所需的最低版本；可能需要先升级 ASA，然后才能升级模块。

有关应用升级的详细信息，请参阅《*FireSIGHT 系统用户指南*》或 FireSIGHT 管理中心中的在线帮助。

监控 ASA FirePOWER 模块

以下主题提供了有关监控模块的指南。有关与 ASA FirePOWER 相关的系统日志消息，请参阅系统日志消息指南。ASA FirePOWER 系统日志消息以消息编号 434001 开头。

- 第 17-21 页上的显示模块状态
- 第 17-23 页上的显示模块统计信息
- 第 17-23 页上的监控模块连接

显示模块状态

要检查模块状态，请输入以下命令之一：

- **show module [1 | sfr] [details]**

  将显示模块状态。包括 1（对于硬件模块）或 sfr（对于软件模块）关键字以查看特定于 ASA FirePOWER 模块的状态。包含关键字 details 以获取附加信息，包括管理模块的设备的地址。

- **show module sfr recover**

  将显示安装模块时所使用的启动映像的位置。

以下是对装有 ASA FirePOWER 硬件模块的 ASA 5585-X 执行 **show module** 命令后的输出示例：

```
hostname# show module
```

```
Mod  Card Type                                    Model              Serial No.
---- ------------------------------------------- ------------------ -----------
   0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAF1507AMKE
   1 ASA 5585-X FirePOWER Security Services Proce ASA5585-SSP-SFR10  JAF1510BLSA

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 5475.d05b.1100 to 5475.d05b.110b  1.0          2.0(7)0      100.10(0)8
   1 5475.d05b.2450 to 5475.d05b.245b  1.0          2.0(13)0     5.3.1-44

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
   1 FirePOWER                      Up               5.3.1-44

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
   1 Up                 Up
```

以下示例显示软件模块的详细信息。请注意，DC Addr 表示管理此设备的 FireSIGHT 管理中心 的地址。

```
hostname# show module sfr details
Getting details from the Service Module, please wait...

Card Type:          FirePOWER Services Software Module
Model:              ASA5555
Hardware version:   N/A
Serial Number:      FCH1714J6HP
Firmware version:   N/A
Software version:   5.3.1-100
MAC Address Range:  bc16.6520.1dcb to bc16.6520.1dcb
App.name:           ASA FirePOWER
App.Status:         Up
App.Status Desc:    Normal Operation
App.version:        5.3.1-100
Data Plane Status:  Up
Status:             Up
DC addr:            10.89.133.202
Mgmt IP addr:       10.86.118.7
Mgmt Network mask:  255.255.252.0
Mgmt Gateway:       10.86.116.1
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

以下示例显示安装模块时，与 **sw-module module sfr recover** 命令配合使用的 ASA FirePOWER 启动映像的位置。

```
hostname# show module sfr recover
Module sfr recover parameters...
Boot Recovery Image: No
Image File Path:     disk0:/asasfr-5500x-boot-5.3.1-44.img
```

显示模块统计信息

使用 show service-policy sfr 命令来显示包括 **sfr** 命令的每个服务策略的统计信息和状态。可以使用 **clear service-policy** 命令，清除计数器。

以下示例显示 ASA FirePOWER 服务策略和当前统计信息，以及模块状态：

```
ciscoasa# show service-policy sfr

Global policy:
Service-policy: global_policy
    Class-map: my-sfr-class
      SFR: card status Up, mode fail-close
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

以下示例显示仅监控策略。在这种情况下，应该看到数据包输入计数器增加，但是数据包输出计数器应保持为零，因为无流量传回至 ASA。

```
hostname# show service-policy sfr
Global policy:
Service-policy: global_policy
    Class-map: bypass
      SFR: card status Up, mode fail-open, monitor-only
        packet input 2626422041, packet output 0, drop 0, reset-drop 0, proxied 0
```

监控模块连接

要显示 ASA FirePOWER 模块的连接，请输入以下命令之一：

- **show asp table classify domain sfr**

  显示为将流量发送至 ASA FirePOWER 模块而创建的 NP 规则。

- **show asp drop**

  将显示丢弃的数据包。丢弃类型说明如下。

- **show conn**

  将显示 ‘X - inspected by service module’ 标记显示连接是否正在被转发到模块。

show asp drop 命令可能包括以下与 ASA FirePOWER 模块相关的丢弃原因。

丢帧：

- sfr-bad-tlv-received - 当 ASA 从 FirePOWER 收到没有 Policy ID TLV 的数据包时发生此情况。如果此 TLV 未在操作字段中设置备用 / 主用位，则必须存在于非控数据包中。
- sfr-request - 此帧由 FirePOWER 根据 FirePOWER 上的一条策略请求丢弃，其中 FirePOWER 将操作设置为 Deny Source、Deny Destination 或 Deny Pkt。如果不该丢弃该帧，请复查拒绝流的模块上的策略。
- sfr-fail-close - 数据包已丢弃，因为卡未正常工作且配置的策略为 “fail-close”（而不是 “fail-open”，该策略即使在卡出现故障的情况下也允许数据包通过）。检查卡状态并尝试重新启动服务或重新启动卡。
- sfr-fail - 已为现有流移除 FirePOWER 配置且无法通过将丢弃它的 FirePOWER 对其进行处理。这种情况十分罕见。
- sfr-malformed-packet - 来自 FirePOWER 的数据包包含无效的报头。例如，报头长度可能有误。

- sfr-ha-request - 当安全设备收到 FirePOWER HA 请求数据包但无法对其进行处理，且数据包已丢弃时，此计数器递增。
- sfr-invalid-encap - 当安全设备收到具有无效消息报头的 FirePOWER 数据包，且数据包已丢弃时，此计数器递增。
- sfr-bad-handle-received - 在来自 FirePOWER 模块的数据包中收到错误的流句柄，因此丢弃流。此计数器递增，FirePOWER 流的句柄在流持续时间期间已更改，因此在 ASA 上丢弃流和数据包。
- sfr-rx-monitor-only - 当安全设备在仅监控模式下收到 FirePOWER 数据包，且数据包已丢弃时，此计数器递增。

流量丢弃：

- sfr-request - FirePOWER 请求终止流量。设置了操作位 0。
- reset-by-sfr - FirePOWER 请求终止并重置流量。设置了操作位 1。
- sfr-fail-close - 流量已终止，因为卡出现故障且配置的策略为 “fail-close”。

ASA FirePOWER 模块的示例

以下示例将所有 HTTP 流量转移至 ASA FirePOWER 模块，并在模块因任何原因出现故障时阻止所有 HTTP 流量。

```
hostname(config)# access-list ASASFR permit tcp any any eq 80
hostname(config)# class-map my-sfr-class
hostname(config-cmap)# match access-list ASASFR
hostname(config-cmap)# policy-map my-sfr-policy
hostname(config-pmap)# class my-sfr-class
hostname(config-pmap-c)# sfr fail-close
hostname(config-pmap-c)# service-policy my-sfr-policy global
```

以下示例将本该转入 10.1.1.0 网络和 10.2.1.0 网络的所有 IP 流量均转移至 ASA FirePOWER 模块，并在模块因任何原因出现故障时允许所有流量通过。

```
hostname(config)# access-list my-sfr-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-sfr-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-sfr-class
hostname(config-cmap)# match access-list my-sfr-acl
hostname(config)# class-map my-sfr-class2
hostname(config-cmap)# match access-list my-sfr-acl2
hostname(config-cmap)# policy-map my-sfr-policy
hostname(config-pmap)# class my-sfr-class
hostname(config-pmap-c)# sfr fail-open
hostname(config-pmap)# class my-sfr-class2
hostname(config-pmap-c)# sfr fail-open
hostname(config-pmap-c)# service-policy my-sfr-policy interface outside
```

ASA FirePOWER 模块的历史记录

功能名称	平台版本	功能信息
适用于匹配 ASA FirePOWER SSP 硬件模块的 ASA 5585-X（所有型号）支持。 适用于 ASA FirePOWER 软件模块的 ASA 5512-X 至 ASA 5555-X 支持。	ASA 9.2(2.4) ASA FirePOWER 5.3.1	ASA FirePOWER 模块提供下一代防火墙服务，包括下一代 IPS (NGIPS)、应用可视性与控制 (AVC)、URL 过滤以及高级恶意软件防护 (AMP)。该模块既可在单情景模式或多情景模式下使用，也可在路由模式或透明模式下使用。 我们引入或修改了以下命令：**capture interface asa_dataplane**、**debug sfr**、 **hw-module module 1 reload**、**hw-module module 1 reset**、**hw-module module 1 shutdown**、**session do setup host ip**、**session do get-config**、**session do password-reset**、**session sfr**、**sfr**、**show asp table classify domain sfr**、**show capture**、**show conn**、**show module sfr**、**show service-policy** 和 **sw-module sfr**。

ASA CX 模块

本章介绍如何配置在 ASA 上运行的 ASA CX 模块。

- 第 18-1 页上的 ASA CX 模块
- 第 18-5 页上的 ASA CX 模块的许可要求
- 第 18-5 页上的 ASA CX 的先决条件
- 第 18-5 页上的 ASA CX 的准则
- 第 18-7 页上的 ASA CX 的默认设置
- 第 18-7 页上的配置 ASA CX 模块
- 第 18-17 页上的管理 ASA CX 模块
- 第 18-19 页上的监控 ASA CX 模块
- 第 18-21 页上的对身份验证代理进行故障排除
- 第 18-22 页上的 ASA CX 模块的示例
- 第 18-23 页上的 ASA CX 模块的历史

ASA CX 模块

通过 ASA CX 模块，您可以根据情况的全部情景实施安全措施。情景包括用户身份（谁）、用户要访问的应用或网站（什么）、尝试访问的来源（哪里）、尝试访问的时间（什么时候）和用于访问的设备的属性（如何）。通过 ASA CX 模块，您可以提取流量的全部情景并执行精细策略，例如允许访问 Facebook，但不允许访问 Facebook 上的游戏，或允许财务人员访问敏感的企业数据库，但不允许其他员工进行同样的访问。

- 第 18-2 页上的 ASA CX 模块如何与 ASA 配合使用
- 第 18-4 页上的 ASA CX 管理访问
- 第 18-4 页上的用于主动活动身份验证的身份验证代理
- 第 18-5 页上的与 ASA 功能的兼容性

ASA CX 模块如何与 ASA 配合使用

ASA CX 模块从 ASA 运行单独应用。本模块可以是一个硬件模块（适用于 ASA 5585-X），也可以是一个软件模块（适用于 5512-X 至 5555-X）。作为硬件模块，设备包括独立的管理和控制台端口，以及由 ASA 直接使用（而非由模块本身使用）的额外数据接口。

您可在正常内联模式或在仅监控模式下配置设备用于演示。

- 在内联部署中，实际流量发送至设备，并且设备的策略会影响将对流量执行的操作。在丢弃不需要的流量并执行由策略应用的任何其他操作后，流量返回至 ASA，以供进一步处理和最终传输。
- 在仅监控部署中，在被动部署中，流量副本将会被发送到设备，但不会被返回到 ASA。在仅监控模式下，您可以看到设备在不影响网络的情况下如何对流量进行处理。您可以使用仅监控服务策略或流量转发接口配置该模式。有关仅监控模式的准则和限制的详细信息，请参阅第 18-5 页上的 ASA CX 的准则。

以下各节对这些模式进行了更详细地说明。

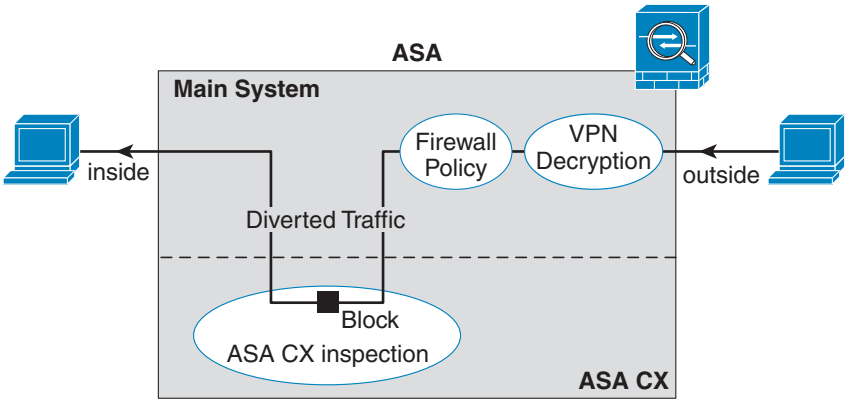
ASA CX 正常内联模式

在正常内联模式下，流量在被转发到 ASA CX 模块之前会通过防火墙检查。当在 ASA 上识别流量以进行 ASA CX 检测时，流量按以下所述顺序流经 ASA 和 ASA CX 模块：

1. 流量进入 ASA。
2. 对传入的 VPN 流量解密。
3. 应用防火墙策略。
4. 流量被发送至 ASA CX 模块。
5. ASA CX 模块将安全策略应用至流量，并采取适当的操作。
6. 有效流量将重新发送到 ASA； ASA CX 模块可能根据其安全策略阻止某些流量，这些流量将不会被传送。
7. 对传出的 VPN 流量加密。
8. 流量退出 ASA。

下图显示在使用 ASA CX 模块时的流量。在本示例中，ASA CX 模块自动阻止了某个应用所不允许的流量。所有其他流量均通过 ASA 转发。

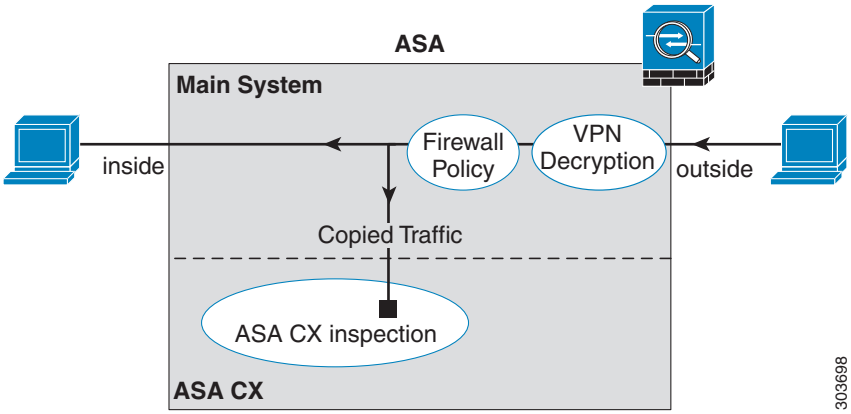
图 18-1　ASA 中的 ASA CX 模块流量



仅监控模式下的服务策略

出于测试和演示的目的，您可以配置 ASA，以将只读流量的副本数据流发送到 ASA CX 模块，这样就可以看出模块如何在不影响 ASA 流量的情况下检查流量。在该模式下，ASA CX 模块照例检查流量、制定策略决策并生成事件。但是，因为数据包是只读副本，因此模块操作不会影响实际流量。相反，检测完成后模块会丢弃副本。下图显示了仅监控模式下的 ASA CX 模块。

