思科 ASA 系列常规操作 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

思科系统公司
www.cisco.com

思科在全球设有 200 多个办事处。
地址、电话号码和传真号
列出在思科网站上，地址为
www.cisco.com/go/offices。

文本部分号：不适用，仅供在线使用

思科 ASA 系列常规操作 CLI 配置指南

目 录

关于本指南 xxix

文档目标 xxix

相关文档 xxix

约定 xxix

获取文档和提交服务请求 xxx

第 1 部分 ASA 使用入门

第 1 章 思科 ASA 简介 1-1

硬件和软件兼容性 1-1

VPN 兼容性 1-1

新功能 1-2

ASA 9.3(1) 版本的新功能 1-2

ASA 服务模块如何与交换机配合使用 1-5

防火墙功能概述 1-7

安全策略概述 1-8

防火墙模式概述 1-10

状态检测概述 1-10

VPN 功能概述 1-11

安全情景概述 1-11

ASA 集群概述 1-12

特殊的服务和传统服务 1-12

特殊服务指南 1-12

传统服务指南 1-12

第 2 章 入门 2-1

访问命令行界面的控制台 2-1

访问设备控制台 2-1

访问 ASA 服务模块控制台 2-2

配置 ASDM 访问 2-6

使用出厂默认配置进行 ASDM 访问 （设备、 ASAv） 2-6

为设备和 ASAv 自定义 ASDM 访问 2-7

为 ASA 服务模块配置 ASDM 访问 2-9

启动 ASDM 2-11
出厂默认配置 2-12
还原出厂默认配置 2-12
还原 ASAv 部署配置 2-13
ASA 设备默认配置 2-14
ASAv 部署配置 2-14
处理配置 2-15
保存配置更改 2-15
将启动配置复制到运行配置 2-17
查看配置 2-17
清除和移除配置设置 2-18
离线创建文本配置文件 2-18
将配置更改应用于连接 2-19
重新加载 ASA 2-19

第 3 章 **适用于思科 ASA 服务模块的交换机配置 3-1**
有关交换机的信息 3-1
受支持的交换机硬件和软件 3-1
背板连接 3-2
ASA 与思科 IOS 之间的功能交互 3-2
有关 SVI 的信息 3-2
准则和限制 3-3
验证模块安装 3-4
将 VLAN 分配给 ASA 服务模块 3-5
将 MSFC 用作直连路由器 (SVI) 3-7
为 ASA 故障转移配置交换机 3-8
将 VLAN 分配给辅助 ASA 服务模块 3-8
在主要交换机与辅助交换机之间添加中继 3-8
确保与透明防火墙模式的兼容性 3-8
启用自动状态消息以进行快速链路故障检测 3-9
重置 ASA 服务模块 3-9
监控 ASA 服务模块 3-10
与 ASA 服务模块配合使用的交换机的功能历史记录 3-12

第 4 章 **功能许可证 4-1**
每个型号的受支持功能许可证 4-1
每个型号的许可证 4-1
许可证说明 4-14

VPN 许可证和功能兼容性 4-18
有关功能许可证的信息 4-18
预安装的许可证 4-19
永久许可证 4-19
基于时间的许可证 4-19
共享 AnyConnect Premium 许可证 4-21
故障转移或 ASA 集群许可证 4-24
无负载加密型号 4-26
许可证常见问题 4-27
准则和限制 4-27
配置许可证 4-28
获取激活密钥 4-29
激活和停用密钥 4-29
配置共享许可证 4-31
监控许可证 4-34
查看您的当前许可证 4-34
监控共享许可证 4-44
许可的功能历史记录 4-45

第 5 章 透明或路由防火墙模式 5-1
有关防火墙模式的信息 5-1
有关路由防火墙模式的信息 5-1
有关透明防火墙模式的信息 5-2
防火墙模式的许可要求 5-6
默认设置 5-6
准则和限制 5-6
设置防火墙模式 5-8
为透明防火墙配置 ARP 检测 5-8
配置 ARP 检测的任务流程 5-8
添加静态 ARP 条目 5-9
启用 ARP 检测 5-9
自定义透明防火墙的 MAC 地址表 5-10
监控透明防火墙 5-11
监控 ARP 检测 5-11
监控 MAC 地址表 5-12
防火墙模式示例 5-12
数据如何在路由防火墙模式中通过 ASA 5-12
数据如何通过透明防火墙 5-18

防火墙模式的功能历史记录 5-23

第 2 部分 高可用性和可扩展性

第 6 章 多情景模式 6-1

安全情景的相关信息 6-1
安全情景的常见用途 6-2
情景配置文件 6-2
ASA 如何对数据包分类 6-2
级联安全情景 6-6
对安全情景的管理访问 6-7
资源管理的相关信息 6-8
有关 MAC 地址的信息 6-10
多情景模式的许可要求 6-12
先决条件 6-13
准则和限制 6-13
默认设置 6-14
配置多情景 6-14
配置多情景模式的任务流程 6-14
启用或禁用多情景模式 6-14
配置用于资源管理的类 6-16
配置安全情景 6-18
自动为情景接口分配 MAC 地址 6-22
在情景和系统执行空间之间切换 6-23
管理安全情景 6-23
移除安全情景 6-23
更改管理情景 6-24
更改安全情景 URL 6-24
重新加载安全情景 6-25
监控安全情景 6-26
查看情景信息 6-27
查看资源分配 6-28
查看资源使用情况 6-31
监控情景中的 SYN 攻击 6-32
查看分配的 MAC 地址 6-34
多情景模式的配置示例 6-36
多情景模式的功能历史记录 6-37

第 7 章 通过故障转移实现高可用性 7-1

关于故障转移 7-1
故障转移概述 7-2
故障转移系统要求 7-2
故障转移和有状态故障转移链路 7-3
MAC 和 IP 地址 7-7
ASA 服务模块 的机箱内和机箱间模块的布置 7-8
无状态和有状态故障转移 7-11
透明防火墙模式要求 7-13
故障转移运行状况监控 7-15
故障转移时间 7-16
配置同步 7-16
关于主用 / 备用故障转移 7-18
关于主用 / 主用故障转移 7-19
故障转移许可 7-21
故障转移的先决条件 7-22
故障转移准则 7-23
故障转移策略的默认内容 7-23
配置主用 / 备用故障转移 7-23
为主用 / 备用故障转移配置主设备 7-24
为主用 / 备用故障转移配置辅助设备 7-27
配置主用 / 主用故障转移 7-27
为主用 / 主用故障转移配置主设备 7-27
为主用 / 主用故障转移配置辅助设备 7-31
配置可选故障转移参数 7-32
配置故障转移条件、 HTTP 复制、组抢占、和 MAC 地址 7-32
配置接口监控 7-35
配置非对称路由数据包支持 （主用 / 主用模式） 7-35
管理故障转移 7-38
远程命令执行 7-41
发送命令 7-41
更改命令模式 7-42
安全注意事项 7-42
远程命令执行的限制 7-43
监控故障转移 7-43
故障转移消息 7-43
监控故障转移 7-44
故障转移功能历史记录 7-44

第 8 章 **ASA 集群** 8-1

关于 ASA 集群 8-1
ASA 集群如何融入网络中 8-2
性能换算系数 8-2
集群成员 8-2
集群接口 8-3
集群控制链路 8-5
ASA 集群中的高可用性 8-8
配置复制 8-9
ASA 集群管理 8-10
负载均衡方法 8-11
站点间集群 8-16
ASA 集群如何管理连接 8-19
ASA 功能和集群 8-21
ASA 集群的许可 8-28
ASA 集群的先决条件 8-28
ASA 集群的指导原则 8-29
ASA 集群的默认设置 8-33
配置 ASA 集群 8-33
使用电缆连接集群设备并配置上游和下游设备 8-33
在每台设备上配置集群接口模式 8-35
在主设备上配置接口 8-35
配置主设备引导程序设置 8-41
配置从设备引导程序设置 8-46
管理 ASA 集群成员 8-48
成为非活动成员 8-48
停用成员 8-49
退出集群 8-50
更改主设备 8-51
在集群范围执行命令 8-51
监控 ASA 集群 8-52
监控集群状态 8-53
在集群范围捕获数据包 8-53
监控集群资源 8-54
监控集群流量 8-54
监控集群路由 8-56
配置集群日志记录 8-56
监控集群接口 8-57
调试集群 8-57

ASA 集群示例 8-57
ASA 和交换机配置示例 8-57
单臂防火墙 8-60
流量分离 8-62
包含备用链路 （传统的 8 活动 /8 备用）的跨网络 EtherChannel 8-64
ASA 集群的历史记录 8-70

第 3 部分 接口

第 9 章 基本接口配置 （ASA 5512-X 及更高版本） 9-1
有关启动 ASA 5512-X 及更高版本接口配置的信息 9-1
Auto-MDI/MDIX 功能 9-2
处于透明模式中的接口 9-2
管理接口 9-2
冗余接口 9-4
EtherChannel 9-4
用最大传输单元、 TCP 最大分段大小控制分片 9-6
ASA 5512-X 及更高版本接口的许可要求 9-9
准则和限制 9-10
默认设置 9-11
开始接口配置 （ASA 5512-X 及更高版本） 9-12
开始接口配置的任务流程 9-12
启用物理接口并配置以太网参数 9-13
配置冗余接口 9-15
配置 EtherChannel 9-17
配置 VLAN 子接口和 802.1Q 中继 9-20
启用巨型帧支持 9-21
将使用中的接口转换为冗余接口或 EtherChannel 接口 9-22
监控接口 9-31
ASA 5512-X 及更高版本接口的配置示例 9-31
物理接口参数示例 9-31
子接口参数示例 9-31
多情景模式示例 9-32
EtherChannel 示例 9-32
后续操作 9-32
ASA 5512-X 及更高版本接口的功能历史记录 9-33

第 10 章 基本接口配置 (ASAv) 10-1
有关启动 ASAv 接口配置的信息 10-1
ASAv 接口和虚拟 NIC 10-1
处于透明模式中的接口 10-3
管理接口 10-3
冗余接口 10-4
用最大传输单元、TCP 最大分段大小控制分片 10-4
ASAv 接口的许可要求 10-6
准则和限制 10-6
默认设置 10-7
开始接口配置 (ASAv) 10-7
开始接口配置的任务流程 10-8
启用物理接口并配置以太网参数 10-8
配置冗余接口 10-9
配置 VLAN 子接口和 802.1Q 中继 10-11
启用巨型帧支持 10-12
监控接口 10-13
ASAv 接口的配置示例 10-13
物理接口参数示例 10-14
子接口参数示例 10-14
后续操作 10-14
ASAv 接口的功能历史记录 10-14

第 11 章 路由模式接口 11-1
在路由模式中完成接口配置的相关信息 11-1
安全级别 11-1
双堆栈 （IPv4 和 IPv6） 11-2
在路由模式中完成接口配置的许可要求 11-2
准则和限制 11-3
默认设置 11-4
在路由模式中完成接口配置 11-5
用于完成接口配置的任务流 11-5
配置常规接口参数 11-5
配置 MAC 地址、MTU 和 TCP MSS 11-7
配置 IPv6 寻址 11-10
允许同一安全级别通信 11-12
关闭和打开接口 11-14

监控接口 11-14
路由模式中接口的功能历史记录 11-15

第 12 章 透明模式接口 12-1
有关透明模式接口的信息 12-1
透明模式的网桥组 12-1
安全级别 12-2
透明模式接口的许可要求 12-2
透明模式接口的准则和限制 12-4
透明模式接口的默认设置 12-5
在透明模式中完成接口配置 12-5
用于完成接口配置的任务流 12-5
配置网桥组 12-6
配置常规接口参数 12-7
配置管理接口 （ASA 5512-X 和更高版本及 ASAv） 12-8
配置 MAC 地址、 MTU 和 TCP MSS 12-10
配置 IPv6 寻址 12-12
允许同一安全级别通信 12-14
关闭和打开接口 12-14
监控接口 12-15
透明模式接口的配置示例 12-15
透明模式接口的功能历史 12-16

第 4 部分 基本设置

第 13 章 基本设置 13-1
设置主机名、域名及启用和 Telnet 密码 13-1
恢复启用和 Telnet 密码 13-2
恢复 ASA 上的密码 13-3
恢复 ASA 5506、 5506-W 和 ASA 5508 上的密码 13-4
恢复 ASAv 上的密码或映像 13-5
禁用密码恢复 13-6
设置日期和时间 13-7
设置时区和夏令时日期 13-7
使用 NTP 服务器设置日期和时间 13-8
手动设置日期和时间 13-9
配置主密码 13-10
添加或更改主密码 13-10

禁用主密码 13-11
移除主密码 13-12
配置 DNS 服务器 13-13
设置 DNS 服务器 13-13
监控 DNS 缓存 13-14
调整 ASP （加速安全路径）性能和行为 13-14
选择规则引擎事务提交模型 13-14
启用 ASP 负载均衡 13-15
基本设置历史 13-15

第 14 章 **动态 DNS** 14-1
关于 DDNS 14-1
DDNS 更新配置 14-1
UDP 数据包大小 14-2
DDNS 准则 14-2
配置 DDNS 14-2
为静态 IP 地址更新 A 和 PTR RR 14-2
更新 A 和 PTR RR 14-3
忽略对任一 RR 的更新 14-4
仅更新 PTR RR 14-5
使用客户端更新 RR 并使用服务器更新 PTR RR 14-6
监控 DDNS 14-7
DDNS 历史记录 14-7

第 15 章 **DHCP 服务** 15-1
关于 DHCP 服务器 15-1
关于 DHCP 中继代理 15-2
DHCP 服务的许可要求 15-2
DHCP 服务准则 15-2
配置 DHCP 服务器 15-3
启用 DHCP 服务器 15-4
配置高级 DHCP 选项 15-5
返回 IP 地址 15-5
返回文本字符串 15-6
返回十六进制值 15-6
使用 DHCP 服务器配置 Cisco IP 电话 15-7
配置 DHCPv4 中继代理 15-9
配置 DHCPv6 中继代理 15-10

监控 DHCP 服务 15-11
DHCP 服务的历史记录 15-11

第 5 部分 对象和 ACL

第 16 章 访问控制对象 16-1
对象准则 16-1
配置对象 16-2
配置网络对象和组 16-2
配置服务对象和服务组 16-4
配置本地用户组 16-6
配置安全组对象组 16-7
配置时间范围 16-8
监控对象 16-9
对象的历史记录 16-10

第 17 章 访问控制列表 17-1
关于 ACL 17-1
ACL 类型 17-1
ACL 名称 17-2
访问控制条目顺序 17-2
允许 / 拒绝与 匹配 / 不匹配 17-3
访问控制隐式拒绝 17-3
使用 NAT 时用于扩展 ACL 的 IP 地址 17-3
基于时间的 ACE 17-4
ACL 准则 17-4
配置 ACL 17-5
基本 ACL 配置和管理选项 17-5
配置扩展 ACL 17-6
配置标准 ACL 17-12
配置 Webtype ACL 17-12
配置 EtherType ACL 17-15
监控 ACL 17-16
ACL 功能历史 17-17

第 6 部分 IP 路由

第 18 章 路由概述 18-1
有关路由 18-1
交换 18-1
路径确定 18-2
支持的路由类型 18-2
路由如何在 ASA 中运行 18-3
传出接口选择进程 18-3
下一跳选择进程 18-4
支持的路由互联网协议 18-4
有关路由表 18-5
显示路由表 18-5
如何填充路由表 18-5
如何制定转发决策 18-7
动态路由和故障转移 18-7
动态路由和集群 18-8
多情景模式中的动态路由 18-9
禁用代理 ARP 请求 18-9

第 19 章 静态路由和默认路由 19-1
有关静态路由和默认路由 19-1
静态路由和默认路由准则 19-2
静态路由配置 19-2
静态 Null0 路由配置 19-2
配置默认静态路由 19-3
默认静态路由配置的限制 19-4
配置 IPv6 默认和静态路由 19-4
监控静态路由或默认路由 19-5
静态路由或默认路由的示例 19-7
静态路由和默认路由的功能历史 19-7

第 20 章 路由映射 20-1
有关路由映射 20-1
Permit 和 Deny 子句 20-2
Match 和 Set 子句值 20-2
BGP Match 和 BGP Set 子句 20-3
路由映射准则 20-3
定义路由映射 20-4

自定义路由映射 20-4
定义路由以匹配特定目标地址 20-4
为路由操作配置度量值 20-5
路由映射的配置示例 20-6
路由映射的功能历史记录 20-6

第 21 章 BGP 21-1
关于 BGP 21-1
何时使用 BGP 21-1
路由表更改 21-1
BGP 路径选择 21-2
BGP 准则 21-3
配置 BGP 21-3
启用 BGP 21-4
定义 BGP 路由进程的最佳路径 21-5
配置策略列表 21-6
配置 AS 路径过滤器 21-7
配置社区规则 21-7
配置 IPv4 地址系列设置 21-8
监控 BGP 21-18
BGP 配置示例 21-20
BGP 历史记录 21-21

第 22 章 OSPF 22-1
关于 OSPF 22-1
快速呼叫数据包 OSPF 支持 22-2
OSPFv2 与 OSPFv3 之间的实施差异 22-3
OSPF 准则 22-4
配置 OSPFv2 22-5
配置 OSPF 快速呼叫数据包 22-6
定制 OSPFv2 22-7
将路由重新分发到 OSPFv2 中 22-7
将路由重新分发到 OSPFv2 中时配置路由摘要 22-9
配置 OSPFv2 区域之间的路由摘要 22-10
配置 OSPFv2 接口参数 22-10
配置 OSPFv2 区域参数 22-13
配置 OSPFv2 NSSA 22-13
为集群配置 IP 地址池 （OSPFv2 和 OSPFv3） 22-15

定义静态 OSPFv2 邻居 22-15
配置路由计算计时器 22-16
记录邻居启动或关闭 22-16
配置 OSPFv3 22-17
启用 OSPFv3 22-18
配置 OSPFv3 接口参数 22-18
配置 OSPFv3 路由器参数 22-23
配置 OSPFv3 区域参数 22-25
配置 OSPFv3 被动接口 22-26
配置 OSPFv3 管理距离 22-27
配置 OSPFv3 计时器 22-27
定义静态 OSPFv3 邻居 22-30
重置 OSPFv3 默认参数 22-31
发送系统日志消息 22-31
抑制系统日志消息 22-32
计算摘要路由成本 22-32
生成到 OSPFv3 路由域中的默认外部路由 22-32
配置 IPv6 摘要前缀 22-33
重新分发 IPv6 路由 22-34
配置无中断重新启动 22-34
配置功能 22-35
为 OSPFv2 配置无中断重新启动 22-35
为 OSPFv3 配置无中断重新启动 22-36
移除 OSPF 配置 22-37
OSPFv2 的配置示例 22-38
OSPFv3 的配置示例 22-39
监控 OSPF 22-40
附加参考资料 22-42
RFC 22-42
OSPF 功能历史记录 22-42

第 23 章 **EIGRP** 23-1
有关 EIGRP 的信息 23-1
使用集群 23-2
EIGRP 许可要求 23-2
准则和限制 23-2
配置 EIGRP 23-3
启用 EIGRP 23-3

启用 EIGRP 末节路由 23-4
自定义 EIGRP 23-4
为 EIGRP 路由进程定义网络 23-5
配置 EIGRP 的接口 23-5
在接口上配置摘要汇聚地址 23-7
更改接口延迟值 23-8
在接口上启用 EIGRP 身份验证 23-8
定义 EIGRP 邻居 23-9
将路由重新分发到 EIGRP 中 23-10
在 EIGRP 中过滤网络 23-11
自定义 EIGRP Hello 时间间隔和保持时间 23-12
禁用自动路由摘要 23-13
在 EIGRP 中配置默认信息 23-14
禁用 EIGRP 水平分割 23-14
重新启动 EIGRP 进程 23-15
监控 EIGRP 23-15
EIGRP 的配置示例 23-16
EIGRP 的功能历史记录 23-17

第 24 章 组播路由 24-1
有关组播路由的信息 24-1
末节组播路由 24-2
PIM 组播路由 24-2
组播组概念 24-2
集群 24-2
组播路由的许可要求 24-3
准则和限制 24-3
启用组播路由 24-3
自定义组播路由 24-4
配置末节组播路由和转发 IGMP 消息 24-4
配置静态组播路由 24-5
配置 IGMP 功能 24-5
配置 PIM 功能 24-9
配置双向邻居过滤器 24-12
配置组播边界 24-13
组播路由的配置示例 24-14
附加参考资料 24-14
相关文档 24-14

RFC 24-14
组播路由的功能历史记录 24-15

第 25 章 IPv6 邻居发现 25-1
有关 IPv6 邻居发现的信息 25-1
邻居请求消息 25-2
邻居可到达时间 25-2
重复地址检测 25-2
路由器通告消息 25-2
静态 IPv6 邻居 25-3
IPv6 邻居发现的许可要求 25-3
IPv6 邻居发现的先决条件 25-3
准则和限制 25-4
IPv6 邻居发现的默认设置 25-5
配置 IPv6 邻居发现 25-5
进入接口配置模式 25-6
配置邻居请求消息间隔 25-6
配置邻居可到达时间 25-7
配置路由器通告传输时间间隔 25-7
配置路由器有效期值 25-8
配置 DAD 设置 25-8
抑制路由器通告消息 25-9
为 IPv6 DHCP 中继配置地址配置标志 25-9
配置路由器通告中的 IPv6 前缀 25-10
配置静态 IPv6 邻居 25-11
监控 IPv6 邻居发现 25-11
附加参考资料 25-11
IPv6 前缀的相关文档 25-12
IPv6 前缀的 RFC 和文档 25-12
IPv6 邻居发现的功能历史记录 25-12

第 7 部分 AAA 服务器和本地数据库

第 26 章 关于 AAA 的信息 26-1
身份验证 26-1
授权 26-2
记帐 26-2

身份验证、授权和记帐之间的交互 26-2
AAA 服务器 26-2
AAA 服务器组 26-2
本地数据库支持 26-2

第 27 章 用于 AAA 的本地数据库 27-1
关于本地数据库 27-1
回退支持 27-2
组中存在多个服务器时的回退方式 27-2
本地数据库准则 27-2
向本地数据库添加用户帐户 27-3
监控本地数据库 27-6
本地数据库的历史 27-7

第 28 章 AAA RADIUS 服务器 28-1
有关 RADIUS 服务器 28-1
支持的身份验证方法 28-1
VPN 连接的用户身份验证 28-2
支持的 RADIUS 属性集 28-2
支持的 RADIUS 授权属性 28-2
支持的 IETF RADIUS 授权属性 28-12
RADIUS 记账断开原因代码 28-12
RADIUS 服务器许可要求 28-13
准则和限制 28-13
配置 RADIUS 服务器 28-14
配置 RADIUS 服务器任务流程 28-14
配置 RADIUS 服务器组 28-14
将 RADIUS 服务器添加到组 28-17
监控 RADIUS 服务器 28-19
附加参考资料 28-19
RFC 28-19
RADIUS 服务器功能历史 28-20

第 29 章 用于 AAA 的 TACACS+ 服务器 29-1
有关 TACACS+ 服务器的信息 29-1
使用 TACACS+ 属性 29-1
TACACS+ 服务器的许可要求 29-2

准则和限制 29-2
配置 TACACS+ 服务器 29-3
配置 TACACS+ 服务器任务流程 29-3
配置 TACACS+ 服务器组 29-3
将 TACACS+ 服务器添加至服务器组 29-5
监控 TACACS+ 服务器 29-5
TACACS+ 服务器的功能历史记录 29-6

第 30 章 **AAA 中的 LDAP 服务器** 30-1
有关 LDAP 和 ASA 的信息 30-1
LDAP 服务器准则 30-1
如何用 LDAP 进行身份验证 30-2
关于 LDAP 层次结构 30-2
关于绑定到 LDAP 服务器 30-3
LDAP 服务器许可要求 30-4
准则和限制 30-4
配置 LDAP 服务器 30-4
用于配置 LDAP 服务器的任务流 30-4
配置 LDAP 属性映射 30-4
配置 LDAP 服务器组 30-7
用 LDAP 为 VPN 配置身份验证 30-9
监控 LDAP 服务器 30-10
LDAP 服务器的功能历史记录 30-10

第 31 章 **身份防火墙** 31-1
关于身份防火墙的信息 31-1
身份防火墙概述 31-1
身份防火墙部署的架构 31-2
身份防火墙功能 31-3
部署方案 31-4
身份防火墙许可 31-6
准则和限制 31-6
先决条件 31-8
配置身份防火墙 31-8
配置身份防火墙任务流程 31-9
配置 Active Directory 域 31-9
配置 Active Directory 代理 31-11
配置身份选项 31-12

配置基于身份的安全策略 31-16
收集用户统计信息 31-17
配置示例 31-17
AAA 规则和访问规则示例 1 31-17
AAA 规则和访问规则示例 2 31-18
VPN 过滤器示例 31-18
监控身份防火墙 31-19
监控 AD 代理 31-19
监控组 31-20
监控身份防火墙的内存使用情况 31-20
监控身份防火墙用户 31-20
身份防火墙的功能历史记录 31-21

第 32 章 **ASA 和思科 TrustSec** 32-1
关于集成思科 TrustSec 的 ASA 32-1
关于思科 TrustSec 32-2
思科 TrustSec 中的 SGT 和 SXP 支持 32-2
思科 TrustSec 功能中的角色 32-2
安全组策略实施 32-3
ASA 如何实施基于安全组的策略 32-4
安全组更改对 ISE 产生的影响 32-5
关于 ASA 上的 Speaker 和 Listener 角色 32-6
SXP 通信速率 32-7
SXP 计时器 32-7
IP-SGT 管理器数据库 32-7
ASA- 思科 TrustSec 集成的功能 32-8
思科 TrustSec 的许可要求 32-9
使用思科 TrustSec 的先决条件 32-9
通过 ISE 注册 ASA 32-10
在 ISE 上创建安全组 32-10
生成 PAC 文件 32-10
准则和限制 32-11
为思科 TrustSec 集成配置 ASA 32-12
为思科 TrustSec 集成配置 AAA 服务器 32-13
导入 PAC 文件 32-14
配置安全交换协议 32-16
添加 SXP 连接对等体 32-18
刷新环境数据 32-18
配置安全策略 32-19

配置第 2 层安全组标记实施 32-20
启用 SGT plus Ethernet Tagging 32-22
在接口上传送安全组标记 32-23
将策略应用到手动配置的思科 TrustSec 链路 32-23
手动配置 IP-SGT 绑定 32-24
配置示例 32-24
面向思科 TrustSec 的 AnyConnect VPN 支持 32-25
远程用户连接到服务器的典型步骤 32-25
将 SGT 添加到本地用户和组 32-26
监控思科 TrustSec 32-26
附加参考资料 32-26
思科 TrustSec 集成的功能历史 32-27

第 33 章 **ASA 和思科移动支持 33-1**
关于 ASA 和思科移动支持 33-1
ASA MDM 代理准则和限制 33-1
将 ASA 配置为 MDM 代理 33-2
监控 Mobile Enablement Proxy 活动 33-3
ASA Mobile Enablement Proxy 的功能历史记录 33-3

第 34 章 **数字证书 34-1**
关于数字证书 34-1
公钥加密 34-1
证书可扩展性 34-2
密钥对 34-2
信任点 34-2
撤销检查 34-3
本地 CA 34-5
证书和用户登录凭证 34-6
本地证书的先决条件 34-7
SCEP 代理支持的先决条件 34-8
数字证书准则 34-8
配置数字证书 34-9
配置密钥对 34-10
移除密钥对 34-10
配置信任点 34-11
为信任点配置 CRL 34-13
导出信任点配置 34-15

导入信任点配置 34-15
配置 CA 证书映射规则 34-16
手动获取证书 34-17
使用 SCEP 自动获取证书 34-18
为 SCEP 请求配置代理支持 34-19
启用本地 CA 服务器 34-20
配置本地 CA 服务器 34-21
自定义本地 CA 服务器 34-22
调试本地 CA 服务器 34-23
禁用本地 CA 服务器 34-24
删除本地 CA 服务器 34-24
配置本地 CA 证书特征 34-24
监控数字证书 34-34
证书管理的功能历史 34-36

第 8 部分 系统管理

第 35 章 管理访问 35-1
配置 ASDM、 Telnet 或 SSH 的 ASA 访问 35-1
ASDM、 Telnet 或 SSH 的 ASA 访问许可要求 35-2
准则和限制 35-2
配置 Telnet 访问 35-3
使用 Telnet 客户端 35-3
配置 SSH 访问 35-4
使用 SSH 客户端 35-5
配置 ASDM 的 HTTPS 访问 35-5
配置 CLI 参数 35-6
CLI 参数许可要求 35-6
准则和限制 35-6
配置登录横幅 35-6
自定义 CLI 提示符 35-7
更改控制台超时 35-8
配置 VPN 隧道上的管理访问 35-9
管理接口的许可要求 35-9
准则和限制 35-9
配置管理接口 35-10
配置系统管理员 AAA 35-10
有关系统管理员 AAA 的信息 35-10
系统管理员的 AAA 许可要求 35-13

先决条件 35-13
准则和限制 35-14
默认设置 35-14
配置 CLIASDM 和 命令访问的身份验证 35-15
配置访问特权 EXEC 模式 （enable 命令）的身份验证 35-16
使用管理授权限制用户的 CLI 和 ASDM 访问 35-18
为本地数据库用户配置密码策略 35-20
配置命令授权 35-22
配置管理访问记帐 35-26
查看当前登录用户 35-27
设置管理会话配额 35-28
在 SSH 会话中交换密钥 35-28
从锁定中恢复 35-29
管理访问的功能历史记录 35-30

第 36 章 软件和配置 36-1
升级软件 36-1
升级路径和迁移 36-1
查看当前版本 36-3
从 Cisco.com 下载软件 36-3
升级独立设备 36-3
升级故障转移对或 ASA 集群 36-4
管理文件 36-10
查看闪存中的文件 36-10
从闪存中删除文件 36-11
擦除闪存文件系统 36-11
配置文件访问 36-11
将文件复制到 ASA 36-15
将文件复制至启动或运行配置 36-17
配置要使用的映像和启动配置 36-19
使用 ROM 监控模式加载映像 36-20
使用 ASA 5500-X 系列的 ROM 监控模式 36-20
使用 ASASM 的 ROM 监控模式 36-21
备份和还原 配置或其他文件 36-23
备份单模式配置或多模式系统配置 36-23
备份闪存中的情景配置或其他文件 36-24
备份情景中的情景配置 36-24
从终端显示复制配置 36-25
使用导出和导入命令备份其他文件 36-25

使用脚本来备份和还原文件 36-25
将您的软件降级 36-31
激活密钥兼容性的相关信息 36-32
执行降级 36-32
配置自动更新 36-33
有关自动更新的信息 36-33
准则和限制 36-36
配置与自动更新服务器的通信 36-36
将客户端更新配置为自动更新服务器 36-37
查看自动更新状态 36-38
软件和配置的功能历史记录 36-39

第 37 章 系统事件的响应自动化 37-1
关于 EEM 37-1
EEM 准则 37-2
配置 EEM 37-3
创建事件管理器小程序并配置事件 37-3
配置操作和操作输出的目标 37-4
运行事件管理器小程序 37-6
EEM 示例 37-6
监控 EEM 37-7
EEM 的历史记录 37-7

第 38 章 故障排除 38-1
查看调试消息 38-1
捕获数据包 38-1
在集群环境中捕获数据包 38-2
查看崩溃转储 38-4
查看核心转储 38-4
ASAv 中的 vCPU 使用率 38-5
CPU 使用率示例 38-5
VMware CPU 使用率报告 38-5
ASAv 和 vCenter 图表 38-5

第 9 部分 记录、SNMP 和 Smart Call Home

第 39 章 日志记录 39-1
关于日志记录 39-1
多情景模式中的日志记录 39-2
系统日志消息分析 39-2
系统日志消息格式 39-2
严重性级别 39-3
消息类和系统日志 ID 范围 39-3
系统日志消息过滤 39-3
自定义消息列表 39-4
集群 39-4
日志记录准则 39-4
配置日志记录 39-5
启用日志记录 39-6
配置输出目标 39-6
监控日志 39-17
日志记录示例 39-18
日志记录的历史记录 39-18

第 40 章 SNMP 40-1
关于 SNMP 40-1
SNMP 术语 40-2
MIB 和陷阱 40-2
SNMP 对象标识符 40-4
物理供应商类型值 40-5
MIB 中受支持的表和对象 40-9
受支持的陷阱（通知） 40-10
接口类型和示例 40-13
SNMP 第 3 版概述 40-14
SNMP 系统日志消息传递 40-15
应用服务和第三方工具 40-15
SNMP 准则 40-16
配置 SNMP 40-18
启用 SNMP 代理和 SNMP 服务器 40-18
配置 SNMP 陷阱 40-18
配置 CPU 使用率阈值 40-19
配置物理接口阀值 40-20
配置 SNMP 第 1 或 2c 版的参数 40-20
配置 SNMP 第 3 版的参数 40-21

配置用户组 40-24
将用户与网络对象相关联 40-24
监控 SNMP 40-25
SNMP 第 1 和 2c 版示例 40-26
SNMP 第 3 版示例 40-26
SNMP 历史记录 40-27

第 41 章 **Anonymous Reporting 和 Smart Call Home** 41-1
关于 Anonymous Reporting 41-1
DNS 需求 41-2
关于 Smart Call Home 41-2
订用警报组 41-2
Anonymous Reporting 和 Smart Call Home 指南 41-6
配置 Anonymous Reporting 和 Smart Call Home 41-7
配置 Anonymous Reporting 41-7
配置 Smart Call Home 41-8
监控 Anonymous Reporting 和 Smart Call Home 41-16
Smart Call Home 的示例 (CLI) 41-17
Anonymous Reporting 和 Smart Call Home 的历史 41-18

第 10 部分 **参考网站**

第 42 章 **使用命令行界面** 42-1
防火墙模式和安全情景模式 42-1
命令模式和提示符 42-2
语法格式化 42-3
缩写命令 42-3
命令行编辑 42-3
命令补全 42-3
命令帮助 42-3
查看运行配置 42-4
过滤 show 和 more 命令输出 42-4
命令输出分页 42-5
添加注释 42-5
文本配置文件 42-5
命令与文本文件中的行的对应方式 42-6

特定于命令的配置模式命令 42-6
自动文本条目 42-6
行顺序 42-6
文本配置中不包含的命令 42-6
密码 42-6
多安全情景文件 42-7
支持的字符集 42-7

第 43 章 地址、协议和端口 43-1
IPv4 地址和子网掩码 43-1
类 43-1
专用网络 43-2
子网掩码 43-2
IPv6 地址 43-4
IPv6 地址格式 43-4
IPv6 地址类型 43-5
IPv6 地址前缀 43-9
协议和应用 43-9
TCP 和 UDP 端口 43-10
本地端口和协议 43-12
ICMP 类型 43-14

关于本指南

- 文档目标，第 xxix 页
- 相关文档，第 xxix 页
- 约定，第 xxix 页
- 获取文档和提交服务请求，第 xxx 页

文档目标

本指南旨在帮助您使用命令行界面 为 Cisco ASA 系列配置常规操作。本指南不涵盖所有功能，只介绍了最常见的配置方案。

通过使用思科自适应安全设备管理器 (ASDM)（一种基于网络的 GUI 应用），您还可以配置和监控 ASA。ASDM 包含用于指导您完成一些常见配置方案的配置向导和不常见方案的联机帮助。

在本指南中，术语“ASA”一般适用于受支持的型号，除非另有规定。

相关文档

有关详细信息，请参阅 *导航 Cisco ASA 系列文档*，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 }	必填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。
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 bold 字体	命令和关键字及用户输入的文本以 **bold courier** 字体显示。
courier italic 字体	您为其提供值的参数以 *courier italic* 字体显示。
< >	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 Cisco Bug 搜索工具 (BST)、提交服务请求和收集更多信息的信息，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

ASA 使用入门

思科 ASA 简介

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

思科 ASA 将高级状态防火墙和 VPN 集中器功能集于一身，某些型号还提供集成服务模块（例如 IPS）。 ASA 包括很多高级功能，例如，多安全情景 （类似于虚拟防火墙）、集群 （将多个防火墙组合到一个防火墙中）、透明 （第 2 层）防火墙或路由 （第 3 层）防火墙操作、高级检测引擎、 IPsec VPN、 SSL VPN 和无客户端 SSL VPN 支持以及其他功能。

- 第 1-1 页的硬件和软件兼容性
- 第 1-1 页的 VPN 兼容性
- 第 1-2 页的新功能
- 第 1-5 页的 ASA 服务模块如何与交换机配合使用
- 第 1-7 页的防火墙功能概述
- 第 1-11 页的 VPN 功能概述
- 第 1-11 页的安全情景概述
- 第 1-12 页的 ASA 集群概述
- 第 1-12 页的特殊的服务和传统服务

硬件和软件兼容性

有关受支持硬件和软件的完整列表，请通过以下链接参阅 *《思科 ASA 兼容性》*：
http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

VPN 兼容性

请通过以下链接参阅 *《支持的 VPN 平台 （思科 ASA 系列）》*：
http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html

新功能

- 第 1-2 页的 ASA 9.3(1) 版本的新功能

注　系统日志消息指南中列出了新的、有变化的以及已弃用的系统日志消息。

ASA 9.3(1) 版本的新功能

发布日期：2014 年 7 月 24 日

表 1-1 列出了 ASA 9.3(1) 版本的新功能。

表 1-1　ASA 9.3(1) 版本的新功能

功能	说明
防火墙功能	
对 IPv6 的 SIP、 SCCP 和 TLS 代理支持	现在使用 SIP、SCCP 和 TLS 代理（使用 SIP 或 SCCP）时可检查 IPv6 流量。 我们未修改任何命令。
支持思科统一通信管理器 8.6	ASA 现在可与思科统一通信管理器 8.6 版本互操作 （包括 SCCPv21 支持）。 我们未修改任何命令。
访问组和 NAT 的规则引擎事务提交模型	一经启用，规则更新在规则编译完成后即可得以应用；不会影响规则匹配性能。 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**
远程访问功能	
XenDesktop 7 对无客户端 SSL VPN 的支持	我们已添加 XenDesktop 7 对无客户端 SSL VPN 的支持。现在，通过自动登录创建书签时，可以指定登录页面 URL 或控制 ID。 我们未修改任何命令。
Mobile Enablement Proxy	Mobile Enablement Proxy 是 ISE Mobile Enablement 解决方案的组件，允许外部移动设备以与内部移动设备完全相同的方式参与移动设备管理。 **注**　在即将于 2015 年年初推出的 ISE 中，Mobile Enablement Proxy 要求有 ISE 支持。 我们引入了 **mdm-proxy** 命令，以进入 config-mdm-proxy 模式。在此新模式中，以下命令适用：**authentication-server-group**、**accounting-server-group**、 **password-management**、 **trusttpoint**、 **port**、**session-limit**、 **session-timeout** 和 **enable**

表 1-1　　ASA 9.3(1) 版本的新功能（续）

功能	说明
AnyConnect 自定义属性增强	自定义属性定义并配置未融入 ASA 的 AnyConnect 功能，如延迟升级。自定义属性配置已得到增强，以允许多个值和更长的值，而且现在需要其类型、名称和值的规格。现在可将其添加至动态访问策略和组策略。升级到 9.3.x 后，以前定义的自定义属性将更新至此增强配置格式。 我们引入或修改了以下命令：**anyconnect-custom-attr**、**anyconnect-custom-data** 和 **anyconnect-custom**
桌面平台的 AnyConnect Identity Extensions (ACIDex)	ACIDex，也称为 AnyConnect Endpoint Attributes 或 Mobile Posture，是 AnyConnect VPN 客户端用于向 ASA 传递状况信息的方法。动态访问策略使用这些终端属性向用户进行授权。 现在，AnyConnect VPN 客户端可为桌面操作系统（Windows、Mac OS X 和 Linux）提供平台识别和可供 DAP 使用的 MAC 地址池。 我们未修改任何命令。
VPN 的 TrustSec SGT 分配	现在，远程用户连接时，TrustSec 安全组标记 (SGT) 可添加至 ASA 上的 SGT-IP 表。 我们引入了以下新命令：**security-group-tag value**
高可用性功能	
改进了对集群中模块运行状况监控的支持	我们增加了对集群中模块运行状况监控的改进支持。 我们修改了以下命令：**show cluster info health**
禁用硬件模块的运行状况监控	默认情况下，ASA 监控已安装的硬件模块（例如 ASA FirePOWER 模块）的运行状况。如果您不希望硬件模块故障触发故障转移，可以禁用模块监控。 我们修改了以下命令：**monitor-interface service-module**
平台功能	

表 1-1　　ASA 9.3(1) 版本的新功能（续）

功能	说明
ASP 负载均衡	**asp load-balance per-packet** 命令中的新 **auto** 选项使 ASA 能够自适应地在每个接口接收环上打开和关闭 ASP 每数据包负载均衡。这一自动机制可检测是否引入了不对称流量，且有助于避免以下问题： • 因偶发的流量高峰而造成溢出 • 因大量流量过度订用特定接口接收环而造成溢出 • 因相对严重过载的接口接收环而造成溢出（这种情况下，一个核心无法维持负载） 我们引入或修改了以下命令：**asp load-balance per-packet auto**、 **show asp load-balance per-packet**、 **show asp load-balance per-packet history** 和 **clear asp load-balance history**
SNMP MIB	CISCO-REMOTE-ACCESS-MONITOR-MIB 现在支持 ASASM。
接口功能	
透明模式的网桥组最大数量增加到 250	网桥组最大数量从 8 增加到 250。在单情景模式和多情景模式的每个情景中，最多可配置 250 个网桥组，每组最多 4 个接口。 我们修改了以下命令：**interface bvi**、 **bridge-group**
路由功能	
ASA 集群的 BGP 支持	我们增加了对 BGP 用于 ASA 集群的支持。 我们引入了以下新命令：**bgp router-id clusterpool**
不间断转发的 BGP 支持	我们增加了 BGP 不间断转发支持。 我们引入了以下新命令：**bgp graceful-restart**、 **neighbor ha-mode graceful-restart**
通告映射的 BGP 支持	我们添加了对 BGPv4 通告映射的支持。 我们引入了以下新命令：**neighbor advertise-map**
对不间断转发 (NSF) 的 OSPF 支持	添加了对 NSF 的 OSPFv2 和 OSPFv3 支持。 我们添加了以下命令：**capability**、 **nsf cisco**、 **nsf cisco helper**、 **nsf ietf**、 **nsf ietf helper**、 **nsf ietf helper strict-lsa-checking**、 **graceful-restart**、 **graceful-restart helper**、 **graceful-restart helper strict-lsa-checking**
AAA 功能	

表 1-1　　ASA 9.3(1) 版本的新功能（续）

功能	说明
第 2 层安全组标记施加	现在，您可以使用结合了以太网标记的安全组标记来实施策略。 SGT 加以太网标记，也称为第 2 层 SGT 强制，使 ASA 能够使用思科专有以太网帧 (Ether Type 0x8909) 在千兆以太网接口上发送和接收安全组标记，从而将源安全组标记插入纯文本以太网帧。 我们引入或修改了以下命令：**cts manual**、 **policy static sgt**、 **propagate sgt**、 **cts role-based sgt-map**、 **show cts sgt-map**、 **packet-tracer**、 **capture**、**show capture**、**show asp drop**、**show asp table classify**、**show running-config all**、 **clear configure all** 和 **write memory**
AAA Windows NT 域身份验证移除	我们移除了对于远程访问 VPN 用户的 NTLM 支持。 我们弃用了以下命令：**aaa-server protocol nt**
监控功能	
监控物理接口的汇聚流量	**show traffic** 命令输出已经更新，包括物理接口信息的汇聚流量。如要启用该功能，必须先输入 **sysopt traffic detailed-statistics** 命令。

ASA 服务模块如何与交换机配合使用

可以在 Catalyst 6500 系列和思科 7600 系列交换机上安装 ASASM，并在交换机管理引擎和集成 MSFC 上都安装思科 IOS 软件。

注　不支持 Catalyst 操作系统 (OS)。

ASA 运行自己的操作系统。

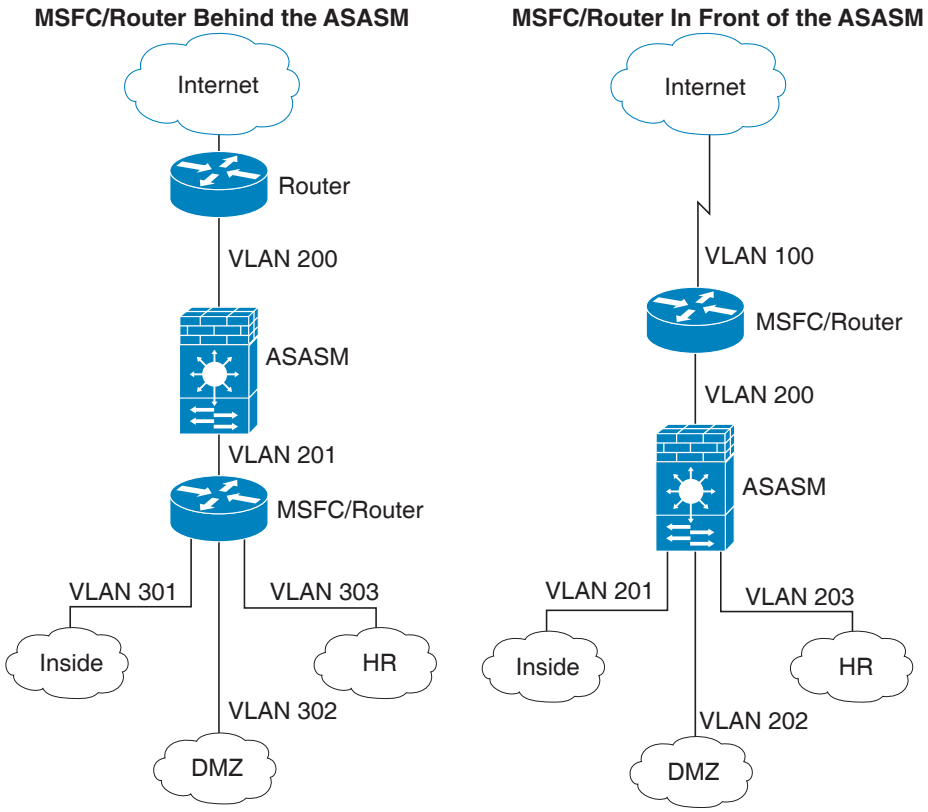
交换机由一个交换处理器 （管理引擎）和一个路由器 (MSFC) 组成。虽然需要将 MSFC 作为系统的一部分，但并不一定要使用它。如果选择使用 MSFC，可以向 MSFC 分配一个或多个 VLAN 接口。或者，可以使用外部路由器来代替 MSFC。

在单情景模式中，可以将路由器放置在防火墙的前面或后面 （请参阅图 1-1）。

路由器的位置完全取决于向其分配的 VLAN。例如，在图 1-1 左侧的示例中，路由器位于防火墙后面，因为向 ASASM 的内部接口分配了 VLAN 201。在图 1-1 右侧的示例中，路由器位于防火墙前面，因为向 ASASM 的外部接口分配了 VLAN 200。

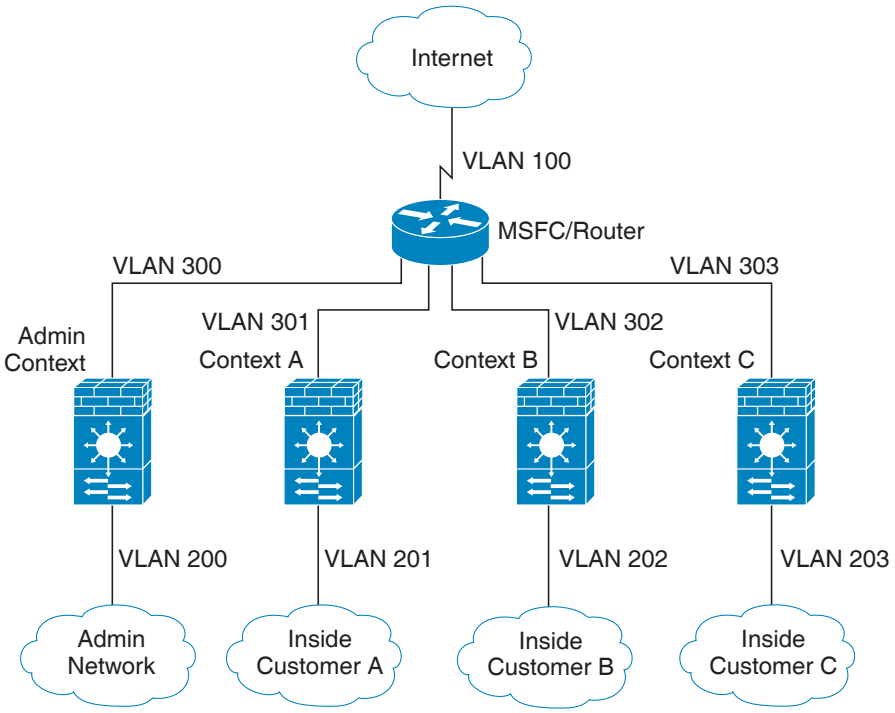
在左侧的示例中，MSFC 或路由器在 VLAN 201、301、302 与 303 之间路由，且没有内部流量可以通过 ASASM，除非是流向互联网的内部流量才可以通过。在右侧的示例中，ASASM 处理和保护内部 VLAN 201、 202 与 203 之间的所有流量。

图 1-1　　MSFC/路由器的放置



在多情景模式中，如果将路由器放置在 ASASM 后面，则只能将路由器连接到一个情景。在这种情况下，如果将路由器连接到多个情景，路由器将在这些情景之间进行路由，而这可能不是您的本意。多情景的典型情况是，在所有情景的前面使用一个路由器，用于在互联网与交换网络之间进行路由 （请参阅图 1-2）。

图 1-2　　多情景模式中 MSFC/路由器的放置



防火墙功能概述

防火墙可防止外部网络上的用户在未经授权的情况下访问内部网络。防火墙还具有其他功能，例如，可以将人力资源网络与用户网络分离开，以在内部网络互相之间提供保护。如果有需要提供给外部用户使用的网络资源 （例如网络服务器或 FTP 服务器），可以将这些资源放置在防火墙后面的单独网络上 （这种网络称为*隔离区* (DMZ)）。防火墙允许有限访问 DMZ，但由于 DMZ 只包括公共服务器，因此，在那里发生的攻击只会影响服务器，而不会影响其他内部网络。还可以通过以下手段来控制内部用户何时可以访问外部网络 （例如，访问互联网）：仅允许访问某些地址；要求身份验证或授权；配合使用外部 URL 过滤服务器。

连接到防火墙的网络通常具有以下特点：*外部*网络在防火墙前面；*内部*网络受保护并位于防火墙后面；*DMZ* 也位于防火墙后面，但允许外部用户进行有限访问。由于 ASA 允许配置具有各种安全策略的很多接口，包括很多内部接口、很多 DMZ，甚至是很多外部接口 （如有需要），因此，这些术语仅具有一般意义

- 第 1-8 页的安全策略概述
- 第 1-10 页的防火墙模式概述
- 第 1-10 页的状态检测概述

安全策略概述

安全策略确定哪些流量可通过防火墙来访问其他网络。默认情况下，ASA 允许流量自由地从内部网络（安全级别较高）流向外部网络（安全级别较低）。您可以将操作应用于流量，以自定义安全策略。

- 第 1-8 页的通过访问列表
- 第 1-8 页的应用 NAT
- 第 1-8 页的保护 IP 分片
- 第 1-8 页的对直通流量使用 AAA
- 第 1-8 页的应用 HTTP、 HTTPS 或 FTP 过滤
- 第 1-9 页的运用应用检测
- 第 1-9 页的向受支持的硬件或软件模块发送流量
- 第 1-9 页的应用 QoS 策略
- 第 1-9 页的应用连接限制和 TCP 规范化
- 第 1-9 页的启用威胁检测
- 第 1-9 页的启用僵尸网络流量过滤器
- 第 1-10 页的配置思科统一通信

通过访问列表

可以应用访问列表，以限制从内部到外部的流量或者允许从外部到内部的流量。在透明防火墙模式中，还可以应用以太网类型访问列表来允许非 IP 流量。

应用 NAT

NAT 的其中一些优点包括：

- 可以在内部网络上使用专用地址。专用地址不可在互联网上进行路由。
- NAT 可隐藏其他网络的本地地址，以使攻击者无法获悉主机的真实地址。
- NAT 可通过支持重叠 IP 地址来解决 IP 路由问题。

保护 IP 分片

ASA 提供 IP 分片保护。此功能对所有 ICMP 错误消息执行完全重组，并对通过 ASA 路由的剩余 IP 分片执行虚拟重组。会丢弃并记录未能通过安全检查的分片。不能禁用虚拟重组。

对直通流量使用 AAA

对某些类型的流量（例如 HTTP），可以要求身份验证和/或授权。 ASA 还会向 RADIUS 或 TACACS+ 服务器发送记帐信息。

应用 HTTP、 HTTPS 或 FTP 过滤

虽然可以使用访问列表来防止对于特定网站或 FTP 服务器的出站访问，但由于互联网的规模和动态性质，以这种方式配置和管理网络使用并不切实际。

可以在 ASA 上配置云网络安全，或者安装提供 URL 和其他过滤服务的 ASA 模块（例如 ASA CX 或 ASA FirePOWER）。还可以将 ASA 与思科网络安全设备 (WSA) 之类的外部产品结合使用。

运用应用检测

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。这些协议要求 ASA 执行深度数据包检测。

向受支持的硬件或软件模块发送流量

某些 ASA 型号允许配置软件模块或者将硬件模块装入到机箱中，以提供高级服务。这些模块提供其他流量检测，并可根据配置的策略阻止流量。您可以将流量发送到这些模块，以利用这些高级服务。

应用 QoS 策略

某些网络流量（例如声音和视频流）不允许出现长时间延迟。 QoS 是一种网络功能，使您可以向此类流量赋予优先级。 QoS 是指一种可以向所选网络流量提供更好服务的网络功能。

应用连接限制和 TCP 规范化

可以限制 TCP 连接、 UDP 连接和半开连接。限制连接和半开连接的数量可防止受到 DoS 攻击。ASA 使用半开限制触发 TCP 拦截，从而防止内部系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。半开连接是指未完成源与目标之间的必要握手的连接请求。

TCP 规范化是指一种包含高级 TCP 连接设置的功能，用以丢弃有异常迹象的数据包。

启用威胁检测

可以配置扫描威胁检测和基本威胁检测，还可以配置如何使用统计数据来分析威胁。

基本威胁检测会检测可能与攻击（例如 DoS 攻击）相关的活动，并自动发送系统日志消息。

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（通过扫描子网中的很多主机或清扫主机或子网中的很多端口）。扫描威胁检测功能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 扫描威胁检测功能维护一个包含主机统计数据的庞大数据库；可以分析这些统计数据以执行扫描活动。

主机数据库跟踪可疑活动，例如，没有返回活动的连接、对关闭服务端口的访问、易受攻击的 TCP 行为（例如非随机 IPID）以及其他行为。

可以将 ASA 配置为会发送有关攻击者的系统日志消息，或者可以自动避开主机。

启用僵尸网络流量过滤器

恶意软件是指安装在未知主机上的恶意软件。对于尝试进行诸如发送专用数据（密码、信用卡号、按键输入或专有数据）等网络活动的恶意软件，僵尸网络流量过滤器可以在它们开始连接到已知的不良 IP 地址时检测到它们。僵尸网络流量过滤器根据已知的不良域名和 IP 地址（黑名单）的动态数据库检查传入和传出连接，然后记录任何可疑活动。当您看到有关恶意软件活动的系统日志消息时，就可以采取措施来隔离主机以及消除主机所包含的危害。

配置思科统一通信

思科 ASA 系列是一个战略平台，为统一通信部署提供代理功能。代理的目标是终止和重新发起客户端与服务器之间的连接。代理提供各种安全功能 （例如，流量检测、协议符合性检查和策略控制），以确保内部网络的安全。一种日益普遍的代理功能是，终止加密连接，以便能够在确保连接机密性的同时应用安全策略。

防火墙模式概述

ASA 在两种不同的防火墙模式中运行：

- 路由
- 透明

在路由模式中，ASA 被视为网络中的路由器跃点。

在透明模式中，ASA 充当“网络嵌入式防火墙”或“隐形防火墙”，而不被视为路由器跃点。ASA 在其内部和外部接口上连接到同一个网络。

可以使用透明防火墙来简化网络配置。如果希望防火墙对攻击者不可见，透明模式同样有用。还可以对在路由模式中会被阻止的流量使用透明防火墙。例如，透明防火墙可通过访问列表允许组播数据流。

状态检测概述

经过 ASA 的所有流量均要使用自适应安全算法进行检测，检测后，流量要么允许通过，要么被丢弃。简单的数据包过滤器可检查源地址、目标地址和端口是否正确，但不会检查数据包序列或标记是否正确。过滤器还可以根据过滤器本身检查*每个*数据包，但这个过程可能比较慢。

注　TCP 状态绕过功能使您可以自定义数据包流量。

但是，状态防火墙 （例如 ASA）会考虑到数据包的状态：

- 这是新连接吗？

  如果是新连接，ASA 必须根据访问列表检查数据包并执行其他任务，以确定应该允许还是拒绝数据包。如要执行这项检查，会话的第一个数据包要通过“会话管理路径”，可能还会通过“控制平面路径”，具体取决于流量类型。

  会话管理路径负责执行以下任务：

  – 执行访问列表检查
  – 执行路由查找
  – 分配 NAT 转换 (xlate)
  – 在“快速路径”中建立会话

  ASA 在 TCP 流量的快速路径中创建正向流量和反向流量；ASA 还会为无连接协议 （例如 UDP、 ICMP）创建连接状态信息 （启用 ICMP 检测时），以便这些协议也可以使用快速路径。

  注　对于其他 IP 协议 （例如 SCTP）， ASA 不会创建反向路径流向。因此，涉及这些连接的 ICMP 错误数据包将会丢弃。

需要第 7 层检测的某些数据包 （必须检测或改变数据包负载）会传递到控制平面路径。具有两个或多个信道 （一个数据信道，使用已知端口号；一个控制信道，对每个会话使用不同的端口号）的协议需要第 7 层检测引擎。这些协议包括 FTP、 H.323 和 SNMP。

- 这是已建立的连接吗？

  如果连接已建立， ASA 无需重新检查数据包；大多数匹配的数据包在两个方向都可以通过“快速”路径。快速路径负责执行以下任务：

  – IP 校验和验证
  – 会话查找
  – TCP 序列号检查
  – 基于现有会话的 NAT 转换
  – 第 3 层和第 4 层报头调整

  需要第 7 层检测的协议的数据包也可以通过快速路径。

  某些建立的会话数据包必须继续通过会话管理路径或控制平面路径。通过会话管理路径的数据包包括需要检测或内容过滤的 HTTP 数据包。通过控制平面路径的数据包包括需要第 7 层检测的协议的控制数据包。

VPN 功能概述

VPN 是跨过 TCP/IP 网络 （例如互联网）的安全连接，显示为私有连接。这种安全连接称为隧道。 ASA 使用隧道协议来执行以下任务：协商安全参数，创建和管理隧道，封装数据包，通过隧道传输或接收数据包，以及解除数据包封装。 ASA 充当双向隧道终端：它可以接收普通数据包，封装数据包，将数据包发送到隧道的另一端 （在那里，数据包将会解除封装并发送到最终目标）。ASA 还可以接收封装数据包，解除数据包封装并将它们发送到最终目标。ASA 调用各种标准协议来实现这些功能。

ASA 执行以下功能：

- 建立隧道
- 协商隧道参数
- 对用户进行身份验证
- 分配用户地址
- 加密和解密数据
- 管理安全密钥
- 管理通过隧道的数据传输
- 作为隧道终端或路由器管理出站和出站数据传输

ASA 调用各种标准协议来实现这些功能。

安全情景概述

可以将一个 ASA 分区到多个虚拟设备中，此类设备称为安全情景。每个情景都是一个独立设备，拥有自己的安全策略、接口和管理员。多情景类似于拥有多台独立设备。多情景模式支持很多功能，包括路由表、防火墙功能、 IPS 和管理；但是，有些功能不受支持。有关详细信息，请参阅讲述功能的章节。

在多情景模式中，ASA 包括每个情景的配置，这些配置用于识别安全策略、接口以及可在独立设备上配置的几乎所有选项。系统管理员可在系统配置中配置情景以添加和管理情景；系统配置类似于单模式配置，都是启动配置。系统配置可识别 ASA 的基本设置。系统配置本身不包括任何网络接口或网络设置；相反，当系统需要访问网络资源时（例如，从服务器下载情景），它将使用被指定为管理员情景的情景之一。

管理员情景类似于任何其他情景，唯一不同之处在于，当用户登录管理员情景时，该用户拥有系统管理员权限并能访问系统和所有其他情景。

ASA 集群概述

通过 ASA 集群，可以将多台 ASA 组合成一个逻辑设备。集群具有单个设备的全部便捷性 （管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。

只能在主设备上执行所有配置 （引导配置除外）；然后，配置将被复制到成员设备中。

特殊的服务和传统服务

对于某些服务，可以在主配置指南和联机帮助以外找到相关文档。有关完整指南的列表，请访问：

http://www.cisco.com/go/asadocs

- 第 1-12 页的特殊服务指南
- 第 1-12 页的传统服务指南

特殊服务指南

特殊服务使 ASA 可以与其他思科产品实现互操作；例如，为电话服务提供安全代理 （统一通信），同时提供僵尸网络流量过滤和思科更新服务器上的动态数据库，或者为思科网络安全设备提供 WCCP 服务。某些特殊服务在单独的指南中进行介绍。

传统服务指南

ASA 仍支持传统服务，但可能还有更好的替代服务可供使用。传统服务在单独的指南中进行介绍。

第 2 章

入门

本章介绍如何开始使用思科 ASA。

- 第 2-1 页的访问命令行界面的控制台
- 第 2-6 页的配置 ASDM 访问
- 第 2-11 页的启动 ASDM
- 第 2-12 页的出厂默认配置
- 第 2-15 页的处理配置
- 第 2-19 页的将配置更改应用于连接
- 第 2-19 页的重新加载 ASA

访问命令行界面的控制台

对于初始配置，请从控制台端口直接访问 CLI。然后，可根据第 35 章，“管理访问”，使用 Telnet 或 SSH 配置远程访问。如果系统已处于多情景模式，则访问控制台端口会将您引导至系统执行空间。

注 有关 ASAv 控制台访问，请参阅 《ASAv 快速入门指南》。

- 第 2-1 页的访问设备控制台
- 第 2-2 页的访问 ASA 服务模块控制台

访问设备控制台

按照以下步骤访问设备控制台。

操作步骤

步骤 1 使用提供的控制台电缆将个人电脑连接到控制台端口，并使用设置为 9600 波特、8 数据位、无奇偶校验、1 停止位、无流量控制的终端仿真器连接到控制台。

有关控制台电缆的详细信息，请参阅 ASA 的硬件指南。

步骤 2　按 **Enter** 键查看以下提示符：

ciscoasa>

该提示符表明您正处于用户 EXEC 模式。从用户 EXEC 模式仅能获取基本命令。

步骤 3　如要访问特权 EXEC 模块，请输入以下命令：

```
ciscoasa> enable
```

系统将显示以下提示符：

```
Password:
```

在特权 EXEC 模式中，所有非配置命令均可用。还可从特权 EXEC 模式进入配置模式。

步骤 4　在提示符处输入启用密码。

默认情况下，密码为空，可按 **Enter** 键继续。如要更改启用密码，请参阅第 13-1 页的设置主机名、域名及启用和 Telnet 密码。

提示符更改为：

```
ciscoasa#
```

如要退出特权模式，请输入 **disable**、 **exit** 或 **quit** 命令。

步骤 5　如要访问全局配置模式，请输入以下命令：

```
ciscoasa# configure terminal
```

提示符将会变为以下形式：

```
ciscoasa(config)#
```

可从全局配置模式开始配置 ASA。如要退出全局配置模式，请输入 **exit**、 **quit** 或 **end** 命令。

访问 ASA 服务模块控制台

对于初始配置，请访问命令行界面，只需依次连接到交换机（至控制台端口或使用 Telnet 或 SSH 远程连接）和 ASASM。本节介绍如何访问 ASASM CLI。

- 第 2-2 页的有关连接方法
- 第 2-3 页的登录 ASA 服务模块
- 第 2-5 页的注销控制台会话
- 第 2-5 页的断开活动控制台连接
- 第 2-6 页的注销 Telnet 会话

有关连接方法

从交换机 CLI，可使用两种方法连接到 ASASM：

- 虚拟控制台连接 - 通过使用 **service-module session** 命令，创建至 ASASM 的虚拟控制台连接，该连接具有实际控制台连接的所有优势和限制。

  优势包括：

  – 连接在重新加载之间是持久性的，且不会超时。

  – 可在 ASASM 重新加载期间保持连接及查看启动消息。

– 如果 ASASM 无法加载映像，则可访问 ROMMON。

– 不需要初始密码配置。

限制包括：

– 连接缓慢 （9600 波特）。

– 每次只能激活一个控制台连接。

– 返回终端服务器提示符的转义序列为 **Ctrl-Shift-6**, **x** 时，不能与终端服务器一起使用该命令。 **Ctrl - Shift - 6**, **x** 也是 ASASM 控制台和返回交换机提示符的转义序列。因此，如果在这种情况下尝试退出 ASASM 控制台，反而会一直退回到终端服务器提示符。如果将终端服务器重新连接到交换机，则 ASASM 控制台会话仍将处于活动状态；绝不能退出到交换机提示符。必须使用直接串行连接使控制台返回交换机提示符。在此情况下，要么更改终端服务器或 Cisco IOS 软件中的交换机转义字符，要么换用 Telnet **session** 命令。

注　由于控制台连接具有持久性，因此，如果未正确注销 ASASM，则该连接存在的时间可能超过预期。如果其他人要登录，则需断开现有连接。

- Telnet 连接 - 通过使用 **session** 命令，创建至 ASASM 的 Telnet 连接。

注　不能使用该方法为新 ASASM 进行连接；该方法要求在 ASASM 上配置 Telnet 登录密码 （无默认密码）。使用 **passwd** 命令设置密码后，就可使用该方法。

优势包括：

– 可同时拥有多个与 ASASM 的会话。

– Telnet 会话是快速连接。

限制包括：

– ASASM 重新加载时，Telnet 会话即被终止，并且可能会超时。

– 您不能访问 ASASM，直到它完成加载；不能访问 ROMMON。

– 必须先设置 Telnet 登录密码；没有默认密码。

登录 ASA 服务模块

对于初始配置，请访问命令行界面，只需依次连接到交换机 （至交换机控制台端口或使用 Telnet 或 SSH 远程连接）和 ASASM。

如果系统已处于多情景模式，则从交换机访问 ASASM 会将您引导至系统执行空间。

然后，可使用 Telnet 或 SSH 配置直接到 ASASM 的远程访问。

操作步骤

步骤 1　从交换机执行以下操作之一：

- 可用于初始访问 - 从交换机 CLI，输入该命令以获得对 ASASM 的控制台访问：

service - module session [**switch** {**1** | **2**}] **slot** *number*

示例：

```
Router# service-module session slot 3
ciscoasa>
```

对于 VSS 中的交换机，请输入 **switch** 参数。

如要查看模块插槽编号，请在交换机提示符处输入 **show module** 命令。

将访问用户 EXEC 模式。

- 在配置登录密码之后可用 - 从交换机 CLI，输入该命令至背板上 ASASM 的 Telnet：

  session [**switch** {**1** | **2**}] **slot** *number* **processor 1**

  系统提示输入登录密码：

  ```
  ciscoasa passwd:
  ```

  示例：

  ```
  Router# session slot 3 processor 1
  ciscoasa passwd: cisco
  ciscoasa>
  ```

  对于 VSS 中的交换机，请输入 **switch** 参数。

  ASASM 不支持其他服务模块支持的 **session** *slot* **processor 0** 命令；ASASM 没有处理器 0。

  如要查看模块插槽编号，请在交换机提示符处输入 **show module** 命令。

  输入 ASASM 的登录密码。使用 **passwd** 命令设置密码。没有默认密码。

  将访问用户 EXEC 模式。

步骤 2　访问特权 EXEC 模式 （拥有最高权限级别）：

enable

示例：

```
ciscoasa> enable
Password:
ciscoasa#
```

在提示符处输入启用密码。默认情况下，密码为空。

如要退出特权 EXEC 模式，请输入 **disable**、 **exit** 或 **quit** 命令。

步骤 3　访问全局配置模式：

configure terminal

如要退出全局配置模式，请输入 **disable**、 **exit** 或 **quit** 命令。

相关主题

- 第 35-1 页的配置 ASDM、 Telnet 或 SSH 的 ASA 访问
- 第 13-1 页的设置主机名、域名及启用和 Telnet 密码

注销控制台会话

如果不注销 ASASM，则控制台连接将继续存在；没有超时。如要结束 ASASM 控制台会话并访问交换机 CLI，请执行以下步骤。

要断开其他用户可能无意保持打开的活动连接，请参阅第 2-5 页的断开活动控制台连接。

操作步骤

步骤 1　如要返回交换机 CLI，请键入以下信息：

Ctrl-Shift-6, **x**

您将返回交换机提示符：

```
asasm# [Ctrl-Shift-6, x]
Router#
```

注　美式和英式键盘的 Shift-6 操作可输出脱字符 (^)。如果使用其他键盘且不能输入脱字符 (^) 作为独立字符，则可暂时或永久地将转义字符更改为另一字符。使用 **terminal escape-character** *ascii_number* 命令 （用于本次会话更改）或 **default escape-character** *ascii_number* 命令 （永久更改）。例如，要将当前会话的序列更改为 **ctrl-w**, **x**，请输入 **terminal escape-character 23**。

断开活动控制台连接

由于控制台连接具有持久性，因此，如果未正确注销 ASASM，则该连接存在的时间可能超过预期。如果其他人要登录，则需断开现有连接。

操作步骤

步骤 1　从交换机 CLI，使用 **show users** 命令显示已连接用户。控制台用户称为“con”。主机地址显示为 127.0.0.*slot*0，其中，*slot* 是模块的插槽编号。

```
Router# show users
```

例如，以下命令输出在模块插槽 2 中 0 行上显示用户“con”：

```
Router# show users
Line       User       Host(s)              Idle       Location
*  0       con 0     127.0.0.20            00:00:02
```

步骤 2　如要清除与控制台连接的行，请输入以下命令：

```
Router# clear line number
```

例如：

```
Router# clear line 0
```

注销 Telnet 会话

如要结束 Telnet 会话并访问交换机 CLI，请执行以下步骤。

操作步骤

步骤 1　如要返回交换机 CLI，请从 ASASM 特权或用户 EXEC 模式键入 **exit**。如果正处于配置模式，可重复输入 **exit**，直到退出 Telnet 会话。

您将返回交换机提示符：

```
asasm# exit
Router#
```

注　或者，也可使用转义序列 **Ctrl-Shift-6**, **x** 转义 Telnet 会话；该转义序列可供您通过在交换机提示符处按 **Enter** 键恢复 Telnet 会话。要从交换机断开 Telnet 会话，请在交换机 CLI 中输入 **disconnect**。如果不断开会话，它最终会根据 ASASM 配置超时。

配置 ASDM 访问

本节介绍如何通过默认配置访问 ASDM，以及在没有默认配置的情况下如何配置访问。

- 第 2-6 页的使用出厂默认配置进行 ASDM 访问 （设备、 ASAv）
- 第 2-7 页的为设备和 ASAv 自定义 ASDM 访问
- 第 2-9 页的为 ASA 服务模块配置 ASDM 访问

使用出厂默认配置进行 ASDM 访问 （设备、 ASAv）

通过出厂默认配置， ASDM 连接已预配置默认网络设置。

操作步骤

步骤 1　使用以下接口和网络设置连接到 ASDM：

- 管理接口取决于设备型号：
  - ASA 5512-X 和更高版本 - 要连接到 ASDM 的接口是 Management 0/0。
  - ASAv- 要连接到 ASDM 的接口是 Management 0/0。
- 默认管理地址为：
  - ASA 设备 - 192.168.1.1.
  - ASAv- 在部署期间设置管理接口 IP 地址。
- 允许访问 ASDM 的客户端：
  - ASA 设备 - 客户端必须在 192.168.1.0/24 网络上。默认配置启用 DHCP，以便向管理工作站分配此范围内的 IP 地址。
  - ASAv- 在部署期间设置管理客户端 IP 地址。ASAv 不充当已连接客户端的 DHCP 服务器。

注　如果切换至多情景模式，则可使用上述网络设置从管理员情景访问 ASDM。

相关主题

- 第 2-12 页的出厂默认配置
- 第 6-14 页的启用或禁用多情景模式
- 第 2-11 页的启动 ASDM

为设备和 ASAv 自定义 ASDM 访问

如果*一个或多个*以下条件适用，可使用该操作步骤：

- 没有出厂默认配置
- 想要更改管理 IP 地址
- 想要更改为透明防火墙模式
- 想要更改为多情景模式

对于单一路由模式，为了实现快速轻松的 ASDM 访问，我们建议应用出厂默认配置，但可选择设置您自己的管理 IP 地址。只有您有特殊需求 （如设置透明或多情景模式）或有需要保留的其他配置时，才能使用本节所述操作步骤。

操作步骤

步骤 1　在控制台端口访问 CLI。

步骤 2　（可选）启用透明防火墙模式：

该命令可清除配置。

```
firewall transparent
```

步骤 3　配置 Management 接口

```
interface management id
   nameif name
   security-level level
   no shutdown
   ip address ip_address mask
```

示例：

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

security-level 是介于 1 到 100 之间的数字，其中，100 为最安全级别。

步骤 4　（对于直连管理主机）为管理网络设置 DHCP 池：

```
dhcpd address ip_address-ip_address
interface_name
dhcpd enable interface_name
```

示例：

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

确保此范围内不包括管理地址。

步骤 5　（对于远程管理主机）配置管理主机路由：

route *management_ifc management_host_ip mask gateway_ip* **1**

示例：

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

步骤 6　为 ASDM 启用 HTTP 服务器：

http server enable

步骤 7　允许管理主机访问 ASDM：

http *ip_address mask interface_name*

示例：

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

步骤 8　保存配置：

write memory

步骤 9　（可选）将模式设置为多模式：

mode multiple

经系统提示时，请确认要将现有配置转换为管理员情景。然后系统将提示重新加载 ASA。

示例

以下配置将防火墙模式转换为透明模式、配置 Management 0/0 接口并为管理主机启用 ASDM：

```
firewall transparent
interface management 0/0
    ip address 192.168.1.1 255.255.255.0
    nameif management
    security-level 100
    no shutdown
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

相关主题

- 第 2-12 页的还原出厂默认配置
- 第 5-8 页的设置防火墙模式
- 第 2-1 页的访问设备控制台
- 第 2-11 页的启动 ASDM
- 第 6 章，“多情景模式”

为 ASA 服务模块配置 ASDM 访问

由于 ASASM 没有物理接口，因此它不会预配置 ASDM 访问；必须使用 ASASM 上的 CLI 配置 ASDM 访问。要为 ASDM 访问配置 ASASM，请执行以下步骤。

准备工作

根据 《ASASM 快速入门指南》将 VLAN 接口分配至 ASASM。

操作步骤

步骤 1　连接到 ASASM 并访问全局配置模式。

步骤 2　（可选）启用透明防火墙模式：

```
firewall transparent
```

该命令可清除配置。

步骤 3　视乎您的模式，执行以下操作之一，以配置管理接口：

- 路由模式 - 在路由模式中配置接口：

```
interface vlan number
   ip address ip_address [mask]
   nameif name
   security-level level
```

示例：

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level 是介于 1 到 100 之间的数字，其中，100 为最安全级别。

- 透明模式 - 配置网桥虚拟接口并分配管理 VLAN 至网桥组：

```
interface bvi number
   ip address ip_address [mask]

interface vlan number
   bridge-group bvi_number
   nameif name
   security-level level
```

示例：

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# bridge-group 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level 是介于 1 到 100 之间的数字，其中，100 为最安全级别。

步骤 4　（对于直接管理主机）为管理接口网络上的管理主机启用 DHCP：

```
dhcpd address ip_address-ip_address
interface_name
dhcpd enable interface_name
```

示例：

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 inside
ciscoasa(config)# dhcpd enable inside
```

确保此范围内不包括管理地址。

步骤 5　（对于远程管理主机）配置管理主机路由：

route *management_ifc management_host_ip mask gateway_ip* **1**

示例：

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50
```

步骤 6　为 ASDM 启用 HTTP 服务器：

http server enable

步骤 7　允许管理主机访问 ASDM：

http *ip_address mask interface_name*

示例：

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

步骤 8　保存配置：

write memory

步骤 9　（可选）将模式设置为多模式：

mode multiple

经系统提示时，请确认要将现有配置转换为管理员情景。然后系统将提示重新加载 ASASM。

示例

以下路由模式配置可配置 VLAN 1 接口并为管理主机启用 ASDM：

```
interface vlan 1
    nameif inside
    ip address 192.168.1.1 255.255.255.0
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

以下配置可将防火墙模式转换为透明模式、配置 VLAN 1 接口并将其分配给 BVI 1，以及为管理主机启用 ASDM：

```
firewall transparent
interface bvi 1
    ip address 192.168.1.1 255.255.255.0
interface vlan 1
    bridge-group 1
    nameif inside
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

相关主题

- 第 2-2 页的访问 ASA 服务模块控制台
- 第 6 章，“多情景模式”
- 第 5-8 页的设置防火墙模式

启动 ASDM

可使用以下两种方法启动 ASDM：

- ASDM-IDM 启动程序 - 该启动程序是使用网络浏览器从 ASA 中下载的应用，可用于连接任何 ASA IP 地址。如果想要连接其他 ASA，无需重新下载该启动程序。通过该启动程序，还可使用本地下载的文件在演示模式中运行虚拟 ASDM。
- Java Web Start - 对于您管理的每个 ASA，均需要与网络浏览器连接，然后保存或启动 Java Web Start 应用。或者，可将快捷方式保存到个人电脑；但是每个 ASA IP 地址均单独的快捷方式。

在 ASDM 内，可选择另一个要管理的 ASA IP 地址；该启动程序与 Java Web Start 功能之间的差异主要在于最初连接 ASA 和启动 ASDM 的方式。

ASDM 允许多台个人电脑或工作站每台拥有一个用同一 ASA 软件打开的浏览器会话。单个 ASA 可在单一路由模式中支持多达五个并发 ASDM 会话。对于指定的 ASA，每台个人电脑或工作站的每个浏览器仅支持一个会话。在多情景模式中，每个情景支持五个并发 ASDM 会话，每个ASA 最多可有 32 个连接。

本节介绍最初如何连接 ASDM，以及如何使用启动程序或 Java Web Start 启动 ASDM。

操作步骤

步骤 1　在指定为 ASDM 客户端的个人电脑上，输入以下 URL：

https://*asa_ip_address***/admin**

系统将显示 ASDM 启动页面和以下按钮：

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

步骤 2　如要下载启动程序，请执行以下操作：

a. 点击 **Install ASDM Launcher and Run ASDM**。

b. 将用户名和密码字段留空 （适用于新安装），然后点击 **OK**。如果未配置 HTTPS 身份验证，您可以在没有用户名和**启用**密码 （默认为空）的情况下获得对 ASDM 的访问权限。注意：如果已启用 HTTPS 身份验证，请输入用户名和关联密码。

c. 将安装程序保存到个人电脑，然后启动安装程序。安装完成后， ASDM-IDM Launcher 将自动打开。

d. 输入管理 IP 地址，将用户名和密码留空 （适用于新安装），然后点击 **OK**。注意：如果已启用 HTTPS 身份验证，请输入用户名和关联密码。

步骤 3　如要使用 Java Web Start，请执行以下操作：

a. 点击 **Run ASDM** 或 **Run Startup Wizard**。

b. 系统提示后，将快捷方式保存到个人电脑上。或者，您也可以选择将其打开，而不是保存。

c. 从该快捷方式启动 Java Web Start。

d. 根据显示的对话框接受所有证书。系统将显示思科 ASDM-IDM 启动程序。

e. 将用户名和密码留空 （适用于新安装），然后点击 **OK**。注意：如果已启用 HTTPS 身份验证，请输入用户名和关联密码。

出厂默认配置

出厂默认配置是思科应用于新 ASA 的配置。

- ASA 设备 - 出厂默认配置可配置管理接口，以便可以使用 ASDM 与其连接，然后通过它完成配置。
- ASAv- 在部署过程中，部署配置 （初始虚拟部署设置）可配置管理接口，以便可以使用 ASDM 与其连接，然后通过它完成配置。还可配置故障转移 IP 地址。还可应用“出厂默认”配置 （如需）。
- ASASM- 无默认配置。要开始配置，请参阅第 2-2 页的访问 ASA 服务模块控制台。

出厂默认配置仅可用于路由防火墙模式和单一情景模式。

注 除映像文件和 （隐藏）默认配置外，以下文件夹和文件是闪存中的标准配置：log/, crypto_archive/ 和 coredumpinfo/coredump.cfg。这些文件上的日期可能不匹配闪存中映像文件的日期。这些文件有助于潜在的故障排除；它们不表示已发生故障。

- 第 2-12 页的还原出厂默认配置
- 第 2-13 页的还原 ASAv 部署配置
- 第 2-14 页的 ASA 设备默认配置
- 第 2-14 页的 ASAv 部署配置

还原出厂默认配置

本节介绍如何还原出厂默认配置。对于 ASAv，该操作步骤可擦除部署配置并应用对于各 ASA 设备均相同的出厂默认配置。

注 在 ASASM 上，还原出厂默认配置即可轻松擦除配置；无出厂默认配置。

准备工作

该功能仅可用于路由防火墙模式；透明模式不支持接口的 IP 地址。此外，该功能仅可用于单一情景模式；已清除配置的 ASA 没有任何定义的情景可使用该功能自动进行配置。

操作步骤

步骤 1 还原出厂默认配置：

configure factory-default [*ip_address* [*mask*]]

示例：

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

如果指定 *ip_address*，则根据设备型号设置内部或管理接口 IP 地址，而不是使用默认 IP 地址 192.168.1.1。**http** 命令使用您指定的子网。与此相似，**dhcpd address** 命令范围包括您指定子网中的地址。

该命令还可清除 **boot system** 命令（如存在）以及其余配置。**boot system** 命令可供您从特定映像上启动，包括外部闪存卡上的映像。下次在还原出厂配置后重新加载 ASA 时，它将从内部闪存的第一个映像启动；如果内部闪存中无映像，ASA 将不启动。

步骤 2　将默认配置保存到闪存：

```
write memory
```

该命令将运行配置保存到启动配置的默认位置，即使以前已将 **boot config** 命令配置为设置另一个位置；配置清除后，该路径也将清除。

还原 ASAv 部署配置

本节介绍如何还原 ASAv 部署配置。

操作步骤

步骤 1　为了执行故障转移，请关闭备用设备。

为了防止激活备用设备，必须将其关闭。如使备用设备保持开启，则当您擦除主用设备配置时，备用设备将激活。以前的主用设备通过转移故障链路重新加载和重新连接时，原配置将从新主用设备同步，擦除您需要的部署配置。

步骤 2　重新加载后，还原部署配置。为了执行故障转移，请在主用设备上输入以下命令：

```
write erase
```

注　ASAv 启动当前运行的映像，因此，不会恢复为原始启动映像。如要使用原始引导映像，请参阅 **boot image** 命令。

请勿保存该配置。

步骤 3　重新加载 ASAv，并加载部署配置：