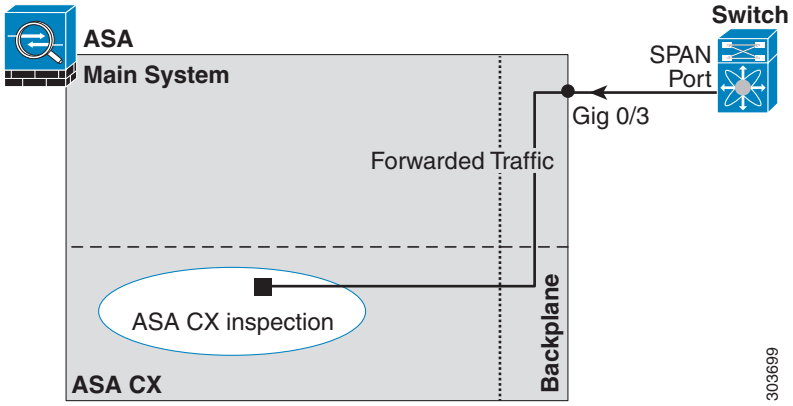
图 18-2　ASA CX 仅监控模式



仅监控模式下的流量转发接口

或者，您可以将 ASA 接口配置为流量转发接口，接收的所有流量将直接被转发到 ASA CX 模块，无需任何 ASA 处理。出于测试和演示的目的，流量转发消除了 ASA 处理的额外复杂情况。只有在仅监控模式下才支持流量转发。因此，ASA CX 模块在检查流量后会丢弃该流量。下图显示了为流量转发配置的 ASA GigabitEthernet 0/3 接口。该接口与交换机 SPAN 端口连接，因此 ASA CX 模块可以检查所有网络流量。

图 18-3　ASA CX 流量转发



ASA CX 管理访问

有两个单独的访问层用于管理 ASA CX 模块：初始配置（及后续故障排除）和策略管理。

- 第 18-4 页上的初始配置
- 第 18-4 页上的策略配置和管理

初始配置

为了进行初始配置，您必须使用 ASA CX 模块上的 CLI 运行 **setup** 命令并配置其他可选设置。

要访问 CLI，您可以使用以下方法：

- ASA 5585-X：
  - ASA CX 控制台端口 - ASA CX 控制台端口是一个单独的外部控制台端口。
  - 使用 SSH 的 ASA CX 管理 1/0 接口 - 您可以连接至默认的 IP 地址 (192.168.8.8)，也可以在使用 ASDM 更改管理 IP 地址后使用 SSH 进行连接。ASA CX 管理接口是一个单独的外部千兆位以太网接口。

  注　您无法使用 **session** 命令来访问 ASA 背板上的 ASA CX 硬件模块 CLI。

- ASA 5512-X 至 ASA 5555-X：
  - 背板上的 ASA 的会话 - 如对 ASA 有 CLI 访问权，则可向模块发起会话并访问模块 CLI。
  - 使用 SSH 的 ASA CX 管理 0/0 接口 - 您可以连接至默认的 IP 地址 (192.168.1.2)，也可以在使用 ASDM 更改管理 IP 地址后使用 SSH 进行连接。这些模式将 ASA CX 模块作为一个软件模块运行。ASA CX 管理接口与 ASA 共用管理 0/0 接口。ASA 和 ASACX 模块支持单独的 MAC 地址和 IP 地址。您必须在 ASA CX 操作系统内（使用 CLI 或 ASDM）配置 ASA CX IP 地址。但是，物理特性（例如启用接口）在 ASA 上配置。您可以移除 ASA 接口配置（具体是指接口名称），将此接口指定为一个仅 ASA CX 接口。此接口仅用于管理。

策略配置和管理

完成初始配置后，应使用思科 Prime 安全管理器 (PRSM) 配置 ASA CX 策略。PRSM（即思科 Prime 安全管理器）既是 ASA CX 配置接口的名称，也是用于配置 ASA CX 设备的独立产品的名称。

然后配置 ASA 策略，以使用 ASDM、ASA CLI 或 PRSM（在多设备模式下）向 ASA CX 模块发送流量。

用于主动活动身份验证的身份验证代理

您可以在 ASA CX 上配置身份策略，以采集用户身份信息用于访问策略。系统可以主动（通过提示输入用户名和密码凭证）或者被动（通过检索 AD 代理或 思科 Context Directory Agent、CDA 所采集的信息）采集用户身份。

如果要使用主动身份验证，您必须将 ASA 配置为身份验证代理。ASA CX 模块将身份验证请求重定向至 ASA 接口 IP 地址 / 代理端口。默认端口为 885，但是，您也可以配置不同的端口。

如第 18-15 页上的创建 ASA CX 服务策略中所述，要启用主动身份验证，您应将身份验证代理启用为将流量重定向至 ASA CX 的服务策略的一部分。

与 ASA 功能的兼容性

ASA 提供许多高级应用检测功能，包括 HTTP 检测。但是，ASA CX 模块比 ASA 提供了更高级的 HTTP 检测，以及适用于其他应用的附加功能，包括监控和控制应用的使用情况。

要充分利用 ASA CX 模块的功能，请按照以下准则处理发送至 ASA CX 模块的流量：

- 请勿对 HTTP 流量配置 ASA 检测。
- 请勿配置云网络安全 (ScanSafe) 检测。如果对同一流量同时配置 ASA CX 操作和云网络安全检测，ASA 只执行 ASA CX 操作。
- ASA 的其他应用检测（包括默认检测）与 ASA CX 模块兼容。
- 勿启用移动用户安全 (MUS) 服务器；此服务器与 ASA CX 模块不兼容。
- 请勿启用 ASA 集群； ASA 集群与 ASA CX 模块不兼容。

ASA CX 模块的许可要求

ASA CX 模块和 PRSM 需要附加许可证，此许可证需安装在模块中而非 ASA 的情景中。ASA 本身不需要附加许可证。有关详细信息，请参阅 ASA 文档。

ASA CX 的先决条件

要使用 PRSM 配置 ASA，您需要在 ASA 上安装证书以确保安全通信。默认情况下，ASA 会生成自签名证书。但是，由于发布者不详，该证书会导致浏览器给出提示，要求您对证书进行验证。要避免这些浏览器提示，您可以安装已知认证中心 (CA) 提供的证书。如果您从 CA 申请证书，应确保证书类型同时是服务器身份验证证书和客户端身份验证证书。有关详细信息，请参阅常规操作配置指南。

ASA CX 的准则

情景模式准则

从 ASA CX 9.1(3) 开始，支持多情景模式。

但是，ASA CX 模块自身（在 PRSM 中配置）是一台单一情景模式设备；来自 ASA 的情景特定流量将根据通用 ASA CX 策略来检查。因此，您无法在多情景中使用相同的 IP 地址；每个情景必须包含唯一的网络。

防火墙模式准则

在路由和透明防火墙模式下受支持。只有透明模式支持流量转发接口。

故障转移准则

不支持直接故障转移；在 ASA 进行故障转移时，所有现有 ASA CX 流量会被传输到新 ASA，但是，允许流量在未被 ASA CX 检查的情况下通过 ASA。ASA CX 模块只对新 ASA 接收到的新流量起作用。

ASA 集群准则

不支持集群。

IPv6 准则

- 支持 IPv6。
- （9.1(1) 和更早版本）不支持 NAT 64。9.1(2) 和后期版本支持 NAT 64。

型号准则

- 仅 ASA 5585-X 和 5512-X 至 ASA 5555-X 支持。有关详细信息，请参阅《*思科 ASA 兼容性矩阵*》：

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- 对于 5512-X 至 ASA 5555-X，必须安装思科固态硬盘 (SSD)。有关详细信息，请参阅《ASA 5500-X 硬件指南》。

仅监控模式准则

仅监控模式不是模块的正常运行方式，该模式严格限制于演示的目的。

- 无法在 ASA 上同时配置仅监控模式和正常内联模式。仅允许使用一种安全策略类型。在多情景模式下，无法为某些情景配置仅监控模式，并同时为其他情景配置常规内联模式。
- 仅监控模式下不支持以下功能：
  - 拒绝策略
  - 主动身份验证
  - 解密策略
- ASA CX 在仅监控模式下不执行数据包缓冲，并会以尽力而为的方式生成事件。例如，某些事件可能会受到缓冲不足的影响，例如带有跨数据包边界的较长 URL 的事件。
- 请确保将 ASA 策略和 ASA CX 都配置为具有匹配的模式：均在仅监控模式下或均在正常内联模式下。

流量转发接口附加准则：

- ASA 必须处于透明模式。
- 您可将多达 4 个接口配置为流量转发接口。其他 ASA 接口可用作普通接口。
- 流量转发接口必须是物理接口，而不是 VLAN 或 BVI。物理接口也不能有任何关联的 VLAN。
- 流量转发接口不能用于 ASA 流量；您无法为 ASA 功能（包括故障转移或仅管理）对这些接口进行命名或配置。
- 您无法为 ASA CX 流量同时配置流量转发接口和服务策略。

附加准则和限制

- 请参阅第 18-5 页上的与 ASA 功能的兼容性。
- 您无法更改安装在硬件模块上的软件的类型；如果购买了 ASA CX 模块，则以后无法为其安装其他软件。

ASA CX 的默认设置

下表列出了 ASA CX 模块的默认设置。

表 18-1　默认网络参数

参数	默认
管理 IP 地址	ASA 5585-X：管理 1/0 192.168.8.8/24 ASA 5512-X 至 ASA 5555-X：管理 0/0 192.168.1.2/24
网关	ASA 5585-X：192.168.8.1/24 ASA 5512-X 至 ASA 5555-X：192.168.1.1/24
SSH 或会话用户名	admin
密码	Admin123

配置 ASA CX 模块

ASA CX 模块的配置过程包括在 ASA CX 模块上配置 ASA CX 安全策略，以及对 ASA 进行配置以将流量发送到 ASA CX 模块。要配置 ASA CX 模块，请执行以下操作：

步骤 1　第 18-7 页上的连接 ASA CX 管理接口。连接 ASA CX 管理接口或者控制台接口。

步骤 2　第 18-10 页上的（适用于 ASA 5512-X 至 ASA 5555-X）安装或重新映像软件模块。

步骤 3　如有必要，第 18-12 页上的（适用于 ASA 5585-X）更改 ASA CX 管理 IP 地址。初次 SSH 访问可能要求此操作。

步骤 4　第 18-12 页上的配置 ASA CX 基本设置。在 ASA CX 模块上执行此操作。

步骤 5　第 18-14 页上的在 ASA CX 模块上配置安全策略。

步骤 6　（可选）第 18-14 页上的配置身份验证代理端口。

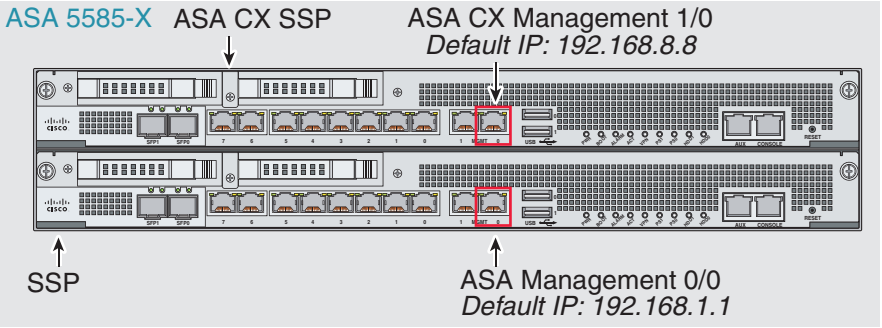
步骤 7　第 18-14 页上的向 ASA CX 模块重定向流量。

连接 ASA CX 管理接口

除提供对 ASA CX 模块的管理访问外，ASA CX 管理接口还需要访问 HTTP 代理服务器或 DNS 服务器以及互联网，以获取签名更新和其他信息。本节描述推荐的网络配置。您的网络可能不同。

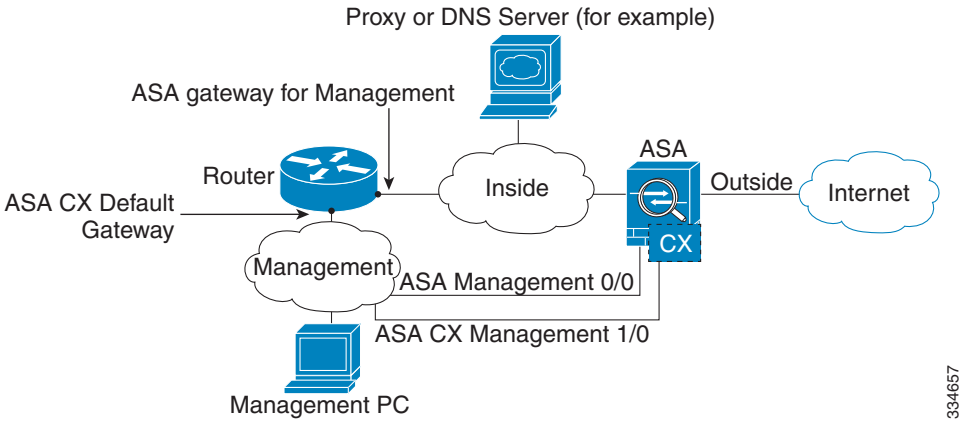
ASA 5585-X（硬件模块）

ASA CX 模块带有一个来自 ASA 的单独管理和控制台接口。对于初始设置，可以使用默认的 IP 地址 (192.168.8.8/24)，通过 SSH 连接到 ASA CX 管理 1/0 接口。如果无法使用默认 IP 地址，则可使用控制台端口，或使用 ASDM 来更改管理 IP 地址，以便使用 SSH。