```
reload
```

步骤 4　为了执行故障转移，请开启备用设备。

主用设备重新加载后，开启备用设备。部署配置将同步备用设备。

ASA 设备默认配置

ASA 设备的默认出厂配置可配置以下方面：

  – 管理接口 - Management 0/0（管理）。

- IP 地址 - 管理地址为 192.168.1.1/24。
- DHCP 服务器 - 已为管理主机启用，以便连接到管理接口的个人电脑可接收介于 192.168.1.2 和 192.168.1.254 之间的地址。
- ASDM 访问 - 允许访问管理主机。

该配置包括以下命令：

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

ASAv 部署配置

部署 ASAv 时，可预设置许多可供您使用 ASDM 连接到 Management 0/0 接口的参数。典型配置包括以下设置：

- Management 0/0 接口：
  – 命名为“management”
  – IP 地址或 DHCP
  – 安全级别为 0
  – 仅管理
- 通过默认网关从管理接口到管理主机 IP 地址的静态路由
- 已启用 ASDM 服务器
- 管理主机 IP 地址的 ASDM 访问
- （可选）GigabitEthernet 0/8 的故障转移链路 IP 地址和 Management0/0 备用 IP 地址。

有关独立设备，请参阅以下配置：

```
interface Management0/0
 nameif management
 security-level 0
 ip address ip_address
 management-only
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
```

有关故障转移对中的主要设备，请参阅以下配置：

```
interface Management0/0
 nameif management
 security-level 0
 ip address ip_address standby standby_ip
 management-only
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

处理配置

本节介绍如何处理配置。 ASA 从文本文件 （称为启动配置）加载配置。默认情况下，该文件作为隐藏文件驻留在内部闪存中。但是，也可为启动配置指定不同路径。

输入命令时，仅对内存中运行配置进行更改。必须将运行配置手动保存到启动配置，以便重新启动后您的更改仍保持有效。

本节中的信息适用于单一安全情景和多安全情景，除非另有说明。

- 第 2-15 页的保存配置更改
- 第 2-17 页的将启动配置复制到运行配置
- 第 2-17 页的查看配置
- 第 2-18 页的清除和移除配置设置
- 第 2-18 页的离线创建文本配置文件

保存配置更改

本节介绍如何保存配置。

- 第 2-15 页的在单一情景模式中保存配置更改
- 第 2-16 页的在多情景模式中保存配置更改

在单一情景模式中保存配置更改

如要将运行配置保存到启动配置，请执行以下操作步骤。

操作步骤

步骤 1　将运行配置保存到启动配置：

```
write memory
```

注　**copy running-config startup-config** 命令等同于 **write memory** 命令。

在多情景模式中保存配置更改

可分别保存每个情景 （和系统）配置，或者，也可同时保存所有情景配置。

- 第 2-16 页的分别保存每个情景和系统
- 第 2-16 页的同时保存所有情景配置

分别保存每个情景和系统

使用以下操作步骤保存系统或情景配置。

操作步骤

步骤 1　从情景或系统中，将运行配置保存到启动配置：

```
write memory
```

对于多情景模式，情景启动配置可能驻留在外部服务器。在此情况下，ASA 将配置保存回在情景 URL 中确定的服务器，HTTP 或 HTTPS URL（不允许将配置保存到服务器）除外。

注　**copy running-config startup-config** 命令等同于 **write memory** 命令。

同时保存所有情景配置

使用以下操作步骤同时保存所有情景配置，以及系统配置。

操作步骤

步骤 1　从系统执行空间，将运行配置保存到所有情景的启动配置和系统配置：

```
write memory all [/noconfirm]
```

如果不输入 **/noconfirm** 关键字，则将看到以下提示符：

```
Are you sure [Y/N]:
```

输入 **Y** 后，ASA 将保存系统配置和每个情景。情景启动配置可能驻留在外部服务器上。在此情况下，ASA 将配置保存回在情景 URL 中确定的服务器，HTTP 或 HTTPS URL（不允许将配置保存到服务器）除外。

ASA 保存每个情景后，系统将显示以下消息：

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

有时，情景会因错误而未保存。有关错误，请参阅以下信息：

- 对于因内存不足而未保存的情景，系统将显示以下消息：

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- 对于因远程目标不可达而未保存的情景，系统将显示以下消息：

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- 如果情景由于已被锁定而未保存，系统将显示以下消息：

  ```
  Unable to save the configuration for the following contexts as these contexts are
  locked.
  context ‘a’ , context ‘x’ , context ‘z’ .
  ```

  只有其他用户已保存配置或正在删除情景时，情景才会锁定。

- 对于因启动配置为只读配置而不能保存的情景（例如，HTTP 服务器），在将所有其他消息的末尾打印以下消息报告：

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context ‘a’ , context ‘b’ , context ‘c’ .
  ```

- 对于因闪存扇区错误而未保存的情景，系统将显示以下消息：

  ```
  The context 'context a' could not be saved due to Unknown errors
  ```

将启动配置复制到运行配置

使用以下命令之一，将新启动配置复制到运行配置：

- **copy startup-config running-config**

  合并启动配置与运行配置。合并会将新配置中的所有新命令添加至运行配置。如果配置相同，则不会发生更改。如果命令有冲突，或者如果命令影响情景运行，则合并的效果取决于命令。可能出现错误，或者出现意外结果。

- **reload**

  重新加载 ASA，其加载启动配置并丢弃运行配置。

- **clear configure all** and then **copy startup-config running-config**

  加载启动配置并丢弃运行配置，无需重新加载。

查看配置

以下命令可供您查看运行配置和启动配置：

- **show running-config**

  查看运行配置。

- **show running-config** *command*

  查看特定命令的运行配置。

- **show startup-config**

  查看启动配置。

清除和移除配置设置

如要擦除设置，请输入以下命令之一：

- **clear configure** *configurationcommand* [*level2configurationcommand*]

  清除指定命令的所有配置。如果只想清除特定版本命令的配置，则可输入 *level2configurationcommand* 的值。

  例如，要清除所有 **aaa** 命令的配置，请输入以下命令：

  ```
  ciscoasa(config)# clear configure aaa
  ```

  要仅清除 **aaa authentication** 命令的配置，请输入以下命令：

  ```
  ciscoasa(config)# clear configure aaa authentication
  ```

- **no** *configurationcommand* [*level2configurationcommand*] *qualifier*

  禁用命令的特定参数或选项。在此情况下，可使用 **no** 命令移除 *qualifier* 确定的特定配置。

  例如，要移除特定 **access - list** 命令，请输入足够命令对其进行唯一标识；可能必须输入整个命令：

  ```
  ciscoasa(config)# no access-list abc extended permit icmp any any object-group
  obj_icmp_1
  ```

- **write erase**

  擦除启动配置。

注　对于 ASAv，该命令可在重新加载后还原部署配置。要完全擦除配置，请使用 **clear configure all** 命令。

- **clear configure all**

  擦除运行配置。

注　在多情景模式中，如果从系统配置输入 **clear configure all**，还将移除所有情景并使它们停止运行。情景配置文件将不擦除，仍保留在原始位置。

该命令还可清除 **boot system** 命令（如存在）以及其余配置。**boot system** 命令可供您从特定映像上启动，包括外部闪存卡上的映像。下次重新加载 ASA 时，它将从内部闪存的第一个映像启动；如果内部闪存中无映像，则 ASA 将不启动。

离线创建文本配置文件

本指南介绍如何使用 CLI 配置 ASA；保存命令时，更改将写入文本文件。但是，如果不使用 CLI，则可以直接在个人电脑上编辑文本文件，并将配置完整地或逐行粘贴在配置模式命令行提示符处。或者，也可将文本文件下载至 ASA 内部闪存。有关如何将配置文件下载至 ASA 的信息，请参阅第 36 章，“软件和配置”。

在大多数情况下，本指南所述的命令之前都有 CLI 提示符。以下示例中的提示符为“ciscoasa(config)#”：

```
ciscoasa(config)# context a
```

在文本配置文件中，系统不提示您输入命令，因此，提示符省略如下：

```
context a
```

有关格式化文件的详细信息，请参阅第 42 章，“使用命令行界面”

将配置更改应用于连接

更改配置的安全策略后，所有*新*连接将使用新安全策略。现有连接将继续使用连接建立时配置的策略。原连接的 **show** 命令输出反映原配置，在某些情况下将不包括关于原连接的数据。

例如，如果要从接口移除 QoS **服务策略**，然后重新添加修改版本，则 **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；旧策略的现有连接不再显示在命令输出中。

如要确保所有连接使用新策略，需要断开当前连接，以便其使用新策略重新连接。

如要断开连接，请输入以下命令之一：

- **clear local-host** [*ip_address*] [**all**]

  该命令将重新初始化每客户端运行时状态，如连接限制和初始化限制。因此，该命令可移除使用那些限制的任何连接。要查**看**每台主机的所有当前连接，请参阅 show local-hos**t all** 命令。

  如果不带参数，该命令将清除所有受影响的出站连接。要清除入站连接 （包括当前的管理会话），请使用关键字 **all**。要清特定 IP 地址的出站或入站连接，请使用 *ip_address* 参数。

- **clear conn** [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]] [**port** *src_port*[**-***src_port*]] [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[**-***dest_port*]]

  该命令可在任何状态中终止连接。要查**看**所有当前连接，请参阅 **show conn** 命令。

  如果不带参数，该命令将清除所有出站连接。要清除入站连接 （包括当前的管理会话），请使用关键字 **all**。要根据源 IP 地址、目标 IP 地址、端口和/或协议清除特定连接，请指定所需选项。

重新加载 ASA

如要重新加载 ASA，请完成以下操作步骤。

操作步骤

步骤 1　重新加载 ASA：

```
reload
```

注　在多情景模式中，仅可从系统执行空间重新加载。

适用于思科 ASA 服务模块的交换机配置

本章介绍如何配置 Catalyst 6500 系列或思科 7600 系列交换机以便于思科ASA 服务模块 (ASASM) 配合使用。在执行本章所述的操作步骤之前，请先配置交换机的基本属性，包括根据随交换机提供的文档向交换机端口分配 VLAN。

- 第 3-1 页的有关交换机的信息
- 第 3-3 页的准则和限制
- 第 3-4 页的验证模块安装
- 第 3-5 页的将 VLAN 分配给 ASA 服务模块
- 第 3-7 页的将 MSFC 用作直连路由器 (SVI)
- 第 3-8 页的为 ASA 故障转移配置交换机
- 第 3-9 页的重置 ASA 服务模块
- 第 3-10 页的监控 ASA 服务模块
- 第 3-12 页的与 ASA 服务模块配合使用的交换机的功能历史记录

有关交换机的信息

- 第 3-1 页的受支持的交换机硬件和软件
- 第 3-2 页的背板连接
- 第 3-2 页的 ASA 与思科 IOS 之间的功能交互

受支持的交换机硬件和软件

可以在 Catalyst 6500 系列和思科 7600 系列交换机上安装 ASASM。交换机由一个交换机 （管理引擎）和一个路由器 (MSFC) 组成。

交换机支持在交换机管理引擎和集成 MSFC 路由器上使用思科 IOS 软件。

注 不支持 Catalyst 操作系统软件。

ASASM 运行自己的操作系统。

注　由于 ASASM 运行自己的操作系统，因此，升级思科 IOS 软件不会影响 ASASM 的运行。

要查看 ASASM 和思科 IOS 版本的硬件和软件兼容性矩阵，请通过以下链接参阅 *《思科 ASA 系列硬件和软件兼容性》*：

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

背板连接

ASASM 与交换机之间的连接是一个 20-GB 的接口。

ASA 与思科 IOS 之间的功能交互

某些 ASASM 功能可与思科 IOS 功能进行交互。以下功能涉及思科 IOS 软件：

- 虚拟交换系统 (VSS) - 不需要进行 ASASM 配置。
- 自动状态 - 如果给定 VLAN 上的最后一个接口出现故障，管理引擎会通知 ASASM，以帮助确定是否需要故障转移交换机。
- 清除故障转移交换机上的管理引擎 MAC 地址表中的条目 - 无需进行 ASASM 配置。
- 版本兼容性 - 如果管理引擎/ASASM 版本兼容性矩阵检查失败， ASASM 将会自动关闭。

有关 SVI 的信息

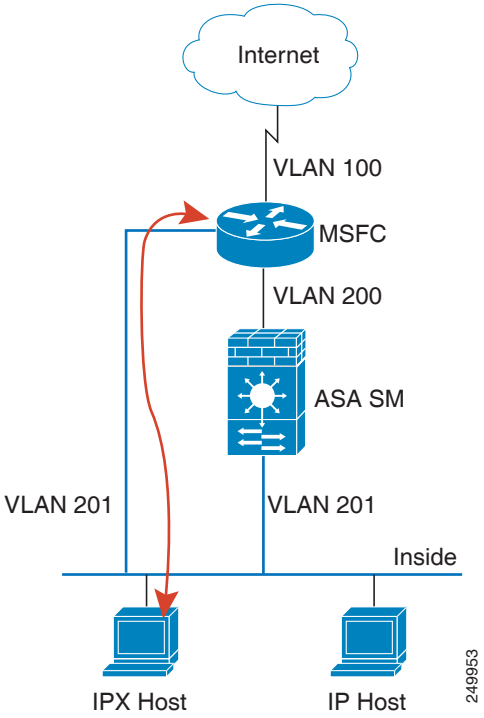
如果要将 MSFC 用作直连路由器（例如，作为模式中 ASASM 外部接口的默认网关），请将一个 ASASM VLAN 接口添加到 MSFC 作为交换虚拟接口 (SVI)。

出于安全原因，默认情况下，可以在 MSFC 与 ASASM 之间配置一个 SVI；可以启用多个 SVI，但务必要确保网络配置正确。

例如，如果使用多个 SVI，您可能会将内部和外部 VLAN 分配给 MSFC，进而意外地允许流量通过 ASASM。

在某些网络环境中，可能需要绕过 ASASM。图 3-1 将同一个以太网段上的 IPX 主机显示为 IP 主机。由于路由防火墙模式中的 ASASM 只处理 IP 流量，并会中断 IPX 之类的其他协议流量（透明防火墙模式可以允许非 IP 流量），因此，您可能希望使 IPX 流量绕过 ASASM。请务必使用仅允许 IPX 流量在 VLAN 201 上通过的访问列表来配置 MSFC。

图 3-1　　适用于 IPX 的多个 SVI



对于多情景模式中的透明防火墙，需要使用多个 SVI，因为每个情景的外部接口都需要有唯一的 VLAN。还可以在路由模式中使用多个 SVI，这样，就无需在外部接口上共享一个 VLAN。

准则和限制

本节包括此功能的准则和限制。

VLAN 准则和限制

- 使用 VLAN ID 2 到 1001。
- 可以将专用 VLAN 与 ASASM 配合使用。将主要 VLAN 分配给 ASASM；ASASM 会自动处理辅助 VLAN 流量。对于此功能，不需要在 ASASM 上进行任何配置；有关详细信息，请参阅交换机配置指南。另请参阅将 VLAN 分配给 ASA 服务模块，第 3-5 页中的示例。
- 不能使用保留的 VLAN。
- 不能使用 VLAN 1。
- 如果要在同一个交换机机箱中使用 ASASM 故障转移，请勿将保留用于故障转移和状态通信的 VLAN 分配给交换机端口。但是，如果要在机箱之间使用故障转移，必须在机箱之间的中继端口中包含 VLAN。
- 如果尚未将 VLAN 分配给 ASASM 就将它们添加到交换机，这些 VLAN 将被存储在管理引擎数据库中，一旦它们添加到交换机，就会被发送到 ASASM。
- 可以在将 VLAN 分配到交换机之前，在 ASASM 配置中配置 VLAN。请注意，交换机将 VLAN 发送到 ASASM 后，VLAN 默认为可使用管理权限在 ASASM 上打开，无论您是否在 ASASM 配置中将其关闭。在这种情况下，您需要再次将其关闭。

SPAN 反射器准则

在思科 IOS 软件 12.2SXJ1 及更低版本中，对于交换机中的每个 ASASM，SPAN 反射器功能已启用。此功能允许来自 ASASM 的组播流量（以及需要中央重写引擎的其他流量）进行交换。SPAN 反射器功能使用一个 SPAN 会话。要禁用此功能，请输入以下命令：

```
Router(config)# no monitor session servicemodule
```

验证模块安装

如要验证交换机已确认 ASASM 并已使其进入联机状态，请输入以下命令。

详细步骤

命令	用途
show module [**switch** {**1** |**2**}] [*mod-num* | **all**]	显示模块信息。对于 VSS 中的交换机，请输入 **switch** 关键字。
示例： `Router# show module 1`	确保 Status 列中对 ASASM 显示“Ok”。

示例

以下是 **show module** 命令的输出示例：

```
Router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
 2    3  ASA Service Module                     WS-SVC-ASA-SM1     SAD143502E8
 4    3  ASA Service Module                     WS-SVC-ASA-SM1     SAD135101Z9
 5    5  Supervisor Engine 720 10GE (Active)    VS-S720-10G        SAL12426KB1
 6   16  CEF720 16 port 10GE                    WS-X6716-10GE      SAL1442WZD1

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
 2  0022.bdd4.016f to 0022.bdd4.017e   0.201 12.2(2010080 12.2(2010121 Ok
 4  0022.bdd3.f64e to 0022.bdd3.f655   0.109 12.2(2010080 12.2(2010121 PwrDown
 5  0019.e8bb.7b0c to 0019.e8bb.7b13   2.0   8.5(2)       12.2(2010121 Ok
 6  f866.f220.5760 to f866.f220.576f   1.0   12.2(18r)S1  12.2(2010121 Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
2/0 ASA Application Processor   SVC-APP-PROC-1     SAD1436015D  0.202  Other
4/0 ASA Application Processor   SVC-APP-INT-1      SAD141002AK  0.106  PwrDown
 5  Policy Feature Card 3       VS-F6K-PFC3C       SAL12437BM2  1.0    Ok
 5  MSFC3 Daughterboard         VS-F6K-MSFC3       SAL12426DE3  1.0    Ok
 6  Distributed Forwarding Card WS-F6700-DFC3C     SAL1443XRDC  1.4    Ok

Base PID:
Mod  Model            Serial No.
---- -----------      ----------
 2 WS-SVC-APP-HW-1    SAD143502E8
 4 TRIFECTA           SAD135101Z9

Mod  Online Diag Status
---- -------------------
 2  Pass
```

```
2/0 Not Applicable
 4  Not Applicable
4/0 Not Applicable
 5  Pass
 6  Pass
```

将 VLAN 分配给 ASA 服务模块

本节介绍如何将 VLAN 分配给 ASASM。 ASASM 不包含任何外部物理接口。相反，它使用 VLAN 接口。将 VLAN 分配到 ASASM 的过程与将 VLAN 分配到交换机端口的过程类似；ASASM 包含用于模式中交换机交换矩阵模块 （如果有）的内部接口或共享总线。

先决条件

有关将 VLAN 添加到交换机以及将 VLAN 分配到交换机端口的信息，请参阅交换机文档。

准则

- 最多可以向每个 ASASM 分配 16 个防火墙 VLAN 组。（可以在思科 IOS 软件中创建多于 16 个 VLAN 组，但最多只能向每个 ASASM 分配 16 个。）例如，可以将所有 VLAN 分配给一个组；或者，可以创建一个内部组和一个外部组；或者，为每个客户创建一个组。
- 每个组的 VLAN 数量均没有限制，但 ASASM 只能使用 ASASM 系统限制范围内的 VLAN（有关详细信息，请参阅 ASASM 许可文档）。
- 不能将同一个 VLAN 分配给多个防火墙组。
- 可以将一个防火墙组分配给多个 ASASM。例如，您希望分配给多个 ASASM 的 VLAN 可以位于与每个 ASASM 所独有的 VLAN 不同的单独组中。
- 请参阅第 3-3 页的 VLAN 准则和限制。

详细步骤

	命令	用途
步骤 1	**firewall vlan-group** *firewall_group vlan_range* **示例：** `Router(config)# firewall vlan-group 1 55-57`	将 VLAN 分配给防火墙组。 *firewall_group* 参数是一个整数。*vlan_range* 参数可以是一个或多个 VLAN（2 到 1001），可通过以下方法之一来识别： • 单个编号 (*n*) • 范围 (*n-x*) 编号或范围之间用逗号分隔，如以下示例所示： **5,7-10,13,45-100**

	命令	用途
步骤 2	**firewall** [**switch** {**1** |**2**}] **module** *slot* **vlan-group** *firewall_group* **示例：** `Router(config)# firewall module 5 vlan-group 1`	Assigns the firewall groups to the ASASM. 对于 VSS 中的交换机，请输入 **switch** 参数。 要查看安装了 ASASM 的插槽，请输入 **show module** 命令。 *firewall_group* 参数是一个或多个组编号，可以是以下其中一种形式： • 单个编号 (*n*) • 范围 (*n-x*) 编号或范围之间用逗号分隔，如以下示例所示： **5,7-10**

示例

以下示例显示如何创建三个防火墙 VLAN 组：两个组分别用于每个 ASASM，第三个组包含分配给两个 ASASM 的 VLAN。

```
Router(config)# firewall vlan-group 10 55-57
Router(config)# firewall vlan-group 11 70-85
Router(config)# firewall vlan-group 12 100
Router(config)# firewall module 5 vlan-group 10,12
Router(config)# firewall module 8 vlan-group 11,12
```

以下示例显示如何通过将主要 VLAN 分配给 ASASM 来在交换机上配置专用 VLAN：

步骤 1　将主要 VLAN 200 添加到一个防火墙 VLAN 组，然后将该组分配给 ASASM：

```
Router(config)# firewall vlan-group 10 200
Router(config)# firewall module 5 vlan-group 10
```

步骤 2　将 VLAN 200 指定为主要 VLAN：

```
Router(config)# vlan 200
Router(config-vlan)# private-vlan primary
```

步骤 3　仅指定一个辅助独立 VLAN。指定一个或多个辅助社区 VLAN。

```
Router(config)# vlan 501
Router(config-vlan)# private-vlan isolated
Router(config)# vlan 502
Router(config-vlan)# private-vlan community
Router(config)# vlan 503
Router(config-vlan)# private-vlan community
```

步骤 4　将辅助 VLAN 与主要 VLAN 关联起来：

```
Router(config)# vlan 200
Router(config-vlan)# private-vlan association 501-503
```

步骤 5　对端口模式进行分类。接口 f1/0/1 模式是主机模式。接口 f1/0/2 模式是混杂模式。

```
Router(config)# interface f1/0/1
Router(config-ifc)# switchport mode private-vlan host
Router(config)# interface f1/0/2
Router(config-ifc)# switchport mode private-vlan promiscuous
```

步骤 6　向主机端口分配 VLAN 成员身份。接口 f1/0/1 是主要 VLAN 200 和辅助独立 VLAN 501 的成员。

```
Router(config)# interface f1/0/1
Router(config-ifc)# switchport private-vlan host-association 200 501
```

步骤 7　向混杂接口分配 VLAN 成员身份。接口 f1/0/2 是主要 VLAN 200 的成员。辅助 VLAN 501-503 被映射到主要 VLAN。

```
Router(config)# interface f1/0/2
Router(config-ifc)# switchport private-vlan mapping 200 501-503
```

步骤 8　如果需要 VLAN 间路由，请配置主要 SVI，然后将辅助 VLAN 映射到主要 SVI。

```
Router(config)# interface vlan 200
Router(config-ifc)# private-vlan mapping 501-503
```

将 MSFC 用作直连路由器 (SVI)

如果要将 MSFC 用作直连路由器（例如，作为模式中 ASASM 外部接口的默认网关），请将一个 ASASM VLAN 接口添加到 MSFC 作为交换虚拟接口 (SVI)。请参阅第 3-2 页的有关 SVI 的信息。

限制

出于安全原因，默认情况下，可以在 MSFC 与 ASASM 之间配置一个 SVI；可以启用多个 SVI，但务必要确保网络配置正确。

详细步骤

	命令	用途
步骤 1	（可选） **firewall multiple-vlan-interfaces** **示例：** `Router(config)# firewall multiple-vlan-interfaces`	可以向 ASASM 添加多于一个 SVI。
步骤 2	**interface vlan** *vlan_number* **示例：** `Router(config)# interface vlan 55`	将一个 VLAN 接口添加到 MSFC。
步骤 3	**ip address** *address mask* **示例：** `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	在 MSFC 上设置此接口的 IP 地址。
步骤 4	**no shutdown** **示例：** `Router(config-if)# no shutdown`	启用接口。

示例

以下示例显示具有多个 SVI 的典型配置：

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall module 8 vlan-group 50-51
Router(config)# firewall multiple-vlan-interfaces
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

为 ASA 故障转移配置交换机

- 第 3-8 页的将 VLAN 分配给辅助 ASA 服务模块
- 第 3-8 页的在主要交换机与辅助交换机之间添加中继
- 第 3-8 页的确保与透明防火墙模式的兼容性
- 第 3-9 页的启用自动状态消息以进行快速链路故障检测

将 VLAN 分配给辅助 ASA 服务模块

由于两个设备都需要具有对访问内部和外部网络的相同访问权限，因此，您必须向交换机上的两个 ASASM 分配相同的 VLAN。请参阅第 3-8 页的将 VLAN 分配给辅助 ASA 服务模块。

在主要交换机与辅助交换机之间添加中继

如要使用交换机间故障转移，应该在两个交换机之间配置一个 802.1Q VLAN 中继，用以传送故障转移和状态链路。应该对该中继启用 QoS，以使 CoS 值为 5（较高优先级）的故障转移 VLAN 数据包在这些端口中得到较优先的处理。

如要配置 EtherChannel 和中继，请参阅相应的交换机文档。

确保与透明防火墙模式的兼容性

为了在透明模式中使用故障转移时避免回路，请使用支持 BPDU 转发的交换机软件。如果 ASASM 处于透明模式，请勿在交换机上全局启用 LoopGuard。LoopGuard 自动应用于交换机与 ASASM 之间的内部 EtherChannel，因此，在故障转移和故障恢复之后，LoopGuard 会因为 EtherChannel 进入假死状态而导致辅助设备断开连接。

启用自动状态消息以进行快速链路故障检测

管理引擎可向 ASASM 发送有关与 ASASM VLAN 关联的物理接口的状态的自动状态消息。例如，如果与 VLAN 关联的所有物理接口都出现故障，自动状态消息会告知 ASASM VLAN 发生故障。借助这些信息，ASASM 可以声明 VLAN 发生故障，从而绕过接口监控测试（确定哪一侧出现链路故障时通常需要进行此测试）。自动状态消息可大大减少 ASASM 检测链路故障所需的时间（如果有自动状态支持，仅需要几毫秒，如果没有，则最多需要 45 秒）。

当发生以下情况时，交换机管理引擎会向 ASASM 发送自动状态消息：

- 属于 VLAN 的最后一个接口出现故障。
- 属于 VLAN 的第一个接口投入使用。

详细步骤

命令	用途
防火墙自动状态 **示例：** `Router(config)# firewall autostate`	在思科 IOS 软件中启用自动状态消息。默认情况下，自动状态消息被禁用。

重置 ASA 服务模块

本节介绍如何重置 ASASM。如果无法通过 CLI 或外部 Telnet 会话访问 ASASM，可能需要重置 ASASM。重置过程可能需要几分钟时间。

详细步骤

命令	用途
hw-module [**switch** {**1** |**2**}] **module** *slot* **reset** **示例：** `Router# hw-module module 9 reset`	重置 ASASM。 对于 VSS 中的交换机，请输入 **switch** 参数。 *slot* 参数表示安装了模块的插槽编号。要查看安装了 ASASM 的插槽，请输入 **show module** 命令。 **注**　如要在已登录的情况下重置 ASASM，请输入 **reload** 或 **reboot** 命令。

示例

以下是 **hw-module module reset** 命令的输出示例：

```
Router# hw-module module 9 reset

Proceed with reload of module?[confirm] y
% reset issued for module 9

Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down.Please wait ...
```

监控 ASA 服务模块

如要监控 ASA，输入以下命令之一：

命令	用途
show firewall module [*mod-num*] **state**	验证 ASA 的状态。
show firewall module [*mod-num*] **traffic**	验证流量是否正在通过 ASA。
show firewall module [*mod-num*] **version**	显示 ASA 的软件版本。
show firewall multiple-vlan-interfaces	指明多个 VLAN 接口的状态（已启用或已禁用）。
show firewall vlan-group	显示所有已配置的 VLAN 组。
show interface vlan	显示已配置的 VLAN 接口的状态及相关信息。

示例

以下是 **show firewall module** [*mod-num*] **state** 命令的输出示例：

```
Router> show firewall module 11 state
Firewall module 11:
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 3,6,7,20-24,40,59,85,87-89,99-115,150,188-191,200,250,
     501-505,913,972
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:
Vlans allowed and active in management domain:
Vlans in spanning tree forwarding state and not pruned:
```

以下是 **show firewall module** [*mod-num*] **traffic** 命令的输出示例：

```
Router> show firewall module 11 traffic
Firewall module 11:

Specified interface is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0014.1cd5.bef6 (bia 0014.1cd5.bef6)
  MTU 1500 bytes, BW 6000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, media type is unknown
  input flow-control is on, output flow-control is on
  Members in this channel: Gi11/1 Gi11/2 Gi11/3 Gi11/4 Gi11/5 Gi11/6
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queuing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 10000 bits/sec, 17 packets/sec
     8709 packets input, 845553 bytes, 0 no buffer
     Received 745 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
```

```
     18652077 packets output, 1480488712 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

以下是 **show firewall multiple-vlan-interfaces** 命令的输出示例：

```
Router# show firewall multiple-vlan-interfaces
Multiple firewall vlan interfaces feature is enabled
```

以下是 **show firewall module** 命令的输出示例：

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

以下是 **show firewall module** [*mod-num*] **version** 命令的输出示例：

```
Router# show firewall module 2 version
ASA Service Module 2:

Sw Version: 100.7(8)19
```

以下是 **show firewall vlan-group** 命令的输出示例：

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

以下是 **show interface vlan** 命令的输出示例：

```
Router# show interface vlan 55
Vlan55 is up, line protocol is up
  Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
  L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
  L3 out Switched:ucast:0 pkt, 0 bytes
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     4 packets output, 256 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

与 ASA 服务模块配合使用的交换机的功能历史记录

表 3-1 列出了各种功能变更以及实施该等功能变更的平台版本

表 3-1　　与 ASASM配合使用的交换机的功能历史记录

功能名称	平台版本	功能信息
Catalyst 6500 交换机的 ASA 服务模块支持	8.5(1)	ASASM 是适用于 Catalyst 6500 系列交换机的高性能安全服务模块，您可以根据本章中所述的操作步骤对此服务模块进行配置。 引入或修改了以下命令：**firewall transparent**、 **mac address auto**、**firewall autostate** (IOS)、**interface vlan**。
思科 7600 交换机的 ASA 服务模块支持	9.0(1)	Cisco 7600 系列现在支持 ASASM。
对于专用 VLAN 的支持	9.1(2)	可以将专用 VLAN 与 ASASM 配合使用。将主要 VLAN 分配给 ASASM；ASASM 会自动处理辅助 VLAN 流量。对于此功能，不需要在 ASASM 上进行任何配置；有关详细信息，请参阅交换机配置指南。

功能许可证

许可证指定在给定思科 ASA 上启用的选项。本文介绍如何获取和激活许可证激活密钥。它还介绍了适用于每个产品型号的许可证。

注 本章介绍 9.3 版本的许可；有关其他版本，请参阅适用于您的版本的许可文档：

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-licensing-information-listing.html

- 第 4-1 页的每个型号的受支持功能许可证
- 第 4-18 页的有关功能许可证的信息
- 第 4-27 页的准则和限制
- 第 4-28 页的配置许可证
- 第 4-34 页的监控许可证
- 第 4-45 页的许可的功能历史记录

每个型号的受支持功能许可证

本节介绍了适用于每个型号的许可证，以及有关这些许可证的重要说明。

- 第 4-1 页的每个型号的许可证
- 第 4-14 页的许可证说明
- 第 4-18 页的 VPN 许可证和功能兼容性

每个型号的许可证

本节列出了适用于每个型号的功能许可证：

- 第 4-2 页的 ASA 5512-X
- 第 4-3 页的 ASA 5515-X
- 第 4-5 页的 ASA 5525-X
- 第 4-6 页的 ASA 5545-X
- 第 4-7 页的 ASA 5555-X

- 第 4-8 页的带 SSP-10 的 ASA 5585-X
- 第 4-9 页的带 SSP-20 的 ASA 5585-X
- 第 4-10 页的带 SSP-40 和 -60 的 ASA 5585-X
- 第 4-11 页的 ASA 服务模块
- 第 4-12 页的带 1 个虚拟 CPU 的 ASAv
- 第 4-13 页的带 4 个虚拟 CPU 的 ASAv

显示为*斜体*的项是可以替代基本 （或增强型安全等）许可证版本的独立可选许可证。您可以混搭使用许可证；例如，24 统一通信许可证和强加密许可证；或 500 AnyConnect Premium 许可证和 GTP/GPRS 许可证；或所有四个许可证。

注　某些功能互不兼容。有关兼容性信息，请参阅个别功能章节。

如果您拥有的是无负载加密型号，则以下的部分功能不受支持。有关不受支持的功能的列表，请参阅第 4-26 页的无负载加密型号。

有关许可证的详细信息，请参阅第 4-14 页的许可证说明。

ASA 5512-X

表 4-1　ASA 5512-X 许可证功能

许可证	基础许可证					增强型安全许可证				
防火墙许可证										
僵尸网络流量过滤器	禁用	*可选的基于时间的许可证：可用*				禁用	*可选的基于时间的许可证：可用*			
并发防火墙连接	100,000					250,000				
GTP/GPRS	不支持					禁用	*可选许可证：可用*			
公司间媒体引擎	禁用	*可选许可证：可用*				禁用	*可选许可证：可用*			
UC 电话代理会话，UC 代理会话总数	2	*可选许可证：*				2	*可选许可证：*			
		24	*50*	*100*	*250*	*500*	*24*	*50*	*100*	*250*	*500*
VPN 许可证										
高级终端评估	禁用	*可选许可证：可用*				禁用	*可选许可证：可用*			
AnyConnect for Cisco VPN Phone	禁用	*可选许可证：可用*				禁用	*可选许可证：可用*			
AnyConnect Essentials	禁用	*可选许可证：可用 （250 个会话）*				禁用	*可选许可证：可用 （250 个会话）*			
AnyConnect for Mobile	禁用	*可选许可证：可用*				禁用	*可选许可证：可用*			

表 4-1　　ASA 5512-X 许可证功能（续）

许可证	基础许可证					增强型安全许可证				
AnyConnect Premium（会话）	2	*可选永久许可证：*				2	*可选永久许可证：*			
		10	*25*	*50*	*100*		*10*	*25*	*50*	*100*
		可选的基于时间的 (VPN Flex) 许可证：			*250*		*可选的基于时间的 (VPN Flex) 许可证：*			*250*
	可选共享许可证：参与者或服务器。对于服务器：					*可选共享许可证：参与者或服务器。对于服务器：*				
	500 - 50,000，增量为 500			*50,000 - 545,000，增量为 1000*		*500 - 50,000，增量为 500*			*50,000 - 545,000，增量为 1000*	
整合所有类型的 VPN 总数（会话）	250					250				
其他 VPN（会话）	250					250				
VPN 负载均衡	不支持					受支持				
通用许可证										
加密	基本 (DES)	*可选许可证：强 (3DES/AES)*				基本 (DES)	*可选许可证：强 (3DES/AES)*			
故障转移	不支持					主用/备用或主用/主用				
所有类型的接口，最大值	716					916				
安全情景	不支持					2	*可选许可证：*			*5*
集群	不支持					2				
IPS 模块	禁用	*可选许可证：可用*				禁用	*可选许可证：可用*			
VLAN，最大值	50					100				

ASA 5515-X

表 4-2　　ASA 5515-X 许可证功能

许可证	基础许可证						
防火墙许可证							
僵尸网络流量过滤器	禁用	*可选的基于时间的许可证：可用*					
并发防火墙连接	250,000						
GTP/GPRS	禁用	*可选许可证：可用*					
公司间媒体引擎	禁用	*可选许可证：可用*					
UC 电话代理会话，UC 代理会话总数	2	*可选许可证：*	*24*	*50*	*100*	*250*	*500*
VPN 许可证							
高级终端评估	禁用	*可选许可证：可用*					
AnyConnect for Cisco VPN Phone	禁用	*可选许可证：可用*					
AnyConnect Essentials	禁用	*可选许可证：可用 （250 个会话）*					
AnyConnect for Mobile	禁用	*可选许可证：可用*					

表 4-2　　ASA 5515-X 许可证功能（续）

许可证	基础许可证					
AnyConnect Premium（会话）	2	*可选永久许可证：*				
		10	*25*	*50*	*100*	*250*
		可选的基于时间的 (VPN Flex) 许可证：				*250*
	可选共享许可证：参与者或服务器。对于服务器：					
	500 - 50,000，增量为 500					*50,000 - 545,000，增量为 1000*
整合所有类型的 VPN 总数（会话）	250					
其他 VPN（会话）	250					
VPN 负载均衡	受支持					
通用许可证						
加密	基本 (DES)	*可选许可证：强 (3DES/AES)*				
故障转移	主用/备用或主用/主用					
所有类型的接口，最大值	916					
安全情景	2	*可选许可证：*	*5*			
集群	2					
IPS 模块	禁用	*可选许可证：可用*				
VLAN，最大值	100					

ASA 5525-X

表 4-3　　ASA 5525-X 许可证功能

许可证	基础许可证								
防火墙许可证									
僵尸网络流量过滤器	禁用	*可选的基于时间的许可证：可用*							
并发防火墙连接	500,000								
GTP/GPRS	禁用	*可选许可证：可用*							
公司间媒体引擎	禁用	*可选许可证：可用*							
UC 电话代理会话，UC 代理会话总数	2	*可选许可证：*	*24*	*50*	*100*	*250*	*500*	*750*	*1000*
VPN 许可证									
高级终端评估	禁用	*可选许可证：可用*							
AnyConnect for Cisco VPN Phone	禁用	*可选许可证：可用*							
AnyConnect Essentials	禁用	*可选许可证：可用 （750 个会话）*							
AnyConnect for Mobile	禁用	*可选许可证：可用*							
AnyConnect Premium（会话）	2	*可选永久许可证：*							
		10	*25*	*50*	*100*	*250*	*500*	*750*	
		可选的基于时间的 (VPN Flex) 许可证：						*750*	
	可选共享许可证：参与者或服务器。对于服务器：								
	500 - 50,000，增量为 500					*50,000 - 545,000，增量为 1000*			
整合所有类型的 VPN 总数（会话）	750								
其他 VPN（会话）	750								
VPN 负载均衡	受支持								
通用许可证									
加密	基本 (DES)	*可选许可证：强 (3DES/AES)*							
故障转移	主用/备用或主用/主用								
所有类型的接口，最大值	1316								
安全情景	2	*可选许可证：*	*5*	*10*	*20*				
集群	2								
IPS 模块	禁用	*可选许可证：可用*							
VLAN，最大值	200								

ASA 5545-X

表 4-4　ASA 5545-X 许可证功能

许可证	基础许可证									
防火墙许可证										
僵尸网络流量过滤器	禁用	*可选的基于时间的许可证：可用*								
并发防火墙连接	750,000									
GTP/GPRS	禁用	*可选许可证：可用*								
公司间媒体引擎	禁用	*可选许可证：可用*								
UC 电话代理会话，UC 代理会话总数	2	*可选许可证：*	*24*	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*
VPN 许可证										
高级终端评估	禁用	*可选许可证：可用*								
AnyConnect for Cisco VPN Phone	禁用	*可选许可证：可用*								
AnyConnect Essentials	禁用	*可选许可证：可用 （2500 个会话）*								
AnyConnect for Mobile	禁用	*可选许可证：可用*								
AnyConnect Premium（会话）	2	*可选永久许可证：*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*
		可选的基于时间的 (VPN Flex) 许可证：								*2500*
	可选共享许可证：参与者或服务器。对于服务器：									
	500 - 50,000，增量为 500					*50,000 - 545,000，增量为 1000*				
整合所有类型的 VPN 总数（会话）	2500									
其他 VPN（会话）	2500									
VPN 负载均衡	受支持									
通用许可证										
加密	基本 (DES)	*可选许可证：强 (3DES/AES)*								
故障转移	主用/备用或主用/主用									
所有类型的接口，最大值	1716									
安全情景	2	*可选许可证：*	*5*	*10*	*20*	*50*				
集群	2									
IPS 模块	禁用	*可选许可证：可用*								
VLAN，最大值	300									

ASA 5555-X

表 4-5　　ASA 5555-X 许可证功能

许可证	基础许可证								
防火墙许可证									
僵尸网络流量过滤器	禁用	*可选的基于时间的许可证：可用*							
并发防火墙连接	1,000,000								
GTP/GPRS	禁用	*可选许可证：可用*							
公司间媒体引擎	禁用	*可选许可证：可用*							
UC 电话代理会话，UC 代理会话总数	2	*可选许可证：*							
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN 许可证									
高级终端评估	禁用	*可选许可证：可用*							
AnyConnect for Cisco VPN Phone	禁用	*可选许可证：可用*							
AnyConnect Essentials	禁用	*可选许可证：可用 （5000 个会话）*							
AnyConnect for Mobile	禁用	*可选许可证：可用*							
AnyConnect Premium（会话）	2	*可选永久许可证：*							
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
		可选的基于时间的 (VPN Flex) 许可证：								*5000*
	可选共享许可证：参与者或服务器。对于服务器：								
	500 - 50,000，增量为 500					*50,000 - 545,000，增量为 1000*			
整合所有类型的 VPN 总数（会话）	5000								
其他 VPN（会话）	5000								
VPN 负载均衡	受支持								
通用许可证									
加密	基本 (DES)	*可选许可证：强 (3DES/AES)*							
故障转移	主用/备用或主用/主用								
所有类型的接口，最大值	2516								
安全情景	2	*可选许可证：*		*5*	*10*	*20*	*50*	*100*	
集群	2								
IPS 模块	禁用	*可选许可证：可用*							
VLAN，最大值	500								

带 SSP-10 的 ASA 5585-X

您可以在同一个机箱中可以使用两个相同级别的 SSP。不支持混合使用不同级别的 SSP （例如，不支持混合使用 SSP-10 和 SSP-20）。每个 SSP 作为独立设备，都有独立的配置和管理。您可以视需要，将两个 SSP 用作故障转移对。

表 4-6　　带 SSP-10 的 ASA 5585-X 的许可证功能

许可证	基本和增强型安全许可证									
防火墙许可证										
僵尸网络流量过滤器	禁用	*可选的基于时间的许可证：可用*								
并发防火墙连接	1,000,000									
GTP/GPRS	禁用	*可选许可证：可用*								
公司间媒体引擎	禁用	*可选许可证：可用*								
UC 电话代理会话，UC 代理会话总数	2	*可选许可证：*								
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN 许可证										
高级终端评估	禁用	*可选许可证：可用*								
AnyConnect for Cisco VPN Phone	禁用	*可选许可证：可用*								
AnyConnect Essentials	禁用	*可选许可证：可用 （5000 个会话）*								
AnyConnect for Mobile	禁用	*可选许可证：可用*								
AnyConnect Premium（会话）	2	*可选永久许可证：*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
		可选的基于时间的 (VPN Flex) 许可证：									*5000*
	可选共享许可证：参与者或服务器。对于服务器：									
	500 - 50,000，增量为 500					*50,000 - 545,000，增量为 1000*				
整合所有类型的 VPN 总数（会话）	5000									
其他 VPN（会话）	5000									
VPN 负载均衡	受支持									
通用许可证										
10 GE I/O	**基础许可证**：禁用；光纤接口运行于 1 GE					**增强型安全许可证**：启用；光纤接口运行于 10 GE				
加密	基本 (DES)	*可选许可证：强 (3DES/AES)*								
故障转移	主用/备用或主用/主用									
所有类型的接口，最大值	4612									
安全情景	2	*可选许可证：*			*5*	*10*	*20*	*50*	*100*	
集群	禁用	*可选许可证：适用于 16 台设备*								
VLAN，最大值	1024									

带 SSP-20 的 ASA 5585-X

您可以在同一个机箱中可以使用两个相同级别的 SSP。不支持混合使用不同级别的 SSP （例如，不支持混合使用 SSP-20 和 SSP-40）。每个 SSP 作为独立设备，都有独立的配置和管理。您可以视需要，将两个 SSP 用作故障转移对。

表 4-7　　带 SSP-20 的 ASA 5585-X 的许可证功能

许可证	基本和增强型安全许可证										
防火墙许可证											
僵尸网络流量过滤器	禁用	*可选的基于时间的许可证：可用*									
并发防火墙连接	2,000,000										
GTP/GPRS	禁用	*可选许可证：可用*									
公司间媒体引擎	禁用	*可选许可证：可用*									
UC 电话代理会话，UC 代理会话总数	2	*可选许可证：*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN 许可证											
高级终端评估	禁用	*可选许可证：可用*									
AnyConnect for Cisco VPN Phone	禁用	*可选许可证：可用*									
AnyConnect Essentials	禁用	*可选许可证：可用 （10,000 个会话）*									
AnyConnect for Mobile	禁用	*可选许可证：可用*									
AnyConnect Premium（会话）	2	*可选永久许可证：*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10,000*
		可选的基于时间的 (VPN Flex) 许可证：										*10,000*
	可选共享许可证：参与者或服务器。对于服务器：										
	500 - 50,000，增量为 500					*50,000 - 545,000，增量为 1000*					
整合所有类型的 VPN 总数（会话）	10,000										
其他 VPN（会话）	10,000										
VPN 负载均衡	受支持										
通用许可证											
10 GE I/O	**基础许可证**：禁用；光纤接口运行于 1 GE					**增强型安全许可证**：启用；光纤接口运行于 10 GE					
加密	基本 (DES)	*可选许可证：强 (3DES/AES)*									
故障转移	主用/备用或主用/主用										
所有类型的接口，最大值	4612										
安全情景	2	*可选许可证：*		*5*	*10*	*20*	*50*	*100*	*250*		
集群	禁用	*可选许可证：适用于 16 台设备*									
VLAN，最大值	1024										

1. 使用 10,000 个会话的 UC 许可证，整合会话总数可以为 10,000 个，但是电话代理会话总数为 5000 个。

带 SSP-40 和 -60 的 ASA 5585-X

您可以在同一个机箱中可以使用两个相同级别的 SSP。不支持混合使用不同级别的 SSP （例如，不支持混合使用 SSP-40 和 SSP-60）。每个 SSP 作为独立设备，都有独立的配置和管理。您可以视需要，将两个 SSP 用作故障转移对。

表 4-8　　带 SSP-40 和 -60 的 ASA 5585-X 的许可证功能

许可证	基础许可证										
防火墙许可证											
僵尸网络流量过滤器	禁用	*可选的基于时间的许可证：可用*									
并发防火墙连接	**带 SSP-40 的 5585-X**：4,000,000					**带 SSP-60 的 5585-X**：10,000,000					
GTP/GPRS	禁用	*可选许可证：可用*									
公司间媒体引擎	禁用	*可选许可证：可用*									
UC 电话代理会话，UC 代理会话总数	2	*可选许可证：*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN 许可证											
高级终端评估	禁用	*可选许可证：可用*									
AnyConnect for Cisco VPN Phone	禁用	*可选许可证：可用*									
AnyConnect Essentials	禁用	*可选许可证：可用 （10,000 个会话）*									
AnyConnect for Mobile	禁用	*可选许可证：可用*									
AnyConnect Premium（会话）	2	*可选永久许可证：*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10,000*
		可选的基于时间的 (VPN Flex) 许可证：										*10,000*
	可选共享许可证：参与者或服务器。对于服务器：										
	500 - 50,000，增量为 500					*50,000 - 545,000，增量为 1000*					
整合所有类型的 VPN 总数（会话）	10,000										
其他 VPN（会话）	10,000										
VPN 负载均衡	受支持										
通用许可证											
10 GE I/O	启用；光纤接口运行于 10 GE										
加密	基本 (DES)	*可选许可证：强 (3DES/AES)*									
故障转移	主用/备用或主用/主用										
所有类型的接口，最大值	4612										
安全情景	2	*可选许可证：*		*5*	*10*	*20*	*50*	*100*	*250*		
集群	禁用	*可选许可证：适用于 16 台设备*									
VLAN，最大值	1024										

1. 使用 10,000 个会话的 UC 许可证，整合会话总数可以为 10,000 个，但是电话代理会话总数为 5000 个。

ASA 服务模块

表 4-9　ASASM 许可证功能

许可证	基础许可证										
防火墙许可证											
僵尸网络流量过滤器	禁用	*可选的基于时间的许可证：可用*									
并发防火墙连接	10,000,000										
GTP/GPRS	禁用	*可选许可证：可用*									
公司间媒体引擎	禁用	*可选许可证：可用*									
UC 电话代理会话，UC 代理会话总数	2	*可选许可证：*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN 许可证											
高级终端评估	禁用	*可选许可证：可用*									
AnyConnect for Cisco VPN Phone	禁用	*可选许可证：可用*									
AnyConnect Essentials	禁用	*可选许可证：可用 （10,000 个会话）*									
AnyConnect for Mobile	禁用	*可选许可证：可用*									
AnyConnect Premium（会话）	2	*可选永久许可证：*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10,000*
		可选的基于时间的 (VPN Flex) 许可证：										*10,000*
		可选共享许可证：参与者或服务器。对于服务器：										
		500 - 50,000，增量为 500					*50,000 - 545,000，增量为 1000*					
整合所有类型的 VPN 总数（会话）	10,000										
其他 VPN（会话）	10,000										
VPN 负载均衡	受支持										
通用许可证											
加密	基本 (DES)	*可选许可证：强 (3DES/AES)*									
故障转移	主用/备用或主用/主用										
安全情景	2	*可选许可证：*									
		5	*10*	*20*	*50*	*100*	*250*				
集群	不支持										
VLAN，最大值	1000										

1. 使用 10,000 个会话的 UC 许可证，整合会话总数可以为 10,000 个，但是电话代理会话总数为 5000 个。

带 1 个虚拟 CPU 的 ASAv

表 4-10　带 1 个虚拟 CPU 的 ASAv 的许可证功能

许可证	标准和高级许可证	
防火墙许可证		
僵尸网络流量过滤器	受支持	
并发防火墙连接	100,000	
GTP/GPRS	受支持	
公司间媒体引擎	受支持	
UC 电话代理会话，UC 代理会话总数	250	
VPN 许可证		
高级终端评估	**标准许可证**：不支持	**高级许可证**：受支持
AnyConnect Essentials	**标准许可证**：不支持	**高级许可证**：不支持
AnyConnect for Cisco VPN Phone	**标准许可证**：不支持	**高级许可证**：受支持
AnyConnect for Mobile	**标准许可证**：不支持	**高级许可证**：受支持
AnyConnect Premium（会话）	**标准许可证**：2	**高级许可证**：250
	共享许可证：不支持	
整合所有类型的 VPN 总数（会话）	250	
其他 VPN（会话）	250	
VPN 负载均衡	受支持	
通用许可证		
加密	强 (3DES/AES)	
故障转移	主用/备用	
所有类型的接口，最大值	716	
安全情景	不支持	
集群	不支持	
VLAN，最大值	50	
RAM 和虚拟 CPU 频率限制	2 GB，5000 MHz	

带 4 个虚拟 CPU 的 ASAv

表 4-11　带 4 个虚拟 CPU 的 ASAv 的许可证功能

许可证	标准和高级许可证	
防火墙许可证		
僵尸网络流量过滤器	受支持	
并发防火墙连接	500,000	
GTP/GPRS	受支持	
公司间媒体引擎	受支持	
UC 电话代理会话，UC 代理会话总数	1000	
VPN 许可证		
高级终端评估	**标准许可证**：不支持	**高级许可证**：受支持
AnyConnect Essentials	**标准许可证**：不支持	**高级许可证**：不支持
AnyConnect for Cisco VPN Phone	**标准许可证**：不支持	**高级许可证**：受支持
AnyConnect for Mobile	**标准许可证**：不支持	**高级许可证**：受支持
AnyConnect Premium（会话）	**标准许可证**：2	**高级许可证**：750
	共享许可证：不支持	
整合所有类型的 VPN 总数（会话）	750	
其他 VPN（会话）	750	
VPN 负载均衡	受支持	
通用许可证		
加密	强 (3DES/AES)	
故障转移	主用/备用	
所有类型的接口，最大值	1316	
安全情景	不支持	
集群	不支持	
VLAN，最大值	200	
RAM 和虚拟 CPU 频率限制	8 GB，20000 MHz **注**　如果您应用 4 个虚拟 CPU 的许可证，但选择部署 2 或 3 个虚拟 CPU，请参阅以下值： 2 个虚拟 CPU - 4 GB RAM，虚拟 CPU 频率限制为 10000 MHz，250,000 个并发防火墙连接。 3 个虚拟 CPU - 4 GB RAM，虚拟 CPU 频率限制为 15000 MHz，350,000 个并发防火墙连接。	

许可证说明

表 4-12 包含由第 4-1 页的每个型号的许可证 中的多个表共享的公用脚注。

表 4-12　　许可证说明

许可证	备注
AnyConnect Essentials	AnyConnect Essentials 会话包括以下 VPN 类型： • SSL VPN • 使用 IKEv2 的 IPsec 远程访问 VPN 此许可证不支持基于浏览器（无客户端）的 SSL VPN 访问或思科安全桌面。对于这些功能，请激活 AnyConnect Premium 许可证，而不是 AnyConnect Essentials 许可证。 **注**　借助 AnyConnect Essentials 许可证，VPN 用户可以使用网络浏览器来进行登录，然后下载并启动 (WebLaunch) AnyConnect 客户端。 AnyConnect 客户端软件提供一组相同的客户端功能，无论是通过此许可证，还是通过 AnyConnect Premium 许可证启用。 AnyConnect Essentials 许可证不能在给定 ASA 上与以下许可证同时处于活动状态：AnyConnect Premium 许可证 （所有类型）或高级终端评估许可证。然而，您可以在同一网络中的不同 ASA 上运行 AnyConnect Essentials 和 AnyConnect Premium 许可证。 默认情况下，ASA 使用 AnyConnect Essentials 许可证，但您可以通过先使用 **webvpn**，然后使用 **no anyconnect-essentials** 命令，或者在 ASDM 中使用 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials** 窗格来禁用该许可证，以便使用其他许可证。 另请参阅第 4-18 页的 VPN 许可证和功能兼容性。
AnyConnect for Cisco VPN Phone	通过与 AnyConnect Premium 许可证相结合，此许可证允许通过拥有内置 AnyConnect 兼容性的硬件 IP 电话进行访问。
AnyConnect for Mobile	此许可证允许运行 Windows Mobile 5.0、6.0 和 6.1 的触摸屏移动设备访问 AnyConnect 客户端。如果您希望支持对 AnyConnect 2.3 及以上版本进行移动访问，我们建议使用此许可证。此许可证要求激活以下任一许可证，以便指定允许的 SSL VPN 会话的总数：AnyConnect Essentials 或 AnyConnect Premium。 **移动安全状态支持** 实施远程访问控制和从移动设备收集安全状态数据，需要在 ASA 上安装有一个 AnyConnect Mobile 许可证和一个 AnyConnect Essentials 许可证或 AnyConnect Premium 许可证。此处为根据您所安装的许可证，可以获得的功能。 • AnyConnect Premium 许可证功能 – 在受支持的移动设备上，基于 DAP 属性和所有其他现有终端属性，实施 DAP 策略。这包括允许或拒绝来自移动设备的远程访问。 • AnyConnect Essentials 许可证功能 – 使用 ASDM，对每个组启用或禁用移动设备访问，并配置该功能。 – 显示有关通过 CLI 或 ASDM 连接的移动设备的信息，无需具有实施 DAP 策略，或者拒绝或允许对这些移动设备的远程访问的能力。

表 4-12　　许可证说明（续）

许可证	备注
AnyConnect Premium	AnyConnect Premium 会话包括以下 VPN 类型： • SSL VPN • 无客户端 SSL VPN • 使用 IKEv2 的 IPsec 远程访问 VPN
AnyConnect Premium Shared	共享许可证允许 ASA 充当多个客户端 ASA 的共享许可证服务器。共享许可证池很大，但每个 ASA 使用的最大会话数，不能超过列出的永久许可证的最大数量。
僵尸网络流量过滤器	要下载动态数据库，需要有强加密 (3DES/AES) 许可证。
加密	无法禁用 DES 许可证。如果您安装了 3DES 许可证，DES 仍可用。您希望仅使用强加密时，要防止使用 DES，请确保配置所有相关命令，以便仅使用强加密。
公司间媒体引擎	当您启用公司间媒体引擎 (IME) 许可证时，可以使用的 TLS 代理会话数最多可为配置的 TLS 代理限制。如果您还安装了高于默认 TLS 代理限制的统一通信 (UC) 许可证，则 ASA 会将该限制设置为 UC 许可证限制与额外会话数（取决于您的型号）之和。您可以使用 **tls-proxy maximum-sessions** 命令，或者在 ASDM 中使用 **Configuration > Firewall > Unified Communications > TLS Proxy** 窗格来手动配置 TLS 代理限制。要查看型号的限制，请输入 **tls-proxy maximum-sessions ?**命令。如果您还安装了 UC 许可证，则可用于 UC 的 TLS 会话也可供 IME 会话使用。例如，如果配置的限制是 1000 个 TLS 代理会话，并且您购买了 750 个会话的 UC 许可证，则前 250 个 IME 会话不会影响可用于 UC 的会话。如果您需要超过 250 个会话用于 IME，则平台限制剩余的 750 个会话由 UC 和 IME 按照先到先得的原则使用。 • 对于以“K8”结尾的许可证部件号，TLS 代理会话数限于 1000 个。 • 对于以“K9”结尾的许可证部件号，TLS 代理限制取决于您的配置和平台型号。 **注**　K8 和 K9 是指许可证是否有出口限制：K8 为不受限制，K9 为受限制。 您也可将 SRTP 加密会话用于您的连接： • 对于 K8 许可证，SRTP 会话数限于 250 个。 • 对于 K9 许可证，没有限制。 **注**　仅需要对媒体进行加密/解密的呼叫会计入 SRTP 限制；如果将呼叫设置为直通，即使两端均为 SRTP，这些呼叫也不计入限制。
所有类型的接口，最大值	最大整合接口数量；例如，VLAN、物理、冗余、网桥组和 EtherChannel 接口。在配置中定义的每个 **interface** 命令均根据此限制进行计数。例如，以下两个接口都计入此限制，即使 GigabitEthernet 0/0 接口定义为 port-channel 1 的一部分： `interface gigabitethernet 0/0` 和 `interface port-channel 1`

表 4-12　　许可证说明（续）

许可证	备注
IPS 模块	IPS 模块许可证允许您在 ASA 上运行 IPS 软件模块。您还需要 IPS 端有 IPS 签名订用。 请参阅以下准则： • 要购买 IPS 签名订用，您需要有预装了 IPS 的 ASA（部件号必须包括“IPS”，例如 ASA5515-IPS-K9）；您不能为非 IPS 部件号 ASA 购买 IPS 签名订用。 • 对于故障转移，您需要两台设备上的 IPS 签名订用；由于此订用不是 ASA 许可证，因此不在故障转移中共享。 • 对于故障转移，IPS 签名订用要求每台设备具有唯一的 IPS 模块许可证。与其他 ASA 许可证一样，IPS 模块许可证在故障转移集群许可证中技术共享。但是，由于 IPS 签名订用要求，您必须为故障转移中的每台设备，购买单独的 IPS 模块许可证。
其他 VPN	其他 VPN Premium 会话包括以下 VPN 类型： • 使用 IKEv1 的 IPsec 远程访问 VPN • 使用 IKEv1 的 IPsec 站点对站点 VPN • 使用 IKEv2 的 IPsec 站点对站点 VPN 此许可证包括在基础许可证中。
整合所有类型的 VPN 总数（会话）	• 虽然最大总计 VPN 会话数超过最大 VPN AnyConnect 和其他 VPN 会话数，整合的会话数不应超过 VPN 会话限制。如果您超过了最大 VPN 会话数，则可能会使 ASA 过载，因此请务必正确设置网络规模。 • 如果您启动无客户端 SSL VPN 会话，并通过门户启动 AnyConnect 客户端会话，则总共使用了 1 个会话。但是，如果先启动 AnyConnect 客户端（例如，通过独立客户端），然后登录无客户端 SSL VPN 门户，则使用了 2 个会话。

表 4-12　许可证说明（续）

许可证	备注
UC 电话代理会话，UC 代理会话总数	以下应用将 TLS 代理会话用于其连接。这些应用 （而且仅这些应用）使用的每个 TLS 代理会话都会计入 UC 许可证限制： • 电话代理 • 状态联合代理 • 加密语音检查 使用 TLS 代理会话的其他应用不计入 UC 限制，例如，移动优势代理（无需许可证）和 IME（需要单独的 IME 许可证）。 有些 UC 应用可能将多个会话用于一个连接。例如，如果您用主和备用思科统一通信管理器配置电话，由于存在 2 个 TLS 代理连接，因此会使用 2 个 UC 代理会话。 您可以使用 **tls-proxy maximum-sessions** 命令，或者在 ASDM 中使用 **Configuration > Firewall > Unified Communications > TLS Proxy** 窗格来单独配置 TLS 代理限制。要查看型号的限制，请输入 **tls-proxy maximum-sessions ?**命令。当您应用高于默认 TLS 代理限制的 UC 许可证时，ASA 会自动设置 TLS 代理限制以匹配 UC 限制。TLS 代理限制优先于 UC 许可证限制；如果您将 TLS 代理限制设置为低于 UC 许可证，则您可能无法使用 UC 许可证中的所有会话。 **注**　对于以“K8”结尾的许可证部件号（例如，低于 250 个用户的许可证），TLS 代理会话数限于 1000 个。对于以“k9”结尾的许可证部件号（例如，250 个用户或更多用户的许可证），TLS 代理限制取决于配置，最多可为型号限制。K8 和 K9 是指许可证是否有出口限制：K8 为不受限制，K9 为受限制。 如果您清除配置（例如，使用**clear configure all** 命令），则 TLS 代理限制会被设置为您的型号的默认值；如果此默认值低于 UC 许可证限制，则您会看到要求您使用 **tls-proxy maximum-sessions** 命令再次提高限制的错误消息（在 ASDM 中，请使用 **TLS Proxy** 窗格）。如果您使用故障切换，并输入 **write standby** 命令，或者在 ASDM 中，在主设备上使用 **File > Save Running Configuration to Standby Unit** 来强制进行配置同步，则 **clear configure all** 命令会在辅助设备上自动生成，因此，您可能会在辅助设备上看到警告消息。由于配置同步会还原在主设备上设置的 TLS 代理限制，您可以忽略该警告。 您也可将 SRTP 加密会话用于您的连接： • 对于 K8 许可证，SRTP 会话数限于 250 个。 • 对于 K9 许可证，没有限制。 **注**　仅需要对媒体进行加密/解密的呼叫会计入 SRTP 限制；如果将呼叫设置为直通，即使两端均为 SRTP，这些呼叫也不计入限制。
虚拟 CPU	您必须在 ASAv 上安装虚拟 CPU 许可证。直到您安装许可证，吞吐量限于 100 kbps，这样您可以进行初步的连接测试。正常运行需要虚拟 CPU 许可证。
VLAN，最大值	对于根据 VLAN 限制计数的接口，您必须为它分配一个 VLAN。例如： `interface gigabitethernet 0/0.100` `  vlan 100`
VPN 负载均衡	VPN 负载均衡需要强加密 (3DES/AES) 许可证。

VPN 许可证和功能兼容性

表 4-13 展示了可以如何整合 VPN 许可证和功能。

有关 AnyConnect Essentials 许可证和 AnyConnect Premium 许可证支持的功能的详细列表，请参阅《*AnyConnect 安全移动客户端功能、许可证和 OS*》：

- 3.1 版本：
  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect31/feature/guide/anyconnect31features.html
- 3.0 版本：
  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/feature/guide/anyconnect30features.html
- 2.5 版本：
  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/feature/guide/anyconnect25features.html

表 4-13　　VPN 许可证和功能兼容性

支持的许可证：	启用以下任一许可证：[1]	
	AnyConnect Essentials	AnyConnect Premium
AnyConnect for Cisco VPN Phone	否	是
AnyConnect for Mobile[2]	是	是
高级终端评估	否	是
AnyConnect Premium Shared	否	是
基于客户端的 SSL VPN	是	是
基于浏览器的（无客户端）SSL VPN	否	是
IPsec VPN	是	是
VPN 负载均衡	是	是
思科安全桌面	否	是

1. 您只能有一个活动的许可证类型，AnyConnect Essentials 许可证或 AnyConnect Premium 许可证。默认情况下，ASA 包括 2 个会话的 AnyConnect Premium 许可证。如果您安装了 AnyConnect Essentials 许可证，默认情况下将使用该许可证。请参阅 **webvpn** 和 **no anyconnect-essentials** 命令，以便启用 Premium license 来进行代替。
2. 移动状态支持对于 AnyConnect 基础版和 AnyConnect 高级版许可证不同。有关详细信息，请参阅第 4-14 页的表 4-12。

有关功能许可证的信息

许可证指定在给定 ASA 上启用的选项。它由一个 160 位（5 个 32 位字或 20 个字节）值的激活密钥表示。此值对序列号 （11 个字符的字符串）和启用的功能进行编码。

- 第 4-19 页的预安装的许可证
- 第 4-19 页的永久许可证
- 第 4-19 页的基于时间的许可证
- 第 4-21 页的共享 AnyConnect Premium 许可证
- 第 4-24 页的故障转移或 ASA 集群许可证

- 第 4-26 页的无负载加密型号
- 第 4-27 页的许可证常见问题

预安装的许可证

默认情况下，ASA 发货时已安装有一个许可证。此许可证可能是您希望对其添加更多许可证的基础许可证，也可能已安装了您的所有许可证，具体取决于您订购的许可证和您的供应商已为您安装的许可证。请参阅第 4-34 页的监控许可证，以便确定您已安装的许可证。

永久许可证

您可以安装一个永久激活密钥。永久激活密钥在单个密钥中包含所有许可功能。如果您还安装了基于时间的许可证，ASA 会将永久许可证和基于时间的许可证整合为运行许可证。有关 ASA 如何整合这些许可证的详细信息，请参阅第 4-20 页的永久许可证和基于时间的许可证如何整合。

基于时间的许可证

除了永久许可证，您还可以购买基于时间的许可证，或者接收有时间限制的评估许可证。例如，您可以购买基于时间的 AnyConnect Premium 许可证，以便处理并发 SSL VPN 用户的短期激增，也可以订购有效期为 1 年的基于时间的僵尸网络流量过滤器许可证。

- 第 4-19 页的基于时间的许可证的激活准则
- 第 4-19 页的基于时间的许可证的计时器如何工作
- 第 4-20 页的永久许可证和基于时间的许可证如何整合
- 第 4-20 页的堆叠基于时间的许可证
- 第 4-21 页的基于时间的许可证的到期

基于时间的许可证的激活准则

- 您可以安装多个基于时间的许可证，包括用于相同功能的多个许可证。然而，每个功能同时仅能有一个基于时间的许可证处于*活动*状态。非活动许可证保持已安装状态，并可随时使用。例如，如果您安装了 1000 个会话的 AnyConnect Premium 许可证和 2500 个会话的 AnyConnect Premium 许可证，则其中仅有一个许可证能够处于活动状态。
- 如果您激活了在密钥中有多个功能的评估许可证，则您无法也激活另一基于时间的许可证，该许可证可用于评估许可证包含的任一功能。例如，如果一个评估许可证包括僵尸网络流量过滤器和 1000 个会话的 AnyConnect Premium 许可证，则您无法也激活独立的基于时间的 2500 个会话的 AnyConnect Premium 许可证。

基于时间的许可证的计时器如何工作

- 当您在 ASA 上激活基于时间的许可证时，其计时器会开始倒计时。
- 如果您在基于时间的许可证到期之前停止使用该许可证，计时器会停止。仅当您重新激活基于时间的许可证时，计时器才会重新启动。

- 如果基于时间的许可证处于活动状态，并且您关闭 ASA，则计时器会继续倒计时。如果您打算长时间关闭 ASA，则您应在关闭前停用基于时间的许可证。

注 安装基于时间的许可证后，我们建议您不要更改系统时钟。如果您将时钟设置为将来的日期，然后，如果重新加载，ASA 会将系统时钟与原始安装时间进行对比，并认为比实际使用的时间过去了更长的时间。如果您将时钟设置为过去的日期，并且实际运行时间大于原始安装时间和系统时钟之间的时间差，则重新加载后，许可证将立即到期。

永久许可证和基于时间的许可证如何整合

当您激活了基于时间的许可证时，永久许可证和基于时间的许可证中的功能将会整合，以形成运行许可证。永久许可证与基于时间的许可证的整合方式取决于许可证类型。表 4-14 列出了每个功能许可证的整合规则。

注 即使使用了永久许可证，如果基于时间的许可证处于活动状态，它也会继续倒计时。

表 4-14　基于时间的许可证的整合规则

基于时间的功能	组合许可证的规则
AnyConnect Premium 会话	将使用基于时间的许可证或永久许可证两者中的较高值。例如，如果永久许可证是 1000 个会话，基于时间的许可证是 2500 个会话，则会启用 2500 个会话。通常，您不会安装功能弱于永久许可证的基于时间的许可证，但是，如果您这么做，则会使用永久许可证。
统一通信代理会话	基于时间的许可证的会话会添加到永久会话，最高值为平台限制。例如，如果永久许可证为 2500 个会话，基于时间的许可证为 1000 个会话，则一旦基于时间的许可证处于活动状态，就会启用 3500 个会话。
安全情景	基于时间的许可证的情景会添加到永久情景，最高值为平台限制。例如，如果永久许可证为 10 个情景，基于时间的许可证为 20 个情景，则一旦基于时间的许可证处于活动状态，就会启用 30 个情景。
僵尸网络流量过滤器	没有可用的永久僵尸网络流量过滤器许可证；将会使用基于时间的许可证。
所有其他	将使用基于时间的许可证或永久许可证两者中的较高值。对于状态为启用或禁用的许可证，将会使用状态为启用的许可证。对于具有数值层的许可证，将使用较高的值。通常，您不会安装功能弱于永久许可证的基于时间的许可证，但是，如果您这么做，则会使用永久许可证。

如要查看整合的许可证，请参阅第 4-34 页的监控许可证。

堆叠基于时间的许可证

在许多情况下，您可能需要更新您的基于时间的许可证，并从旧许可证无缝过渡到新许可证。对于仅在使用基于时间的许可证时才可用的功能，在您应用新许可证前，许可证没有到期尤为重要。ASA 允许您*堆叠*基于时间的许可证，因此您不必担心许可证到期，也不必担心因为过早安装新许可证而损失许可证时间。

当您安装与已安装的许可证相同的基于时间的许可证时，许可证会被整合，持续时间等于整合后的持续时间。

例如：

1. 您安装有 52 周的僵尸网络流量过滤器许可证，并使用了该许可证 25 周 （剩余 27 周）。
2. 然后，您又购买了另一个 52 周的僵尸网络流量过滤器许可证。当您安装第二个许可证时，许可证会被整合为拥有 79 周的持续时间 （52 周加上 27 周）。

类似地：

1. 您安装有 8 周 1000 个会话的 AnyConnect Premium 许可证，并使用了该许可证 2 周 （剩余 6 周）。
2. 然后您又安装了另一个 8 周 1000 个会话的许可证，许可证会被整合为 14 周 1000 个会话的许可证 （8 周加上 6 周）。

如果许可证不同（例如，1000 会话 AnyConnect 高级版许可证与 2500 会话许可证），则*不*合并许可证。由于每个功能仅能有一个基于时间的许可证处于活动状态，这些许可证中仅有一个许可证可以处于活动状态。有关激活许可证的详细信息，请参阅第 4-29 页的激活和停用密钥。

虽然不同的许可证不会整合，但当前许可证到期时， ASA 会自动激活已安装的同一功能的许可证（如可用）。有关详细信息，请参阅第 4-21 页的基于时间的许可证的到期。

基于时间的许可证的到期

某个功能的当前许可证到期时，ASA 会自动激活已安装的同一功能的许可证（如可用）。如果没有其他适用于此功能的基于时间的许可证，则将使用永久许可证。

如果您为某个功能安装了多个额外的基于时间的许可证，ASA 会使用它找到的第一个许可证；将会使用哪个许可证不是用户可配置的，而是取决于内部操作。如果您希望使用的许可证不是 ASA 激活的基于时间的许可证，则必须手动激活您希望使用的许可证。请参阅第 4-29 页的激活和停用密钥。

例如，您有一个基于时间的 2500 个会话 AnyConnect Premium 许可证（活动）、一个基于时间的 1000 个会话 AnyConnect Premium 许可证（非活动），以及一个永久的 500 个会话的 AnyConnect Premium 许可证。当 2500 个会话的许可证到期时，ASA 会激活 1000 个会话的许可证。1000 个会话的许可证到期后，ASA 会使用 500 个会话的永久许可证。

共享 AnyConnect Premium 许可证

共享许可证允许您购买大量 AnyConnect Premium 会话，然后视需要在一组 ASA 之间共享这些会话 （通过将其中一台 ASA 配置为共享许可服务器，同时将其他 ASA 配置为共享许可参与者）。此部分介绍共享许可证如何工作。

- 第 4-22 页的有关共享许可服务器和参与者的信息
- 第 4-22 页的参与者和服务器之间的通信问题
- 第 4-23 页的有关共享许可备用服务器的信息
- 第 4-23 页的故障转移和共享许可证
- 第 4-24 页的最大参与者数量

有关共享许可服务器和参与者的信息

以下步骤说明共享许可证的工作方式：

1. 确定哪一台 ASA 应充当共享许可服务器，然后使用该设备的序列号购买共享许可服务器许可证。
2. 确定哪些 ASA 应充当共享许可参与者，其中包括共享许可备用服务器，并使用每台设备的序列号，获取每台设备的共享许可参与者许可证。
3. （可选）将另一台 ASA 指定为共享许可备用服务器。您仅能指定一台备用服务器。

   注　共享许可备用服务器仅需要参与者许可证。

4. 在共享许可服务器上配置一个共享机密；具有该共享机密的所有参与者，都可以使用共享许可证。
5. 当您将 ASA 配置为参与者时，它会发送有关自身的信息 （包括本地许可证和型号信息），从而向共享许可服务器注册。

   注　参与者需要能够通过 IP 网络与服务器通信；它不必在同一子网中。

6. 共享许可服务器会以参与者应轮询服务器的频率的相关信息进行响应。
7. 当参与者用尽本地许可证的会话时，它会向共享许可服务器发出请求，要求获得更多会话（增量为 50 个会话）。
8. 共享许可服务器会以共享许可证进行响应。参与者使用的会话总数，不能超过平台型号的最大会话数。

   注　共享许可服务器也可以参与共享许可证池。它参与共享许可证池不需要参与者许可证，也不需要服务器许可证。

   a. 如果在共享许可证池中没有为参与者留下足够多的会话，则服务器将以尽可能多的可用会话进行响应。
   b. 参与者将会继续发送请求更多会话的刷新消息，直到服务器可以充分满足请求。
9. 参与者之上的负载减少时，它会向服务器发送消息，以便释放共享会话。

注　ASA 在服务器和参与者之间使用 SSL 来加密所有通信。

参与者和服务器之间的通信问题

有关参与者和服务器之间的通信问题的信息，请参阅以下准则：

- 如果参与者在 3 倍刷新间隔过后未能发送刷新信息，则服务器会将会话释放回共享许可证池。
- 如果参与者无法访问许可证服务器，以便发送刷新消息，则参与者可以继续使用其从服务器收到的共享许可证，最多可使用 24 小时。
- 如果在 24 小时后，参与者仍无法与许可证服务器通信，则参与者将释放共享许可证，即使其仍然需要会话。参与者会保留已建立的现有连接，但无法接受超过许可证限制的新连接。
- 如果参与者在 24 小时的时间到期之前，服务器使参与者会话到期之后，重新与服务器连接，则参与者需要为会话发送新的请求；服务器会以能重新分配至该参与者的尽可能多的会话进行响应。

有关共享许可备用服务器的信息

共享许可备用服务器必须先成功注册至主共享许可服务器，然后才能承担备用角色。当其注册时，主共享许可服务器将与备用服务器同步服务器设置以及共享许可证信息，其中包括已注册参与者的列表以及当前的许可证使用情况。主服务器和备用服务器以 10 秒为间隔同步数据。在最初的同步之后，即使经过重新加载，备份服务器也能够成功履行备用职责。

主服务器发生故障时，备用服务器会接管服务器操作。备用服务器可以连续运行最多 30 天，在此之后，备用服务器会停止向参与者颁发会话，而且现有会话将会超时。请确保在此 30 天的时段内恢复主服务器。关键级别的系统日志消息会在 15 天时发送，并在 30 天时再次发送。

当主服务器恢复正常运行时，它将与备用服务器同步，然后接管服务器操作。

备用服务器不处于主用状态时，它会充当主共享许可服务器的普通参与者。

注　您首次启动主共享许可服务器时，备用服务器仅可独立运行 5 天。运行限制将逐日延长，直到到达 30 天。此外，如果此后主服务器停止运行任意时长，备用服务器的运行限制会逐日缩短。主服务器恢复正常运行时，备用服务器的运行限制会开始再次逐日延长。例如，如果主服务器停止运行 20 天，在此期间备用服务器处于主用状态，则备用服务器的运行限制将仅剩余 10 天。备份服务器在继续充当非主用的备用服务器 20 天后，将“充电”至最长的 30 天运行限制。实施此充电功能是为了防止滥用共享许可证。

故障转移和共享许可证

此部分介绍共享许可证如何与故障转移交互。

- 第 4-23 页的故障转移和共享许可证服务器
- 第 4-24 页的故障转移和共享许可证参与者

故障转移和共享许可证服务器

此部分介绍主服务器和备用服务器如何与故障转移交互。由于共享许可服务器还会与 ASA 一样履行普通职责，包括执行诸如充当 VPN 网关和防火墙之类的功能，您可能需要为主和备用共享许可服务器配置故障转移，以便提高可靠性。

注　备用服务器机制独立于故障转移，但与其兼容。

共享许可证仅在单情景模式中受支持，因此主用/主用故障转移不受支持。

对于主用/备用故障转移，主设备将充当主共享许可服务器，发生故障转移后，备用设备将充当主共享许可服务器。备用设备*不会*充当备用共享许可证服务器。取而代之的是，您可以视需要，让另一对设备充当备用服务器。

例如，您有带 2 个故障转移对的网络。第 1 个对包含主许可服务器。第 2 个对包含备用服务器。第 1 个对中的主设备发生故障时，备用设备会立即变为新的主许可服务器。第 2 个对中的备用服务器绝对不会使用。仅当第 1 个对中的两台设备均发生故障时，第 2 个对中的备用服务器才会用作共享许可服务器。如果第 1 个对保持故障状态，并且第 2 个对中的主设备发生故障，则第 2 个对中的备用单元将会用作共享许可服务器。

辅助备用服务器与主备用服务器共享相同的运行限制；如果辅助设备变为主用设备，它会在主设备停止的位置继续倒计时。有关详细信息，请参阅第 4-23 页的有关共享许可备用服务器的信息。

故障转移和共享许可证参与者

对于参与者对，两台设备会使用单独的参与者 ID 注册至共享许可服务器。主用设备会将其参与者 ID 与备用设备同步。当备用设备切换到主用角色时，它会使用此 ID 生成转移请求。此转移请求用于将共享会话，从先前的主用设备移至新的主用设备。

最大参与者数量

ASA 不限制共享许可证的参与者数量；但是，非常大的共享网络可能会影响许可服务器的性能。在这种情况下，您可以延长参与者刷新之间的延迟，也可以创建两个共享网络。

故障转移或 ASA 集群许可证

除了一些例外情况之外，故障转移和集群设备不要求每台设备上具有相同的许可证。有关早期版本，请参阅您的版本的许可文档。

- 第 4-24 页的故障转移许可证要求和例外情况
- 第 4-25 页的 ASA 集群许可证要求和例外情况
- 第 4-25 页的故障转移或 ASA 集群许可证如何整合
- 第 4-26 页的故障转移或 ASA 集群设备之间的通信丢失
- 第 4-26 页的升级故障转移对

故障转移许可证要求和例外情况

故障转移设备不要求每台设备上具有相同的许可证。

ASA 软件的早期版本要求每台设备上的许可证匹配。从 8.3(1) 版本开始，您不再需要安装相同的许可证。通常，您仅为主设备购买许可证；对于主用/备用故障转移，辅助设备在其变为主用状态时，会继承主许可证。如果您在两台设备上都有许可证，它们将组合成一个运行的故障转移集群许可证。

此规则的例外情况包括：

- ASA 5512-X 的增强型安全许可证 - 基础许可证不支持故障转移，因此，您不能在只有基础许可证的备用设备上，启用故障转移。
- 加密许可证 - 两台设备必须拥有相同的加密许可证。
- ASA 5512-X 至 ASA 5555-X 的 IPS 模块许可证 - 两台设备都需要 IPS 模块许可证。您还需要两台设备的 IPS 端上的 IPS 签名订用。请参阅以下准则：
  - 要购买 IPS 签名订用，您需要有预装了 IPS 的 ASA（部件号必须包括“IPS”，例如 ASA5515-IPS-K9）；您不能为非 IPS 部件号 ASA 购买 IPS 签名订用。
  - 您需要两台设备上的 IPS 签名订用；由于此订用不是 ASA 许可证，因此不在故障转移中共享。
  - IPS 签名订用要求每台设备具有唯一的 IPS 模块许可证。与其他 ASA 许可证一样，IPS 模块许可证在故障转移集群许可证中技术共享。但是，由于 IPS 签名订用要求，您必须为每台设备购买单独的 IPS 模块许可证。
- ASAv 虚拟 CPU - 用于故障转移部署，请确保备用设备分配到的虚拟 CPU 数量与主要设备相同 （以及匹配的虚拟 CPU 许可证）。

注　需要一个有效的永久密钥；在极少数情况下，您的身份验证密钥可以被移除。如果您的密钥完全由 0 组成，则您需要重新安装有效的身份验证密钥，然后才能启用故障转移。

ASA 集群许可证要求和例外情况

集群设备不要求每台设备上具有相同的许可证。通常，您仅为主设备购买许可证；从属设备会继承主许可证。如果您在多台设备上都有许可证，它们将整合为单个运行 ASA 集群许可证。

此规则的例外情况包括：

- 集群许可证 - 每台设备必须具有一个集群许可证。
- 加密许可证 - 每台设备必须拥有相同的加密许可证。

故障转移或 ASA 集群许可证如何整合

对于故障转移对或 ASA 集群，每台设备上的许可证将整合为单个运行集群许可证。如果您为每台设备购买单独的许可证，则整合的许可证采用以下规则：

- 对于具有数字层 （例如，会话数）的许可证，每台设备的许可证的值会整合至平台限制。如果正在使用的所有许可证都是基于时间的许可证，则许可证将同时倒计时。

  例如，对于故障转移：

  - 您有两台 ASA，这两台设备都安装了 10 个 AnyConnect Premium 会话的许可证；这些许可证会被整合，从而拥有总计 20 个 AnyConnect Premium 会话。
  - 您有两台都拥有 500 个 AnyConnect Premium 会话的 ASA 5525-X；由于平台限制为 750，整合后的许可证允许 750 个 AnyConnect Premium 会话。

    注　在上述示例中，如果 AnyConnect Premium 许可证是基于时间的，您可能想要禁用其中一个许可证，以便您不会“浪费”一个 500 个会话的许可证，因为平台限制，您仅能使用 250 个会话。

  - 您有两台 ASA 5545-X ASA，一台有 20 个情景，另一台有 10 个情景；整合后的许可证允许 30 个情景。对于主用/主用故障转移，情景将在两台设备之间划分。例如，一台设备可以使用 18 个情景，而另一台设备可以使用 12 个情景，总数为 30 个。

  例如，对于 ASA 集群：

  - 您有四台带 SSP-10 的 ASA 5585-X ASA，三台设备都有 50 个情景，一台设备有默认的 2 个情景。由于平台限制是 100 个，整合后的许可证允许最多 100 个情景。因此，您可以在主设备上配置最多 100 个情景；每台从属设备通过配置复制也将拥有 100 个情景。
  - 您有四台带 SSP-60 的 ASA 5585-X ASA，三台设备都有 50 个情景，一台设备有默认的 2 个情景。由于平台限制为 250 个，这些许可证会被整合，从而拥有总计 152 个情景。因此，您可以在主设备上配置最多 152 个情景；每台从属设备通过配置复制也将拥有 152 个情景。

- 对于状态为启用或禁用的许可证，将会使用状态为启用的许可证。
- 对于启用或禁用的基于时间的许可 （而且没有数值层），持续时间是所有许可证的整合持续时间。主/主设备首先对其许可证进行倒计时，当其许可证到期时，辅助/从属设备将开始对其许可证进行倒计时，依此类推。此规则也适用于主用/主用故障转移和 ASA 集群，即使所有设备均以主用状态在运行。

  例如，如果两台设备上的僵尸网络流量过滤器许可证剩下 48 周，则整合的持续时间为 96 周。

要查看整合的许可证，请参阅第 4-34 页的监控许可证。

故障转移或 ASA 集群设备之间的通信丢失

如果设备丢失通信超过 30 天，则每台设备将还原到本地安装的许可证。在 30 天宽限期内，所有设备将继续使用整合的运行许可证。

在 30 天的宽限期内，如果您还原通信，对于基于时间的许可证，将从主/主许可证中减去过去的时间；如果主/主许可证已到期，仅当此时辅助/从属许可证才会开始倒计时。

如果您在 30 天内，不能还原通信，对于基于时间的许可，将从所有设备许可证 （如已安装）中减去过去的时间。它们会将被视为独立许可证，不会受益于组合许可证。过去的时间中包括 30 天的宽限期。

例如：

1. 您在两台设备上都安装了 52 周的僵尸网络流量过滤器许可证。整合的运行许可证允许 104 周的总持续时间。
2. 这两台设备作为故障转移设备/ASA 集群运行 10 周，整合的许可证会剩余 94 周 （主/主设备上剩余 42 周，辅助/从属设备上剩余 52 周）。
3. 如果设备丢失通信 （例如，主/主设备发生故障），辅助/从属设备会继续使用组合许可证，并继续从 94 周倒计时。
4. 基于时间的许可证的行为取决于还原通信的时间：

- 在 30 天内 - 将从主/主设备许可证中减去过去的时间。在这种情况下，通信将在 4 周后还原。因此，将从主/主许可证中减去 4 周，剩余的 90 周会被整合 （主设备上剩余 38 周，辅助设备上剩余 52 周）。
- 在 30 天后 - 将从两台设备的许可证中减去过去的时间。在这种情况下，通信将在 6 周后还原。因此，将从主/主许可证和辅助/从属许可证中减去 6 周，剩余的 84 周会被整合 （主/主设备上剩余 36 周，辅助/从属设备上剩余 46 周）。

升级故障转移对

由于故障转移对不需要在两台设备上有相同的许可证，您可以将新许可证应用于每台设备，无需任何停机时间。如果您应用需要重新加载的永久许可证 （请参阅第 4-29 页的表 4-15），则你可以在重新加载时，故障转移到另一台设备。如果两台设备都需要重新加载，则您可以单独重新加载它们，以便不产生停机时间。

无负载加密型号

您可以购买某些无负载加密的型号。出口至某些国家/地区的思科 ASA 系列产品不能启用负载加密。 ASA 软件可感知无负载加密型号，并禁用以下功能：

- 统一通信
- VPN

您仍然可以安装强加密 （3DES/AES）许可证，以便用于管理连接。例如，您可以使用 ASDM HTTPS/SSL、 SSHv2、 Telnet 和 SNMPv3。您还可以为僵尸网络流量过滤器下载动态数据库 （使用 SSL）。

当您查看许可证 （请参阅第 4-34 页的监控许可证）时，将不会列出 VPN 和统一通信许可证。

许可证常见问题

Q. 我能否激活多个基于时间的许可证，例如，AnyConnect Premium 和僵尸网络流量过滤器？

A. 能。对于每个功能，您仅能同时使用一个基于时间的许可证。

Q. 我能否“堆叠”基于时间的许可证，以便时间限制耗尽时，会自动使用下一个许可证？

A. 能。对于相同的许可证，当您安装多个基于时间的许可证时，时间限制会被整合。对于不相同的许可证（例如，1000 个会话的 AnyConnect Premium 许可证和 2500 个会话的许可证），ASA 会自动激活其为该功能的找到的下一个基于时间的许可证。

Q. 我能否在使基于时间的许可证保持活动的同时，安装新的永久许可证？

A. 能。激活永久许可证不会影响基于时间的许可证。

Q. 对于故障转移，我能否将共享许可服务器用作主设备，并将共享许可备用服务器用作辅助设备？

A. 编号 辅助设备具有与主设备相同的运行许可证；对于共享许可服务器，它们需要服务器许可证。备用服务器需要参与者许可证。备用服务器可以处于两台备用服务器的单独故障转移对中。

Q. 我是否需要为故障转移对中的辅助设备，购买相同的许可证？

A. 编号 从 8.3(1) 版本开始，您不必在两台设备上拥有匹配的许可证。通常，您仅为主设备购买许可证；辅助设备在其变为主用状态时，会继承主许可证。对于您在辅助设备上也有独立许可证的情况 （例如，如果您购买了 8.3 版本之前的软件的许可证），这些许可证会被整合为运行故障转移集群许可证，限制最多为型号限制。

Q. 除共享 AnyConnect Premium 许可证之外，我能否使用基于时间的或永久的 AnyConnect Premium 许可证？

A. 能。仅当本地安装的许可证 （基于时间的或永久的许可证）中的会话用尽后，才会使用共享许可证。**注意**：在共享许可服务器上，不会使用永久 AnyConnect Premium 许可证；但是您可以同时使用基于时间的许可证和共享许可服务器许可证。在这种情况下，基于时间的许可证会话仅供本地 AnyConnect Premium 会话使用；不能将它们添加到共享许可池供参与者使用。

准则和限制

请参阅激活密钥的以下准则：

情景模式准则

- 在多情景模式中，请在系统执行空间中应用激活密钥。
- 共享许可证在多情景模式中不受支持。

防火墙模式准则

所有许可证类型在路由和透明模式中均可用。

故障转移准则

- 共享许可证在主用/主用模式中不受支持。有关详细信息，请参阅第 4-23 页的故障转移和共享许可证。
- 请参阅第 4-24 页的故障转移或 ASA 集群许可证。

升级和降级准则

如果您从任何之前的版本升级至最新版本，您的激活密钥会保持兼容。但是，如果您想要保持降级能力，则可能会遇到问题。

- 降级到 8.1 版本或更早的版本 - 在升级之后，如果您激活了在 *8.2 版本之前*引入的附加功能许可证，激活密钥在您降级时，会继续与更早的版本兼容。但是，如果您激活在 *8.2 版本或更高的版本*中引入的功能许可证，激活密钥不会向后兼容。如果您有不兼容的许可证密钥，请参阅以下准则：
  - 如果您之前在早期版本中输入了激活密钥，ASA 会使用该密钥（不包括在 8.2 版本或更高的版本中激活的任意新许可证）。
  - 如果您有新的系统，并且没有早期的激活密钥，您需要请求与早期版本兼容的新激活密钥。
- 降级至 8.2 版本或更早的版本 - 8.3 版本引入了更可靠的基于时间的密钥用法以及故障转移许可证更改：
  - 如果您有多个基于时间的激活密钥处于活动状态，当您降级时，只有最新的基于时间的密钥可以处于活动状态。所有其他密钥将进入非活动状态。如果最后的基于时间的许可证是用于 8.3 版本中引入的功能，则该许可证仍会保持活动状态，即使它不能在早期版本中使用。重新输入永久密钥，或者有效的基于时间的密钥。
  - 如果您在故障转移对上具有不匹配的许可证，降级将会禁用故障转移。即使密钥匹配，使用的许可证也不再是组合许可证。
  - 如果您安装了一个基于时间的许可证，但是它用于 8.3 版本中引入的功能，在您降级之后，该基于时间的许可将保持活动状态。您需要重新输入永久密钥，以便禁用该基于时间的许可证。

附加准则和限制

- 激活密钥不会存储在您的配置文件中；它会以隐藏文件的形式，存储在闪存中。
- 激活密钥会与设备的序列号绑定。功能许可证无法在设备之间转移（硬件发生故障的情况除外）。如果您由于硬件故障必须更换设备，而且 Cisco TAC 涵盖该设备，请联系思科许可团队，以便将您现有的许可证转移至新的序列号。思科许可团队将要求提供产品授权密钥参考编号和现有序列号。
- 一旦购买，您将无法退还许可证，以获取退款或升级的许可证。
- 在单个设备上，您无法将用于相同功能的两个单独许可证相加；例如，如果您购买了一个 25 个会话的 SSL VPN 许可证，此后又购买了 50 个会话的许可证，则您无法使用 75 个会话；您可以使用最多 50 个会话。（您能以升级价格购买更大的许可证，例如从 25 个到 75 个会话；应将这种升级，与将两个单独许可证相加区分开来）。
- 虽然您可以激活所有许可证类型，但有些功能互不兼容。对于 AnyConnect Essentials 许可证，此许可证与以下许可证不兼容：AnyConnect Premium 许可证、共享 AnyConnect Premium 许可证以及高级终端评估许可证。默认情况下，如果您安装了 AnyConnect Essentials 许可证（如果它对于您的模式可用），将使用该许可证，而不是上述许可证。您可以在配置中禁用 AnyConnect Essentials 许可证，以便还原为使用其他许可证，方式是：先使用 **webvpn**，然后使用 **no anyconnect-essentials** 命令窗格。

配置许可证

- 第 4-29 页的获取激活密钥
- 第 4-29 页的激活和停用密钥
- 第 4-31 页的配置共享许可证

获取激活密钥

如要获得激活密钥，您需要产品授权密钥，您可以从您的思科客户代表处购买此密钥。您需要为每个功能许可证购买单独的产品授权密钥。例如，如果您有基础许可证，您可以为高级终端评估和额外的 AnyConnect Premium 会话购买单独的密钥。

获得产品授权密钥后，请执行以下操作步骤，从而在 Cisco.com 上注册这些密钥。

详细步骤

步骤 1　通过 输入以下命令获取您的 ASA 的序列号：