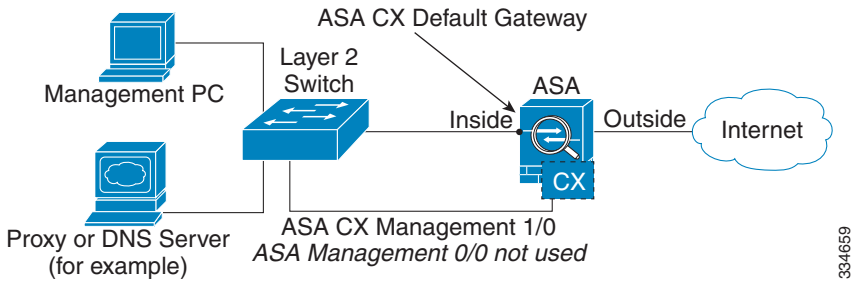
如果有内部路由器

如果有内部路由器，您可以在管理网络（可以包括 ASA 管理 0/0 和 ASA CX 管理 1/0 接口）和 ASA 内部网络之间建立路由，以访问互联网。另外，务必在 ASA 上添加一个路由，以便通过内部路由器访问管理网络。



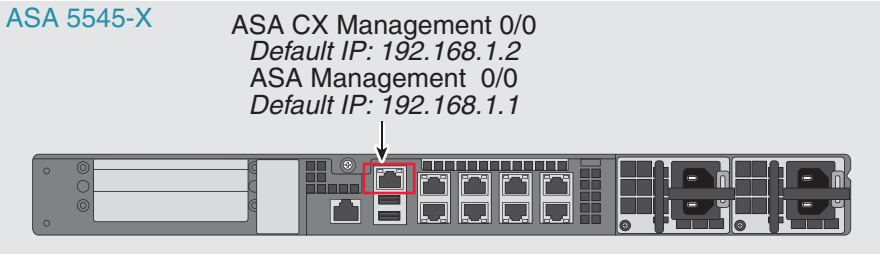
如果没有内部路由器

如果只有一个内部网络，您就无法拥有一个单独管理网络，这需要内部路由器实现网络之间的路由。在这种情况下，可从内部接口而非管理 0/0 接口管理 ASA。由于 ASA CX 模块是来自 ASA 的单独设备，您可以将 ASA CX 管理 1/0 地址配置为与内部接口处于相同的网络。



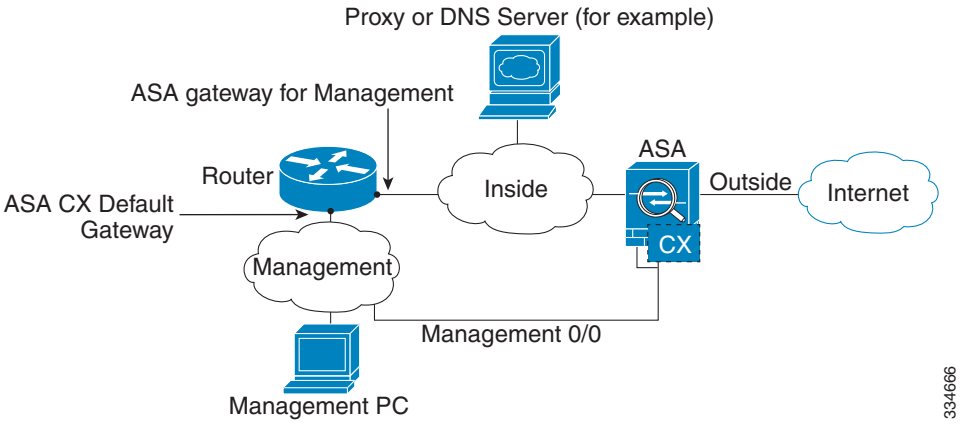
ASA 5512-X 至 ASA 5555-X（软件模块）

模块在这些型号中作为一个软件模块运行，且 ASA CX 管理接口与 ASA 共用管理 0/0 接口。对于初始设置，可以使用 SSH 连接到 ASA CX 默认的 IP 地址 (192.168.1.2/24)。如果无法使用默认的 IP 地址，可以与背板上的 ASA CX 会话或使用 ASDM 更改管理 IP 地址，以使用 SSH。



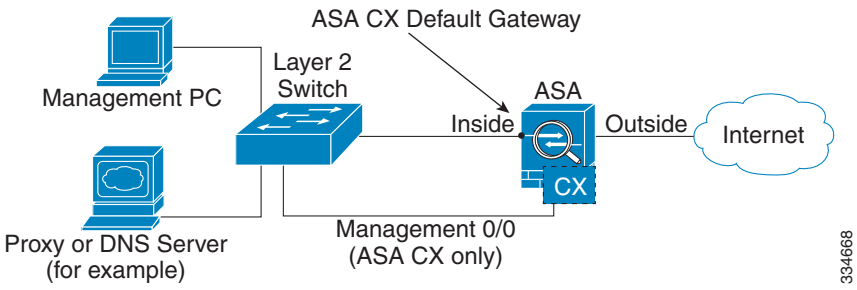
如果有内部路由器

如果有内部路由器，您可以在管理 0/0 网络（包括 ASA 和 ASA CX 管理 IP 地址）和内部网络之间建立路由，以访问互联网。另外，务必在 ASA 上添加一个路由，以便通过内部路由器访问管理网络。



如果没有内部路由器

如果只有一个内部网络，您就无法拥有一个单独的管理网络。在这种情况下，可从内部接口而非管理 0/0 接口管理 ASA。如果从管理 0/0 接口移除 ASA 配置的名称，您仍可以配置该接口的 ASA CX IP 地址。由于 ASA CX 模块实质上是来自 ASA 的单独设备，您 *可以*将 ASA CX 管理地址配置为与内部接口处于相同的网络。



注　您必须移除管理 0/0 的 ASA 配置名称；如果在 ASA 已配置该名称，则 ASA CX 地址必须与 ASA 在同一网络，并且排除所有已在其他 ASA 接口上配置的网络。如果该名称未配置，则 ASA CX 地址可在任何网络，例如，ASA 内部网络。

（适用于 ASA 5512-X 至 ASA 5555-X）安装或重新映像软件模块

如果您购买了含有 ASA CX 模块的 ASA，则模块软件和所需的固态驱动器 (SSD) 已预先安装好并准备就绪。如果要向现有 ASA 添加 ASA CX 或需要更换 SSD，您需要根据此操作步骤安装 ASA CX 启动软件并对 SSD 进行分区。要物理安装 SSD，请参阅《ASA 硬件指南》。

重新映像模块的操作步骤与此相同，不同之处在于您首先要卸载 ASA CX 模块。如果更换 SSD，需要重新映像系统。

注　对于 ASA 5585-X 硬件模块，您必须在 ASA CX 模块内安装或升级映像。有关详细信息，请参阅 ASA CX 模块文档。

准备工作

- 除去启动软件所占空间外，闪存 (disk0) 上的可用空间至少应为 3GB。
- 在多情景模式下，请在系统执行空间中执行此操作步骤。
- 必须先关闭可能正在运行的任何其他软件模块；设备一次可运行一个软件模块。必须从 ASA CLI 执行此操作。例如，以下命令关闭并卸载 IPS 软件模块，然后重新加载 ASA。

```
hostname# sw-module module ips shutdown
hostname# sw-module module ips uninstall
hostname# reload
```

注　如果有活动服务策略将流量重定向至 IPS 模块，您必须移除该策略。例如，如果策略为全局策略，则将使用 **no service-policy** *ips_policy* **global**。可以使用 CLI 或 ASDM 移除策略。

- 如果重新映像模块，请使用相同关闭和卸载命令来移除旧映像。例如，**sw-module module cxsc uninstall**。
- 从 Cisco.com 获取 ASA CX 启动映像和系统软件包：http://software.cisco.com/download/type.html?mdfid=284325223&flowid=34503。

操作步骤

步骤 1　下载启动映像至设备。请勿传输系统软件；稍后会将其下载至 SSD。您有以下选项：

- ASDM - 首先，下载启动映像至工作站，或将其放在 FTP、TFTP、HTTP、HTTPS、SMB 或 SCP 服务器上。然后，在 ASDM 中，选择 **Tools > File Management**，然后选择适当的 **File Transfer** 命令，**Between Local PC and Flash** 或 **Between Remote Server and Flash**。传输启动软件至 ASA 上的 disk0。

- ASA CLI - 首先，将启动映像放在 TFTP、FTP、HTTP 或 HTTPS 服务器上，然后使用 **copy** 命令将其下载至闪存。以下示例使用 TFTP ；请使用服务器的 IP 地址或主机名替换 <TFTP Server>。

  ```
  ciscoasa# copy tftp://<TFTP SERVER>/asacx-5500x-boot-9.3.1.1-112.img
  disk0:/asacx-5500x-boot-9.3.1.1-112.img
  ```

步骤 2　从 Cisco.com 将 ASA CX 系统软件下载到可以通过 ASA CX 管理接口访问的 HTTP、HTTPS 或 FTP 服务器。

步骤 3　输入以下命令，在 ASA disk0 中设置 ASA CX 模块启动映像的位置：

```
hostname# sw-module module cxsc recover configure image disk0:file_path
```

注　如果收到类似 “ERROR: Another service (ips) is running, only one service is allowed to run at any time,” 的消息，表明您已经配置了不同的软件模块。必须将其关闭并移除，以安装以上 “ 先决条件 ” 一节所述的新模块。

示例：

```
hostname# sw-module module cxsc recover configure image
disk0:asacx-5500x-boot-9.3.1.1-112.img
```

步骤 4　输入下列命令加载 ASA CX 启动映像：

```
hostname# sw-module module cxsc recover boot
```

步骤 5　等待 5 分钟左右，ASA CX 模块启动完成后，打开控制台会话至正在运行的 ASA CX 启动映像。默认用户名是 **admin**，默认密码是 **Admin123**。

```
hostname# session cxsc console
Establishing console session with slot 1
Opening console session with module cxsc.
Connected to module cxsc.Escape character sequence is 'CTRL-SHIFT-6 then x'.
cxsc login: admin
Password: Admin123
```

提示　如果模块启动未完成，则 **session** 命令将失败，并显示有关无法通过 ttyS1 连接的消息。请稍后重试。

步骤 6　对 SSD 进行分区：

```
asacx-boot> partition
....
Partition Successfully Completed
```

步骤 7　使用 **setup** 命令根据第 18-12 页上的配置 ASA CX 基本设置（请勿退出 ASA CX CLI），进行基本的网络设置，然后返回该操作步骤安装软件映像。

步骤 8　使用 **system install** 命令安装系统软件映像：

system install [**noconfirm**] *url*

如果不想回复确认消息，请在命令中添加 **noconfirm** 选项。使用 HTTP、HTTPS 或 FTP URL ；如果需要用户名和密码，系统将提示您提供这些信息。

安装完成后，系统重启，重启时控制台会话会关闭。应用组件安装以及 ASA CX 服务启动需要 10 分钟或更长的时间。（**show module cxsc** 输出应将所有进程显示为 Up。）

以下命令安装 asacx-sys-9.3.1.1-112.pkg 系统软件。

```
asacx-boot> system install https://upgrades.example.com/packages/asacx-sys-9.3.1.1-112.pkg

Username: buffy
Password: angelforever
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA CX 9.3.1.1-112 System Install
        Requires reboot:                Yes

Do you want to continue with upgrade?[n]: Y
Warning: Please do not interrupt the process or turn off the system.Doing so might leave
system in unusable state.
Upgrading
Stopping all the services ...
Starting upgrade process ...
Reboot is required to complete the upgrade.Press Enter to reboot the system.
```

（适用于 ASA 5585-X）更改 ASA CX 管理 IP 地址

如果无法使用默认的管理 IP 地址 (192.168.8.8)，可以从 ASA 设置管理 IP 地址。设置管理 IP 地址后，可以使用 SSH 访问 ASA CX 模块执行初始设置。

注　对于软件模块，可以访问 ASA CX CLI，通过从 ASA 发起会话来执行设置；然后在设置过程中设置 ASA CX 管理 IP 地址。请参阅第 18-12 页上的配置 ASA CX 基本设置。

要通过 ASA 更改管理 IP 地址，请执行以下操作之一。在多情景模式下，请在系统执行空间中执行此操作步骤。

- 在 CLI 中，使用以下命令设置 ASA CX 管理 IP 地址、掩码和网关。

  session 1 do setup host ip *ip_address*/*mask*,*gateway_ip*

  例如，**session 1 do setup host ip 10.1.1.2/24,10.1.1.1**。
- （仅限单一情景模式）在 ASDM 中，选择 **Wizards > Startup Wizard**，并向前浏览向导直至进入 ASA CX Basic Configuration 界面，在该界面中，您可以设置 IP 地址、掩码和默认网关。如果默认设置不适合，您还可以设置另外一个身份验证代理端口。

配置 ASA CX 基本设置

配置安全策略之前，您必须在 ASA CX 模块上模块配置基本网络设置和其他参数。您只能通过 ASA CX CLI 配置这些设置。

操作步骤

步骤 1　执行以下操作之一：

- （适用于所有型号）使用 SSH 连接至 ASA CX 管理 IP 地址。
- （适用于 ASA 5512-X 至 ASA 5555-X）从 ASA CLI 打开与模块的控制台会话。在多情景模式下，从系统执行空间发起会话。

```
hostname# session cxsc console
```

步骤 2　使用用户名 **admin** 和密码 **Admin123** 登录。在此操作步骤中，您可以更改密码。

步骤 3　输入以下命令：

```
asacx> setup
```

示例：

```
asacx> setup
Welcome to Cisco Prime Security Manager Setup
[hit Ctrl-C to abort]
Default values are inside [ ]
```