```
ciscoasa# show version | grep Serial
```

步骤 2　如果您尚未注册至 Cisco.com，请创建帐户。

步骤 3　转至以下许可网站：

http://www.cisco.com/go/license

步骤 4　收到提示时，请输入以下信息：

- 产品授权密钥 （如果您有多个密钥，请先输入其中一个密钥。您必须单独输入每个密钥）。
- 您的 ASA 的序列号
- 您的邮件地址

激活密钥将会自动生成，并发送到您提供的邮件地址。此密钥包含到目前为止，您已注册的永久许可证的所有功能。对于基于时间的许可证，每个许可证具有单独的激活密钥。

步骤 5　如果您有其他的产品授权密钥，请为每个产品授权密钥重复步骤 4。在您输入所有产品授权密钥后，提供的最终激活密钥包含您注册的所有永久功能。

激活和停用密钥

此部分介绍如何输入新的激活密钥，以及如何激活和停用基于时间的密钥。

先决条件

- 如果您已处于多情景模式中，请在系统执行空间中输入激活密钥。
- 在您激活某些永久许可证之后，它们可能会要求您重新加载 ASA。表 4-15 列出了要求重新加载的许可证。

表 4-15　永久许可证重新加载要求

型号	要求重新加载的许可证操作
所有型号	降级加密许可证。
ASAv	降级虚拟 CPU 许可证。

限制

如果您从任何之前的版本升级至最新版本，您的激活密钥会保持兼容。但是，如果您想要保持降级能力，则可能会遇到问题。

- 降级到 8.1 版本或更早的版本 - 在升级之后，如果您激活了在 *8.2 版本之前*引入的附加功能许可证，激活密钥在您降级时，会继续与更早的版本兼容。但是，如果您激活在 *8.2 版本或更高的版本*中引入的功能许可证，激活密钥不会向后兼容。如果您有不兼容的许可证密钥，请参阅以下准则：
  - 如果您之前在早期版本中输入了激活密钥，ASA 会使用该密钥（不包括在 8.2 版本或更高的版本中激活的任意新许可证）。
  - 如果您有新的系统，并且没有早期的激活密钥，您需要请求与早期版本兼容的新激活密钥。
- 降级至 8.2 版本或更早的版本 - 8.3 版本引入了更可靠的基于时间的密钥用法以及故障转移许可证更改：
  - 如果您有多个基于时间的激活密钥处于活动状态，当您降级时，只有最新的基于时间的密钥可以处于活动状态。所有其他密钥将进入非活动状态。
  - 如果您在故障转移对上具有不匹配的许可证，降级将会禁用故障转移。即使密钥匹配，使用的许可证也不再是组合许可证。

详细步骤

	命令	用途
步骤 1	**activation-key** *key* [**activate** | **deactivate**] **示例：** `ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490`	将激活密钥应用到 ASA。*key* 为包括五个部分的十六进制字符串，在每个部分之间有一个空格。前导的 0x 说明符是可选的；所有值都会被认为是十六进制。 您可以安装一个永久密钥，以及多个基于时间的密钥。如果您输入一个新的永久密钥，它会覆盖已安装的永久密钥。 **activate** 和 **deactivate** 关键字仅适用于基于时间的密钥。如果您不输入任何值，**activate** 为默认值。您为给定功能激活的最后一个基于时间的密钥是活动密钥。要停用所有活动的基于时间的密钥，请输入 **deactivate** 关键字。如果您第一次输入密钥，并指定 **deactivate**，则密钥会以非活动状态安装在 ASA 上。有关详细信息，请参阅第 4-19 页的基于时间的许可证。
步骤 2	（可能需要）。 **reload** **示例：** `ciscoasa# reload`	重新加载 ASAASA。在您输入新的激活密钥之后，某些永久许可证会要求您重新加载 ASAASA。有关需要重新加载的许可证的列表，请参阅第 4-29 页的表 4-15。如果您需要重新加载，您将会看到以下消息： `WARNING: The running activation key was not updated with the requested key.The flash activation key was updated with the requested key, and will become active after the next reload.`

配置共享许可证

此部分介绍如何配置共享许可服务器和参与者。有关共享许可证的详细信息，请参阅第 4-21 页的共享 AnyConnect Premium 许可证。

- 第 4-31 页的配置共享许可服务器
- 第 4-32 页的配置共享许可备用服务器 （可选）
- 第 4-33 页的配置共享许可参与者

配置共享许可服务器

此部分介绍如何将 ASA 配置为共享许可服务器。

先决条件

服务器必须具有共享许可服务器密钥。

详细步骤

	命令	用途
步骤 1	**license-server secret** *secret* **示例：** `ciscoasa(config)# license-server secret farscape`	设置共享机密，一个长度介于 4 至 128 个 ASCII 字符的字符串。拥有此机密的所有参与者，都可以使用许可服务器。
步骤 2	（可选） **license-server refresh-interval** *seconds* **示例：** `ciscoasa(config)# license-server refresh-interval 100`	设置介于 10 至 300 秒的刷新间隔；此值会提供给参与者，用于设置它们应与服务器通信的频率。默认值为 30 秒。
步骤 3	（可选） **license-server port** *port* **示例：** `ciscoasa(config)# license-server port 40000`	设置端口，服务器会在该端口上侦听来自参与者的 SSL 连接，该端口介于 1 和 65535 之间。默认值为 TCP 端口 50554。
步骤 4	（可选） **license-server backup** *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*] **示例：** `ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3`	确定备份服务器 IP 地址和序列号。如果备用服务器是故障转移对的一部分，也会确定备用设备序列号。您仅能确定 1 台备用服务器及其可选的备用设备。

	命令	用途
步骤 5	**license-server enable** *interface_name* **示例：** ciscoasa(config)# license-server enable inside	使此设备成为共享许可服务器。指定参与者在其上联系服务器的接口。您可以为所需数量的接口，重复此命令。

示例

以下示例设置共享密钥、更改刷新间隔和端口、配置备用服务器，并在内部接口和 dmz 接口上，使此设备成为共享许可服务器：

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

后续操作

请参阅第 4-32 页的配置共享许可备用服务器 （可选），或第 4-33 页的配置共享许可参与者。

配置共享许可备用服务器 （可选）

此部分使共享许可参与者在主服务器发生故障时，充当备用服务器。

先决条件

备用服务器必须具有共享许可参与者密钥。

详细步骤

	命令	用途
步骤 1	**license-server address** *address* **secret** *secret* [**port** *port*] **示例：** ciscoasa(config)# license-server address 10.1.1.1 secret farscape	确定共享许可服务器 IP 地址和共享机密。如果您更改了服务器配置中的默认端口，请设置该端口，以便备用服务器能够匹配。
步骤 2	**license-server backup enable** *interface_name* **示例：** ciscoasa(config)# license-server backup enable inside	使此设备成为共享许可备用服务器。指定参与者在其上联系服务器的接口。您可以为所需数量的接口，重复此命令。

示例

以下示例确定许可服务器和共享机密，并在内部接口和 dmz 接口上，使此设备成为备用共享许可服务器：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

后续操作

请参阅第 4-33 页的配置共享许可参与者。

配置共享许可参与者

此部分配置共享许可参与者，以便与共享许可服务器通信。

先决条件

参与者必须具有共享许可参与者密钥。

详细步骤

	命令	用途
步骤 1	**license-server address** *address* **secret** *secret* [**port** *port*] **示例：** `ciscoasa(config)# license-server address 10.1.1.1 secret farscape`	确定共享许可服务器 IP 地址和共享机密。如果您更改了服务器配置中的默认端口，请设置该端口，以便参与者能够匹配。
步骤 2	（可选） **license-server backup address** *address* **示例：** `ciscoasa(config)# license-server backup address 10.1.1.2`	如果您配置了备用服务器，请输入备用服务器地址。

示例

以下示例设置许可服务器 IP 地址和共享机密，以及备用许可服务器 IP 地址：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

监控许可证

- 第 4-34 页的查看您的当前许可证
- 第 4-44 页的监控共享许可证

查看您的当前许可证

此部分介绍如何查看您的当前许可证，以及对于基于时间的激活密钥，该许可证的剩余时间。

准则

如果您拥有的是无负载加密型号，则在您查看许可证时，VPN 和统一通信许可证不会列出。有关详细信息，请参阅第 4-26 页的无负载加密型号。

详细步骤

命令	用途
show activation-key [**detail**]	此命令显示永久许可证、活动的基于时间的许可证以及运行许可证，该许可证由永久许可证和活动的基于时间的许可证整合而成。**detail** 关键字还显示非活动的基于时间的许可证。
示例： ciscoasa# show activation-key detail	对于故障转移或集群设备，该命令还显示“集群”许可证，该许可证时所有设备的整合密钥。

示例

示例 4-1　　独立设备运行 show activation-key 命令的输出

以下内容是独立设备运行 **show activation-key** 命令的示例输出，其中显示了运行许可证 （整合的永久许可证和基于时间的许可证），以及每个活动的基于时间的许可证：

```
ciscoasa# show activation-key

Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
```

```
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

示例 4-2　　独立设备运行 show activation-key detail 命令的输出

以下内容是独立设备运行 **show activation-key detail** 命令的示例输出，其中显示了运行许可证（整合的永久许可证和基于时间的许可证），以及永久许可证和每个已安装的基于时间的许可证（活动和非活动）：

```
ciscoasa# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5512-X Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
```

```
Inside Hosts                  : Unlimited      perpetual
Failover                      : Active/Standby perpetual
VPN-DES                       : Enabled        perpetual
VPN-3DES-AES                  : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions       : 2              perpetual
Total UC Proxy Sessions       : 2              perpetual
Botnet Traffic Filter         : Enabled        39 days
Intercompany Media Engine     : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days

Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                  : 25     7 days
```

示例 4-3　　故障转移对中的主设备运行 show activation-key detail 命令的输出

以下内容是主故障转移设备运行 **show activation-key detail** 命令的示例输出，其中显示了：

- 主设备许可证 （整合的永久许可证和基于时间的许可证）。
- “故障转移集群”许可证，该许可证是主设备和辅助设备的组合许可证。该许可证是在 ASA 上实际运行的许可证。该许可证中，反映主设备和辅助设备许可证的整合的值，会以粗体显示。
- 主设备的永久许可证。
- 主设备的已安装的基于时间的许可证 （活动和非活动）。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
```

```
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers       : 4           perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts               : 2          7 days
```

```
AnyConnect Premium Peers                  : 100        7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions         : 100        14 days
```

示例 4-4　　故障转移对中的辅助设备运行 show activation-key detail 命令的输出

以下内容是辅助故障转移设备运行 **show activation-key detail** 命令的示例输出，其中显示了：

- 辅助设备许可证 （整合的永久许可证和基于时间的许可证）。
- “故障转移集群”许可证，该许可证是主设备和辅助设备的组合许可证。该许可证是在 ASA 上实际运行的许可证。该许可证中，反映主设备和辅助设备许可证的整合的值，会以粗体显示。
- 辅助设备的永久许可证。
- 辅助设备的已安装的基于时间的许可证 （活动和非活动）。该设备没有任何基于时间的许可证，所以此示例输出中没有显示任何此类许可证。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 10             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
```

```
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
```

示例 4-5　　没有许可证的 ASAv 运行 show activation-key 命令的输出

部署的 1 个虚拟 CPU 的 ASAv 的以下输出，显示了空白激活密钥、未许可状态，以及要求安装 1 个虚拟 CPU 的许可证的消息。

注　命令输出显示“This platform has an ASAv VPN Premium license.” 此消息指定 ASAv 可以执行负载加密，它不是指 ASAv 标准版与 高级版许可证。

```
ciscoasa# show activation-key
Serial Number:  9APM1G4RV41
Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000

ASAv Platform License State: Unlicensed
*Install 1 vCPU ASAv platform license for full functionality.
The Running Activation Key is not valid, using default settings:

Licensed features for this platform:
Virtual CPUs                   : 0              perpetual
Maximum Physical Interfaces    : 10             perpetual
Maximum VLANs                  : 50             perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
Encryption-DES                 : Enabled        perpetual
Encryption-3DES-AES            : Enabled        perpetual
Security Contexts              : 0              perpetual
```

```
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

Failed to retrieve flash permanent activation key.
The flash permanent activation key is the SAME as the running permanent key.
```

示例 4-6　　具有 4 个虚拟 CPU 的标准许可证的 ASAv，运行 show activation-key 命令的独立设备输出

注　命令输出显示“This platform has an ASAv VPN Premium license.” 此消息指定 ASAv 可以执行负载加密，它不是指 ASAv 标准版与 高级版许可证。

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x0013e945 0x685a232c 0x1153fdac 0xeae8b068 0x4413f4ae

ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

The flash permanent activation key is the SAME as the running permanent key.
```

示例 4-7　　具有 4 个虚拟 CPU 的高级许可证的 ASAv，运行 show activation-key 命令的独立设备输出

注 命令输出显示“This platform has an ASAv VPN Premium license.” 此消息指定 ASAv 可以执行负载加密，它不是指 ASAv 标准版与 高级版许可证。

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x8224dd7d 0x943ed77c 0x9d71cdd0 0xd90474d0 0xcb04df82

ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 750            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

The flash permanent activation key is the SAME as the running permanent key.
ciscoasa#
```

示例 4-8　　故障转移对中的 ASA 服务模块 运行 show activation-key 命令的主设备输出

以下内容是主故障转移设备运行 **show activation-key** 命令的示例输出，其中显示了：

- 主设备许可证 （整合的永久许可证和基于时间的许可证）。
- “故障转移集群”许可证，该许可证是主设备和辅助设备的组合许可证。该许可证是在 ASA 上实际运行的许可证。该许可证中，反映主设备和辅助设备许可证的整合的值，会以粗体显示。
- 主设备的已安装的基于时间的许可证 （活动和非活动）。

```
ciscoasa# show activation-key

erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
```

```
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Active  perpetual
DES                             : Enabled        perpetual
3DES-AES                        : Enabled        perpetual
Security Contexts               : 25             perpetual
GTP/GPRS                        : Enabled        perpetual
Botnet Traffic Filter           : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces              : 1024           perpetual
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Active  perpetual
DES                             : Enabled        perpetual
3DES-AES                        : Enabled        perpetual
Security Contexts               : 50             perpetual
GTP/GPRS                        : Enabled        perpetual
Botnet Traffic Filter           : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

示例 4-9　故障转移对中的 ASA 服务模块 运行 show activation-key 命令的辅助设备输出

以下内容是辅助故障转移设备运行 **show activation-key** 命令的示例输出，其中显示了：

- 辅助设备许可证 （整合的永久许可证和基于时间的许可证）。
- “故障转移集群”许可证，该许可证是主设备和辅助设备的组合许可证。该许可证是在 ASA 上实际运行的许可证。该许可证中，反映主设备和辅助设备许可证的整合的值，会以粗体显示。
- 辅助设备的已安装的基于时间的许可证 （活动和非活动）。该设备没有任何基于时间的许可证，所以此示例输出中没有显示任何此类许可证。

```
ciscoasa# show activation-key detail

Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces              : 1024           perpetual
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Active  perpetual
DES                             : Enabled        perpetual
3DES-AES                        : Enabled        perpetual
Security Contexts               : 25             perpetual
GTP/GPRS                        : Disabled       perpetual
Botnet Traffic Filter           : Disabled       perpetual

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces              : 1024           perpetual
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Active  perpetual
```

```
DES                                 : Enabled        perpetual
3DES-AES                            : Enabled        perpetual
Security Contexts                   : 50             perpetual
GTP/GPRS                            : Enabled        perpetual
Botnet Traffic Filter               : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.
```

示例 4-10　在集群中运行 show activation-key 命令的输出

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9

 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 2 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 2 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 2 perpetual
 Total UC Proxy Sessions : 2 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

 Failover cluster licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 4 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 4 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 4 perpetual
 Total UC Proxy Sessions : 4 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
```

```
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

The flash permanent activation key is the SAME as the running permanent key.
```

监控共享许可证

如要监控共享许可证，输入以下任一命令。

命令	用途
show shared license [**detail** | **client** [*hostname*] | **backup**]	显示共享许可证统计信息。可选关键字仅适用于许可服务器：**detail** 关键字用于显示每个参与者的统计信息。要将显示内容限制为一个参与者的相关信息，请使用 **client** 关键字。 **backup** 关键字用于显示有关备用服务器的信息。 要清除共享许可证统计信息，请输入 **clear shared license** 命令。
show activation-key	显示在 ASA 上安装的许可证。**show version** 命令也可用于显示许可证信息。
show vpn-sessiondb	显示有关 VPN 会话的许可证信息。

示例

以下内容是在许可参与者上运行 **show shared license** 命令的示例输出。

```
ciscoasa>  show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
```

以下内容是在许可服务器上运行 **show shared license detail** 命令的示例输出。

```
ciscoasa>  show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
```

```
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0


Client Info:

Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

许可的功能历史记录

表 4-16 列出了各种功能变更以及实施该等功能变更的平台版本。

表 4-16　　许可的功能历史记录

功能名称	平台版本	功能信息
增加的连接数和 VLAN 数量	7.0(5)	增加了以下限制： • ASA5510 基础许可证连接数从 32000 提高至 50000；VLAN 数从 0 提高至 10。 • ASA5510 增强型安全许可证连接数从 64000 提高至 130000；VLAN 数从 10 提高至 25。 • ASA5520 连接数从 130000 提高至 280000；VLAN 数从 25 提高至 100。 • ASA5540 连接数从 280000 提高至 400000；VLAN 数从 100 提高至 200。
SSL VPN 许可证	7.1(1)	引入了 SSL VPN 许可证。
增加的 SSL VPN 许可证数量	7.2(1)	为 ASA 5550 及更高版本引入了 5000 名用户的 SSL VPN 许可证。

表 4-16　　许可的功能历史记录（续）

功能名称	平台版本	功能信息
ASA 5510 上基础许可证增加的接口数	7.2(2)	对于 ASA 5510 上的基础许可证，最大接口数从 3 个加上管理接口数，增至不受限制。
增加的 VLAN 数量	7.2(2)	ASA 5505 上增强型安全许可证 VLAN 的最大数量从 5（3 个全功能；1 个故障转移；一个限定于备用接口）增加至 20 个全功能接口。此外，中继端口数量从 1 增加到 8。现在有 20 个全功能接口，您不需要使用 backup interface 命令削弱备份 ISP 接口；您可以对其使用全功能接口。备用接口命令对于 Easy VPN 配置仍非常有用。 以下型号的 VLAN 数量限制也有增加：ASA 5510（对于基础许可证，从 10 增加到 50，对于增强型安全许可证，从 25 增加到 100）、ASA 5520（从 100 增加到 150）和 ASA 5550（从 200 增加到 250）。
对于 ASA 5510 增强型安全许可证的千兆以太网支持	7.2(3)	具有增强型安全许可证的 ASA 5510 现在在 Ethernet 0/0 和 0/1 端口上支持千兆以太网 (1000 Mbps)。在基础许可证中，它们将继续用作快速以太网 (100 Mbps) 端口。对于两种许可证，Ethernet 0/2、0/3 和 0/4 仍为快速以太网端口。 **注**　接口名称仍为 Ethernet 0/0 和 Ethernet 0/1。 使用 **speed** 命令更改接口上的速度，使用 **show interface** 命令查看当前为每个接口配置的速度。
高级终端评估许可证	8.0(2)	引入了高级终端评估许可证。作为 Cisco AnyConnect 或无客户端 SSL VPN 连接完成的一个条件，远程计算机扫描大幅扩展的防病毒软件和反间谍软件应用、防火墙、操作系统和关联更新的集合。它还扫描您指定的所有注册表项、文件名和进程名。它会将扫描结果发送至 ASA。ASA 使用用户登录凭据，以及计算机扫描结果来分配动态访问策略 (DAP)。 借助高级终端评估许可证，您可以配置更新不合规计算机，以使其符合版本要求的尝试，从而增强主机扫描。 思科可在独立于思科安全桌面的软件包中，提供主机扫描支持的应用和版本的列表的及时更新。
ASA 5510 的 VPN 负载均衡	8.0(2)	ASA 5510 增强型安全许可证现在支持 VPN 负载均衡。
AnyConnect for Mobile 许可证	8.0(3)	引入了 AnyConnect for Mobile 许可证。它允许 Windows 移动设备使用 AnyConnect 客户端连接到 ASA。
基于时间的许可证	8.0(4)/8.1(2)	引入了对基于时间的许可证的支持。
为 ASA 5580 增加的 VLAN 数	8.1(2)	ASA 5580 支持的 VLAN 数量从 100 增加到 250。
统一通信代理会话许可证	8.0(4)	引入了 UC 代理会话许可证。电话代理、状态联合代理和加密语音检查应用会将 TLS 代理会话用于其连接。每个 TLS 代理会话都将计入 UC 许可证限制。所有这些应用都在 UC 代理伞状结构下许可，可以混搭使用。 此功能在 8.1 版本中不可用。

表 4-16　　许可的功能历史记录（续）

功能名称	平台版本	功能信息
僵尸网络流量过滤器许可证	8.2(1)	引入了僵尸网络流量过滤器许可证。僵尸网络流量过滤器可以跟踪通向已知不良域名和 IP 地址的连接，从而防御恶意软件网络活动。
AnyConnect Essentials 许可证	8.2(1)	引入了 AnyConnect Essentials 许可证。此许可证允许 AnyConnect VPN 客户端访问 ASA。此许可证不支持基于浏览器的 SSL VPN 访问或思科安全桌面。对于这些功能，请激活 AnyConnect Premium 许可证，而不是 AnyConnect Essentials 许可证。 **注**　借助 AnyConnect Essentials 许可证，VPN 用户可以使用网络浏览器来进行登录，然后下载并启动 (WebLaunch) AnyConnect 客户端。 AnyConnect 客户端软件提供一组相同的客户端功能，无论是通过此许可证，还是通过 AnyConnect Premium 许可证启用。 AnyConnect Essentials 许可证不能在给定 ASA 上与以下许可证同时处于活动状态：AnyConnect Premium 许可证（所有类型）或高级终端评估许可证。然而，您可以在同一网络中的不同 ASA 上运行 AnyConnect Essentials 和 AnyConnect Premium 许可证。 默认情况下，ASA 使用 AnyConnect Essentials 许可证，但您可以通过先使用 **webvpn**，然后使用 **no anyconnect-essentials** 命令来禁用该许可证，以便使用其他许可证。
SSL VPN 许可证更改为 AnyConnect Premium SSL VPN 版本许可证	8.2(1)	SSL VPN 许可证的名称更改为 AnyConnect Premium SSL VPN 版本许可证。
SSL VPN 共享许可证	8.2(1)	引入了 SSL VPN 共享许可证。多个 ASA 可以根据需要共享 SSL VPN 会话池。
移动代理应用不再需要统一通信代理许可证	8.2(2)	移动代理不再需要 UC 代理许可证。
带 SSP-20 的 ASA 5585-X 的 10 GE I/O 许可证	8.2(3)	我们引入了带 SSP-20 的 ASA 5585-X 的 10 GE I/O 许可证，以便在光纤端口上支持 10 千兆以太网速度。默认情况下，SSP-60 支持 10 千兆以太网速度。 **注**　ASA 5585-X 在 8.3(x) 版本中不受支持。
带 SSP-10 的 ASA 5585-X 的 10 GE I/O 许可证	8.2(4)	我们引入了带 SSP-10 的 ASA 5585-X 的 10 GE I/O 许可证，以便在光纤端口上支持 10 千兆以太网速度。默认情况下，SSP-40 支持 10 千兆以太网速度。 **注**　ASA 5585-X 在 8.3(x) 版本中不受支持。
不相同的故障转移许可证	8.3(1)	在每台设备上不再需要相同的故障转移许可证。用于两台设备的许可证是主设备和辅助设备的组合许可证。 我们修改了以下命令：**show activation-key** 和 **show version**。

表 4-16　　许可的功能历史记录（续）

功能名称	平台版本	功能信息
可堆叠的基于时间的许可证	8.3(1)	基于时间的许可证现在可堆叠。在许多情况下，您可能需要更新您的基于时间的许可证，并从旧许可证无缝过渡到新许可证。对于仅在使用基于时间的许可证时才可用的功能，在您应用新许可证前，许可证没有到期尤为重要。ASA 允许您*堆叠*基于时间的许可证，因此您不必担心许可证到期，也不必担心因为过早安装新许可证而损失许可证时间。
公司间媒体引擎许可证	8.3(1)	引入了 IME 许可证。
多个基于时间的许可证同时处于活动状态	8.3(1)	您现在可以安装多个基于时间的许可证，每个功能同时只能有一个许可证处于活动状态。 我们修改了以下命令：**show activation-key** 和 **show version**。
基于时间的许可证的独立激活和停用。	8.3(1)	您现在可以使用一个命令来激活或停用基于时间的许可证。 我们修改了以下命令：**activation-key** [**activate** | **deactivate**]。
AnyConnect Premium SSL VPN 版本许可证更改为 AnyConnect Premium SSL VPN 许可证	8.3(1)	AnyConnect Premium SSL VPN 版本许可证的名称更改为 AnyConnect Premium SSL VPN 许可证。
用于出口的无负载加密映像	8.3(2)	如果您在 ASA 5505 至 5550 上安装无负载加密软件，则将禁用统一通信、强加密 VPN 和强加密管理协议。 **注**　此特殊映像仅在 8.3(x) 版本中受支持；要在 8.4(1) 及更高版本中获得无负载加密支持，您需要购买 ASA 的特殊硬件版本。
增加的 ASA 5550、5580 和 5585-X 的情景数	8.4(1)	对于带 SSP-10 的 ASA 5550 和 ASA 5585-X，最大情景数从 50 个增加至 100 个。对于带 SSP-20 的 ASA 5580 和 5585-X，最大情景数从 50 个增加至 250 个。
增加的 ASA 5580 和 5585-X 的 VLAN 数量	8.4(1)	对于 ASA 5580 和 5585-X，最大 VLAN 数从 250 个增加至 1024 个。
增加的 ASA 5580 和 5585-X 的连接数	8.4(1)	我们提高了防火墙连接限制： • ASA 5580-20 - 1,000,000 至 2,000,000。 • ASA 5580-40 - 2,000,000 至 4,000,000。 • 带 SSP-10 的 ASA 5585-X：750,000 至 1,000,000。 • 带 SSP-20 的 ASA 5585-X：1,000,000 至 2,000,000。 • 带 SSP-40 的 ASA 5585-X：2,000,000 至 4,000,000。 • 带 SSP-60 的 ASA 5585-X：2,000,000 至 10,000,000。
AnyConnect Premium SSL VPN 许可证更改为 AnyConnect Premium 许可证	8.4(1)	AnyConnect Premium SSL VPN 许可证的名称更改为 AnyConnect Premium 许可证。许可证信息显示从“SSL VPN Peers”更改为“AnyConnect Premium Peers”。
增加的 ASA 5580 的 AnyConnect VPN 会话数	8.4(1)	AnyConnect VPN 会话限制从 5,000 增加到 10,000。

表 4-16　　许可的功能历史记录（续）

功能名称	平台版本	功能信息
增加的 ASA 5580 的其他 VPN 会话的会话数	8.4(1)	其他 VPN 会话的限制从 5,000 增加到 10,000。
使用 IKEv2 的 IPsec 远程访问 VPN	8.4(1)	使用 IKEv2 的 IPsec 远程访问 VPN 已添加到 AnyConnect Essentials 和 AnyConnect Premium 许可证。 **注**　在我们对 ASA 上的 IKEv2 的支持中存在以下限制： 我们目前不支持重复的安全关联。 IKEv2 站点对站点会话已添加到其他 VPN 许可证（以前的 IPsec VPN）。其他 VPN 许可证包含在基础许可证中。
用于出口的无负载加密硬件	8.4(1)	对于无负载加密的型号（例如 ASA 5585-X），ASA 软件会禁用统一通信和 VPN 功能，从而使 ASA 可出口至特定国家/地区。
适用于 SSP-20 和 SSP-40 的双 SSP	8.4(2)	对于 SSP-40 和 SSP-60，您可以在同一个机箱中使用两个相同级别的 SSP。不支持混合使用不同级别的 SSP（例如，不支持混合使用 SSP-40 和 SSP-60）。每个 SSP 作为独立设备，都有独立的配置和管理。您可以视需要，将两个 SSP 用作故障转移对。当在机箱中使用两个 SSP 时，VPN 不受支持；注意，尽管如此，VPN 未被禁用。
ASA 5512-X 至 ASA 5555-X 的 IPS 模块许可证	8.6(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 上的 IPS SSP 软件模块需要 IPS 模块许可证。
ASA 5580 和 5585-X 的集群许可证。	9.0(1)	添加了 ASA 5580 和 5585-X 的集群许可证。
ASASM 上的 VPN 支持	9.0(1)	ASASM 现在支持所有 VPN 功能。
ASASM 上的统一通信支持	9.0(1)	ASASM 现在支持所有统一通信功能。
SSP-10 和 SSP-20 的 ASA 5585-X 双 SSP 支持（SSP-40 和 SSP-60 除外）；双 SSP 的 VPN 支持	9.0(1)	ASA 5585-X 现在支持使用所有 SSP 型号的双 SSP（在同一个机箱中，您可以使用两个相同级别的 SSP）。使用双 SSP 时，现在支持 VPN。
ASA 5500-X 对集群的支持	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 现在支持由 2 台设备组成的集群。默认情况下，在基础许可证中支持两台设备的集群；对于 ASA 5512-X，您需要增强型安全许可证。
对 ASA 5585-X 支持 16 个集群成员	9.2(1)	ASA 5585-X 现在支持由 16 台设备组成的集群。
引入了 ASAv 的 1 个虚拟 CPU 和 4 个虚拟 CPU 的标准与高级许可证	9.2(1)	引入了采用简单许可方案的 ASAv：标准或高级级别的 1 个虚拟 CPU 或 4 个虚拟 CPU 的永久许可证。无可用的附加许可证。

透明或路由防火墙模式

本章介绍如何将防火墙模式设置为路由或透明模式，以及防火墙在各种防火墙模式中是如何工作的。本章还包含有关自定义透明防火墙操作的信息。

可以在多情景模式中为每个情景独立设置防火墙模式。

- 第 5-1 页的有关防火墙模式的信息
- 第 5-6 页的防火墙模式的许可要求
- 第 5-6 页的默认设置
- 第 5-6 页的准则和限制
- 第 5-8 页的设置防火墙模式
- 第 5-8 页的为透明防火墙配置 ARP 检测
- 第 5-10 页的自定义透明防火墙的 MAC 地址表
- 第 5-11 页的监控透明防火墙
- 第 5-12 页的防火墙模式示例
- 第 5-23 页的防火墙模式的功能历史记录

有关防火墙模式的信息

- 第 5-1 页的有关路由防火墙模式的信息
- 第 5-2 页的有关透明防火墙模式的信息

有关路由防火墙模式的信息

在路由模式中，思科 ASA 被视为网络中的路由器跃点。路由模式支持多个接口。每个接口都位于不同的子网中。可以在各情景之间共享接口。

ASA 充当已连接网络之间的路由器，而每个接口都要求不同的子网上有一个 IP 地址。 ASA 支持多种动态路由协议。但是，我们建议使用上游和下游路由器的高级路由功能，而不是依靠 ASA 来满足各种各样的路由需求。

有关透明防火墙模式的信息

传统上，防火墙是路由跃点，并充当与其中一个屏蔽子网连接的主机的默认网关。另一方面，透明防火墙是第 2 层防火墙，充当“网络嵌入式防火墙”或“隐形防火墙”，而不被视为已连接设备的路由器跃点。

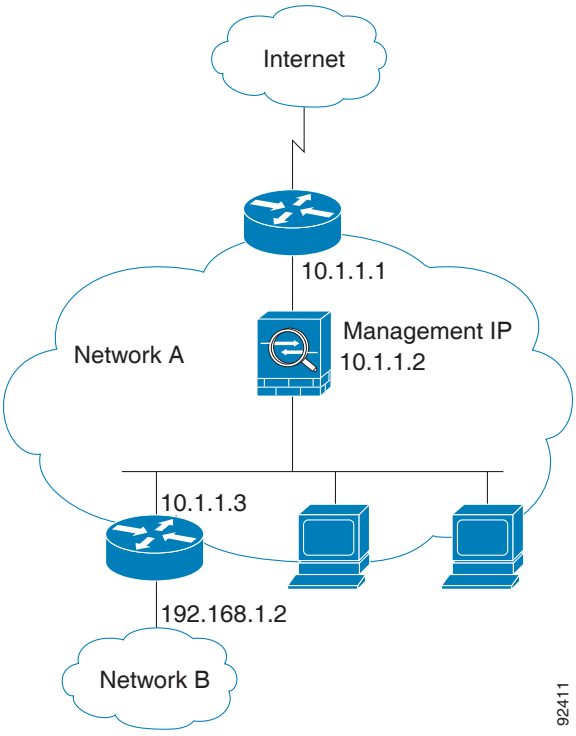
- 第 5-2 页的在网络中使用透明防火墙
- 第 5-3 页的网桥组
- 第 5-3 页的管理接口 （ASA 5512-X 及更高版本）
- 第 5-4 页的允许第 3 层流量
- 第 5-4 页的允许的 MAC 地址
- 第 5-4 页的不允许在路由模式中通过流量
- 第 5-4 页的 BPDU 处理
- 第 5-5 页的 MAC 地址与 路由查找
- 第 5-5 页的 ARP 检测
- 第 5-6 页的 MAC 地址表

在网络中使用透明防火墙

ASA 在其接口之间连接同一个网络。由于防火墙不是路由跃点，因此，您可以将透明防火墙轻松引入到现有网络中。

图 5-1 显示了典型的透明防火墙网络，其中的外部设备与内部设备在同一个子网上。内部路由器和主机显示为与外部路由器直接连接。

图 5-1　　透明防火墙网络

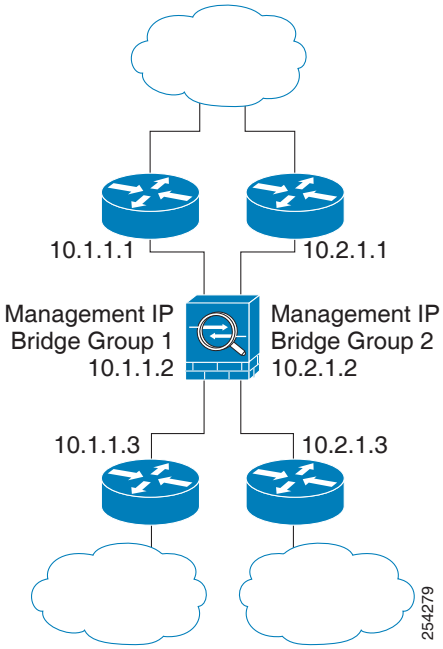


网桥组

如果不想产生安全情景开销，或者要最大限度地使用安全情景，请将接口一起组合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组流量与其他网桥组是隔离开的；流量不会路由到 ASA 内的另一个网桥组，且流量必须退出 ASA 后才能被外部路由器路由回到 ASA 中的另一个网桥组。虽然每个网桥组的桥接功能互为独立，但许多其他功能可以供所有网桥组共享。例如，所有网桥组共享一个系统日志服务器或 AAA 服务器配置。如需完全分隔安全策略，请将安全情景与每个情景中的一个网桥组配合使用。

图 5-2 显示了连接到 ASA 的两个网络，其中的 ASA 具有两个网桥组。

图 5-2　　具有两个网桥组的透明防火墙网络



注　每个网桥组均需要一个管理 IP 地址。 ASA 使用此 IP 地址作为源自网桥组的数据包的源地址。管理 IP 地址必须与所连接的网络位于相同的子网上。有关另一种管理方法，请参阅第 5-3 页的管理接口 （ASA 5512-X 及更高版本）。

ASA 不支持辅助网络上的流量；仅支持与管理 IP 地址相同的网络上的流量。

管理接口 （ASA 5512-X 及更高版本）

除了每个网桥组管理 IP 地址，还可以添加不属于任何网桥组的单独的管理*插槽/端口*接口，这种接口仅允许流向 ASA 的管理流量。有关详细信息，请参阅第 9-2 页的管理接口。

允许第 3 层流量

- 单播 IPv4 和 IPv6 流量可通过透明防火墙从安全性较高的接口自动流向安全性较低的接口，而无需 ACL。

注　可使用访问规则允许广播和组播流量通过。有关详细信息，请参阅 《防火墙配置指南

- ARP 可在两个方向通过透明防火墙，而无需 ACL。 ARP 流量可通过 ARP 检测进行控制。
- 对于从低安全性接口流向高安全性接口的第 3 层流量，要求低安全性接口上有扩展 ACL。有关详细信息，请参阅 《防火墙配置指南》。

允许的 MAC 地址

以下目标 MAC 地址可通过透明防火墙。下面未列出的任何 MAC 地址均已被丢弃。

- 真实的广播目标 MAC 地址等于 FFFF.FFFF.FFFF
- IPv4 组播 MAC 地址的范围是 0100.5E00.0000 到 0100.5EFE.FFFF
- IPv6 组播 MAC 地址的范围是 3333.0000.0000 到 3333.FFFF.FFFF
- BPDU 组播地址等于 0100.0CCC.CCCD
- AppleTalk 组播 MAC 地址的范围是 0900.0700.0000 到 0900.07FF.FFFF

不允许在路由模式中通过流量

在路由模式中，某些类型的流量无法通过 ASA，即使在 ACL 中允许这些流量。但是，透明防火墙可使用扩展 ACL（用于 IP 流量）或以太网类型 ACL（用于非 IP 流量）来允许几乎任何流量通过。

非 IP 流量 （例如 AppleTalk、 IPX、 BPDU 和 MPLS）可配置为使用以太网类型 ACL 通过。

注　透明模式 ASA 不允许 CDP 数据包以及没有大于或等于 0x600 的有效以太网类型的任何数据包通过。 BPDU 和 IS-IS 是例外，它们受支持。

允许路由模式功能通过流量

对于透明防火墙不直接支持的功能，可以允许流量通过，以使上游和下游路由器能够支持这些功能。例如，通过使用扩展 ACL，可以允许 DHCP 流量 （而不是不受支持的 DHCP 中继功能）或组播流量 （例如 IP/TV 产生的流量）。还可以通过透明防火墙建立路由协议邻接；可以根据扩展 ACL 允许 OSPF、RIP、EIGRP 或 BGP 流量通过。同样，诸如 HSRP 或 VRRP 之类的协议也可以通过 ASA。

BPDU 处理

为防止环路使用生成树协议，默认情况下允许 BPDU 通过。要阻止 BPDU，需要将以太网类型 ACL 配置为拒绝 BPDU。如果使用故障转移功能，您可能想要阻止 BPDU，以防止交换机端口在拓扑结构改变时进入阻止状态。有关详细信息，请参阅第 7-13 页的透明防火墙模式要求。

MAC 地址与 路由查找

当 ASA 在透明模式中运行时，是通过执行 MAC 地址查找而不是路由查找来确定数据包的传出接口。

但是，路由查找对于以下流量类型是必要的：

- 源自 ASA 的流量 - 例如，如果系统日志服务器位于远程网络上，必须使用静态路由，以便 ASA 可以到达该子网。
- 在 NAT 启用的情况下距离 ASA 至少一个跃点的流量 - ASA 需要执行路由查找来找到下一跳网关；您需要在 ASA 上添加静态路由以获得真实主机地址。
- 在检测已启用且终端至少距离 ASA 一个跃点的情况下出现的 IP 语音 (VoIP) 和 DNS 流量 - 例如，如果在 CCM 与 H.323 网关之间使用透明防火墙，且透明防火墙与 H.323 网关之间有一个路由器，则需要在 ASA 上添加静态路由，以使 H.323 网关能够成功完成调用。如果对检测的流量启用 NAT，将需要静态路由来确定嵌入在数据包中的真实主机地址的出口接口。受影响的应用包括：
  - CTIQBE
  - DNS
  - GTP
  - H.323
  - MGCP
  - RTSP
  - SIP
  - 瘦客户端 (SCCP)

ARP 检测

默认情况下，所有 ARP 数据包都可以通过 ASA。可以通过启用 ARP 检测来控制 ARP 数据包的流量。

当您启用 ARP 检测时，ASA 会将所有 ARP 数据包中的 MAC 地址、IP 地址和源接口与 ARP 表中的静态条目作比较，并执行以下操作：

- 如果 IP 地址、MAC 地址和源接口与 ARP 条目相匹配，ASA 将会允许数据包通过。
- 如果 MAC 地址、IP 地址或接口之间不匹配，ASA 将会丢弃数据包。
- 如果 ARP 数据包与静态 ARP 表中的任何条目都不匹配，可以将 ASA 设置为会将数据包从所有接口转发出去（泛洪）或者丢弃数据包。

注　专用管理接口 （如果有）不会以泛洪方式传输数据包，即使此参数被设置使用泛洪传输方式。

ARP 检测可防止恶意用户模拟其他主机或路由器（称为 ARP 欺骗）。ARP 欺骗可启用“中间人”攻击。例如，主机向网关路由器发送 ARP 请求；网关路由器以网关路由器的 MAC 地址作出响应。但是，攻击者会利用攻击者 MAC 地址而不是路由器 MAC 地址向主机发送另一个 ARP 响应。这样，攻击者就可以在将流量转发到路由器之前拦截所有的主机流量。

ARP 检测可确保，只要静态 ARP 表中的 MAC 地址和相关 IP 地址是正确的，攻击者就不能利用攻击者 MAC 地址发送 ARP 响应。

MAC 地址表

ASA 以与一般网桥或交换机类似的方式了解和构建 MAC 地址表：当设备通过 ASA 发送数据包时，ASA 会将 MAC 地址添加到自己的表中。此表将 MAC 地址与源接口关联起来，从而使 ASA 了解如何将要发送到设备的任何数据包从正确的接口发送出。

由于 ASA 是防火墙，因此，如果数据包的目标 MAC 地址不在此表中，ASA 将不会像一般网桥那样以泛洪方式传输所有接口上的原始数据包。相反，它会为直连设备或远程设备生成以下数据包：

- 面向直连设备的数据包 - ASA 生成目标 IP 地址的 ARP 请求，从而使 ASA 可以了解哪个接口接收 ARP 响应。
- 面向远程设备的数据包 - ASA 生成指向目标 IP 地址的 ping，从而使 ASA 可以了解哪个接口接收 ping 应答。

原始数据包将被丢弃。

防火墙模式的许可要求

下表显示了此功能的许可要求。

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

默认设置

默认模式为路由模式。

透明模式的默认设置

- 默认情况下，所有 ARP 数据包都可以通过 ASA。
- 如果启用 ARP 检测，默认情况下，会以泛洪方式传输不匹配的数据包。
- 动态 MAC 地址表条目的默认超时值为 5 分钟。
- 默认情况下，每个接口会自动获悉进入流量的 MAC 地址，ASA 会将相应的条目添加到 MAC 地址表中。

准则和限制

情景模式准则

应根据情景设置防火墙模式。

透明防火墙准则

- 在透明防火墙模式中，管理接口以与数据接口相同的方式更新 MAC 地址表；因此，不应将管理和数据接口连接到同一个交换机，除非将其中一个交换机端口配置为路由端口（默认情况下，Catalyst 交换机在所有的 VLAN 交换机端口上共享一个 MAC 地址）。否则，如果流量从物

理连接的交换机到达管理接口，ASA 会更新 MAC 地址表，以使用*管理*接口（而不是数据接口）来访问交换机。此操作会导致临时流量中断；出于安全原因，ASA 至少在 30 秒内不会再次更新从交换机到数据接口的数据包 MAC 地址表。

- 各个直连网络必须在同一个子网上。
- 请勿将网桥组管理 IP 地址指定为所连接设备的默认网关；设备需要将位于 ASA 另一端的路由器指定为默认网关。
- 透明防火墙的默认路由 （为管理流量提供返回路径需要有该路由）仅适用于来自一个网桥组网络的管理流量。这是因为，默认路由指定网桥组中的接口以及网桥组网络上的路由器 IP 地址，而您只能定义一个默认路由。如果您具有来自多个网桥组网络的管理流量，需要指定静态路由来确定您预期将会发出管理流量的网络。

有关更多准则，请参阅第 12-4 页的透明模式接口的准则和限制。

IPv6 准则

支持 IPv6。

附加准则和限制

- 如果更改防火墙模式，ASA 将会清除运行配置，因为很多命令在这两种模式中不受支持。启动配置将保持不变。如果在不保存的情况下重新加载，将会加载启动配置，且模式会恢复为原始设置。有关备份配置文件的信息，请参阅第 5-8 页的设置防火墙模式。
- 如果要将文本配置下载到 ASA 中以使用 **firewall transparent** 命令来更改模式，请务必将此命令置于配置的顶层；ASA 会在读取命令时更改模式，然后继续读取下载的配置。如果此命令显示在配置的后面部分，ASA 将会清除配置中在此命令前面的所有行。有关下载文本文件的信息，请参阅第 36-19 页的配置要使用的映像和启动配置。

透明模式中不支持的功能

表 5-1 列出了透明模式中不支持的功能。

表 5-1　　透明模式中不支持的功能

功能	说明
动态 DNS	-
DHCP 中继	透明防火墙可用作 DHCP 服务器，但它不支持 DHCP 中继命令。DHCP 中继并非必要的，因为可以使用两个扩展 ACL 来允许 DHCP 流量通过：一个允许 DCHP 请求从内部接口传输到外部，另一个允许应答从服务器朝着另一个方向传输。
动态路由协议	但是，可以为源自 ASA 的流量添加静态路由。还可以使用扩展 ACL 来允许动态路由协议通过 ASA。
组播 IP 路由	可以在扩展 ACL 中允许组播流量，从而允许这些流量通过 ASA。
QoS	-
针对直通流量的 VPN 终止	透明防火墙仅支持用于管理连接的站点到站点 VPN 隧道。它不会针对通过 ASA 的流量终止 VPN 连接。可以使用扩展 ACL 来允许 VPN 流量通过 ASA，但 ASA 不会终止非管理连接。也不支持无客户端 SSL VPN。
统一通信	-

设置防火墙模式

注　本节介绍如何 更改防火墙模式。我们建议先设置防火墙模式再执行任何其他配置，因为更改防火墙模式会清除运行配置。

先决条件

如果更改模式，ASA 将会清除运行配置（有关详细信息，请参阅第 5-6 页的准则和限制）。

- 如果有已填充的配置，请务必在更改模式前备份配置；创建新配置时，可以将备份的配置作为参考。请参阅第 36-23 页的备份和还原 配置或其他文件。
- 使用控制台端口处的 CLI 来更改模式。如果使用任何其他类型的会话（包括 ASDM 命令行界面工具或 SSH），将会在清除配置时断开连接，而且在任何情况下都必须使用控制台端口重新连接到 ASA。
- 在情景中设置模式。

详细步骤

注　如要将防火墙模式设置为透明模式，并要在配置被清除后配置 ASDM 管理访问，请参阅第 2-6 页的配置 ASDM 访问或第 2-6 页的配置 ASDM 访问。

命令	用途
firewall transparent **示例：** `ciscoasa(config)# firewall transparent`	将防火墙模式设置为透明模式。如要将模式更改为路由模式，请输入 **no firewall transparent** 命令。 **注**　系统不会提示您确认防火墙模式更改；更改会立即发生。

为透明防火墙配置 ARP 检测

本节介绍如何配置 ARP 检测。

- 第 5-8 页的配置 ARP 检测的任务流程
- 第 5-9 页的添加静态 ARP 条目
- 第 5-9 页的启用 ARP 检测

配置 ARP 检测的任务流程

如要配置 ARP 检测，请执行以下步骤：

步骤 1　按照第 5-9 页的添加静态 ARP 条目中所述添加静态 ARP 条目。ARP 检测会将 ARP 数据包与 ARP 表中的静态 ARP 条目作比较，因此，此功能需要静态 ARP 条目。

步骤 2　按照第 5-9 页的启用 ARP 检测中所述启用 ARP 检测。

添加静态 ARP 条目

ARP 检测会将 ARP 数据包与 ARP 表中的 ARP 条目进行比较。虽然主机通过 IP 地址识别数据包目标，但数据包在以太网上的实际传送依赖于以太网 MAC 地址。当路由器或主机要通过直连网络传送数据包时，它会发送 ARP 请求以获取与 IP 地址相关的 MAC 地址，然后根据 ARP 响应向 MAC 地址传送数据包。主机或路由器会保留一个 ARP 表，这样，就无需为要传送的每个数据包发送 ARP 请求。一旦有 ARP 响应在网络上发送，ARP 表就会动态更新；如果某个条目在一段时间内没有使用，该条目即会超时。如果条目不正确（例如，某个给定 IP 地址的 MAC 地址发生变化），不正确的条目将会超时，然后可以进行更新。

注　透明防火墙将 ARP 表中的动态 ARP 条目用于往返 ASA 的流量 （例如管理流量）。

详细步骤

命令	用途
arp *interface_name ip_address mac_address* **示例：** `ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100`	添加静态 ARP 条目。

示例

例如，如要允许使用外部接口上的 MAC 地址 0009.7cbe.2100 从 10.1.1.1 处的路由器作出 ARP 响应，请输入以下命令：

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

后续操作

按照第 5-9 页的启用 ARP 检测中所述启用 ARP 检测。

启用 ARP 检测

本节介绍如何启用 ARP 检测。

详细步骤

命令	用途
arp-inspection *interface_name* **enable** [**flood** | **no-flood**] **示例：** `ciscoasa(config)# arp-inspection outside enable no-flood`	启用 ARP 检测。 **flood** 关键字将不匹配的 ARP 数据包转发出所有接口，**no-flood** 关键字丢弃不匹配的数据包。 **注**　默认设置是以泛洪方式传输不匹配的数据包。要将通过 ASA 的 ARP 限制为仅限于静态条目，请将此命令设置为 **no-flood**。

示例

例如，如要在外部接口上启用 ARP 检测并丢弃所有不匹配的 ARP 数据包，请输入以下命令：

```
ciscoasa(config)# arp-inspection outside enable no-flood
```

自定义透明防火墙的 MAC 地址表

本节介绍如何自定义 MAC 地址表。

- 第 5-10 页的添加静态 MAC 地址
- 第 5-11 页的设置 MAC 地址超时
- 第 5-11 页的禁用 MAC 地址学习

添加静态 MAC 地址

通常情况下，当来自特定 MAC 地址的流量进入某个接口时，MAC 地址会动态添加到 MAC 地址表中。如有必要，您可以将静态 MAC 地址添加到 MAC 地址表中。添加静态条目的一个好处是，可以防止 MAC 欺骗。如果与静态条目具有相同 MAC 地址的客户端尝试向不匹配静态条目的接口发送流量，ASA 会丢弃这些流量并生成系统消息。当您添加静态 ARP 条目时（请参阅第 5-9 页的添加静态 ARP 条目），静态 MAC 地址条目会自动添加到 MAC 地址表中。

如要将静态 MAC 地址添加到 MAC 地址表中，请输入以下命令：

命令	用途
mac-address-table static *interface_name mac_address* **示例：** `ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100`	添加静态 MAC 地址条目。 *interface_name* 是源接口。

设置 MAC 地址超时

动态 MAC 地址表条目的默认超时值为 5 分钟，但您可以更改超时。如要更改超时，请输入以下命令：

命令	用途
mac-address-table aging-time *timeout_value* **示例：** `ciscoasa(config)# mac-address-table aging-time 10`	设置 MAC 地址条目超时。 *timeout_value*（以分钟为单位）介于 5 到 720（12 小时）之间。默认值为 5 分钟。

禁用 MAC 地址学习

默认情况下，每个接口会自动获悉进入流量的 MAC 地址，ASA 会将相应的条目添加到 MAC 地址表中。如有必要，可以禁用 MAC 地址学习；但一般情况下，没有流量可以通过 ASA，除非向该地址表静态添加了 MAC 地址。

如要禁用 MAC 地址学习，请输入以下命令：

命令	用途
mac-learn *interface_name* **disable** **示例：** `ciscoasa(config)# mac-learn inside disable`	禁用 MAC 地址学习。 此命令的 **no** 形式会重新启用 MAC 地址学习。**clear configure mac-learn** 命令会对所有接口重新启用 MAC 地址学习。

监控透明防火墙

- 第 5-11 页的监控 ARP 检测
- 第 5-12 页的监控 MAC 地址表

监控 ARP 检测

如要监控 ARP 检测，请执行以下任务：

命令	用途
show arp-inspection	显示所有接口上的 ARP 检测的当前设置。

监控 MAC 地址表

可以查看整个 MAC 地址表（包括两个接口的静态和动态条目），也可以查看某个接口的 MAC 地址表。如要查看 MAC 地址表，请输入以下命令：

命令	用途
show mac-address-table [*interface_name*]	显示 MAC 地址表。

示例

以下是 **show mac-address-table** 命令（显示整个 MAC 地址表）的输出示例：

```
ciscoasa# show mac-address-table
interface          mac address       type      Time Left
-----------------------------------------------------------------------
outside            0009.7cbe.2100    static      -
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