按照设置向导提示操作。以下示例通过向导显示了一个典型路径；如果在提示符下输入 **Y** 而不是 **N**，您可以配置其他的设置。此示例显示如何配置 IPv4 和 IPv6 静态地址。如果要配置 IPv6 无状态自动配置，您可以在系统询问您是否要配置静态 IPv6 地址时回答 **N**。

```
Enter a hostname [asacx]: asa-cx-host
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n)[N]: N
Enter an IPv4 address [192.168.8.8]: 10.89.31.65
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 10.89.31.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: Y
Enter an IPv6 address: 2001:DB8:0:CD30::1234/64
Enter the gateway: 2001:DB8:0:CD30::1
Enter the primary DNS server IP address [ ]: 10.89.47.11
Do you want to configure Secondary DNS Server?(y/n) [N]: N
Do you want to configure Local Domain Name?(y/n) [N] Y
Enter the local domain name: example.com
Do you want to configure Search domains?(y/n) [N] Y
Enter the comma separated list for search domains: example.com
Do you want to enable the NTP service?(y/n) [N]: Y
Enter the NTP servers separated by commas: 1.ntp.example.com, 2.ntp.example.com
```

步骤 4　在完成最终提示后，系统将显示设置汇总。浏览摘要以确认这些值都正确，然后输入 **Y** 以应用更改后的配置。输入 **N** 将撤消更改。

示例：

```
Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Done.
Generating self-signed certificate, the web server will be restarted after that
...
Done.
Press ENTER to continue...
asacx>
```

注　如果您更改了主机名，直到您注销并重新登录后才提示会显示新名称。

步骤 5　如果不使用 NTP，您应配置时间设置。默认时区为 UTC 时区。使用 **show time** 命令查看当前设置。您可以使用以下命令更改时间设置：

```
asacx> config timezone
asacx> config time
```

步骤 6　输入下列命令更改管理员密码：

```
asacx> config passwd
```

示例：

```
asacx> config passwd
The password must be at least 8 characters long and must contain
at least one uppercase letter (A-Z), at least one lowercase letter
(a-z) and at least one digit (0-9).
Enter password: Farscape1
Confirm password: Farscape1
SUCCESS: Password changed for user admin
```

步骤 7　输入 **exit** 命令注销。

在 ASA CX 模块上配置安全策略

使用 PRSM 在 ASA CX 模块上配置安全策略。安全策略控制模块所提供的服务。您无法通过 ASA CX CLI、ASA CLI 或 ASDM 配置策略。

PRSM（即思科 Prime 安全管理器）既是 ASA CX 配置接口的名称，也是用于配置 ASA CX 设备的独立产品的名称。访问配置接口的方法与如何使用 PRSM 的方法相同。有关使用 PRSM 配置 ASA CX 安全策略的详细信息，请参阅《ASA CX/PRSM 用户指南》或联机帮助。

要打开 PRSM，请使用网络浏览器打开以下 URL：

https://*management_address*

其中，*management_address* 是 ASA CX 管理接口或 PRSM 服务器的 DNS 名称或 IP 地址。例如 https://asacx.example.com.

配置身份验证代理端口

如果您在 ASA CX 策略中使用活动身份验证，ASA 使用端口 885 作为身份验证代理端口。如果 885 不能被接受，则配置另一个端口，但非默认端口编号必须大于 1024。有关身份验证代理的详细信息，请参阅第 18-4 页上的用于主动活动身份验证的身份验证代理。

在多情景模式下，应在每个安全情景内更改端口。

要更改身份验证代理端口，请输入以下命令：

cxsc auth-proxy port *port*

例如，**cxsc auth-proxy port 5000**。

向 ASA CX 模块重定向流量

您可以创建识别特定流量的服务策略，将流量重定向至 ASA CX 模块。仅在进行演示时，您可以为服务策略启用仅监控模式，将流量副本转发到 ASA CX 模块，而原有流量不会受到影响。

另外，演示时您可以配置流量转发接口，而不配置仅监控模式下的服务策略。流量转发接口绕过 ASA，将所有流量直接发送到 ASA CX 模块。

- 第 18-15 页上的创建 ASA CX 服务策略
- 第 18-16 页上的配置流量转发接口（仅监控模式）

创建 ASA CX 服务策略

您可以创建识别特定流量的服务策略，将流量重定向至 ASA CX 模块。

注　ASA CX 重定向是双向的。因此，如果为一个接口配置服务策略，该接口上的主机间建立了连接且有一个接口未配置重定向，则这些主机间的所有流量都会被发送到 ASA CX 模块，包括来自非 ASA CX 接口的流量。但是，由于身份验证代理仅适用于进口流量，因此 ASA 仅在应用了服务策略的接口上执行身份验证代理。

准备工作

- 如果使用此操作步骤在 ASA 上启用身份验证代理，则应确保也为 ASA CX 模块上的身份验证配置目录区域。有关详细信息，请参阅《ASA CX 用户指南》。
- 如果有活动服务策略将流量重定向流量至 IPS 模块（之前被 ASA CX 替换的模块），您必须在在配置 ASA CX 服务策略前将该策略移除。
- 请确保将 ASA 策略和 ASA CX 都配置为具有匹配的模式：均在仅监控模式下或均在正常内联模式下。
- 在多情景模式下，请在每个安全情景中执行此操作步骤。
- 在多设备模式下使用 PRSM 时，可以配置 ASA 策略用于将流量发送到 PRSM 内的 ASA CX 模块，而非使用 ASDM 或如下所述的 ASA CLI。但是，配置 ASA 服务策略时，PRSM 有一些限制；有关详细信息，请参阅《ASA CX 用户指南》。

操作步骤

步骤 1　创建 L3/L4 类映射以确定要发送至模块的流量。

```
class-map name
match parameter
```

示例：

```
hostname(config)# class-map cx_class
hostname(config-cmap)# match access-list cx_traffic
```

如果要将多个流量类发送至模块，则可创建多个类映射以用于安全策略。

有关匹配语句的信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。

步骤 2　添加或编辑策略映射，以用于设置要对类映射流量执行的操作。

```
policy-map name
```

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3　确定在此操作步骤开始时创建的类映射。

```
class name
```

示例：

```
hostname(config-pmap)# class cx_class
```

步骤 4　将流量发送到 ASA CX 模块。

cxsc {**fail-close** | **fail-open**} [**auth-proxy** | **monitor-only**]

其中：

- 关键字 **fail-close** 将 ASA 设置为在 ASA CX 模块不可用时阻止所有流量。
- **fail-open** 关键字将 ASA 设置为在模块不可用时允许所有流量未经检查即可通过。
- 可选关键字 **auth-proxy** 启用身份验证代理；主动身份验证需要身份验证代理。
- 仅限于示范，指定 **monitor-only** 将流量的只读副本发送到 ASA CX 模块。您必须将所有类和策略配置为仅监控模式或正常内联模式；您无法在同一 ASA 上同时配置两种模式。

示例：

```
hostname(config-pmap-c)# cxsc fail-close auth-proxy
```

步骤 5　如果为 ASA CX 流量创建了多个类映射，您可为策略指定另一个类，并应用 **cxsc** 重定向操作。

有关策略映射内类顺序的重要性的详细信息，请参阅第 1-5 页上的服务策略内的功能匹配。对于同一操作类型，流量无法匹配多个类映射。

步骤 6　如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口，**interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

配置流量转发接口（仅监控模式）

仅限于演示时，您可以配置流量转发接口，将所有流量直接转发到 ASA CX 模块。有关 ASA CX 正常运行的详细信息，请参阅第 18-15 页上的创建 ASA CX 服务策略。

有关详细信息，请参阅第 18-3 页上的仅监控模式下的流量转发接口。有关流量转发接口的专用准则和限制，也请参阅第 18-5 页上的 ASA CX 的准则。

准备工作

- 确保将 ASA 策略和 ASA CX 都配置为具有匹配的模式：均在仅监控模式下。
- 在多情景模式下，请在每个安全情景中执行此操作步骤。

操作步骤

步骤 1　为需要用于流量转发的物理接口输入接口配置模式。

interface *physical_interface*

示例：

```
hostname(config)# interface gigabitethernet 0/5
```

步骤 2　移除为该接口配置的所有名称。如果在任何 ASA 配置中使用了该接口，则移除该配置。您无法在已命名的接口上配置流量转发。

```
no nameif
```

步骤 3　启用流量转发。

```
traffic-forward cxsc monitor-only
```

步骤 4　启用接口。

```
no shutdown
```

为附加接口重复此操作步骤。

示例

以下示例采用 GigabitEthernet 0/5 为流量转发接口：

```
interface gigabitethernet 0/5
  no nameif
  traffic-forward cxsc monitor-only
  no shutdown
```

管理 ASA CX 模块

本节包括用于管理模块的操作步骤。

- 第 18-17 页上的重置密码
- 第 18-18 页上的重新加载或重置模块
- 第 18-18 页上的关闭模块
- 第 18-18 页上的（ ASA 5512-X 至 ASA 5555-X）卸载软件模块映像
- 第 18-19 页上的（ASA 5512-X 至 ASA 5555-X）从 ASA 向模块发起会话

重置密码

可将模块密码重置为默认值。用户 **admin** 的默认密码为 **Admin123**。重置密码后，应使用模块应用将其更改为一个唯一值。

重置模块密码将导致模块重新启动。重启模块时，服务不可用。

要将模块密码重置为默认密码，您可以采用以下方法之一。在多情景模式下，请在系统执行空间中执行此操作步骤。

- (CLI) 硬件模块 (ASA 5585-X)：

  ```
  hw-module module 1 password-reset
  ```

- （CLI）软件模块（ASA 5512-X 至 ASA 5555-X）：

  ```
  sw-module module cxsc password-reset
  ```

重新加载或重置模块

要重新加载，或重置并重新加载模块，请在 ASA CLI 处输入以下命令之一。在多情景模式下，请在系统执行空间中执行此操作步骤。

- 硬件模块 (ASA 5585-X)：

  hw-module module 1 {**reload** | **reset**}

- 软件模块（ASA 5512-X 至 ASA 5555-X）：

  sw-module module cxsc {**reload** | **reset**。

关闭模块

通过关闭模块软件，可让模块做好准备，在不丢失配置数据的情况下安全断电。要正确关闭模块，请在 ASA CLI 处输入以下命令之一。在多情景模式下，请在系统执行空间中执行此操作步骤。

注　如果重新加载 ASA，模块将不自动关闭，因此，我们建议先关闭模块，再重新加载 ASA。

- 硬件模块 (ASA 5585-X)：

  hw-module module 1 shutdown

- 软件模块（ASA 5512-X 至 ASA 5555-X）：

  sw-module module cxsc shutdown

（ASA 5512-X 至 ASA 5555-X）卸载软件模块映像

可卸载软件模块映像及其关联配置。在多情景模式下，请在系统执行空间中执行此操作步骤。

操作步骤

步骤 1　卸载软件模块映像以及关联配置。

```
hostname# sw-module module cxsc uninstall

Module cxsc will be uninstalled.This will completely remove the disk image
associated with the sw-module including any configuration that existed within it.

Uninstall module cxsc?[confirm]
```

步骤 2　重新加载 ASA。必须先重新加载 ASA，然后才能安装新模块。

```
hostname# reload
```

（ASA 5512-X 至 ASA 5555-X）从 ASA 向模块发起会话

使用 ASA CX CLI 配置基本网络设置并对模块进行故障排除。

要通过 ASA 访问 ASA CX 软件模块 CLI，您可以通过 ASA 进行会话。可向模块发起会话（使用 Telnet），也可创建虚拟控制台会话。如果控制面板已关闭且无法建立 Telnet 会话，则控制台会话可能有用。在多情景模式下，从系统执行空间发起会话。

在 Telnet 或控制台会话中，会提示您输入用户名和密码。使用用户名 **admin** 及其密码（默认密码为 **Admin123**）。

- Telnet 会话：

  ```
  session cxsc
  ```

  要从 ASA CX CLI 退回到 ASA CLI，请使用 **exit** 命令或同时按下 **Ctrl-Shift-6, x**。

- 控制台会话：

  ```
  session cxsc console
  ```

  退出控制台会话的唯一途径为同时按下 **Ctrl-Shift-6, x**。从模块注销后，您将回到模块登录提示符处。

注　请勿将 **session cxsc console** 命令与终端服务器结合使用，在该服务器上，**Ctrl-Shift-6, x** 是返回终端服务器提示符的转义字符串。**Ctrl-Shift-6, x** 也是退出 ASA CX 控制台并返回 ASA 提示符的字符串。因此，在这种情况下，如果您尝试退出 ASA CX 控制台，反而会一直退出到终端服务器提示符处。如果将终端服务器重新连接到 ASA，ASA CX 控制台会话仍处于活动状态；您无法退出到 ASA 提示符处。必须使用直接串行连接才能将控制台返回至 ASA 提示符。当出现这种情况时，请使用 **session cxsc** 命令而非控制台命令。

监控 ASA CX 模块

以下主题提供了有关监控模块的指南。有关 ASA CX 相关系统日志消息的详细信息，请参阅系统日志消息指南。ASA CX 系统日志消息的编号以 429001 开始。

- 第 18-19 页上的显示模块状态
- 第 18-20 页上的显示模块统计信息
- 第 18-20 页上的监控模块连接

显示模块状态

要检查模块状态，请输入以下命令之一：

- **show module [1 | cxsc] [details]**

  将显示模块状态。包含关键字 1（适用于硬件模块）或关键字 cxsc（适用于软件模块）以查看 ASA CX 模块的特定状态。包含关键字 details 以获取附加信息，包括管理模块的设备的地址。

- **show module cxsc recover**

  将显示安装模块时所使用的启动映像的位置。

以下为 **show module** 命令的输出示例，该命令用于安装了 ASA CX SSP 的 ASA：

```
hostname# show module
```

```
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAF1507AMKE
  1 ASA 5585-X CX Security Services Processor-10 ASA5585-SSP-CX10   JAF1510BLSA

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 5475.d05b.1100 to 5475.d05b.110b  1.0          2.0(7)0      100.7(6)78
  1 5475.d05b.2450 to 5475.d05b.245b  1.0          2.0(13)0     0.6.1

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 ASA CX Security Module         Up               0.6.1

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

显示模块统计信息

您可以使用 **show service-policy cxsc** 命令，显示包含 **cxsc** 命令的每个服务策略的统计信息和状态。可以使用 **clear service-policy** 命令清除计数器。

以下为 **show service-policy** 命令的输出示例，显示了 ASA CX 策略和当前统计信息以及身份验证代理禁用时的模块状态：