以下是 **show mac-address-table** 命令（显示内部接口的 MAC 地址表）的输出示例：

```
ciscoasa# show mac-address-table inside
interface          mac address       type      Time Left
-----------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

防火墙模式示例

本节包括说明流量如何通过 ASA 的示例。

- 第 5-12 页的数据如何在路由防火墙模式中通过 ASA
- 第 5-18 页的数据如何通过透明防火墙

数据如何在路由防火墙模式中通过 ASA

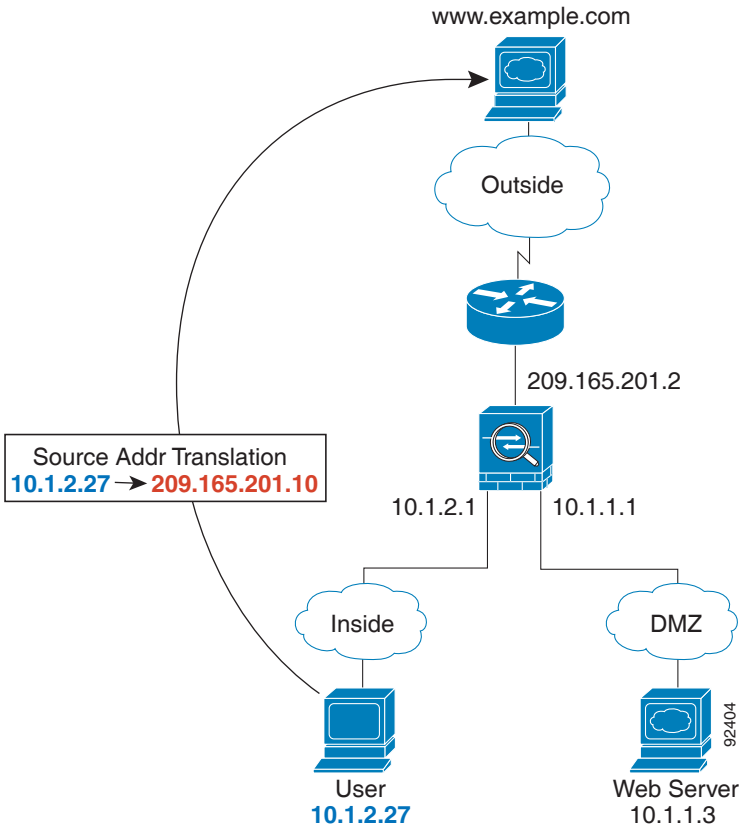
本节介绍数据如何在路由防火墙模式中通过 ASA。

- 第 5-13 页的内部用户访问网络服务器
- 第 5-13 页的外部用户访问 DMZ 上的网络服务器
- 第 5-15 页的内部用户访问 DMZ 上的网络服务器
- 第 5-16 页的外部用户尝试访问内部主机
- 第 5-17 页的 DMZ 用户尝试访问内部主机

内部用户访问网络服务器

图 5-3 显示了内部用户访问外部网络服务器。

图 5-3　　从内部到外部



以下步骤介绍数据如何通过 ASA（请参阅图 5-3）：

1. 内部网络中的用户从 www.example.com 请求访问网页。
2. ASA 接收数据包；由于是新会话，因此，ASA 会根据安全策略条款（访问列表、过滤器、AAA）验证数据包是否获允许。

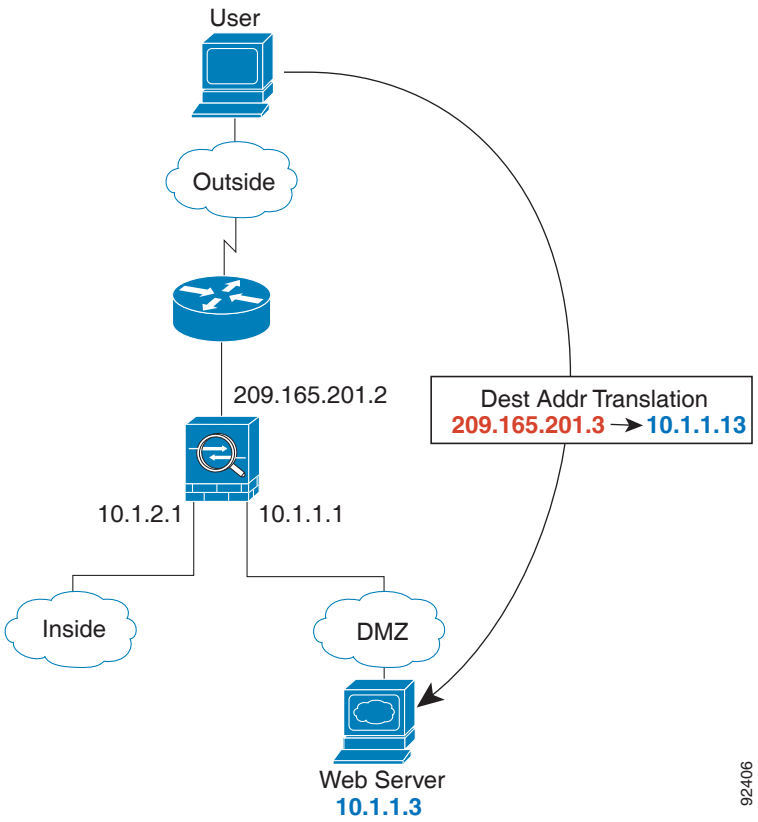
   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. ASA 将本地源地址 (10.1.2.27) 转换为全局地址 209.165.201.10 （该地址位于外部接口子网上）。

   全局地址可以位于任何子网上，但如果全局地址位于外部接口子网上，路由将会变得简单。
4. 然后， ASA 会记录有关会话已建立的信息，并从外部接口转发数据包。
5. 当 www.example.com 响应请求时，数据包会通过 ASA；由于会话已建立，因此，数据包会绕过与新连接相关的很多查找。ASA 通过将全局目标地址逆向转换为本地用户地址 10.1.2.27 来执行 NAT。
6. ASA 将数据包转发给内部用户。

外部用户访问 DMZ 上的网络服务器

图 5-4 显示了外部用户访问 DMZ 网络服务器。

图 5-4　从外部到 DMZ



以下步骤介绍数据如何通过 ASA（请参阅图 5-4）：

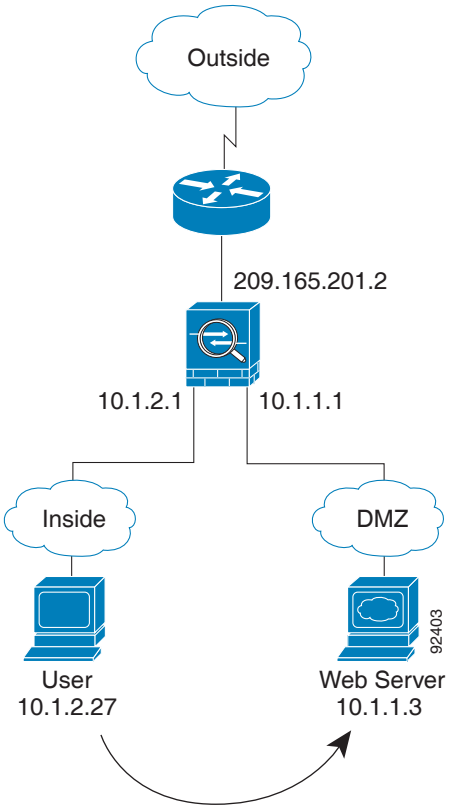
1. 外部网络上的用户使用全局目标地址 209.165.201.3（该地址位于外部接口子网上）从 DMZ 网络服务器请求访问网页。
2. ASA 接收数据包，并将目标地址逆向转换为本地地址 10.1.1.3。
3. 由于是新会话，因此，ASA 会根据安全策略条款（访问列表、过滤器、AAA）验证数据包是否获允许。

   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
4. 然后，ASA 会将会话条目添加到快速路径，并从 DMZ 接口转发数据包。
5. 当 DMZ 网络服务器响应请求时，数据包会通过 ASA；由于会话已建立，因此，数据包会绕过与新连接相关的很多查找。 ASA 通过将本地源地址转换为 209.165.201.3 来执行 NAT。
6. ASA 将数据包转发给外部用户。

内部用户访问 DMZ 上的网络服务器

图 5-5 显示了内部用户访问 DMZ 网络服务器。

图 5-5　从内部到 DMZ



以下步骤介绍数据如何通过 ASA（请参阅图 5-5）：

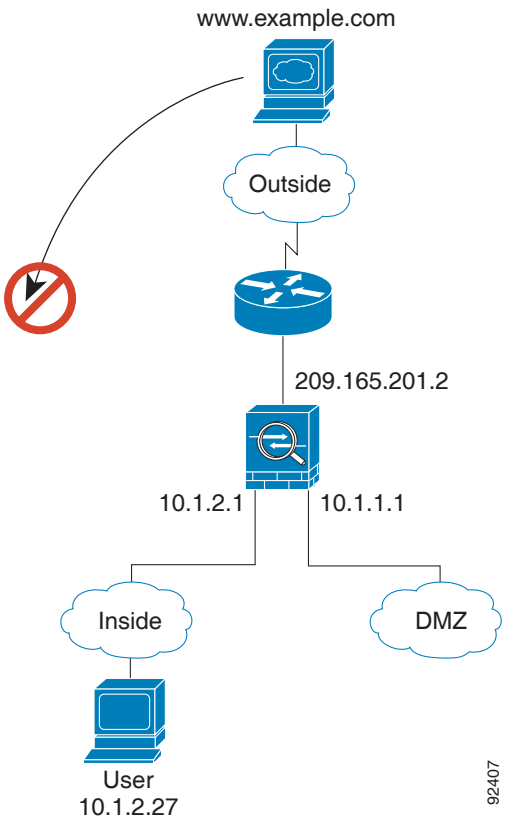
1. 内部网络上的用户使用目标地址 10.1.1.3 从 DMZ 网络服务器请求访问网页。
2. ASA 接收数据包；由于是新会话，因此，ASA 会根据安全策略条款（访问列表、过滤器、AAA）验证数据包是否获允许。

   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. 然后，ASA 会记录有关会话已建立的信息，并从 DMZ 接口将数据包转发出去。
4. 当 DMZ 网络服务器响应请求时，数据包会通过快速路径，这样可使数据包绕过与新连接相关的很多查找。
5. ASA 将数据包转发给内部用户。

外部用户尝试访问内部主机

图 5-6 显示了外部用户尝试访问内部网络。

图 5-6　从外部到内部



以下步骤介绍数据如何通过 ASA（请参阅图 5-6）：

1. 外部网络上的用户尝试访问内部主机（假设主机具有可路由的 IP 地址）。

   如果内部网络使用专用地址，则外部用户在没有执行 NAT 的情况下将无法访问内部网络。外部用户可能会通过使用现有 NAT 会话尝试访问内部用户。

2. ASA 接收数据包；由于是新会话，因此，ASA 会根据安全策略（访问列表、过滤器、AAA）验证数据包是否获允许。

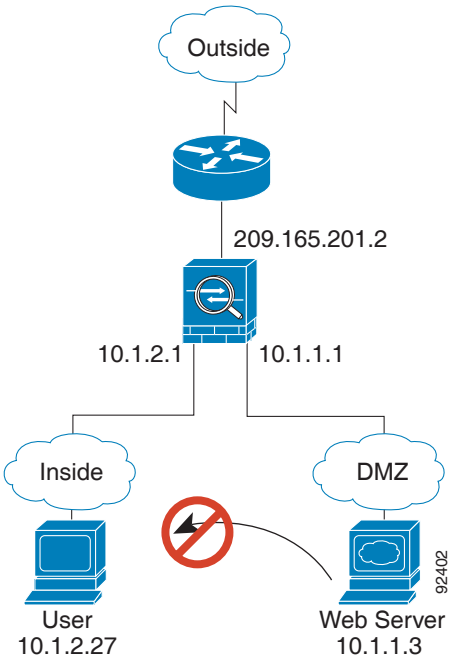
3. 数据包被拒绝，且 ASA 丢弃数据包且记录连接尝试情况。

   如果外部用户尝试攻击内部网络，ASA 会采用很多技术来确定数据包是否对已建立的会话有效。

DMZ 用户尝试访问内部主机

图 5-7 显示了 DMZ 中的用户尝试访问内部网络。

图 5-7　　从 DMZ 到内部



以下步骤介绍数据如何通过 ASA（请参阅图 5-7）：

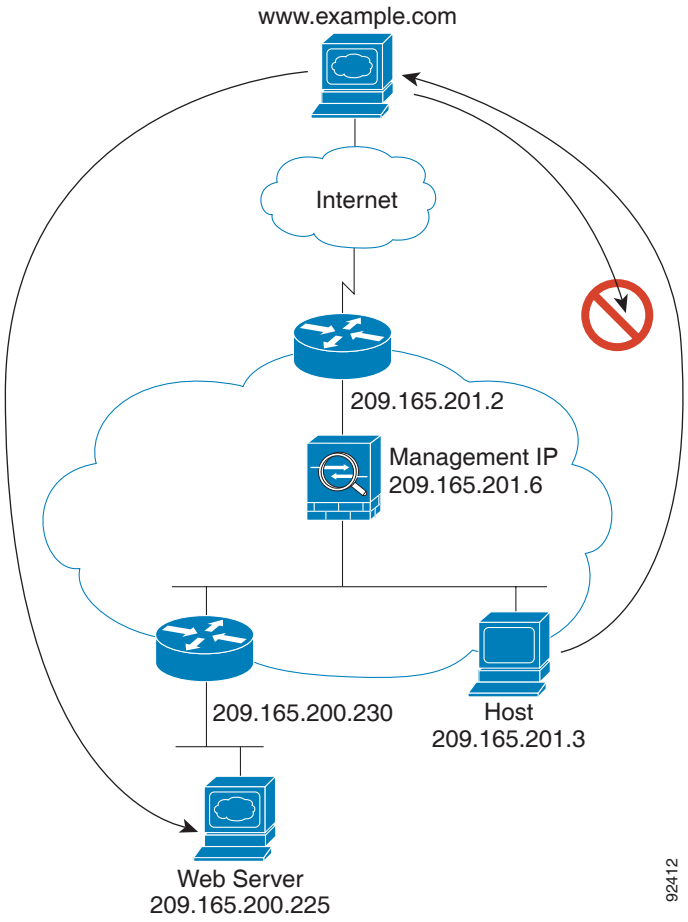
1. DMZ 网络上的用户尝试访问内部主机。由于 DMZ 不必路由互联网上的流量，因此，专用寻址方案不会防止路由。
2. ASA 接收数据包；由于是新会话，因此，ASA 会根据安全策略（访问列表、过滤器、AAA）验证数据包是否获允许。

   数据包被拒绝，且 ASA 丢弃数据包且记录连接尝试情况。

数据如何通过透明防火墙

图 5-8 显示了包含公共网络服务器的内部网络上的典型透明防火墙实施。ASA 有一个允许内部用户访问互联网资源的访问列表。另一个访问列表则允许外部用户只能访问内部网络上的网络服务器。

图 5-8　典型的透明防火墙数据路径



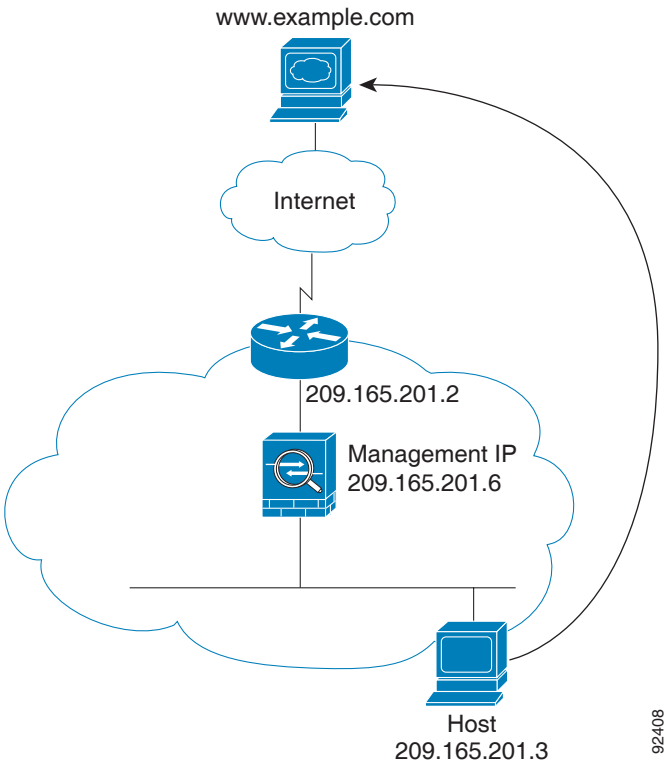
本节介绍数据如何通过 ASA。

- 第 5-19 页的内部用户访问网络服务器
- 第 5-20 页的内部用户使用 NAT 访问网络服务器
- 第 5-21 页的外部用户访问内部网络上的网络服务器
- 第 5-22 页的外部用户尝试访问内部主机

内部用户访问网络服务器

图 5-9 显示了内部用户访问外部网络服务器。

图 5-9　从内部到外部



以下步骤介绍数据如何通过 ASA（请参阅图 5-9）：

1. 内部网络中的用户从 www.example.com 请求访问网页。
2. ASA 接收数据包，并在必要时将源 MAC 地址添加到 MAC 地址表中。由于是新会话，因此，ASA 会根据安全策略条款（访问列表、过滤器、AAA）验证数据包是否获允许。

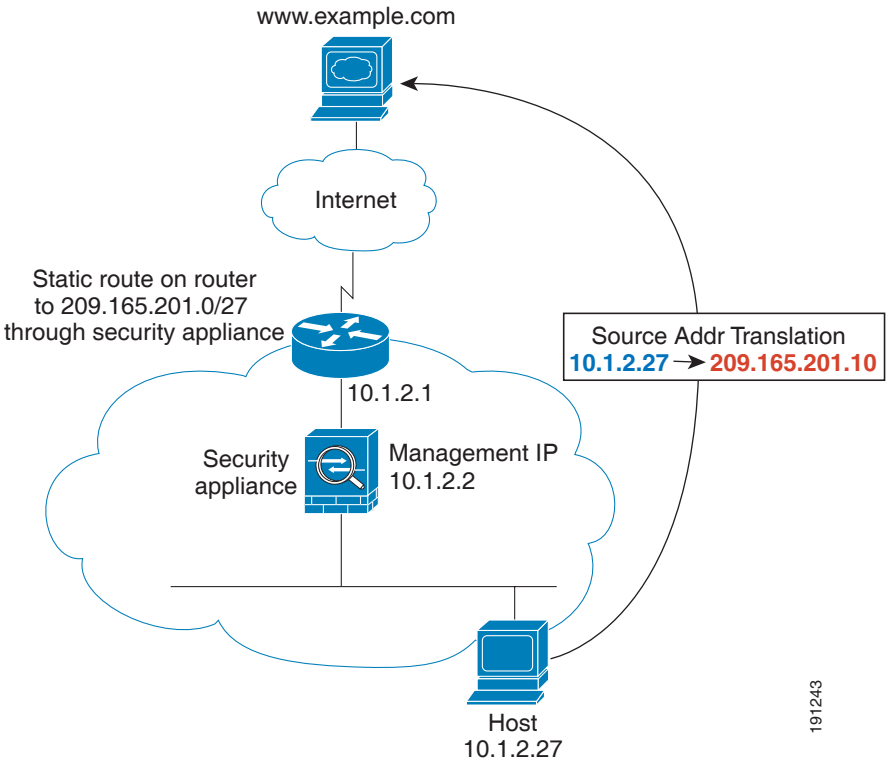
   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. ASA 记录有关会话已建立的信息。
4. 如果目标 MAC 地址在其表中，ASA 会将数据包从外部接口转发出去。目标 MAC 地址是上游路由器的地址 (209.165.201.2)。

   如果目标 MAC 地址不在 ASA 表中，ASA 会通过发送 ARP 请求或 ping 来尝试发现 MAC 地址。第一个数据包将被丢弃。
5. 网络服务器响应请求；由于会话已建立，因此，数据包会绕过与新连接相关的很多查找。
6. ASA 将数据包转发给内部用户。

内部用户使用 NAT 访问网络服务器

图 5-10 显示了内部用户访问外部网络服务器。

图 5-10　使用 NAT 从内部到外部



以下步骤介绍数据如何通过 ASA（请参阅图 5-10）：

1. 内部网络中的用户从 www.example.com 请求访问网页。
2. ASA 接收数据包，并在必要时将源 MAC 地址添加到 MAC 地址表中。由于是新会话，因此，ASA 会根据安全策略条款 （访问列表、过滤器、 AAA）验证数据包是否获允许。

   对于多情景模式，ASA 会首先根据唯一接口对数据包进行分类。
3. ASA 会将真实地址 (10.1.2.27) 转换为映射地址 209.165.201.10。

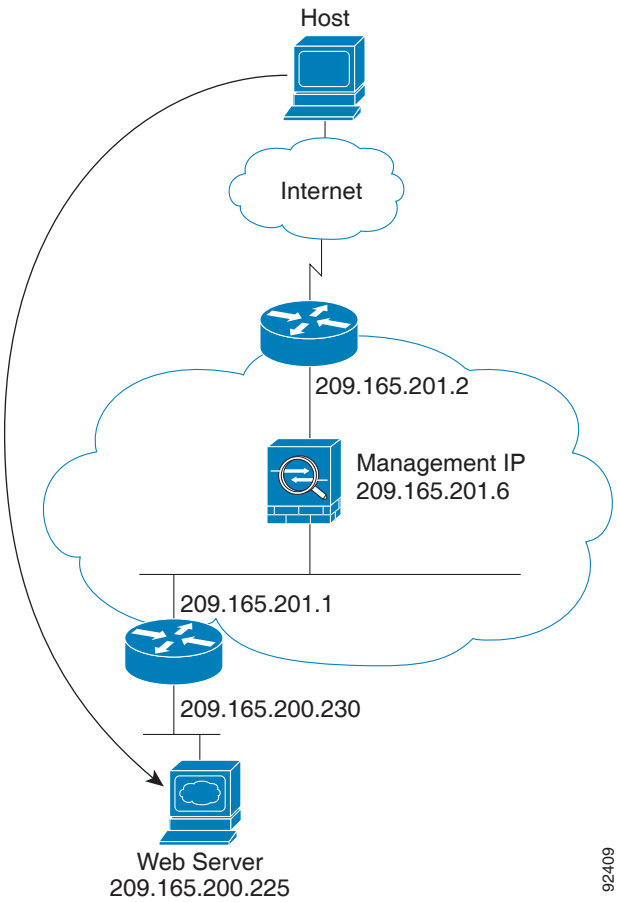
   由于映射地址与外部接口不在相同的网络上，因此，请确保上游路由器具有至映射网络（该网络指向 ASA）的静态路由。
4. 然后，ASA 会记录有关会话已建立的信息，并从外部接口转发数据包。
5. 如果目标 MAC 地址在其表中，ASA 会将数据包从外部接口转发出去。目标 MAC 地址是上游路由器的地址 (10.1.2.1)。

   如果目标 MAC 地址不在 ASA 表中，ASA 会通过发送 ARP 请求和 ping 来尝试发现 MAC 地址。第一个数据包将被丢弃。
6. 网络服务器响应请求；由于会话已建立，因此，数据包会绕过与新连接相关的很多查找。
7. ASA 通过将映射地址逆向转换为真实地址 10.1.2.27 来执行 NAT。

外部用户访问内部网络上的网络服务器

图 5-11 显示了外部用户访问内部网络服务器。

图 5-11　从外部到内部



以下步骤介绍数据如何通过 ASA（请参阅图 5-11）：

1. 外部网络上的用户从内部网络服务器请求访问网页。
2. ASA 接收数据包，并在必要时将源 MAC 地址添加到 MAC 地址表中。由于是新会话，因此，ASA 会根据安全策略条款（访问列表、过滤器、AAA）验证数据包是否获允许。

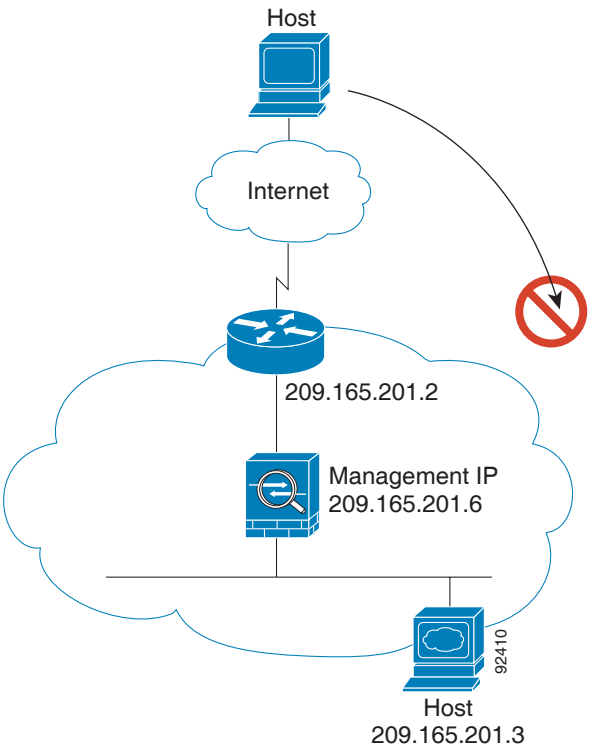
   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. ASA 记录有关会话已建立的信息。
4. 如果目标 MAC 地址在其表中，ASA 会将数据包从内部接口转发出去。目标 MAC 地址是下游路由器的地址 (209.165.201.1)。

   如果目标 MAC 地址不在 ASA 表中，ASA 会通过发送 ARP 请求和 ping 来尝试发现 MAC 地址。第一个数据包将被丢弃。
5. 网络服务器响应请求；由于会话已建立，因此，数据包会绕过与新连接相关的很多查找。
6. ASA 将数据包转发给外部用户。

外部用户尝试访问内部主机

图 5-12 显示了外部用户尝试访问内部网络上的主机。

图 5-12　从外部到内部



以下步骤介绍数据如何通过 ASA（请参阅图 5-12）：

1. 外部网络上的用户尝试访问内部主机。
2. ASA 接收数据包，并在必要时将源 MAC 地址添加到 MAC 地址表中。由于是新会话，因此，ASA 会根据安全策略条款（访问列表、过滤器、AAA）验证数据包是否获允许。

   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. 由于没有允许外部主机的访问列表，因此数据包被拒绝，且 ASA 丢弃数据包。
4. 如果外部用户尝试攻击内部网络，ASA 会采用很多技术来确定数据包是否对已建立的会话有效。

防火墙模式的功能历史记录

表 5-2 列出了各种功能变更以及实施该等功能变更的平台版本。

表 5-2　　防火墙模式的功能历史记录

功能名称	平台版本	功能信息
透明防火墙模式	7.0(1)	透明防火墙是第 2 层防火墙，充当类似于“网络嵌入式防火墙”或“隐形防火墙”，而不被视为已连接设备的路由器跃点。 我们引入了以下命令：**firewall transparent**、 **show firewall**。
ARP 检测	7.0(1)	ARP 检测会将所有 ARP 数据包中的 MAC 地址、IP 地址和源接口与 ARP 表中的静态条目作比较。 我们引入了以下命令：**arp**、 **arp-inspection** 和 **show arp-inspection**。
MAC 地址表	7.0(1)	透明防火墙模式使用 MAC 地址表。 我们引入了以下命令：**mac-address-table static**、**mac-address-table aging-time**、 **mac-learn disable** 和 **show mac-address-table**。
透明防火墙网桥组	8.4(1)	如果不想产生安全情景开销，或者要最大限度地使用安全情景，请将接口一起组合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组流量与其他网桥组是隔离开的。可以在单模式或多模式中为每个情境最多配置 8 个网桥组，每个网桥组最多可配置 4 个接口。 **注**　虽然可以在 ASA 5505 上配置多个网桥组，但在 ASA 5505 上，透明模式中 2 个数据接口这一限制意味着只能有效使用 1 个网桥组。 我们引入了以下命令：**interface bvi**、 **bridge-group**、 **show bridge-group**。
针对未连接的子网增加 ARP 缓存	8.4(5)/9.1(2)	默认情况下，ASA ARP 缓存仅包含来自直连子网的条目。现在，可以启用 ARP 缓存，以将非直连子网也包含在内。除非您了解安全风险，否则我们不建议启用此功能。此功能有助于缓解针对 ASA 的拒绝服务攻击 (DoS)；任何接口上的用户都可以发出很多 ARP 应答，还可以使用虚假条目来造成 ASA ARP 表过载。 在以下情况下，可能需要使用此功能： • 使用辅助子网。 • 使用邻接路由器上的代理 ARP 来进行流量转发。 我们引入了以下命令：**arp permit-nonconnected**。

表 5-2　　防火墙模式的功能历史记录（续）

功能名称	平台版本	功能信息
多情景模式中的混合防火墙模式支持	8.5(1)/9.0(1)	可以在多情景模式中为每个情景独立设置防火墙模式，因此，有些可以在透明模式中运行，有些可以在路由模式中运行。 我们修改了以下命令：**firewall transparent**。
透明模式的网桥组最大数量增加到 250	9.3(1)	网桥组最大数量从 8 增加到 250。在单情景模式和多情景模式的每个情景中，最多可配置 250 个网桥组，每组最多 4 个接口。 我们修改了以下命令：**interface bvi**、 **bridge-group**。

第 2 部分

高可用性和可扩展性

多情景模式

本章介绍如何在思科 ASA 上配置多个安全情景。

- 第 6-1 页的安全情景的相关信息
- 第 6-12 页的多情景模式的许可要求
- 第 6-13 页的准则和限制
- 第 6-14 页的默认设置
- 第 6-14 页的配置多情景
- 第 6-23 页的在情景和系统执行空间之间切换
- 第 6-23 页的管理安全情景
- 第 6-26 页的监控安全情景
- 第 6-36 页的多情景模式的配置示例
- 第 6-37 页的多情景模式的功能历史记录

安全情景的相关信息

您可以将单台 ASA 分区为多台称为安全情景的虚拟设备。每个情景都可以作为独立设备，拥有自己的安全策略、接口和管理员。多情景类似于拥有多台独立设备。有关在多情景模式中不受支持的功能，请参阅第 6-13 页的准则和限制。

本节提供安全情景的概述。

- 第 6-2 页的安全情景的常见用途
- 第 6-2 页的情景配置文件
- 第 6-2 页的 ASA 如何对数据包分类
- 第 6-6 页的级联安全情景
- 第 6-7 页的对安全情景的管理访问
- 第 6-8 页的资源管理的相关信息
- 第 6-10 页的有关 MAC 地址的信息

安全情景的常见用途

您可能想要在以下情况下使用多安全情景：

- 您是服务提供商，并想要将安全服务销售给许多客户。通过在 ASA 上启用多安全情景，您可以实施经济高效、节省空间的解决方案，该解决方案可使所有客户流量彼此分隔而又安全，同时还能简化配置。
- 您所在的组织是大型企业或大学校园，并且希望使各部门完全分隔开。
- 您所在的组织是需要为不同部门提供不同安全策略的企业。
- 您有需要多个 ASA 的任何网络。

情景配置文件

本节介绍 ASA 如何实施多情景模式配置。

- 第 6-2 页的情景配置
- 第 6-2 页的系统配置
- 第 6-2 页的管理情景配置

情景配置

对于每个情景，ASA 包括一个配置，该配置确定安全策略、接口和您可以在独立设备上配置的所有选项。您可以在闪存中存储情景配置，也可以从 TFTP、 FTP 或 HTTP(S) 服务器下载情景配置。

系统配置

在系统配置 （与单模式配置类似，为启动配置）中，系统管理员可以配置每个情景配置位置、分配的接口以及其他的情景运行参数，从而添加和管理情景。系统配置可识别 ASA 的基本设置。系统配置本身不包括任何网络接口或网络设置；相反，当系统需要访问网络资源时 （例如，从服务器下载情景），它将使用被指定为*管理员情景*的情景之一。系统配置会包含仅用于故障转移流量的专用故障转移接口。

管理情景配置

管理情景与任何其他情景一样，不同之处在于，当用户登录管理情景时，该用户将具有系统管理员权限，能够访问系统和所有其他情景。管理情景在任何情况下都不受限制，可用作常规情景。但是，登录至管理情景会授予您所有情景的管理员特权，因此您可能需要限制对管理情景的访问，限制为适当用户可以访问。管理情景必须驻留在闪存上，而不是远程驻留。

如果您的系统已处于多情景模式中，或者，您从单模式进行转换，管理情景会自动创建为内部闪存上名为 admin.cfg 的文件。此情景名为“admin”。如果您不希望将 admin.cfg 用作管理情景，则可以更改管理情景。

ASA 如何对数据包分类

进入 ASA 的每个数据包都必须进行分类，以便 ASA 能够确定将数据包发送到哪个情景。

- 第 6-3 页的有效分类器条件
- 第 6-4 页的分类示例

注　如果目标 MAC 地址为组播或广播 MAC 地址，则数据包将会被复制并发送到每个情景。

有效分类器条件

本节介绍分类器使用的条件。

- 第 6-3 页的唯一接口
- 第 6-3 页的唯一 MAC 地址
- 第 6-3 页的 NAT 配置

注　对于目标是接口的管理流量，接口 IP 地址将用于分类。

路由表不会被用于数据包分类。

唯一接口

如果仅有一个情景与入口接口关联，则 ASA 会将数据包分类至该情景。在透明防火墙模式中，会要求有用于情景的唯一接口，因此，总是会使用此方法来对数据包进行分类。

唯一 MAC 地址

如果多个情景共享一个接口，则分类器会在每个情景中使用分配至该接口的唯一 MAC 地址。上游路由器无法直接路由至不具有唯一 MAC 地址的情景。默认情况下，MAC 地址的自动生成会被启用。配置每个接口时，您也可以手动设置 MAC 地址。

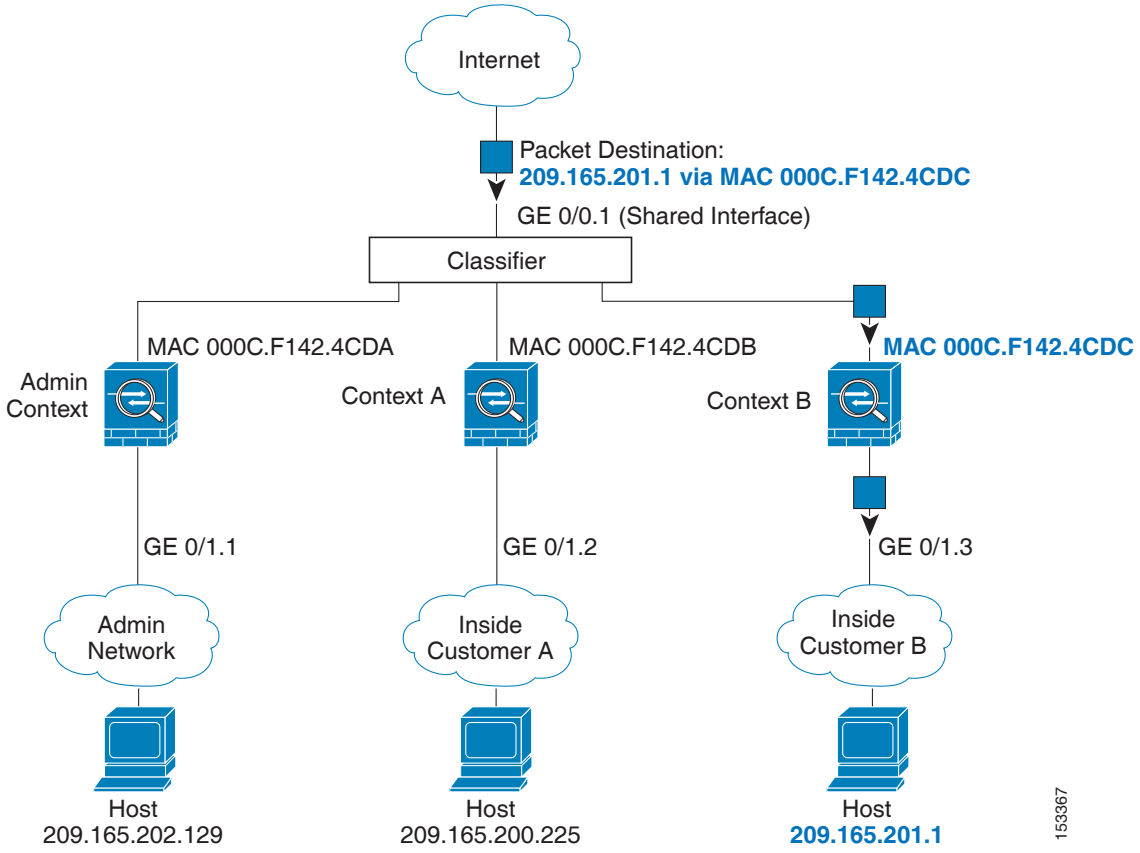
NAT 配置

如果您禁用唯一 MAC 地址，ASA 会使用 NAT 配置中的映射地址对数据包进行分类。我们建议使用 MAC 地址而不是 NAT，这样，无论 NAT 配置的完整度如何，都可以对流量进行分类。

分类示例

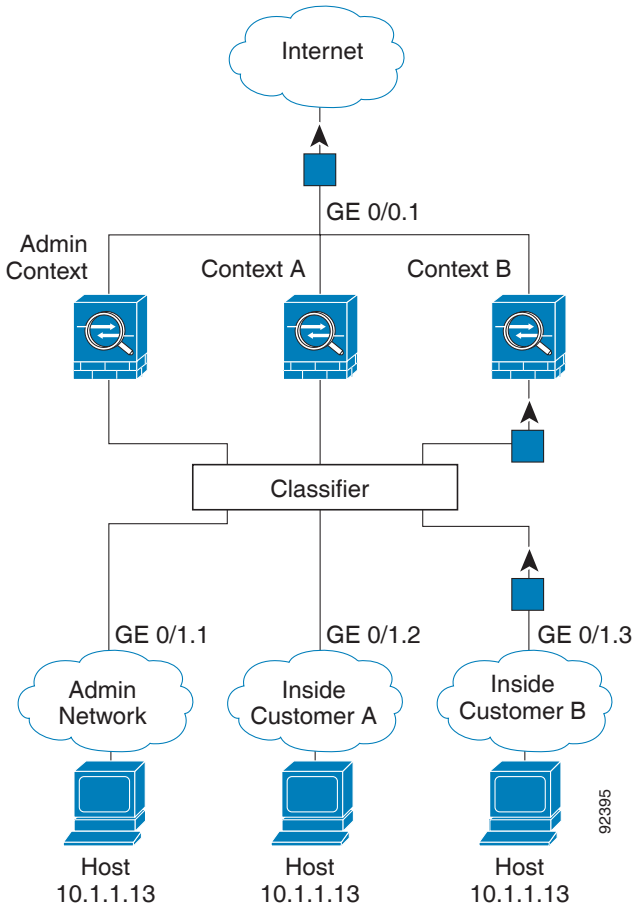
图 6-1 展示了共享一个外部接口的多情景。因为情景 B 包括路由器向其发送数据包的 MAC 地址，分类器会将该数据包分配至情景 B。

图 6-1　使用 MAC 地址的共享接口数据包分类



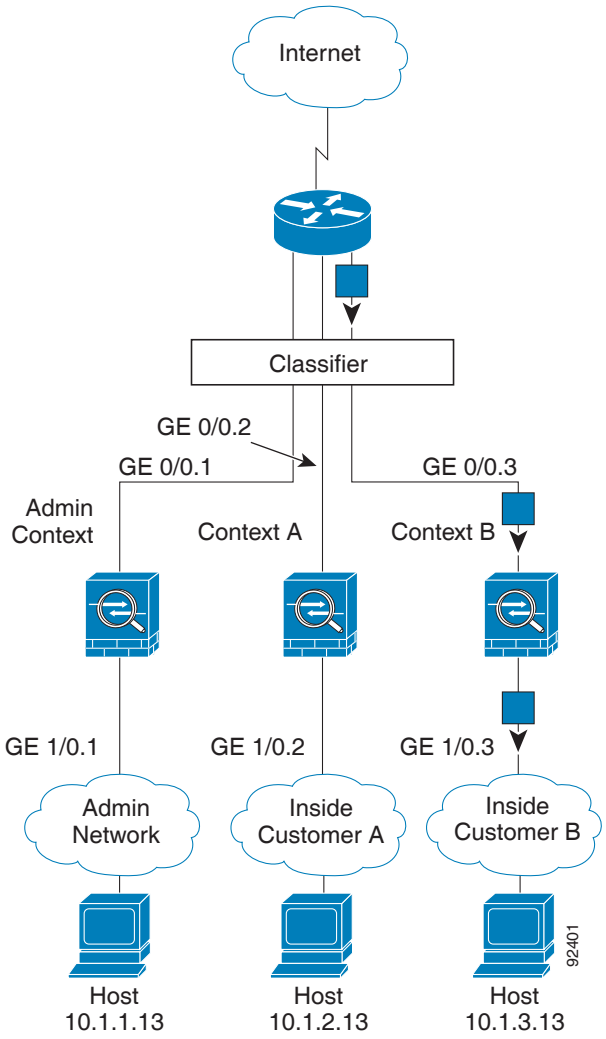
请注意，所有新的传入流量都必须加以分类，即使其来自内部网络。图 6-2 展示了访问互联网的情景 B 内部网络上的主机。因为入口接口是已分配至情景 B 的 Gigabit Ethernet 0/1.3，分类器会将数据包分配至情景 B。

图 6-2　来自内部网络的传入流量



对于透明防火墙，您必须使用唯一接口。图 6-3 展示了来自互联网，目标为情景 B 内部网络上的一台主机的数据包。因为入口接口是已分配至情景 B 的 Gigabit Ethernet 1/0.3，分类器会将数据包分配至情景 B。

图 6-3　透明防火墙情景



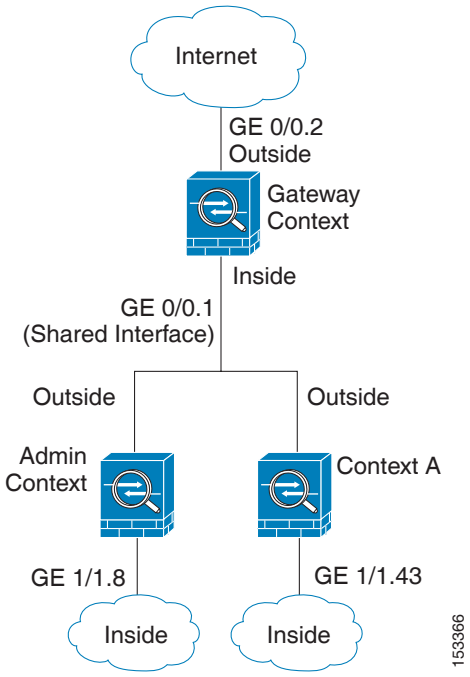
级联安全情景

将一个情景直接置于另一情景之前称为*级联情景*；一个情景的外部接口与另一个情景的内部接口是同一接口。如果您想要在顶级情景中配置共享参数，从而简化某些情景的配置，您可能会想要级联情景。

注　级联情景需要用于每个情景接口的唯一 MAC 地址（默认设置）。由于在不采用 MAC 地址的共享接口上分类数据包存在的限制，我们不建议使用不采用唯一 MAC 地址的级联情景。

图 6-4 展示了网关之后有两个情景的网关情景。

图 6-4　　级联情景



对安全情景的管理访问

ASA 提供了多情景模式中的系统管理员访问，以及个别情景的管理员访问。以下部分描述了作为系统管理员或情景管理员的登录：

- 第 6-7 页的系统管理员访问
- 第 6-8 页的情景管理员访问

系统管理员访问

您可以通过两种方式作为系统管理员访问 ASA：

- 访问 ASA 控制台。

  您可以从控制台访问*系统执行空间*，这意味着，您输入的所有命令仅会影响系统配置或系统的运行 （因为运行时命令）。

- 使用 Telnet、SSH 或 ASDM 访问管理情景。

  如要启用 Telnet、SSH 和 ASDM 访问，请参阅第 35 章，“管理访问”。

作为系统管理员，您可以访问所有情景。

当您从管理员或系统切换到某个情景时，您的用户名会更改为默认的“enable_15”用户名。如果您在该情景中配置了命令授权，您需要为“enable_15”用户配置授权权限，也可以用您已提供足够权限的不同用户名登录。如要使用新用户名登录，请输入 **login** 命令。例如，您可以使用用户名“admin” 登录至管理情景。管理情景没有任何命令授权配置，但是，所有其他情景都包含命

令授权。为方便起见，每个情景配置都包含有拥有最高权限的“admin”用户。当您从管理情景切换到情景 A 时，您的用户名会更改为 enable_15，因此，您必须输入 **login** 命令，作为“admin”再次登录。当您切换到情景 B 时，必须再次输入 **login** 命令，作为“admin”登录。

系统执行空间不支持任何 AAA 命令，但是，您可以在本地数据库中配置其自己的启用密码及用户名，以便提供单独的登录。

情景管理员访问

您可以使用 Telnet、 SSH 或 ASDM 访问情景。如果您登录非管理情景，则只能访问该情景的配置。您可以提供该情景的单独登录。如要启用 Telnet、 SSH 和 ASDM 访问以及配置管理身份验证，请参阅第 35 章，“管理访问”。

资源管理的相关信息

默认情况下，所有安全情景均可无限制地访问 ASA 的资源，除非实施了每个情景的最大限制；唯一的例外是 VPN 资源，默认情况下会禁用该资源。例如，如果您发现，一个或者多个情景使用了过多的资源，并且它们会导致其他情景的连接被拒绝，则您可以配置资源管理来限制每个情景的资源的使用。对于 VPN 资源，您必须配置资源管理以允许所有 VPN 隧道。

- 第 6-8 页的资源类
- 第 6-8 页的资源限制
- 第 6-9 页的默认类
- 第 6-9 页的使用过度订用的资源
- 第 6-10 页的使用无限制的资源

资源类

ASA 通过将情景分配至资源类来管理资源。每个情景使用类设置的资源限制。如要使用某个类的设置，在您定义情景时，请将情景分配至该类。所有未分配至其他类的情景都属于默认类；您不必主动将一个情景分配至默认类。您仅可将一个情景分配至一个资源类。此规则的例外是，在成员类中未定义的限制会从默认类继承；因此，一个情景实际上是默认类和另一个类的成员。

资源限制

您可以将个别资源的限制设置为百分比 （如果存在硬性系统限制）或绝对值。

对于大多数资源，ASA 不会为分配至该类的每个情景预留部分资源，而是会为情景 ASA 设置最大限制。如果您过度订用资源，或者允许某些资源不受限制，则若干情景可能会“耗尽”这些资源，从而可能会影响为其他情景提供的服务。例外的是 VPN 资源类型，您无法过度订用此类资源，因此，分配至每个情景的资源会得到保证。为了适应超过分配的数量的 VPN 会话临时突发，ASA 会支持“突发” VPN 资源类型，其数量等于剩余的未分配 VPN 会话。突发会话*可以*被过度订用，并按照先到先得原则提供给情景。

默认类

所有未分配至其他类的情景都属于默认类；您不必主动将一个情景分配至默认类。

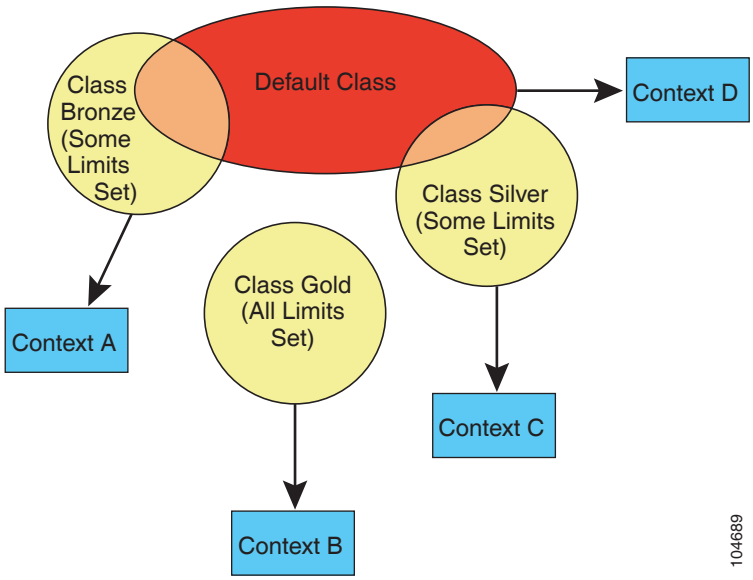
如果某个情景属于默认类之外的其他类，这些类的设置会始终覆盖默认类的设置。但是，如果其他类有任何未定义的设置，则对于这些限制，成员情景会使用默认类的设置。例如，如果您创建一个对所有并发连接有 2% 限制的类，但没有其他限制，则所有其他限制将从默认类继承。相反地，如果您创建一个有着对所有资源的限制的类，则该类不会使用默认类中的任何设置。

对于大多数的资源，默认类会为所有情景提供无限制的资源访问，但以下限制除外：

- Telnet 会话 - 5 个会话 （每个情景的最大值）。
- SSH 会话 - 5 个会话 （每个情景的最大值）。
- IPsec 会话 - 5 个会话 （每个情景的最大值）。
- MAC 地址 - 65,535 个条目。（每个情景的最大值）。
- VPN 站点对站点隧道 - 0 个会话 （您必须手动配置类，以便允许任意 VPN 会话）。

图 6-5 展示了默认类与其他类之间的关系。情景 A 和 C 属于设置了某些限制的类；其他限制会从默认类继承。情景 B 不会从默认类继承任何限制，因为在其类 （Gold 类）中设置了所有限制。情景 D 未分配至某个类，会默认成为默认类的成员。

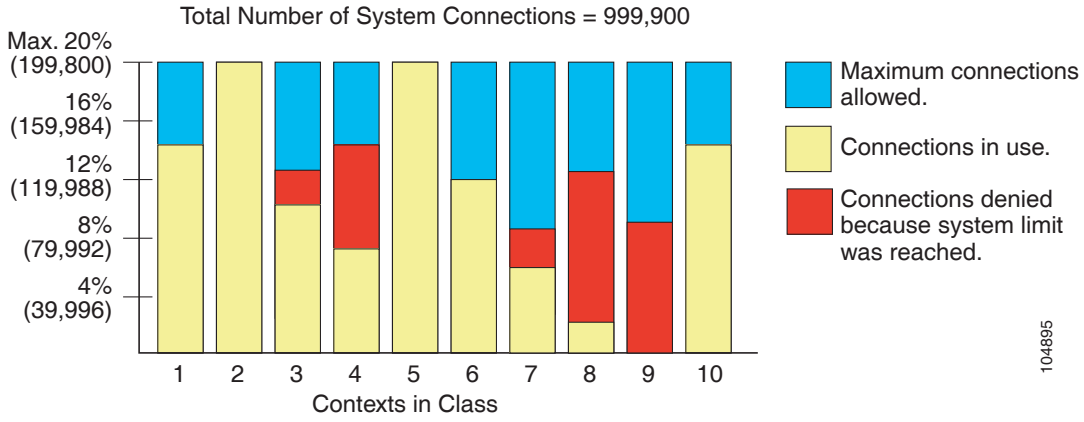
图 6-5　　资源类



使用过度订用的资源

您可以跨所有情景分配超过 100% 的资源 （非突发性 VPN 资源除外），从而过度订用 ASA。例如，您可以设置 Bronze 类，以便将连接限制为每个情景 20%，然后将 10 个情景分配至该类，因而总计为 200%。如果情景并发使用超过系统限制，则每个情景获得的数量少于您想要设置的 20%。（请参阅图 6-6。）

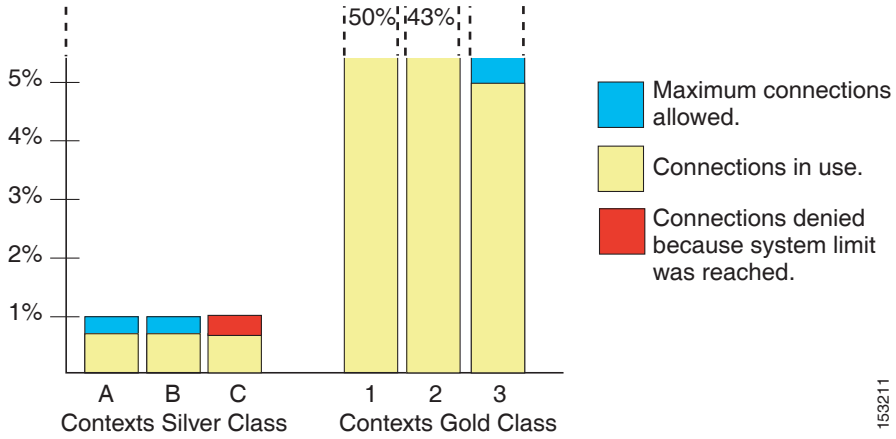
图 6-6　资源过度订用



使用无限制的资源

ASA 允许您分配对一个类中的一种或多种资源的不受限制的访问，而非百分比或绝对数量。当资源不受限制时，情景可以使用系统可提供的所有资源。例如，情景 A、B 和 C 属于 Silver 类，该类限制每个类成员可使用 1% 的连接，总计 3%；但三个情景当前仅在使用共计 2% 的连接。Gold 类不限制对连接的访问。Gold 类中的情景可使用超过 97% 的“未分配”连接。它们还可以使用情景 A、B 和 C 当前未使用的 1% 的连接，即使这意味着，情景 A、B 和 C 无法到达其 3% 的整合限制。（请参阅图 6-7）。设置不受限制的访问与过度订用 ASA 类似，不同之处是，对于过度订用系统的程度，您拥有的控制能力相对较弱。

图 6-7　不受限制的资源



有关 MAC 地址的信息

为了允许情景共享接口，ASA 会默认为每个共享情景接口分配虚拟 MAC 地址。如要自定义或禁用自动生成，请参阅第 6-22 页的自动为情景接口分配 MAC 地址。

MAC 地址用于在情景中对数据包进行分类。如果您共享某个接口，但在每个情景中没有用于该接口的唯一 MAC 地址，则会尝试可能不提供完全覆盖的其他分类方法。有关对数据包进行分类的信息，请参阅第 6-2 页的 ASA 如何对数据包分类。

在生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突的罕见情况下，您可以在情景中为接口手动设置 MAC 地址。如要手动设置 MAC 地址，请参阅第 11-7 页的配置 MAC 地址、MTU 和 TCP MSS。

- 第 6-11 页的默认 MAC 地址
- 第 6-11 页的用手动 MAC 地址交互
- 第 6-11 页的故障转移 MAC 地址
- 第 6-11 页的 MAC 地址格式

默认 MAC 地址

自动 MAC 地址生成会默认启用。ASA 会根据接口 (ASA 5500-X) 或背板 (ASASM) 的 MAC 地址的最后两个字节自动生成前缀。如果需要，您也可以自定义该前缀。

如果您禁用 MAC 地址生成，请参阅以下默认 MAC 地址：

- 对于 ASA 5500-X 系列设备 - 物理接口使用固化 MAC 地址，该物理接口的所有子接口使用相同的固化 MAC 地址。
- 对于 ASASM - 所有 VLAN 接口使用背板 MAC 地址派生的相同 MAC 地址。

另请参阅第 6-11 页的 MAC 地址格式。

注　（8.5(1.6) 和更早版本）为了保持故障转移对的无中断升级功能，ASA 在重新加载时，不会转换现有旧版自动生成配置（如果已启用故障转移）。但是，使用故障转移时，我们强烈建议您手动更改为生成的前缀方法，对于 ASASM 尤其如此。如果不使用前缀方法，安装在不同插槽编号中的 ASASM 在故障转移时会发生 MAC 地址更改，并且会出现流量中断。升级后，如要使用 MAC 地址生成的前缀方法，请重新启用 MAC 地址自动生成来使用前缀。有关旧版方法的详细信息，请参阅《命令参考》中的 **mac-address auto** 命令。

用手动 MAC 地址交互

如果您手动分配 MAC 地址并启用自动生成，则会使用手动分配的 MAC 地址。如果您以后删除手动 MAC 地址，则会使用自动生成的地址。

由于自动生成的地址（使用前缀时）从 A2 开始，如果您也想要使用自动生成，则不能使用从 A2 开始的手动 MAC 地址。

故障转移 MAC 地址

为了用于故障切换，ASA 会为每个接口同时生成主用和备用 MAC 地址。如果主用设备进行故障转移，并且备用设备成为主用设备，新的主用设备将开始使用主用 MAC 地址以最大限度地减少网络中断。有关详细信息，请参阅 第 6-11 页的 MAC 地址格式部分。

MAC 地址格式

ASA 会使用以下格式生成 MAC 地址：

A2*xx.yyzz.zzzz*

其中 *xx.yy* 是用户定义的前缀或根据接口 (ASA 5500-X) 或背板 (ASASM) MAC 地址的最后两个字节自动生成的前缀，而 *zz.zzzz* 是由 ASA 生成的内部计数器。对于备用 MAC 地址，地址是相同的，但内部计数器会加 1。

如何使用前缀的示例如下：如果您将前缀设置为 77，则 ASA 会将 77 转换为十六进制值 004D (*yyxx*)。在 MAC 地址中使用时，该前缀会反转 (*xxyy*) 以便与 ASA 的本机形式匹配：

A2**4D.00***zz.zzzz*

对于前缀 1009 (03F1)，MAC 地址为：

A2**F1.03***zz.zzzz*

注　没有前缀的 MAC 地址格式是旧版本，在较新的 ASA 版本上不受支持。有关旧版格式的详细信息，请参阅 《命令参考》中的 **mac-address auto** 命令。

多情景模式的许可要求

型号	许可证要求
ASA 5512-X	• 基础许可证：不支持。 • 增强型安全许可证：2 个情景。 *可选许可证：5 个情景。*
ASA 5515-X	基础许可证：2 个情景。 *可选许可证：5 个情景。*
ASA 5525-X	基础许可证：2 个情景。 *可选许可证：5、10 或 20 个情景。*
ASA 5545-X	基础许可证：2 个情景。 *可选许可证：5、10、20 或 50 个情景。*
ASA 5555-X	基础许可证：2 个情景。 *可选许可证：5、10、20、50 或 100 个情景。*
带 SSP-10 的 ASA 5585-X	基础许可证：2 个情景。 *可选许可证：5、10、20、50 或 100 个情景。*
带 SSP-20、-40 和 -60 的 ASA 5585-X	基础许可证：2 个情景。 *可选许可证：5、10、20、50、100 或 250 个情景。*
ASASM	基础许可证：2 个情景。 *可选许可证：5、10、20、50、100 或 250 个情景。*
ASAv	不支持。

先决条件

在您处于多情景模式后，请连接到系统或管理情景，以便访问系统配置。您不能在非管理情景中配置系统。默认情况下，在启用多情景模式之后，您可以使用默认管理 IP 地址连接到管理情景。有关连接到 ASA 的详细信息，请参阅第 2 章，“入门”。

准则和限制

本节包括此功能的准则和限制。

防火墙模式准则

在路由和透明防火墙模式中受支持；可以设置每个情景的防火墙模式。

故障转移准则

主用/主用模式故障转移仅在多情景模式中受支持。

IPv6 准则

支持 IPv6。

注　跨情景 IPv6 路由不受支持。

不受支持的功能

多情景模式不支持以下功能：

- RIP
- OSPFv3（OSPFv2 受支持）。
- 组播路由
- 威胁检测
- 统一通信
- QoS
- 远程访问 VPN（站点对站点 VPN 受支持）。

其他指导原则

- 情景模式 （单情景或多情景）不会存储在配置文件中，即使该模式经过重新启动也是如此。如果您需要将配置复制到另一台设备，请将新设备设置为匹配的模式。
- 如果在闪存根目录中存储情景配置，在某些产品型号上您可能会用尽该目录中的空间，即使当前仍有可用内存也是如此。在这种情况下，请为您的配置文件创建子目录。背景：某些型号 （如 ASA 5585-X）的内部闪存使用 FAT16 文件系统，并且，如果您未使用 8.3 兼容的短名称，或使用大写字符，则只能存储数量少于 512 个的文件和文件夹，因为文件系统存储长文件名会用尽空间 （请参阅 http://support.microsoft.com/kb/120138/en-us）。

默认设置

- 默认情况下，ASA 处于单情景模式中。
- 请参阅第 6-9 页的默认类。
- 请参阅第 6-11 页的默认 MAC 地址。

配置多情景

本节介绍如何配置多情景模式。

- 第 6-14 页的配置多情景模式的任务流程
- 第 6-14 页的启用或禁用多情景模式
- 第 6-16 页的配置用于资源管理的类
- 第 6-18 页的配置安全情景
- 第 6-22 页的自动为情景接口分配 MAC 地址

配置多情景模式的任务流程

如要配置多情景模式，请执行以下步骤：

步骤 1　启用多情景模式。请参阅第 6-14 页的启用或禁用多情景模式。

步骤 2　（可选）配置用于资源管理的类。请参阅第 6-16 页的配置用于资源管理的类。**注意**：对于 VPN 支持，您必须在资源类中配置 VPN 资源；默认类不允许使用 VPN。

步骤 3　在系统执行空间中配置接口。

- ASA 5500-X - 第 9 章，“基本接口配置（ASA 5512-X 及更高版本）”
- ASASM-第 3 章，“适用于思科 ASA 服务模块的交换机配置”

步骤 4　配置安全情景。请参阅第 6-18 页的配置安全情景。

步骤 5　（可选）自定义 MAC 地址分配。请参阅第 6-22 页的自动为情景接口分配 MAC 地址。

步骤 6　完成情景中的接口配置。请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。

启用或禁用多情景模式

取决于您从思科订购多情景模式的方式，ASA 可能已为多安全情景进行过配置。如果您需要从单模式转换为多模式，请执行本节中的操作步骤。

- 第 6-15 页的启用多情景模式
- 第 6-15 页的还原单情景模式

启用多情景模式

当您从单模式转换为多模式时，ASA 会将运行配置转换到两个文件中：包括系统配置的新启动配置和包括管理情景的 admin.cfg（位于内部闪存的根目录中）。原始运行配置保存为 old_running.cfg（位于内部闪存的根目录中）。系统将不保存原始启动配置。ASA 自动在系统配置中添加一个管理情景的条目，名称为“admin”。

先决条件

备份您的启动配置。当您从单模式转换到多模式时，ASA 会将运行配置转换到两个文件中。系统将不保存原始启动配置。请参阅 第 36-23 页的备份和还原 配置或其他文件。

详细步骤

命令	用途
mode multiple **示例：** `ciscoasa(config)# mode multiple`	更改为多情景模式。系统将提示您重新启动 ASA。

还原单情景模式

如要将旧运行配置复制到启动配置，并将模式切换到单情景模式，请执行以下操作步骤：

先决条件

在系统执行空间中执行此操作步骤。

详细步骤

	命令	用途
步骤 1	**copy disk0:old_running.cfg startup-config** **示例：** `ciscoasa(config)# copy disk0:old_running.cfg startup-config`	将您的原始运行配置的备份版本复制至当前启动配置。
步骤 2	**mode single** **示例：** `ciscoasa(config)# mode single`	将模式设置为单模式。系统将提示您重新启动 ASA。

配置用于资源管理的类

如要在系统配置中配置一个类，请执行以下操作步骤：您可以通过重新输入带新值的命令，更改特定资源限制的值。

先决条件

在系统执行空间中执行此操作步骤。

准则

表 6-1 列出了资源类型和限制。另请参阅 **show resource types** 命令。

表 6-1　资源名称和限制

资源名称	速率或并发	每个情景的最小和最大数量	系统限制[1]	说明
asdm	并发	最少 1 个 最多 5 个	32	ASDM 管理会话。 **注** ASDM 会话使用两个 HTTPS 连接：一个用于监控（始终存在），另一个用于进行配置更改（仅当您进行更改时才存在）。例如，系统的 32 个 ASDM 会话限制代表 64 个 HTTPS 会话限制。
conns[2]	并发或速率	不适用	并发连接：有关您的型号的可用连接限制，请参阅第 4-1 页的每个型号的受支持功能许可证。 速率：不适用	任意两台主机之间的 TCP 或 UDP 连接，包括一台主机和多台其他主机之间的连接。
hosts	并发	不适用	不适用	可以通过 ASA 连接的主机。
inspects	速率	不适用	不适用	每秒应用检查数。
mac-addresses	并发	不适用	65,535	对于透明防火墙模式，表示 MAC 地址表中允许的 MAC 地址数量。
routes	并发	不适用	不适用	动态路由。
vpn burst other	并发	不适用	您的型号的其他 VPN 会话数量减去分配至 **vpn other** 的所有情景的会话数总和。	允许的站点对站点 VPN 会话超出分配至具有**vpn other** 的情景的会话的数量。例如，如果您的产品型号支持 5000 个会话，您为具有**vpn other** 的所有情景分配了 4000 个会话，其余 1000 个会话可用于 **vpn burst other**。与vpn other（确保情景可使用分配的会话）不同的是，**站点对站点 VPN 突发** vpn burst other可以过度订用；突发池按照先到先得的原则供所有情景使用。
vpn other	并发	不适用	有关对您的产品型号可用的其他 VPN 会话，请参阅第 4-1 页的每个型号的受支持功能许可证。	站点对站点 VPN 会话。您无法过度订用此资源；分配至所有情景的总和不得超出产品型号限制。您分配的此资源会话数保证可供相应情景使用。

表 6-1　资源名称和限制（续）

资源名称	速率或并发	每个情景的最小和最大数量	系统限制[1]	说明
ssh	并发	最少 1 个 最多 5 个	100	SSH 会话。
syslogs	速率	不适用	不适用	每秒系统日志消息数。
telnet	并发	最少 1 个 最多 5 个	100	Telnet 会话。
xlates[2]	并发	不适用	不适用	网络地址转换。

1. 如果此列的值为不适用，则您无法设置该资源的百分比，因为该资源不存在硬性系统限制。
2. 将生成有关限制（xlates 或 conns 中的较低者）的系统日志消息。例如，如果您将 xlates 限制为 7，将 conns 限制为 9，则 ASA 仅会生成日志消息 321001（“Resource 'xlates' limit of 7 reached for context 'ctx1'”），而不会生成 321002（“Resource 'conn rate' limit of 5 reached for context 'ctx1'”）。

详细步骤

	命令	用途
步骤 1	**class** *name* **示例：** `ciscoasa(config)# class gold`	指定类名称，并输入类配置模式。*name* 是最大长度为 20 个字符的字符串。如要设置默认类的限制，请输入 **default** 作为名称。
步骤 2	**limit-resource** [**rate**] *resource_name number*[**%**] **示例：** `ciscoasa(config-class)# limit-resource rate inspects 10`	设置资源类型的资源限制。要获得资源类型列表，请参阅表 6-1。如果您指定 **all**，则会将所有资源配置为相同的值。如果您还指定了特定资源的值，该限制将覆盖为 **all** 设置的限制。 输入 **rate** 参数设置特定资源的每秒速率。 对于大多数资源，请将 *number* 指定为 **0**，将资源设置为不受限制或使用系统限制（如有）。对于 VPN 资源，**0** 会将限制设置为无。 对于没有系统限制的资源，您不能设置百分比 (**%**)；您只能设置绝对值。

示例

例如，如要将默认类对连接数的限制设置为 10% 而非不受限制，并允许使用 5 个站点对站点 VPN 隧道（其中两个隧道预留给 VPN 突发），请输入以下命令：

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 5
ciscoasa(config-class)# limit-resource vpn burst other 2
```

所有其他资源保持不受限制。

如要添加名为 gold 的类，请输入以下命令：

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
```

```
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 5000
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5
```

配置安全情景

系统配置中的安全情景定义确定情景名称、配置文件 URL、情景可使用的接口以及其他设置。

先决条件

- 在系统执行空间中执行此操作步骤。
- 对于 ASASM，根据第 3 章，“适用于思科 ASA 服务模块的交换机配置”将 VLAN 分配至交换机上的 ASASM。
- 对于 ASA 5500-X，请根据第 9 章，“基本接口配置 （ASA 5512-X 及更高版本）”配置物理接口参数、 VLAN 子接口、 EtherChannel 和冗余接口。
- 如果您没有管理情景 （例如，如果您清除配置），则必须先通过输入以下命令指定管理情景名称：

  ```
  ciscoasa(config)# admin-context name
  ```

  虽然此情景在您的配置中尚不存在，但您可随后输入 **context** *name* 命令，继续进行管理情景配置。

详细步骤

	命令	用途
步骤 1	**context** *name* **示例：** `ciscoasa(config)# context administrator`	添加或修改情景。*name* 是最大长度为 32 个字符的字符串。该名称区分大小写，因此，您可以有名为“customerA”和“CustomerA”的两个情景。您可以使用字母、数字或连字符，但是，名称不能以连字符开始或结束。 “System”或“Null”（大写或小写字母）是保留名称，不能使用。
步骤 2	（可选） **description** *text* **示例：** `ciscoasa(config-ctx)# description Administrator Context`	为此情景添加说明。

命令	用途
步骤 3 如要分配接口，请执行以下操作： **allocate-interface** *interface_id* [*mapped_name*] [**visible** | **invisible**] 如要分配一个或多个子接口，请执行以下操作： **allocate-interface** *interface_id*.*subinterface*[-*interface_id*.*subinterface*] [*mapped_name*[-*mapped_name*]] [**visible** | **invisible**] **示例：** ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1 ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2 ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305 int3-int8	指定您可在情景中使用的接口。接口类型和端口号之间不得包含空格。 可以多次输入这些命令，以便指定不同的范围。如果使用此命令的 **no** 形式移除分配，则会从运行配置中移除包含该接口的所有情景命令。 透明防火墙模式允许有限数量的接口传输流量；然而，您可以将专用管理接口、管理*插槽/端口*（物理、子接口、冗余或 EtherChannel）用作管理流量的额外接口。单独的管理接口对于 ASASM 不可用。 需要时，您可以将相同接口分配至路由模式中的多个情景。透明模式不允许共享接口。 *mapped_name* 是接口的字母数字别名，可在情景中用于代替接口 ID。如果您未指定映射名称，则会在情景中使用接口 ID。出于安全性考虑，您可能不希望情景管理员知道情景正使用哪些接口。映射名称必须以字母开头，以字母或数字结尾，并且仅可包含字母、数字或下划线内部字符。例如，您可以使用以下名称： **int0**、**inta** 或 **int_0** 如果指定子接口范围，您可以指定匹配的映射名称范围。请遵循适用于范围的以下准则： • 映射名称必须包含一个字母部分 （在前）和一个数字部分（在后）。对于范围的两端，映射名称的字母部分必须匹配。例如，可以输入以下范围： **int0-int10** 例如，如果您输入 gig0/1.1-gig0/1.5 **happy**1-**sad**5，则命令将会失败。 • 映射名称的数字部分必须包含与子接口范围相同数量的数值。例如，两个范围都包含 100 个接口。 **gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100** 例如，如果您输入 gig0/0.**100**-gig0/0.**199** int**1**-int**15**，命令将会失败。 如果您设置了映射名称，指定 **visible** 可在 **show interface** 命令中查看真实接口 ID。默认的 **invisible** 关键字仅显示映射名称。

命令	用途
步骤 3 如要分配接口，请执行以下操作： **allocate-interface** *interface_id* [*mapped_name*] [**visible** | **invisible**] 如要分配一个或多个子接口，请执行以下操作： **allocate-interface** *interface_id.subinterface*[**-***interface_id.subinterface*] [*mapped_name*[**-***mapped_name*]] [**visible** | **invisible**] **示例：** `ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1` `ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2` `ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet 0/2.305 int3-int8`	指定您可在情景中使用的接口。接口类型和端口号之间不得包含空格。 可以多次输入这些命令，以便指定不同的范围。如果使用此命令的 **no** 形式移除分配，则会从运行配置中移除包含该接口的所有情景命令。 透明防火墙模式允许有限数量的接口传输流量；然而，您可以将专用管理接口、管理*插槽/端口*（物理、子接口、冗余或 EtherChannel）用作管理流量的额外接口。单独的管理接口对于 ASASM 不可用。 需要时，您可以将相同接口分配至路由模式中的多个情景。透明模式不允许共享接口。 *mapped_name* 是接口的字母数字别名，可在情景中用于代替接口 ID。如果您未指定映射名称，则会在情景中使用接口 ID。出于安全性考虑，您可能不希望情景管理员知道情景正使用哪些接口。映射名称必须以字母开头，以字母或数字结尾，并且仅可包含字母、数字或下划线内部字符。例如，您可以使用以下名称： **int0**、**inta** 或 **int_0** 如果指定子接口范围，您可以指定匹配的映射名称范围。请遵循适用于范围的以下准则： • 映射名称必须包含一个字母部分 （在前）和一个数字部分（在后）。对于范围的两端，映射名称的字母部分必须匹配。例如，可以输入以下范围： **int0-int10** 例如，如果您输入 `gig0/1.1-gig0/1.5` **happy**`1-`**sad**`5`，则命令将会失败。 • 映射名称的数字部分必须包含与子接口范围相同数量的数值。例如，两个范围都包含 100 个接口。 **gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100** 例如，如果您输入 `gig0/0.`**100**`-gig0/0.`**199** `int`**1**`-int`**15**，命令将会失败。 如果您设置了映射名称，指定 **visible** 可在 **show interface** 命令中查看真实接口 ID。默认的 **invisible** 关键字仅显示映射名称。

	命令	用途
步骤 4	**config-url** *url* **示例：** `ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg`	确定系统从中下载情景配置的 URL。当您添加情景 URL 时，系统会立即加载情景，因此，如果配置可用，情景将会运行。 **注**　在您输入 **config-url** 命令前，请输入 **allocate-interface** 命令。如果您先输入 **config-url** 命令，ASA 将立即加载情景配置。如果情景包含引用（尚未配置的）接口的任何命令，这些命令将会失败。 文件名不需要文件扩展名，不过，我们建议使用“.cfg”。服务器必须能够从管理情景访问。如果配置文件不可用，您将会看到以下消息： `WARNING: Could not fetch the URL url` `INFO: Creating context with default config` 对于非 HTTP(S) URL 位置，在您指定 URL 之后，可以切换到该情景，在 CLI 上对其进行配置，然后输入 **write memory** 命令将文件写至该 URL 位置。（HTTP(S) 是只读的）。 **注**　管理情景文件必须存储在内部闪存上。 可用的 URL 类型包括：**磁盘***编号*（对于闪存）、 **ftp**、 **http**、**https** 或 **tftp**。 如要更改 URL，请重新输入带新 URL 的 **config-url** 命令。有关更改 URL 的详细信息，请参阅第 6-24 页的更改安全情景 URL。
步骤 5	（可选） **member** *class_name* **示例：** `ciscoasa(config-ctx)# member gold`	将情景分配至资源类。如果您不指定类，情景将属于默认类。您仅可将一个情景分配至一个资源类。
步骤 6	（可选） **allocate-ips** *sensor_name* [*mapped_name*] [**default**] **示例：** `ciscoasa(config-ctx)# allocate-ips sensor1 highsec`	如果您已安装 IPS 模块，请将 IPS 虚拟传感器分配至此情景。 有关虚拟传感器的详细信息，请参阅《防火墙配置指南》。
步骤 7	（可选） **join-failover-group** {**1** | **2**) **示例：** `ciscoasa(config-ctx)# join-failover-group 2`	将情景分配至主用/主用故障转移中的一个故障转移组。默认情况下，情景处于组 1。管理情景必须始终处于组 1。 有关故障转移组的详细信息，请参阅第 7-32 页的配置可选故障转移参数。
步骤 8	（可选） **scansafe** [**license** *key*] **示例：** `ciscoasa(config-ctx)# scansafe`	为此情景启用云网络安全。 如果您未指定**许可证**，此情景将使用在系统配置中配置的许可证。ASA 会将身份验证密钥发送至云网络安全代理服务器，以便指示请求来自哪个组织。身份验证密钥为 16 字节的十六进制数值。 有关 ScanSafe 的详细信息，请参阅《防火墙配置指南》。

示例

以下示例将管理情景设置为“administrator”，在内部闪存中创建一个名为“administrator”的情景，然后从 FTP 服务器添加两个情景：

```
ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold


ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

自动为情景接口分配 MAC 地址

本节介绍如何配置 MAC 地址的自动生成。

MAC 地址用于在情景中对数据包进行分类。有关详细信息，请参阅第 6-10 页的有关 MAC 地址的信息，尤其是您从早期 ASA 版本升级时。另请参阅第 6-34 页的查看分配的 MAC 地址。

准则

- 在情景中为接口配置 **nameif** command 时，会立即生成新的 MAC 地址。如果您在配置情景接口后启用此功能，则在您启用之后，会立即为所有接口生成 MAC 地址。如果您禁用此功能，每个接口的 MAC 地址将还原为默认 MAC 地址。例如，GigabitEthernet0/1 子接口还原为使用 GigabitEthernet0/1 的 MAC 地址。
- 在生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突的罕见情况下，您可以在情景中为接口手动设置 MAC 地址。要手动设置 MAC 地址，请参阅第 11-7 页的配置 MAC 地址、MTU 和 TCP MSS。

详细步骤

命令	用途
mac-address auto [**prefix** *prefix*] **示例：** `ciscoasa(config)# mac-address auto prefix 19`	自动为每个情景接口分配专用 MAC 地址。 如果您未输入前缀，则 ASA 将根据接口 (ASA 5500-X) 或背板 (ASASM) MAC 地址的最后两个字节自动生成前缀。 如果您手动输入前缀，则*前缀*是介于 0 和 65535 之间的一个十进制数值。此前缀会被转换为四位数的十六进制数值，并用作 MAC 地址的一部分。有关此前缀使用方式的详细信息，请参阅 第 6-11 页的 MAC 地址格式。

在情景和系统执行空间之间切换

如果您登录到系统执行空间（或管理情景），则可以在情景之间切换，并在每个情景中执行配置和监控任务。您在配置模式中编辑或者用于 **copy** 或 **write** 命令中的运行配置取决于您的位置。当您处于系统执行空间时，运行配置仅包含系统配置；当您处于某个情景时，运行配置仅包含该情景。例如，您无法通过输入 **show running-config** 命令查看所有运行配置（系统加所有情景）。屏幕上仅显示当前配置。

详细步骤

命令	用途
changeto context *name*	切换到某个情景。提示符将会变为以下形式： `ciscoasa/name#`
changeto system	切换到系统执行空间。提示符将会变为以下形式： `ciscoasa#`

管理安全情景

此部分介绍如何管理安全情景。

- 第 6-23 页的移除安全情景
- 第 6-24 页的更改管理情景
- 第 6-24 页的更改安全情景 URL
- 第 6-25 页的重新加载安全情景

移除安全情景

您不能移除当前管理情景，除非您使用 **clear context** 命令移除所有情景。

注　如果使用故障转移，从您在主用设备上移除情景到该情景在备用设备上被移除之间存在一定延迟。您可能会看到错误消息，表明主用设备和备用设备上的接口数量不一致；此错误是临时的，可以忽略。

先决条件

在系统执行空间中执行此操作步骤。

详细步骤

命令	用途
no context *name*	移除单个情景。所有情景命令也将会被移除。情景配置文件不会从配置 URL 位置移除。
clear context	移除所有情景（包括管理情景）。情景配置文件不会从配置 URL 位置移除。

更改管理情景

系统配置本身不包括任何网络接口或网络设置；相反，当系统需要访问网络资源时 （例如，从服务器下载情景），它将使用被指定为管理员情景的情景之一。

管理情景与任何其他情景一样，不同之处在于，当用户登录管理情景时，该用户将具有系统管理员权限，能够访问系统和所有其他情景。管理情景在任何情况下都不受限制，可用作常规情景。但是，登录至管理情景会授予您所有情景的管理员特权，因此您可能需要限制对管理情景的访问，限制为适当用户可以访问。

准则

您可以将任意情景设置为管理情景，只要其配置文件存储在内部闪存中。

先决条件

在系统执行空间中执行此操作步骤。

详细步骤

命令	用途
admin-context *context_name* **示例：** `ciscoasa(config)# admin-context administrator`	设置管理情景。连接到管理情景的所有远程管理会话（如 Telnet、SSH 或 HTTP）都将会终止。您必须重新连接到新的管理情景。 **注**　某些系统配置命令（包括 **ntp server**）会标识属于管理情景的接口名称。如果您更改管理情景，并且新的管理情景中不存在该接口名称，请务必更新引用该接口的所有系统命令。

更改安全情景 URL

本节介绍如何更改情景 URL。

准则

- 在没有通过新的 URL 重新加载配置的情况下，您不能更改安全情景 URL。 ASA 会将新配置与当前运行配置合并。
- 重新输入相同 URL 也会将保存的配置与运行配置合并。
- 合并会将新配置中的所有新命令添加至运行配置。
  - 如果配置相同，则不会发生更改。
  - 如果命令有冲突，或者如果命令影响情景运行，则合并的效果取决于命令。可能出现错误，或者出现意外结果。如果运行配置为空 （例如，如果服务器不可用并且从未下载过配置），则会使用新配置。
- 如果您不想合并配置，可以清除运行配置 （这会中断通过该情景的所有通信），然后通过新的 URL 重新加载配置。

先决条件

在系统执行空间中执行此操作步骤。

详细步骤

	命令	用途
步骤 1	（可选，如果您不希望执行合并） **changeto context** *name* **clear configure all** **示例：** ciscoasa(config)# changeto context ctx1 ciscoasa/ctx1(config)# clear configure all	切换到情景并清除其配置。如果您想要执行合并，请跳至步骤 2。
步骤 2	**changeto system** **示例：** ciscoasa/ctx1(config)# changeto system ciscoasa(config)#	切换到系统执行空间。
步骤 3	**context** *name* **示例：** ciscoasa(config)# context ctx1	进入您想要更改的情景的情景配置模式。
步骤 4	**config-url** *new_url* **示例：** ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg	输入新的 URL。系统会立即加载情景，因此情景将会运行。

重新加载安全情景

您可以通过两种方式重新加载情景：

- 清除运行配置，然后导入启动配置。

  此操作会清除与情景关联的大多数属性，例如，连接和 NAT 表。

- 从系统配置中移除情景。

  此操作会清除其他属性，例如，可能对故障排除很有用的内存分配。但是，将情景添加回系统要求您重新指定 URL 和接口。

- 第 6-26 页的通过清除配置来重新加载
- 第 6-26 页的通过删除情景然后重新添加来重新加载

通过清除配置来重新加载

如要通过清除情景配置并通过 URL 重新加载配置来重新加载情景，请执行以下操作步骤。

详细步骤

	命令	用途
步骤 1	**changeto context** *name* **示例：** `ciscoasa(config)# changeto context ctx1` `ciscoasa/ctx1(comfig)#`	切换到要重新加载的情景。
步骤 2	**clear configure all** **示例：** `ciscoasa/ctx1(config)# clear configure all`	清除运行配置。此命令会清除所有连接。
步骤 3	**copy startup-config running-config** **示例：** `ciscoasa/ctx1(config)# copy startup-config running-config`	重新加载配置。ASA 会通过系统配置中指定的 URL 复制配置。您不能在情景中更改此 URL。

通过删除情景然后重新添加来重新加载

如要通过删除情景，然后重新添加来重新加载该情景，请执行以下部分中的操作步骤：

1. 第 6-23 页的移除安全情景
2. 第 6-18 页的配置安全情景

监控安全情景

本节介绍如何查看和监控情景信息。

- 第 6-27 页的查看情景信息
- 第 6-28 页的查看资源分配
- 第 6-31 页的查看资源使用情况
- 第 6-32 页的监控情景中的 SYN 攻击
- 第 6-34 页的查看分配的 MAC 地址

查看情景信息

从系统执行空间中，您可以查看包括名称、分配的接口和配置文件 URL 的情景列表。

从系统执行空间中，输入以下命令，以便查看所有情景：

命令	用途
show context [*name* | **detail**| **count**]	显示所有情景。 如果您想要显示特定情景的信息，请指定 *name*。 **detail** 选项用于显示其他信息。有关详细信息，请参阅以下示例输出。 **count** 选项用于显示情景的总数。

以下是 **show context** 命令的示例输出。以下示例输出显示三个情景：

```
ciscoasa# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      disk0:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      disk0:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      disk0:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

表 6-2 显示了每个字段的说明。

表 6-2　　show context Fields

字段	说明
Context Name	列出所有情景名称。带有星号 (*) 的情景名称是管理情景。
Interfaces	分配至情景的接口。
URL	ASA 从中加载情景配置的 URL。

以下内容为 **show context detail** 命令的示例输出：

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
Mapped Interfaces: Control0/0, GigabitEthernet0/0,
```

```
    GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
    GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
    GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
Real Interfaces:
Mapped Interfaces:
Flags: 0x00000009, ID: 258
```

有关 **detail** 输出的详细信息，请参阅 《命令参考》。

以下内容为 **show context count** 命令的示例输出：

```
ciscoasa# show context count
Total active contexts: 2
```

查看资源分配

从系统执行空间中，您可以查看每种资源跨所有类和类成员的分配情况。

如要查看资源分配，请输入以下命令：

命令	用途
show resource allocation [**detail**]	显示资源分配。此命令显示资源分配，但不显示实际使用的资源。有关实际资源使用情况的详细信息，请参阅第 6-31 页的查看资源使用情况。 **detail** 参数用于显示其他信息。有关详细信息，请参阅以下示例输出。

以下示例输出以绝对值和可用系统资源百分比的形式，显示每个资源的总分配情况：

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Routes                      5000           N/A
 Telnet                        35           35.00%
 Xlates                     91749           N/A
 Other VPN Sessions            20           2.66%
 Other VPN Burst               20           2.66%
 All                    unlimited
```

表 6-3 显示了每个字段的说明。

表 6-3　　show resource allocation 的字段

字段	说明
Resource	您可以限制的资源的名称。

表 6-3　show resource allocation 的字段

字段	说明
Total	跨所有情景分配的资源的总量。此数量是并发实例数或每秒实例数的绝对数值。如果您在类定义中指定的是百分比，ASA 会将百分比转换为此处显示的绝对数值。
% of Avail	跨所有情景分配的总系统资源的百分比（如果资源有硬性系统限制）。如果资源没有系统限制，此列将显示 N/A。

以下内容为 **show resource allocation detail** 命令的示例输出：

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource          Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]      default          all      CA  unlimited
                  gold               1       C      34000      34000     N/A
                  silver             1      CA      17000      17000     N/A
                  bronze             0      CA       8500
                  All Contexts:      3                         51000     N/A

Inspects [rate]   default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      10000      10000     N/A
                  bronze             0      CA       5000
                  All Contexts:      3                         10000     N/A

Syslogs [rate]    default          all      CA  unlimited
                  gold               1       C       6000       6000     N/A
                  silver             1      CA       3000       3000     N/A
                  bronze             0      CA       1500
                  All Contexts:      3                          9000     N/A

Conns             default          all      CA  unlimited
                  gold               1       C     200000     200000     20.00%
                  silver             1      CA     100000     100000     10.00%
                  bronze             0      CA      50000
                  All Contexts:      3                        300000     30.00%

Hosts             default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      26214      26214      N/A
                  bronze             0      CA      13107
                  All Contexts:      3                         26214      N/A

SSH               default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
                  bronze             0      CA          5
                  All Contexts:      3                            20     20.00%

Telnet            default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
                  bronze             0      CA          5
                  All Contexts:      3                            20     20.00%

Routes            default          all       C  unlimited                N/A
                  gold               1       D  unlimited          5      N/A
```

```
                  silver              1      CA          10          10       N/A
                  bronze              0      CA           5                   N/A
                  All Contexts:       3                                20       N/A

Xlates            default           all      CA   unlimited
                  gold                1      DA   unlimited
                  silver              1      CA       23040       23040      N/A
                  bronze              0      CA       11520
                  All Contexts:       3                           23040      N/A

mac-addresses     default           all       C       65535
                  gold                1       D       65535       65535   100.00%
                  silver              1      CA        6553        6553     9.99%
                  bronze              0      CA        3276
                  All Contexts:       3                          137623   209.99%
```

表 6-4 显示了每个字段的说明。

表 6-4　show resource allocation detail 的字段

字段	说明
Resource	您可以限制的资源的名称。
Class	各个类的名称，包括默认类。 All Contexts 字段显示跨所有类的总值。
Mmbrs	分配至各个类的情景的数量。
Origin	资源限制的来源，如下所示： • A - 您使用 **all** 选项设置此限制，而不是针对单一资源设置限制。 • C - 此限制从成员类派生。 • D - 此限制在成员类中未定义，但是会从默认类派生。对于分配至默认类的情景，此值将为“C”而不是“D”。 ASA 可以将“A”与“C”或“D”合并。
Limit	每个情景的资源限制，绝对数值形式。如果您在类定义中指定的是百分比，ASA 会将百分比转换为此处显示的绝对数值。
Total	跨类中的所有情景分配的资源的总量。此数量是并发实例数或每秒实例数的绝对数值。如果资源不受限制，此字段的显示为空白。
% of Avail	跨类中的所有情景分配的总系统资源的百分比。如果资源不受限制，此字段的显示为空白。如果资源没有系统限制，则此列会显示 N/A。

查看资源使用情况

从系统执行空间中，您可以查看每个情景的资源使用情况，并显示系统资源使用情况。

命令	用途
show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**] [**resource** {*resource_name* | **all**} | **detail**] [**counter** *counter_name* [*count_threshold*]]	默认情况下，系统会显示**所有**情景的使用情况；每个情景会单独列出。 输入 **top** *n* 关键字，以便显示为指定资源前 *n* 大使用者的情景。使用此选项，您必须指定单个资源类型，而不是 **resource all**。 **summary** 选项用于显示所有情景的整合使用情况。 **system** 选项用于显示所有情景的整合使用情况，但显示的是资源的系统限制，而不是整合的情景限制。 有关 **resource** *resource_name*，请参阅表 6-1 中的可用资源名称。另请参阅 **show resource type** 命令。指定 **all**（默认值）表示所有类型。 **detail** 选项用于显示所有资源的资源使用情况，包括您无法管理的那些资源。例如，您可以查看 TCP 拦截的数量。 **counter** *counter_name* 为以下任一关键字： • **current** - 显示资源的活动并发实例数或当前速率。 • **denied** - 显示由于实例数超出 Limit 列中显示的资源限制而被拒绝的实例数。 • **peak** - 显示从上次清除统计信息（使用 **clear resource usage** 命令或因为设备重启）以来，资源的峰值并发实例数或峰值速率。 • **all** -（默认值）显示所有统计信息。 *count_threshold* 设置一个数值，如果超出此数值，将显示资源。默认值为 1。如果资源使用量低于您设置的数值，则不会显示该资源。如果您将计数器名称指定为 **all**，则 *count_threshold* 会应用至当前使用情况。 **注**　要显示所有资源，请将 *count_threshold* 设置为 **0**。

以下内容为 **show resource usage context** 命令的示例输出，其中显示了管理情景的资源使用情况：

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

以下内容为 **show resource usage summary** 命令的示例输出，其中显示了所有情景和所有资源的资源使用情况：此示例显示了六个情景的限制。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132        N/A          0 Summary
Conns                     584          763     280000(S)       0 Summary
Xlates                   8526         8966        N/A          0 Summary
Hosts                     254          254        N/A          0 Summary
Conns [rate]              270          535        N/A       1704 Summary
Inspects [rate]           270          535        N/A          0 Summary
Other VPN Sessions          0           10         10        740 Summary
Other VPN Burst             0           10         10        730 Summary
```

```
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

以下是 **show resource usage summary** 命令的示例输出，其中显示了 25 个情景的限制：由于 Telnet 和 SSH 连接的情景限制是每个情景 5 个连接，因此整合限制为 125 个连接。系统限制仅为 100 个链接，因此，系统限制会显示。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit    Denied   Context
Telnet                      1            1        100[S]      0   Summary
SSH                         2            2        100[S]      0   Summary
Conns                      56           90        130000(S)   0   Summary
Hosts                      89          102        N/A         0   Summary
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

以下内容是 **show resource usage system** 命令的示例输出，其中显示了所有情景的资源使用情况，但是该命令显示的是系统限制，而不是整合的情景限制。 **counter all 0** 选项用于显示当前未使用的资源。 Denied statistics 显示由于系统限制 （如有），资源使用被拒的次数。

```
ciscoasa# show resource usage system counter all 0

Resource              Current         Peak      Limit        Denied    Context
Telnet                      0            0        100               0    System
SSH                         0            0        100               0    System
ASDM                        0            0         32               0    System
Routes                      0            0        N/A               0    System
IPSec                       0            0          5               0    System
Syslogs [rate]              1           18        N/A               0    System
Conns                       0            1     280000               0    System
Xlates                      0            0        N/A               0    System
Hosts                       0            2        N/A               0    System
Conns [rate]                1            1        N/A               0    System
Inspects [rate]             0            0        N/A               0    System
Other VPN Sessions          0           10        750             740    System
Other VPN Burst             0           10        750             730    System
```

监控情景中的 SYN 攻击

ASA 使用 TCP 拦截防止 SYN 攻击。TCP 拦截使用 SYN C ookie 算法防止 TCP SYN 泛洪攻击。SYN 泛洪攻击通常包括来自欺骗性 IP 地址的大量 SYN 数据包。持续的 SYN 数据包泛洪攻击会使服务器 SYN 队列总是处于已满状态，这会使其无法为连接请求提供服务。超过初期连接阈值时，ASA 将会充当服务器代理，并生成对客户端 SYN 请求的 SYN-ACK 响应。当 ASA 收到客户端发回的 ACK 响应时，它可以对客户端进行身份验证，并允许与服务器的连接。

请使用以下命令监控 SYN 攻击：

命令	用途
show perfmon	监控各个情景的攻击速率。
show resource usage detail	监控对于各个情景，TCP 拦截使用的资源的数量。
show resource usage summary detail	监控对于整个系统，TCP 拦截使用的资源的数量。

以下内容是 **show perfmon** 命令的示例输出，其中显示了称为 admin 的情景的 TCP 拦截的速率。

```
ciscoasa/admin# show perfmon

Context:admin
PERFMON STATS:   Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept    322779/s      322779/s
```

以下内容是 **show resource usage detail** 命令的示例输出，其中显示了对于各个情景，TCP 使用的资源的数量。（采用**粗体**的示例文本显示了 TCP 拦截信息）。

```
ciscoasa(config)# show resource usage detail
Resource              Current         Peak      Limit         Denied Context
memory                 843732       847288  unlimited             0 admin
chunk:channels             14           15  unlimited             0 admin
chunk:fixup                15           15  unlimited             0 admin
chunk:hole                  1            1  unlimited             0 admin
chunk:ip-users             10           10  unlimited             0 admin
chunk:list-elem            21           21  unlimited             0 admin
chunk:list-hdr              3            4  unlimited             0 admin
chunk:route                 2            2  unlimited             0 admin
chunk:static                1            1  unlimited             0 admin
tcp-intercepts         328787       803610  unlimited             0 admin
np-statics                  3            3  unlimited             0 admin
statics                     1            1  unlimited             0 admin
ace-rules                   1            1  unlimited             0 admin
console-access-rul          2            2  unlimited             0 admin
fixup-rules                14           15  unlimited             0 admin
memory                 959872       960000  unlimited             0 c1
chunk:channels             15           16  unlimited             0 c1
chunk:dbgtrace              1            1  unlimited             0 c1
chunk:fixup                15           15  unlimited             0 c1
chunk:global                1            1  unlimited             0 c1
chunk:hole                  2            2  unlimited             0 c1
chunk:ip-users             10           10  unlimited             0 c1
chunk:udp-ctrl-blk          1            1  unlimited             0 c1
chunk:list-elem            24           24  unlimited             0 c1
chunk:list-hdr              5            6  unlimited             0 c1
chunk:nat                   1            1  unlimited             0 c1
chunk:route                 2            2  unlimited             0 c1
chunk:static                1            1  unlimited             0 c1
tcp-intercept-rate      16056        16254  unlimited             0 c1
globals                     1            1  unlimited             0 c1
np-statics                  3            3  unlimited             0 c1
statics                     1            1  unlimited             0 c1
nats                        1            1  unlimited             0 c1
ace-rules                   2            2  unlimited             0 c1
console-access-rul          2            2  unlimited             0 c1
fixup-rules                14           15  unlimited             0 c1
memory              232695716    232020648  unlimited             0 system
chunk:channels             17           20  unlimited             0 system
```

```
chunk:dbgtrace              3            3  unlimited            0 system
chunk:fixup                15           15  unlimited            0 system
chunk:ip-users              4            4  unlimited            0 system
chunk:list-elem          1014         1014  unlimited            0 system
chunk:list-hdr              1            1  unlimited            0 system
chunk:route                 1            1  unlimited            0 system
block:16384               510          885  unlimited            0 system
block:2048                 32           34  unlimited            0 system
```

以下示例输出显示了，对于整个系统，TCP 拦截使用的资源的数量。（采用**粗体**的示例文本显示了 TCP 拦截信息）。

```
ciscoasa(config)# show resource usage summary detail
Resource              Current         Peak      Limit         Denied Context
memory              238421312    238434336  unlimited             0 Summary
chunk:channels             46           48  unlimited             0 Summary
chunk:dbgtrace              4            4  unlimited             0 Summary
chunk:fixup                45           45  unlimited             0 Summary
chunk:global                1            1  unlimited             0 Summary
chunk:hole                  3            3  unlimited             0 Summary
chunk:ip-users             24           24  unlimited             0 Summary
chunk:udp-ctrl-blk          1            1  unlimited             0 Summary
chunk:list-elem          1059         1059  unlimited             0 Summary
chunk:list-hdr             10           11  unlimited             0 Summary
chunk:nat                   1            1  unlimited             0 Summary
chunk:route                 5            5  unlimited             0 Summary
chunk:static                2            2  unlimited             0 Summary
block:16384               510          885  unlimited             0 Summary
block:2048                 32           35  unlimited             0 Summary
tcp-intercept-rate     341306       811579  unlimited             0 Summary
globals                     1            1  unlimited             0 Summary
np-statics                  6            6  unlimited             0 Summary
statics                     2            2        N/A             0 Summary
nats                        1            1        N/A             0 Summary
ace-rules                   3            3        N/A             0 Summary
console-access-rul          4            4        N/A             0 Summary
fixup-rules                43           44        N/A             0 Summary
```

查看分配的 MAC 地址

您可以查看系统配置或情景中的自动生成的 MAC 地址。

- 第 6-34 页的查看系统配置中的 MAC 地址
- 第 6-36 页的查看情景中的 MAC 地址

查看系统配置中的 MAC 地址

本节介绍如何查看系统配置中的 MAC 地址。

准则

如果您手动为接口分配 MAC 地址，但也启用了自动生成，自动生成的地址会继续显示在配置中，即使正在使用的是手动 MAC 地址。如果您随后移除手动 MAC 地址，则会使用所显示的自动生成的地址。

详细步骤

命令	用途
show running-config all context [*name*]	可以显示在系统执行空间中分配的 MAC 地址。 查看分配的 MAC 地址需要使用 **all** 选项。虽然 **mac-address auto** 命令仅在全局配置模式中是用户可配置的，该命令在情景配置模式中会与分配的 MAC 地址一起显示为只读条目。仅情景中使用 **nameif** 命令配置的已分配接口，会拥有分配的 MAC 地址。

示例

show running-config all context admin 命令的以下输出，显示了分配至 Management0/0 接口的主 MAC 地址和辅助 MAC 地址。

```
ciscoasa# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

show running-config all context 命令的以下输出，显示了所有情景接口的所有 MAC 地址（主 MAC 地址和辅助 MAC 地址）。请注意，由于未在情景中使用 **nameif** 命令配置 GigabitEthernet0/0 和 GigabitEthernet0/1 主接口，因此没有为它们生成 MAC 地址。

```
ciscoasa# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
```

```
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

查看情景中的 MAC 地址

本节介绍如何查看情景中的 MAC 地址。

详细步骤

命令	用途
show interface | include (Interface)|(MAC)	用于显示情景中的每个接口正在使用的 MAC 地址。

示例

例如：

```
ciscoasa/context# show interface | include (Interface)|(MAC)

Interface GigabitEthernet1/1.1 "g1/1.1", is down, line protocol is down
        MAC address a201.0101.0600, MTU 1500
Interface GigabitEthernet1/1.2 "g1/1.2", is down, line protocol is down
        MAC address a201.0102.0600, MTU 1500
Interface GigabitEthernet1/1.3 "g1/1.3", is down, line protocol is down
        MAC address a201.0103.0600, MTU 1500
...
```

注　**show interface** 命令显示正在使用的 MAC 地址；如果您手动分配 MAC 地址，并且也启用了自动生成，则您只能查看系统配置中未使用的自动生成地址。

多情景模式的配置示例

以下示例：

- 使用自定义前缀自动设置情景中的 MAC 地址。
- 将默认类的连接数限制设置为 10%，而不是不受限制，并将 VPN 其它会话连接数限制设置为 10 个，VPN 突发连接数限制设置为 5 个。
- 创建 gold 资源类。
- 将管理情景设置为“administrator”。
- 在内部闪存上创建一个名为“administrator”的情景，该情景会属于默认资源类。
- 通过 FTP 服务器添加两个情景，这两个情景会属于 gold 资源类。

```
ciscoasa(config)# mac-address auto prefix 19

ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
```

```
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5

ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
ciscoasa(config-class)# limit-resource vpn other 100
ciscoasa(config-class)# limit-resource vpn burst other 50

ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member gold
```

多情景模式的功能历史记录

表 6-5 列出了各种功能变更以及实施该等功能变更的平台版本。

表 6-5　　多情景模式的功能历史记录

功能名称	平台版本	功能信息
多个安全情景	7.0(1)	引入了多情景模式。 我们引入了以下命令：**context**、 **mode** 和 **class**。
自动的 MAC 地址分配	7.2(1)	引入了至情景接口的 MAC 地址自动分配。 我们引入了以下命令：**mac-address auto**。

表 6-5　　多情景模式的功能历史记录（续）

功能名称	平台版本	功能信息
资源管理	7.2(1)	引入了资源管理。 我们引入了以下命令：**class**、 **limit-resource** 和 **member**。
IPS 的虚拟传感器	8.0(2)	运行 IPS 软件 6.0 版本及更高版本的 AIP SSM 可以运行多个虚拟传感器，这意味着您可以在该 AIP SSM 上配置多个安全策略。您可以将每个情景或单模式 ASA 分配至一个或多个虚拟传感器，也可以将多个安全情景分配至相同的虚拟传感器。 我们引入了以下命令：**allocate-ips**。
增强的自动 MAC 地址分配	8.0(5)/8.2(2)	MAC 地址格式更改为使用前缀，以便使用固定起始值 (A2)，并将不同方案用于故障转移对中的主设备和辅助设备 MAC 地址。现在，MAC 地址在重新加载之后也会保持不变。现在，命令解析器会检查是否已启用自动生成；如果您还想要手动分配 MAC 地址，则不能使用以 A2 开头的手动 MAC 地址。 我们引入了以下命令：**mac-address auto prefix**。
增加了 ASA 5550 和 5580 的最大情景数量。	8.4(1)	ASA 5550 的最大安全情景数量已从 50 增加到 100。ASA 5580 的最大安全情景数量已从 50 增加到 250。
自动的 MAC 地址分配默认启用。	8.5(1)	自动的 MAC 地址分配现在已默认启用。 我们引入了以下命令：**mac-address auto**。
MAC 地址前缀的自动生成	8.6(1)	在多情景模式中，ASA 现在会将自动 MAC 地址生成配置转换为使用默认前缀。ASA 会根据接口 (ASA 5500-X) 或背板 (ASASM) 的 MAC 地址的最后两个字节自动生成前缀。当您重新加载或重新启用 MAC 地址生成时，系统将自动执行此转换。前缀生成方法有很多的优势，包括更好地保证 MAC 地址在网段上的唯一性。您可以通过输入 **show running-config mac-address** 命令查看自动生成的前缀。如果您想要更改此前缀，可以使用自定义前缀重新配置此功能。旧版的 MAC 地址生成方法不再可用。 **注**　为了保持故障转移对的无中断升级功能，ASA 在重新加载时（如果已启用故障转移）*不会*转换现有配置中的 MAC 地址方法。但是，使用故障转移时，我们强烈建议您手动更改为生成的前缀方法，对于 ASASM 尤其如此。如果不使用前缀方法，安装在不同插槽编号中的 ASASM 在故障转移时会发生 MAC 地址更改，并且会出现流量中断。升级后，如要使用 MAC 地址生成的前缀方法，请重新启用 MAC 地址自动生成来使用默认前缀。 我们引入了以下命令：**mac-address auto**。
安全情景中的动态路由	9.0(1)	多情景模式中现在支持 EIGRP 和 OSPFv2 动态路由协议。OSPFv3、RIP 和组播路由不受支持。

表 6-5　　多情景模式的功能历史记录（续）

功能名称	平台版本	功能信息
用于路由表条目的新资源类型	9.0(1)	创建了新资源类型 routes，以用于设置每个情景中的最大路由表条目数。 我们修改以下命令：**limit-resource**、 **show resource types**、**show resource usage** 和 **show resource allocation**。
多情景模式中的站点对站点 VPN	9.0(1)	多情景模式中现在支持站点对站点 VPN 隧道。
用于站点对站点 VPN 隧道的新资源类型	9.0(1)	创建了新资源类型 vpn other 和 vpn burst other，以用于设置每个情景中的站点对站点 VPN 隧道最大数目。 我们修改以下命令：**limit-resource**、 **show resource types**、**show resource usage** 和 **show resource allocation**。

通过故障转移实现高可用性

本章介绍如何配置主用/备用或主用/主用故障转移以实现思科 ASA 的高可用性。

- 第 7-1 页的关于故障转移
- 第 7-21 页的故障转移许可
- 第 7-22 页的故障转移的先决条件
- 第 7-23 页的故障转移准则
- 第 7-23 页的故障转移策略的默认内容
- 第 7-23 页的配置主用/备用故障转移
- 第 7-27 页的配置主用/主用故障转移
- 第 7-32 页的配置可选故障转移参数
- 第 7-38 页的管理故障转移
- 第 7-43 页的监控故障转移
- 第 7-44 页的故障转移功能历史记录

关于故障转移

- 第 7-2 页的故障转移概述
- 第 7-2 页的故障转移系统要求
- 第 7-3 页的故障转移和有状态故障转移链路
- 第 7-7 页的 MAC 和 IP 地址
- 第 7-8 页的 ASA 服务模块 的机箱内和机箱间模块的布置
- 第 7-11 页的无状态和有状态故障转移
- 第 7-13 页的透明防火墙模式要求
- 第 7-15 页的故障转移运行状况监控
- 第 7-16 页的故障转移时间
- 第 7-16 页的配置同步
- 第 7-18 页的关于主用/备用故障转移
- 第 7-19 页的关于主用/主用故障转移

故障转移概述

配置故障转移需要通过专用故障转移链路和有状态链路 （可选）相互连接的两台相同的 ASA。系统会对主用设备和接口的运行状况进行监控，以便确定是否符合特定的故障转移条件。如果符合这些条件，将执行故障转移。

ASA 支持两种故障转移模式：主用/主用故障转移和主用/备用故障转移。每种故障转移模式都有自己确定和执行故障转移的方法。

- 在主用/备用故障转移中，一台设备是主用设备。它会传送流量。备用设备不会主动传送流量。发生故障转移时，主用设备会故障转移到备用设备，后者随即变为主用状态。您可以将主用/备用故障转移用于单情景或多情景模式中的 ASA。
- 在主用/主用故障转移配置下，两台 ASA 都可以传送网络流量。主用/主用故障转移仅适用于多情景模式中的 ASA。在主用/主用故障转移中，您可将 ASA 上的安全情景划分为 2 个*故障转移组*。故障转移组就是一个或多个安全情景的逻辑组。一个组会分配到主 ASA 上，处于主用状态；另一个组会分配到辅助 ASA 上，处于主用状态。发生故障转移时，会在故障转移组级别进行。

两种故障转移模式都支持有状态或无状态故障转移。

故障转移系统要求

本部分介绍，在故障转移配置下，对于 ASA 的硬件、软件和许可证要求。

- 第 7-2 页的硬件要求
- 第 7-2 页的软件要求
- 第 7-3 页的许可证要求

硬件要求

故障转移配置下的两台设备必须：

- 型号相同。
- 拥有相同数量和类型的接口。
- 安装有相同的模块 （如有）
- 安装有相同的 RAM。

如果您在故障转移配置中，使用闪存大小不同的设备，请确保闪存较小的设备有足够的空间来容纳软件映像文件和配置文件。如果闪存较小的设备没有足够的空间，从闪存较大的设备向闪存较小的设备进行配置同步将会失败。

软件要求

故障转移配置下的两台设备必须：

- 处于相同的防火墙模式 （路由或透明）。
- 处于相同的情景模式 （单情景或多情景）。
- 具有相同的主要 （第一个数字）和次要 （第二个数字）软件版本。然而，您可以在升级过程中临时使用不同的软件版本；例如，您可以将一台设备从 8.3(1) 版本升级到 8.3(2) 版本，并使故障转移保持活动状态。我们建议将两台设备都升级为相同版本，以便确保长期的兼容性。

  有关升级故障转移对上的软件的详细信息，请参阅第 36-4 页的升级故障转移对或 ASA 集群。

- 安装有相同的 AnyConnect 映像。如果在执行无中断升级时，故障转移对具有不匹配的映像，则无客户端 SSL VPN 连接会在升级过程的最终重新启动步骤终止，数据库会显示一个孤立会话，并且 IP 池会显示分配给客户端的 IP 地址“正在使用中”。

许可证要求

故障转移配置下的两台设备不需要具有相同的许可证；许可证将整合为故障转移集群许可证。有关详细信息，请参阅第 4-24 页的故障转移或 ASA 集群许可证。

故障转移和有状态故障转移链路

故障转移链路和可选的有状态故障转移链路是两台设备之间的专用连接。

- 第 7-3 页的故障转移链路
- 第 7-4 页的有状态故障转移链路
- 第 7-5 页的避免中断故障转移和数据链路

注意事项　除非您使用 IPsec 隧道或故障转移密钥保护通信，否则所有信息会以明文形式通过故障转移和有状态链路发送。如果使用 ASA 终止 VPN 隧道，此信息包括用于建立隧道的所有用户名、密码和预共享密钥。以明文形式发送该敏感数据可能会带来严重的安全风险。如果您使用 ASA 来终止 VPN 隧道，我们建议使用 IPsec 隧道或故障转移密钥来保护故障转移通信。

故障转移链路

故障转移对中的两台设备会不断地通过故障转移链路进行通信，以便确定每台设备的运行状态。

- 第 7-3 页的故障转移链路数据
- 第 7-3 页的故障转移链路接口
- 第 7-4 页的连接故障转移链路

故障转移链路数据

以下信息将通过故障转移链路传输：

- 设备状态 （主用或备用）
- Hello 消息 （保持活动状态）
- 网络链路状态
- MAC 地址交换
- 配置复制和同步

故障转移链路接口

您可以将任意未使用的接口 （物理、冗余或 EtherChannel）用作故障转移链路；然而，您不能指定当前已配置名称的接口。故障转移链路接口不会配置为常规网络接口；该接口仅会因为故障转移而存在。此接口仅可用于故障转移链路 （或者也用于有状态链路）。

连接故障转移链路

可以使用以下两种方法之一连接故障转移链路：

- 使用不与任何其他设备处于相同网段（广播域或 VLAN）的交换机作为 ASA 的故障转移接口。
- 使用以太网电缆直接连接设备，无需外部交换机。

如果您不在设备之间使用交换机，当接口出现故障时，两台对等设备之间的链路将会断开。这种情况可能会妨碍故障排除工作，因为您无法轻松确定接口发生故障，导致链路断开的设备。

ASA 在其铜缆以太网端口上支持自动 MDI/MDIX，因此，您可以使用交叉电缆或直通电缆。如果您使用的是直通电缆，接口会自动检测该电缆，并将其中一个发送/接收对交换为 MDIX。

有状态故障转移链路

如要使用有状态故障转移，您必须配置有状态故障转移链路 （也称为有状态链路），以便传送连接状态信息。

您有三种可用于有状态链路的接口选项：

- 第 7-4 页的专用接口（建议）
- 第 7-4 页的共享故障转移链路
- 第 7-4 页的共享常规数据接口（不推荐）

注　请勿将管理接口用于有状态链路。

专用接口 （建议）

您可以将专用接口 （物理、冗余或 EtherChannel）用于有状态链路。可以使用以下两种方法之一连接专用的有状态链路：

- 使用不与任何其他设备处于相同网段（广播域或 VLAN）的交换机作为 ASA 的故障转移接口。
- 使用以太网电缆直接连接设备，无需外部交换机。

  如果您不在设备之间使用交换机，当接口出现故障时，两台对等设备之间的链路将会断开。这种情况可能会妨碍故障排除工作，因为您无法轻松确定接口发生故障，导致链路断开的设备。

  ASA 在其铜缆以太网端口上支持自动 MDI/MDIX，因此，您可以使用交叉电缆或直通电缆。如果您使用的是直通电缆，接口会自动检测该电缆，并将其中一个发送/接收对交换为 MDIX。

使用长距离故障转移时，为实现最佳性能，故障转移链路的延迟应该低于 10 毫秒且不超过 250 毫秒。如果延迟超过 10 毫秒，重新传输故障转移消息会导致一些性能降级。

共享故障转移链路

如果您没有足够的接口，可能有必要共享故障转移链路。如果您将故障转移链路用作有状态链路，应使用最快的可用以太网接口。如果该接口存在性能问题，请考虑将一个独立接口专门用于有状态链路。

共享常规数据接口 （不推荐）

与有状态链路共享数据接口，可能会使您易于遭受重播攻击。此外，大量有状态故障转移流量可能会在接口上发送，从而导致该网段上出现性能问题。

将数据接口用作有状态链路，仅在单情景路由模式中受支持。

避免中断故障转移和数据链路

我们建议，让故障转移链路和数据接口使用不同的路径，以便降低所有接口同时发生故障的可能性。如果故障转移链路发生故障，ASA 可使用数据接口来确定是否需要进行故障转移。随后，故障转移操作会被挂起，直到故障转移链路恢复正常。

请参阅以下连接方案，以便设计具有弹性的故障转移网络。

方案 1 - 不推荐

如果单台交换机或一组交换机用于连接两台 ASA 之间的故障转移和数据接口，则交换机或交换机间链路发生故障时，两台 ASA 都将处于主用状态。因此，不推荐使用图 7-1 和图 7-2 中展示的以下两种连接方法。

图 7-1　使用单台交换机进行连接 - 不推荐

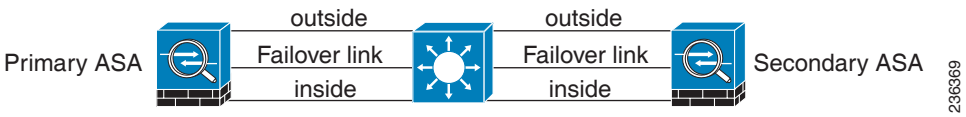
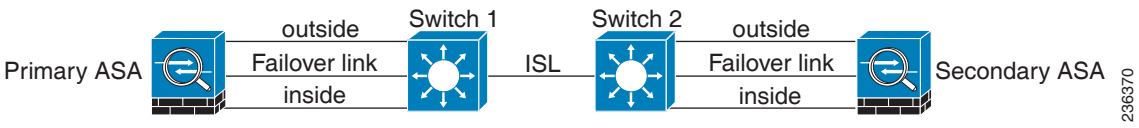


图 7-2　使用两台交换机进行连接 - 不推荐



方案 2 - 推荐

我们不推荐让故障转移链路和数据接口使用相同的交换机。而是应使用不同的交换机或使用直连电缆来连接故障转移链路，如图 7-3 和图 7-4 中所示。

图 7-3　使用不同的交换机进行连接

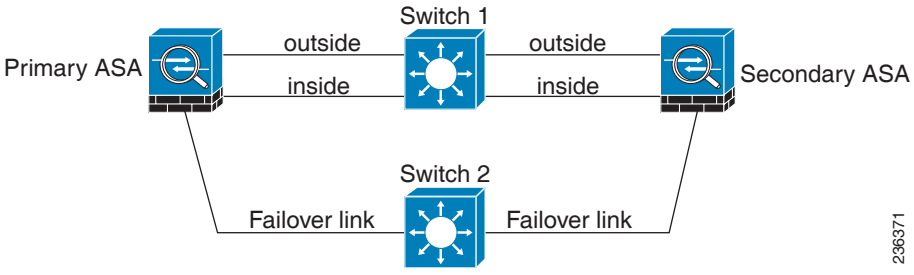
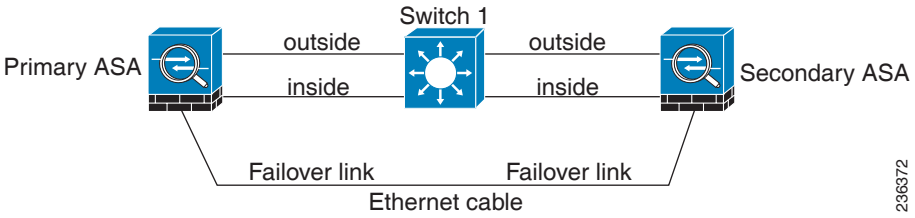


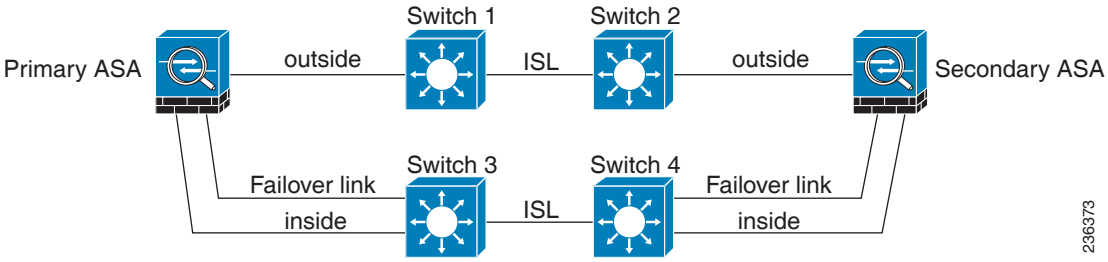
图 7-4　使用电缆进行连接



方案 3 - 推荐

如果 ASA 数据接口连接到多台交换机，则故障转移链路可以连接到其中一台交换机，最好是处于网络的安全一侧 （内部）的交换机，如图 7-5 中所示。

图 7-5　使用安全的交换机进行连接



方案 4 - 推荐

最可靠的故障转移配置使用故障转移链路上的冗余接口，如图 7-6 和图 7-7 中所示。

图 7-6　使用冗余接口进行连接

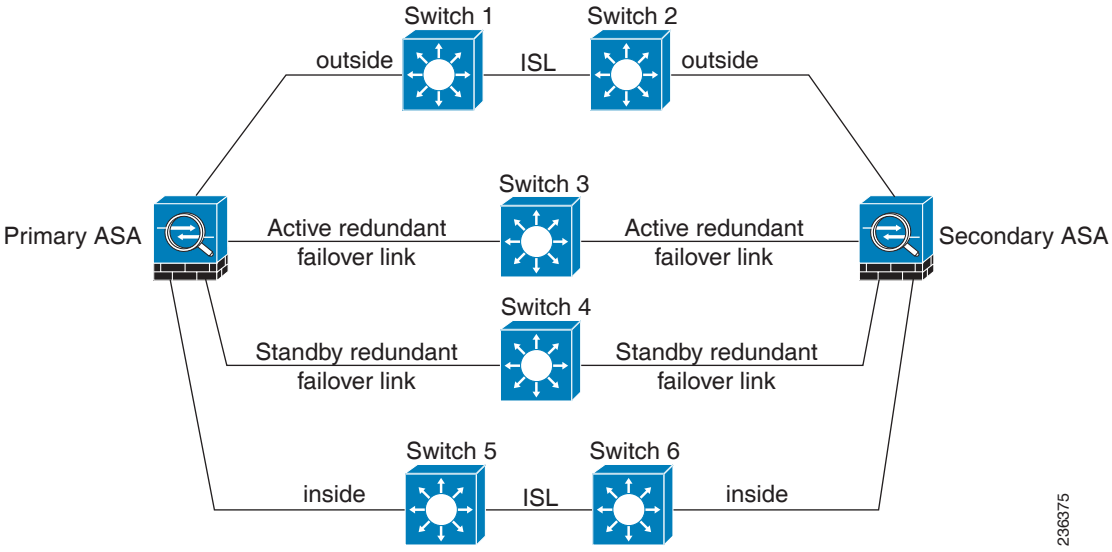
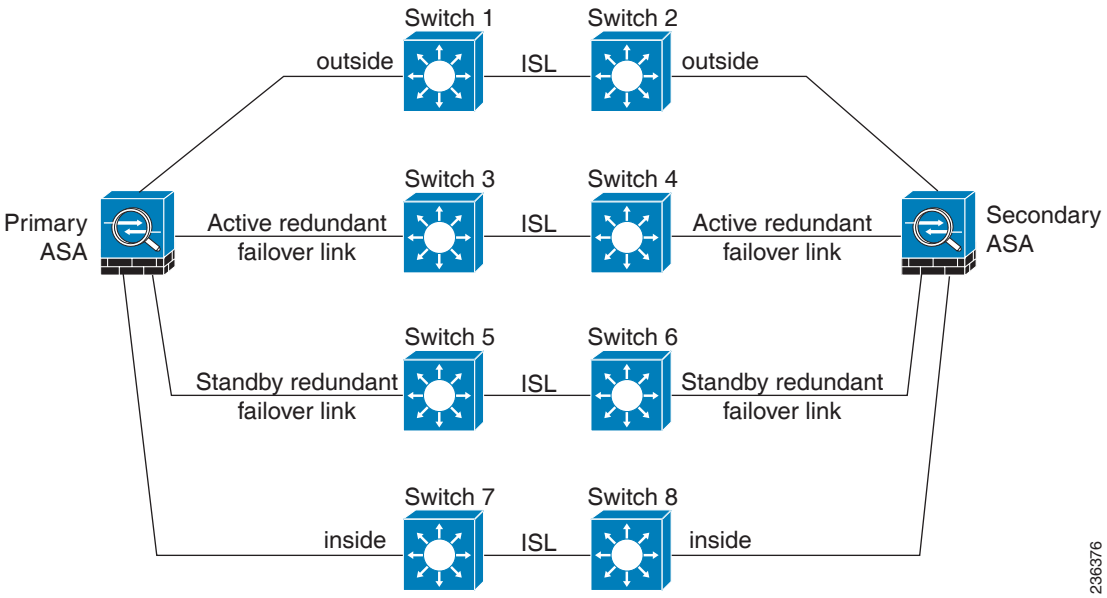


图 7-7　使用交换机间链路进行连接



MAC 和 IP 地址

当您配置接口时，必须在相同网络上指定一个主用 IP 地址和一个备用 IP 地址。

1. 当主设备或故障转移组进行故障转移时，辅助设备会使用主设备的 IP 地址和 MAC 地址，并开始传送流量。
2. 此时处于备用状态的设备会接管备用 IP 地址和 MAC 地址。

由于网络设备不会发现 MAC 与 IP 地址配对的变化，网络上的任意位置都不会发生 ARP 条目变化或超时。

注　如果辅助设备启动时未检测到主设备，辅助设备将成为主用设备，并使用其自己的 MAC 地址，因为它不知道主设备的 MAC 地址。但是，当主设备变得可用时，辅助（主用）设备会将 MAC 地址更改为主设备的地址，这会导致网络流量中断。同样地，如果使用新硬件替换主设备，也会使用新的 MAC 地址。

使用虚拟 MAC 地址可防范这种中断，因为对于启动时的辅助设备，主用 MAC 地址是已知的，并在采用新的主设备硬件时保持不变。在多情景模式中，ASA 会默认生成虚拟的主用和备用 MAC 地址。有关详细信息，请参阅第 6-10 页的有关 MAC 地址的信息。在单情景模式中，您可以手动配置虚拟 MAC 地址；有关详细信息，请参阅第 7-27 页的配置主用/主用故障转移。

如果您没有配置虚拟 MAC 地址，您可能需要清除连接的路由器上的 ARP 表，以便还原流量。ASA 在 MAC 地址变化时，不会为静态 NAT 地址发送无故 ARP，因此，连接的路由器不会知道这些地址的 MAC 地址变化。

注　进行故障转移时，有状态链路的 IP 地址和 MAC 地址不会更改；唯一例外的是，在常规数据接口上配置了有状态链路的情况。

ASA 服务模块 的机箱内和机箱间模块的布置

您可以将主和辅助 ASASM 布置在相同交换机内，也可以将其布置在两台不同的交换机中。以下部分介绍各个选项：

- 第 7-8 页的机箱内故障转移
- 第 7-8 页的机箱间故障转移

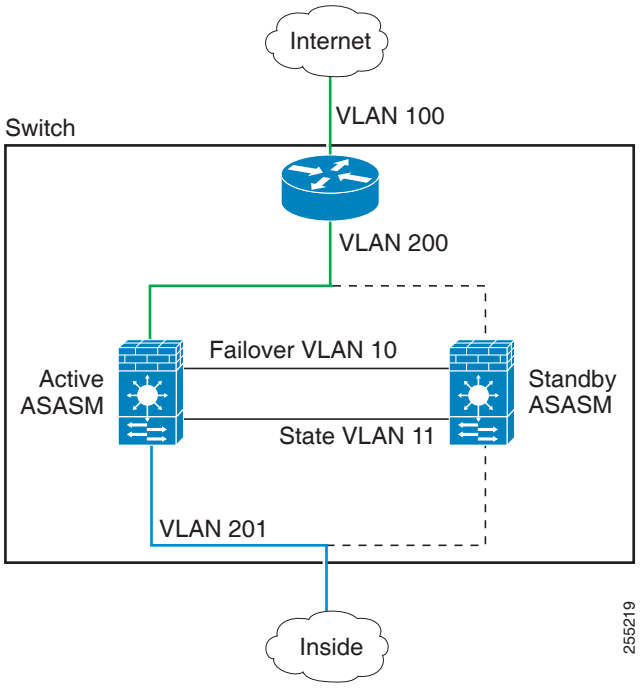
机箱内故障转移

如果您将辅助 ASASM 与主 ASASM 安装在相同交换机中，则可以防御模块级别的故障。如要防御交换机级别的故障以及模块级别的故障，请参阅第 7-8 页的机箱间故障转移。

即使两台 ASASM 均已分配相同的 VLAN，仅主用模块会参与联网。备用模块不会传送任何流量。

图 7-8 展示了典型的交换机内配置。

图 7-8　交换机内故障转移



机箱间故障转移

如要防御交换机级别的故障，您可以将辅助 ASASM 安装在不同的交换机中。ASASM 不直接与交换机协调故障转移，但是，它可以协调地配合交换机故障转移操作。请参阅交换机文档，以便配置交换机的故障转移。

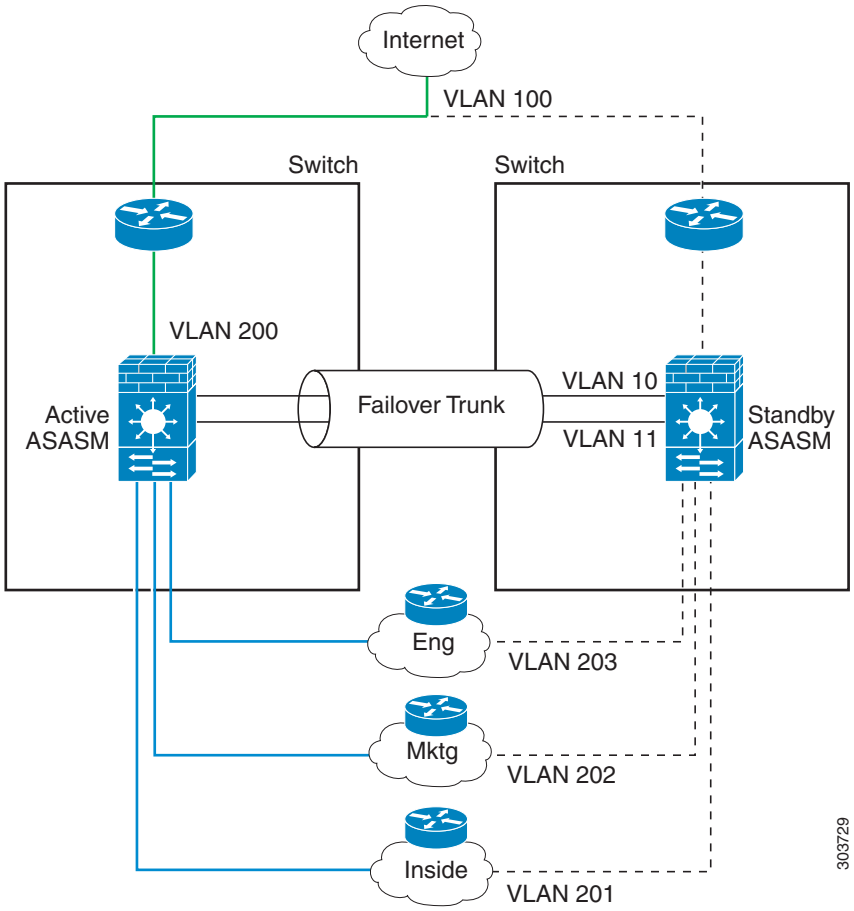
如要在 ASASM 之间实现最佳的故障转移通信可靠性，我们建议您在两台交换机之间配置 EtherChannel Trunk 端口，以便承载故障转移和有状态 VLAN。

对于其他 VLAN，您必须确保两台交换机都可以访问所有防火墙 VLAN，并且受监控的 VLAN 能够成功地在两台交换机之间发送 Hello 数据包。

图 7-9 展示了典型的交换机和 ASASM 冗余配置。两台交换机之间的 Trunk 会承载故障转移 ASASM VLAN （VLAN 10 和 11）。

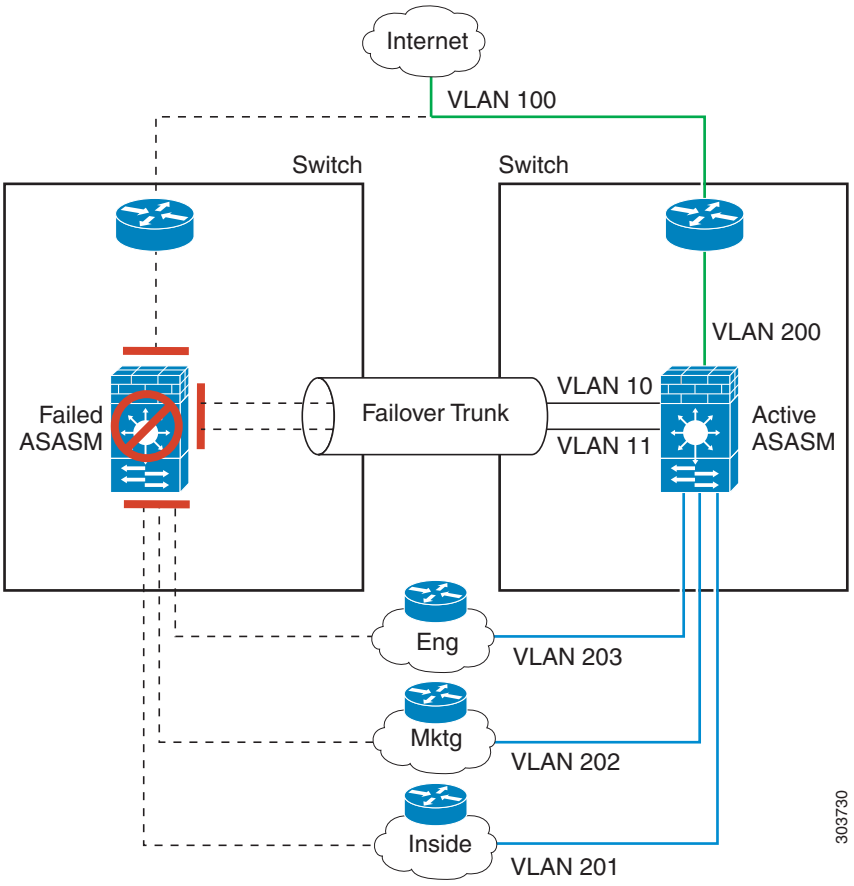
注 ASASM 故障转移与交换机故障转移操作无关；但是，ASASM 可在任何一种交换机故障转移方案下工作。

图 7-9　正常操作



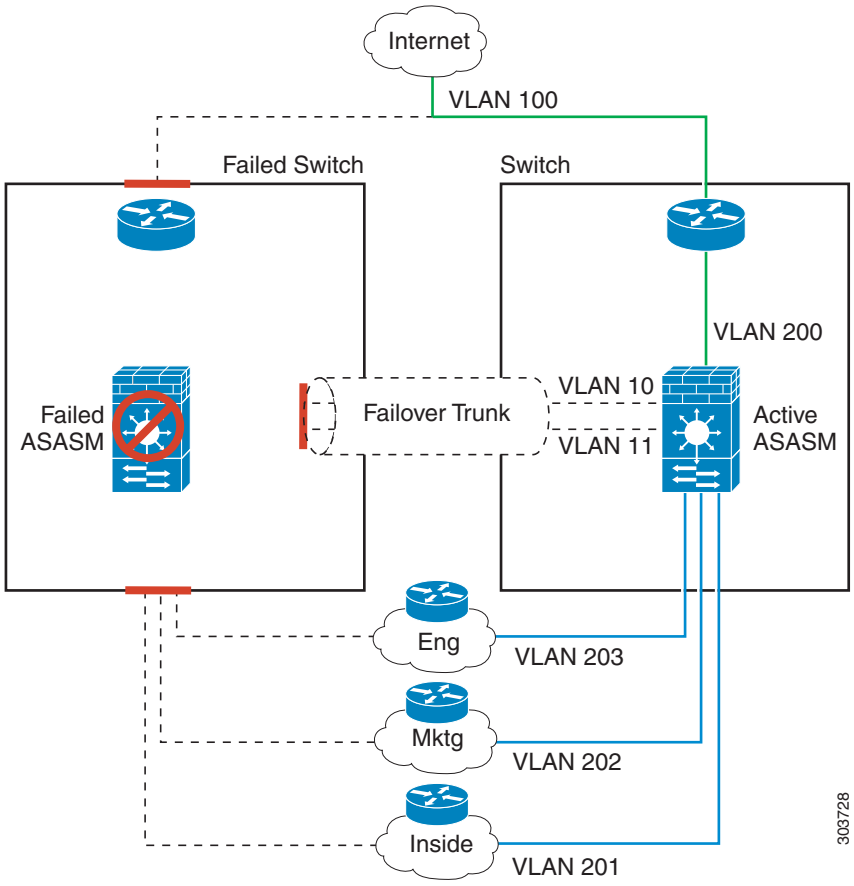
如果主 ASASM 发生故障，则辅助 ASASM 会成为主用设备，并成功传送防火墙 VLAN（图 7-10）。

图 7-10　ASASM 故障



如果整个交换机发生故障，并且 ASASM 也发生故障 （如电源故障），则交换机和 ASASM 均会故障转移到其辅助设备 （图 7-11）。

图 7-11　　交换机故障



无状态和有状态故障转移

ASA 支持主用/备用和主用/主用模式中的两种类型的故障转移，即无状态和有状态故障转移。

- 第 7-12 页的无状态故障转移
- 第 7-12 页的有状态故障转移

注　无客户端 SSL VPN 的某些配置元素 （如书签和自定义）使用 VPN 故障转移子系统，该子系统是有状态故障转移的一部分。您必须使用有状态故障转移，在同步故障转移对中的成员之间同步这些元素。不推荐将无状态故障转移用于无客户端 SSL VPN。

无状态故障转移

发生故障转移时，所有活动连接将会被丢弃。在新的主用设备接管时，客户端需要重新建立连接。

注　无客户端 SSL VPN 的某些配置元素 （如书签和自定义）使用 VPN 故障转移子系统，该子系统是有状态故障转移的一部分。您必须使用有状态故障转移，在同步故障转移对中的成员之间同步这些元素。不推荐将无状态 （常规）故障转移用于无客户端 SSL VPN。

有状态故障转移

启用有状态故障转移时，主用设备会持续将每连接状态信息传送到备用设备，或者在主用/主用故障转移中，在主用和备用故障转移组之间传送此信息。发生故障转移之后，相同的连接信息在新主用设备上可用。受支持的最终用户应用不需要通过重新连接来保持同一通信会话。

- 第 7-12 页的受支持的功能
- 第 7-13 页的不受支持的功能

受支持的功能

启用有状态故障转移时，以下状态信息会传送到备用 ASA：

- NAT 转换表
- TCP 连接状态
- UDP 连接状态
- ARP 表
- 第 2 层网桥表 （在透明防火墙模式中运行时）
- HTTP 连接状态（如果启用了 HTTP 复制）- 默认情况下，启用了有状态故障转移时，ASA 不会复制 HTTP 会话信息。HTTP 会话通常是短期的，因为 HTTP 客户端通常会重试失败的连接尝试，不复制 HTTP 会话可以提高系统性能，而不会产生严重的数据或连接丢失。
- ISAKMP 和 IPsec SA 表
- GTP PDP 连接数据库
- SIP 信令会话
- ICMP 连接状态 - 仅当相应的接口分配给非对称路由组时，才会启用 ICMP 连接复制。
- 动态路由协议 - 有状态故障转移会参与动态路由协议（如 OSPF 和 EIGRP），因此通过主用设备上的动态路由协议获悉的路由，将会保留在备用设备的路由信息库 (RIB) 表中。发生故障转移事件时，数据包可以正常传输，并且只会对流量产生极小的影响，因为主用辅助 ASA 一开始就具有镜像自主 ASA 的规则。进行故障转移后，新的主用设备上的重新融合计时器会立即启动。随后 RIB 表中的代编号将会增加。在重新融合期间，OSPF 和 EIGRP 路由将使用新的代编号进行更新。一旦计时器到期，过时的路由条目（由代编号确定）将从表中移除。于是 RIB 将包含新主用设备上的最新的路由协议转发信息。

注　路由仅会因为主用设备上的链路打开或关闭事件而同步。如果备用设备上的链路打开或关闭，从主用设备发出的动态路由可能会丢失。这是预期的正常行为。

- Cisco IP SoftPhone 会话 - 如果在活动 Cisco IP SoftPhone 会话期间发生故障转移，呼叫将保持活动，因为呼叫会话状态信息已复制到备用设备。呼叫被终止时，IP SoftPhone 客户端将丢失与 Cisco Call Manager 的连接。发生此连接丢失是因为，没有备用设备上的 CTIQBE 挂机消息的会话信息。如果 IP SoftPhone 客户端在特定时间内未从 Call Manager 收到响应，则会认为 Call Manager 不可访问，并会注销自身。
- VPN - 进行故障转移后，VPN 最终用户无需重新进行身份验证，或重新连接 VPN 会话。但是，在 VPN 连接上运行的应用程序，在故障转移过程中可能会丢失数据包，并且无法从数据包丢失中恢复。

不受支持的功能

启用有状态故障转移时，以下状态信息*不会*传送至备用 ASA：

- HTTP 连接表 （除非启用了 HTTP 复制）
- 用户身份验证 (uauth) 表
- 属于高级 TCP 状态跟踪的应用检查 - 这些连接的 TCP 状态不会被自动复制。这些连接被复制到备用设备时，将会进行尽力而为的尝试来重新建立 TCP 状态。
- DHCP 服务器地址租用
- 模块的状态信息，如 ASA IPS SSP 或 ASA CX SSP。
- 电话代理连接 - 主用设备发生故障时，呼叫会失败，媒体数据流会停止传输，并且电话会从故障设备注销，并注册到主用设备。呼叫必须重新建立。
- 选定的无客户端 SSL VPN 功能：
  - 智能隧道
  - 端口转发
  - 插件
  - Java Applets
  - IPv6 无客户端或 Anyconnect 会话
  - Citrix 身份验证 （Citrix 用户在故障转移后必须重新进行身份验证）

透明防火墙模式要求

- 第 7-13 页的设备的透明模式要求
- 第 7-14 页的模块的透明模式要求

设备的透明模式要求

当主用设备故障转移到备用设备时，所连接的运行生成树协议 (STP) 的交换机端口在感知到拓扑变化时，会进入阻塞状态 30 秒至 50 秒。当端口处于阻塞状态时，为避免流量丢失，您可以根据交换机端口模式，配置以下任一变通方案：

- 访问模式 - 启用交换机上的 STP PortFast 功能：

```
interface interface_id
  spanning-tree portfast
```

链路打开时，PortFast 功能会立即使端口转换至 STP 转发模式。该端口仍会参与 STP。因此，如果该端口是环路的一部分，则该端口最终会转换为 STP 阻塞模式。

- Trunk 模式 - 使用 EtherType 访问规则阻止 ASA 内部和外部接口上的 BPDU。

```
access-list id ethertype deny bpdu
access-group id in interface inside_name
access-group id in interface outside_name
```

阻止 BPDU 会在交换机上禁用 STP。在您的网络布局中，确保没有任何环路涉及 ASA。

如果以上选项均不可行，则您可以使用以下任一不太理想的变通方案，这些方案可能会影响故障转移功能或 STP 稳定性。

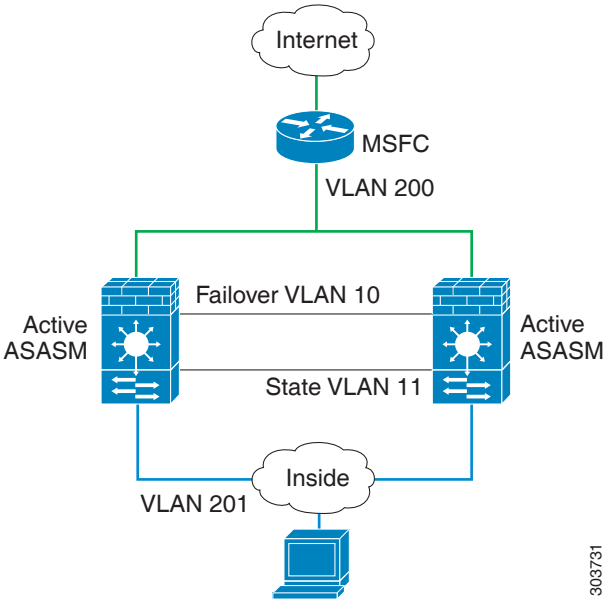
- 禁用接口监控。
- 将接口保持时间增大到一个高值，这将允许 STP 在 ASA 进行故障转移之前融合。
- 降低 STP 计时器的值，以便 STP 在接口保持时间之内融合。

模块的透明模式要求

当您在透明模式中使用故障转移时，为避免出现环路，应允许 BPDU 通过 （默认），并且，您必须使用支持 BPDU 转发的交换机软件。

如果两个模块同时处于活动状态，可能会出现环路，例如，当两个模块同时发现彼此的存在时，或者由于发生故障的故障转移链路。由于 ASASM 会在相同的两个 VLAN 之间桥接数据包，发往外部的内部数据包会被两台 ASASM 不断地复制，这时可能会出现环路 （请参阅图 7-12）。如果及时交换 BPDU，则生成树协议可以断开此类环路。如要断开环路，在 VLAN 200 和 VLAN 201 之间发送的 BPDU 需要桥接。

图 7-12　　透明模式环路



故障转移运行状况监控

ASA 会监控每台设备的整体运行状况和接口运行状况。本部分包括有关 ASA 如何执行测试以确定每台设备状态的信息。

- 第 7-15 页的设备运行状况监控
- 第 7-15 页的接口监控

设备运行状况监控

ASA 会通过监控故障转移链路来确定其他设备的运行状况。当设备在故障转移链路上没有收到三条连续的 Hello 消息时，设备将在每个数据接口（包括故障转移链路）上发送接口 Hello 消息，以便验证对等设备是否响应。 ASA 采取的操作取决于来自其他设备的响应。请参阅以下的可能操作：

- 如果 ASA 在故障转移链路上收到响应，则不会进行故障转移。
- 如果 ASA 在故障转移链路上未收到响应，但在数据接口上收到响应，则设备不会进行故障转移。故障转移链路会标记为发生故障。您应该尽快还原故障转移链路，因为当故障转移链路发生故障时，设备无法故障转移到备用设备。
- 如果 ASA 未在任何接口上收到响应，则备用设备会切换至主用模式，并将另一个设备分类为故障设备。

接口监控

您可以监控最多 250 个接口（在多模式中，会在所有情景之间进行分配）。您应该监控重要的接口。例如，在多模式中，您可以配置一个用于监控共享接口的情景。（由于此接口是共享的，因此所有情景都会受益于监控。）

配置的保持时间过半后，如果设备未在受监控的接口上收到 Hello 消息，将会运行以下测试：

1. 链路打开/关闭测试 - 接口状态测试。如果链路打开/关闭测试表明接口工作正常，ASA 会执行网络测试。这些测试旨在生成网络流量，以便确定发生故障的设备（如有）。每项测试开始时，每台设备会清除其接口的收到的数据包计数。每项测试结束时，每台设备会检查是否收到了任何流量。如果收到了流量，接口会被视为正常工作。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备都没有收到流量，则会进行下一项测试。
2. 网络活动测试 - 收到的网络活动的测试。设备会对最多 5 秒内收到的所有数据包进行计数。如果在此时间间隔内的任意时刻收到任何数据包，接口会被认为正常工作，并且会停止测试。如果没有收到流量，ARP 测试将会开始。
3. ARP 测试 - 读取设备 ARP 缓存，以获取 2 个最近获得的条目。设备会逐一向这些设备发送 ARP 请求，从而尝试激发网络流量。在每次请求之后，设备会对最多 5 秒内收到的所有流量进行计数。如果收到流量，该接口会被视为正常工作。如果未收到任何流量，系统会将 ARP 请求发送到下一台设备。如果列表结束后，仍未收到任何流量，则会开始 Ping 测试。
4. 广播 Ping 测试 - 发送广播 Ping 请求的 Ping 测试。随后设备会对最多 5 秒内收到的所有数据包进行计数。如果在此时间间隔内的任意时刻收到任何数据包，接口会被认为正常工作，并且会停止测试。

受监控接口可以具有以下状态：

- Unknown - 初始状态。此状态还用于表示无法确定状态。
- Normal - 接口正在接收流量。
- Testing - 在该接口上，五次轮询时间内均未收到 Hello 消息。

- Link Down - 接口或 VLAN 通过管理方式关闭。
- No Link - 接口的物理链路关闭。
- Failed - 在接口上未接收到任何流量，但在对等接口上接收到流量。

如果接口上配置了 IPv4 和 IPv6 地址，ASA 会使用 IPv4 地址执行运行状况监控。

如果接口上仅配置了 IPv6 地址，ASA 会使用 IPv6 邻居发现，而不是 ARP 来执行运行状况监控测试。对于广播 Ping 测试，ASA 会使用所有的 IPv6 节点地址 (FE02::1)。

如果对于某个接口，所有网络测试均失败，但在另一设备上的此接口继续成功传送流量，则此接口会被视为发生故障。如果达到故障接口的阀值，则会进行故障转移。如果另一设备的接口在所有网络测试中也全部失败，则这两个接口会进入“Unknown”状态，并且不会计入故障转移限制。

如果接口收到任何流量，则该接口会再次变为正常工作状态。如果不再满足接口故障阈值，发生故障的 ASA 会回到备用模式。

注　如果故障设备未恢复，并且您认为其应该未发生故障，则可通过输入 **failover reset** 命令重置状态。然而，如果故障转移条件仍然存在，设备将再次失败。

故障转移时间

表 7-1 显示了最小、默认和最大故障转移时间。

表 7-1　　ASA 故障转移时间

故障转移条件	最小	默认值	最大
主用设备断电或停止正常操作。	800 毫秒	15 秒	45 秒
主用设备主板接口链路发生故障。	500 毫秒	5 秒	15 秒
主用设备 4GE 模块接口链路发生故障。	2 秒	5 秒	15 秒
主用设备 IPS 或 CSC 模块发生故障。	2 秒	2 秒	2 秒
主用设备接口正常运行，但是连接问题导致接口测试。	5 秒	25 秒	75 秒

配置同步

故障转移包含两种类型的配置同步：

- 第 7-16 页的运行配置复制
- 第 7-17 页的命令复制

运行配置复制

当故障转移对中的一台或两台设备启动时，会进行运行配置复制。配置始终会从主用设备同步到备用设备。备用设备完成其初始启动后，会清除其运行配置 （需要与主用设备通信的故障转移命令除外），而主用设备则会向备用设备发送其完整配置。

复制开始时，主用设备上的 ASA 控制台会显示消息“Beginning configuration replication: Sending to mate”，复制完成时，ASA 会显示消息“End Configuration Replication to mate”。取决于配置的大小，复制过程可能需要几秒到几分钟时间。

在备用设备上，配置仅存在于运行内存中。您应该根据第 2-15 页的保存配置更改 将配置保存到闪存。

注　在复制期间，在主用设备上输入的命令可能无法正确复制到备用设备，在备用设备上输入的命令可能会被从主用设备复制的配置覆盖。在配置复制过程中，应避免在任一设备上输入命令。

注　**crypto ca server** 命令和相关子命令不会同步到故障转移对等设备。

注　配置同步不复制以下文件和配置组件，因此，您必须手动复制这些文件，以便它们匹配：

- AnyConnect 映像
- CSD 映像
- AnyConnect 配置文件
- 本地证书颁发机构 (CA)
- ASA 映像
- ASDM 映像

命令复制

启动后，您在主用设备上输入的命令会被立即复制到备用设备。您不需要将主用配置保存到闪存以复制命令。

在主用/主用故障转移中，在系统执行空间中输入的命令会从其上的故障转移组 1 处于主用状态的设备复制。

未在要进行命令复制的相应设备上输入命令会导致配置失去同步。在进行下一次初始配置同步时，这些更改可能会丢失。

以下命令会复制到备用 ASA：

- 除 **mode**、 **firewall** 和 **failover lan unit** 外的所有配置命令。
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

以下命令*不会*复制至备用 ASA：

- 所有形式的 **copy** 命令 （**copy running-config startup-config** 除外）
- 所有形式的 **write** 命令 （**write memory** 除外）
- **debug**
- **failover lan unit**
- **firewall**

- **show**
- **terminal pager** 和 **pager**

关于主用/备用故障转移

主用/备用故障转移允许您使用备用 ASA 来接管故障设备的功能。主用设备发生故障时，会变为备用状态，同时备用设备会变为主用状态。

注　对于多情景模式，ASA 可以故障转移整个设备（包括所有情景），但不能对各个情景单独进行故障转移。

- 第 7-18 页的主/辅助角色和主用/备用状态
- 第 7-18 页的启动时的主用设备确定
- 第 7-18 页的故障转移事件

主/辅助角色和主用/备用状态

故障转移对中两台设备之间的主要差别与哪一设备为主用设备，哪一设备为备用设备，换句话说，使用哪一个 IP 地址以及哪一台设备会主动传送流量有关。

然而，设备之间还存在一些取决于哪一设备为主设备 （在配置中指定），哪一设备为辅助设备的一些差别：

- 如果两台设备同一时间启动 （并且运行状况相同），主设备总是会成为主用设备。
- 主设备的 MAC 地址总是与主用 IP 地址耦合。此规则的例外情况是，辅助设备处于活动状态，而且无法通过故障转移链路获取主设备的 MAC 地址。在这种情况下，会使用辅助设备的 MAC 地址。

启动时的主用设备确定

主用设备会如下确定：

- 如果某台设备启动，并检测到对等体已作为主用设备运行，则该设备会成为备用设备。
- 如果某台设备启动，并且未检测到对等体，则该设备会成为主用设备。
- 如果两台设备同时启动，则主设备成为主用设备，辅助设备成为备用设备。

故障转移事件

在主用/备用故障转移中，故障转移会在设备级别进行。即使在多情景模式中运行的系统上，您也无法对个别情景或一组情景进行故障转移。

表 7-2 显示每种故障事件的故障转移操作。对于每种故障事件，该表显示了故障转移策略（故障转移或不进行故障转移）、主用设备执行的操作、备用设备执行的操作，以及有关故障转移条件和操作的所有特别说明。

表 7-2　故障转移行为

故障事件	策略	主用设备操作	备用设备操作	备注
主用设备发生故障（电源或硬件）	故障转移	不适用	变为主用 将主用设备标记为发生故障	在任何受监控接口或故障转移链路上，均未收到 Hello 消息。
以前的主用设备恢复	不进行故障转移	成为备用设备	不进行操作	无。
备用设备发生故障（电源或硬件）	不进行故障转移	将备用设备标记为发生故障	不适用	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。
故障转移链路在运行期间发生故障	不进行故障转移	将故障转移链路标记为发生故障	将故障转移链路标记为发生故障	您应该尽快还原故障转移链路，因为当故障转移链路发生故障时，设备无法故障转移到备用设备。
故障转移链路在启动时发生故障	不进行故障转移	将故障转移链路标记为发生故障	变为主用	如果故障转移链路在启动时发生故障，则两台设备都会成为主用设备。
有状态链路发生故障	不进行故障转移	不进行操作	不进行操作	如果发生故障转移，状态信息会过时，而且会话会被终止。
主用设备上的接口故障超过阈值	故障转移	将主用设备标记为发生故障	变为主用	无。
备用设备上的接口故障超过阈值	不进行故障转移	不进行操作	将备用设备标记为发生故障	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。

关于主用/主用故障转移

本部分介绍主用/主用故障转移。

- 第 7-19 页的主用/主用故障转移概述
- 第 7-20 页的故障转移组的主/辅助角色和主用/备用状态
- 第 7-20 页的故障转移事件

主用/主用故障转移概述

在主用/主用故障转移配置下，两台 ASA 都可以传送网络流量。主用/主用故障转移仅适用于多情景模式中的 ASA。在主用/主用故障转移中，您可将 ASA 上的安全情景划分为最多 2 个故障转移组。

故障转移组就是一个或多个安全情景的逻辑组。您可以将故障转移组指定为在主 ASA 上处于主用状态，并将故障转移组 2 指定为在辅助 ASA 上处于主用状态。发生故障转移时，会在故障转移组级别进行。例如，根据接口故障模式，故障转移组 1 可能会故障转移到辅助 ASA，相应地，故

障转移组 2 可能故障转移到主 ASA。在以下情况下可能发生此事件：故障转移组 1 中的接口在主 ASA 上发生故障，但在辅助 ASA 上正常工作，而故障转移组 2 中的接口在辅助 ASA 上发生故障，但在主 ASA 上正常工作。

管理情景始终是故障转移组 1 的成员。默认情况下，所有未分配的安全情景也是故障转移组 1 的成员。如果希望使用主用/主用故障转移，但对多情景不感兴趣，最简单的配置是添加一个额外的情景并将其分配给故障转移组 2。

注　配置主用/主用故障转移时，请确保两台设备的整合流量在每台设备的处理能力之内。

注　需要时，可将两个故障转移组分配到一台 ASA，但您将无法利用具有两台主用 ASA 的优势。

故障转移组的主/辅助角色和主用/备用状态

就像在主用/备用故障转移中一样，主用/主用故障转移对中的一台设备会被指定为主设备，另一设备会被指定为辅助设备。不同于主用/备用故障转移的是，当两台设备同时启动时，该指定不指示哪一台设备会成为主用设备。相反，主/辅助指定会做两件事：

- 两台设备同时启动时，主设备会提供运行配置。
- 配置中的每个故障转移组都配置了主或辅助设备首选项。

启动时的故障转移组主用设备确定

故障转移组在其上变为主用状态的设备如下确定：

- 一台设备启动时，如果对等设备不可用，两个故障转移组都会在该设备上变为主用状态。
- 一台设备启动时，如果对等设备处于主用状态 （而且两个故障转移组都处于主用状态），故障转移组将在主用设备上保持主用状态，而无论故障转移组的主设备或辅助设备首选项如何，直到出现以下情形之一：
  - 发生故障转移。
  - 您手动强制执行故障转移。
  - 您为故障转移组配置了抢占，这导致故障转移组在设备变得可用时，自动在首选设备上变为主用状态。
- 两台设备同时启动时，在同步配置后，每个故障转移组都会在其首选设备上变为主用状态。

故障转移事件

在主用/主用故障转移配置中，故障转移会在故障转移组级别，而不是系统级别进行。例如，如果您将两个故障转移组指定为主设备上的主用故障转移组，并且故障转移组 1 发生故障，则故障转移组 2 会在主设备上保持主用，而故障转移组 1 则会在辅助设备上变为主用。

由于故障转移组可以包含多个情景，并且每个情景可以包含多个接口，因此单个情景中的所有接口都发生故障而不导致相关故障转移组发生故障是有可能的。

表 7-3 显示每种故障事件的故障转移操作。对于每种故障事件，给出了策略 （是否发生故障转移）、主用故障转移组的操作和备用故障转移组的操作。

表 7-3　　主用/主用故障转移的故障转移行为

故障事件	策略	主用组操作	备用组操作	备注
设备发生电源或软件故障	故障转移	变为备用，并标记为发生故障	变为主用 将主用设备标记为发生故障	故障转移对中的一台设备发生故障时，该设备上的所有主用故障转移组都会被标记为发生故障，并在对等设备上变为主用。
主用故障转移组上的接口故障超过阈值	故障转移	将主用组标记为发生故障	变为主用	无。
备用故障转移组上的接口故障超过阈值	不进行故障转移	不进行操作	将备用组标记为发生故障	备用故障转移组被标记为发生故障后，主用故障转移组不会尝试进行故障转移，即使超过接口故障阈值也是如此。
以前的主用故障转移组恢复	不进行故障转移	不进行操作	不进行操作	除非配置了故障转移组抢占，否则故障转移组会在其当前设备上保持主用状态。
故障转移链路在启动时发生故障	不进行故障转移	变为主用	变为主用	如果故障转移链路在启动时发生故障，则两台设备上的故障转移组都会变为主用。
有状态链路发生故障	不进行故障转移	不进行操作	不进行操作	如果发生故障转移，状态信息会过时，而且会话会被终止。
故障转移链路在运行期间发生故障	不进行故障转移	不适用	不适用	每台设备都会将故障转移链路标记为发生故障。您应该尽快还原故障转移链路，因为当故障转移链路发生故障时，设备无法故障转移到备用设备。

故障转移许可

主用/备用故障转移

型号	许可证要求
ASA 5512-X	增强型安全许可证。
ASAv	标准许可证和高级许可证。
所有其他型号	基础许可证。

故障转移设备不要求每台设备上具有相同的许可证。如果您在两台设备上都有许可证，它们将组合成一个运行的故障转移集群许可证。此规则的例外情况包括：

- 5512-X 的增强型安全许可证 - 基础许可证不支持故障转移，因此，您不能在只有基础许可证的备用设备上启用故障转移。
- 加密许可证 - 两台设备必须拥有相同的加密许可证。

- ASA 5512-X 至 ASA 5555-X 的 IPS 模块许可证 - 两台设备都需要 IPS 模块许可证。您还需要两台设备的 IPS 端上的 IPS 签名订用。请参阅以下准则：
  - 如要购买 IPS 签名订用，您需要有预装了 IPS 的 ASA （部件号必须包括“IPS”，例如 ASA5515-IPS-K9）；您不能为非 IPS 部件号 ASA 购买 IPS 签名订用。
  - 您需要两台设备上的 IPS 签名订用；由于此订用不是 ASA 许可证，因此不在故障转移中共享。
  - IPS 签名订用要求每台设备具有唯一的 IPS 模块许可证。与其他 ASA 许可证一样，IPS 模块许可证在故障转移集群许可证中技术共享。但是，由于 IPS 签名订用要求，您必须为每台设备购买单独的 IPS 模块许可证。
- ASAv 虚拟 CPU - 用于故障转移部署，请确保备用设备分配到的虚拟 CPU 数量与主要设备相同 （以及匹配的虚拟 CPU 许可证）。

主用/主用故障转移

型号	许可证要求
ASA 5512-X	增强型安全许可证。
ASAv	不支持。
所有其他型号	基础许可证。

故障转移设备不要求每台设备上具有相同的许可证。如果您在两台设备上都有许可证，它们将组合成一个运行的故障转移集群许可证。此规则的例外情况包括：

- 5512-X 的增强型安全许可证 - 基础许可证不支持故障转移，因此，您不能在只有基础许可证的备用设备上启用故障转移。
- 加密许可证 - 两台设备必须拥有相同的加密许可证。
- ASA 5512-X 至 ASA 5555-X 的 IPS 模块许可证 - 两台设备都需要 IPS 模块许可证。您还需要两台设备的 IPS 端上的 IPS 签名订用。请参阅以下准则：
  - 如要购买 IPS 签名订用，您需要有预装了 IPS 的 ASA（部件号必须包括“IPS”，例如 ASA5515-IPS-K9）；您不能为非 IPS 部件号 ASA 购买 IPS 签名订用。
  - 您需要两台设备上的 IPS 签名订用；由于此订用不是 ASA 许可证，因此不在故障转移中共享。
  - IPS 签名订用要求每台设备具有唯一的 IPS 模块许可证。与其他 ASA 许可证一样，IPS 模块许可证在故障转移集群许可证中技术共享。但是，由于 IPS 签名订用要求，您必须为每台设备购买单独的 IPS 模块许可证。
- ASAv 虚拟 CPU - 用于故障转移部署，请确保备用设备分配到的虚拟 CPU 数量与主要设备相同 （以及匹配的虚拟 CPU 许可证）。

故障转移的先决条件

请参阅第 7-2 页的故障转移系统要求。

故障转移准则

情景模式准则

- 主用/备用模式在单情景和多情景模式中受支持。
- 主用/主用模式仅在多情景模式中受支持。
- 对于多情景模式，除非另外说明，请在系统执行空间中执行所有操作步骤。
- 如果您尝试同时在两个或更多情景中进行配置更改，ASA 故障转移复制将会失败。变通方案是在每个情景中连续进行配置更改。

附加准则和限制

- 发生故障转移事件时，在连接到 ASA 故障转移对的交换机上配置端口安全性，可能会导致通信问题。一个安全端口上配置或获悉的安全 MAC 地址移至另一安全端口，交换机端口安全功能标记违例时，会发生此问题。
- 您可以在一台设备上监控跨所有情景的最多 250 个接口。
- 对于主用/主用故障转移，不应在相同 ASR 组中配置相同情景中的两个接口。
- 对于主用/主用故障转移，您可以定义最多两个故障转移组。
- 对于主用/主用故障转移，移除故障转移组时，您必须最后移除故障转移组 1。故障转移组 1 始终包含管理情景。未分配到故障转移组的所有情景将默认分配到故障转移组 1。您不能移除已显式为其分配情景的故障转移组。

相关主题

- 第 36-33 页的故障转移配置中的自动更新服务器支持

故障转移策略的默认内容

默认情况下，故障转移策略包含以下内容：

- 在有状态故障转移中不进行 HTTP 复制。
- 单个接口故障导致故障转移。
- 接口轮询时间为 5 秒。
- 接口保持时间为 25 秒。
- 设备轮询时间为 1 秒。
- 设备保持时间为 15 秒。
- 虚拟 MAC 地址在多情景模式中启用；在单情景模式中禁用。
- 监控所有物理接口，或者对于 ASASM，所有 VLAN 接口。

配置主用 / 备用故障转移

- 第 7-24 页的为主用/备用故障转移配置主设备
- 第 7-27 页的为主用/备用故障转移配置辅助设备

为主用/备用故障转移配置主设备

遵循此部分介绍的操作步骤，以便配置主用/备用故障转移配置中的主设备。这些步骤提供在主设备上启用故障转移所需的最小配置。

准备工作

- 根据第 11 章，“路由模式接口”或第 12 章，“透明模式接口”，为除故障转移和有状态链路外的所有接口配置备用 IP 地址
- 请勿为故障转移和有状态链路配置 **nameif**。
- 对于多情景模式，请在系统执行空间中完成本操作步骤。要从该情景切换至系统执行空间，请输入 **changeto system** 命令。

操作步骤

步骤 1　将此设备指定为主设备：

```
failover lan unit primary
```

步骤 2　指定要用作故障转移链路的接口：

```
failover lan interface if_name interface_id
```

示例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

此接口不可用于任何其他用途 （但用于有状态链路除外）。

if_name 参数可为接口指定名称。

interface_id 参数可以是物理接口、子接口、冗余接口或 EtherChannel 接口 ID。在 ASASM 上，*interface_id* 可以指定 VLAN ID。

尽管您可以将 EtherChannel 用作故障转移或有状态链路，但为了防止错序数据包，仅会使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。不能作为故障转移链路处于使用状态的 EtherChannel 配置。

步骤 3　为故障转移链路分配主用和备用 IP 地址：

```
failover interface ip failover_if_name {ip_address mask | ipv6_address/prefix} standby
ip_address
```

示例：

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

或：

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

此地址应处于未使用的子网上。

备用 IP 地址必须与主用 IP 地址位于同一子网。

步骤 4　启用故障转移链路：

```
interface failover_interface_id
  no shutdown
```

示例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

步骤 5　（可选）指定要用作有状态链路的接口：

failover link *if_name interface_id*

示例：

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

我们建议，指定与故障转移链路或数据接口不同的独立接口。

if_name 参数可为接口指定名称。

interface_id 参数可以是物理接口、子接口、冗余接口或 EtherChannel 接口 ID。在 ASASM 上，*interface_id* 可以指定 VLAN ID。

尽管您可以将 EtherChannel 用作故障转移或有状态链路，但为了防止错序数据包，仅会使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。不能作为故障转移链路处于使用状态的 EtherChannel 配置。

步骤 6　如果您指定了单独的有状态链路，可以将主用和备用 IP 地址分配给有状态链路：

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

示例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

或：

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

此地址应在不同于故障转移链路的未使用子网上。

备用 IP 地址必须与主用 IP 地址位于同一子网。

如果您将共享有状态链路，请跳过此步骤。

步骤 7　如果您指定了单独的有状态链路，请启用有状态链路。

interface *state_interface_id*
  no shutdown

示例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

如果您将共享有状态链路，请跳过此步骤。

步骤 8　（可选）请执行以下任一操作，以便加密故障转移和有状态链路上的通信：

- （首选）在设备之间的故障转移和有状态链路上建立 IPsec LAN 对 LAN 隧道，以便加密所有的故障转移通信：

  failover ipsec pre-shared-key [**0** | **8**] *key*

  示例：

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

该 *key* 的最大长度为 128 个字符。确定两台设备上的相同密钥。此密钥由 IKEv2 用于建立隧道。

如果您使用主密码 （请参阅第 13-10 页的配置主密码），则该密钥在配置中会被加密。如果您从配置 （例如，从 **more system:running-config** 输出）复制，请通过使用 **8** 关键字来指定已对该密钥加密。默认情况下使用 **0**，表明未加密的密码。

failover ipsec pre-shared-key 在 **show running-config** 输出中显示为 *****；此已屏蔽的密钥不可复制。

如果您未配置故障转移和有状态链路加密，故障转移通信 （包括在命令复制期间发送的配置中的所有密码或密钥）将采用明文形式。

您不能同时使用 IPsec 加密和旧版**故障转移密钥**加密。如果您配置两种方法，将会使用 IPsec。然而，如果您使用主密码 （请参阅第 13-10 页的配置主密码），在配置 IPsec 加密之前，必须先使用 **nofailover key** 命令移除故障转移密钥。

故障转移 LAN 对 LAN 隧道不计入 IPsec（其他 VPN）许可证。

- （可选）对故障转移和有状态链路上的故障转移通信进行加密：

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  示例：

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  可以使用 1 至 63 个字符的 *shared_secret*，或者 32 个字符的 **hex** *key*。对于 *shared_secret*，您可以使用数字、字母或标点符号的任意组合。该共享机密或十六进制密钥用于生成加密密钥。确定两台设备上的相同密钥。

  如果您使用主密码 （请参阅第 13-10 页的配置主密码），则共享机密或十六进制密钥在配置中会被加密。如果您从配置 （例如，从 **more system:running-config** 输出）复制，请通过使用 **8** 关键字来指定共享机密或十六进制密钥。默认情况下使用 **0**，表明未加密的密码。

  failover key 共享机密在 **show running-config** 输出中显示为 *****；此已屏蔽的密钥不可复制。

  如果您未配置故障转移和有状态链路加密，故障转移通信 （包括在命令复制期间发送的配置中的所有密码或密钥）将采用明文形式。

步骤 9　启用故障转移：

failover

步骤 10　将系统配置保存到闪存：

write memory

示例

以下示例配置主设备的故障转移参数：

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4
failover interface ip statelink 172.27.49.1 255.255.255.0 standby 172.27.49.2
interface gigabitethernet 0/4
  no shutdown
failover ipsec pre-shared-key a3rynsun
failover
```

为主用/备用故障转移配置辅助设备

在辅助设备上只需要配置故障转移链路。最初辅助设备需要这些命令来与主设备进行通信。在主设备将其配置发送到辅助设备后，两个配置之间的唯一永久性差别是 **failover lan unit** 命令，该命令确定每台设备是主设备，还是辅助设备。

准备工作

- 请勿为故障转移和有状态链路配置 **nameif**。
- 对于多情景模式，请在系统执行空间中完成本操作步骤。要从该情景切换至系统执行空间，请输入 **changeto system** 命令。

操作步骤

步骤 1　在主设备上重新输入完全相同的命令，**failover lan unit primary** 命令*除外*。或者，您可以使用 **failover lan unit secondary** 命令代替该命令，但这并非必需，因为 **secondary** 是默认设置。请参阅第 7-24 页的为主用/备用故障转移配置主设备。

例如：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its
sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
  no shutdown
ciscoasa(config)# failover link statelink gigabitethernet0/4
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its
sub-interfaces
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
ciscoasa(config)# interface gigabitethernet 0/4
  no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

步骤 2　故障转移配置同步之后，会将配置保存到闪存：

```
ciscoasa(config)# write memory
```

配置主用 / 主用故障转移

- 第 7-27 页的为主用/主用故障转移配置主设备
- 第 7-31 页的为主用/主用故障转移配置辅助设备

为主用/主用故障转移配置主设备

遵循此部分介绍的操作步骤，以便配置主用/主用故障转移配置中的主设备。这些步骤提供在主设备上启用故障转移所需的最小配置。

准备工作

- 根据第 6-14 页的启用或禁用多情景模式启用多情景模式。
- 根据第 11 章，“路由模式接口”或第 12 章，“透明模式接口”，为除故障转移和有状态链路外的所有接口配置备用 IP 地址
- 请勿为故障转移和有状态链路配置 **nameif**。
- 在系统执行空间中完成此操作步骤。如要从该情景切换至系统执行空间，请输入 **changeto system** 命令。

操作步骤

步骤 1　将此设备指定为主设备：

```
failover lan unit primary
```

步骤 2　指定要用作故障转移链路的接口：

```
failover lan interface if_name interface_id
```

示例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

此接口不可用于任何其他用途（但用于有状态链路除外）。

if_name 参数可为接口指定名称。

interface_id 参数可以是物理接口、子接口、冗余接口或 EtherChannel 接口 ID。在 ASASM 上，*interface_id* 可以指定 VLAN ID。

尽管您可以将 EtherChannel 用作故障转移或有状态链路，但为了防止错序数据包，仅会使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。不能作为故障转移链路处于使用状态的 EtherChannel 配置。

步骤 3　为故障转移链路分配主用和备用 IP 地址：

```
failover interface ip if_name {ip_address mask | ipv6_address/prefix} standby ip_address
```

示例：

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

或：

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

此地址应处于未使用的子网上。

备用 IP 地址必须与主用 IP 地址位于同一子网。

步骤 4　启用故障转移链路：

```
interface failover_interface_id
  no shutdown
```

示例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

步骤 5　（可选）指定要用作有状态链路的接口：

failover link *if_name interface_id*

示例：

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

我们建议，指定与故障转移链路或数据接口不同的独立接口。

if_name 参数可为接口指定名称。

interface_id 参数可以是物理接口、子接口、冗余接口或 EtherChannel 接口 ID。在 ASASM 上，*interface_id* 可以指定 VLAN ID。

尽管您可以将 EtherChannel 用作故障转移或有状态链路，但为了防止错序数据包，仅会使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。不能作为故障转移链路处于使用状态的 EtherChannel 配置。

步骤 6　如果您指定了单独的有状态链路，可以将主用和备用 IP 地址分配给有状态链路：

此地址应在不同于故障转移链路的未使用子网上。

备用 IP 地址必须与主用 IP 地址位于同一子网。

如果您将共享有状态链路，请跳过此步骤。

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

示例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

或：

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

步骤 7　如果您指定了单独的有状态链路，请启用有状态链路：

interface *state_interface_id*
  no shutdown

示例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

如果您将共享有状态链路，请跳过此步骤。

步骤 8　（可选）请执行以下任一操作，以便加密故障转移和有状态链路上的通信：

- （首选）在设备之间的故障转移和有状态链路上建立 IPsec LAN 对 LAN 隧道，以便加密所有的故障转移通信：

  failover ipsec pre-shared-key [**0** | **8**] *key*

  示例：

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  该 *key* 的最大长度为 128 个字符。确定两台设备上的相同密钥。此密钥由 IKEv2 用于建立隧道。

  如果您使用主密码 （请参阅第 13-10 页的配置主密码），则该密钥在配置中会被加密。如果您从配置 （例如，从 **more system:running-config** 输出）复制，请通过使用 **8** 关键字来指定已对该密钥加密。默认情况下使用 **0**，表明未加密的密码。

failover ipsec pre-shared-key 在 **show running-config** 输出中显示为 *****；此已屏蔽的密钥不可复制。

如果您未配置故障转移和有状态链路加密，故障转移通信 （包括在命令复制期间发送的配置中的所有密码或密钥）将采用明文形式。

您不能同时使用 IPsec 加密和旧版**故障转移密钥**加密。如果您配置两种方法，将会使用 IPsec。然而，如果您使用主密码 （请参阅第 13-10 页的配置主密码），在配置 IPsec 加密之前，必须先使用 **nofailover key** 命令移除故障转移密钥。

故障转移 LAN 对 LAN 隧道不计入 IPsec（其他 VPN）许可证。

- （可选）对故障转移和有状态链路上的故障转移通信进行加密：

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  示例：

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  可以使用 1 至 63 个字符的 *shared_secret*，或者 32 个字符的 **hex** *key*。

  对于 *shared_secret*，您可以使用数字、字母或标点符号的任意组合。该共享机密或十六进制密钥用于生成加密密钥。确定两台设备上的相同密钥。

  如果您使用主密码（请参阅第 13-10 页的配置主密码），则共享机密或十六进制密钥在配置中会被加密。如果您从配置（例如，从 **more system:running-config** 输出）复制，请通过使用 **8** 关键字来指定共享机密或十六进制密钥。默认情况下使用 **0**，表明未加密的密码。

  failover key 共享机密在 **show running-config** 输出中显示为 *****；此已屏蔽的密钥不可复制。

  如果您未配置故障转移和有状态链路加密，故障转移通信 （包括在命令复制期间发送的配置中的所有密码或密钥）将采用明文形式。

步骤 9　创建故障转移组 1：

```
failover group 1
```

默认情况下，该组将被分配给主设备。通常，您可以将组 1 分配给主设备，将组 2 分配给辅助设备。如果您需要一个非标准配置，可以使用 **primary** 或 **secondary** 子命令视需要指定不同的设备首选项。

步骤 10　创建故障转移组 2，并将其分配给辅助设备：

```
failover group 2
  secondary
```

步骤 11　进入给定情景的情景配置模式，然后将该情景分配给故障转移组：

```
context name
  join-failover-group {1 | 2}
```

示例：

```
ciscoasa(config)# context Eng
ciscoasa(config-ctx)# join-failover-group 2
```

对每个情景重复此命令。

所有未分配的情景会自动分配到故障转移组 1。管理情景始终是故障转移组 1 的成员；您不能将其分配给组 2。

步骤 12　启用故障转移：

```
failover
```

步骤 13　将系统配置保存到闪存：

```
write memory
```

示例

以下示例配置主设备的故障转移参数：

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4
failover interface ip statelink 172.27.49.1 255.255.255.0 standby 172.27.49.2
interface gigabitethernet 0/4
  no shutdown
failover group 1
failover group 2
  secondary
context admin
  join-failover-group 1
failover ipsec pre-shared-key a3rynsun
failover
```

为主用/主用故障转移配置辅助设备

在辅助设备上只需要配置故障转移链路。最初辅助设备需要这些命令来与主设备进行通信。在主设备将其配置发送到辅助设备后，两个配置之间的唯一永久性差别是 **failover lan unit** 命令，该命令确定每台设备是主设备，还是辅助设备。

准备工作

- 根据第 6-14 页的启用或禁用多情景模式启用多情景模式。
- 请勿为故障转移和有状态链路配置 **nameif**。
- 在系统执行空间中完成此操作步骤。如要从该情景切换至系统执行空间，请输入 **changeto system** 命令。

操作步骤

步骤 1　在主设备上重新输入完全相同的命令，**failover lan unit primary** 命令*除外*。或者，您可以使用 **failover lan unit secondary** 命令代替该命令，但这并非必需，因为 **secondary** 是默认设置。您也不需要输入 **failover group** 和 **join-failover-group** 命令，因为这些命令会从主设备复制。请参阅第 7-27 页的为主用/主用故障转移配置主设备。

例如：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its
sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
  no shutdown
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

```
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its
sub-interfaces
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
ciscoasa(config)# interface gigabitethernet 0/4
  no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

步骤 2　故障转移配置通过主设备同步后，将配置保存到闪存：

```
ciscoasa(config)# write memory
```

步骤 3　如果需要，可强行要求故障转移组 2 在辅助设备上处于主用状态：

```
failover active group 2
```

配置可选故障转移参数

您可以视需要自定义故障转移设置。

- 第 7-32 页的配置故障转移条件、 HTTP 复制、组抢占、和 MAC 地址
- 第 7-35 页的配置接口监控
- 第 7-35 页的配置非对称路由数据包支持 （主用/主用模式）

配置故障转移条件、 HTTP 复制、组抢占、和 MAC 地址

有关您可在此部分中更改的许多参数的默认设置，请参阅第 7-23 页的故障转移策略的默认内容。对于主用/主用模式，您可以设置每个故障转移组的大多数条件。

准备工作

在多情景模式中，可在系统执行空间中配置这些设置。

操作步骤

步骤 1　更改设备的轮询和保持时间：

在主用/主用模式中，您可以为系统设置此速率；您不能为每个故障转移组设置此速率。

您输入的保持时间值不得短于设备轮询时间的 3 倍。轮询时间越短，ASA 就可以越快地检测到故障和触发故障转移。然而，网络临时拥塞时，更快的检测会导致不必要的切换。

如果设备在一个轮询周期内未收到故障转移通信的 Hello 数据包，则会通过其余接口进行其他的测试。如果在保持时间内，仍未收到来自对等设备的响应，该设备会被视为发生故障，如果故障设备为主用设备，则备用设备会进行接管，成为主用设备。

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

示例：

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

步骤 2　以每秒连接数为单位设置 HTTP 复制速率：

设置介于 8341 和 50000 之间的速率。默认值为 50000。在主用/主用模式中，您可以为系统设置此速率；您不能为每个故障转移组设置此速率。

failover replication rate *conns*

示例：

```
ciscoasa(config)# failover replication rate 20000
```

步骤 3　（仅主用/主用模式）指定您想要自定义的故障转移组：

failover group {**1** | **2**}

示例：

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

步骤 4　（仅主用/主用模式）为故障转移组 1 配置故障转移抢占：

preempt [*delay*]

示例：

```
ciscoasa(config-fover-group)# preempt 1200
```

如果一台设备在另一台设备之前启动，则两个故障转移组都会在该设备上变为主用状态，而无论主设备或辅助设置如何。当指定设备变得可用时，此命令会使故障转移组自动在该设备上变为主用状态。

您可以输入可选的 *delay* 值，该值指定故障转移组在指定设备上自动变为主用状态之前，在当前设备上保持主用状态的秒数。有效值范围为 1 至 1200。

如果启用有状态故障转移，抢占将延迟，直到从故障转移组当前处于主用状态的设备复制连接。

步骤 5　启用 HTTP 状态复制：

- 对于主用/备用模式：

  failover replication http

- 对于主用/主用模式：

  replication http

如要允许在状态信息复制中包含 HTTP 连接，您需要启用 HTTP 复制。由于 HTTP 连接通常是短期的，并且因为 HTTP 客户端通常会重试失败的连接尝试，HTTP 连接不会自动包含在复制的状态信息中。

步骤 6　设置接口发生故障时的故障转移阈值：

- 对于主用/备用模式：

  failover interface-policy *num*[%]

  示例：

  ```
  ciscoasa (config)# failover interface-policy 20%
  ```

- 对于主用/主用模式：

  interface-policy *num*[%]

  示例：

  ```
  ciscoasa(config-fover-group)# interface-policy 20%
  ```

默认情况下，一个接口故障将导致故障转移。

指定特定接口数时，*num* 参数可以介于 1 和 250 之间。

指定接口百分比时，*num* 参数可以介于 1 和 100 之间。

步骤 7　更改接口的轮询和保持时间：

- 对于主用/备用模式：

  failover polltime interface [**msec**] *time* [**holdtime** *time*]

  示例：

  ```
  ciscoasa(config)# failover polltime interface msec 500 holdtime 5
  ```

- 对于主用/主用模式：

  polltime interface [**msec**] *time* [**holdtime** *time*]

  示例：

  ```
  ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
  ```

轮询时间的有效值介于 1 和 15 秒之间，或者如果使用了可选的 **msec** 关键字，从 500 至 999 毫秒。保持时间确定，从一个 Hello 数据包丢失，到将接口标记为发生故障的时长。保持时间的有效值范围为 5 到 75 秒。您输入的保持时间不得短于设备轮询时间的 5 倍。

如果接口链路关闭，则不会执行接口测试，如果发生故障的接口数达到或超出配置的故障转移条件，备用设备可能在仅一个接口轮询周期内就会变为主用状态。

步骤 8　配置接口的虚拟 MAC 地址：

- 对于主用/备用模式：

  failover mac address *phy_if active_mac standby_mac*

  示例：

  ```
  ciscoasa(config)# failover mac address gigabitethernet0/2 00a0.c969.87c8
  00a0.c918.95d8
  ```

- 对于主用/主用模式：

  mac address *phy_if active_mac standby_mac*

  示例：

  ```
  ciscoasa(config-fover-group)# mac address gigabitethernet0/2 00a0.c969.87c8
  00a0.c918.95d8
  ```

phy_if 参数是接口的物理名称，例如， gigabitethernet0/1。

active_mac 和 *standby_mac* 参数是 H.H.H 格式的 MAC 地址，其中 H 是 16 位十六进制数字。例如，MAC 地址 00-0C-F1-42-4C-DE 应以 000C.F142.4CDE 的形式输入。

该 *active_mac* 地址与接口的主用 IP 地址关联，而 *standby_mac* 与接口的备用 IP 地址关联。

您还可以使用其他命令或方法设置 MAC 地址，但是，我们建议仅使用一种方法。如果您使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。

使用 **show interface** 命令可以显示接口使用的 MAC 地址。

步骤 9　（仅主用/主用模式）视需要为其他故障转移组，重复此操作步骤。

配置接口监控

默认情况下，会在所有物理接口或 （对于 ASASM）所有 VLAN 接口以及在 ASA 上安装的所有硬件模块上启用监控。您可能希望排除连接到非关键网络的接口，以免影响故障转移策略。

准备工作

- 您可以监控一台设备上的最多 250 个接口 （跨多情景模式中的所有情景）。
- 在多情景模式中，请在每个情景中配置接口。

操作步骤

步骤 1　启用或禁用接口运行状况监控：

[**no**] **monitor-interface** {*if_name* | **service-module**}

示例：

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)# no monitor-interface eng1
```

如果您不希望硬件模块故障 （如 ASA FirePOWER 模块）触发故障转移，则可使用 **no monitor-interface service-module** 命令禁用模块监控。

配置非对称路由数据包支持 （主用/主用模式）

在主用/主用故障转移下运行时，设备可能会收到其对等设备发起的连接的一个返回数据包。由于收到该数据包的 ASA 没有该数据包的任何连接信息，该数据包会被丢弃。主用/主用故障转移对中的两台 ASA 连接到不同的服务提供商，并且出站连接不使用 NAT 地址时，最常发生此丢弃。

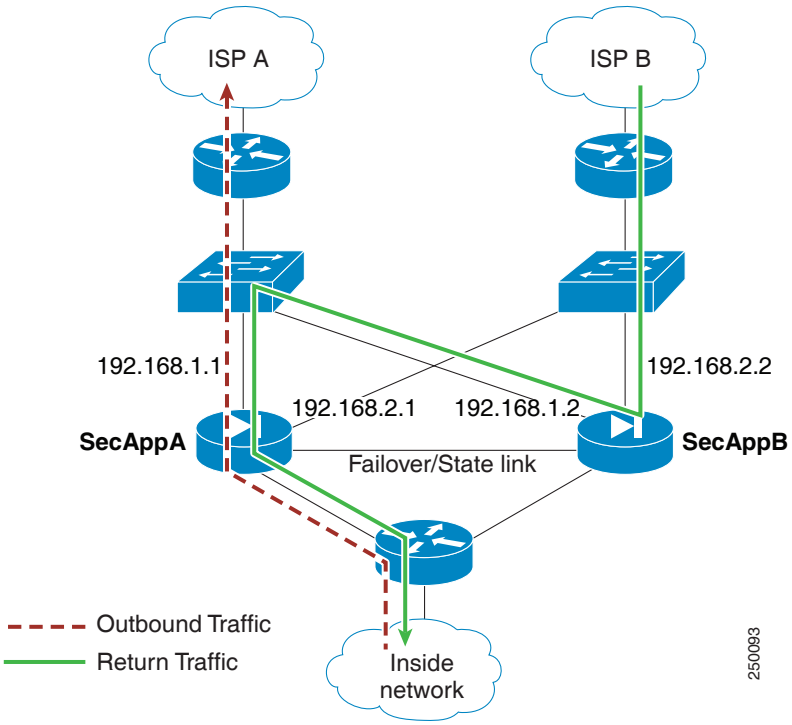
您可以通过允许非对称路由数据包来防止返回数据包。为此，您需要将每台 ASA 上的相似接口分配到同一个 ASR 组。例如，两台 ASA 的内部接口连接到内部网络，但外部接口连接到不同的 ISP。在主设备上，将主用情景外部接口分配给 ASR 组 1；在辅助设备上，将主用情景外部接口分配给相同 ASR 组 1。当主设备外部接口收到到没有其会话信息的数据包时，它会检查相同组中处于备用情景中的另一接口的会话信息；在此示例中，即 ASR 组 1。如果它没有找到匹配项，数据包将会被丢弃。如果它找到匹配项，则会进行以下的操作：

- 如果传入流量来自对等设备，第 2 层标头的部分或全部内容将会被重写，数据包将会被重定向到另一设备。一旦会话处于活动状态，此重定向将会继续。
- 如果传入流量来自相同设备上的不同接口，第 2 层标头的部分或全部内容将会被重写，数据包将会被重新注入数据流。

注　此功能不提供非对称路由；它会将非对称路由数据包还原至正确接口。

图 7-13 展示了一个非对称路由数据包的示例。

图 7-13　　ASR 示例



1. 出站会话使用主用 SecAppA 情景通过 ASA。该会话退出接口 outsideISP-A (192.168.1.1)。
2. 由于上游某处配置了非对称路由，返回流量使用主用 SecAppA 情景通过 ASA 上的接口 outsideISP-B (192.168.2.2) 传回。
3. 由于没有接口 192.168.2.2 上的流量的会话信息，返回流量通常会被丢弃。但是，此接口被配置为 ASR 组 1 的一部分。设备会在配置为相同的 ASR 组 ID 的所有其他接口上查找该会话。
4. 会话信息会在接口 outsideISP-A (192.168.1.2) 上找到，该接口在使用 SecAppB 情景的设备上处于备用状态。有状态故障转移会将会话信息从 SecAppA 复制到 SecAppB。
5. 第 2 层标头会使用接口 192.168.1.1 的信息重写，流量会被重定向，通过接口 192.168.1.2，在该接口上，流量随后会通过设备上的来源接口 （SecAppA 上的 192.168.1.1）返回，而不是将流量丢弃。此转发会视需要继续，直到会话结束。

先决条件

- 有状态故障转移 - 将主用故障转移组中的接口上的会话的状态信息，传送给备用故障转移组。
- 复制 HTTP - HTTP 会话状态信息不会传送给备用故障转移组，因此不存在于备用接口上。为了使 ASA 能够重新路由非对称路由的 HTTP 数据包，您需要复制 HTTP 状态信息。
- 请在主设备和辅助设备上的每个主用情景中，执行此操作步骤。