```
hostname# show service-policy cxsc
Global policy:
Service-policy: global_policy
    Class-map: bypass
      CXSC: card status Up, mode fail-open, auth-proxy disabled
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

以下为 **show service-policy** 命令的输出示例，显示了 ASA CX 策略和当前统计信息以及身份验证代理禁用时的模块状态；在此情况下，被代理的计数也会递增：

```
hostname# show service-policy cxsc
Global policy:
Service-policy: pmap
    Class-map: class-default
      Default Queueing      Set connection policy: random-sequence-number disable
        drop 0
      CXSC: card status Up, mode fail-open, auth-proxy enabled
        packet input 7724, packet output 7701, drop 0, reset-drop 0, proxied 10
```

监控模块连接

要显示通过 ASA CX 模块的连接，请输入以下某个命令：

- **show asp table classify domain cxsc**

  将显示为了将流量发送到 ASA CX 模块而创建的 NP 规则。

- **show asp table classify domain cxsc-auth-proxy**

  将显示为 ASA CX 模块的身份验证代理而创建的 NP 规则。以下为输出示例，这里显示一条规则，目标 “port=2000” 为 **cxsc auth-proxy port 2000** 命令配置的身份验证代理端口，而目标 “ip/id=192.168.0.100” 为 ASA 接口的 IP 地址。

```
hostname# show asp table classify domain cxsc-auth-proxy
Input Table
in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=inside, output_ifc=identity
```

- **show asp drop**

  将显示丢弃的数据包。丢弃类型说明如下。

- **show asp event dp-cp cxsc-msg**

  此输出显示 dp-cp 队列上有多少 ASA CX 模块消息。只有来自 ASA CX 模块的 VPN 查询会被发送到 dp-cp。

- **show conn**

  将显示 ‘X - inspected by service module’ 标记显示连接是否正在被转发到模块。

show asp drop 命令也可包含以下与 ASA CX 模块有关的丢弃原因。

丢帧：

- cxsc-bad-tlv-received - 当 ASA 从 CXSC 收到不包含 Policy ID TLV 的数据包时，发生丢帧。如果 actions 字段中未设置 Standby Active 位，该 TLV 必须出现在非控制数据包中。
- cxsc-request - CXSC 根据 CXSC 上的策略请求丢弃帧，CXSC 在策略中将操作设置为 Deny Source、Deny Destination 或 Deny Pkt。
- cxsc-fail-close - 由于卡片未开启且所配置的策略是 “fail-close”（而非即使在卡片关闭的状态下也允许数据包通过的 “fail-open”），因此数据包被丢弃。
- cxsc-fail - CXSC 配置已为现有流量移除，我们无法通过 CXSC 对其进行处理；因此选择丢失。这种情况十分罕见。
- cxsc-malformed-packet - 来自 CXSC 的数据包包含无效标头。例如，报头长度可能有误。

流量丢弃：

- cxsc-request - CXSC 要求终止流量。设置了操作位 0。
- reset-by-cxsc - CXSC 要求终止并重置流量。设置了操作位 1。
- cxsc-fail-close - 由于卡片关闭且已配置的策略是 “fail-close”，因此流量被终止。

对身份验证代理进行故障排除

如果您在使用身份验证代理功能时遇到问题，请按以下步骤对配置和连接进行故障排除。

注 如果在两个 ASA 接口上的主机间有连接，且仅为其中一个接口配置了 ASA CX 服务策略，则这些主机间的所有流量都会被发送到 ASA CX 模块，包括来自非 ASA CX 接口的流量（此功能是双向的）。但是，由于该功能仅限于进口，因此 ASA 仅对应用了服务策略的接口执行身份验证代理。

操作步骤

步骤 1　检查配置。

- 在 ASA 上，检查 **show asp table classify domain cxsc-auth-proxy** 命令的输出，确保已安装规则且这些规则是正确的。
- 在 PRSM 中，确保使用正确的凭证创建目录区域并测试连接，以便确保可以访问身份验证服务器；同时确保为身份验证配置了一个或多个策略对象。

步骤 2　检查 **show service-policy cxsc** 命令的输出，查看是否已代理任何数据包。

步骤 3　在背板 (**capture** *name* **interface asa_dataplane**) 上执行数据包捕获，并检查是否正在正确的已配置端口上重定向流量。您可以使用 **show running-config cxsc** 命令或 **show asp table classify domain cxsc-auth-proxy** 命令检查已配置的端口。

示例

确保始终使用了端口 2000：

1. 检查身份验证代理端口：

```
hostname# show running-config cxsc
cxsc auth-proxy port 2000
```

2. 检查身份验证代理规则：

```
hostname# show asp table classify domain cxsc-auth-proxy

Input Table
in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=inside, output_ifc=identity
```

3. 在数据包捕获中，重定向请求应该发往目标端口 2000。

ASA CX 模块的示例

以下示例将所有 HTTP 流量都转向 ASA CX 模块，并在 ASA CX 模块卡片由于任何原因发生故障时阻止所有 HTTP 流量：

```
hostname(config)# access-list ASACX permit tcp any any eq port 80
hostname(config)# class-map my-cx-class
hostname(config-cmap)# match access-list ASACX
hostname(config-cmap)# policy-map my-cx-policy
hostname(config-pmap)# class my-cx-class
hostname(config-pmap-c)# cxsc fail-close auth-proxy
hostname(config-pmap-c)# service-policy my-cx-policy global
```

以下示例将所有以 10.1.1.0 网络和 10.2.1.0 网络为目标的 IP 流量都转向 ASA CX 模块，并在 ASA CX 模块卡片由于任何原因发生故障时允许所有流量通过。

```
hostname(config)# access-list my-cx-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-cx-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-cx-class
hostname(config-cmap)# match access-list my-cx-acl
hostname(config)# class-map my-cx-class2
```

```
hostname(config-cmap)# match access-list my-cx-acl2
hostname(config-cmap)# policy-map my-cx-policy
hostname(config-pmap)# class my-cx-class
hostname(config-pmap-c)# cxsc fail-open auth-proxy
hostname(config-pmap)# class my-cx-class2
hostname(config-pmap-c)# cxsc fail-open auth-proxy
hostname(config-pmap-c)# service-policy my-cx-policy interface outside
```

ASA CX 模块的历史

功能名称	平台版本	说明
ASA CX SSP-10 和 -20 支持带 SSP-10 和 -20 的 ASA 5585-X	ASA 8.4(4.1) ASA CX 9.0(1)	通过 ASA CX 模块，您可以根据情况的全部情景实施安全措施。情景包括用户身份（谁）、用户要访问的应用或网站（什么）、尝试访问的来源（哪里）、尝试访问的时间（什么时候）和用于访问的设备的属性（如何）。通过 ASA CX 模块，您可以提取流量的全部情景并执行精细策略，例如允许访问 Facebook，但不允许访问 Facebook 上的游戏，或允许财务人员访问敏感的企业数据库，但不允许其他员工进行同样的访问。 引入或修改了以下命令：**capture**、**cxsc**、**cxsc auth-proxy**、**debug cxsc**、**hw-module module password-reset**、**hw-module module reload**、**hw-module module reset**、**hw-module module shutdown**、**session do setup host ip, session do get-config, session do password-reset, show asp table classify domain cxsc**、**show asp table classify domain cxsc-auth-proxy**、**show capture**、**show conn**、**show module** 和 **show service-policy**。
ASA CX SSP 支持 ASA 5512-X 至 ASA 5555-X	ASA 9.1(1) ASA CX 9.1(1)	为 ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 引入了 ASA CX SSP 软件模块支持。 修改了以下命令：**session cxsc**、**show module cxsc** 和 **sw-module cxsc**。
仅限于演示的仅监控模式	ASA 9.1(2) ASA CX 9.1(2)	仅在进行演示时，您可以为服务策略启用仅监控模式，将流量副本转发到 ASA CX 模块，而原有流量不会受到影响。 另外，演示时您可以配置流量转发接口，而不配置仅监控模式下的服务策略。流量转发接口绕过 ASA，将所有流量直接发送到 ASA CX 模块。 修改或引入了以下命令：**cxsc** {**fail-close** | **fail-open**} **monitor-only** 和 **traffic-forward cxsc monitor-only**。

功能名称	平台版本	说明
ASA CX 模块支持 NAT 64	ASA 9.1(2) ASA CX 9.1(2)	您现在可以结合 ASA CX 模块使用 NAT 64。 我们未修改任何命令。
ASA CX SSP-40 和 -60 支持带 SSP-40 和 -60 的 ASA 5585-X	ASA 9.1(3) ASA CX 9.2(1)	ASA CX SSP-40 和 -60 模块可以与匹配级别带 SSP-40 和 -60 的 ASA 5585-X 一起使用。 我们未修改任何命令。
ASA CX 模块支持多情景模式	ASA 9.1(3) ASA CX 9.2(1)	您现在可以在 ASA 上按情景配置 ASA CX 服务策略。 **注**　虽然您可以配置每情景 ASA 服务策略，但是，ASA CX 模块自身（在 PRSM 中配置）是一台单一情景模式设备；来自 ASA 的情景特定流量将根据通用 ASA CX 策略来检查。 我们未修改任何命令。
过滤在 ASA CX 背板上捕获的数据包	ASA 9.1(3) ASA CX 9.2(1)	您现在可以使用关键字 **match** 或 **access-list** 与 **capture interface asa_dataplane** 命令来过滤在 ASA CX 背板上捕获的数据包。 ASA CX 模块的特定控制流量不受访问列表或匹配过滤的影响； ASA 可以捕获所有控制流量。 在多情景模式下，按情景配置数据包捕获。请注意，在多情景模式下的所有控制流量仅流向系统执行空间。由于无法使用访问列表或匹配来过滤控制流量，因此这些选项在系统执行空间中不可用。 修改了以下命令：**capture interface asa_dataplane**。

ASA IPS 模块

本章介绍如何配置 ASA IPS 模块。ASA IPS 模块可能是硬件模块，也可能是软件模块，取决于 ASA 型号。有关每个 ASA 型号所支持的 ASA IPS 模块的列表，请参阅《*思科 ASA 兼容性矩阵*》：

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- 第 19-1 页上的有关 ASA IPS 模块的信息
- 第 19-5 页上的 ASA IPS 模块的许可要求
- 第 19-5 页上的准则和限制
- 第 19-6 页上的默认设置
- 第 19-6 页上的配置 ASA IPS 模块
- 第 19-16 页上的管理 ASA IPS 模块
- 第 19-20 页上的监控 ASA IPS 模块
- 第 19-21 页上的 ASA IPS 模块的配置示例
- 第 19-21 页上的 ASA IPS 模块的功能历史记录

有关 ASA IPS 模块的信息

ASA IPS 模块运行高级 IPS 软件，该软件提供主动、全面的入侵防御服务，可在蠕虫和网络病毒等恶意流量影响网络之前，及时将其拦截。

- 第 19-1 页上的 ASA IPS 模块如何与 ASA 配合使用
- 第 19-2 页上的操作模式
- 第 19-3 页上的使用虚拟传感器
- 第 19-4 页上的有关管理访问权的信息

ASA IPS 模块如何与 ASA 配合使用

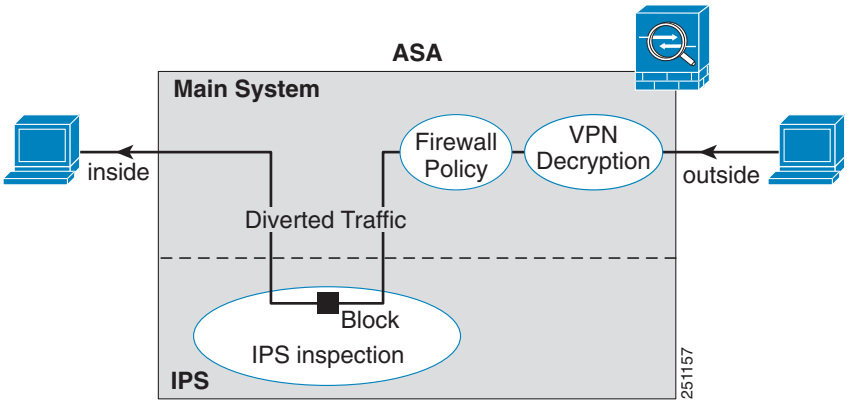
ASA IPS 模块从 ASA 运行独立应用。ASA IPS 模块可能包含外部管理接口，以便您直接连接至 ASA IPS 模块；如果它没有管理接口，则可通过 ASA 接口连接至 ASA IPS 模块。ASA 5585-X 上的 ASA IPS SSP 带有数据接口；这些接口为 ASA 提供了额外的端口密度。然而，ASA 的整体吞吐量不会增加。

流量先通过防火墙检查，然后再转发至 ASA IPS 模块。在确定要在 ASA 上接受 IPS 检测的流量之后，这些流量将按以下方式流经 ASA 和 ASA IPS 模块。**注意**：此示例适用于“内联模式”。请参阅第 19-2 页上的操作模式了解“混杂模式”的相关信息，在该模式下，ASA 仅向 ASA IPS 模块发送流量副本。

1. 流量进入 ASA。
2. 对传入的 VPN 流量解密。
3. 应用防火墙策略。
4. 流量发送至 ASA IPS 模块。
5. ASA IPS 模块向流量应用其安全策略，并采取相应的措施。
6. 有效流量发回 ASA； ASA IPS 模块可能会根据其安全策略阻止某些流量，被阻止的流量不会传递下去。
7. 对传出的 VPN 流量加密。
8. 流量退出 ASA。

图 19-1 展示了在内联模式下运行 ASA IPS 模块时的流量流。在此示例中，ASA IPS 模块将自动阻止其确定为攻击的流量。所有其他流量均通过 ASA 转发。

图 19-1　　ASA 中的 ASA IPS 模块流量流：内联模式

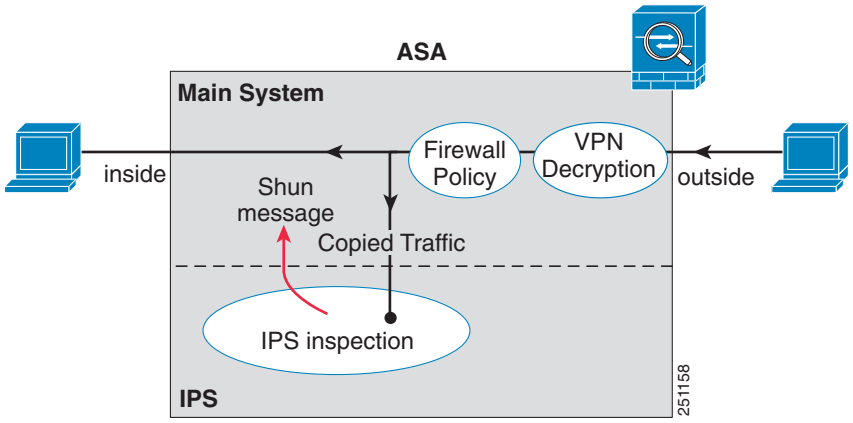


操作模式

可使用以下任一模式将流量发送到 ASA IPS 模块：

- 内联模式 - 此模式直接将 ASA IPS 模块置于流量流中（请参阅图 19-1）。对于已确定要接受 IPS 检测的流量，如果其未首先通过 ASA IPS 模块且由该模块进行检查，则该流量将无法继续通过 ASA。这种模式是最安全的，因为它先对确定要检测的每个数据包进行分析，然后才允许其通过。此外，ASA IPS 模块还可对数据包逐一实施阻止策略。不过，这种模式可能会影响吞吐量。
- 混杂模式 - 此模式会向 ASA IPS 模块发送流量流副本。其安全性较低，但对流量吞吐量几乎无影响。与内联模式不同的是，在混杂模式下，ASA IPS 模块只能通过指示 ASA 避开流量或重置 ASA 上的连接来阻止流量。此外，当 ASA IPS 模块分析流量时，可能会有少量 ASA IPS 模块来不及避开的流量通过 ASA。图 19-2 展示了混杂模式下的 ASA IPS 模块。在此示例中，ASA IPS 模块会针对其确定为威胁的流量向 ASA 发送避开消息。

图 19-2　　ASA 中的 ASA IPS 模块流量流：混杂模式



使用虚拟传感器

运行 IPS 软件 6.0 版及更高版本的 ASA IPS 模块可以运行多个虚拟传感器，这意味着可以在 ASA IPS 模块上配置多个安全策略。可将每个 ASA 安全情景或单模式 ASA 分配给一个或多个虚拟传感器，也可将多个安全情景分配给同一个虚拟传感器。请参阅 IPS 文档，了解有关虚拟传感器的详细信息，包括受支持的传感器最大数量。

图 19-3 展示了一个安全情景配备一个虚拟传感器（内联模式），而另外两个安全情景共用同一个虚拟传感器。

图 19-3　　安全情景和虚拟传感器

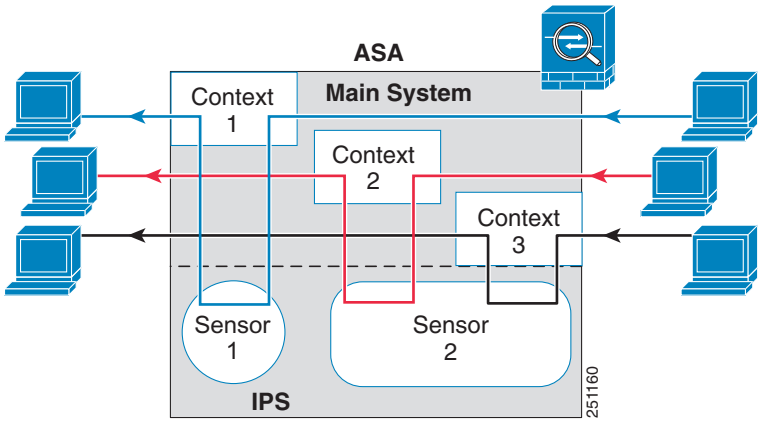
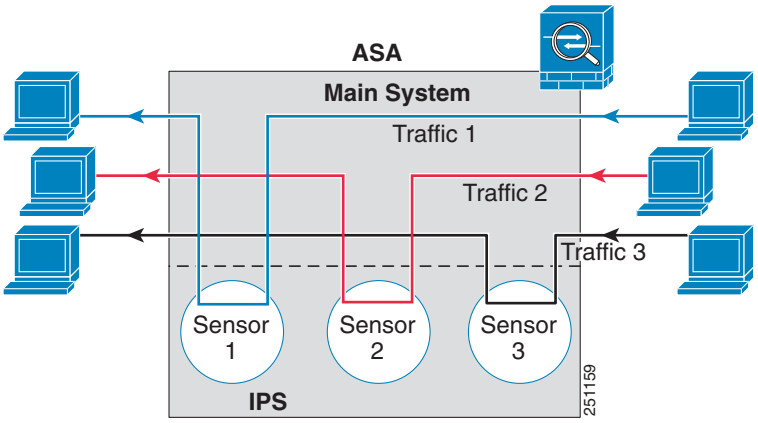


图 19-4 展示了一个单模式 ASA 配备多个虚拟传感器（内联模式）；各个已定义的流量流转至不同的传感器。

图 19-4　配备多个虚拟传感器的单模式 ASA



有关管理访问权的信息

可采用以下方法来管理 IPS 应用：

- 从 ASA 向模块发起会话 - 如果可以通过 CLI 访问 ASA，则可以向模块发起会话并访问模块 CLI。请参阅第 19-10 页上的从 ASA 向模块发起会话。
- 使用 ASDM 或 SSH 连接至 IPS 管理接口 - 从 ASA 启动 ASDM 之后，管理站将连接至该模块管理接口以配置 IPS 应用。对于 SSH，可在该模块管理接口上直接访问模块 CLI。（需要在模块应用中进行额外配置才能执行 Telnet 访问）。该模块管理接口还可用于发送系统日志消息或允许进行模块应用更新，如签名数据库更新。

请参阅有关该管理接口的以下信息：

  - ASA 5585-X - IPS 管理接口是一个独立的外部千兆以太网接口。
  - ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X - 这些型号将 ASA IPS 模块作为软件模块运行。IPS 管理接口与 ASA 共用管理 0/0 接口。ASA 和 ASA IPS 模块分别支持不同的 MAC 地址和 IP 地址。IPS IP 地址的配置必须在 IPS 操作系统内进行（使用 CLI 或 ASDM）。但是，物理特性（例如启用接口）在 ASA 上配置。可移除 ASA 接口配置（特别是接口名称），以便将此接口专门用作纯 IPS 接口。此接口仅用于管理。

ASA IPS 模块的许可要求

下表显示此功能的许可要求：

型号	许可证要求
ASA 5512-X、 ASA 5515-X、 ASA 5525-X、 ASA 5545-X、 ASA 5555-X	IPS 模块许可证。 **注**　IPS 模块许可证可用于在 ASA 上运行 IPS 软件模块。还必须另行购买 IPS 签名订用；要实现故障转移，请为每个设备购买一个订用。要获得 IPS 签名支持，必须购买预装有 IPS 的 ASA（部件号必须包含 “IPS”）。组合的故障转移集群许可证不允许将非 IPS 设备与 IPS 设备配对。例如，如果购买了 ASA 5515-X 的 IPS 版本（部件号 ASA5515-IPS-K9），并试图与非 IPS 版本（部件号 ASA5515-K9）配成故障转移对，则将无法获取 ASA5515-K9 设备的 IPS 签名更新，即使它从其他设备继承了 IPS 模块许可证也是如此。
ASA 5585-X	基础许可证。
所有其他型号	不支持。

准则和限制

此节包括该功能的指导原则和限制。

型号准则

- 请参阅《*思科 ASA 兼容性矩阵*》，了解有关哪些型号支持哪些模块的信息：
  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

其他准则

- ASA 与 IPS 模块的吞吐量之和小于 ASA 单独一项的吞吐量。
  - ASA 5512-X 至 ASA 5555-X - 请参阅 http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-700608.html
  - ASA 5585-X - 请参阅 http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-617018.html
- 无法更改模块上安装的软件类型；如已购买 ASA IPS 模块，则以后无法在该模块上安装其他软件。

默认设置

表 19-1 列出了 ASA IPS 模块的默认设置。

表 19-1　默认网络参数

参数	默认
管理 IP 地址	192.168.1.2/24
网关	192.168.1.1/24（默认 ASA 管理 IP 地址）
用户名	cisco
密码	cisco

注　ASA 上的默认管理 IP 地址是 192.168.1.1/24。

配置 ASA IPS 模块

本节介绍如何配置 ASA IPS 模块。

- 第 19-6 页上的 ASA IPS 模块的任务流
- 第 19-7 页上的连接 ASA IPS 管理接口
- 第 19-10 页上的从 ASA 向模块发起会话
- 第 19-11 页上的配置基本 IPS 模块网络设置
- 第 19-11 页上的（ASA 5512-X 至 ASA 5555-X）启动软件模块
- 第 19-12 页上的配置 ASA IPS 模块上的安全策略
- 第 19-13 页上的向安全情景分配虚拟传感器
- 第 19-14 页上的将流量转移至 ASA IPS 模块

ASA IPS 模块的任务流

ASA IPS 模块的配置过程包括：在 ASA IPS 模块上配置 IPS 安全策略，然后将 ASA 配置为将流量发送至 ASA IPS 模块。要配置 ASA IPS 模块，请执行下列步骤：

步骤 1　为 ASA IPS 管理接口布线。请参阅第 19-7 页上的连接 ASA IPS 管理接口。

步骤 2　向模块发起会话。找到背板上方的 IPS CLI。请参阅第 19-10 页上的从 ASA 向模块发起会话。

步骤 3　（ASA 5512-X 至 ASA 5555-X；可能需要）安装软件模块。请参阅第 19-11 页上的（ASA 5512-X 至 ASA 5555-X）启动软件模块。

步骤 4　ASA 为 IPS 模块配置基本网络设置。请参阅第 19-11 页上的配置基本 IPS 模块网络设置。

步骤 5　在模块上配置检测和保护策略，该策略用于确定流量检查方式以及检测到入侵时应执行的操作。请参阅第 19-12 页上的配置 ASA IPS 模块上的安全策略。

步骤 6　（可选）在处于多情景模式的 ASA 上，指定可用于每个情景的 IPS 虚拟传感器（如果配置了虚拟传感器）。请参阅第 19-13 页上的向安全情景分配虚拟传感器。

步骤 7　在 ASA 上，确定要转移到 ASA IPS 模块的流量。请参阅第 19-14 页上的将流量转移至 ASA IPS 模块。

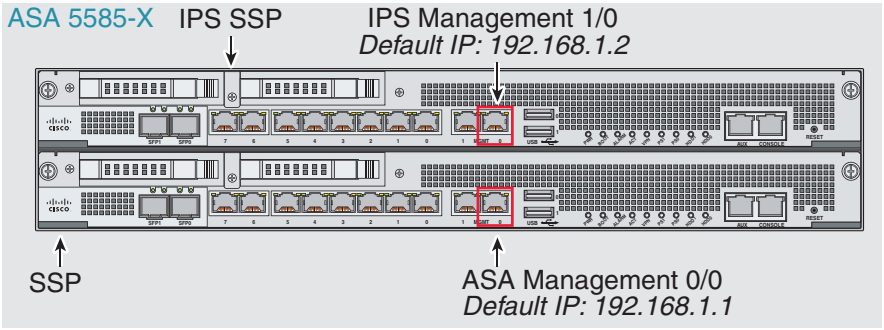
连接 ASA IPS 管理接口

除了提供对 IPS 模块的管理访问权，IPS 管理接口还需要访问 HTTP 代理服务器或 DNS 服务器和互联网，以便下载全局相关性、签名更新和许可证请求。本节描述推荐的网络配置。您的网络可能不同。

- 第 19-7 页上的 ASA 5585-X（硬件模块）
- 第 19-8 页上的 ASA 5512-X 至 ASA 5555-X（软件模块）

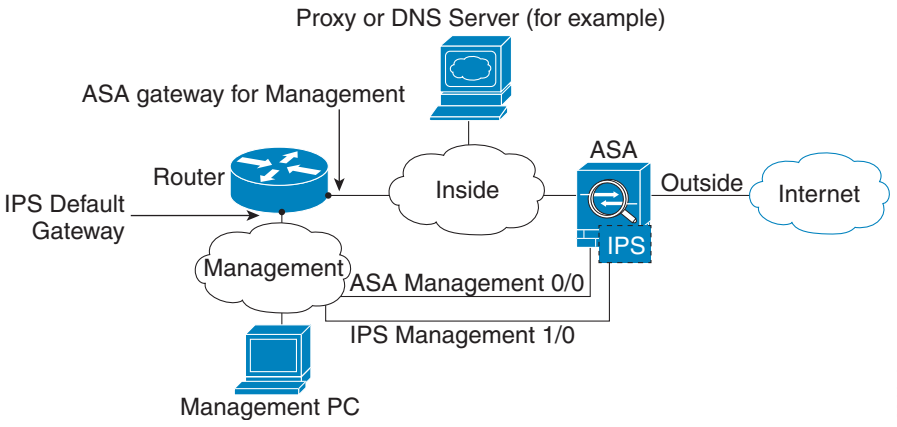
ASA 5585-X（硬件模块）

IPS 模块包括一个独立于 ASA 的管理接口。



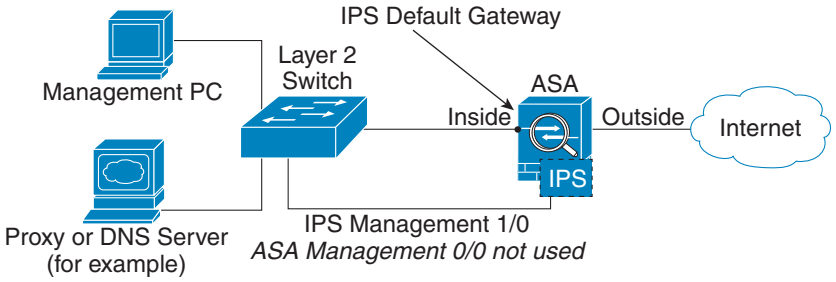
如果有内部路由器

如果有内部路由器，则可在管理网络（可能同时包括 ASA 管理 0/0 接口和 IPS 管理 1/0 接口）与 ASA 内部网络之间路由。另外，务必在 ASA 上添加一个路由，以便通过内部路由器访问管理网络。