详细步骤

	命令	用途
步骤 1	在主设备上： **interface** *phy_if* **示例：** `primary/admin(config)# interface gigabitethernet 0/0`	在主设备上，指定要允许非对称路由数据包的接口。
步骤 2	**asr-group** *num* **示例：** `primary/admin(config-ifc)# asr-group 1`	设置接口的 ASR 组编号。*num* 的有效值范围为 1 至 32。
步骤 3	在辅助设备上： **interface** *phy_if* **示例：** `secondary/ctx1(config)# interface gigabitethernet 0/1`	在辅助设备上，指定要允许非对称路由数据包的类似接口。
步骤 4	**asr-group** *num* **示例：** `secondary/ctx1(config-ifc)# asr-group 1`	设置接口的 ASR 组编号，以便与主设备接口匹配。

示例

两台设备具有以下配置（配置仅显示相关命令）。图中标记为 SecAppA 的设备是故障转移对中的主设备。

示例 7-1　　主设备系统配置

```
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
interface GigabitEthernet0/2
  no shutdown
interface GigabitEthernet0/3
  no shutdown
interface GigabitEthernet0/4
  no shutdown
interface GigabitEthernet0/5
  no shutdown
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/1
failover link folink
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
  primary
failover group 2
  secondary
admin-context SecAppA
context admin
  allocate-interface GigabitEthernet0/2
  allocate-interface GigabitEthernet0/3
```

```
  config-url flash:/admin.cfg
  join-failover-group 1
context SecAppB
  allocate-interface GigabitEthernet0/4
  allocate-interface GigabitEthernet0/5
  config-url flash:/ctx1.cfg
  join-failover-group 2
```

示例 7-2　SecAppA Context Configuration

```
interface GigabitEthernet0/2
  nameif outsideISP-A
  security-level 0
  ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  asr-group 1
interface GigabitEthernet0/3
  nameif inside
  security-level 100
  ip address 10.1.0.1 255.255.255.0 standby 10.1.0.11
monitor-interface outside
```

示例 7-3　SecAppB Context Configuration

```
interface GigabitEthernet0/4
  nameif outsideISP-B
  security-level 0
  ip address 192.168.2.2 255.255.255.0 standby 192.168.2.1
  asr-group 1
interface GigabitEthernet0/5
  nameif inside
  security-level 100
  ip address 10.2.20.1 255.255.255.0 standby 10.2.20.11
```

管理故障转移

- 第 7-38 页的强制故障转移
- 第 7-39 页的禁用故障转移
- 第 7-40 页的还原故障设备
- 第 7-40 页的重新同步配置
- 第 7-40 页的测试故障转移功能

强制故障转移

如要强制要求备用设备成为主用设备，请执行以下操作步骤。

先决条件

在多情景模式中，请在系统执行空间中执行此操作步骤。

详细步骤

命令	用途
对于备用设备上的主用/备用模式： **failover active** 对于备用设备上的主用/主用模式： **failover active** [**group** *group_id*] **示例：** `standby# failover active` 或： `standby# failover active group 1`	在*备用*设备上输入时，可以强制故障转移。备用设备将成为主用设备。 如果您指定 **group** *group_id*，则在指定主用/主用故障转移组的*备用*设备上输入此命令时，将强制进行故障转移。备用设备将变为故障转移组的主用设备。
对于主用设备上的主用/备用模式： **no failover active** 对于主用设备上的主用/主用模式： **no failover active** [**group** *group_id*] **示例：** `active# no failover active` 或： `active# no failover active group 1`	在*主用*设备上输入时，可以强制故障转移。主用设备将成为备用设备。 如果您指定 **group** *group_id*，则在指定故障转移组的*主用*设备上输入此命令时，将强制进行故障转移。主用设备将成为故障转移组的备用设备。

禁用故障转移

如要禁用故障转移，请执行以下操作步骤。

先决条件

在多情景模式中，请在系统执行空间中执行此操作步骤。

详细步骤

命令	用途
no failover **示例：** `ciscoasa(config)# no failover`	禁用故障转移。 在一个主用/备用对上禁用故障转移，将会导致每台设备保持其主用和备用状态，直到您重新加载。例如，备用设备保持处于备用模式，因此两台设备都会不开始传送流量。如要使备用设备变为主用状态（即使在禁用故障转移的情况下），请参阅第 7-38 页的强制故障转移。 在主用/主用故障转移对上禁用故障转移，将会导致故障转移组在其处于主用状态的设备上保持主用状态，而无论它们被配置为首选哪一设备。

还原故障设备

如要将故障设备还原到无故障状态，请执行以下操作步骤。

先决条件

在多情景模式中，请在系统执行空间中执行此操作步骤。

详细步骤

命令	用途
对于主用/备用模式： **failover reset** 对于主用/主用模式： **failover reset** [**group** *group_id*] **示例：** `ciscoasa(config)# failover reset` 或： `ciscoasa(config)# failover reset group 1`	将故障设备还原到无故障状态。将故障设备还原到无故障状态，不会自动使其成为主用设备；还原后的设备将保持处于备用状态，直到故障转移（强制或自然）使其变为主用状态。一个例外是，配置了故障转移抢占的故障转移组（仅主用/主用模式）。如果故障转移组之前处于主用状态且配置了抢占，并且它是在首选设备上发生故障的，则该故障转移组将变为主用状态。 如果您指定 **group** *group_id*，此命令会将发生故障的主用/主用故障转移组，还原到无故障状态。

重新同步配置

如果在主用设备上输入 **write standby** 命令，备用设备将清除其运行配置 （用于与主用设备进行通信的故障转移命令除外），并且，主用设备会将其完整配置发送到备用设备。

对于多情景模式，当您在系统执行空间中输入 **write standby** 命令时，系统将复制所有情景。如果在情景中输入 **write standby** 命令，该命令只会复制该情景配置。

复制命令会被存储在运行配置中。

测试故障转移功能

如要测试故障转移功能，请执行以下操作步骤。

详细步骤

步骤 1　测试您的主用设备是否在通过使用 FTP （例如）来在不同接口上的主机之间发送文件，从而如预期传送流量。

步骤 2　在主用设备上输入以下命令，从而强制进行故障转移：

主用/备用模式：

```
ciscoasa(config)# no failover active
```

主用/主用模式：

```
ciscoasa(config)# no failover active group group_id
```

步骤 3　使用 FTP 在相同的两台主机之间发送另一个文件。

步骤 4　如果测试不成功，请输入 **show failover** 命令检查故障转移状态。

步骤 5　完成后，您可以在新的主用设备上输入以下命令，从而将设备还原到主用状态：

主用/备用模式：

```
ciscoasa(config)# no failover active
```

主用/主用模式：

```
ciscoasa(config)# failover active group group_id
```

注　当 ASA 接口发生故障时，对于故障转移而言，仍然会将其视为设备问题。如果 ASA 检测到接口发生故障，将立即进行故障转移，而无需在接口保持时间内进行等待。仅当 ASA 认为接口状态良好（尽管其未收到对等设备的 Hello 数据包）的情况下，接口保持时间才有用。要模拟接口保持时间，请关闭交换机上的 VLAN，以阻止对等设备收到彼此的 Hello 数据包。

远程命令执行

远程命令执行允许您将在命令行输入的命令发送到特定的故障转移对等设备。

- 第 7-41 页的发送命令
- 第 7-42 页的更改命令模式
- 第 7-42 页的安全注意事项
- 第 7-43 页的远程命令执行的限制

发送命令

由于配置命令从主用设备或情景复制到备用设备或情景，您可以使用 **failover exec** 命令在正确的设备上输入配置命令，而无论您登录的是哪一设备。例如，如果您登录到备用设备，您可以使用 **failover exec active** 命令将配置更改发送到主用设备。这些更改随后会被复制到备用设备。请勿使用 **failover exec** 命令将配置命令发送到备用设备或情景；这些配置更改不会复制到主用设备，并且两个配置将不再同步。

configuration、exec 和 **show** 命令的输出会显示在当前终端会话中，因此您可以使用 **failover exec** 命令在对等设备上发出 **show** 命令并在当前终端中查看结果。

要在对等设备上执行该命令，您必须具有在本地设备上执行命令的足够权限。

详细步骤

步骤 1　如果您处于多情景模式，请使用 **changeto context** *name* 命令更改要配置的情景。您无法使用 **failover exec** 命令更改故障转移对等设备上的情景。

步骤 2　使用以下命令，将命令发送到指定的故障转移设备：

```
ciscoasa(config)# failover exec {active | mate | standby}
```

使用 **active** 或 **standby** 关键字在指定设备上执行命令，即使该设备为当前设备。使用 **mate** 关键字，以便在故障转移对等设备上执行命令。

导致命令模式更改的命令不会更改当前会话的提示符。您必须使用 **show failover exec** 命令来显示在其中执行命令的命令模式。有关详细信息，请参阅第 7-42 页的更改命令模式。

更改命令模式

failover exec 命令会保持独立于您的终端会话命令模式的命令模式状态。默认情况下，**failover exec** 命令在指定设备的全局配置模式中启动。您可以通过使用 **failover exec** 命令发送适当命令（例如 **interface** 命令）来更改该命令模式。当您使用 **failover exec** 更改模式时，会话提示符不会更改。

例如，如果您登录到故障转移对的主用设备的全局配置模式，然后使用 **failover exec active** 命令切换到接口配置模式，终端提示符将保持处于全局配置模式，但使用 **failover exec** 输入的命令在接口配置模式中输入。

以下示例展示了终端会话模式和 **failover exec** 命令模式之间的差异。在此示例中，管理员将主用设备上的 **failover exec** 模式更改为 GigabitEthernet0/1 接口的接口配置模式。之后，使用 **failover exec active** 输入的所有命令将发送到 GigabitEthernet0/1 接口的接口配置模式。然后，管理员使用 failover exec active 为该接口分配 IP 地址。虽然提示符表明处于全局配置模式， **failover exec active** 模式实际上处于接口配置模式。

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# failover exec active ip address 192.168.1.1 255.255.255.0 standby
192.168.1.2
ciscoasa(config)# router rip
ciscoasa(config-router)#
```

更改您当前与设备进行的会话的命令模式，不会影响 **failover exec** 命令使用的命令模式。例如，如果您在主用设备上处于接口配置模式，并且您未更改 **failover exec** 命令模式，以下命令将在全局配置模式中执行。结果是您与设备的会话将保持处于接口配置模式，而使用 **failover exec active** 输入的命令将发送到指定的路由进程的路由器配置模式。

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

使用 **show failover exec** 命令显示指定设备上的命令模式，使用 **failover exec** 命令发送的命令是在该命令模式中执行的。 **show failover exec** 命令接受与 **failover exec** 命令相同的关键字：**active**、**mate** 或 **standby**。系统将单独跟踪每台设备的 **failover exec** 模式。

例如，以下内容是在备用设备上输入的 **show failover exec** 命令的示例输出：

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# sh failover exec active
主用设备的 Failover EXEC 处于接口子命令模式

ciscoasa(config)# sh failover exec standby
备用设备 Failover EXEC 处于 config 模式

ciscoasa(config)# sh failover exec mate
主用设备的 Failover EXEC 处于接口子命令模式
```

安全注意事项

failover exec 命令使用故障转移链路来向对等设备发送命令，并中接收命令执行的输出。您应该在故障转移链路上启用加密，以防止窃听或中间人攻击。

远程命令执行的限制

当您使用远程命令时，会面临以下限制：

- 如果您使用零停机时间升级操作步骤来升级一台设备，并且不升级另一设备，两台设备必须都运行支持 **failover exec** 命令的软件，以便该命令能够工作。
- 命令补全和情景帮助不适用于 *cmd_string* 参数中的命令。
- 在多情景模式中，您只能将命令发送到对等设备上的对等情景。如要将命令发送到不同情景，您必须在所登录的设备上切换到该情景。
- 您不能将以下命令与 **failover exec** 命令配合使用：
  - **changeto**
  - **debug** (**undebug**)
- 如果备用设备处于故障状态，并且故障是由服务卡故障导致，则它仍然可以收到 **failover exe** 命令发送的命令；否则，远程命令执行将失败。
- 您无法使用 **failover exec** 命令从特权执行模式切换到故障转移对等设备上的全局配置模式。例如，如果当前设备处于特权执行模式，并且您输入 **failover exec mate configure terminal**，**show failover exec mate** 的输出将会显示 failover exec 会话处于全局配置模式。然而，使用 **failover exec** 为对等设备输入的配置命令将失败，直到您在当前设备上进入全局配置模式。
- 您不能输入递归的 failover exec 命令，如 **failover exec mate failover exec mate** 命令。
- 要求用户输入或确认的命令必须使用 **/nonconfirm** 选项。

监控故障转移

- 第 7-43 页的故障转移消息
- 第 7-44 页的监控故障转移

故障转移消息

发生故障转移时，两台 ASA 都会发送系统消息。

- 第 7-43 页的故障转移系统日志消息
- 第 7-44 页的故障转移调试消息
- 第 7-44 页的 SNMP 故障转移陷阱

故障转移系统日志消息

ASA 发出一系列与优先级为 2 的故障转移有关的系统日志消息，指示一个严重情况。如要查看这些信息，请参阅 《系统日志消息指南》。如要启用记录，请参阅第 39 章，“日志记录”

注　在故障转移期间，故障转移会在逻辑上关闭然后打开接口，生成系统日志消息 411001 和 411002。这是正常活动。

故障转移调试消息

如要查看调试消息，请输入 **debug fover** 命令。有关详细信息，请参阅 《命令参考》。

注　由于调试输出在 CPU 进程中分配的高优先级，它可能极大地影响系统性能。为此，请仅使用 **debug fover** 命令来针对特定问题进行故障排除，或在与思科 TAC 的故障排除会话中使用该命令。

SNMP 故障转移陷阱

如要接收故障转移的 SNMP 系统日志陷阱，请配置 SNMP 代理发送 SNMP 陷阱到 SNMP 管理站、定义系统日志主机，并将思科系统日志 MIB 汇集到 SNMP 管理站中。有关详细信息，请参阅第 40 章，“SNMP”。

监控故障转移

如要监控故障转移，请输入以下命令之一：

命令	用途
`show failover`	显示有关设备的故障转移状态的信息。
`show failover group`	显示有关故障转移组的故障转移状态的信息。显示的信息类似于 **show failover** 命令的输出，但仅限于指定的组。
`show monitor-interface`	显示有关受监控的接口的信息。
`show running-config failover`	显示运行配置中的故障转移命令。

有关监控命令输出的详细信息，请参阅 《命令参考》。

故障转移功能历史记录

表 7-4 列出了此功能的版本历史记录。

表 7-4　可选主用/备用故障转移设置的功能历史记录

功能名称	版本	功能信息
主用/备用故障转移	7.0(1)	引入此功能。
主用/主用故障转移	7.0(1)	引入此功能。
故障转移密钥支持使用十六进制值	7.0(4)	现在您可以指定十六进制值用于故障转移链路加密。 我们修改了以下命令：**failover key hex**。

表 7-4　　可选主用/备用故障转移设置的功能历史记录（续）

功能名称	版本	功能信息
支持故障转移密钥的主密码	8.3(1)	故障转移密钥现在支持主密码，该密码用于加密运行配置和启动配置中的共享密钥。如果您要将共享密钥从一台 ASA 复制到另一台（例如，通过 **more system:running-config** 命令），您可以成功复制并粘贴加密的共享密钥。 **注**　**failover key** 共享机密在 **show running-config** 输出中显示为 *****；此已屏蔽的密钥不可复制。 我们修改了以下命令：**failover key [0 | 8]**。
添加了故障转移的 IPv6 支持。	8.2(2)	我们修改了以下命令：**failover interface ip**、 **show failover**、 **ipv6 address**、 **show monitor-interface**。
支持 IPsec LAN 对 LAN 隧道加密故障转移和状态链路通信。	9.1(2)	您现在可以将 IPsec LAN 对 LAN 隧道用于故障转移和状态链路加密，而不是对故障转移密钥使用专有加密（**failover key** 命令）。 **注**　故障转移 LAN 对 LAN 隧道不计入 IPsec（其他 VPN）许可证。 我们引入或修改了以下命令：**failover ipsec pre-shared-key**、 **show vpn-sessiondb**。
禁用硬件模块的运行状况监控	9.3(1)	默认情况下，ASA 监控已安装的硬件模块（例如 ASA FirePOWER 模块）的运行状况。如果您不希望硬件模块故障触发故障转移，可以禁用模块监控。 我们修改了以下命令：**monitor-interface service-module**

ASA 集群

通过集群，可以将多台 ASA 组合成一个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。

注 使用集群时，有些功能不受支持。请参阅第 8-22 页的集群不支持的功能。

- 第 8-1 页的关于 ASA 集群
- 第 8-28 页的 ASA 集群的许可
- 第 8-28 页的 ASA 集群的先决条件
- 第 8-29 页的 ASA 集群的指导原则
- 第 8-33 页的 ASA 集群的默认设置
- 第 8-33 页的配置 ASA 集群
- 第 8-48 页的管理 ASA 集群成员
- 第 8-52 页的监控 ASA 集群
- 第 8-57 页的 ASA 集群示例
- 第 8-70 页的 ASA 集群的历史记录

关于 ASA 集群

本节介绍集群架构及其工作原理。

- 第 8-2 页的 ASA 集群如何融入网络中
- 第 8-2 页的性能换算系数
- 第 8-2 页的集群成员
- 第 8-3 页的集群接口
- 第 8-5 页的集群控制链路
- 第 8-8 页的 ASA 集群中的高可用性
- 第 8-9 页的配置复制
- 第 8-10 页的 ASA 集群管理
- 第 8-11 页的负载均衡方法
- 第 8-16 页的站点间集群

- 第 8-19 页的 ASA 集群如何管理连接
- 第 8-21 页的 ASA 功能和集群

ASA 集群如何融入网络中

集群包含多台 ASA，作为单一设备工作。如要用作集群，ASA 需要以下基础设施：

- 独立的高速背板网络，称为*集群控制链路*，用于集群内的通信。
- 对每台 ASA 的管理访问权限，用于进行配置和监控。

将集群接入网络中时，上游和下游路由器需要能够使用以下方法之一使出入集群的数据实现负载均衡：

- 跨网络 EtherChannel（推荐）- 将多个集群成员上的接口分组为一个 EtherChannel；EtherChannel 在设备之间执行负载均衡。
- 基于策略的路由（仅适用于路由防火墙模式）- 上游和下游路由器使用路由映射和 ACL 在设备之间执行负载均衡。
- 等价多路径路由（仅适用于路由防火墙模式）- 上游和下游路由器使用等价静态或动态路由在设备之间执行负载均衡。

相关主题

- 第 8-28 页的 ASA 集群的许可
- 第 8-5 页的集群控制链路
- 第 8-10 页的 ASA 集群管理
- 第 8-11 页的跨网络 EtherChannel（推荐）
- 第 8-15 页的基于策略的路由（仅适用于路由防火墙模式）
- 第 8-16 页的等价多路径路由（仅适用于路由防火墙模式）

性能换算系数

将多台设备组成一个集群时，预计可以达到近似如下的性能：

- 合并吞吐量的 70%
- 最大连接数的 60%
- 每秒连接数的 50%

以吞吐量为例，带 SSP-40 的 ASA 5585-X 在单独运行时大约可处理 10 Gbps 的实际防火墙流量。因此，由 8 台设备组成的集群的最大合并吞吐量约为 80 Gbps （8 台设备 x 10 Gbps）的 70%：56 Gbps。

集群成员

集群成员共同作用来实现安全策略和流量的共享。本节介绍每种成员角色的性质。

- 第 8-3 页的引导程序配置
- 第 8-3 页的主设备和从设备角色
- 第 8-3 页的主设备选举

引导程序配置

您要在每台设备上配置最低的引导程序配置，包括集群名称、集群控制链路接口和其他集群设置。第一台启用集群的设备通常会成为*主*设备。在后续设备上启用集群时，这些设备将作为*从*设备加入集群。

主设备和从设备角色

集群的一个成员是主设备。主设备由引导程序配置中的优先级设置决定；优先级可设置为 1 到 100，其中 1 为最高优先级。所有其他成员都是从设备。通常，在首次创建集群时，添加的第一台设备将成为主设备，只因为它是集群中当时唯一的设备。

必须仅在主设备上执行所有配置 （除引导程序配置之外）；随后，配置将被复制到从设备。如果是接口等物理资产，主设备的配置将被镜像到所有从设备。例如，如果将 GigabitEthernet 0/1 配置为内部接口并将 GigabitEthernet 0/0 配置为外部接口，则从设备上也会将这些接口用作内部和外部接口。

有些功能在集群中无法扩展，主设备将处理这些功能的所有流量。

相关主题

- 第 8-22 页的集群的集中功能

主设备选举

集群成员通过集群控制链路通信，如下选举主设备：

1. 为设备启用集群时 （或已经启用集群的设备首次启动时），设备将每 3 秒广播一次选举请求。
2. 优先级较高的其他所有设备将响应选举请求；优先级可设置为 1 到 100，其中 1 为最高优先级。
3. 如果在 45 秒后设备没有收到优先级更高的其他设备的响应，则该设备将成为主设备。

   注　如果有多台设备并列最高优先级，则先使用集群设备名称、再使用序列号来确定主设备。

4. 如果稍后有优先级更高的设备加入集群，该设备不会自动成为主设备；现有主设备将一直作为主设备，除非它停止响应，届时将选举新的主设备。

注　您可以手动强制一台设备成为主设备。对集中功能而言，如果强制更改主设备，则所有连接都将断开，而您必须在新的主设备上重新建立连接。

相关主题

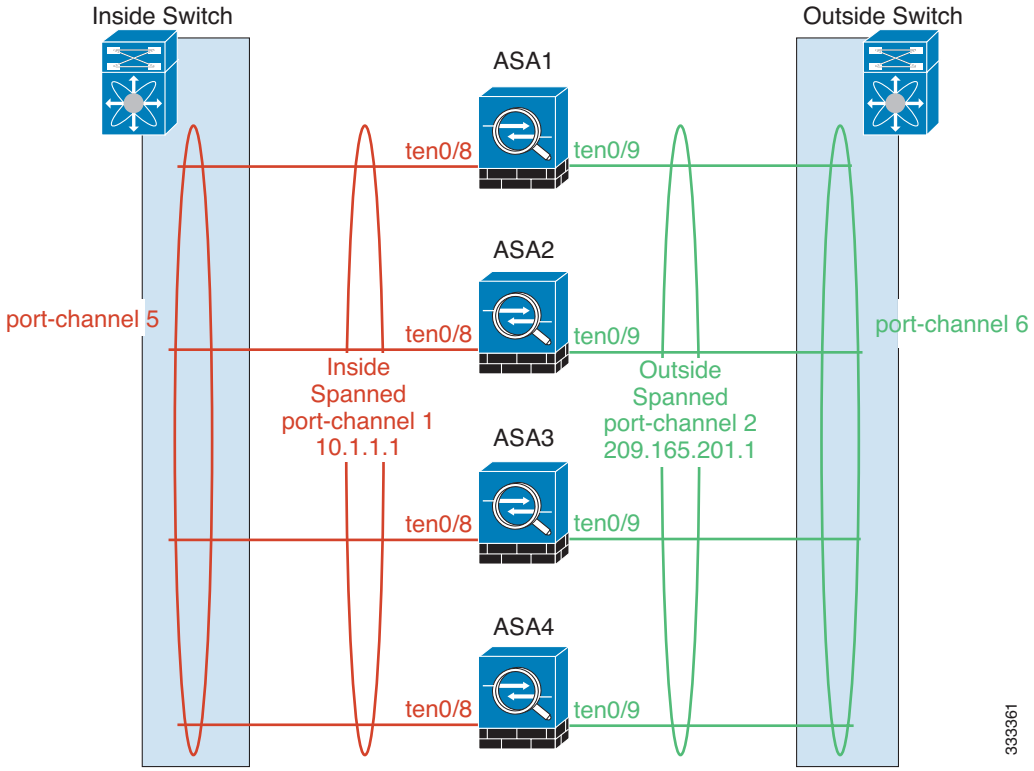
- 第 8-22 页的集群的集中功能

集群接口

可以将数据接口配置为跨网络 EtherChannel 或独立接口。集群中的所有数据接口只能是一种类型。

跨网络 EtherChannel（推荐）

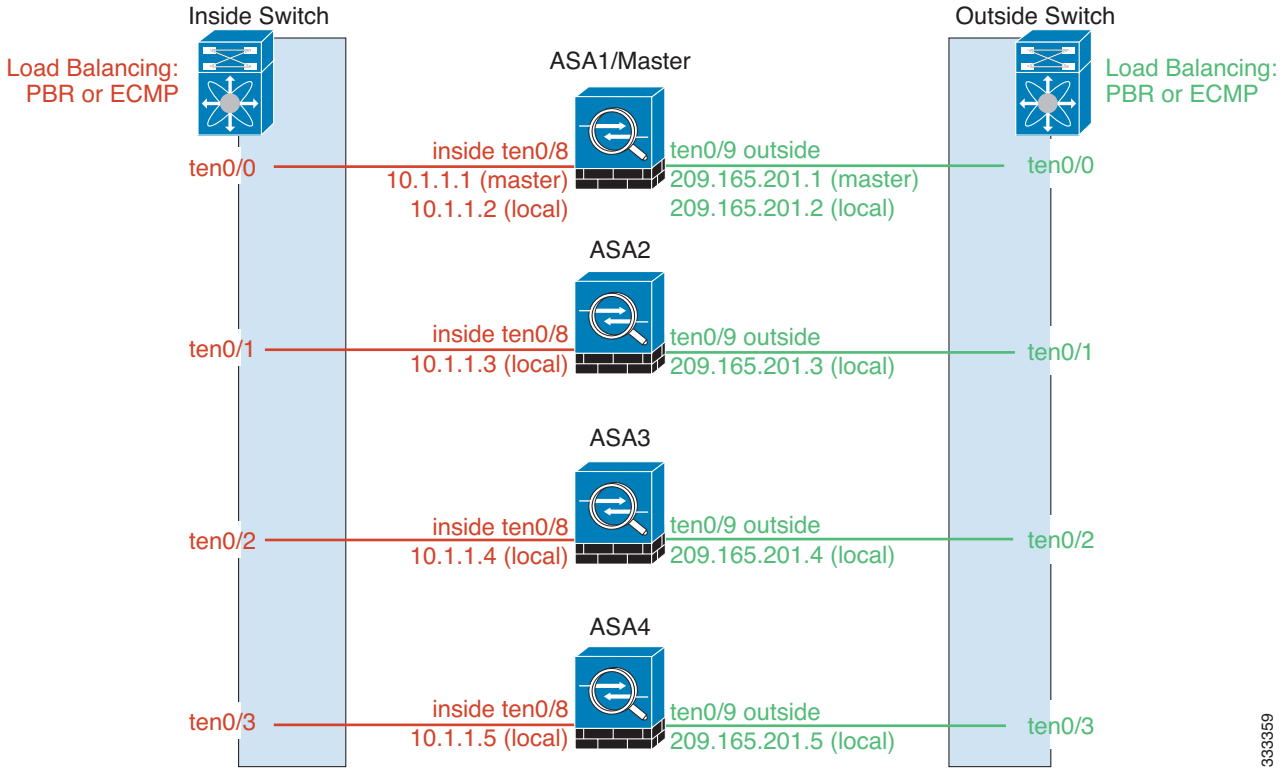
您可以将每台设备的一个或多个接口分组为跨集群中所有设备的 EtherChannel。EtherChannel 汇聚信道中所有可用活动接口上的流量。在路由模式和透明防火墙模式中都可以配置跨网络 EtherChannel。在路由模式中，EtherChannel 被配置为只有一个 IP 地址的路由接口。在透明模式中，IP 地址被分配到网桥组而非接口。负载均衡属于 EtherChannel 固有的基本操作。



独立接口 （仅适用于路由防火墙模式）

独立接口是正常的路由接口，每个接口都有自己的*本地 IP 地址*。由于接口配置只能在主设备上配置，因此，您可以通过接口配置设置一个 IP 地址池，供集群成员上的给定接口 （包括主设备上的一个接口）使用。集群的*主集群 IP 地址*是集群的固定地址，始终属于当前的主设备。主集群 IP 地址是主设备的辅助 IP 地址；本地 IP 地址始终是用于路由的主要地址。主集群 IP 地址提供对地址的统一管理访问；当主设备更改时，主集群 IP 地址将转移到新的主设备，使集群的管理得以无缝继续。不过，在此情况下必须在上游交换机上分别配置负载均衡。

注　我们建议使用跨网络 EtherChannel 而不要使用独立接口，因为独立接口依靠路由协议来实现流量的负载均衡，而路由协议在链路发生故障时通常收敛速度缓慢。



相关主题

- 第 8-11 页的负载均衡方法

集群控制链路

每台设备至少必须将一个硬件接口专门用作集群控制链路。

- 第 8-5 页的集群控制链路流量概述
- 第 8-6 页的集群控制链路接口和网络
- 第 8-6 页的调整集群控制链路的吞吐量大小
- 第 8-7 页的集群控制链路冗余
- 第 8-7 页的集群控制链路可靠性
- 第 8-7 页的集群控制链路故障

集群控制链路流量概述

集群控制链路流量包括控制流量和数据流量。

控制流量包括：

- 主设备选举。
- 配置复制。
- 运行状况监控。

数据流量包括：

- 状态复制。
- 连接所有权查询和数据包转发。

相关主题

- 第 8-2 页的集群成员
- 第 8-9 页的配置复制
- 第 8-8 页的设备运行状况监控
- 第 8-9 页的数据路径连接状态复制
- 第 8-21 页的在集群中再均衡新的 TCP 连接

集群控制链路接口和网络

您可以将任何数据接口用于集群控制链路，但以下情况除外：

- VLAN 子接口不能用作集群控制链路。
- 管理 *x/x* 接口 （无论是作为独立接口还是作为 EtherChannel），都不能用作集群控制链路。
- 对于带 ASA IPS 模块的 ASA 5585-X，不能将模块接口用于集群控制链路；不过，可以使用 ASA 5585-X 网络模块上的接口。

可以使用 EtherChannel 或冗余接口。

如果带 SSP-10 和 SSP-20 的 ASA 5585-X 包含两个万兆以太网接口，建议将一个接口用于集群控制链路，另一个用于数据 （可将子接口用于数据）。尽管此设置无法满足集群控制链路的冗余要求，但可以满足调整集群控制链路使之符合数据接口流量大小的需要。

每条集群控制链路都有一个属于同一子网的 IP 地址。此子网应该与所有其他流量隔离，并且只包括 ASA 集群控制链路接口。

对于有 2 个成员的集群，请勿将集群控制链路从一台 ASA 直接连接到另一台 ASA。如果直接连接两个接口，则当一台设备发生故障时，集群控制链路失效，会导致剩下的那台正常设备也发生故障。而如果通过交换机连接集群控制链路，则集群控制链路仍会对正常设备打开。

相关主题

- 第 8-7 页的集群控制链路冗余
- 第 8-6 页的调整集群控制链路的吞吐量大小

调整集群控制链路的吞吐量大小

您应当调整集群控制链路的吞吐量大小，使之符合每个成员的预期吞吐量。例如，如果使用带 SSP-60 的 ASA 5585-X，集群中每台设备最多可传输 14 Gbps 的流量，则您也应该将接口分配到至少可传输 14 Gbps 流量的集群控制链路。在此情况下，可以将 EtherChannel 中的 2 个万兆以太网接口用于集群控制链路，并将其余接口根据需要用于数据链路。

集群控制链路流量主要由状态更新和转发的数据包组成。集群控制链路在任一给定时间的流量大小不尽相同。例如，如果经过的流量完全由持续时间极短的 TCP 连接组成，则状态更新在经过的流量中所占的比例可能高达 10%。转发流量的大小取决于负载均衡的功效或是否存在大量用于集中功能的流量。例如：

- NAT 会使连接的负载均衡不佳，需要对所有返回流量进行再均衡，将其转发到正确的设备。
- 用于网络访问的 AAA 是集中功能，因此所有流量都会转发到主设备。
- 当成员身份更改时，集群需要对大量连接进行再均衡，因此会暂时耗用大量集群控制链路带宽。

带宽较高的集群控制链路可以帮助集群在发生成员身份更改时更快地收敛，并防止出现吞吐量瓶颈。

注　如果集群中存在大量非对称 （再均衡）流量，应增加集群控制链路的吞吐量大小。

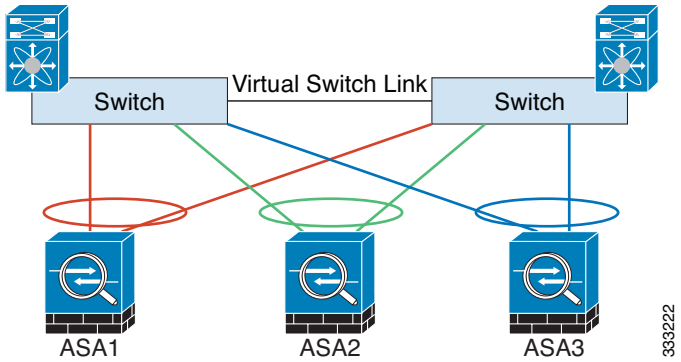
相关主题

- 第 8-16 页的站点间集群。

集群控制链路冗余

我们建议将 EtherChannel 用于集群控制链路，以便在 EtherChannel 中的多条链路上传输流量，同时又仍能实现冗余。

下图显示了如何在虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 环境中使用 EtherChannel 作为集群控制链路。EtherChannel 中的所有链路都是活动链路。如果交换机是 VSS 或 vPC 的一部分，则可将同一个 EtherChannel 中的 ASA 接口连接到 VSS 或 vPC 中单独的交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台单独的交换机的行为就像一台交换机一样。请注意，此 EtherChannel 是设备本地的，而非跨网络 EtherChannel。



集群控制链路可靠性

为了确保集群控制链路的功能，设备之间的往返时间 (RTT) 务必要小于 20 毫秒。此最大延迟能够增强与不同地理位置安装的集群成员的兼容性。如要检查延迟，请在设备之间的集群控制链路上执行 ping 操作。

集群控制链路必须可靠，没有数据包顺序错乱或丢弃数据包的情况；例如，站点间部署应使用专用链路。

集群控制链路故障

如果某台设备的集群控制链路线路协议关闭，则集群将被禁用；数据接口关闭。当您修复集群控制链路之后，必须通过重新启用集群来手动重新加入集群。

注　当 ASA 处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。管理接口将保持打开，使用设备从集群 IP 池接收的 IP 地址。但是，如果您重新加载而设备在集群中仍然处于非活动状态，管理接口将无法访问 （因为它届时将使用与主设备相同的主 IP 地址）。您必须使用控制台端口来进行任何进一步配置。

相关主题

第 8-9 页的重新加入集群

ASA 集群中的高可用性

ASA 集群通过监控设备和接口的运行状况并在设备之间复制连接状态来提供高可用性。

- 第 8-8 页的设备运行状况监控
- 第 8-8 页的接口监控
- 第 8-8 页的设备或接口故障
- 第 8-9 页的数据路径连接状态复制

设备运行状况监控

主设备通过在集群控制链路上定期 （此周期可配置）发送 keepalive 消息来监控每台从设备。每台从设备也使用相同的机制来监控主设备。

接口监控

每台设备都会监控使用中的所有硬件接口的链路状态，并向主设备报告状态更改。

- 跨网络 EtherChannel - 使用集群链路聚合控制协议 (cLACP)。每台设备都会监控链路状态和 cLACP 协议消息，以便确定 EtherChannel 中的端口是否仍处于活动状态。此状态将会报告给主设备。
- 独立接口 （仅适用于路由模式） - 每台设备都会监控自己的接口并向主设备报告接口状态。

设备或接口故障

启用运行状况监控时，如果某台设备或其接口发生故障，将从集群中删除该设备。如果特定设备上的一个接口发生故障，但其他设备上的相同接口处于活动状态，则会从集群中删除该设备。ASA 在多长时间后从集群中删除成员取决于接口的类型以及该设备是既定成员还是正在加入集群的设备。对于 EtherChannel（无论是否跨网络），如果既定成员上的接口关闭，ASA 将在 9 秒后删除该成员。ASA 在设备加入集群后的最初 90 秒不监控接口。在此期间的接口状态更改不会导致 ASA 从集群中删除。如果是非 EtherChannel，则无论设备的成员状态如何，都会在 500 毫秒后删除设备。

当集群中的设备发生故障时，该设备承载的连接将无缝转移到其他设备；流量的状态信息将通过集群控制链路共享。

如果主设备发生故障，则优先级最高（数字最小）的另一个集群成员将成为主设备。

ASA 将自动尝试重新加入集群。

注　当 ASA 处于非活动状态且无法自动重新加入集群时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。管理接口将保持打开，使用设备从集群 IP 池接收的 IP 地址。但是，如果您重新加载而设备在集群中仍然处于非活动状态，管理接口将无法访问 （因为它届时将使用与主设备相同的主 IP 地址）。您必须使用控制台端口来进行任何进一步配置。

相关主题

第 8-9 页的重新加入集群

重新加入集群

当集群成员从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路发生故障 - 解决集群控制链路的问题之后，必须在控制台端口上通过输入 **cluster** *name*，然后输入 **enable** 重新启用集群来手动重新加入集群。
- 数据接口发生故障 - ASA 会依次在第 5 分钟、第 10 分钟和第 20 分钟时自动尝试重新加入。如果 20 分钟后仍加入失败，ASA 将禁用集群。解决数据接口问题之后，必须在控制台端口上通过输入 **cluster** *name*，然后输入 **enable** 手动启用集群。
- 设备发生故障 - 如果设备因设备运行状况检查失败而从集群中删除，则如何重新加入集群取决于失败的原因。例如，临时电源故障意味设备将在重新启动时重新加入集群，只要集群控制链路打开并且仍然使用 **enable** 命令启用集群。

相关主题

- 第 8-41 页的配置主设备引导程序设置

数据路径连接状态复制

每个连接在集群中都有一个所有者和至少一个备用所有者。备用所有者在发生故障时不会接管连接；而是存储 TCP/UDP 状态信息，使连接在发生故障时可以无缝转移到新的所有者。

如果所有者变得不可用，从该连接接收数据包的第一台设备 （根据负载均衡而定）将联系备用所有者获取相关的状态信息以便成为新的所有者。

有些流量需要 TCP 或 UDP 层以上的状态信息。请参阅下表了解支持或不支持此类流量的集群。

表 8-1　　在集群中复制的 ASA 功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	仅透明模式。
MAC 地址表	是	仅透明模式。
用户标识	是	包括 AAA 规则 (uauth) 和标识防火墙。
IPv6 邻居数据库	是	-
动态路由	是	-
SNMP 引擎 ID	否	-
VPN（站点到站点）	否	如果主设备发生故障，VPN 会话将断开连接。

配置复制

集群中的所有设备共享一个配置。除初始引导程序配置之外，您只能在主设备上进行配置更改，这些更改将自动复制到集群中的所有其他设备。

ASA 集群管理

使用 ASA 集群的优点之一是易于管理。本节介绍如何管理集群。

- 第 8-10 页的管理网络
- 第 8-10 页的管理接口
- 第 8-10 页的主设备管理与从设备管理
- 第 8-11 页的 RSA 密钥复制
- 第 8-11 页的 ASDM 连接证书 IP 地址不匹配

管理网络

我们建议将所有设备都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理接口

对于管理接口，我们建议使用一个专用管理接口。您可以将管理接口配置为独立接口 （适用于路由和透明模式）或跨网络 EtherChannel 接口。

即便使用跨网络 EtherChannel 作为数据接口，我们仍然建议使用独立接口作为管理接口。独立接口可以根据需要直接连接到每台设备，而跨网络 EtherChannel 接口则只允许远程连接到当前的主设备。

注　如果使用跨网络 EtherChannel 接口模式并将管理接口配置为独立接口，则无法为管理接口启用动态路由。您必须使用静态路由。

对于独立接口，主集群 IP 地址是集群的固定地址，始终属于当前的主设备。您还要为每个接口配置一个地址范围，以便包括当前主设备在内的每台设备都可以使用该范围内的本地地址。主集群 IP 地址提供对地址的统一管理访问；当主设备更改时，主集群 IP 地址将转移到新的主设备，使集群的管理得以无缝继续。本地 IP 地址用于路由，在排除故障时也非常有用。

例如，您可以连接到主集群 IP 地址来管理集群，该地址始终属于当前的主设备。如要管理单个成员，可以连接到本地 IP 地址。

对于 TFTP 或系统日志等出站管理流量，包括主设备在内的每台设备都使用本地 IP 地址连接到服务器。

对于跨网络 EtherChannel 接口，只能配置一个 IP 地址，该 IP 地址始终属于主设备。您无法使用 EtherChannel 接口直接连接到从设备；我们建议将管理接口配置为独立接口，以便您连接到每台设备。请注意，可以使用设备本地 EtherChannel 进行管理。

主设备管理与从设备管理

除了引导程序配置外，所有管理和监控都可以在主设备上进行。您可以从主设备检查所有设备的运行时统计信息、资源使用率或其他监控信息。您也可以向集群中的所有设备发出命令，并将控制台消息从从设备复制到主设备。

如果需要，您可以直接监控从设备。虽然可以从主设备执行文件管理，但您也可以在从设备上执行 （包括备份配置和更新映像）。以下功能不可从主设备使用：

- 监控每台设备的集群特定统计信息。
- 每台设备的系统日志监控。

- SNMP
- NetFlow

RSA 密钥复制

在主设备上创建 RSA 密钥时，该密钥将被复制到所有从设备。如果您有连接到主集群 IP 地址的 SSH 会话，会在主设备发生故障时断开连接。新的主设备使用同一密钥进行 SSH 连接，因此在重新连接到新的主设备时，无需更新缓存的 SSH 主机密钥。

ASDM 连接证书 IP 地址不匹配

默认情况下，ASDM 连接将根据本地 IP 地址使用自签证书。如果使用 ASDM 连接到主集群 IP 地址，则会因证书使用本地 IP 地址而非主集群 IP 地址而显示一则警告消息，指出 IP 地址不匹配。您可以忽略该消息并建立 ASDM 连接。不过，为了避免此类警告，您也可以注册一个包含主集群 IP 地址和 IP 地址池中所有本地 IP 地址的证书。然后，您可将此证书用于每个集群成员。

相关主题

- 第 34 章，“数字证书”

负载均衡方法

可用的负载均衡方法取决于防火墙模式和接口类型。

- 第 8-11 页的跨网络 EtherChannel（推荐）
- 第 8-15 页的基于策略的路由（仅适用于路由防火墙模式）
- 第 8-16 页的等价多路径路由（仅适用于路由防火墙模式）

跨网络 EtherChannel （推荐）

您可以将每台设备的一个或多个接口分组为跨集群中所有设备的 EtherChannel。 EtherChannel 汇聚信道中所有可用活动接口上的流量。

- 第 8-11 页的跨网络 EtherChannel 的优点
- 第 8-12 页的最大吞吐量指导原则
- 第 8-12 页的负载均衡
- 第 8-12 页的 EtherChannel 冗余
- 第 8-12 页的连接到 VSS 或 vPC

跨网络 EtherChannel 的优点

我们优先推荐 EtherChannel 负载均衡方法，因其具有以下优点：

- 发现故障更快。
- 收敛速度更快。独立接口依靠路由协议来实现流量的负载均衡，而路由协议在链路发生故障时通常收敛速度缓慢。
- 易于配置。

相关主题

第 9-4 页的 EtherChannel

最大吞吐量指导原则

如要实现最大吞吐量，建议采取以下措施：

- 使用“对称”的负载均衡哈希算法，亦即来自两个方向的数据包具有相同的哈希值，并将在跨网络 EtherChannel 中发送到同一台 ASA。我们建议将源和目标 IP 地址 （默认设置）或源和目标端口用作哈希算法。
- 将 ASA 连接到交换机时使用相同类型的线路卡，以使应用于所有数据包的哈希算法都相同。

负载均衡

EtherChannel 链路使用专有哈希算法并且根据源或目标 IP 地址以及 TCP 和 UDP 端口号进行选择。

注 在 ASA 上，请勿更改默认的负载均衡算法。在交换机上，建议使用以下算法之一：**source-dest-ip** 或 **source-dest-ip-port**（请参阅思科 Nexus OS 或思科 IOS **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中 ASA 的流量分摊不均。

EtherChannel 中的链路数量会影响负载均衡。

对称的负载均衡有时并不能够实现。如果配置了 NAT，则转发和返回数据包具有不同的 IP 地址和/或端口。返回流量将根据哈希值被发送到不同的设备，因此集群不得不将大部分返回流量重定向到正确的设备。

相关主题

- 第 9-19 页的自定义 EtherChannel
- 第 9-6 页的负载均衡
- 第 8-26 页的 NAT 和集群

EtherChannel 冗余

EtherChannel 有内置冗余。它监控所有链路的线路协议状态。如果一条链路发生故障，将在其余链路之间再均衡流量。如果 EtherChannel 中的所有链路在特定设备上发生故障，但其他设备仍然处于活动状态，则会从集群中删除该设备。

连接到 VSS 或 vPC

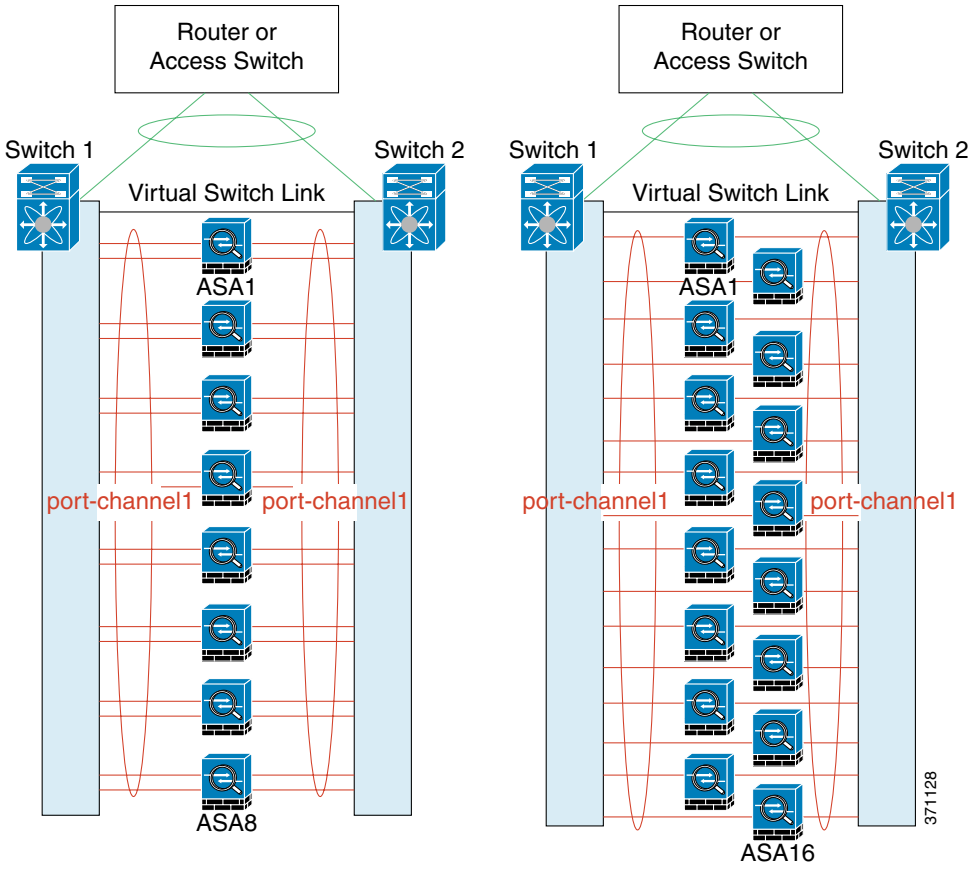
您可以在跨网络 EtherChannel 中包含每台 ASA 的多个接口。每台 ASA 多个接口对于连接到 VSS 或 vPC 中两台交换机的情况特别有用。

根据交换机的不同，最多可在跨网络 EtherChannel 中配置 32 条活动链路。此功能需要 vPC 中的两台交换机都支持各有 16 条活动链路的 EtherChannel（例如带 F2 系列 10 千兆以太网模块的思科 Nexus 7000）。

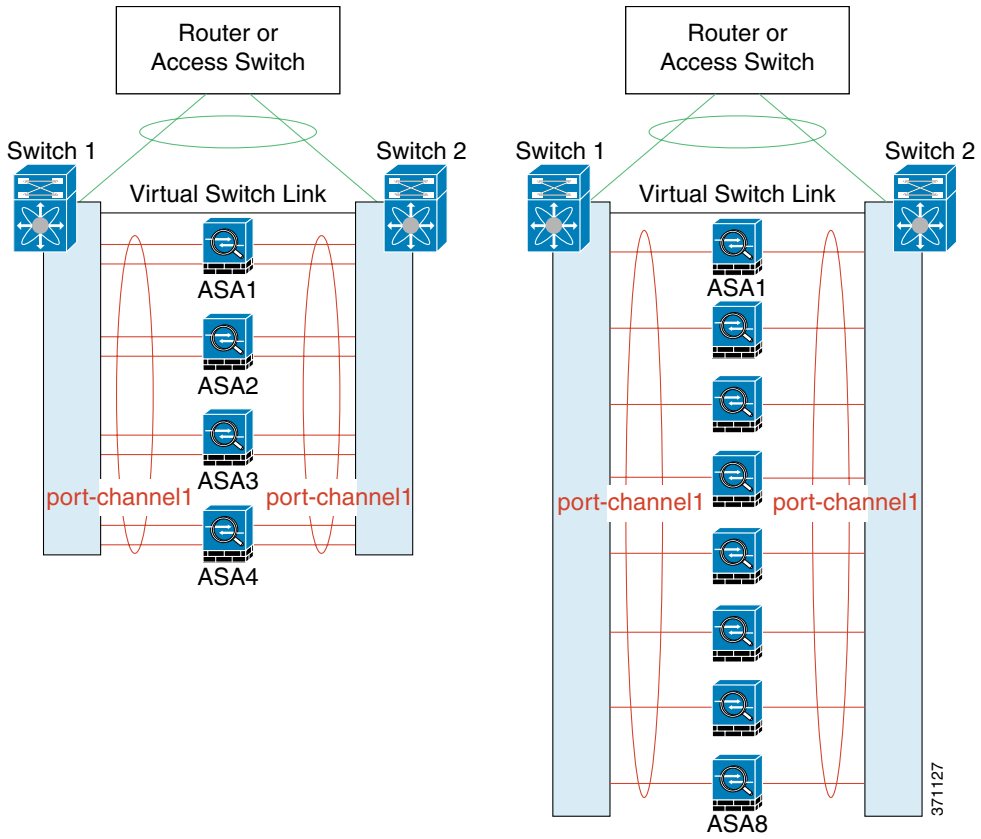
对于支持 EtherChannel 中有 8 条活动链路的交换机，在连接到 VSS/vPC 中的两台交换机时，最多可在跨网络 EtherChannel 中配置 16 条活动链路。

如果要在跨网络 EtherChannel 中使用 8 条以上的活动链路，则无法同时拥有备用链路；支持 9 到 32 条活动链路需要禁用允许使用备用 链路的 cLACP 动态端口优先级。如果需要，您仍然可以使用 8 条活动链路和 8 条备用链路，例如在连接到一台交换机时。

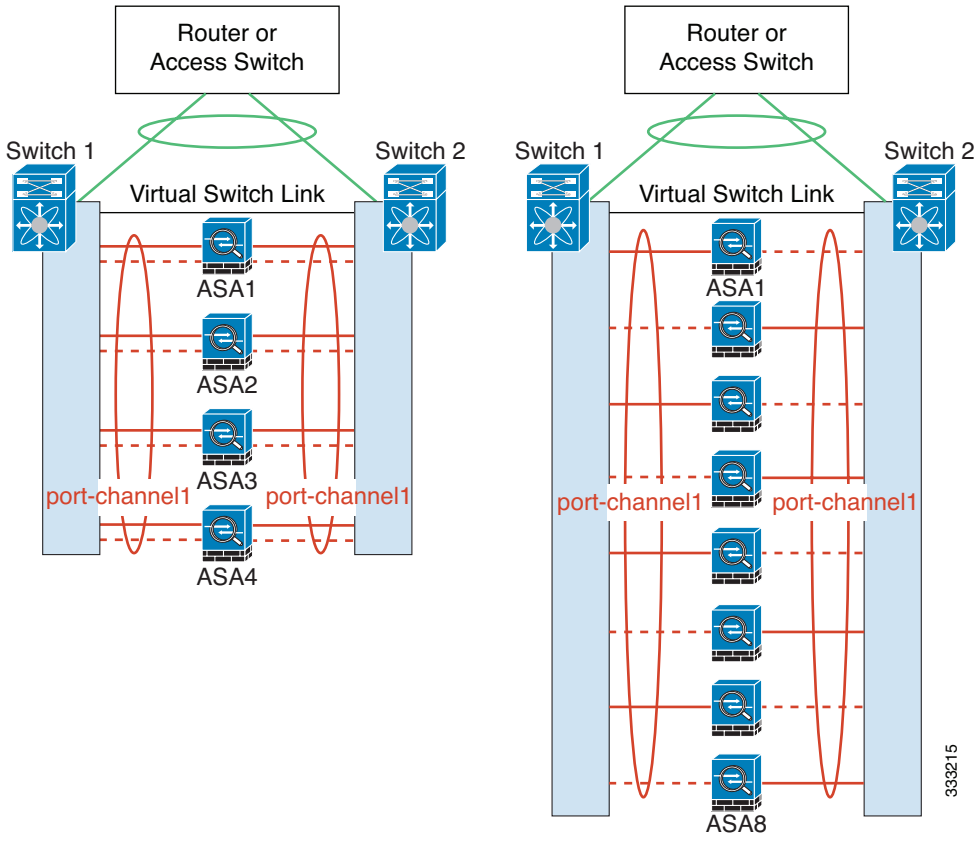
下图所示为 8-ASA 集群和 16-ASA 集群中有 32 条活动链路的跨网络 EtherChannel。



下图所示为 4-ASA 集群和 8-ASA 集群中有 16 条活动链路的跨网络 EtherChannel。



下图所示为 4-ASA 集群和 8-ASA 集群中的有 8 条活动和 8 条备用链路的传统跨网络 EtherChannel。活动链路以实线表示，非活动链路以虚线表示。 cLACP 负载均衡可自动选择最佳的 8 条链路作为 EtherChannel 中的活动链路。如图所示， cLACP 可以帮助在链路层面实现负载均衡。



基于策略的路由 （仅适用于路由防火墙模式）

使用独立接口时，每个 ASA 接口都会保留自己的 IP 地址和 MAC 地址。基于策略的路由 (PBR) 是一种负载均衡方法。

如果已经在使用 PBR 并希望充分利用现有的基础设施，建议使用此方法。与跨网络 EtherChannel 相比，此方法也可以提供其他调整选项。

PBR 根据路由映射和 ACL 作出路由决定。您必须在集群中的所有 ASA 之间手动划分流量。由于 PBR 是静态路由，因此可能有时候无法实现最佳的负载均衡效果。如要实现最佳性能，建议您通过配置 PBR 策略，将一条连接的转发和返回数据包定向到同一台物理 ASA。例如，如果您有一台思科路由器，使用带对象跟踪的思科 IOS PBR 即可实现冗余。思科 IOS 对象跟踪使用 ICMP ping 监控每台 ASA。然后，PBR 可根据特定 ASA 的可接通性来启用或禁用路由映射。有关详细信息，请参阅以下 URL：

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

注　如果使用此负载均衡方法，则可使用设备本地 EtherChannel 作为独立接口。

等价多路径路由 （仅适用于路由防火墙模式）

使用独立接口时，每个 ASA 接口都会保留自己的 IP 地址和 MAC 地址。等价多路径 (ECMP) 路由是一种负载均衡方法。

如果已经在使用 ECMP 并希望充分利用现有的基础设施，建议使用此方法。与跨网络 EtherChannel 相比，此方法也可以提供其他调整选项。

ECMP 路由可以通过路由度量并列最优的多条“最佳路径”转发数据包。它与 EtherChannel 一样，也可以使用源和目标 IP 地址及/或源和目标端口的哈希值将数据包发送到下一跳之一。如果将静态路由用于 ECMP 路由，则 ASA 故障会导致问题；如果继续使用该路由，发往故障 ASA 的流量将丢失。因此，如果使用静态路由，请务必要使用静态路由监控功能，例如对象跟踪。我们还建议使用动态路由协议来添加和删除路由，在这种情况下，您必须配置每台 ASA 使之加入动态路由。

注　如果使用此负载均衡方法，则可使用设备本地 EtherChannel 作为独立接口。

站点间集群

对于站点间安装，只要遵循以下指导原则就可以充分发挥 ASA 集群的作用。

- 第 8-16 页的站点间集群指导原则
- 第 8-17 页的确定数据中心互联的规格
- 第 8-17 页的站点间集群示例

站点间集群指导原则

请参阅有关站点间集群的以下指导原则：

- 在以下接口和防火墙模式中，支持站点间集群：

	防火墙模式	
接口模式	**路由**	**透明**
独立接口	**是**	不适用
跨网络 EtherChannel	否	**是**

- 集群控制链路的延迟必须小于 20 微秒往返时间 (RTT)。
- 集群控制链路必须可靠，没有数据包顺序错乱或丢弃数据包的情况；例如，应该使用专用链路。
- 请勿配置连接再均衡；您不需要将连接再均衡到位于不同站点的集群成员。
- 位于多个站点的成员之间的集群实施没有区别；因此，给定连接的连接角色可以跨越所有站点。这是预期行为。
- 对于透明模式，必须确保两台内部路由器共用同一个 MAC 地址，两台外部路由器也共用同一个 MAC 地址。当位于站点 1 的集群成员将连接转发到位于站点 2 的成员时，目标 MAC 地址会被保留。如果该 MAC 地址与位于站点 1 的路由器相同，则数据包只会到达位于站点 2 的路由器。
- 对于跨网络 EtherChannel 模式，请勿扩展直接连接到站点间 ASA 集群的数据 VLAN；会造成环路。任何扩展的数据 VLAN 都必须以路由器与集群分隔开来。

相关主题

- 第 8-21 页的在集群中再均衡新的 TCP 连接
- 第 8-20 页的连接角色

确定数据中心互联的规格

您应该在数据中心互联 (DCI) 上为集群控制链路流量保留等同于以下计算结果的带宽：

$$\frac{\text{每个站点的集群成员数量}}{2} \times \text{每个成员的集群控制链路大小}$$

如果各站点的成员数不同，请使用较大的数量进行计算。 DCI 的最低带宽不得低于一个成员的集群控制链路的流量大小。

例如：

- 位于 2 个站点的 4 个成员：
  - 总共 4 个集群成员
  - 每个站点 2 个成员
  - 每个成员 5 Gbps 集群控制链路

  保留的 DCI 带宽 = 5 Gbps (2/2 x 5 Gbps)。
- 对位于 2 个站点的 8 个成员而言，规格加大：
  - 总共 8 个集群成员
  - 每个站点 4 个成员
  - 每个成员 5 Gbps 集群控制链路

  保留的 DCI 带宽 = 10 Gbps (4/2 x 5 Gbps)。
- 位于 3 个站点的 6 个成员：
  - 总共 6 个集群成员
  - 站点 1 有 3 个成员，站点 2 有 2 个成员，站点 3 有 1 个成员
  - 每个成员 10 Gbps 集群控制链路

  保留的 DCI 带宽 = 15 Gbps (3/2 x 10 Gbps)。
- 位于 2 个站点的 2 个成员：
  - 总共 2 个集群成员
  - 每个站点 1 个成员
  - 每个成员 10 Gbps 集群控制链路

  保留的 DCI 带宽 = 10 Gbps（1/2 x 10 Gbps = 5 Gbps；但最低带宽不得低于集群控制链路的流量大小 (10 Gbps)）。

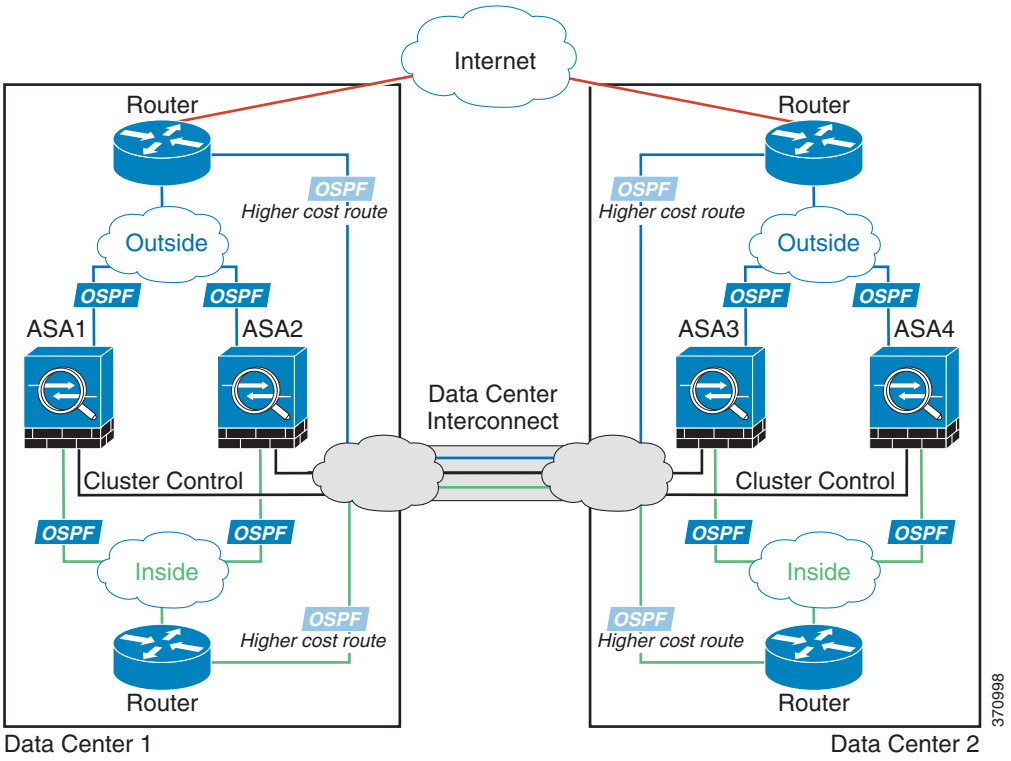
站点间集群示例

以下示例显示支持的集群部署。

- 第 8-18 页的独立接口站点间集群示例
- 第 8-18 页的跨网络 EtherChannel 透明模式站点间集群示例

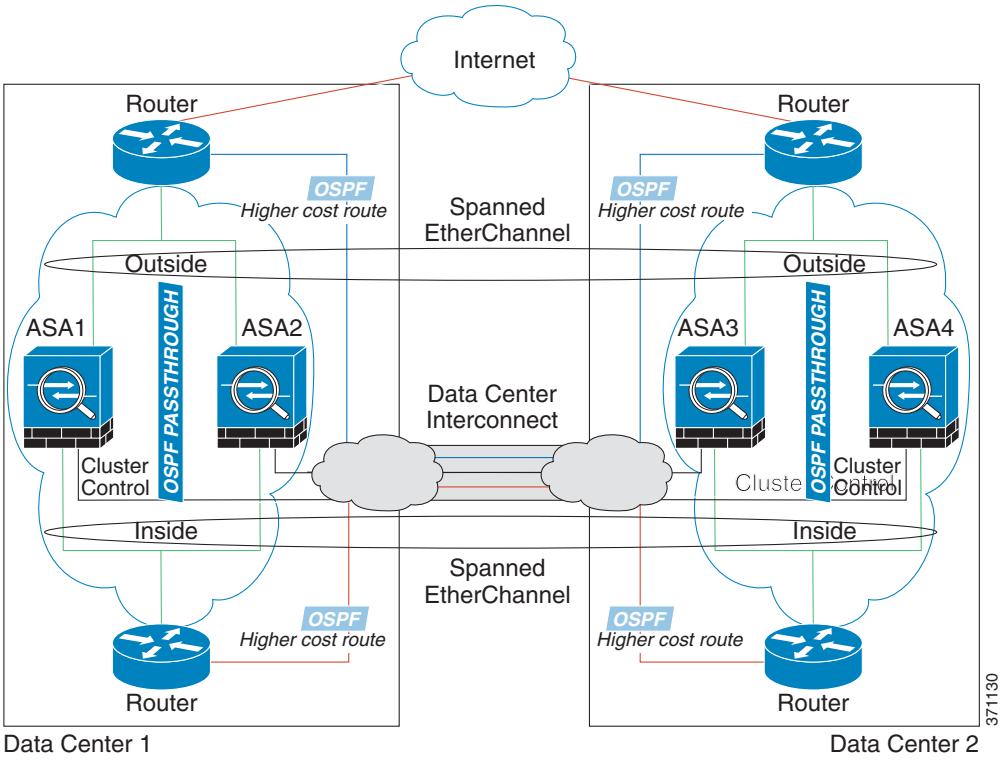
独立接口站点间集群示例

以下图例显示了分别位于 2 个数据中心的 2 个 ASA 集群成员。集群成员由集群控制链路通过 DCI 连接。位于每个数据中心的内部和外部路由器使用 OSPF 和 PBR 或 ECMP 在集群成员之间对流量执行负载均衡。通过指定 DCI 中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有 ASA 集群成员都中断连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的 ASA 集群成员。



跨网络 EtherChannel 透明模式站点间集群示例

以下图例显示了分别位于 2 个数据中心的 2 个 ASA 集群成员。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部的跨网络 EtherChannel 连接到本地交换机。ASAEtherChannel 跨越集群中的所有 ASA。位于每个数据中心的内部和外部路由器使用 OSPF 经过透明的 ASA。与 MAC 地址不同，路由器 IP 地址在所有路由器上都是唯一的。通过指定 DCI 中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有 ASA 集群成员都中断连接。通过 ASA 的开销较低的路由必须经过位于每个站点的同一网桥组才能使集群维持非对称连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的 ASA 集群成员。



位于每个站点的交换机的实施可包括：

- 站点间 VSS/vPC - 在此情景中，一台交换机安装在数据中心 1，另一台交换机安装在数据中心 2。一个方案是将位于每个数据中心的 ASA 集群设备只连接到本地交换机，而 VSS/vPC 流量通过 DCI 传输。在此情况下，连接多半会保持在每个数据中心本地。如果 DCI 可以处理额外的流量，您也可以选择将每台 ASA 设备通过 DCI 连接到两台交换机。在此情况下，流量跨数据中心分摊，因此 DCI 必须非常强健稳定。
- 位于每个站点的本地 VSS/vPC - 为了获得更高的交换机冗余能力，可以在每个站点安装 2 对单独的 VSS/vPC。在此情况下，尽管 ASA 仍然有一个跨网络 EtherChannel 将数据中心 1 的 ASA 仅连接到两台本地交换机，将数据中心 2 的 ASA 连接到本地交换机，但跨网络 EtherChannel 本质上是“分离的”。每个本地 VSS/vPC 都会将跨网络 EtherChannel 视为站点本地的 EtherChannel。

ASA 集群如何管理连接

可以将连接负载均衡到多个集群成员。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。

- 第 8-20 页的连接角色
- 第 8-20 页的新连接所有权
- 第 8-21 页的数据流示例
- 第 8-21 页的在集群中再均衡新的 TCP 连接

连接角色

为每个连接定义了 3 种不同的 ASA 角色：

- 所有者 - 最初接收连接的设备。所有者负责维护 TCP 状态并处理数据包。一个连接只有一个所有者。
- 导向者 - 处理来自转发者的所有者查找请求，同时也维护连接状态，在所有者发生故障时作为备用设备。当所有者收到新连接时，会根据源/目标 IP 地址和 TCP 端口的哈希值选择导向者，然后向导向者发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他设备，该设备会向导向者查询哪一台设备是所有者，以便转发数据包。一个连接只有一个导向者。
- 转发者 - 向所有者转发数据包的设备。如果转发者收到并非其所有的连接的数据包，则会向导向者查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向者也可以是转发者。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN cookie 直接获知所有者，因此无需向导向者查询。（如果禁用 TCP 序列随机化，则不会使用 SYN cookie；必须向导向者查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向者，然后由其发送到所有者。一个连接可有多个转发者；采用良好的负载均衡方法可以做到没有转发者，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。

新连接所有权

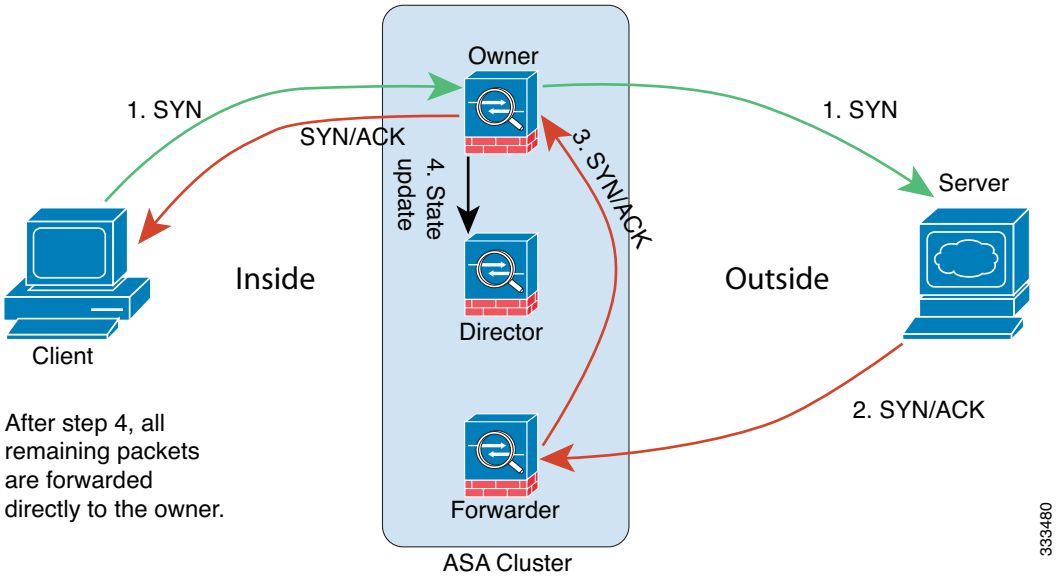
通过负载均衡将新连接定向到集群成员时，该连接的两个方向都由此设备所有。如果该连接有任何数据包到达其他设备，这些数据包都会通过集群控制链路被转发到所有者设备。为了获得最佳性能，对于要到达同一台设备的流量的两个方向以及要在设备之间均摊的流量，都需要执行适当的外部负载均衡。如果反向流量到达其他设备，会被重定向回原始设备。

相关主题

- 第 8-11 页的负载均衡方法

数据流示例

以下图例显示了新连接的建立。



1. SYN 数据包从客户端发出，被传送到一台 ASA（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 ASA（基于负载均衡方法）。此 ASA 是转发者。
3. 由于转发者不是该连接的所有者，因此它将解码 SYN cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向者，然后将 SYN-ACK 数据包转发到客户端。
5. 导向者接收来自所有者的状态更新，创建发往所有者的流量，并记录 TCP 状态信息以及所有者。导向者将充当该连接的备用所有者。
6. 传送到转发者的任何后续数据包都会被转发到所有者。
7. 如果数据包被传送到任何其他设备，它将向导向者查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向者发送状态更新。

在集群中再均衡新的 TCP 连接

如果上游或下游路由器的负载均衡功能导致流量分摊不均衡，可以将过载的设备配置为将新的 TCP 流量重定向到其他设备。现有流量不会被转移到其他设备。

ASA 功能和集群

有些 ASA 功能不受 ASA 集群支持，还有些功能只有在主设备上才受支持。其他功能可能对如何正确使用规定了注意事项。

- 第 8-22 页的集群不支持的功能
- 第 8-22 页的集群的集中功能
- 第 8-23 页的应用到各设备的功能

- 第 8-24 页的动态路由和集群
- 第 8-25 页的组播路由和集群
- 第 8-26 页的 NAT 和集群
- 第 8-26 页的用于网络访问的 AAA 和集群
- 第 8-27 页的系统日志与 NetFlow 和集群
- 第 8-27 页的 SNMP 和集群
- 第 8-27 页的 VPN 和集群
- 第 8-27 页的 FTP 和集群
- 第 8-27 页的思科 TrustSec 和集群

集群不支持的功能

以下功能在启用集群的情况下无法配置，相关命令会被拒绝。

- 统一通信
- 远程接入 VPN（SSL VPN 和 IPsec VPN）
- 以下应用检查：
  - CTIQBE
  - GTP
  - H323、 H225 和 RAS
  - IPsec 直通
  - MGCP
  - MMP
  - RTSP
  - SIP
  - SCCP (Skinny)
  - WAAS
  - WCCP
- 僵尸网络流量过滤器
- 自动更新服务器
- DHCP 客户端、服务器、中继和代理
- VPN 负载均衡
- 故障转移
- ASA CX 模块

集群的集中功能

以下功能只有在主设备上才受支持，且无法为集群扩展。例如，您有一个由 8 台设备 （带 SSP-60 的 5585-X）组成的集群。“其他 VPN”许可证允许一台带 SSP-60 的 5585-X 最多有 10,000 个站点间 IPsec 隧道。对于由 8 台设备组成的整个集群，您只能使用 10,000 个隧道；此功能无法扩展。

注　集中功能的流量从成员设备通过集群控制链路转发到主设备。

如果使用再均衡功能，则会先将集中功能的流量再均衡到非主设备的设备，然后再将该流量归类为集中功能；如果发生此情况，该流量随后将被发送回主设备。

对集中功能而言，如果主设备发生故障，则所有连接都将断开，而您必须在新的主设备上重新建立连接。

- 站点到站点 VPN
- 以下应用检查：
  - DCERPC
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- 动态路由 （仅适用于跨网络 EtherChannel 模式）
- 组播路由 （仅适用于独立接口模式）
- 静态路由监控
- IGMP 组播控制层面协议的处理 （数据层面转发分布于整个集群中）
- PIM 组播控制层面协议的处理 （数据层面转发分布于整个集群中）
- 网络访问的身份验证和授权。记帐被分散。
- 过滤服务

相关主题

- 第 8-6 页的调整集群控制链路的吞吐量大小
- 第 8-21 页的在集群中再均衡新的 TCP 连接

应用到各设备的功能

以下功能将应用到每台 ASA 设备而非整个集群或主设备。

- QoS - QoS 策略将于配置复制过程中在集群中同步。不过，该策略是在每台设备上独立实施。例如，如果对输出配置管制，则要对流出特定 ASA 的流量应用符合速率和符合突发量值。在由 8 台设备组成且流量均摊的集群中，符合速率实际上变成了集群*速率*的 8 倍。
- 威胁检测 - 威胁检测在各台设备上独立工作；例如，排名统计信息就要视具体设备而定。以端口扫描检测为例，由于扫描的流量将在所有设备间进行负载均衡，而一台设备无法看到所有流量，因此端口扫描检测无法工作。
- 资源管理 - 多情景模式中的资源管理根据本地使用情况在每台设备上分别执行。

- ASA FirePOWER 模块 - ASA FirePOWER 模块之间不存在配置同步或状态共享。您要负责使用 FireSIGHT 管理中心在集群中的 ASA FirePOWER 模块上保持策略的一致性。请勿对集群内的设备使用不同的基于 ASA 接口的区域定义。
- ASA IPS 模块 - IPS 模块之间不存在配置同步或状态共享。有些 IPS 签名需要 IPS 跨多个连接保存状态信息。例如，当 IPS 模块检测到有人打开多个连接到同一台服务器的连接但端口不同时，将使用端口扫描签名。在集群中，这些连接将在多台 ASA 设备之间进行均衡，其中每台设备都有自己的 IPS 模块。由于这些 IPS 模块并不共享状态信息，因此集群可能无法检测端口扫描。

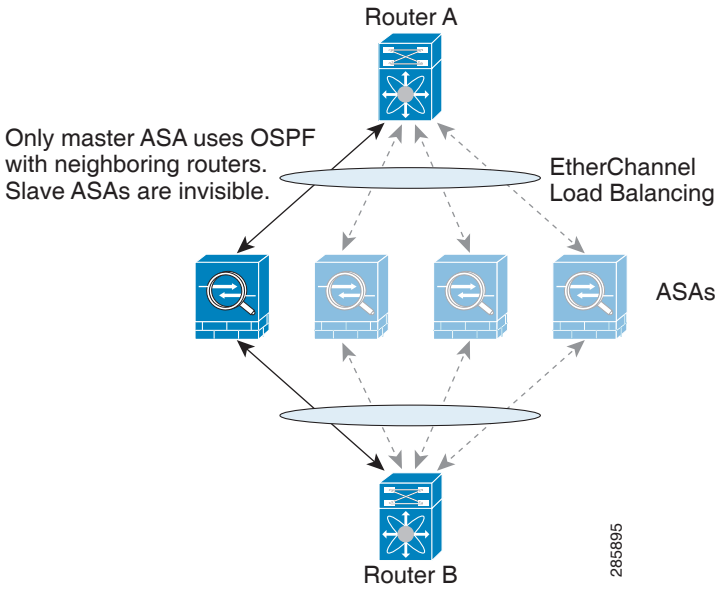
动态路由和集群

- 第 8-24 页的跨网络 EtherChannel 模式中的动态路由
- 第 8-25 页的独立接口模式中的动态路由

跨网络 EtherChannel 模式中的动态路由

在跨网络 EtherChannel 模式中，路由进程仅在主设备上运行，路由通过主设备获知并复制到从设备。如果路由数据包到达从设备，会被重定向到主设备。

图 8-1　跨网络 EtherChannel 模式中的动态路由



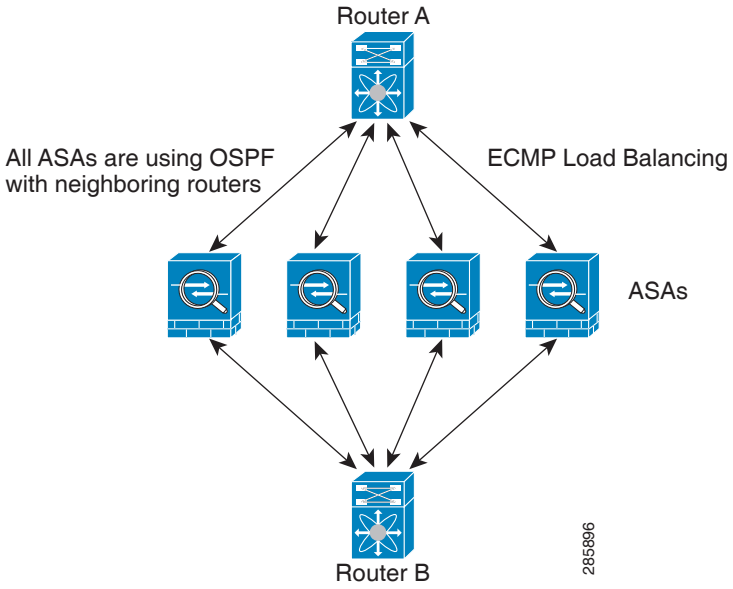
当从设备成员从主设备获知路由后，每台设备将独立作出转发决定。

OSPF LSA 数据库不会从主设备同步到从设备。如果发生主设备切换，邻居路由器将检测到重新启动；切换并非透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。

独立接口模式中的动态路由

在独立接口模式中，每台设备作为独立的路由器运行路由协议，且每台设备独立获知路由。

图 8-2　　独立接口模式中的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一台 ASA。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每台 ASA 在与外部路由器通信时，会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每台设备都有单独的路由器 ID。

组播路由和集群

组播路由的行为因接口模式而异。

- 第 8-25 页的跨网络 EtherChannel 模式中的组播路由
- 第 8-25 页的独立接口模式中的组播路由

跨网络 EtherChannel 模式中的组播路由

在跨网络 EtherChannel 模式中，主设备负责处理所有组播路由数据包和数据包，直到建立快速路径转发为止。在连接建立之后，每台从设备都可以转发组播数据包。

独立接口模式中的组播路由

在独立接口模式中，设备并不独立处理组播。所有数据包和路由数据包都由主设备处理和转发，从而避免数据包复制。

NAT 和集群

NAT 可能会影响集群的整体吞吐量。入站和出站 NAT 数据包可被发送到集群中不同的 ASA，因为负载均衡算法取决于 IP 地址和端口，NAT 会导致入站和出站数据包具有不同的 IP 地址和/或端口。当数据包到达并非连接所有者的 ASA 时，会通过集群控制链路被转发到所有者，导致集群控制链路上存在大量流量。

如果您仍想在集群中使用 NAT，请考虑以下指导原则：

- 不使用代理 ARP - 对于独立接口，切勿为映射的地址发送代理 ARP 应答。这可以防止邻接路由器与可能已经不在集群中的 ASA 保持对等关系。对于指向主集群 IP 地址的映射地址，上游路由器需要静态路由或带对象跟踪的 PBR。这对跨网络 EtherChannel 来说不是问题，因为只有一个 IP 地址与集群接口关联。
- 不对独立接口使用接口 PAT - 独立接口不支持接口 PAT。
- 对动态 PAT 使用 NAT 池地址分配 - 主设备在整个集群中预先平均分配地址。如果成员收到连接却没有剩余的地址，即使其他成员仍有可用地址，该连接仍会断开。因此，请确保至少包含与集群中的设备数量相同的 NAT 地址，务必让每台设备都收到一个地址。使用 **show nat pool cluster** 命令查看地址分配。
- 不使用轮询 - 集群不支持 PAT 池轮询。
- 主设备管理的动态 NAT 转换项 - 主设备负责维护转换表并将其复制到从设备。当从设备收到需要动态 NAT 的连接而转换项不在表中时，将向主设备请求该转换项。从设备是该连接的所有者。
- 每会话 PAT 功能 - 每会话 PAT 功能并非集群专用功能，但它能提高 PAT 的可扩展性，而且对集群而言，它允许每台从设备成为 PAT 连接的所有者；相比之下，多会话 PAT 连接则必须转发到主设备并由主设备所有。默认情况下，所有 TCP 流量和 UDP DNS 流量都使用每会话 PAT 转换项。对于 H.323、 SIP 或 Skinny 等需要多会话 PAT 的流量，可禁用每会话 PAT。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。
- 对以下检查不使用静态 PAT -
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - 所有 IP 语音应用

用于网络访问的 AAA 和集群

用于网络访问的 AAA 由三部分组成：身份验证、授权和记帐。身份验证和记帐作为集中功能在集群主设备上实施，数据结构被复制到集群从设备。如果选举出主设备，新的主设备将获得所需的全部信息，让通过身份验证的既定用户及其关联的授权能够继续操作而不中断。发生主设备更改时，用户身份验证的空闲超时和绝对超时会被保留。

记帐作为分散的功能在集群中实施。记帐按每次流量完成，因此在为流量配置记帐时，作为流量所有者的集群设备会将记帐开始和停止消息发送到 AAA 服务器。

系统日志与 NetFlow 和集群

- 系统日志 - 集群中的每台设备都会生成自己的系统日志消息。您可以配置日志记录，使每台设备在系统日志消息的报头字段中使用相同或不同的设备 ID。例如，集群中的所有设备都会复制和共享主机名配置。如果将日志记录配置为使用主机名作为设备 ID，则所有设备生成的系统日志消息都会看似来自一台设备。如果将日志记录配置为使用集群引导程序配置中指定的本地设备名称作为设备 ID，系统日志消息就会看似来自不同设备。
- NetFlow - 集群中的每台设备都会生成自己的 NetFlow 数据流。 NetFlow 采集器只能将每台 ASA 视为单独的 NetFlow 导出器。

相关主题

- 第 39-15 页的在非 EMBLEM 格式系统日志消息中包含设备 ID

SNMP 和集群

SNMP 代理按照本地 IP 地址轮询每台单独的 ASA。您无法轮询集群的合并数据。

应该始终使用本地地址而非主集群 IP 地址进行 SNMP 轮询。如果 SNMP 代理轮询主集群 IP 地址，则当选举出新的主设备时，对新的主设备的轮询将失败。

VPN 和集群

站点到站点 VPN 是集中功能；只有主设备支持 VPN 连接。

注　集群不支持远程接入 VPN。

VPN 功能仅限主设备使用，且不能利用集群的高可用性功能。如果主设备发生故障，所有现有的 VPN 连接都将丢失， VPN 用户将遇到服务中断。选举出新的主设备后，必须重新建立 VPN 连接。