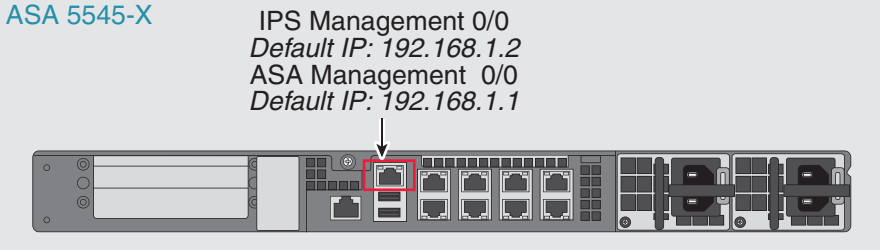
如果没有内部路由器

如果只有一个内部网络，您就无法拥有一个单独管理网络，这需要内部路由器实现网络之间的路由。在这种情况下，可从内部接口而非管理 0/0 接口管理 ASA。由于 IPS 模块是独立于 ASA 的设备，因此，可将 IPS 管理 1/0 地址配置为位于内部接口所在的网络上。



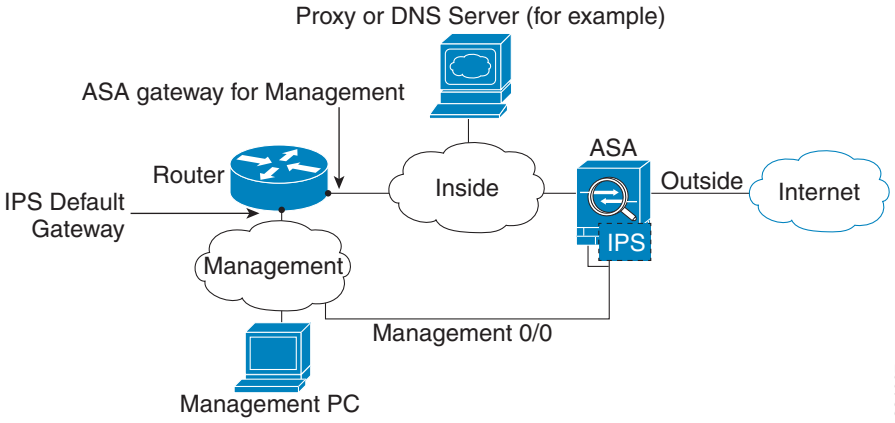
ASA 5512-X 至 ASA 5555-X（软件模块）

这些型号将 IPS 模块作为软件模块运行，并且 IPS 管理接口与 ASA 共用管理 0/0 接口。



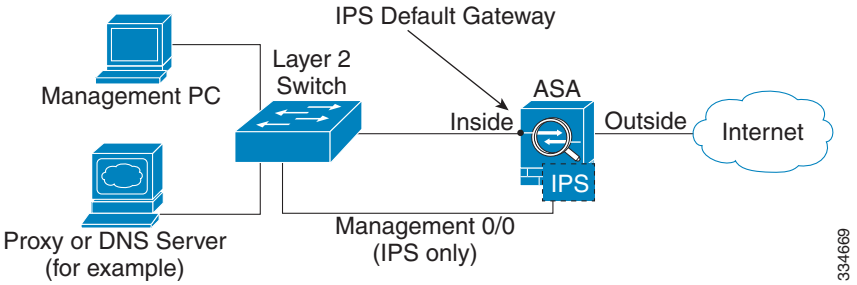
如果有内部路由器

如果有内部路由器，则可在管理 0/0 网络（同时包括 ASA 和 IPS 管理 IP 地址）与内部网络之间路由。另外，务必在 ASA 上添加一个路由，以便通过内部路由器访问管理网络。



如果没有内部路由器

如果只有一个内部网络，您就无法拥有一个单独的管理网络。在这种情况下，可从内部接口而非管理 0/0 接口管理 ASA。即使从管理 0/0 接口移除 ASA 配置的名称，仍可配置该接口的 IPS IP 地址。由于 IPS 模块本质上是独立于 ASA 的设备，因此，*可*将 IPS 管理地址配置为位于内部接口所在的网络上。



注　必须为管理 0/0 接口移除 ASA 配置的名称；如果该名称是在 ASA 上配置的，则 IPS 地址必须位于 ASA 所在的网络上，这其中不包括已在其他 ASA 接口上配置的任何网络。如未配置名称，则 IPS 地址可能位于任何网络上，例如，ASA 内部网络。

后续操作

- 配置基本网络设置。请参阅第 19-11 页上的配置基本 IPS 模块网络设置。

从 ASA 向模块发起会话

要从 ASA 访问 IPS 模块 CLI，可从 ASA 发起会话。对于软件模块，可向模块发起会话（使用 Telnet），也可创建虚拟控制台会话。如果控制面板已关闭且无法建立 Telnet 会话，则控制台会话可能有用。

详细步骤

命令	用途

Telnet 会话。
对于硬件模块（例如，ASA 5585-X）：
session 1
对于软件模块（例如，ASA 5545-X）：
session ips
 	
示例：
`hostname# session 1`
 	
`Opening command session with slot 1.`
`Connected to slot 1.Escape character sequence is 'CTRL-^X'.`
 	
`sensor login: cisco`
`Password: cisco`
	使用 Telnet 访问模块。系统会提示输入用户名和密码。默认用户名是 **cisco**，默认密码是 **cisco**。
	注　首次登录模块时，系统将提示更改默认密码。密码长度必须至少为八个字符，并且不能使用词典中的单词。

控制台会话（仅限软件模块）。
session ips console
 	
示例：
`hostname# session ips console`
 	
`Establishing console session with slot 1`
`Opening console session with module ips.`
`Connected to module ips.Escape character sequence is 'CTRL-SHIFT-6 then x'.`
 	
`sensor login: cisco`
`Password: cisco`
	访问模块控制台。系统会提示输入用户名和密码。默认用户名是 **cisco**，默认密码是 **cisco**。
	注　请勿将此命令与终端服务器结合使用，其中 **Ctrl-Shift-6, x** 是用于返回到终端服务器提示符的转义序列。**Ctrl-Shift-6, x** 序列也用于对 IPS 控制台转义并返回至 ASA 提示符。因此，如果在此情况下尝试退出 IPS 控制台，反而会一直退回至终端服务器提示符。如将终端服务器重新连接至 ASA，则 IPS 控制台会话仍然会处于活动状态；您将永远无法退回至 ASA 提示符。必须使用直接串行连接才能将控制台返回至 ASA 提示符。
	
	改用 **session ips** 命令。

（ASA 5512-X 至 ASA 5555-X）启动软件模块

ASA 通常附带的 IPS 模块软件位于 Disk0 上。如果模块未运行，或要向现有 ASA 添加 IPS 模块，则必须启动模块软件。如果不确定模块是否在运行，且无法向其发起会话。

详细步骤

步骤 1　执行以下操作之一：

- 预装有 IPS 的新 ASA - 要查看闪存中的 IPS 模块软件文件名，请输入：。

  ```
  hostname# dir disk0:
  ```

  例如，查找与 IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip 类似的文件名。请记下该文件名；在后续操作步骤中将用到该文件名。

- 新装有 IPS 的现有 ASA - 从 Cisco.com 将 IPS 软件下载至 TFTP 服务器。如有 Cisco.com 登录名，则可从以下网站获取该软件：

  http://www.cisco.com/cisco/software/navigator.html?mdfid=282164240

  将软件复制至 ASA：

  ```
  hostname# copy tftp://server/file_path disk0:/file_path
  ```

  有关其他下载服务器类型，请参阅常规操作配置指南。

  请记下该文件名；在后续操作步骤中将用到该文件名。

步骤 2　要设置 IPS 模块软件在 disk0 中的位置，请输入以下命令，：

```
hostname# sw-module module ips recover configure image disk0:file_path
```

例如，使用第 1 步的示例中的文件名，输入：

```
hostname# sw-module module ips recover configure image
disk0:IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip
```

步骤 3　要安装并加载 IPS 模块软件，请输入以下命令，：

```
hostname# sw-module module ips recover boot
```

步骤 4　要检查映像传输和模块重启过程的进度，请输入以下命令，：

```
hostname# show module ips details
```

输出中的 Status 字段表示模块的运行状态。正在运行的模块通常显示状态 “Up”。当 ASA 向模块传输应用映像时，输出中的 Status 字段显示 “Recover”。当 ASA 完成映像传输并重启模块时，新传输的映像正在运行。

配置基本 IPS 模块网络设置

会话，并使用 **setup** 命令配置基本设置。

注　（ASA 5512-X 至 ASA 5555-X）如果无法向模块发起会话，则表示 IPS 模块未运行。请参阅第 19-11 页上的（ASA 5512-X 至 ASA 5555-X）启动软件模块，然后在安装模块后重复此操作步骤。

详细步骤

	命令	用途
步骤 1	按照第 19-10 页上的从 ASA 向模块发起会话向 IPS 模块发起会话。	
步骤 2	**设置** **示例：** `sensor# setup`	运行设置实用程序对 ASA IPS 模块进行初始配置。系统将提示您输入基本设置。对于默认网关，请指定上游路由器的 IP 地址。请参阅第 19-7 页上的连接 ASA IPS 管理接口了解网络要求。ASA 管理 IP 地址的默认设置将不起作用。

配置 ASA IPS 模块上的安全策略

本节介绍如何配置 ASA IPS 模块应用。

详细步骤

步骤 1　使用以下任一方法访问 ASA IPS 模块 CLI：

- 从 ASA 向 ASA IPS 模块发起会话。请参阅第 19-10 页上的从 ASA 向模块发起会话。
- 使用 SSH 连接至 IPS 管理接口。未更改过的默认管理 IP 地址为 192.168.1.2。默认用户名是 **cisco**，默认密码是 **cisco**。有关管理接口的详细信息，请参阅第 19-4 页上的有关管理访问权的信息。

步骤 2　按照 IPS 文档配置 IPS 安全策略。

要访问与 IPS 相关的所有文档，请转至：
http://www.cisco.com/c/en/us/support/security/ips-4200-series-sensors/products-documentation-roadmaps-list.html

步骤 3　如已配置虚拟传感器，则需将其中一个传感器确定为默认传感器。如果 ASA 未在其配置中指定虚拟传感器名称，则使用默认传感器。

步骤 4　完成 ASA IPS 模块配置之后，请输入以下命令以退出 IPS 软件：

```
sensor# exit
```

如已从 ASA 向 ASA IPS 模块发起会话，则您将返回至 ASA 提示符。

后续操作

- 有关多情景模式下的 ASA，请参阅第 19-13 页上的向安全情景分配虚拟传感器。
- 有关单情景模式下的 ASA，请参阅第 19-14 页上的将流量转移至 ASA IPS 模块。

向安全情景分配虚拟传感器

如果 ASA 处于多情景模式，则可向每个情景分配一个或多个 IPS 虚拟传感器。然后，在将该情景配置为将流量发送至 ASA IPS 模块时，可指定分配给该情景的传感器；不能指定未分配给该情景的传感器。如未向某个情景分配任何传感器，则使用 ASA IPS 模块上配置的默认传感器。可将同一个传感器分配至多个情景。

注　使用虚拟传感器并不一定要处于多情景模式；在单模式下也可将不同的传感器用于不同的流量流。

先决条件

有关配置情景的详细信息，请参阅常规操作配置指南。

详细步骤

	命令	用途

步骤 1	**context** *name*
	
	示例：
	`hostname(config)# context admin`
	`hostname(config-ctx)#`
		确定要配置的情景。在系统执行空间中输入此命令。

步骤 2	**allocate-ips** *sensor_name* [*mapped_name*] [**default**] **示例：** `hostname(config-ctx)# allocate-ips sensor1 highsec`	为要分配给该情景的每个传感器输入此命令。 *sensor _name* 参数是 ASA IPS 模块上配置的传感器名称。要查看 ASA IPS 模块上配置的传感器，请输入 **allocate-ips ?**。系统将列出所有可用传感器。也可输入 **show ips** 命令。在系统执行空间中，**show ips** 命令将列出所有可用传感器；如果在情景中输入该命令，则将显示已分配给该情景的传感器。如果指定的传感器名称在 ASA IPS 模块上尚不存在，则将收到一个错误，但仍然按原样输入 **allocate-ips** 命令。如果不在 ASA IPS 模块上以该名称创建一个传感器，该情景会一直假定该传感器已关闭。 将 *mapped_name* 参数用作可用于情景中传感器名称（而非实际传感器名称）的别名。如未指定映射名称，则在情景中使用传感器名称。为安全起见，您可能不想让情景管理员知道该情景所使用的传感器。或者，您可能想让情景配置一般化。例如，如果希望所有情景都使用名为 “sensor1” 和 “sensor2” 的传感器，则可在情景 A 中将 “highsec” 和 “lowsec” 传感器映射至 sensor1 和 sensor2，但在情景 B 中将 “medsec” 和 “lowsec” 传感器映射至 sensor1 和 sensor2。 **default** 关键字会为每个情景设置一个传感器作为默认传感器；如果情景配置未指定传感器名称，则该情景将使用此默认传感器。每个情景只能配置一个默认传感器。如要更改默认传感器，请输入 **no allocate-ips** *sensor_name* 命令以移除当前默认传感器，然后再分配新的默认传感器。如果未指定传感器作为默认传感器，并且情景配置不包含传感器名称，则流量使用 ASA IPS 模块上指定的默认传感器。

	命令	用途

步骤 3	**changeto context** *context_name*
	
	示例：
	`hostname# changeto context customer1`
	`hostname/customer1#`
		切换至该情景，以便按第 19-14 页上的将流量转移至 ASA IPS 模块中所述配置 IPS 安全策略。

示例

以下示例将 sensor1 和 sensor2 分配至情景 A，将 sensor1 和 sensor3 分配至情景 B。这两个情景都将传感器名称映射为 “ips1” 和 “ips2”。在情景 A 中，sensor1 设置为默认传感器，但在情景 B 中，未设置默认传感器，因此使用 ASA IPS 模块上配置的默认传感器。

```
hostname(config-ctx)# context A
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1 default
hostname(config-ctx)# allocate-ips sensor2 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1
hostname(config-ctx)# allocate-ips sensor3 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver

hostname(config-ctx)# changeto context A
...
```

后续操作

切换至每个情景，以按第 19-14 页上的将流量转移至 ASA IPS 模块中所述配置 IPS 安全策略。

将流量转移至 ASA IPS 模块

本节确定要从 ASA 转移至 ASA IPS 模块的流量。

先决条件

在多情景模式下，在每个情景执行空间中执行以下步骤。要切换至某个情景，请在 Configuration > Device List 窗格中输入 **changeto context** *context_name* 命令。

详细步骤

	命令	用途
步骤 1	**class-map** *name* **示例：** `hostname(config)# class-map ips_class`	创建类映射以确定要为其发送至 ASA IPS 模块的流量。 如果要将多个流量类发送至 ASA IPS 模块，则可创建多个类映射以用于安全策略。
步骤 2	**match** *parameter* **示例：** `hostname(config-cmap)# match access-list ips_traffic`	指定类映射中的流量。有关详细信息，请参阅第 1-12 页上的识别流量（第 3/4 层类映射）。
步骤 3	**policy-map** *name* **示例：** `hostname(config)# policy-map ips_policy`	添加或编辑策略映射，以设置要对类映射流量执行的操作。
步骤 4	**class** *name* **示例：** `hostname(config-pmap)# class ips_class`	确定在步骤 1 中创建的类映射。
步骤 5	**ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}] **示例：** `hostname(config-pmap-c)# ips promiscuous fail-close`	指定应发送至 ASA IPS 模块的流量。 **inline** 和 **promiscuous** 关键字控制 ASA IPS 模块的操作模式。有关更多详细信息，请参阅第 19-2 页上的操作模式。 **fail-close** 关键字将 ASA 设置为在 ASA IPS 模块不可用时阻止所有流量。 **fail-open** 关键字将 ASA 设置为在 ASA IPS 模块不可用时允许所有流量在未经检查的情况下通过。 如果使用虚拟传感器，则可使用 **sensor** *sensor_name* 参数指定传感器名称。要查看可用的传感器名称，请输入 **ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} **sensor ?** 命令。系统将列出可用传感器。也可使用 **show ips** 命令。如果在 ASA 上使用多情景模式，则只能指定已分配给该情景的传感器（请参阅第 19-13 页上的向安全情景分配虚拟传感器）。如果在情景中配置了 *mapped_name*，则使用该名称。如未指定传感器名称，则流量将使用默认传感器。在多情景模式下，可为情景指定默认传感器。在单模式下，或者，如在多模式下未指定默认传感器，则流量将使用 ASA IPS 模块上设置的默认传感器。如果输入的名称在 ASA IPS 模块上尚不存在，则将收到一个错误，并且该命令将被拒。

	命令	用途
步骤 6	（可选） **class** *name2* **示例：** hostname(config-pmap)# class ips_class2	如为 IPS 流量创建了多个类映射，则可为该策略指定另一个类。 有关策略映射内类顺序的重要性的详细信息，请参阅第 1-5 页上的服务策略内的功能匹配。同一操作类型的流量无法匹配多个类映射；因此，如果希望网络 A 转到 sensorA，但希望其他所有流量都转到 sensorB，则需要先对网络 A 输入 **class** 命令，再对所有流量输入 **class** 命令；否则，所有流量（包括网络 A）都将与第一个 **class** 命令匹配，从而发送至 sensorB。
步骤 7	（可选） **ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}] **示例：** hostname(config-pmap-c)# ips promiscuous fail-close	指定应发送至 ASA IPS 模块的第二类流量。 重复以上步骤，按需尽量多地添加类。
步骤 8	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **示例：** hostname(config)# service-policy tcp_bypass_policy outside	在一个或多个接口上激活策略映射。**global** 可以将策略映射应用到所有接口，**interface** 可以将策略应用到某个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

管理 ASA IPS 模块

本节包括的操作步骤有助于恢复模块或排除模块的故障。

- 第 19-16 页上的安装并启动模块上的映像
- 第 19-18 页上的关闭模块
- 第 19-18 页上的卸载软件模块映像
- 第 19-19 页上的重置密码
- 第 19-19 页上的重新加载或重置模块

安装并启动模块上的映像

如果模块出现故障，并且模块应用映像无法运行，则可从 TFTP 服务器（针对硬件模块）或本地磁盘（软件模块）在模块上重新安装新映像。

注　请勿在模块软件中使用 **upgrade** 命令来安装映像。

先决条件

- 硬件模块 - 确保所指定的 TFTP 服务器可传输最大 60 MB 的文件。

  注　此过程可能约需 15 分钟左右才能完成，具体取决于网络和映像大小。

- 软件模块 - 先将映像复制至 ASA 内部闪存 (disk0)，然后再完成此操作步骤。

  注　在将 IPS 软件下载至 disk0 之前，请确保至少有 50% 的可用闪存。安装 IPS 时，IPS 会为其文件系统保留 50% 的内部闪存。

详细步骤

	命令	用途

步骤 1	对于硬件模块（例如，ASA 5585-X）：
	hw-module module 1 recover configure
	对于软件模块（例如，ASA 5545-X）：
	sw-module module ips recover configure image disk0:*file_path*
	示例：
	`hostname# hw-module module 1 recover configure`
	`Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg`
	`Port IP Address [127.0.0.2]: 10.1.2.10`
	`Port Mask [255.255.255.254]: 255.255.255.0`
	`Gateway IP Address [1.1.2.10]: 10.1.2.254`
	`VLAN ID [0]: 100`
		指定新映像的位置。
		对于硬件模块 - 此命令将提示您输入 TFTP 服务器的 URL、管理接口 IP 地址和子网掩码以及网关地址。这些网络参数将在 ROMMON 中配置；模块应用配置中配置的网络参数不可用于 ROMMON，因此，必须在此处单独设置。
		对于软件模块 - 指定映像在本地磁盘上的位置。
		可使用 **show module {1 | ips} recover** 命令查看恢复配置。
		在多情景模式下，在系统执行空间中输入此命令。

步骤 2	对于硬件模块： **hw-module module 1 recover boot** 对于软件模块： **sw-module module ips recover boot** **示例：** `hostname# hw-module module 1 recover boot`	安装并启动 IPS 模块软件。
步骤 3	对于硬件模块： **show module 1 details** 对于软件模块： **show module ips details** **示例：** `hostname# show module 1 details`	检查映像传输和模块重启进程的进度。 输出中的 Status 字段表示模块的运行状态。正在运行的模块通常显示状态 “Up”。当 ASA 向模块传输应用映像时，输出中的 Status 字段显示 “Recover”。当 ASA 完成映像传输并重启模块时，新传输的映像正在运行。

关闭模块

通过关闭模块软件，可让模块做好准备，在不丢失配置数据的情况下安全断电。**注意**：如果重新加载 ASA，模块不会自动关闭，因此，建议在重新加载 ASA 之前，先关闭模块。要正常关闭模块，请在 ASA CLI 处执行下列步骤。

详细步骤

命令	用途
对于硬件模块（例如，ASA 5585-X）： **hw-module module 1 shutdown** 对于软件模块（例如，ASA 5545-X）： **sw-module module ips shutdown** **示例：** `hostname# hw-module module 1 shutdown`	关闭模块。

卸载软件模块映像

要卸载软件模块映像和关联配置，请执行下列步骤。

详细步骤

	命令	用途

步骤 1	**sw-module module ips uninstall**
	示例：
	`hostname# sw-module module ips uninstall`
	`Module ips will be uninstalled.This will completely remove the`
	`disk image associated with the sw-module including any configuration`
	`that existed within it.`
	`Uninstall module <id>?[confirm]`
		永久卸载软件模块映像及关联配置。

步骤 2	**reload** **示例：** `hostname# reload`	重新加载 ASA。必须先重新加载 ASA，然后才能安装新模块类型。

重置密码

可将模块密码重置为默认值。对于用户 **cisco**，默认密码为 **cisco**。重置密码后，应使用模块应用将其更改为一个唯一值。

重置模块密码将导致模块重新启动。重启模块时，服务不可用。

要将模块密码重置为默认值 cisco，请执行下列步骤。

详细步骤

命令	用途
对于硬件模块（例如，ASA 5585-X）： **hw-module module 1 password-reset** 对于软件模块（例如，ASA 5545-X）： **sw-module module ips password-reset** **示例：** `hostname# hw-module module 1 password-reset`	将用户 **cisco** 的模块密码重置为 **cisco**。

重新加载或重置模块

要重新加载或重置模块，请在 ASA CLI 处输入以下任一命令。

详细步骤

命令	用途
对于硬件模块（例如，ASA 5585-X）： **hw-module module 1 reload** 对于软件模块（例如，ASA 5545-X）： **sw-module module ips reload** **示例：** `hostname# hw-module module 1 reload`	重新加载模块软件。
对于硬件模块： **hw-module module 1 reset** 对于软件模块： **sw-module module ips reset** **示例：** `hostname# hw-module module 1 reset`	执行重置，然后重新加载模块。

监控 ASA IPS 模块

要检查模块状态，请输入以下命令之一：

命令	用途
show module	显示状态。
show module {**1** | **ips**} **details**	显示其他状态信息。为硬件模块指定 **1**，为软件模块指定 **ips**。
show module {**1** | **ips**} **recover**	显示用于向模块传输映像的网络参数。为硬件模块指定 **1**，为软件模块指定 **ips**。

示例

以下是 **show module details** 命令的输出示例，其中提供了装有 SSC 的 ASA 的附加信息：

```
hostname# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Card-5
Hardware version: 0.1
Serial Number: JAB11370240
Firmware version: 1.0(14)3
Software version: 6.2(1)E2
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App.Name: IPS
App.Status: Up
App.Status Desc: Not Applicable
App.Version: 6.2(1)E2
Data plane Status: Up
Status: Up
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
Mgmt Gateway: 209.165.201.30
Mgmt Access List: 209.165.201.31/32
                  209.165.202.158/32
                  209.165.200.254/24
Mgmt Vlan: 20
```

以下是对装有 IPS SSP 软件模块的 ASA 5525-X 执行 **show module ips** 命令后的输出示例：

```
hostname# show module ips
Mod Card Type                                    Model           Serial No.
--- -------------------------------------------- ------------------------------
ips IPS 5525 Intrusion Protection System         IPS5525         FCH1504V03P

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ---------------------------
ips 503d.e59c.6f89 to 503d.e59c.6f89  N/A          N/A          7.1(1.160)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ----------------------------------------
ips IPS                            Up               7.1(1.160)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
ips Up                 Up

Mod License Name      License Status  Time Remaining
--- ----------------- --------------- ---------------
ips IPS Module        Enabled         7 days
```

ASA IPS 模块的配置示例

以下示例在混杂模式下将所有 IP 流量转移至 ASA IPS 模块，并在 ASA IPS 模块卡因任何原因出现故障时阻止所有 IP 流量：

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

以下示例在内联模式下将本该转入 10.1.1.0 网络和 10.2.1.0 网络的所有 IP 流量都转移至 AIP SSM，并在 AIP SSM 因任何原因出现故障的情况下允许所有流量通过。对于 my-ips-class 流量，使用 sensor1 ；对于 my-ips-class2 流量，使用 sensor2。

```
hostname(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list my-ips-acl
hostname(config)# class-map my-ips-class2
hostname(config-cmap)# match access-list my-ips-acl2
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-open sensor sensor1
hostname(config-pmap)# class my-ips-class2
hostname(config-pmap-c)# ips inline fail-open sensor sensor2
hostname(config-pmap-c)# service-policy my-ips-policy interface outside
```

ASA IPS 模块的功能历史记录

表 19-2 列出了各项功能变更以及实施了该变更的平台版本。

表 19-2　ASA IPS 模块的功能历史记录

功能名称	平台版本	功能信息
AIP SSM	7.0(1)	我们为 ASA 5510、5520 和 5540 引入了对 AIP SSM 的支持。 引入了以下命令：**ips**。
虚拟传感器（ASA 5510 及更高版本）	8.0(2)	引入了虚拟传感器支持。借助于虚拟传感器，可在 ASA IPS 模块上配置多个安全策略。 引入了以下命令：**allocate-ips**。
适用于 ASA 5505 的 AIP SSC	8.2(1)	我们为 ASA 5505 引入了对 AIP SSC 的支持。 引入了以下命令：**allow-ssc-mgmt**、**hw-module module ip** 和 **hw-module module allow-ip**。

表 19-2　ASA IPS 模块的功能历史记录（续）

功能名称	平台版本	功能信息
对适用于 ASA 5585-X 的 ASA IPS SSP-10、-20、-40 和 -60 的支持	8.2(5)/ 8.4(2)	我们为 ASA 5585-X 引入了对 ASA IPS SSP-10、-20、-40 和 -60 的支持。只能安装带有匹配级别 SSP 的 ASA IPS SSP；例如，SSP-10 和 ASA IPS SSP-10。 **注**　8.3 版本不支持 ASA 5585-X。
对适用于 SSP-40 和 SSP-60 的双 SSP 的支持	8.4(2)	对于 SSP-40 和 SSP-60，可在同一机箱中使用两个相同级别的 SSP。不支持级别混合的 SSP（例如，不支持混合使用 SSP-40 和 SSP-60）。每个 SSP 均可充当具有独立配置并进行独立管理的独立设备。如果需要，可使用两个 SSP 作为故障转移对。 **注**　在机箱中使用两个 SSP 时，VPN 不受支持；然而，请注意，尚未禁用 VPN。 我们修改了以下命令：**show module**、**show inventory**、**show environment**。
对适用于 ASA 5512-X 至 ASA 5555-X 的 ASA IPS SSP 的支持	8.6(1)	我们为 ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 引入了对 ASA IPS SSP 软件模块的支持。 我们引入或修改了以下命令：**session**、**show module**、**sw-module**。