将 VPN 隧道连接到跨网络 EtherChannel 地址时，连接会自动转移到主设备。对于使用 PBR 或 ECMP 时与独立接口的连接，必须始终连接到主集群 IP 地址而非本地地址。

与 VPN 相关的密钥和证书将被复制到所有设备。

FTP 和集群

- 如果 FTP 数据信道和控制信道流量由不同的集群成员所有，数据信道所有者会将空闲超时更新定期发送到控制信道所有者并更新空闲超时值。但是，如果重新加载控制流量所有者并重新托管控制流量，则不会再保持父/子流量关系；控制流量空闲超时不会更新。
- 如果将 AAA 用于 FTP 访问，则控制信道流量将集中在主设备上。

思科 TrustSec 和集群

只有主设备可获知安全组标记 (SGT) 信息。然后，主设备将向从设备提供 SGT，从设备可根据安全策略为 SGT 作出匹配项决定。

ASA 集群的许可

型号	许可证要求
ASA 5585-X	集群许可证，最多可支持 16 台设备。 每台设备上都需要集群许可证。对于其他功能许可证，集群设备并不要求每台设备上的许可证相同。如果多台设备上有功能许可证，这些许可证将合并成一个 ASA 集群运行许可证。 **注**　每台设备必须拥有相同的加密许可证和相同的 10 GE I/O 许可证。
ASA 5512-X	增强型安全许可证，支持 2 台设备。 **注**　每台设备必须拥有相同的加密许可证。
ASA 5515-X、 ASA 5525-X、 ASA 5545-X 和 ASA 5555-X	基础许可证，支持 2 台设备。 **注**　每台设备必须拥有相同的加密许可证。
所有其他型号	不支持。

ASA 集群的先决条件

ASA 硬件和软件要求

集群中的所有设备：

- 必须为相同型号且 DRAM 相同。闪存的大小不必相同。
- 必须运行相同的软件，映像升级时除外。支持无中断升级。
- 使用独立接口模式时，集群成员可以位于不同的地理位置 （站点间）。
- 必须处于相同的安全情景模式中，无论是单情景模式还是多情景模式。
- （单情景模式）必须处于相同的防火墙模式中，无论是路由模式还是透明模式。
- 在配置复制之前，新的集群成员对初始集群控制链路通信必须使用与主设备相同的 SSL 加密设置 （**ssl encryption** 命令）。
- 必须有相同的集群和加密许可证，ASA 5585-X 还必须有相同的 10 GE I/O 许可证。

交换机先决条件

- 请务必完成交换机配置后再在 ASA 上配置集群。
- 下表列出了支持与 ASA 集群交互操作的外部硬件和软件。

表 8-2　ASA 集群的外部硬件和软件支持

外部硬件	外部软件	ASA 版本
思科 Nexus 9300	思科 NX-OS 6.1(2)I2(1) 及更高版本	9.2(1) 及更高版本
思科 Nexus 7000	思科 NX-OS 5.2(5) 及更高版本	9.0(1) 及更高版本
思科 Nexus 5000	思科 NX-OS 7.0(1) 及更高版本	9.1(4) 及更高版本

表 8-2　ASA 集群的外部硬件和软件支持（续）

外部硬件	外部软件	ASA 版本
带 Supervisor 32、720 和 720-10GE 的 Catalyst 6500	思科 IOS 12.2(33)SXI7、SXI8、SXI9 及更高版本	9.0(1) 及更高版本
Catalyst 3750-X	思科 IOS 15.0(2) 及更高版本	9.1(4) 及更高版本

ASA 先决条件

- 将设备加入管理网络之前，为每台设备提供唯一的 IP 地址。
  - 有关连接到 ASA 并设置管理 IP 地址的详细信息，请参阅“入门”一章。
  - 除用作主设备 （通常为添加到集群中的第一台设备）使用的 IP 地址外，这些管理 IP 地址仅供临时使用。
  - 从设备加入集群后，其管理接口配置将替换为从主设备复制的配置。
- 如要在集群控制链路上使用巨型帧 （推荐），必须在启用集群之前启用巨型帧保留。

其他先决条件

建议使用终端服务器访问所有集群成员设备的控制台端口。为了进行初始设置和持续管理 （例如在设备发生故障时），终端服务器对于远程管理非常有用。

相关主题

- 第 8-29 页的 ASA 集群的指导原则
- 第 9-21 页的启用巨型帧支持
- 第 8-3 页的引导程序配置

ASA 集群的指导原则

情景模式

每台成员设备上的模式必须相符。

防火墙模式

对于单情景模式，所有设备上的防火墙模式必须相符。

故障转移

集群不支持故障转移。

IPv6

集群控制链路只有在使用 IPv4 时才受支持。

型号

支持的型号：

- ASA 5585-X

  如果带 SSP-10 和 SSP-20 的 ASA 5585-X 包含两个万兆以太网接口，建议将一个接口用于集群控制链路，另一个用于数据 （可将子接口用于数据）。尽管此设置无法满足集群控制链路的冗余要求，但可以满足调整集群控制链路使之符合数据接口流量大小的需要。

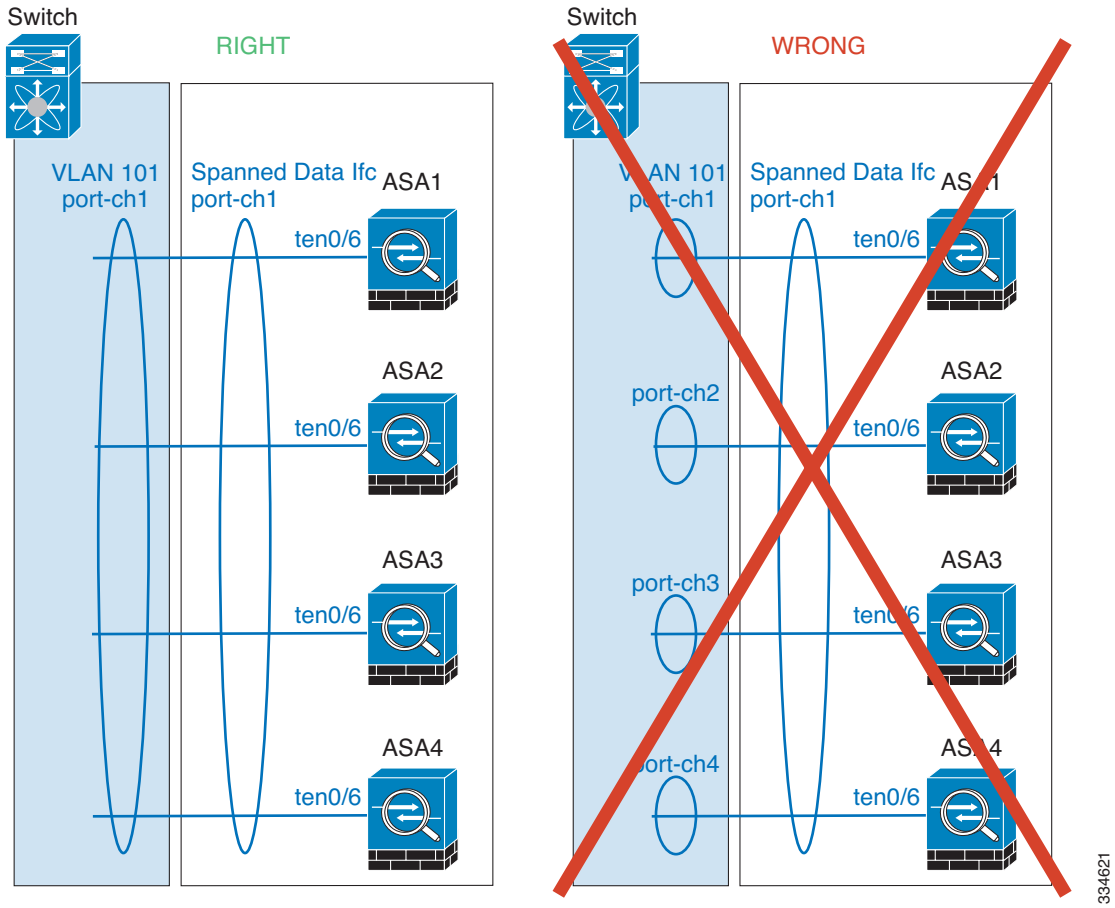
- ASA 5512-X、 ASA 5515-X、 ASA 5525-X、 ASA 5545-X 和 ASA 5555-X

交换机

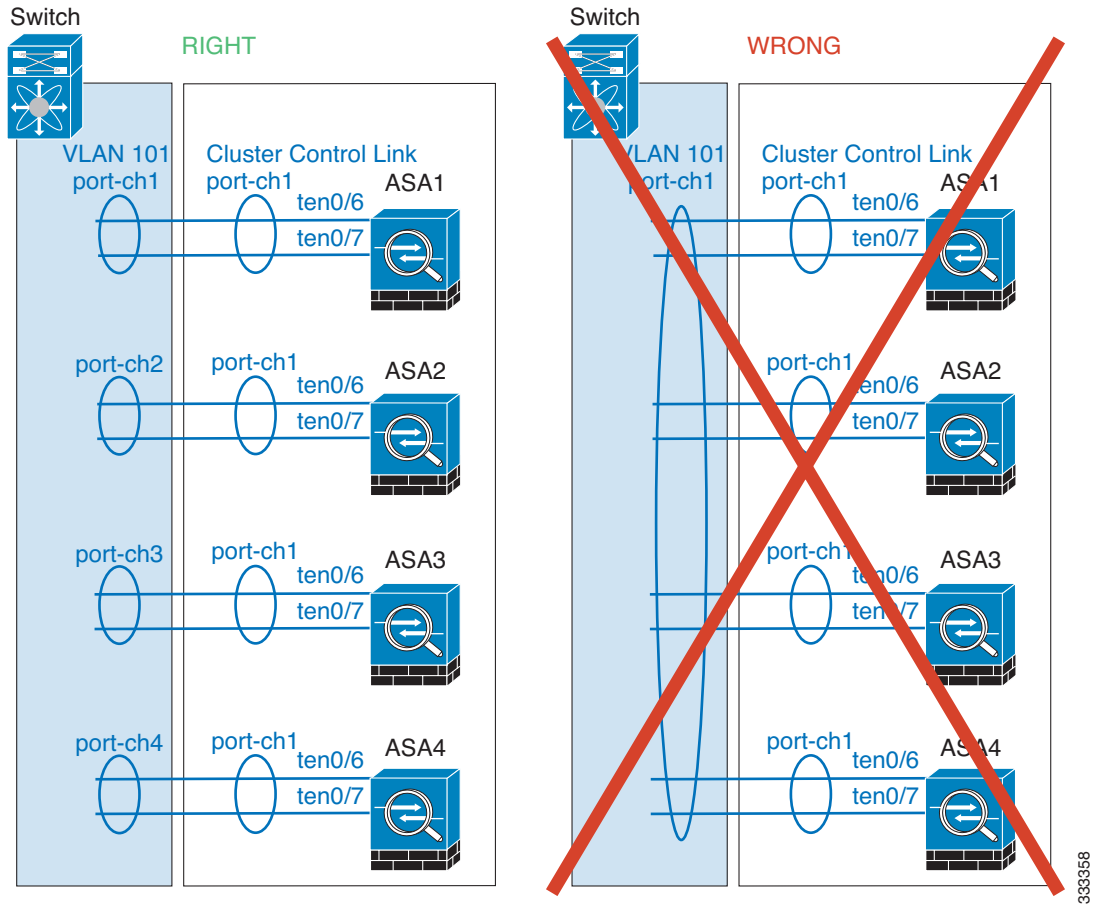
- 在用于集群控制链路接口的交换机上，可以选择在连接到 ASA 的交换机端口上启用生成树 PortFast 来加快新设备加入集群的过程。
- 当交换机上的跨网络 EtherChannel 绑定缓慢时，可以为交换机上的一个独立接口启用快速 LACP 速率。
- 在交换机上，建议使用以下 EtherChannel 负载均衡算法之一：**source-dest-ip** 或 **source-dest-ip-port**（请参阅思科 Nexus OS 和思科 IOS **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中 ASA 的流量分摊不均。*请勿*更改 ASA 上默认的负载均衡算法 （**port-channel load-balance** 命令中）。
- 如果在交换机上更改 EtherChannel 的负载均衡算法，交换机上的 EtherChannel 接口将暂时停止转发流量，生成树协议重新启动。在流量再次开始传输之前会存在延迟。
- 应该在所有面向集群的 EtherChannel 接口上为思科 Nexus 交换机禁用 LACP Graceful Convergence 功能。
- 有些交换机不支持 LACP 动态端口优先级 （活动链路和备用链路）。您可以禁用动态端口优先级，使跨网络 EtherChannel 具有更高兼容性。
- 集群控制链路路径上的网络要素不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。
- 端口通道绑定中断时间不得超过配置的 keepalive 间隔。

EtherChannel

- ASA 不支持将 EtherChannel 连接到交换机堆叠。如果跨堆叠连接 ASA EtherChannel，则当主交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。
- 跨网络与 设备本地 EtherChannel 的配置 - 请务必为交换机进行正确的跨网络 EtherChannel 与设备本地 EtherChannel 配置。
  - 跨网络 EtherChannel - 对于跨越所有集群成员的 ASA *跨网络* EtherChannel，所有接口在交换机上合并为一个 EtherChannel。请确保每个接口都属于交换机上的同一个通道组。



– 设备本地 EtherChannel - 对于 ASA *设备本地* EtherChannel，包括为集群控制链路配置的任何 EtherChannel，请务必在交换机上配置分散的 EtherChannel；请勿在交换机上将多个 ASA EtherChannel 合并为一个 EtherChannel。



其他指导原则

- 当拓扑结构发生显著更改时（例如添加或删除 EtherChannel 接口，启用或禁用 ASA 或交换机上的接口，添加额外的交换机形成 VSS 或 vPC），应禁用运行状况检查功能。当拓扑结构更改完成且配置更改已同步到所有设备后，可以重新启用运行状况检查功能。
- 将设备添加到现有集群时或重新加载设备时，会有限地暂时丢弃数据包/断开连接；这是预期行为。有些时候，丢弃的数据包会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包将使 FTP 客户端挂起。在此情况下，需要重新建立 FTP 连接。
- 如果使用连接到跨网络 EtherChannel 的 Windows 2003 服务器，当系统日志服务器端口关闭且服务器没有限制 ICMP 错误信息时，将会有大量 ICMP 消息被发送回 ASA 集群。这些消息会导致 ASA 集群的某些设备 CPU 使用率极高，进而影响性能。因此，建议限制 ICMP 错误信息。

相关主题

- 第 8-6 页的调整集群控制链路的吞吐量大小
- 第 8-3 页的引导程序配置
- 第 8-22 页的集群不支持的功能
- 第 9-17 页的配置 EtherChannel
- 第 9-11 页的 EtherChannel 准则

ASA 集群的默认设置

- 使用跨网络 EtherChannel 时，将自动生成 cLACP 系统 ID 且系统优先级默认为 1。
- 集群运行状况检查功能默认启用，保持时间为 3 秒。
- 连接再均衡默认禁用。如果启用连接再均衡，交换负载信息的默认间隔时间为 5 秒。

配置 ASA 集群

注　如要启用或禁用集群，必须使用控制台连接 （适用于 CLI）或 ASDM 连接。

如要配置集群，请执行以下任务：

步骤 1　按照第 8-28 页的 ASA 集群的先决条件和第 8-29 页的 ASA 集群的指导原则，在交换机和 ASA 上完成所有预配置。

步骤 2　第 8-33 页的使用电缆连接集群设备并配置上游和下游设备。

步骤 3　第 8-35 页的在每台设备上配置集群接口模式。只能为集群配置一种类型的接口：跨网络 EtherChannel 或独立接口。

步骤 4　第 8-35 页的在主设备上配置接口。如果接口未准备好加入集群，则无法启用集群。

步骤 5　第 8-41 页的配置主设备引导程序设置。

步骤 6　第 8-46 页的配置从设备引导程序设置。

步骤 7　在主设备上配置安全策略。如要在主设备上配置支持的功能，请参阅本指南中的相关章节。配置将被复制到从设备。

使用电缆连接集群设备并配置上游和下游设备

在配置集群之前，需要先使用电缆连接集群控制链路网络、管理网络和数据网络。

注　在配置要加入集群的设备之前，至少需要有一个活动的集群控制链路网络。

此外，还应该配置上游和下游设备。例如，如果使用 EtherChannel，则应为上游和下游设备进行 EtherChannel 配置。

示例

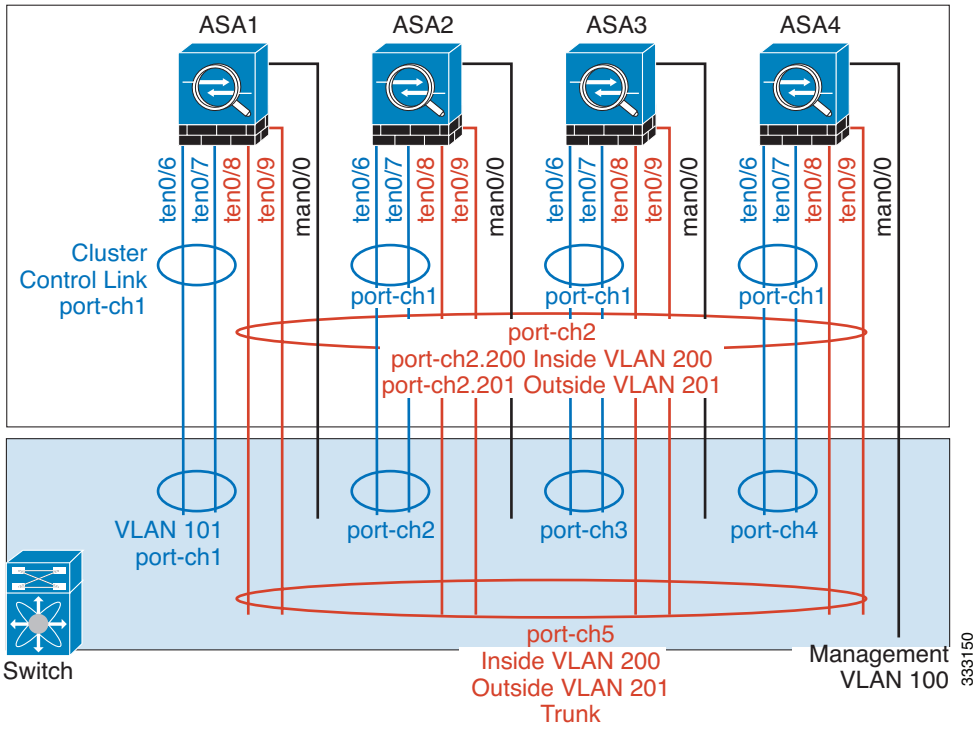
注　本示例使用 EtherChannel 进行负载均衡。如果使用 PBR 或 ECMP，交换机配置会有所不同。

例如，在这 4 台 ASA 5585-X 中，每一台都需要：

- 将设备本地 EtherChannel 中的 2 个万兆以太网接口用于集群控制链路。

- 将跨网络 EtherChannel 中的 2 个万兆以太网接口用于内部和外部网络；每个接口都是 EtherChannel 的 VLAN 子接口。使用子接口可以让内部和外部接口都能充分利用 EtherChannel 的优点。
- 使用 1 个管理接口。

将一台交换机用于内部和外部网络。



用途	逐一连接 4 台 ASA 上的接口	连接到交换机端口
集群控制链路	TenGigabitEthernet 0/6 和 TenGigabitEthernet 0/7	总计 8 个端口 对于每一对 TenGigabitEthernet 0/6 和 TenGigabitEthernet 0/7 接口，配置 4 个 EtherChannel（每台 ASA 1 个 EC）。 这些 EtherChannel 必须全部位于同一个独立的集群控制 VLAN 中，例如 VLAN 101。
内部和外部接口	TenGigabitEthernet 0/8 和 TenGigabitEthernet 0/9	总计 8 个端口 配置一个 EtherChannel（跨所有 ASA）。 现在，在交换机上配置这些 VLAN 和网络；例如配置一个中继，其中 VLAN 200 用于内部而 VLAN 201 用于外部。
管理接口	Management 0/0	总计 4 个端口 将所有接口都放入同一个独立的管理 VLAN 中，例如 VLAN 100。

在每台设备上配置集群接口模式

只能为集群配置一种类型的接口：跨网络 EtherChannel 或独立接口；不能在集群中混合使用不同的接口类型。

准备工作

- 必须在要添加到集群中的每台 ASA 上分别设置模式。
- 您始终可以将管理专用接口配置为独立接口 （推荐），即使是在跨网络 EtherChannel 模式中亦如此。即使是在透明防火墙模式中，管理接口也可以是独立接口。
- 在跨网络 EtherChannel 模式中，如果将管理接口配置为独立接口，将无法为管理接口启用动态路由。您必须使用静态路由。
- 在多情景模式中，必须为所有情景选择一种接口类型。例如，如果使用透明和路由模式的混合情景，则必须将跨网络 EtherChannel 模式用于所有情景，因为这是透明模式允许的唯一接口类型。

操作步骤

步骤 1　显示任何不兼容的配置，以便稍后强制设置接口模式并修复配置；该模式不会随以下命令而更改：

cluster interface-mode {**individual** | **spanned**} **check-details**

示例：

```
ciscoasa(config)# cluster interface-mode spanned check-details
```

步骤 2　为集群设置接口模式：

cluster interface-mode {**individual** | **spanned**} **force**

示例：

```
ciscoasa(config)# cluster interface-mode spanned force
```

不存在默认设置；您必须明确选择模式。如果尚未设置模式，则无法启用集群。

force 选项可直接更改模式而无需检查配置中是否存在不兼容的设置。更改模式后，需要手动修复任何配置问题。由于任何接口配置都只能在设置完模式后修复，因此我们建议使用 **force** 选项，这样您至少可以从现有配置着手。设置模式后，可以重新运行 **check-details** 选项来获得更多参考信息。

如果不使用 **force** 选项，当存在任何不兼容的配置时，系统将提示您清除配置并重新加载，从而需要您连接到控制台端口来重新配置管理访问。如果您的配置兼容 （极为罕见），则会更改模式并保留配置。如果不想清除配置，可以键入 **n** 退出命令。

要删除接口模式，请输入 **no cluster interface-mode** 命令。

在主设备上配置接口

启用集群*之前*，必须修改所有当前配置了 IP 地址的接口，使其准备好加入集群。至于其他接口，可以在启用集群之前或之后配置；我们建议预配置所有接口，以便将完整的配置同步到新的集群成员。

本节介绍如何将接口配置为与集群兼容。可以将数据接口配置为跨网络 EtherChannel 或独立接口。每种方法使用的负载均衡机制不同。在同一个配置中不能配置两种接口类型，只有管理接口除外，它即使在跨网络 EtherChannel 模式中也可以是独立接口。

- 第 8-36 页的配置独立接口 （管理接口的推荐配置）
- 第 8-38 页的配置跨网络 EtherChannel

相关主题

- 第 8-3 页的集群接口

配置独立接口 （管理接口的推荐配置）

独立接口是正常的路由接口，每个接口都从 IP 地址池获取自己的 IP 地址。集群的主集群 IP 地址是集群的固定地址，始终属于当前的主设备。

在跨网络 EtherChannel 模式中，建议将管理接口配置为独立接口。独立的管理接口可以根据需要直接连接到每台设备，而跨网络 EtherChannel 接口则只允许连接到当前的主设备。

准备工作

- 除管理专用接口之外，您必须处于独立接口模式中。
- 对于多情景模式，请在每个情景下执行本操作步骤。如果尚未进入情景配置模式，请输入 **changeto context** *name* 命令。
- 独立接口要求在邻居设备上配置负载均衡。管理接口不需要外部负载均衡。
- （可选）将接口配置为设备本地 EtherChannel 接口、冗余接口并/或配置子接口。
  - 如果配置为 EtherChannel，此 EtherChannel 是设备本地的，而非跨网络 EtherChannel。
  - 管理专用接口不能作为冗余接口。

操作步骤

步骤 1　配置本地 IP 地址池 （IPv4 和/或 IPv6），其中一个地址将被分配到每个集群设备作为接口地址：

(IPv4)

ip local pool *poolname first-address-last-address* [**mask** *mask*]

(IPv6)

ipv6 local pool *poolname ipv6-address/prefix-length number_of_addresses*

示例：

```
ciscoasa(config)# ip local pool ins 192.168.1.2-192.168.1.9
ciscoasa(config-if)# ipv6 local pool insipv6 2001:DB8::1002/32 8
```

至少包含与集群中的设备数量相同的地址。如果计划扩展集群，则应包含更多地址。属于当前主设备的主集群 IP 地址*不*在此地址池中；请务必在同一个网络中为主集群 IP 地址保留一个 IP 地址。

您无法预先确定分配到每台设备的确切本地地址；如要查看每台设备上使用的地址，请输入 **show ip[v6] local pool** *poolname* 命令。每个集群成员在加入集群时都会分配到一个成员 ID。此 ID 决定了所用的来自地址池中的本地 IP。

步骤 2　进入接口配置模式：

interface *interface_id*

示例：

```
ciscoasa(config)# interface tengigabitethernet 0/8
```

步骤 3　（仅适用于管理接口）将一个接口设置为管理专用模式，确保不会有流量流经该接口：

management-only

默认情况下，管理类型的接口被配置为管理专用。在透明模式中，此命令对管理类型的接口始终启用。

如果集群接口模式为跨网络，则必须配置此设置。

步骤 4　为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside
```

name 是文本字符串，最长 48 个字符且不区分大小写。使用一个新值重新输入此命令可更改名称。

步骤 5　设置主集群 IP 地址并确定集群池：

(IPv4)

ip address *ip_address* [*mask*] **cluster-pool** *poolname*

(IPv6)

ipv6 address *ipv6-address/prefix-length* **cluster-pool** *poolname*

示例：

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ciscoasa(config-if)# ipv6 address 2001:DB8::1002/32 cluster-pool insipv6
```

此 IP 地址必须与集群池地址属于同一个网络，但不在地址池中。您可以配置 IPv4 和/或 IPv6 地址。

不支持 DHCP、 PPPoE 和 IPv6 自动配置；必须手动配置 IP 地址。

步骤 6　设置安全级别，其中 *number* 为 0（最低）到 100（最高）之间的整数：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 100
```

步骤 7　启用接口：

no shutdown

示例

以下示例将 Management 0/0 和 Management 0/1 接口配置为设备本地 EtherChannel，然后将 EtherChannel 配置为独立接口：

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8

interface management 0/0
    channel-group 1 mode active
    no shutdown

interface management 0/1
    channel-group 1 mode active
    no shutdown
```

```
interface port-channel 1
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8:45:1001/64 cluster-pool mgmtipv6
    security-level 100
    management-only
```

相关主题

- 第 8-10 页的管理接口
- 第 8-35 页的在每台设备上配置集群接口模式
- 第 8-11 页的负载均衡方法
- 第 9-17 页的配置 EtherChannel
- 第 9-15 页的配置冗余接口
- 第 9-20 页的配置 VLAN 子接口和 802.1Q 中继
- 第 11-1 页的安全级别

配置跨网络 EtherChannel

跨网络 EtherChannel 跨越集群中的所有 ASA，并在 EtherChannel 操作的过程中提供负载均衡。

准备工作

- 必须处于跨网络 EtherChannel 接口模式中。
- 对于多情景模式，请在系统执行空间中开始本操作步骤。如果尚未进入系统配置模式，请输入 **changeto system** 命令。
- 对于透明模式，请配置网桥组。
- *请勿*指定 EtherChannel 中的最大和最小链路数 - 建议不要在 ASA 或交换机上指定 EtherChannel 中的最大和最小链路数（**lacp max-bundle** 和 **port-channel min-bundle** 命令）。如果需要使用这些设置，请注意以下事项：
  - 在 ASA 上设置的最大链路数是整个集群的活动端口总数。请确保在交换机上配置的最大链路数值不超过 ASA 值。
  - 在 ASA 上设置的最小链路数是*每台设备*启用一个端口通道接口所需的最小活动端口数。在交换机上，最小链路数是整个集群中的最小链路数，所以此值与 ASA 值不符。
- *请勿*更改默认的负载均衡算法（请参阅 **port-channel load-balance** 命令）。在交换机上，建议使用以下算法之一：**source-dest-ip** 或 **source-dest-ip-port**（请参阅思科 Nexus OS 和思科 IOS **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中 ASA 的流量分摊不均。
- 跨网络 EtherChannel 不使用 **lacp port-priority** 和 **lacp system-priority** 命令。
- 使用跨网络 EtherChannel 时，端口通道接口在集群完全启用之前不会进入工作状态。此要求可防止将流量转发到集群中并非处于活动状态的设备。

操作步骤

步骤 1　指定要添加到通道组的接口：

interface *physical_interface*

示例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID 包含类型、插槽和端口号作为 *type slot/port*。通道组中的第一个接口决定了该组中所有其他接口的类型和速度。

步骤 2　将此接口分配到 EtherChannel：

channel-group *channel_id* **mode active** [**vss-id** {**1** | **2**}]

示例：

```
ciscoasa(config-if)# channel-group 1 mode active
```

channel_id 的值为 1 到 48。如果配置中尚没有此通道 ID 的端口通道接口，将自动添加一个接口：

interface port-channel *channel_id*

跨网络 EtherChannel 只支持 **active** 模式。

如果将 ASA 连接到 VSS 或 vPC 中的两台交换机，请配置 **vss-id** 关键字来确定要将此接口连接到哪台交换机 （1 还是 2）。此外，还必须在步骤 6 中对端口通道接口使用 **port-channel span-cluster vss-load-balance** 命令。

步骤 3　启用接口：

no shutdown

步骤 4　（可选）重复步骤 3 至步骤 1，将更多接口添加到 EtherChannel。

示例：

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# no shutdown
```

每台设备在 EtherChannel 中有多个接口对于连接到 VSS 或 vPC 中交换机的情况非常有用。请注意，在默认情况下，跨网络 EtherChannel 最多只能将所有集群成员的 16 个接口中的 8 个作为活动接口；其余 8 个接口备用，以防链路发生故障。如要使用 8 个以上的活动接口 （但没有备用接口），请使用 **clacp static-port-priority** 命令禁用动态端口优先级。禁用动态端口优先级时，最多可在整个集群中使用 32 条活动链路。例如，对于由 16 台 ASA 组成的集群，每台 ASA 上最多可以使用 2 个接口，跨网络 EtherChannel 中共有 32 个接口。

步骤 5　指定端口通道接口：

interface port-channel *channel_id*

示例：

```
ciscoasa(config)# interface port-channel 1
```

在将接口添加到通道组时，将自动创建此接口。

步骤 6　将此 EtherChannel 设置为跨网络 EtherChannel：

port-channel span-cluster [**vss-load-balance**]

示例：

```
ciscoasa(config-if)# port-channel span-cluster
```

如果准备将 ASA 连接到 VSS 或 vPC 中的两台交换机，则应使用 **vss-load-balance** 关键字启用 VSS 负载均衡。此功能可确保 ASA 与 VSS（或 vPC）对之间的物理链路连接达到均衡。在启用负载均衡之前，必须在 **channel-group up** 命令中为每个成员接口配置 **vss-id** 关键字（请参阅步骤 2）。

步骤 7　（可选）您可以为端口通道接口设置以太网属性，覆盖独立接口上设置的属性。

此方法提供了设置这些参数的快捷键，因为通道组中所有接口的这些参数必须匹配。

步骤 8　（可选）如果准备在此 EtherChannel 上创建 VLAN 子接口，请立即执行此操作。

示例：

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

本操作步骤的其余部分适用于子接口。

步骤 9　（多情景模式）将接口分配到情景。然后输入：

changeto context *name*
interface port-channel *channel_id*

示例：

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

对于多情景模式，其余的接口配置将在每个情景中完成。

步骤 10　为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside
```

name 是文本字符串，最长 48 个字符且不区分大小写。使用一个新值重新输入此命令可更改名称。

步骤 11　根据防火墙模式，执行以下操作之一。

- 路由模式 - 设置 IPv4 和/或 IPv6 地址：

  (IPv4)

  ip address *ip_address* [*mask*]

  (IPv6)

  ipv6 address *ipv6-prefix/prefix-length*

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
  ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
  ```

  不支持 DHCP、 PPPoE 和 IPv6 自动配置。

- 透明模式 - 将接口分配到网桥组：

  bridge-group *number*

  示例：

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

  number 为 1 到 100 之间的整数。最多可将四个接口分配到网桥组。不能将同一个接口分配到多个网桥组。请注意，BVI 配置包含 IP 地址。

步骤 12　设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 为 0（最低）到 100（最高）之间的整数。

步骤 13　为跨网络 EtherChannel 配置 MAC 地址，使 MAC 地址不会在当前主设备退出集群时更改：

mac-address *mac_address*

示例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

如果是手动配置的 MAC 地址，该 MAC 地址将始终属于当前的主设备。在多情景模式中，如果不同情景之间共享接口，将默认启用自动生成 MAC 地址，因此若要禁用自动生成，只需为共享接口手动设置 MAC 地址即可。请注意，必须为非共享接口手动配置 MAC 地址。

mac_address 的格式为 H.H.H，其中 H 是 16 位十六进制数字。例如，MAC 地址 00-0C-F1-42-4C-DE 需要输入 000C.F142.4CDE。

如果您还想使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。

相关主题

- 第 8-35 页的在每台设备上配置集群接口模式
- 第 12-6 页的配置网桥组
- 第 8-41 页的配置主设备引导程序设置
- 第 9-17 页的配置 EtherChannel
- 第 9-11 页的 EtherChannel 准则
- 第 8-12 页的连接到 VSS 或 vPC
- 第 9-13 页的启用物理接口并配置以太网参数
- 第 9-20 页的配置 VLAN 子接口和 802.1Q 中继
- 第 6-18 页的配置安全情景
- 第 11-1 页的安全级别
- 第 8-29 页的 ASA 集群的指导原则

配置主设备引导程序设置

集群中的每台设备都需要有引导程序配置才能加入集群。通常，第一台配置为加入集群的设备会成为主设备。启用集群后，集群会在选举时间结束后选举出一台主设备。由于集群中最初只有一台设备，因此该设备将成为主设备。添加到集群中的后续设备将成为从设备。

准备工作

- 您必须使用控制台端口来启用或禁用集群。不能使用 Telnet 或 SSH。
- 请备份配置，以防稍后要退出集群而需要恢复配置。
- 对于多情景模式，请在系统执行空间中完成这些操作步骤。如要从该情景切换至系统执行空间，请输入 **changeto system** 命令。

- 建议启用巨型帧保留用于集群控制链路。
- 除集群控制链路外，配置中的任何接口都必须根据接口模式使用集群 IP 池进行配置，或者配置为跨网络 EtherChannel，然后才能启用集群。如果有以前就存在的接口配置，您可以清除该接口配置 (**clear configure interface**)，也可以将接口转换为集群接口后再启用集群。
- 将设备添加到正在运行的集群时，可能会有限地暂时丢弃数据包/断开连接；这是预期行为。
- 确定集群控制链路的吞吐量大小。

操作步骤

步骤 1　加入集群之前，先启用集群控制链路接口。

稍后，您要在启用集群时将此接口确定为集群控制链路。

如果有足够的接口，建议将多个集群控制链路接口合并为一个 EtherChannel。此 EtherChannel 是 ASA 本地的，而非跨网络 EtherChannel。

集群控制链路接口配置不会从主设备复制到从设备；但是，您必须在每台设备上使用相同的配置。由于此配置不会复制，您必须在每台设备上分别配置集群控制链路接口。

- VLAN 子接口不能用作集群控制链路。
- 管理 *x*/*x* 接口 （无论是作为独立接口还是作为 EtherChannel），都不能用作集群控制链路。
- 对于带 ASA IPS 模块的 ASA 5585-X，不能将模块的接口用于集群控制链路。

a. 进入接口配置模式：

interface *interface_id*

示例：

```
ciscoasa(config)# interface tengigabitethernet 0/6
```

b. （可选，适用于 EtherChannel）将此物理接口分配到 EtherChannel：

channel-group *channel_id* **mode on**

示例：

```
ciscoasa(config-if)# channel-group 1 mode on
```

channel_id 的值为 1 到 48。如果配置中尚没有此通道 ID 的端口通道接口，将自动添加一个接口：

interface port-channel *channel_id*

建议对集群控制链路成员接口使用 ON 模式来减少集群控制链路上不必要的流量。集群控制链路不需要 LACP 流量开销，因为它是独立和稳定的网络。**注：**建议将*数据* EtherChannel 设置为 Active 模式。

c. 启用接口：

no shutdown

只需要启用接口；不要为接口配置名称或任何其他参数。

d. （适用于 EtherChannel）对每个要添加到 EtherChannel 的其他接口重复此操作：

示例：

```
ciscoasa(config)# interface tengigabitethernet 0/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

步骤 2　（可选）为集群控制链路接口指定最大传输单位：

mtu cluster *bytes*

示例：

```
ciscoasa(config)# mtu cluster 9000
```

设置值为 64 到 65,535 字节的 MTU。默认 MTU 为 1500 字节。

建议将 MTU 设置为 1600 字节或更大值，这需要启用巨型帧保留后再继续本操作步骤。巨型帧保留需要重新加载 ASA。

此命令是全局配置命令，但是也属于不会在设备之间复制的引导程序配置。

步骤 3　为集群命名并进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

名称必须是长度为 1 到 38 个字符的 ASCII 字符串。每台设备只能配置一个集群组。所有集群成员都必须使用同一个名称。

步骤 4　为此集群成员命名：

local-unit *unit_name*

```
ciscoasa(cfg-cluster)# local-unit unit1
```

使用唯一的 ASCII 字符串，长度必须为 1 到 38 个字符。每台设备必须有一个唯一的名称。集群中不允许存在名称重复的设备。

步骤 5　指定集群控制链路接口，最好是 EtherChannel：

cluster-interface *interface_id* **ip** *ip_address mask*

示例：

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.1 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

不允许指定子接口和管理接口。

指定 IPv4 地址作为 IP 地址；此接口不支持 IPv6。此接口不能配置 **nameif**。

为每台设备指定属于同一个网络的不同 IP 地址。

步骤 6　设置此设备用于主设备选举的优先级：

priority *priority_number*

示例：

```
ciscoasa(cfg-cluster)# priority 1
```

优先级的值为 1 到 100，其中 1 为最高优先级。

步骤 7　（可选）设置身份验证密钥以便控制集群控制链路上的流量：

key *shared_secret*

示例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

共享密钥是长度为 1 到 63 个字符的 ASCII 字符串。共享密钥用于生成密钥。此命令不影响数据路径流量，包括始终以明文发送的连接状态更新和转发数据包。

步骤 8　（可选）自定义集群运行状况检查功能，该功能包括设备运行状况监控和接口运行状况监控：

health-check [**holdtime** *timeout*] [**vss-enabled**]

示例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

holdime 用于确定设备 keepalive 状态消息的间隔时间，其值为 .8 到 45 秒；默认值为 3 秒。请注意，保持时间值只影响*设备*运行状况检查；对于接口运行状况，ASA 使用接口状态（打开或关闭）。

为了确定设备运行状况，ASA 集群设备会在集群控制链路上将 keepalive 消息发送到其他设备。如果设备在保持时间内未收到来自对等设备的任何 keepalive 消息，则会认为该对等设备没有响应或已损坏。如果将集群控制链路配置为 EtherChannel（推荐），而且链路连接到 VSS 或 vPC 对，则可能需要启用 **vss-enabled** 选项。对某些交换机而言，当 VSS/vPC 中的一台设备正在关闭或启动时，连接到这些交换机的 EtherChannel 成员接口可能看似对 ASA 打开，但在交换机端却并未传输流量。如果将 ASA 保持时间超时设置为比较小的值（例如 .8 秒），而 ASA 在这些 EtherChannel 接口中的一个接口上发送 keepalive 消息，ASA 可能会被错误地从集群中删除。启用 **vss-enabled** 时，ASA 将在集群控制链路中的所有 EtherChannel 接口上泛洪 keepalive 消息，以确保至少有一台交换机可以收到这些消息。

接口运行状况检查将监控链路故障。如果特定设备上的一个接口发生故障，但其他设备上的相同接口处于活动状态，则会从集群中删除该设备。 ASA 在多长时间后从集群中删除成员取决于接口的类型以及该设备是既定成员还是正在加入集群的设备。

运行状况检查默认启用。您可以使用此命令的 **no** 形式将其禁用。

当拓扑结构发生任何更改时 （例如添加或删除数据接口，启用或禁用 ASA 或交换机上的接口，或者添加额外的交换机形成 VSS 或 vPC），应禁用运行状况检查功能。当拓扑结构更改完成且配置更改已同步到所有设备后，可以重新启用运行状况检查功能。

步骤 9　（可选）为 TCP 流量启用连接再均衡：

conn-rebalance [**frequency** *seconds*]

示例：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

此命令默认禁用。如果已启用， ASA 会定期交换负载信息，并将新连接从负载较高的设备分担给负载较低的设备。此频率的值为 1 到 360 秒，用于指定多长时间交换一次负载信息。默认值为 5 秒。

请勿为站点间拓扑结构配置连接再均衡；您不需要将连接再均衡到位于不同站点的集群成员。

步骤 10　（可选）启用从设备到主设备的控制台复制：

console-replicate

此功能默认禁用。对于特定的重要事件，ASA 会将某些消息直接打印输出到控制台。如果启用了控制台复制，从设备会将控制台消息发送到主设备，因此您只需要监控集群的一个控制台端口。

步骤 11　（可选）禁用 LACP 中的动态端口优先级：

clacp static-port-priority

有些交换机不支持动态端口优先级，所以此命令可提高交换机兼容性。此外，它还能支持 8 个以上的活动跨网络 EtherChannel 成员，最多可支持 32 个成员。如果不使用此命令，则只能支持 8 个活动成员和 8 个备用成员。如果启用此命令，则无法使用任何备用成员；所有成员都是活动成员。

步骤 12　（可选）手动指定 cLACP 系统 ID 和系统优先级：

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

示例：

```
ciscoasa(cfg-cluster)# clacp system-mac 000a.0000.aaaa
```

使用跨网络 EtherChannel 时，ASA 使用 cLACP 与邻居交换机协商 EtherChannel。集群中的 ASA 在 cLACP 协商中协作，使其在交换机看来就好似一台 （虚拟）设备。 cLACP 协商中的一个参数是 MAC 地址格式的系统 ID。集群中的所有 ASA 都使用同一个系统 ID：由主设备 （默认）自动生成并复制到所有从设备；也可以在此命令中按照 *H.H.H* 的格式手动指定，其中 H 是 16 位十六进制数字。（例如， MAC 地址 00-0A-00-00-AA-AA 需要输入 000A.0000.AAAA。）例如，您可能出于排除故障的目的而要手动配置 MAC 地址，以便使用易于识别的 MAC 地址。通常情况下，您会使用自动生成的 MAC 地址。

系统优先级的值为 1 到 65535，用于确定哪台设备负责作出绑定决定。默认情况下，ASA 使用优先级 1，这是最高优先级。此优先级需要高于交换机上的优先级。

此命令是从主设备复制到从设备的，并非引导程序配置的一部分。但是在启用集群后，您将无法更改此值。

步骤 13　启用集群：

enable [**noconfirm**]

示例：

```
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands?[Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

输入 **enable** 命令时，ASA 将扫描正在运行的配置，查找集群不支持的功能的不兼容命令，包括默认配置中可能存在的命令。系统将提示您删除不兼容的命令。如果回答 **No**，则不会启用集群。使用 **noconfirm** 关键字可绕过确认并自动删除不兼容的命令。

启用第一台设备后，将进行主设备选举。由于第一台设备应该是截至目前为止唯一的集群成员，因此它将成为主设备。请勿在此期间执行任何配置更改。

如要禁用集群，请输入 **no enable** 命令。

注　如果禁用集群，所有数据接口都将关闭；只有管理专用接口处于活动状态。

示例

以下示例先配置管理接口，再为集群控制链路配置设备本地 EtherChannel，然后是名为“unit1”的 ASA 启用集群，由于该设备是第一台添加到集群的设备，因此将成为主设备。

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
```

```
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown

interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown

interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown

cluster group pod1
    local-unit unit1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

相关主题

- 第 9-21 页的启用巨型帧支持
- 第 8-35 页的在主设备上配置接口
- 第 8-6 页的调整集群控制链路的吞吐量大小
- 第 8-3 页的主设备选举
- 第 8-8 页的接口监控
- 第 8-50 页的退出集群

配置从设备引导程序设置

执行以下操作步骤配置从设备。

准备工作

- 您必须使用控制台端口来启用或禁用集群。不能使用 Telnet 或 SSH。
- 请备份配置，以防稍后要退出集群而需要恢复配置。
- 对于多情景模式，请在系统执行空间中完成本操作步骤。要从该情景切换至系统执行空间，请输入 **changeto system** 命令。
- 建议启用巨型帧保留用于集群控制链路。
- 如果配置中存在任何尚未进行集群配置的接口 （例如，默认配置的 Management 0/0 接口），可以作为从设备加入集群 （不可能在当前选举中成为主设备）。
- 将设备添加到正在运行的集群时，可能会有限地暂时丢弃数据包/断开连接；这是预期行为。

操作步骤

步骤 1　配置集群控制链路接口，其必须与您为主设备配置的接口相同。

示例：

```
ciscoasa(config)# interface tengigabitethernet 0/6
ciscoasa(config-if)# channel-group 1 mode on
```

```
ciscoasa(config-if)# no shutdown
ciscoasa(config)# interface tengigabitethernet 0/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

步骤 2　指定 MTU，其必须与您为主设备配置的 MTU 相同：

示例：

```
ciscoasa(config)# mtu cluster 9000
```

步骤 3　确定集群名称，其必须与您为主设备配置的集群名称相同：

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 4　用唯一的字符串为此集群成员命名：

local-unit *unit_name*

示例：

```
ciscoasa(cfg-cluster)# local-unit unit2
```

指定长度为 1 到 38 个字符的 ASCII 字符串。

每台设备必须有一个唯一的名称。集群中不允许存在名称重复的设备。

步骤 5　指定集群控制链路接口，其必须与您为主设备配置的接口相同，但是要为每台设备指定属于同一个网络的不同 IP 地址：

cluster-interface *interface_id* **ip** *ip_address mask*

示例：

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.2 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

指定 IPv4 地址作为 IP 地址；此接口不支持 IPv6。此接口不能配置 **nameif**。

步骤 6　设置此设备用于主设备选举的优先级，通常设置为比主设备优先级值大的值：

priority *priority_number*

示例：

```
ciscoasa(cfg-cluster)# priority 2
```

设置值为 1 到 100 的优先级，其中 1 为最高优先级。

步骤 7　设置一个身份验证密钥，使其与您为主设备设置的密钥相同：

示例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

步骤 8　启用集群：

enable as-slave

使用 **enable as-slave** 命令可避免任何配置不兼容（主要是任何尚未进行集群配置的接口的存在）。此命令可确保加入集群的从设备不可能在任何当前选举中成为主设备。其配置会被从主设备同步的配置所覆盖。

要禁用集群，请输入 **no enable** 命令。

注　如果禁用集群，所有数据接口都将关闭；只有管理接口处于活动状态。

示例

以下示例包括从设备 unit2 的配置：

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown

interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown

cluster group pod1
    local-unit unit2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

相关主题

- 第 9-21 页的启用巨型帧支持
- 第 8-3 页的主设备选举
- 第 8-50 页的退出集群

管理 ASA 集群成员

部署集群后，可以更改配置和管理集群成员。

- 第 8-48 页的成为非活动成员
- 第 8-49 页的停用成员
- 第 8-50 页的退出集群
- 第 8-51 页的更改主设备
- 第 8-51 页的在集群范围执行命令

成为非活动成员

如要成为集群的非活动成员，请在设备上禁用集群，同时保持集群配置不变。

注　当 ASA 处于非活动状态时 （无论是通过手动设置还是因运行状况检查失败），所有数据接口关闭；只有管理专用接口可以发送和接收流量。要恢复流量传输，请重新启用集群；或者，您也可以从集群中完全删除该设备。管理接口将保持打开，使用设备从集群 IP 池接收的 IP 地址。但是，如果您重新加载而设备在集群中仍然处于非活动状态，管理接口将无法访问 （因为它届时将使用与主设备相同的主 IP 地址）。您必须使用控制台端口来进行任何进一步配置。

准备工作

- 您必须使用控制台端口；不能通过远程 CLI 连接启用或禁用集群。
- 对于多情景模式，请在系统执行空间中执行本操作步骤。如果尚未进入系统配置模式，请输入 **changeto system** 命令。

操作步骤

步骤 1　进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2　禁用集群：

no enable

如果此设备是主设备，此时将选举新的主设备，另一个成员将成为主设备。

集群配置保持不变，因此您可于稍后再次启用集群。

相关主题

- 第 8-50 页的退出集群

停用成员

如要从任何设备停用成员，请执行以下步骤。

注　当 ASA 处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。如要恢复流量传输，请重新启用集群；或者，您也可以从集群中完全删除该设备。管理接口将保持打开，使用设备从集群 IP 池接收的 IP 地址。但是，如果您重新加载而设备在集群中仍然处于非活动状态，管理接口将无法访问 （因为它届时将使用与主设备相同的主 IP 地址）。您必须使用控制台端口来进行任何进一步配置。

准备工作

对于多情景模式，请在系统执行空间中执行本操作步骤。如果尚未进入系统配置模式，请输入 **changeto system** 命令。

操作步骤

步骤 1　从集群中删除该设备：

cluster remove unit *unit_name*

示例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2
```

```
ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2.To bring it back
to the cluster please logon to that unit and re-enable clustering
```

引导程序配置保持不变，从主设备同步的最新配置也保持不变，因此您可于稍后重新添加该设备而不会丢失配置。如果在从设备上输入此命令删除主设备，将会选举新的主设备。

如要查看成员名称，请输入 **cluster remove unit ?**，或输入 **show cluster info** 命令。

相关主题

- 第 8-50 页的退出集群

退出集群

如果要完全退出集群，需要删除整个集群引导程序配置。由于每个成员上的当前配置相同 （从主设备同步），因此退出集群就意味着要么从备份恢复集群前的配置，要么清除现有配置并重新开始配置以免 IP 地址冲突。

准备工作

您必须使用控制台端口；删除集群配置时，所有接口都会关闭，包括管理接口和集群控制链路。而且，您不能通过远程 CLI 连接启用或禁用集群。

操作步骤

步骤 1　对从设备禁用集群：

cluster group *cluster_name*
no enable

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

在从设备上启用集群时，无法进行配置更改。

步骤 2　清除集群配置：

clear configure cluster

ASA 将关闭所有接口，包括管理接口和集群控制链路。

步骤 3　禁用集群接口模式：

no cluster interface-mode

模式并非存储于配置中，因此必须手动重置。

步骤 4　如果有备份配置，可将备份配置复制到正在运行的配置中：

copy *backup_cfg* **running-config**

示例：

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?
```

```
Destination filename [startup-config]?
ciscoasa(config)#
```

步骤 5　将配置保存到启动配置：

```
write memory
```

步骤 6　如果没有备份配置，请重新配置管理访问。例如，确保更改接口 IP 地址，并恢复正确的主机名。

相关主题

- 第 2 章，“入门”

更改主设备

注意事项　如要更改主设备，最好的方法是在主设备上禁用集群，等到新的主设备选举后再重新启用集群。如果必须指定要成为主设备的具体设备，请使用本节中的操作步骤。但是请注意，对集中功能而言，如果使用本操作步骤强制更改主设备，则所有连接都将断开，而您必须在新的主设备上重新建立连接。

如要更改用主设备，请执行以下步骤。

准备工作

对于多情景模式，请在系统执行空间中执行本操作步骤。如果尚未进入系统配置模式，请输入 **changeto system** 命令。

操作步骤

步骤 1　将一台新设备设置为主设备：

cluster master unit *unit_name*

示例：

```
ciscoasa(config)# cluster master unit asa2
```

您需要重新连接到主集群 IP 地址。

如要查看成员名称，请输入 **cluster master unit ?**（查看除当前设备外的所有名称），或输入 **show cluster info** 命令。

相关主题

- 第 8-48 页的成为非活动成员
- 第 8-22 页的集群的集中功能

在集群范围执行命令

如要向集群中的所有成员或某个特定成员发送命令，请执行以下步骤。向所有成员发送 **show** 命令，收集所有输出并将其显示在当前设备的控制台上。诸如 **capture** 和 **copy** 之类的其他命令也可以充分利用在集群范围执行的优势。

操作步骤

步骤 1　向所有成员发送命令，或者指定设备名称向某个特定成员发送命令：

cluster exec [**unit** *unit_name*] *command*

示例：

```
ciscoasa# cluster exec show xlate
```

如要查看成员名称，请输入 **cluster exec unit ?**（查看除当前设备外的所有名称），或输入 **show cluster info** 命令。

示例

如要将相同的捕获文件从集群中所有设备同时复制到 TFTP 服务器，请在主设备上输入以下命令：

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

分别来自每台设备（各一个）的多个 PCAP 文件被复制到 TFTP 服务器。目标捕获文件名会自动附加设备名称，例如 capture1_asa1.pcap、capture1_asa2.pcap 等。在本例中，asa1 和 asa2 是集群设备名称。

以下是 **cluster exec show port-channel summary** 命令的输出示例，显示了集群中每个成员的 EtherChannel 信息：

```
ciscoasa# cluster exec show port-channel summary
primary(LOCAL):*************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP      Yes  Gi0/0(P)
2         Po2             LACP      Yes  Gi0/1(P)
 secondary:*********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP      Yes   Gi0/0(P)
2         Po2             LACP      Yes   Gi0/1(P)
```

监控 ASA 集群

您可以监控集群状态和连接并排除故障。

- 第 8-53 页的监控集群状态
- 第 8-53 页的在集群范围捕获数据包
- 第 8-54 页的监控集群资源
- 第 8-54 页的监控集群流量
- 第 8-56 页的监控集群路由
- 第 8-56 页的配置集群日志记录
- 第 8-57 页的监控集群接口
- 第 8-57 页的调试集群

监控集群状态

请参阅以下用于监控集群状态的命令：

- **show cluster info** [**health**]

  如果没有关键字，**show cluster info** 命令将显示所有集群成员的状态。

  show cluster info health 命令将显示接口、设备和整个集群的当前运行状况。

  请参阅 **show cluster info** 命令的以下输出：

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state SLAVE
      ID        : 0
      Version   : 100.8(0.52)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
Unit "D" in state SLAVE
      ID        : 1
      Version   : 100.8(0.52)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state MASTER
      ID        : 2
      Version   : 100.8(0.52)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state SLAVE
      ID        : 3
      Version   : 100.8(0.52)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster history**

  显示集群历史记录。

在集群范围捕获数据包

请参阅以下用于在集群中捕获数据包的命令：

cluster exec capture

如要支持集群范围的故障排除，可以使用 **cluster exec capture** 命令在主设备上启用捕获集群特定流量的功能，随后集群中的所有从设备上将自动启用此功能。

相关主题

- 第 38-1 页的捕获数据包

监控集群资源

请参阅以下用于监控集群资源的命令：

show cluster {**cpu** | **memory** | **resource**} [*options*]

显示整个集群的汇总数据。可用 *options* 取决于数据类型。

监控集群流量

请参阅以下用于监控集群流量的命令：

- **show conn [detail], cluster exec show conn**

  show conn 命令显示一个传输是导向者、备用还是转发者传输。在任何设备上使用 **cluster exec show conn** 命令都可以查看所有连接。此命令可以显示一个传输的流量如何到达集群中的不同 ASA。集群的吞吐量取决于负载均衡的效率和配置。此命令可以让您很方便地查看某个连接的流量如何流经集群，也可以帮助您了解负载均衡器对传输的性能有何影响。

  以下是 **show conn detail** 命令的输出示例：

```
ciscoasa/ASA2/slave# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
            B - initial SYN from outside, b - TCP state-bypass or nailed,
            C - CTIQBE media, c - cluster centralized,
            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 - GTP t3-response
            k - Skinny media, M - SMTP data, m - SIP media, n - GUP
            O - outbound data, P - inside back connection, p - Phone-proxy TFTP
            connection,
            q - SQL*Net data, R - outside acknowledged FIN,
            R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
            s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
            V - VPN orphan, W - WAAS,
            X - inspected by service module,
            x - per session, Y - director stub flow, y - backup stub flow,
            Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
uptime 1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255)
Traffic received at interface outside Locally received: 7544 (93 byte/s) Traffic
received at interface NP Identity Ifc Locally received: 0 (0 byte/s) UDP outside:
10.1.227.1/500 NP Identity Ifc: 10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s,
timeout 2m0s, bytes 1580, cluster sent/rcvd bytes 0/0, cluster sent/rcvd total bytes
0/0, owners (0,255) Traffic received at interface outside Locally received: 864 (10
byte/s) Traffic received at interface NP Identity Ifc Locally received: 716 (8 byte/s)
```

  如要排除连接的传输故障，请先在任意设备上输入 **cluster exec show conn** 命令查看所有设备上的连接。寻找带有以下标志的传输：导向者 (Y)、备用 (y) 和转发者 (z)。下例显示了三台 ASA 上的一条从 172.18.124.187:22 到 192.168.103.131:44727 的 SSH 连接；ASA 1 带有 z 标志，表示其是该连接的转发者；ASA3 带有 Y 标志，表示其是该连接的导向者；而 ASA2 则

没有特殊的标志，表示其是所有者。在出站方向，此连接的数据包进入 ASA2 上的内部接口并从外部接口流出。在入站方向，此连接的数据包进入 ASA 1 和 ASA3 上的外部接口，通过集群控制链路被转发到 ASA2，然后流出 ASA2 上的内部接口。

```
ciscoasa/ASA1/master# cluster exec show conn
ASA1(LOCAL):**********************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:**********************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:**********************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0,
flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance**]

  show cluster info conn-distribution 和 **show cluster info packet-distribution** 命令显示跨所有集群设备的流量分摊。这些命令可以帮助您评估和调整外部负载均衡器。

  show cluster info loadbalance 命令显示连接再均衡统计信息。

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

  显示整个集群的汇总数据。可用 *options* 取决于数据类型。

  请参阅 **show cluster access-list** 命令的以下输出：

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
```

```
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

如要显示所有设备正在使用的连接的汇总计数，请输入：

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):**********************************************************
  100 in use, 100 most used

  cl1:*****************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  此命令对于排除数据路径故障非常有用。

相关主题

- “连接角色”，第 11-22 页

监控集群路由

请参阅以下用于监控集群路由的命令：

show route cluster

debug route cluster

显示集群的路由信息。

配置集群日志记录

请参阅以下用于配置集群日志记录的命令：

logging device-id

集群中的每台设备将独立生成系统日志消息。您可以使用 **logging device-id** 命令生成具有相同或不同设备 ID 的系统日志消息，使消息看似来自集群中的相同或不同设备。

相关主题

- 第 39-15 页的在非 EMBLEM 格式系统日志消息中包含设备 ID

监控集群接口

请参阅以下用于监控集群接口的命令：

- **show cluster interface-mode**

  显示集群接口模式。

- **show port-channel**

  包括有关端口通道是否跨网络的信息。

- **show lacp cluster {system-mac | system-id}**

  显示 cLACP 系统 ID 和优先级。

- **debug lacp cluster [all | ccp | misc | protocol]**

  显示 cLACP 的调试消息。

调试集群

请参阅以下用于调试集群的命令：

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  显示集群的调试消息。

- **show cluster info trace**

  show cluster info trace 命令显示调试信息，供进一步排除故障之用。

  请参阅 **show cluster info trace** 命令的以下输出：

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
MASTER
```

ASA 集群示例

这些示例包括典型部署中所有与集群相关的 ASA 配置。

- 第 8-57 页的 ASA 和交换机配置示例
- 第 8-60 页的单臂防火墙
- 第 8-62 页的流量分离
- 第 8-64 页的包含备用链路 （传统的 8 活动/8 备用）的跨网络 EtherChannel

ASA 和交换机配置示例

以下配置示例连接 ASA 与交换机之间的下列接口：

ASA 接口	交换机接口
GigabitEthernet 0/2	GigabitEthernet 1/0/15
GigabitEthernet 0/3	GigabitEthernet 1/0/16
GigabitEthernet 0/4	GigabitEthernet 1/0/17
GigabitEthernet 0/5	GigabitEthernet 1/0/18

- 第 8-58 页的 ASA 配置
- 第 8-59 页的思科 IOS 交换机配置

ASA 配置

每台设备上的接口模式

```
cluster interface-mode spanned force
```

ASA1 主设备引导程序配置

```
interface GigabitEthernet0/0
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit A
 cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
 priority 10
 key emphyri0
 enable noconfirm
```

ASA2 从设备引导程序配置

```
interface GigabitEthernet0/0
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit B
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 11
 key emphyri0
 enable as-slave
```

主设备接口配置

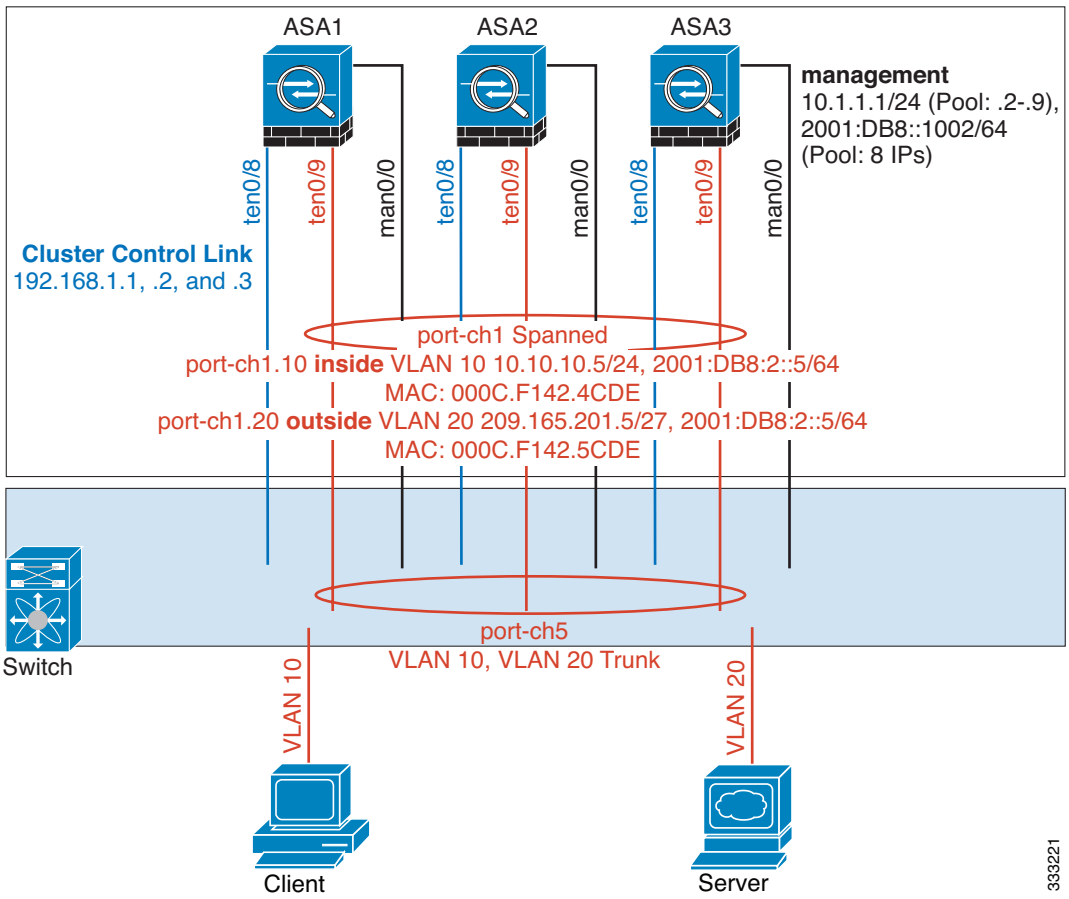
```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface GigabitEthernet0/2
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/3
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/4
 channel-group 11 mode active
 no shutdown
!
interface GigabitEthernet0/5
 channel-group 11 mode active
 no shutdown
!
interface Management0/0
 management-only
 nameif management
 ip address 10.53.195.230 cluster-pool mgmt-pool
 security-level 100
 no shutdown
!
interface Port-channel10
 port-channel span-cluster
 mac-address aaaa.bbbb.cccc
 nameif inside
 security-level 100
 ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
 port-channel span-cluster
 mac-address aaaa.dddd.cccc
 nameif outside
 security-level 0
 ip address 209.165.201.1 255.255.255.224
```

思科 IOS 交换机配置

```
interface GigabitEthernet1/0/15
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/16
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/17
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active
!
interface GigabitEthernet1/0/18
```

```
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active

interface Port-channel10
 switchport access vlan 201
 switchport mode access

interface Port-channel11
 switchport access vlan 401
 switchport mode access
```

单臂防火墙



来自不同安全域的数据流量与不同的 VLAN 关联，例如， VLAN 10 用于内部网络而 VLAN 20 用于外部网络。每台 ASA 都有一个连接到外部交换机或路由器的物理端口。启用中继使物理链路上的所有数据包都采用 802.1q 封装。 ASA 是 VLAN 10 与 VLAN 20 之间的防火墙。

使用跨网络 EtherChannel 时，所有数据链路在交换机端分组为一个 EtherChannel。如果一台 ASA 变得不可用，交换机将在其余设备之间再均衡流量。

每台设备上的接口模式

```
cluster interface-mode spanned force
```

ASA1 主设备引导程序配置

```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

cluster group cluster1
    local-unit asa1
    cluster-interface tengigabitethernet0/8 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

ASA2 从设备引导程序配置

```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

cluster group cluster1
    local-unit asa2
    cluster-interface tengigabitethernet0/8 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

ASA3 从设备引导程序配置

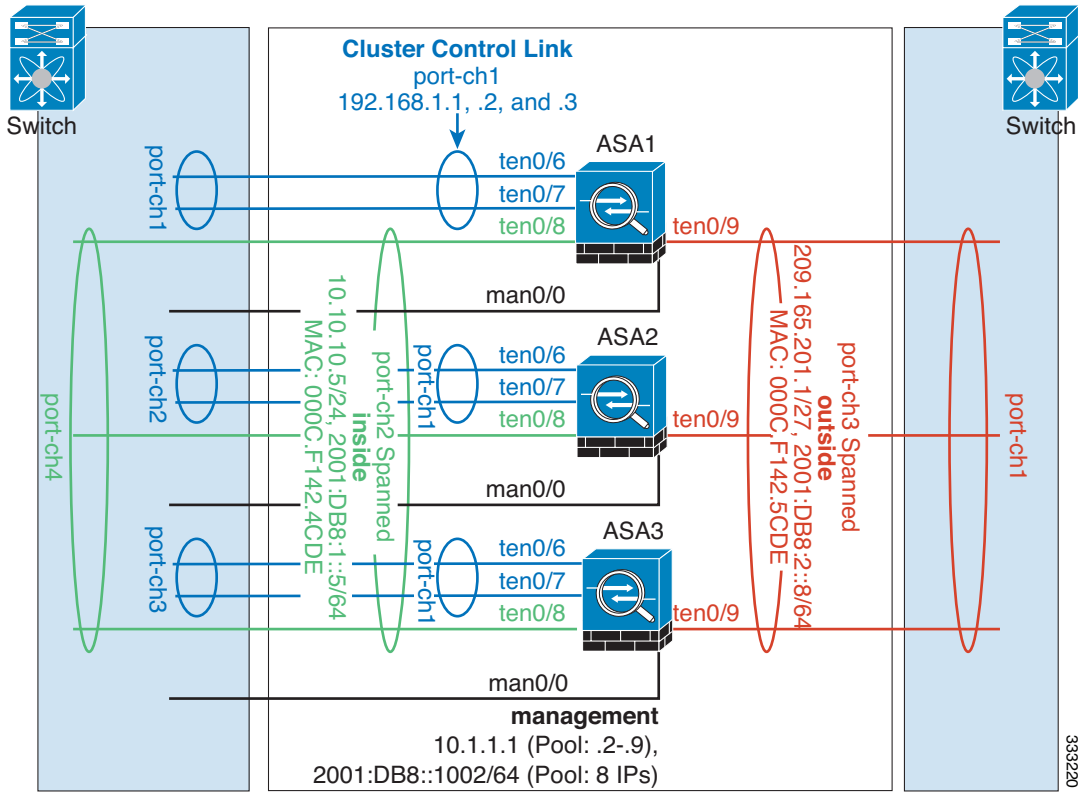
```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

cluster group cluster1
    local-unit asa3
    cluster-interface tengigabitethernet0/8 ip 192.168.1.3 255.255.255.0
    priority 3
    key chuntheunavoidable
    enable as-slave
```

主设备接口配置

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown

interface tengigabitethernet 0/9
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    port-channel span-cluster
interface port-channel 2.10
```

```
    vlan 10
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    ipv6 address 2001:DB8:1::5/64
    mac-address 000C.F142.4CDE
interface port-channel 2.20
    vlan 20
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    ipv6 address 2001:DB8:2::8/64
    mac-address 000C.F142.5CDE
```

流量分离



您可能更愿意在内部和外部网络之间采用物理方式分离流量。

如上图所示，左侧有一个跨网络 EtherChannel 连接到内部交换机，而右侧的另一个跨网络 EtherChannel 连接到外部交换机。如果需要，您还可以在每个 EtherChannel 上创建 VLAN 子接口。

每台设备上的接口模式

```
cluster interface-mode spanned force
```

ASA1 主设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
```

```
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

ASA2 从设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

ASA3 从设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa3
    cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
    priority 3
    key chuntheunavoidable
    enable as-slave
```

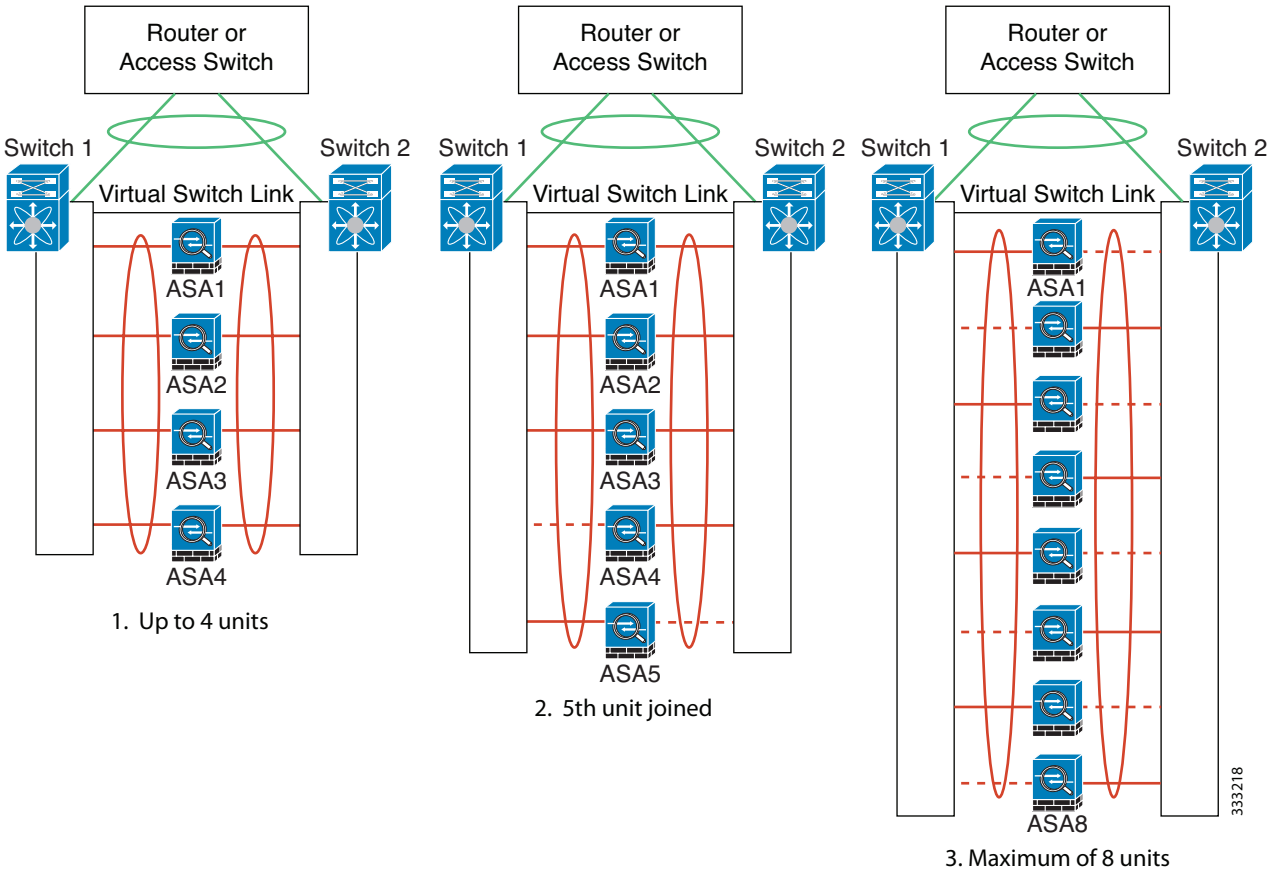
主设备接口配置

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown
```

```
interface tengigabitethernet 0/8
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    port-channel span-cluster
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    ipv6 address 2001:DB8:1::5/64
    mac-address 000C.F142.4CDE

interface tengigabitethernet 0/9
    channel-group 3 mode active
    no shutdown
interface port-channel 3
    port-channel span-cluster
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    ipv6 address 2001:DB8:2::8/64
    mac-address 000C.F142.5CDE
```

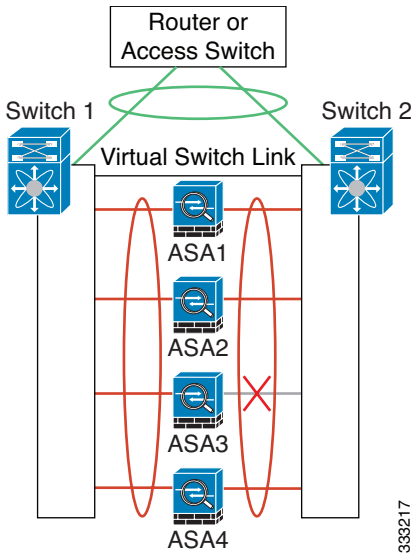
包含备用链路 （传统的 8 活动/8 备用）的跨网络 EtherChannel

在传统的 EtherChannel 中，最大活动端口数限制为 8 个来自交换机端的端口。如果您在 8-ASA 集群中将每台设备的 2 个端口分配到 EtherChannel，总计 16 个端口，则其中 8 个端口必须处于备用模式。 ASA 使用 LACP 来协商哪些链路应为活动链路，哪些应为备用链路。如果使用 VSS 或 vPC 启用多交换机 EtherChannel，则可实现交换机间冗余。在 ASA 上，所有物理端口将先按插槽号、后按端口号排序。在下图中，排序较低的端口是“主要”端口 （例如 GigabitEthernet 0/0），另一个是“辅助”端口 （例如 GigabitEthernet 0/1）。您必须保证硬件连接对称：如果使用 VSS/vPC，所有主要链路必须在一台交换机上终止，所有辅助链路必须在另一台交换机上终止。下图显示了当更多设备加入集群导致链路总数增加时会发生什么情况：

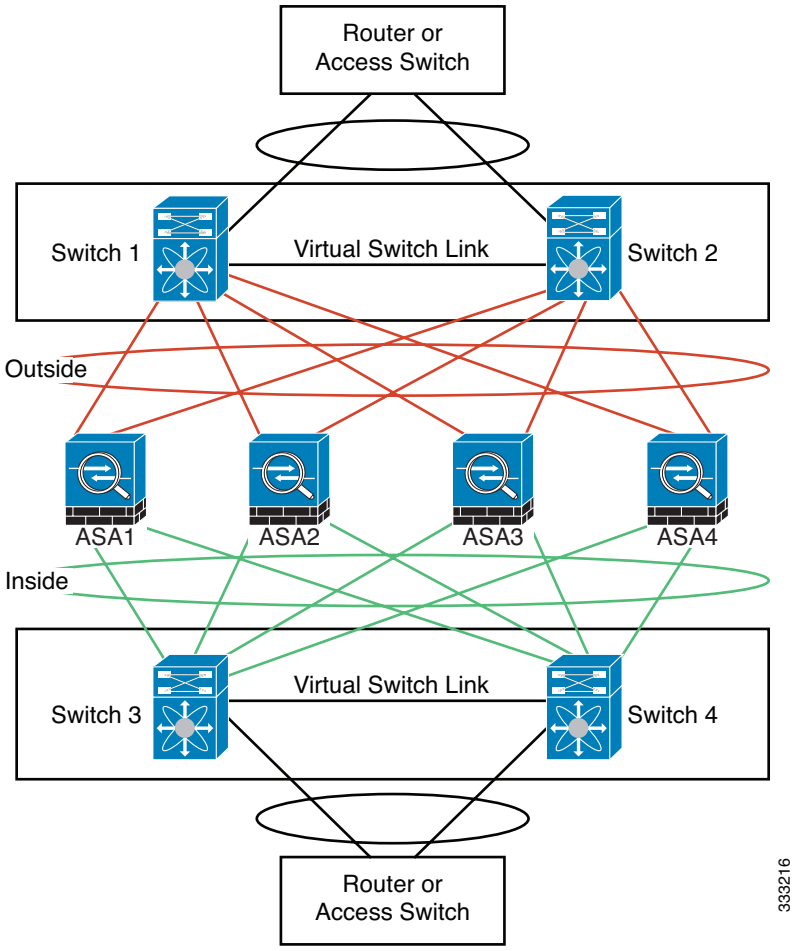


此时的处理原则是，首先将通道中的活动端口数增加到最大值，其次是保持活动的主要端口数与活动的辅助端口数之间的均衡。请注意，当第 5 台设备加入集群时，流量并未在所有设备之间达到均衡。

处理链路或设备故障时也遵循相同的原则。最终的负载均衡状况可能并不尽如人意。下图所示为 4 台设备组成的集群，其中一台设备上有一个链路发生故障。



该网络中可能配置了多个 EtherChannel。下图所示为一个内部 EtherChannel 和一个外部 EtherChannel。如果 EtherChannel 中的主要链路和辅助链路都发生故障，则会从集群中删除 ASA。这可以防止 ASA 在已经与内部网络断开连接的情况下收到来自外部网络的流量。



每台设备上的接口模式

```
cluster interface-mode spanned force
```

ASA1 主设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
```

```
    local-unit asa1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

ASA2 从设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

ASA3 从设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa3
    cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
    priority 3
    key chuntheunavoidable
    enable as-slave
```

ASA4 从设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
```

```
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa4
    cluster-interface port-channel1 ip 192.168.1.4 255.255.255.0
    priority 4
    key chuntheunavoidable
    enable as-slave
```

主设备接口配置

```
ip local pool mgmt 10.1.1.2-10.1.1.9

interface management 0/0
    channel-group 2 mode active
    no shutdown
interface management 0/1
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    security-level 100
    management-only

interface tengigabitethernet 1/6
    channel-group 3 mode active vss-id 1
    no shutdown
interface tengigabitethernet 1/7
    channel-group 3 mode active vss-id 2
    no shutdown
interface port-channel 3
    port-channel span-cluster vss-load-balance
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    mac-address 000C.F142.4CDE

interface tengigabitethernet 1/8
    channel-group 4 mode active vss-id 1
    no shutdown
interface tengigabitethernet 1/9
    channel-group 4 mode active vss-id 2
    no shutdown
interface port-channel 4
    port-channel span-cluster vss-load-balance
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    mac-address 000C.F142.5CDE
```

ASA 集群的历史记录

功能名称	平台版本	功能信息
ASA 5580 和 5585-X 的 ASA 集群	9.0(1)	通过 ASA 集群，可以将多台 ASA 组合成一个逻辑设备。集群具有单个设备的全部便捷性 （管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。 ASA 5580 和 ASA 5585-X 支持 ASA 集群；集群中的所有设备必须为相同型号且硬件规格相同。有关启用集群时不支持的功能列表，请参阅配置指南。 我们引入或修改了以下命令：**channel-group**、**clacp system-mac**、**clear cluster info**、**clear configure cluster**、**cluster exec**、**cluster group**、**cluster interface-mode**、**cluster-interface**、**conn-rebalance**、**console-replicate**、**cluster master unit**、**cluster remove unit**、**debug cluster**、**debug lacp cluster**、**enable**（集群组）、**health-check**、**ip address**、**ipv6 address**、**key**（集群组）、**local-unit**、**mac-address**（接口）、**mac-address pool**、**mtu cluster**、**port-channel span-cluster**、**priority**（集群组）、**prompt cluster-unit**、**show asp cluster counter**、**show asp table cluster chash-table**、**show cluster**、**show cluster info**、**show cluster user-identity**、**show lacp cluster** 和 **show running-config cluster**。
ASA 5500-X 对集群的支持	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 现在支持由 2 台设备组成的集群。默认情况下，在基础许可证中支持两台设备的集群；对于 ASA 5512-X，您需要增强型安全许可证。 我们未修改任何命令。
提高了 VSS 和 vPC 对运行状况检查监控的支持	9.1(4)	如果将集群控制链路配置为 EtherChannel（推荐），而且链路连接到 VSS 或 vPC 对，则现在可提高运行状况检查监控的稳定性。对某些交换机（例如思科 Nexus 5000）而言，当 VSS/vPC 中的一台设备正在关闭或启动时，连接到这些交换机的 EtherChannel 成员接口可能看似对 ASA 打开，但在交换机端却并未传输流量。如果将 ASA 保持时间超时设置为比较小的值（例如 .8 秒），而 ASA 在这些 EtherChannel 接口中的一个接口上发送 keepalive 消息，ASA 可能会被错误地从集群中删除。启用 VSS/vPC 运行状况检查功能时，ASA 将在集群控制链路中的所有 EtherChannel 接口上泛洪 keepalive 消息，以确保至少有一台交换机可以收到这些消息。 我们修改了以下命令：**health-check [vss-enabled]**
支持集群成员位于不同的地理位置 （站点间）；仅限独立接口模式	9.1(4)	使用独立接口模式时，集群成员现在可位于不同的地理位置。 我们未修改任何命令。
对透明模式支持集群成员位于不同的地理位置（站点间）	9.2(1)	在透明防火墙模式中使用跨网络 EtherChannel 模式时，集群成员现在可位于不同的地理位置。不支持在路由防火墙模式中使用跨网络 EtherChannel 的站点间集群。 我们未修改任何命令。

功能名称	平台版本	功能信息
对集群的静态 LACP 端口优先级支持	9.2(1)	有些交换机不支持 LACP 动态端口优先级 （活动链路和备用链路）。您现在可以禁用动态端口优先级，使跨网络 EtherChannel 具有更高兼容性。您还应该遵循以下指导原则： • 集群控制链路路径上的网络要素不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。 • 端口通道绑定中断时间不得超过配置的 keepalive 间隔。 我们引入了以下命令：**clacp static-port-priority**。
支持跨网络 EtherChannel 中有 32 条活动链路	9.2(1)	ASA EtherChannel 现在最多可支持 16 条活动链路。借助*跨网络* EtherChannel，此功能已扩展为在使用 vPC 中的两台交换机且禁用动态端口优先级时，最多可在整个集群中支持 32 条活动链路。交换机必须支持有 16 条活动链路的 EtherChannel；例如带 F2 系列 10 千兆以太网模块的思科 Nexus 7000。 对于 VSS 或 vPC 中支持 8 条活动链路的交换机，现在可以在跨网络 EtherChannel 中配置 16 条活动链路 （每台交换机各连接 8 条）。以前，即便使用 VSS/vPC，跨网络 EtherChannel 也只支持 8 条活动链路和 8 条备用链路。 **注**　如果要在跨网络 EtherChannel 中使用 8 条以上的活动链路，则无法同时拥有备用链路；支持 9 到 32 条活动链路需要禁用允许使用备用 链路的 cLACP 动态端口优先级。 我们引入了以下命令：**clacp static-port-priority**
对 ASA 5585-X 支持 16 个集群成员	9.2(1)	ASA 5585-X 现在支持由 16 台设备组成的集群。 我们未修改任何命令。
ASA 集群的 BGP 支持	9.3(1)	我们增加了对 BGP 用于 ASA 集群的支持。 我们引入了以下新命令：**bgp router-id clusterpool**

第 3 部分

接口

基本接口配置 （ASA 5512-X 及更高版本）

本章介绍启动思科 ASA 5512-X 及更高版本接口配置的任务，包括配置以太网设置、冗余接口和 EtherChannel。

注 在多情景模式中，请在系统执行空间中完成本节所述的所有任务。如要从该情景切换至系统执行空间，请输入 **changeto system** 命令。

有关具有特殊要求的 ASA 集群接口，请参阅第 8 章，“ASA 集群”。

- 第 9-1 页的有关启动 ASA 5512-X 及更高版本接口配置的信息
- 第 9-9 页的 ASA 5512-X 及更高版本接口的许可要求
- 第 9-10 页的准则和限制
- 第 9-11 页的默认设置
- 第 9-12 页的开始接口配置 （ASA 5512-X 及更高版本）
- 第 9-31 页的监控接口
- 第 9-31 页的 ASA 5512-X 及更高版本接口的配置示例
- 第 9-32 页的后续操作
- 第 9-33 页的 ASA 5512-X 及更高版本接口的功能历史记录

有关启动 ASA 5512-X 及更高版本接口配置的信息

- 第 9-2 页的 Auto-MDI/MDIX 功能
- 第 9-2 页的处于透明模式中的接口
- 第 9-2 页的管理接口
- 第 9-4 页的冗余接口
- 第 9-4 页的 EtherChannel
- 第 9-6 页的用最大传输单元、 TCP 最大分段大小控制分片

Auto-MDI/MDIX 功能

对于 RJ-45 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。对于千兆以太网，当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

处于透明模式中的接口

处于透明模式中的接口属于“网桥组”，每个网络都有一个网桥组。4 个接口最多可以有 8 个网桥组，每个情境或单一模式中有一个。有关网桥组的详细信息，请参阅第 12-1 页的透明模式的网桥组。

管理接口

- 第 9-2 页的管理接口概述
- 第 9-2 页的管理插槽/端口界面
- 第 9-3 页的将任何接口用于仅管理流量
- 第 9-3 页的用于透明模式的管理接口
- 第 9-3 页的不支持冗余管理接口
- 第 9-4 页的 ASA 5512-X 到 ASA 5555-X 上的 Management 0/0 接口

管理接口概述

可以通过连接到以下接口来管理 ASA：

- 任何直通流量接口
- 专用的管理*插槽/端口*接口 （如果适用于所用的型号）

可能需要按照第 35 章，“管理访问”中所述配置对接口的管理访问。

管理*插槽/端口*界面

表 9-1 显示了每个型号的管理接口。

表 9-1　每个型号的管理接口

型号	Management 0/0[1]	Management 0/1	Management 1/0	Management 1/1	可针对直通流量进行配置[2]	允许子接口
ASA 5512-X	是	否	否	否	否	否
ASA 5515-X	是	否	否	否	否	否
ASA 5525-X	是	否	否	否	否	否
ASA 5545-X	是	否	否	否	否	否
ASA 5555-X	是	否	否	否	否	否

表 9-1　每个型号的管理接口

型号	Management 0/0[1]	Management 0/1	Management 1/0	Management 1/1	可针对直通流量进行配置[2]	允许子接口
ASA 5585-X	是	是	是[3]	是[3]	是	是
ASASM	否	否	否	否	不适用	不适用
ASAv	是	否	否	否	否	否

1. 作为默认出厂配置的一部分，已配置了用于 ASDM 访问的 Management 0/0 接口。有关详细信息，请参阅第 2-12 页的出厂默认配置。
2. 默认情况下，Management 0/0 接口配置为用于管理流量（**management-only** 命令）。对于处于路由模式中的受支持型号，可以取消这一限制并传递直通流量。如果型号包含其他管理接口，还可以将这些接口用于直通流量。但是，管理接口可能不会进行直通流量方面的优化。
3. 如果在插槽 1 中安装了 SSP，则管理 1/0 接口和管理 1/1 接口仅在插槽 1 中提供对 SSP 的管理访问。

注　如果安装了一个模块，该模块的管理接口仅提供对该模块的管理访问。对于 ASA 5512-X 到 ASA 5555-X，该软件模块将同一个物理 Management 0/0 接口用作 ASA。

将任何接口用于仅管理流量

若想将任何接口（包括 EtherChannel 接口）用作管理专用接口，只需将该接口配置为用于管理流量（请参阅 **management-only** 命令）。

用于透明模式的管理接口

在透明防火墙模式中，除了允许的最大数量范围内的直通流量接口，还可以将管理接口 （物理接口、子接口[如果所用的型号支持]或由管理接口组成的 EtherChannel 接口[如果有多个管理接口]）用作单独的管理接口。不能将任何其他接口类型用作管理接口。

在多情景模式中，无法在情景之间共享任何接口，包括管理接口。如要为每个情景提供管理，可创建管理接口的子接口，然后向每个情景分配管理子接口。请注意，从 ASA 5512-X 到 ASA 5555-X 都不允许管理接口上有子接口，因此，对于每个情景管理，必须连接到数据接口。

管理接口不属于普通网桥组的一部分。请注意，出于操作目的，管理接口属于不可配置网桥组的一部分。

注　在透明防火墙模式中，管理接口以与数据接口相同的方式更新 MAC 地址表；因此，不应将管理和数据接口连接到同一个交换机，除非将其中一个交换机端口配置为路由端口（默认情况下，Catalyst 交换机在所有的 VLAN 交换机端口上共享一个 MAC 地址）。否则，如果流量从物理连接的交换机到达管理接口，ASA 会更新 MAC 地址表，以使用*管理*接口（而不是数据接口）来访问交换机。此操作会导致临时流量中断；出于安全原因，ASA 至少在 30 秒内不会再次更新从交换机到数据接口的数据包 MAC 地址表。

不支持冗余管理接口

冗余接口不支持作为成员的管理*插槽/端口*接口。也不能将组成非管理接口的冗余接口设置为管理专属接口。

ASA 5512-X 到 ASA 5555-X 上的 Management 0/0 接口

ASA 5512-X 到 ASA 5555-X 上的 Management 0/0 接口具有以下特征：

- 不支持直通流量
- 不支持子接口
- 不支持优先级队列
- 不支持组播 MAC
- 软件模块共享 Management 0/0 接口。ASA 和模块支持单独的 MAC 地址和 IP 地址。必须在模块操作系统中执行模块 IP 地址的配置。但是，物理特性 （例如启用接口）在 ASA 上进行配置。

冗余接口

一个逻辑冗余接口包括一对物理接口：主用和备用接口。如果主用接口发生故障，备用接口将激活并开始传输流量。可以配置冗余接口来提高 ASA 的可靠性。此功能独立于设备级故障转移，如果需要，可以配置冗余接口和设备级故障转移。

冗余接口 MAC 地址

冗余接口使用您添加的第一个物理接口的 MAC 地址。如果在配置中更改成员接口的顺序，则 MAC 地址发生更改，以匹配现第一个列出的接口的 MAC 地址。或者，无论成员接口 MAC 地址如何，均可以将 MAC 址址分配给冗余接口 （请参阅第 11-7 页的配置 MAC 地址、 MTU 和 TCP MSS或第 6-14 页的配置多情景）。如果主用接口故障转移到备用接口，系统将维护同一 MAC 地址，以防流量中断。

EtherChannel

802.3ad EtherChannel 是逻辑接口 （称为端口通道接口），该接口由一组单独的以太网链路 （通道组）组成，使得可以提高单个网络的带宽。配置接口相关功能时，可以像使用物理接口一样来使用端口通道接口。

最多可配置 48 个 EtherChannel。

- 第 9-4 页的通道组接口
- 第 9-5 页的连接到另一台设备上的 EtherChannel
- 第 9-6 页的链路聚合控制协议
- 第 9-6 页的负载均衡
- 第 9-6 页的 EtherChannel MAC 地址

通道组接口

每个通道组最多可以有 16 个主用接口。对于仅支持 8 个主用接口的交换机，最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。对于 16 个主用接口，请确保交换机支持此功能 （例如，带有 F2 系列 10 千兆以太网模块的思科 Nexus 7000 支持此功能）。

通道组中的所有接口必须具有相同的类型和速度。添加到通道组中的第一个接口确定正确的类型和速度。

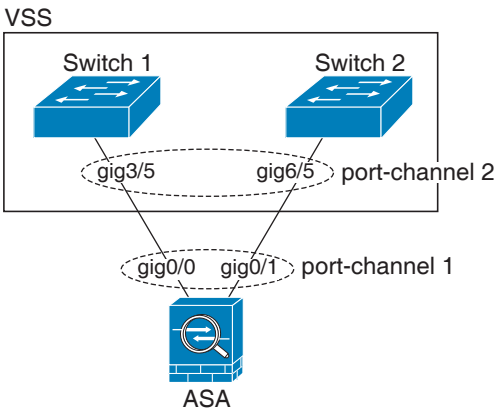
EtherChannel 汇聚信道中所有可用活动接口上的流量。会根据源或目标 MAC 地址、 IP 地址、 TCP 端口号、 UDP 端口号和 VLAN 编号，使用专有的哈希算法来选择接口。

连接到另一台设备上的 EtherChannel

连接 ASA EtherChannel 的设备必须同时支持 802.3ad EtherChannel；例如，可以连接到 Catalyst 6500 交换机或思科 Nexus 7000。

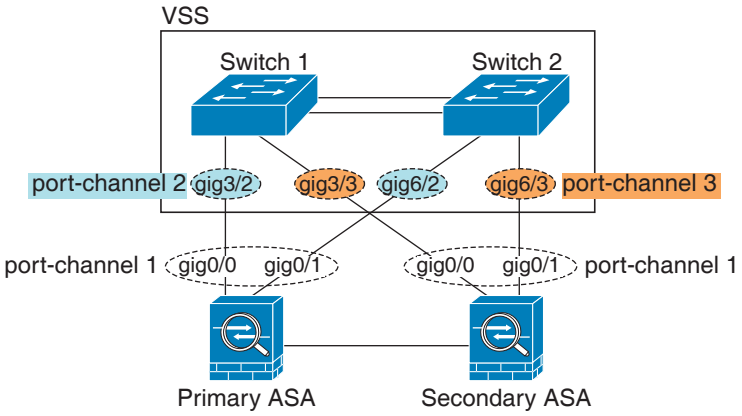
如果交换机属于虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 的一部分，可以在同一个 EtherChannel 内的 ASA 接口连接到 VSS/vPC 中单独交换机。交换机接口属于同一个 EtherChannel 端口通道接口的成员，因为单独交换机的作用方式类似于单个交换机 （请参阅图 9-1）。

图 9-1　　连接到 VSS/vPC



如果在主用/备用故障转移部署中使用 ASA，需要在 VSS/vPC 中的交换机上创建单独的 EtherChannel - 为每个 ASA 创建一个 （请参阅图 9-1）。在每个 ASA 上，可以将一个 EtherChannel 连接到两台交换机。即使您可以将所有的交换机接口分组到连接两个 ASA 的一个 EtherChannel 中 （在这种情况下，将不会建立 EtherChannel，因为 ASA 系统 ID 是单独的），并不需要单个 EtherChannel，因为您不希望将流量发送到备用 ASA。

图 9-2　　主用/备用故障转移和 VSS/vPC



链路聚合控制协议

链路聚合控制协议 (LACP) 通过在两个网络设备之间交换链路聚合控制协议数据单元 (LACPDU) 来聚合接口。

可以在 EtherChannel 中将每个物理接口配置为：

- Active - 发送并接收 LACP 更新。活动 EtherChannel 可与活动或被动 EtherChannel 建立连接。应使用活动模式，除非需要尽可能减少 LACP 流量。
- Passive - 接收 LACP 更新。被动 EtherChannel 只能与活动 EtherChannel 建立连接。
- On - EtherChannel 始终开启，LACP 未使用。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

在没有用户干预的情况下， LACP 会协调对于指向 EtherChannel 的链路的自动添加和删除。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

负载均衡

ASA 通过对数据包的源 IP 地址和目标 IP 地址进行哈希处理，来向 EtherChannel 的接口中分发数据包 （此条件可配置；请参阅第 9-19 页的自定义 EtherChannel）。在取模运算中用得出的哈希值除以活动链路数量，这样得出的余数将确定哪个接口拥有流量。*hash_value* **mod** *active_links* 结果为 0 的所有数据包将转至 EtherChannel 中的第一个接口，结果为 1 的数据包将转至第二个接口，结果为 2 的数据包将转至第三个接口，依此类推。例如，如果有 15 个活动链路，取模运算将提供 0 到 14 的值。如果有 6 个活动链路，则值为 0 到 5，依此类推。

对于集群中的跨网络 EtherChannel，会逐个 ASA 进行负载均衡。例如，如果 8 个 ASA 之间的跨网络 EtherChannel 中有 32 个主用接口，EtherChannel 中的每个 ASA 有 4 个接口，则仅会在 ASA 上的 4 个接口之间进行负载均衡。

如果主用接口发生故障且不能由备用接口替代，则流量会在剩余的链路之间重新平衡。该故障将会在第 2 层的生成树和第 3 层的路由表中被屏蔽，因此，故障恢复对其他网络设备是透明的。

EtherChannel MAC 地址

属于通道组一部分的所有接口共享同一个 MAC 地址。该功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；他们不知道单个链路。

端口通道接口使用编号最小的通道组接口 MAC 地址作为端口通道 MAC 地址。或者，您可以为端口通道接口手动配置 MAC 地址。在多情景模式中，可将唯一 MAC 地址自动分配给各个接口，包括 EtherChannel 端口接口。在组通道接口成员资格发生变化的情况下，我们建议手动或 （在多情景模式中）自动配置唯一的 MAC 地址。如果移除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址更改至下一个编号最小的接口，从而导致流量中断。

用最大传输单元、 TCP 最大分段大小控制分片

- 第 9-7 页的 MTU 概述
- 第 9-7 页的默认 MTU
- 第 9-7 页的路径 MTU 发现
- 第 9-7 页的设置 MTU 和巨型帧
- 第 9-7 页的 TCP 最大分段大小概述

- 第 9-8 页的默认 TCP MSS
- 第 9-8 页的设置 VPN 和非 VPN 流量的 TCP MSS
- 第 9-8 页的示例

MTU 概述

最大传输单元 (MTU) 指定 ASA 可在给定以太网接口上传输的最大帧负载大小。MTU 值是*没有*以太网报头、FCS 或 VLAN 标记的帧大小。以太网报头为 14 字节，而 FCS 为 4 字节。如果将 MTU 设置为 1500，预期的帧大小（包括报头）为 1518 字节。如果使用 VLAN 标记（这样将会增加额外 4 字节），并将 MTU 设置为 1500，预期的帧大小为 1522。请勿为容纳这些报头而将 MTU 的值设得过高。如要调整 TCP 报头以便进行封装，请勿更改 MTU 设置，而是应该更改 TCP 最大分段大小（第 9-7 页的 TCP 最大分段大小概述）。

如果传出的 IP 数据包大于指定 MTU，该数据包会分片成 2 个或更多个帧。片段在目标处（有时在中间跃点处）重组，而分片可能会导致性能下降。因此，IP 数据包大小应在 MTU 大小范围内，以避免分片。

注　只要有内存空间，ASA 就可接收大于所配置的 MTU 的帧。有关如何增加内存以接收较大的帧，请参阅第 9-21 页的启用巨型帧支持。

默认 MTU

ASA 上的默认 MTU 为 1500 字节。此值不包括以太网报头、CRC、VLAN 标记等的 18 个或更多字节。

路径 MTU 发现

ASA 支持路径 MTU 发现（如 RFC 1191 中所定义），从而使两个主机之间的网络路径中的所有设备均可协调 MTU，以便它们可以标准化路径中的最低 MTU。

设置 MTU 和巨型帧

请参阅第 11-7 页的配置 MAC 地址、MTU 和 TCP MSS。对于多情景模式，请在每个情景中设置 MTU。

请参阅第 9-21 页的启用巨型帧支持。对于多情景模式，请在系统执行空间中设置巨型帧支持。

请参阅以下准则：

- 与流量路径上的 MTU 相匹配 - 我们建议将所有 ASA 接口以及流量路径的其他设备接口上的 MTU 设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 适应巨型帧 - 如果启用巨型帧，最多可以将 MTU 设置为 9198 字节。

TCP 最大分段大小概述

TCP 最大分段尺寸 (TCP MSS) 是 TCP 负载在添加任何 TCP 报头之*前*的大小。UDP 数据包不会受到影响。建立连接时，客户端和服务器会在三次握手期间交换 TCP MSS 值。

可以在 ASA 上设置 TCP MSS。如果一个连接的任意终端要求 TCP MSS 的值大于 ASA 上设置的值，则 ASA 将用 ASA 最大值覆盖请求数据包内的 TCP MSS。如果主机或服务器不请求 TCP MSS，则 ASA 会假设 RFC 793 的默认值为 536 字节，但不会修改数据包。您还可以配置最小 TCP MSS；如果主机或服务器请求一个非常小的 TCP MSS，则 ASA 可将该值调高。默认情况下，最小 TCP MSS 未启用。

例如，可以将默认 MTU 配置为 1500 字节。主机请求 1700 的 MSS。如果 ASA 的最大 TCP MSS 是 1380，ASA 会将 TCP 请求数据包中的 MSS 值更改为 1380。然后，服务器会发送 1380 字节的数据包。

默认 TCP MSS

默认情况下，ASA 上的最大 TCP MSS 是 1380 字节。此默认值符合 VPN 连接的要求（在 VPN 连接中，报头最多可增加 120 字节）；此值在默认 MTU（1500 字节）范围内。

设置 VPN 和非 VPN 流量的 TCP MSS

请参阅第 11-7 页的配置 MAC 地址、MTU 和 TCP MSS。对于多情景模式，请在每个情景中设置 TCP MSS。

请参阅以下准则：

- 非 VPN 流量 - 如果不使用 VPN 且不需要额外的报头空间，应该禁用 TCP MSS 限制并接受连接终端之间建立的值。由于连接终端一般是从 MTU 获得 TCP MSS，因此，非 VPN 数据包通常符合此 TCP MSS。
- VPN 流量 - 将最大 TCP MSS 设置为 MTU - 120。例如，如果使用巨型帧并将 MTU 设置为较大的值，需要将 TCP MSS 设置为符合新的 MTU。

示例

以下示例将启用巨型帧、增加所有接口上的 MTU 并为非 VPN 流量禁用 TCP MSS（将 TCP MSS 设置为 0，表示无限制）：

```
jumbo frame-reservation
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 0
```

以下示例启用巨型帧，增大所有接口上的 MTU，并将 VPN 流量的 TCP MSS 更改为 9078（MTU 减去 120）：

```
jumbo frame-reservation
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 9078
```

ASA 5512-X 及更高版本接口的许可要求

型号	许可证要求
ASA 5512-X	VLAN： 基础许可证：50 增强型安全许可证：100 所有类型的接口： 基础许可证：716 增强型安全许可证：916
ASA 5515-X	VLAN： 基础许可证：100 所有类型的接口： 基础许可证：916
ASA 5525-X	VLAN： 基础许可证：200 所有类型的接口： 基础许可证：1316
ASA 5545-X	VLAN： 基础许可证：300 所有类型的接口： 基础许可证：1716
ASA 5555-X	VLAN： 基础许可证：500 所有类型的接口： 基础许可证：2516
ASA 5585-X	VLAN： 基础许可证和增强型安全许可证：1024 SSP-10 和 SSP-20 的接口速度： 基础许可证 - 适用于光纤接口的 1 千兆以太网 10 GE I/O 许可证（增强型安全许可证）- 适用于光纤接口的 10 千兆以太网 （默认情况下，SSP-40 和 SSP-60 支持 10 千兆以太网。） 所有类型的接口： 基础许可证和增强型安全许可证：4612

注　对于根据 VLAN 限制计数的接口，您必须为它分配一个 VLAN。例如：

```
interface gigabitethernet 0/0.100
 vlan 100
```

所有类型的接口构成最大数量的组合接口；例如，VLAN 接口、物理接口、冗余接口，桥组接口和 EtherChannel 接口。在配置中定义的每个 **interface** 命令均根据此限制进行计数。例如，以下两个接口都计入此限制，即使 GigabitEthernet 0/0 接口定义为 port-channel 1 的一部分：
interface gigabitethernet 0/0
和
interface port-channel 1

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在多情景模式中，应在系统执行空间中配置物理接口（如第 9-12 页的开始接口配置（ASA 5512-X 及更高版本）中所述）。然后，在情景执行空间中配置逻辑接口参数（如第 11 章，“路由模式接口”或第 12 章，“透明模式接口”中所述）。

防火墙模式准则

- 对于透明模式，可以为每个情景或单模式设备最多配置 8 个桥接组。
- 每个网桥组最多可包括 4 个接口。
- 对于多情景透明模式，每个情景必须使用不同的接口；不能在情景之间共享一个接口。

故障转移准则

- 如果要将冗余接口或 EtherChannel 接口用作故障转移链路，必须在故障转移对中的两台设备上预配置要使用接口；不能在主要设备上配置该接口并期望它会复制到辅助设备，因为*复制需要使用故障转移链路本身*。
- 如果将冗余接口或 EtherChannel 接口用于状态链路，不需要进行特殊配置；配置可从主要设备中如常复制。
- 可以使用 **monitor-interface** 命令监控冗余接口或 EtherChannel 接口；请务必引用逻辑冗余接口名称。如果活动成员接口故障转移到备用接口，该活动不会在监控设备级故障转移时导致冗余接口或 EtherChannel 接口出现故障。仅在所有物理接口都出现故障的情况下，冗余接口或 EtherChannel 接口才会出现故障（对于 EtherChannel 接口，可配置允许出现故障的成员接口数量）。
- 如果将 EtherChannel 接口用于故障转移或状态链路，然后防止无序数据包，则只会使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。不能作为故障转移链路处于使用状态的 EtherChannel 配置。如要更改配置，需要在进行更改时关闭 EtherChannel 或临时禁用故障转移；这两种操作都可在持续时间内防止故障转移发生。
- 不能与数据接口共享一个故障转移接口或状态接口。

集群准则

- 如果要将冗余接口或 EtherChannel 接口用作集群控制链路，必须在该集群中的所有设备上预配置要使用的接口；不能在主要设备上配置该接口并期望它会复制到成员设备，因为*复制需要使用集群控制链路本身*。
- 如要配置跨网络 EtherChannel，请参阅第 8-38 页的配置跨网络 EtherChannel。
- 如要配置单个集群接口，请参阅第 8-36 页的配置独立接口（管理接口的推荐配置）。

冗余接口准则

- 最多可以配置 8 个冗余接口对。
- 所有 ASA 配置均引用逻辑冗余接口，而不是成员物理接口。
- 不能将冗余接口用作 EtherChannel 的一部分，也不能将 EtherChannel 用作冗余接口的一部分。不能在冗余接口和 EtherChannel 接口中使用相同的物理接口。但是，如果这两种接口不是使用相同的物理接口，可以在 ASA 上配置这两种接口。
- 如果关闭主用接口，则将激活备用接口。
- 冗余接口不支持作为成员的管理*插槽/端口*接口。也不能将组成非管理接口的冗余接口设置为管理专属接口。
- 有关故障转移准则，请参阅第 9-10 页的故障转移准则。
- 有关集群准则，请参阅第 9-10 页的集群准则。

EtherChannel 准则

- 最多可配置 48 个 EtherChannel。
- 每个通道组最多可以有 16 个主用接口。对于仅支持 8 个主用接口的交换机，最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。
- 通道组中的所有接口必须具有相同的类型和速度。添加到通道组中的第一个接口确定正确的类型和速度。
- 连接 ASA EtherChannel 的设备必须同时支持 802.3ad EtherChannel；例如，可以连接到 Catalyst 6500 交换机或思科 Nexus 7000 交换机。
- ASA 不支持带有 VLAN 标记的 LACPDU。如果使用思科 IOS **vlan dot1Q tag native** 命令在相邻的交换机上启用本地 VLAN 标记，ASA 将会丢弃附上了标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。在多情景模式中，这些消息不包含在数据包捕获范围内，因此，对这个问题的诊断并不容易。
- ASA 不支持将 EtherChannel 连接到交换机堆叠。如果跨堆叠连接 ASA EtherChannel，则当主交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。
- 所有 ASA 配置均引用逻辑 EtherChannel 接口，而不是成员物理接口。
- 不能将冗余接口用作 EtherChannel 的一部分，也不能将 EtherChannel 用作冗余接口的一部分。不能在冗余接口和 EtherChannel 接口中使用相同的物理接口。但是，如果这两种接口不是使用相同的物理接口，可以在 ASA 上配置这两种接口。
- 有关故障转移准则，请参阅第 9-10 页的故障转移准则。
- 有关集群准则，请参阅第 9-10 页的集群准则。

默认设置

本节列出了接口的默认设置 （如果没有出厂默认配置）。有关出厂默认配置的信息，请参阅第 2-12 页的出厂默认配置。

接口的默认状态

接口的默认状态取决于类型和情景模式。

在多情景模式中，所有分配的接口均默认启用，无论系统执行空间中接口的状态如何。但是，为使流量通过接口，还必须在系统执行空间中启用接口。如果关闭系统执行空间中的接口，则该接口将在共享它的所有情景中处于关闭状态。

在单模式中或系统执行空间中，接口具有以下默认状态：

- 物理接口 - 已禁用。
- 冗余接口 - 已启用。但是，对于通过冗余接口的流量，还必须启用成员物理接口。
- 子接口 - 已启用。但是，对于通过子接口的流量，还必须启用物理接口。
- EtherChannel 端口通道接口 - 已启用。但是，如要使流量能够通过 EtherChannel 接口，还必须启用通道组物理接口。

默认速度和双工

- 默认情况下，铜缆 (RJ-45) 接口的速度和双工设置为自动协商。
- 对于 5585-X 的光纤接口，会针对自动链路协商设置速度。

默认连接器类型

有些型号包含两个连接器类型：铜缆 RJ-45 和光纤 SFP。 RJ-45 是默认接口。可以将 ASA 配置为使用光纤 SFP 连接器。

默认 MAC 地址

默认情况下，物理接口使用烧录 MAC 地址，物理接口的所有子接口均使用相同的烧录 MAC 地址。

开始接口配置 （ASA 5512-X 及更高版本）

- 第 9-12 页的开始接口配置的任务流程
- 第 9-13 页的启用物理接口并配置以太网参数
- 第 9-15 页的配置冗余接口
- 第 9-17 页的配置 EtherChannel
- 第 9-20 页的配置 VLAN 子接口和 802.1Q 中继
- 第 9-21 页的启用巨型帧支持
- 第 9-22 页的将使用中的接口转换为冗余接口或 EtherChannel 接口

开始接口配置的任务流程

注　如果拥有现有配置，并且要将使用中的接口转换为冗余接口或 EtherChannel 接口，请脱机执行配置以最大程度减少中断。请参阅第 9-22 页的将使用中的接口转换为冗余接口或 EtherChannel 接口。

如要开始配置接口，请执行以下步骤：

步骤 1　（多情景模式）在系统执行空间中完成本节所述的所有任务。如要从该情景切换至系统执行空间，请输入 **changeto system** 命令。

步骤 2　启用物理接口，或者更改以太网参数。请参阅第 9-13 页的启用物理接口并配置以太网参数。

默认情况下，物理接口已禁用。

步骤 3　（可选）配置冗余接口对。请参阅第 9-15 页的配置冗余接口。

逻辑冗余接口将一个主用接口和一个备用物理接口进行配对。如果主用接口发生故障，备用接口将激活并开始传输流量。

步骤 4　（可选）配置 EtherChannel。请参阅第 9-17 页的配置 EtherChannel。

一个 EtherChannel 将多个以太网接口分组到一个逻辑接口中。

步骤 5　（可选）配置 VLAN 子接口。请参阅第 9-20 页的配置 VLAN 子接口和 802.1Q 中继。

步骤 6　（可选）根据第 9-21 页的启用巨型帧支持启用巨型帧支持。

步骤 7　（仅限多情景模式）如要在系统执行空间中完成接口配置，请执行第 6 章，“多情景模式”中所述的以下任务：

- 要将接口分配给情景，请参阅第 6-18 页的配置安全情景。
- （可选）要将唯一的 MAC 地址自动分配给情景接口，请参阅第 6-22 页的自动为情景接口分配 MAC 地址。

MAC 地址用于在情景中对数据包进行分类。如果共享一个接口但每个情景中没有该接口的唯一 MAC 地址，将会使用目标 IP 地址对数据包进行分类。或者，可以按照第 11-7 页的配置 MAC 地址、 MTU 和 TCP MSS中所述在情景中手动分配 MAC 地址。

步骤 8　按照第 11 章，“路由模式接口”或第 12 章，“透明模式接口”中所述完成接口配置。

启用物理接口并配置以太网参数

本节介绍如何执行以下操作：

- 启用物理接口
- 设置特定的速度和双工 （如果有）
- 启用暂停帧以进行流量控制

先决条件

对于多情景模式，请在系统执行空间中完成本操作步骤。如要从该情景切换至系统执行空间，请输入 **changeto system** 命令。

详细步骤

	命令	用途
步骤 1	**interface** *physical_interface* **示例：** `ciscoasa(config)# interface gigabitethernet 0/0`	指定要配置的接口。 其中，*physical_interface* ID 包含类型、插槽和端口号，其格式为 *type*[*slot*/]*port*。 物理接口类型包括： • **千兆以太网** • **10 千兆以太网** • **管理** 依次输入类型和*插槽*/*端口*，例如 **gigabitethernet0/1**。类型与插槽/端口之间的空格是可选的。

	命令	用途
步骤 2	（可选） **media-type sfp** **示例：** ciscoasa(config-if)# media-type sfp	将媒体类型设置为 SFP（如果适用）。要恢复默认 RJ-45，请输入 **media-type rj45** 命令。
步骤 3	（可选） **speed** {**auto** | **10** | **100** | **1000** | **nonegotiate**} **示例：** ciscoasa(config-if)# speed 100	设置速度。 RJ-45 接口的默认设置为 **auto**。 SFP 接口的默认设置为 **no speed nonegotiate**；此默认设置将速度设置为最大速度，并启用流量控制参数和远程故障信息的链路协商。**nonegotiate** 关键字是唯一可用于 SFP 接口的关键字。**speed nonegotiate** 命令禁用链路协商。
步骤 4	（可选） **duplex** {**auto** | **full** | **half**} **示例：** ciscoasa(config-if)# duplex full	设置 RJ-45 接口的双工。**auto** 设置是默认设置。 **注**　EtherChannel 接口的双工设置必须为 Full 或 Auto。
步骤 5	（可选） **flowcontrol send on** [*low_water high_water pause_time*] [**noconfirm**] **示例：** ciscoasa(config-if)# flowcontrol send on 95 200 10000	启用暂停 (XOFF) 帧可对千兆以太网接口和 10 千兆以太网接口进行流量控制。 如果流量激增，数据包会在激增量超过 NIC 上的 FIFO 缓冲区的缓冲容量且接收环缓冲的情况下发生中断。启用暂停帧来进行流量控制可缓解此问题。暂停 (XOFF) 和 XON 帧根据 FIFO 缓冲区的使用量由 NIC 硬件自动生成。如果缓冲区使用量超过高水位，会发送暂停帧。默认的 *high_water* 值为 128 KB（10 千兆以太网）和 24 KB（千兆以太网）；可以将此值设置为介于 0 到 511（10 千兆以太网）或介于 0 到 47 KB（千兆以太网）之间的值。发送暂停后，当缓冲区使用量降低到低水位以下时，可发送 XON 帧。默认的 *low_water* 值为 64 KB（10 千兆以太网）和 16 KB（千兆以太网）；可以将此值设置为介于 0 到 511（10 千兆以太网）或介于 0 到 47 KB（千兆以太网）之间的值。链路伙伴可能会在接收 XON 后或 XOFF 到期后耗用流量，具体由暂停帧中的计时器值控制。默认的 *pause_time* 值为 26624；可以将此值设置为介于 0 到 65535 之间的值。如果缓冲区使用量始终在高水位之上，将会重复发送暂停帧（具体由暂停刷新阈值控制）。 使用此命令时，系统会显示以下警告： `Changing flow-control parameters will reset the interface.Packets may be lost during the reset. Proceed with flow-control changes?` 如要在没有提示的情况下更改参数，请使用 **noconfirm** 关键字。 **注**　仅支持 802.3x 中定义的流量控制帧。不支持基于优先级的流量控制。
步骤 6	**no shutdown** **示例：** ciscoasa(config-if)# no shutdown	启用接口。如要禁用该接口，请输入 **shutdown** 命令。如果输入 **shutdown** 命令，则还可关闭所有子接口。如果关闭系统执行空间中的接口，则该接口在共享它的所有情景中关闭。

后续操作

可选任务：

- 配置冗余接口对。请参阅第 9-15 页的配置冗余接口。
- 配置 EtherChannel。请参阅第 9-17 页的配置 EtherChannel。
- 配置 VLAN 子接口。请参阅第 9-20 页的配置 VLAN 子接口和 802.1Q 中继。
- 配置巨型帧支持。请参阅第 9-21 页的启用巨型帧支持。

必要任务：

- 对于多情景模式，请将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 6-14 页的配置多情景。
- 对于单情景模式，请完成接口配置。请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。

配置冗余接口

一个逻辑冗余接口包括一对物理接口：主用和备用接口。如果主用接口发生故障，备用接口将激活并开始传输流量。可以配置冗余接口来提高 ASA 的可靠性。此功能独立于设备级故障转移，但您可以在必要时配置冗余接口和故障转移。

本节介绍如何配置冗余接口。

- 第 9-15 页的配置冗余接口
- 第 9-16 页的更改主用接口

配置冗余接口

本节介绍如何创建冗余接口。默认情况下，冗余接口已启用。

准则和限制

- 最多可以配置 8 个冗余接口对。
- 冗余接口延迟值可配置，但在默认情况下，ASA 根据其成员接口的物理类型继承默认延迟值。
- 另请参阅第 9-11 页的冗余接口准则。

先决条件

- 两个成员接口必须为相同的物理类型。例如，两个都必须是千兆以太网接口。
- 不能将已配置了名称的物理接口添加到冗余接口。若要这样做，必须先使用 **no nameif** 命令移除名称。
- 对于多情景模式，请在系统执行空间中完成本操作步骤。如要从该情景切换至系统执行空间，请输入 **changeto system** 命令。

注意事项　如果使用已在配置中的物理接口，移除该接口的名称将会清除引用该接口的任何配置。

详细步骤

	命令	用途
步骤 1	**interface redundant** *number* **示例：** `ciscoasa(config)# interface redundant 1`	添加逻辑冗余接口，其中 *number* 参数是介于 1 到 8 之间的整数。 **注**　如要配置冗余接口的逻辑参数（例如名称），需要先向该接口至少添加一个成员接口。
步骤 2	**member-interface** *physical_interface* **示例：** `ciscoasa(config-if)# member-interface gigabitethernet 0/0`	将第一个成员接口添加到冗余接口。 有关物理接口 ID 的说明，请参阅第 9-13 页的启用物理接口并配置以太网参数。 冗余接口不支持作为成员的管理*插槽/端口*接口。 添加该接口后，将移除其任何配置（例如 IP 地址）。
步骤 3	**member-interface** *physical_interface* **示例：** `ciscoasa(config-if)# member-interface gigabitethernet 0/1`	将第二个成员接口添加到冗余接口。 确保第二个接口的物理类型与第一个接口相同。 如要移除成员接口，请输入 **no member-interface** *physical_interface* 命令。您无法从冗余接口中删除两个成员接口；冗余接口至少需要一个成员接口。

示例

以下示例将创建两个冗余接口：

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

后续操作

可选任务：

- 配置 VLAN 子接口。请参阅第 9-20 页的配置 VLAN 子接口和 802.1Q 中继。
- 配置巨型帧支持。请参阅第 9-21 页的启用巨型帧支持。

必要任务：

- 对于多情景模式，请将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 6-14 页的配置多情景。
- 对于单情景模式，请完成接口配置。请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。

更改主用接口

默认情况下，主用接口 （如果有）是配置中列出的第一个接口。如要查看哪个接口是主用接口，请在 工具中输入以下命令：

```
ciscoasa# show interface redundantnumber detail | grep Member
```

例如：

```
ciscoasa# show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

如要更改主用接口，请输入以下命令：

```
ciscoasa# redundant-interface redundantnumber active-member physical_interface
```

其中，**redundant***number* 参数是冗余接口 ID，例如 **redundant1**。

physical_interface 是想激活的成员接口 ID。

配置 EtherChannel

本节介绍如何创建 EtherChannel 端口通道接口，如何将接口分配给 EtherChannel，以及如何自定义 EtherChannel。

- 第 9-17 页的将接口添加到 EtherChannel
- 第 9-19 页的自定义 EtherChannel

将接口添加到 EtherChannel

本节介绍如何创建 EtherChannel 端口通道接口并向 EtherChannel 分配接口。默认情况下，端口通道接口已启用。

准则和限制

- 最多可配置 48 个 EtherChannel。
- 每个通道组最多可以有 16 个主用接口。对于仅支持 8 个主用接口的交换机，最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。
- 如要配置集群的跨网络 EtherChannel，请参阅第 8-38 页的配置跨网络 EtherChannel而不是此操作步骤。
- 另请参阅第 9-11 页的 EtherChannel 准则。

先决条件

- 通道组中的所有接口必须具有相同的类型、速度和双工。不受支持半双工。
- 不能将已配置了名称的物理接口添加到通道组。若要这样做，必须先使用 **no nameif** 命令移除名称。
- 对于多情景模式，请在系统执行空间中完成本操作步骤。如要从该情景切换至系统执行空间，请输入 **changeto system** 命令。

注意事项　如果使用已在配置中的物理接口，移除该接口的名称将会清除引用该接口的任何配置。

详细步骤

	命令	用途
步骤 1	**interface** *physical_interface* **示例：** `ciscoasa(config)# interface gigabitethernet 0/0`	指定要添加到通道组的接口，其中，*physical_interface* ID 包含类型、插槽和端口号，其格式为 *type*[*slot*/]*port*。通道组中的第一个接口决定了该组中所有其他接口的类型和速度。 在透明模式中，如果用多个管理接口创建一个通道组，可以将 EtherChannel 用作管理专用接口。
步骤 2	**channel-group** *channel_id* **mode** {**active** | **passive** | **on**} **示例：** `ciscoasa(config-if)# channel-group 1 mode active`	将物理接口分配给 *channel_id* 介于 1 到 48 之间的 EtherChannel。如果此通道 ID 的端口通道接口尚未存在于配置中，将会添加一个： **interface port-channel** *channel_id* 我们建议使用 **Active** 模式。有关主用模式、备用模式和开启模式的信息，请参阅第 9-6 页的链路聚合控制协议。
步骤 3	（可选） **lacp port-priority** *number* **示例：** `ciscoasa(config-if)# lacp port-priority 12345`	将通道组中物理接口的优先级设置为一个介于 1 到 65535 之间的值。默认值为 32768。数值越大，优先级越低。如果分配的接口多于可用的接口，ASA 将使用此设置决定哪些接口是主用接口，哪些是备用接口。如果所有接口的端口优先级设置都是相同的，则优先级由接口 ID（插槽/端口）确定。最低的接口 ID 优先级最高。例如，千兆以太网 0/0 的优先级高于千兆以太网 0/1 的优先级。 如果要将某个接口优先确定为主用接口，即使它具有较高的接口 ID，请将此命令设置为具有较低的值。例如，如要使千兆以太网 1/3 在千兆以太网 0/7 之前变为主用接口，请将 1/3 接口上的 **lacp port-priority** 值更改为 12345，将 0/7 接口上的这个值更改为默认值 32768。 如果 EtherChannel 另一端的设备端口存在优先级冲突，将会使用系统优先级来确定使用哪些端口优先级。请参阅第 9-19 页的自定义 EtherChannel中的 **lacp system-priority** 命令。
步骤 4	对于要添加到通道组中的每个接口，请重复第 1 步到第 3 步。	通道组中的所有接口必须具有相同的类型和速度。不受支持半双工。如果添加不匹配的接口，接口在添加后将处于暂停状态。

后续操作

可选任务：

- 自定义 EtherChannel 接口。请参阅第 9-19 页的自定义 EtherChannel。
- 配置 VLAN 子接口。请参阅第 9-20 页的配置 VLAN 子接口和 802.1Q 中继。

必要任务：

- 对于多情景模式，请将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 6-14 页的配置多情景。
- 对于单情景模式，请完成接口配置。请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。

自定义 EtherChannel

本节介绍如何设置 EtherChannel 中的最大接口数量， EtherChannel 要成为主用接口所需的最小操作接口数量、负载均衡算法以及其他可选参数。

详细步骤

	命令	用途
步骤 1	**interface port-channel** *channel_id* **示例：** `ciscoasa(config)# interface port-channel 1`	指定端口通道接口。在将接口添加到通道组时，将自动创建此接口。如果尚未添加接口，此命令会创建端口通道接口。 **注**　要配置端口通道接口的逻辑参数（例如名称），需要先向该接口至少添加一个成员接口。
步骤 2	**lacp max-bundle** *number* **示例：** `ciscoasa(config-if)# lacp max-bundle 6`	指定通道组中允许的最大主用接口数量（1 到 16）。默认值为 16。如果交换机不支持 16 个主用接口，请务必将此命令设置为 8 或更小的值。
步骤 3	**port-channel min-bundle** *number* **示例：** `ciscoasa(config-if)# port-channel min-bundle 2`	指定端口通道接口要成为主用接口所需的最小主用接口数量（1 到 16）。默认值为 1。如果通道组中的主用接口数量小于这个值，端口通道接口将会发生故障，并可能会触发设备级故障转移。
步骤 4	**port-channel load-balance** {**dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port**} **示例：** `ciscoasa(config-if)# port-channel load-balance src-dst-mac`	配置负载均衡算法。默认情况下，ASA 根据数据包的源 IP 地址和目标 IP 地址 (**src-dst-ip**) 来平衡接口上的数据包负载。如果要更改数据包分类所依据的属性，请使用此命令。例如，如果流量严重偏向于相同的源 IP 地址和目标 IP 地址，那么，分配给 EtherChannel 中的接口的流量将失去平衡。更改为其他算法可使流量分布更均匀。有关负载均衡的详细信息，请参阅第 9-6 页的负载均衡。
步骤 5	**lacp system-priority** *number* **示例：** `ciscoasa(config)# lacp system-priority 12345`	设置 LACP 系统的优先级（1 到 65535）。默认值为 32768。数值越大，优先级越低。对于 ASA 来说，此命令是全局的。 如果 EtherChannel 另一端的设备端口存在优先级冲突，将会使用系统优先级来确定使用哪些端口优先级。有关 EtherChannel 中的接口优先级，请参阅第 9-17 页的将接口添加到 EtherChannel中的 **lacp port-priority** 命令。
步骤 6	（可选） 可以将端口通道接口的以太网属性设置为覆盖各个接口上设置的属性。	有关以太网命令，请参阅第 9-13 页的启用物理接口并配置以太网参数。此方法提供了设置这些参数的快捷键，因为通道组中所有接口的这些参数必须匹配。

后续操作

可选任务：

- 配置 VLAN 子接口。请参阅第 9-20 页的配置 VLAN 子接口和 802.1Q 中继。
- 配置巨型帧支持。请参阅第 9-21 页的启用巨型帧支持。

必要任务：

- 对于多情景模式，请将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 6-14 页的配置多情景。
- 对于单情景模式，请完成接口配置。请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。

配置 VLAN 子接口和 802.1Q 中继

子接口可用于将物理接口、冗余接口或 EtherChannel 接口分成标记有不同 VLAN ID 的多个逻辑接口。具有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 可使在给定的物理接口上保持流量分离，因此，可以增加可用于网络的接口数量，而无需添加额外的物理接口或 ASA。此功能对多情景模式尤其有用，使得可以向每个情景分配唯一的接口。

准则和限制

- 最大子接口数 - 如要确定您的型号可使用多少个 VLAN 子接口，请参阅第 9-9 页的ASA 5512-X 及更高版本接口的许可要求。
- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常也不想要物理接口传输流量，因为物理接口将传递未标记的数据包。此属性对冗余接口对中的主用物理接口以及 EtherChannel 链路同样适用。由于必须启用物理接口、冗余接口或 EtherChannel 接口才能使子接口允许流量通过，因此，请省去 **nameif** 命令，以确保物理接口、冗余接口或 EtherChannel 接口不允许流量通过。如果要使物理接口、冗余接口或 EtherChannel 接口允许未标记的数据包通过，可以如常配置 **nameif** 命令。有关完成接口配置的详细信息，请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。
- （ASA 5512-X 到 ASA 5555-X）不能在 Management 0/0 接口上配置子接口。
- ASA 不支持动态中继协议 (DTP)，因此，必须无条件地将连接的交换机端口配置到中继上。

先决条件

对于多情景模式，请在系统执行空间中完成本操作步骤。如要从该情景切换至系统执行空间，请输入 **changeto system** 命令。

详细步骤

	命令	用途
步骤 1	**interface** {*physical_interface* | **redundant** *number* | **port-channel** *number*}.*subinterface* **示例：** `ciscoasa(config)# interface 千兆以太网 0/1.100`	指定新的子接口。有关物理接口 ID 的说明，请参阅第 9-13 页的启用物理接口并配置以太网参数一节。 **redundant** *number* 参数是冗余接口 ID，例如 **redundant 1**。 **port-channel** *number* 参数是 EtherChannel 接口 ID，如 **port-channel 1**。 *子接口* ID 是介于 1 和 4294967293 之间的整数。

	命令	用途
步骤 2	**vlan** *vlan_id* **示例：** `ciscoasa(config-subif)# vlan 101`	指定子接口的 VLAN。*vlan_id* 是介于 1 和 4094 之间的整数。某些 VLAN ID 可能保留在连接的交换机上，因此，请检查交换机文档了解详细信息。 一个子接口只能分配有一个 VLAN，且不能将同一个 VLAN 分配给多个子接口。无法将 VLAN 分配给物理接口。每个子接口必须有 VLAN ID 才能传输流量。要更改 VLAN ID，无需移除带有 **no** 选项的旧 VLAN ID；可以输入带有不同 VLAN ID 的 **vlan** 命令，这样 ASA 就会更改旧 ID。

后续操作

可选任务：

- 配置巨型帧支持。请参阅第 9-21 页的启用巨型帧支持。

必要任务：

- 对于多情景模式，请将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 6-14 页的配置多情景。
- 对于单情景模式，请完成接口配置。请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。

启用巨型帧支持

巨型帧是指大于标准最大字节数 （1518 字节）的以太网数据包 （包括第 2 层报头和 FCS），最大可达 9216 字节。可通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配更多内存可能会限制对其他功能的最充分利用，如 ACL。有关详细信息，请参阅第 9-6 页的用最大传输单元、 TCP 最大分段大小控制分片。

先决条件

- 在多情景模式中，请在系统执行空间中设置此选项。
- 如果更改此设置，需要重新加载 ASA。
- 请务必为需要向高于默认值 1500 的值传输巨型帧的每个接口设置 MTU；例如，使用 **mtu** 命令将该值设置为 9198。请参阅第 11-7 页的配置 MAC 地址、 MTU 和 TCP MSS。在多情景模式中，请在每个情景中设置 MTU。
- 请务必调整 TCP MSS，以对非 VPN 流量禁用此功能 （使用 **sysopt connection tcpmss 0** 命令），或者根据 MTU 增加 TCP MSS 的值 （如第 11-7 页的配置 MAC 地址、 MTU 和 TCP MSS中所述）。

详细步骤

命令	用途
jumbo-frame reservation **示例：** `ciscoasa(config)# jumbo-frame reservation`	启用巨型帧支持。要禁用巨型帧，请使用此命令的 **no** 形式。

示例

以下示例启用巨型帧保留，保存配置并重新加载 ASA：

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted.Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload?[confirm] Y
```

后续操作

- 对于多情景模式，请将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 6-14 页的配置多情景。
- 对于单情景模式，请完成接口配置。请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。

将使用中的接口转换为冗余接口或 EtherChannel 接口

如果拥有现有配置，并想要利用当前所用接口的冗余或 EtherChannel 接口功能，在转换到逻辑接口时，将会出现一段停机时间。

本节简要介绍如何在最短的停机时间内将现有的接口转换为冗余接口或 EtherChannel 接口。有关详细信息，请参阅第 9-15 页的配置冗余接口和第 9-17 页的配置 EtherChannel。

- 第 9-22 页的详细步骤 （单模式）
- 第 9-27 页的详细步骤 （多模式）

详细步骤 （单模式）

出于以下理由，我们建议在脱机状态下将配置更新为文本文件，并重新导入整个配置：

- 由于不能将已命名的接口添加为冗余接口或 EtherChannel 接口的成员，因此必须移除接口的名称。移除接口的名称后，引用该名称的任何命令都将被删除。由于引用接口名称的命令在整个配置中普遍存在且影响多个功能，因此，围绕新接口名称重新配置所有功能时，如果从 CLI 或 ASDM 中正在使用的接口移除名称，将会严重损坏配置和长时间停机。
- 在脱机状态下更改配置可以对新逻辑接口使用原来的接口名称，从而无需改变引用接口名称的功能配置。只需要更改接口配置。
- 清除运行配置并立即应用新配置可最大程度减少接口的停机时间。这样将无需等待实时配置接口。

步骤 1　连接 ASA；如果要使用故障转移，请连接到主用 ASA。

步骤 2　如果要使用故障转移，请输入 **no failover** 命令。

步骤 3　输入 **more system:running-config** 命令并将显示输出复制到文本编辑器中，以复制运行配置。

如果在编辑时出错，请务必保存旧配置的额外副本。

步骤 4　对于要添加到冗余接口或 EtherChannel 接口的每个使用中的接口，请在 **interface** 命令下将所有命令剪切并粘贴到接口配置部分的结尾，以用于创建新逻辑接口。以下命令是唯一的例外，这些命令应与物理接口配置放在一起：

- **media-type**
- **speed**
- **duplex**
- **flowcontrol**

注　只能将*物理*接口添加到 EtherChannel 或冗余接口；不能为物理接口配置 VLAN。

请务必在给定的 EtherChannel 或冗余接口中为所有接口匹配上述值。请注意，EtherChannel 接口的双工设置必须为 Full 或 Auto。

例如，接口配置如下。粗体的命令是要用于三个新 EtherChannel 接口的命令，应该将这些命令剪切并粘贴到接口部分的结尾。

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 no shutdown
!
```

```
interface Management0/1
 shutdown
 no nameif
 no security-level
 no ip address
```

步骤 5　在每个粘贴的命令部分上方，通过输入以下命令之一创建新逻辑接口：

- **interface redundant** *number* [1-8]
- **interface port-channel** *channel_id* [1-48]

例如：

```
...

interface port-channel 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 no shutdown
!
interface port-channel 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface port-channel 3
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 no shutdown
```

步骤 6　向新逻辑接口分配物理接口：

- 冗余接口 - 在新的 **interface redundant** 命令下输入以下命令：

  member-interface *physical_interface1*
  member-interface *physical_interface2*

  其中，物理接口是同一种类型的任意两个接口 （之前使用的或未使用的）。不能将管理接口分配给冗余接口。

  例如，要利用现有布线，应继续按其原来的角色使用之前使用的接口，以作为内部和外部冗余接口的一部分：

```
interface redundant 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 member-interface GigabitEthernet0/0
 member-interface GigabitEthernet0/2

interface redundant 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 member-interface GigabitEthernet0/1
 member-interface GigabitEthernet0/3
```

- EtherChannel 接口 - 在要添加到 EtherChannel 的每个接口下输入以下命令 （之前使用的或未使用的）。最多可以为每个 EtherChannel 分配 16 个接口，但只有 8 个接口可作为主用接口；其他接口在故障情况下处于备用状态。

  channel-group *channel_id* **mode active**

例如，要利用现有布线，应继续按其原来的角色使用之前使用的接口，以作为内部和外部 EtherChannel 接口的一部分：

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 shutdown
 no nameif
 no security-level
 no ip address

...
```

步骤 7　在 **shutdown** 命令前面添加 **no**，启用当前属于逻辑接口一部分的之前未使用的每个接口。

例如，最终 EtherChannel 配置如下：

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
!
```

```
interface GigabitEthernet0/2
 channel-group 1 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface port-channel 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
!
interface port-channel 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
!
interface port-channel 3
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
```

注　导入新配置后，可配置其他可选的 EtherChannel 参数。请参阅第 9-17 页的配置 EtherChannel。

步骤 8　在 ASA CLI 提示符后，根据连接 （控制台或远程）执行以下步骤。

- 控制台连接：
  a. 将整个新配置 （包括更改的接口部分）复制到剪贴板。

b. 输入以下命令以清除运行配置：

```
ciscoasa(config)# clear configure all
```

通过 ASA 的流量将会停止。

c. 在提示符后粘贴新配置。

通过 ASA 的流量将会恢复。

- 远程连接：

a. 将新配置保存到 TFTP 或 FTP 服务器，以便可以将其复制到 ASA 上的启动配置中。例如，可以在 PC 上运行 TFTP 或 FTP 服务器。

b. 输入以下命令以清除启动配置：

```
ciscoasa(config)# write erase
```

c. 输入以下命令，以将新配置复制到启动配置中：

```
ciscoasa(config)# copy url startup-config
```

请参阅第 36-15 页的将文件复制到 ASA。

d. 使用 **reload** 命令重新加载 ASA。请勿保存运行配置。

步骤 9　输入 **failover** 命令。

详细步骤 （多模式）

出于以下理由，我们建议在脱机状态下将系统和情景配置更新为文本文件，并重新导入这些配置：

- 由于不能将分配的接口添加为冗余接口或 EtherChannel 接口的成员，因此，必须从任何情景中解除接口分配。解除接口分配后，引用该接口的任何情景命令都将被删除。由于引用接口的命令在整个配置中普遍存在且影响多个功能，因此，围绕新接口重新配置所有功能时，如果从 CLI 或 ASDM 中正在使用的接口移除分配，将会严重损坏配置和长时间停机。
- 在脱机状态下更改配置可以对新逻辑接口使用原来的接口名称，从而无需改变引用接口名称的功能配置。只需要更改接口配置。
- 清除运行系统配置并立即应用新配置可最大程度减少接口的停机时间。这样将无需等待实时配置接口。

步骤 1　连接到 ASA 并更改系统；如果要使用故障转移，请连接到主用 ASA。

步骤 2　如果要使用故障转移，请输入 **no failover** 命令。

步骤 3　在系统中，输入 **more system:running-config** 命令 并将显示输出复制到文本编辑器，以复制运行配置。

如果在编辑时出错，请务必保存旧配置的额外副本。

例如，系统配置中具有以下接口配置和分配，且两个情景之间共享接口。

System

```
interface GigabitEthernet0/0
   no shutdown
interface GigabitEthernet0/1
   no shutdown
interface GigabitEthernet0/2
   shutdown
interface GigabitEthernet0/3
```

```
    shutdown
interface GigabitEthernet0/4
    shutdown
interface GigabitEthernet0/5
    shutdown
interface Management0/0
    no shutdown
interface Management1/0
    shutdown
!
context customerA
    allocate-interface gigabitethernet0/0 int1
    allocate-interface gigabitethernet0/1 int2
    allocate-interface management0/0 mgmt
context customerB
    allocate-interface gigabitethernet0/0
    allocate-interface gigabitethernet0/1
    allocate-interface management0/0
```

步骤 4　获取将使用新 EtherChannel 或冗余接口的*所有*情景配置的副本。请参阅第 36-23 页的备份和还原配置或其他文件。

例如，下载以下情景配置 （显示接口配置）：

CustomerA Context

```
interface int1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
!
interface int2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface mgmt
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 management-only
```

CustomerB Context

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.20.15.5 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.6.78 255.255.255.0
!
interface Management0/0
 nameif mgmt
 security-level 100
 ip address 10.8.1.8 255.255.255.0
 management-only
```

步骤 5　在系统配置中，按照第 9-15 页的配置冗余接口或第 9-17 页的配置 EtherChannel 中所述创建新逻辑接口。请务必在要用作逻辑接口一部分的任何附加物理接口上输入 **no shutdown** 命令。

注　只能将*物理*接口添加到 EtherChannel 或冗余接口；不能为物理接口配置 VLAN。

请务必在给定的 EtherChannel 或冗余接口中匹配所有接口的物理接口参数 （例如，速度和双工）。请注意， EtherChannel 接口的双工设置必须为 Full 或 Auto。

例如，新配置如下：

System

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 no shutdown
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 no shutdown
!
interface port-channel 1
interface port-channel 2
interface port-channel 3
```

步骤 6　更改每个情景的接口分配，以使用新的 EtherChannel 或冗余接口。请参阅第 6-18 页的配置安全情景。

例如，如要利用现有布线，应继续按其原来的角色使用之前使用的接口，以作为内部和外部冗余接口的一部分：

```
context customerA
    allocate-interface port-channel1 int1
    allocate-interface port-channel2 int2
    allocate-interface port-channel3 mgmt
context customerB
    allocate-interface port-channel1
    allocate-interface port-channel2
    allocate-interface port-channel3
```

注　如果尚未这样做，可能要借此机会将映射名称分配给接口。例如， customerA 的配置完全不需要更改；只需要将该配置重新应用于 ASA。但是， customerB 配置需要更改所有的接口 ID；如果为 customerB 分配映射名称，仍需要在情景配置中更改接口 ID，但映射名称可能会有助于将来进行接口更改。

步骤 7　对于不使用映射名称的情景，请将情景配置更改为使用新的 EtherChannel 或冗余接口 ID。（使用映射接口名称的情景不需要任何更改。）

例如：

CustomerB Context

```
interface port-channel1
 nameif outside
 security-level 0
 ip address 10.20.15.5 255.255.255.0
!
interface port-channel2
 nameif inside
 security-level 100
 ip address 192.168.6.78 255.255.255.0
!
interface port-channel3
 nameif mgmt
 security-level 100
 ip address 10.8.1.8 255.255.255.0
 management-only
```

步骤 8　用新的情景配置文件覆盖旧文件。例如，如果情景在 FTP 服务器上，可使用 FTP 复制现有文件（在必要时进行备份）。如果情景在闪存中，可以使用 **copy** 命令并在 PC 上运行 TFTP 或 FTP 服务器，或者使用安全复制。请参阅第 36-15 页的将文件复制到 ASA。此更改仅影响启动配置；运行配置仍使用旧的情景配置。

步骤 9　在 ASA 系统 CLI 提示符后，根据连接 （控制台或远程）执行以下步骤。

- 控制台连接：
  - **a.** 将整个新系统配置 （包括更改的接口部分）复制到剪贴板。
  - **b.** 输入以下命令以清除运行配置 （系统和情景）：

    ```
    ciscoasa(config)# clear configure all
    ```

    通过 ASA 的流量将会停止。
  - **c.** 在提示符后粘贴新系统配置。

    将会重新加载所有的新情景配置。重新加载完毕后，通过 ASA 的流量将会恢复。
- 远程连接：
  - **a.** 将新系统配置保存到 TFTP 或 FTP 服务器，以便可以将其复制到 ASA 上的启动配置中。例如，可以在 PC 上运行 TFTP 或 FTP 服务器。
  - **b.** 输入以下命令以清除启动配置：

    ```
    ciscoasa(config)# write erase
    ```
  - **c.** 输入以下命令，以将新系统配置复制到启动配置中：

    ```
    ciscoasa(config)# copy url startup-config
    ```

    请参阅第 36-15 页的将文件复制到 ASA。

d. 使用 **reload** 命令重新加载 ASA。请勿保存运行配置。

步骤 10　输入 **failover** 命令。

监控接口

命令	用途
show interface	显示接口统计信息。
show interface ip brief	显示接口的 IP 地址和状态。
show lacp {[*channel_group_number*] {**counters** | **internal** | **neighbor**} | **sys-id**}	对于 EtherChannel，显示 LACP 信息，例如流量统计信息、系统标识符和邻居详细信息。
show port-channel [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]	对于 EtherChannel，以详细的一行摘要形式显示 EtherChannel 信息。此命令还显示端口和端口通道信息。
show port-channel *channel_group_number* **load-balance** [**hash-result** {**ip** | **ipv6** | **l4port** | **mac** | **mixed** | **vlan-only**} *parameters*]	对于 EtherChannel，显示端口通道负载均衡信息以及为给定的一组参数选择的哈希结果和成员接口。

ASA 5512-X 及更高版本接口的配置示例

- 第 9-31 页的物理接口参数示例
- 第 9-31 页的子接口参数示例
- 第 9-32 页的多情景模式示例
- 第 9-32 页的 EtherChannel 示例

物理接口参数示例

以下示例在单模式中配置物理接口的参数：

```
interface gigabitethernet 0/1
    speed 1000
    duplex full
    no shutdown
```

子接口参数示例

以下示例在单模式中配置子接口的参数：

```
interface gigabitethernet 0/1.1
    vlan 101
    no shutdown
```

多情景模式示例

以下示例在多情景模式中配置系统配置的接口参数，并将千兆以太网 0/1.1 子接口分配给 contextA：

```
interface gigabitethernet 0/1
    speed 1000
    duplex full
    no shutdown
interface gigabitethernet 0/1.1
    vlan 101
context contextA
    allocate-interface gigabitethernet 0/1.1
```

EtherChannel 示例

以下示例将三个接口配置为 EtherChannel 的一部分。此示例还将系统优先级设置为较高的优先级，并在 EtherChannel 分配有超过 8 个接口的情况下将千兆以太网 0/2 的优先级设置得比其他接口更高。

```
lacp system-priority 1234
interface GigabitEthernet0/0
    channel-group 1 mode active
interface GigabitEthernet0/1
    channel-group 1 mode active
interface GigabitEthernet0/2
    lacp port-priority 1234
    channel-group 1 mode passive
interface Port-channel1
    lacp max-bundle 4
    port-channel min-bundle 2
    port-channel load-balance dst-ip
```

后续操作

- 在多情景模式中：
  a. 将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 6 章，“多情景模式”
  b. 按照第 11 章，“路由模式接口”或第 12 章，“透明模式接口”中所述完成接口配置。
- 对于单情景模式，请按照第 11 章，“路由模式接口”或第 12 章，“透明模式接口”中所述完成接口配置。

ASA 5512-X 及更高版本接口的功能历史记录

表 9-2 列出了此功能的版本历史记录。

表 9-2　　接口的功能历史记录

功能名称	版本	功能信息
增加的 VLAN 数量	7.0(5)	增加了以下限制： • ASA5510 基础许可证的 VLAN 数从 0 增加到 10。 • ASA5510 增强型安全许可证的 VLAN 数从 10 增加到 25。 • ASA5520 的 VLAN 数从 25 增加到 100。 • ASA5540 的 VLAN 数从 100 增加到 200。
ASA 5510 上基础许可证增加的接口数	7.2(2)	对于 ASA 5510 上的基础许可证，最大接口数从 3 个加上管理接口数，增至不受限制。
增加的 VLAN 数量	7.2(2)	提高了以下型号的 VLAN 上限：ASA 5510 的（对于基础许可证，从 10 提高到 50；对于增强型安全许可证，从 25 提高到 100）、ASA 5520（从 100 提高到 150）、ASA 5550（从 200 提高到 250）。
对于 ASA 5510 增强型安全许可证的千兆以太网支持	7.2(3)	现在，ASA 5510 ASA 通过增强型安全许可证为端口 0 和 1 提供 GE（千兆以太网）支持。如果从基础许可证升级至增强型安全许可证，则外部 Ethernet 0/0 和 Ethernet0/1 端口的容量将从原始的 FE（快速以太网）(100 Mbps) 增加到 GE (1000 Mbps)。接口名称仍保持为 Ethernet 0/0 和 Ethernet0/1。使用 **speed** 命令更改接口上的速度，使用 **show interface** 命令查看当前为每个接口配置的速度。
冗余接口	8.0(2)	逻辑冗余接口将一个主用接口和一个备用物理接口进行配对。如果主用接口发生故障，备用接口将激活并开始传输流量。可以配置冗余接口来提高 ASA 的可靠性。此功能独立于设备级故障转移，但您可以在必要时配置冗余接口和故障转移。最多可以配置 8 个冗余接口对。
对 ASA 5580 的巨型数据包支持	8.1(1)	思科 ASA 5580 支持巨型帧。巨型帧是一个以太网数据包，其大小大于标准的最大值 1518 字节（包括第 2 层报头和 FCS），最大可达 9216 字节。可通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配更多内存可能会限制对其他功能的最充分利用，如 ACL。 ASA 5585-X 也支持此功能。 我们引入了以下命令：**jumbo-frame reservation**。
为 ASA 5580 增加的 VLAN 数	8.1(2)	ASA 5580 支持的 VLAN 数量从 100 增加到 250。

表 9-2　　接口的功能历史记录（续）

功能名称	版本	功能信息
在 ASA 5580 的 10 千兆以太网接口上支持暂停帧以进行流量控制	8.2(2)	现可为流量控制启用暂停 (XOFF) 帧。 ASA 5585-X 也支持此功能。 我们引入了以下命令：**flowcontrol**。
在千兆以太网接口上支持暂停帧以进行流量控制	8.2(5)/8.4(2)	现在，可以在所有型号的千兆以太网接口上启用暂停 (XOFF) 帧以进行流量控制。 我们修改了以下命令：**flowcontrol**。
EtherChannel 支持	8.4(1)	可以为八个主用接口各配置多达 48 个 802.3ad EtherChannel。 我们引入了以下命令：**channel-group**、**lacp port-priority**、**interface port-channel**、**lacp max-bundle**、**port-channel min-bundle**、**port-channel load-balance**、**lacp system-priority**、**clear lacp counters**、**show lacp**、**show port-channel**。 **注**　ASA 5505 不支持 EtherChannel。
一个 EtherChannel 中支持 16 个活动链路	9.2(1)	现在，在一个 EtherChannel 中最多可以配置 16 个活动链路。以前可以有 8 个活动链路和 8 个备用链路。确保交换机可以支持 16 个活动链路（例如，可使用带有 F2 系列 10 千兆以太网模块的思科 Nexus 7000）。 **注**　如果从较低 ASA 版本进行升级，为了实现兼容，可将最大主用接口数量设置为 8（**lacp max-bundle** 命令）。 我们修改了以下命令：**lacp max-bundle** 和 **port-channel min-bundle**。

基本接口配置 (ASAv)

本章包含启动思科 ASAv 接口配置的任务，包括配置以太网设置、冗余接口和 VLAN 子接口。

- 第 10-1 页的有关启动 ASAv 接口配置的信息
- 第 10-6 页的 ASAv 接口的许可要求
- 第 10-6 页的准则和限制
- 第 10-7 页的默认设置
- 第 10-7 页的开始接口配置 (ASAv)
- 第 10-13 页的监控接口
- 第 10-13 页的 ASAv 接口的配置示例
- 第 10-14 页的后续操作
- 第 10-14 页的 ASAv 接口的功能历史记录

有关启动 ASAv 接口配置的信息

- 第 10-1 页的 ASAv 接口和虚拟 NIC
- 第 10-3 页的处于透明模式中的接口
- 第 10-3 页的管理接口
- 第 10-4 页的冗余接口
- 第 10-4 页的用最大传输单元、 TCP 最大分段大小控制分片

ASAv 接口和虚拟 NIC

作为虚拟化平台上的访客，ASAv 使用基础物理平台的网络接口。每个 ASAv 接口映射到一个虚拟 NIC (vNIC)。

- 第 10-2 页的 ASAv 接口
- 第 10-2 页的受支持的 vNIC
- 第 10-2 页的 ASAv 接口与 VMware 中 vNIC 的一致性

ASAv 接口

ASAv 包括以下千兆以太网接口：

- Management 0/0
- GigabitEthernet 0/0 至 0/8。注意，如果将 ASAv 部署为故障转移对的一部分，则 GigabitEthernet 0/8 用于故障转移链路。

受支持的 vNIC

ASAv 支持以下 vNIC：

vNIC 类型	虚拟机监控程序支持		ASAv 版本	备注
	Vmware	KVM		
VMXNET3	是	否	9.2(1) 及更高版本	如在使用 VMXNET3，则需禁用 Large Receive Offload (LRO)，以免 TCP 性能不佳。请参阅以下有关 VMware 支持的文章: http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1027511 http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=2055140
e1000	是	是	9.2(1) 及更高版本	默认值。

ASAv 接口与 VMware 中 vNIC 的一致性

vSphere Client Virtual Machine Properties 屏幕（右键单击 ASAv 实例，并选择 **Edit Settings**）显示每个网络适配器和已分配的网络。但是，该屏幕不会显示 ASAv 接口 ID（仅网络适配器 ID）。请参阅网络适配器 ID 与 ASAv ID 的以下一致性：

网络适配器 ID	ASAv 接口 ID
网络适配器 1	Management0/0
网络适配器 2	GigabitEthernet0/0
网络适配器 3	GigabitEthernet0/1
网络适配器 4	GigabitEthernet0/2
网络适配器 5	GigabitEthernet0/3
网络适配器 6	GigabitEthernet0/4
网络适配器 7	GigabitEthernet0/5
网络适配器 8	GigabitEthernet0/6
网络适配器 9	GigabitEthernet0/7
网络适配器 10	GigabitEthernet0/8

处于透明模式中的接口

处于透明模式中的接口属于“网桥组”，每个网络都有一个网桥组。处于透明模式中的接口属于“网桥组”，每个网络都有一个网桥组。有关网桥组的详细信息，请参阅第 12-1 页的透明模式的网桥组。

管理接口

- 第 10-3 页的管理接口概述
- 第 10-3 页的将任何接口用于仅管理流量
- 第 10-3 页的用于透明模式的管理接口
- 第 10-3 页的不支持直通流量

管理接口概述

可以通过连接到以下接口来管理 ASA：

- 任何直通流量接口
- 专用 Management 0/0 接口

可能需要按照第 35 章，“管理访问”中所述配置对接口的管理访问。

将任何接口用于仅管理流量

可将任何接口用作管理专属接口，只需将其配置为用于管理流量 （请参阅 **management-only** 命令）。

用于透明模式的管理接口

在透明防火墙模式中，除了允许的最大直通流量接口数，还可以将 Management 0/0 接口 （物理接口或子接口）用作单独的管理接口。不能将任何其他接口类型用作管理接口。管理接口不属于普通网桥组的一部分。请注意，出于操作目的，管理接口属于不可配置网桥组的一部分。

注　在透明防火墙模式中，管理接口以与数据接口相同的方式更新 MAC 地址表；因此，不应将管理和数据接口连接到同一个交换机，除非将其中一个交换机端口配置为路由端口（默认情况下，Catalyst 交换机在所有的 VLAN 交换机端口上共享一个 MAC 地址）。否则，如果流量从物理连接的交换机到达管理接口，ASA 会更新 MAC 地址表，以使用*管理*接口（而不是数据接口）来访问交换机。此操作会导致临时流量中断；出于安全原因，ASA 至少在 30 秒内不会再次更新从交换机到数据接口的数据包 MAC 地址表。

不支持直通流量

Management 0/0 接口始终设置为仅管理；该接口不可用于直通流量支持。

冗余接口

一个逻辑冗余接口包括一对物理接口：主用和备用接口。如果主用接口发生故障，备用接口将激活并开始传输流量。可以配置冗余接口来提高 ASA 的可靠性。此功能独立于设备级故障转移，如果需要，可以配置冗余接口和设备级故障转移。

冗余接口 MAC 地址

冗余接口使用您添加的第一个物理接口的 MAC 地址。如果在配置中更改成员接口的顺序，则 MAC 地址发生更改，以匹配现第一个列出的接口的 MAC 地址。或者，无论成员接口 MAC 地址如何，均可以将 MAC 址址分配给冗余接口 （请参阅第 11-7 页的配置 MAC 地址、 MTU 和 TCP MSS或第 6-14 页的配置多情景）。如果主用接口故障转移到备用接口，系统将维护同一 MAC 地址，以防流量中断。

用最大传输单元、 TCP 最大分段大小控制分片

- 第 10-4 页的 MTU 概述
- 第 10-4 页的默认 MTU
- 第 10-5 页的路径 MTU 发现
- 第 10-5 页的设置 MTU 和巨型帧
- 第 10-5 页的 TCP 最大分段大小概述
- 第 10-5 页的默认 TCP MSS
- 第 10-5 页的设置 VPN 和非 VPN 流量的 TCP MSS
- 第 10-6 页的示例

MTU 概述

最大传输单元 (MTU) 指定 ASA 可在给定以太网接口上传输的最大帧负载大小。MTU 值是*没有*以太网报头、FCS 或 VLAN 标记的帧大小。以太网报头为 14 字节，而 FCS 为 4 字节。如果将 MTU 设置为 1500，预期的帧大小 （包括报头）为 1518 字节。如果使用 VLAN 标记 （这样将会增加额外 4 字节），并将 MTU 设置为 1500，预期的帧大小为 1522。请勿为容纳这些报头而将 MTU 的值设得过高。对于容纳封装 TCP 报头的信息，请勿修改 MTU 设置；相反，请更改 TCP 最大分片大小 (第 10-5 页的 TCP 最大分段大小概述)。

注　只要有内存空间，ASA 就可接收大于所配置的 MTU 的帧。有关如何增加内存以接收较大的帧，请参阅第 10-12 页的启用巨型帧支持。

默认 MTU

ASA 上的默认 MTU 为 1500 字节。此值不包括以太网报头、CRC、VLAN 标记等的 18 个或更多字节。

路径 MTU 发现

ASA 支持路径 MTU 发现 （如 RFC 1191 中定义），允许两台主机之间网络路径中的所有设备均与 MTU 协调，以便能够对路径中的最小 MTU 进行标准化。

设置 MTU 和巨型帧

请参阅第 11-7 页的配置 MAC 地址、 MTU 和 TCP MSS。

请参阅第 10-12 页的启用巨型帧支持。

请参阅以下准则：

- 与流量路径上的 MTU 相匹配 - 我们建议将所有 ASA 接口以及流量路径的其他设备接口上的 MTU 设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧 - 如果启用巨型帧，则可将 MTU 设置为高达 9000 字节。

TCP 最大分段大小概述

TCP 最大分段尺寸 (TCP MSS) 是 TCP 负载在添加任何 TCP 报头*之前*的大小。UDP 数据包不会受到影响。建立连接时，客户端和服务器会在三次握手期间交换 TCP MSS 值。

可以在 ASA 上设置 TCP MSS。如果一个连接的任意终端要求 TCP MSS 的值大于 ASA 上设置的值，则 ASA 将用 ASA 最大值覆盖请求数据包内的 TCP MSS。如果主机或服务器不请求 TCP MSS，则 ASA 会假设 RFC 793 的默认值为 536 字节，但不会修改数据包。您还可以配置最小 TCP MSS；如果主机或服务器请求一个非常小的 TCP MSS，则 ASA 可将该值调高。默认情况下，最小 TCP MSS 未启用。

例如，可以将默认 MTU 配置为 1500 字节。主机请求 1700 的 MSS。如果 ASA 的最大 TCP MSS 是 1380， ASA 会将 TCP 请求数据包中的 MSS 值更改为 1380。然后，服务器会发送 1380 字节的数据包。

默认 TCP MSS

默认情况下，ASA 上的最大 TCP MSS 是 1380 字节。此默认值符合 VPN 连接的要求（在 VPN 连接中，报头最多可增加 120 字节）；此值在默认 MTU（1500 字节）范围内。

设置 VPN 和非 VPN 流量的 TCP MSS

请参阅第 11-7 页的配置 MAC 地址、 MTU 和 TCP MSS。

请参阅以下准则：

- 非 VPN 流量 - 如果不使用 VPN 且不需要额外的报头空间，应该禁用 TCP MSS 限制并接受连接终端之间建立的值。由于连接终端一般是从 MTU 获得 TCP MSS，因此，非 VPN 数据包通常符合此 TCP MSS。
- VPN 流量 - 将最大 TCP MSS 设置为 MTU - 120。例如，如果使用巨型帧并将 MTU 设置为较大的值，需要将 TCP MSS 设置为符合新的 MTU。

示例

以下示例将启用巨型帧、增加所有接口上的 MTU 并为非 VPN 流量禁用 TCP MSS（将 TCP MSS 设置为 0，表示无限制）：

```
jumbo frame-reservation
mtu inside 9000
mtu outside 9000
sysopt connection tcpmss 0
```

以下示例将启用巨型帧、增加所有接口上的 MTU，并将 VPN 流量的 TCP MSS 更改为 8880（MTU 减去 120）：

```
jumbo frame-reservation
mtu inside 9000
mtu outside 9000
sysopt connection tcpmss 8880
```

ASAv 接口的许可要求

型号	许可证要求
带 1 个虚拟 CPU 的 ASAv	VLAN： 　　标准许可证和高级许可证：50 所有类型的接口： 　　标准许可证和高级许可证：716
带 4 个虚拟 CPU 的 ASAv	VLAN： 　　标准许可证和高级许可证：200 所有类型的接口： 　　标准许可证和高级许可证：1316

注　对于根据 VLAN 限制计数的接口，您必须为它分配一个 VLAN。例如：
interface gigabitethernet 0/0.100
vlan 100

所有类型的接口均包括最大数量的组合接口；例如，VLAN、物理、冗余和网桥组接口。在配置中定义的每个 **interface** 命令均根据此限制进行计数。

准则和限制

本节包括此功能的准则和限制。

防火墙模式准则

- 对于透明模式，您可以配置多达 8 个网桥组。
- 每个网桥组最多可包括 4 个接口。

故障转移准则

- 如果将冗余接口用作故障转移链路，则必须在故障转移对中的两台设备上对其进行预配置；由于*故障转移链路本身需用于复制*，因此，您不能在主要设备上对其进行配置，也不能期望将其复制到次要设备。
- 如果将冗余接口用于状态链路，无需特别配置；该配置可照常从主要设备复制。
- 可使用 **monitor-interface** 命令监控用于故障转移的冗余接口；请务必引用逻辑冗余接口名称。如果主用成员接口故障转移到备用接口，监控设备级故障转移时，本活动不导致冗余接口故障。只有当所有物理接口均发生故障时，冗余接口才会发生故障。
- 不能与数据接口共享一个故障转移接口或状态接口。

冗余接口准则

- 最多可以配置 8 个冗余接口对。
- 所有 ASA 配置均引用逻辑冗余接口，而不是成员物理接口。
- 如果关闭主用接口，则将激活备用接口。
- 冗余接口不能设置为仅管理。
- 有关故障转移准则，请参阅第 10-7 页的故障转移准则。

默认设置

本节列出了接口的默认设置 （如果没有出厂默认配置）。有关出厂默认配置的信息，请参阅第 2-12 页的出厂默认配置。

接口的默认状态

- 物理接口 - 已禁用。
- 冗余接口 - 已启用。但是，对于通过冗余接口的流量，还必须启用成员物理接口。
- 子接口 - 已启用。但是，对于通过子接口的流量，还必须启用物理接口。

默认速度和双工

- 默认情况下，接口的速度和双工设置为自动协商。

默认 MAC 地址

默认情况下，物理接口使用烧录 MAC 地址，物理接口的所有子接口均使用相同的烧录 MAC 地址。

默认 vNIC

所有接口均使用 E1000 仿真。

开始接口配置 (ASAv)

- 第 10-8 页的开始接口配置的任务流程
- 第 10-8 页的启用物理接口并配置以太网参数
- 第 10-9 页的配置冗余接口
- 第 10-11 页的配置 VLAN 子接口和 802.1Q 中继
- 第 10-12 页的启用巨型帧支持

开始接口配置的任务流程

如要开始配置接口，请执行以下步骤：

步骤 1　启用物理接口，或者更改以太网参数。请参阅第 10-8 页的启用物理接口并配置以太网参数。

默认情况下，物理接口已禁用。

步骤 2　（可选）配置冗余接口对。请参阅第 10-9 页的配置冗余接口。

逻辑冗余接口将一个主用接口和一个备用物理接口进行配对。如果主用接口发生故障，备用接口将激活并开始传输流量。

步骤 3　（可选）配置 VLAN 子接口。请参阅第 10-11 页的配置 VLAN 子接口和 802.1Q 中继。

步骤 4　（可选）根据第 10-12 页的启用巨型帧支持启用巨型帧支持。

启用物理接口并配置以太网参数

本节介绍如何执行以下操作：

- 启用物理接口
- 设置特定速度和双工
- 启用暂停帧以进行流量控制

详细步骤

	命令	用途
步骤 1	**interface** *physical_interface* **示例：** `ciscoasa(config)# interface gigabitethernet 0/0`	指定要配置的接口。 其中，*physical_interface* ID 包含类型、插槽和端口号，其格式为 *type*[*slot*/]*port*。 物理接口类型包括： • **千兆以太网** • **管理** 依次输入类型和*插槽*/*端口*，例如 **gigabitethernet0/1**。类型与插槽/端口之间的空格是可选的。
步骤 2	（可选） **speed** {**auto** | **10** | **100** | **1000**} **示例：** `ciscoasa(config-if)# speed 100`	设置速度。默认设置为 **auto**。
步骤 3	（可选） **duplex** {**auto** | **full** | **half**} **示例：** `ciscoasa(config-if)# duplex full`	设置双工。**auto** 设置是默认设置。

	命令	用途
步骤 4	（可选） **flowcontrol send on** [*low_water high_water pause_time*] [**noconfirm**] **示例：** `ciscoasa(config-if)# flowcontrol send on 95 200 10000`	为流量控制启用暂停 (XOFF) 帧。 如果流量激增，数据包会在激增量超过 NIC 上的 FIFO 缓冲区的缓冲容量且接收环缓冲的情况下发生中断。启用暂停帧来进行流量控制可缓解此问题。暂停 (XOFF) 和 XON 帧根据 FIFO 缓冲区的使用量由 NIC 硬件自动生成。如果缓冲区使用量超过高水位，会发送暂停帧。默认的 *high_water* 值为 24 KB；该值可以设置在 0 至 47 KB 之间。发送暂停后，当缓冲区使用量降低到低水位以下时，可发送 XON 帧。默认的 *low_water* 值为 16 KB；该值可以设置在 0 至 47 KB 之间。链路伙伴可能会在接收 XON 后或 XOFF 到期后耗用流量，具体由暂停帧中的计时器值控制。默认的 *pause_time* 值为 26624；可以将此值设置为介于 0 到 65535 之间的值。如果缓冲区使用量始终在高水位之上，将会重复发送暂停帧（具体由暂停刷新阈值控制）。 使用此命令时，系统会显示以下警告： `Changing flow-control parameters will reset the interface.Packets may be lost during the reset. Proceed with flow-control changes?` 如要在没有提示的情况下更改参数，请使用 **noconfirm** 关键字。 **注**　仅支持 802.3x 中定义的流量控制帧。不支持基于优先级的流量控制。
步骤 5	**no shutdown** **示例：** `ciscoasa(config-if)# no shutdown`	启用接口。如要禁用该接口，请输入 **shutdown** 命令。如果输入 **shutdown** 命令，则还可关闭所有子接口。如果关闭系统执行空间中的接口，则该接口在共享它的所有情景中关闭。

后续操作

可选任务：

- 配置冗余接口对。请参阅第 10-9 页的配置冗余接口。
- 配置 VLAN 子接口。请参阅第 10-11 页的配置 VLAN 子接口和 802.1Q 中继。
- 配置巨型帧支持。请参阅第 10-12 页的启用巨型帧支持。

必要任务：

- 完成接口配置。请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。

配置冗余接口

一个逻辑冗余接口包括一对物理接口：主用和备用接口。如果主用接口发生故障，备用接口将激活并开始传输流量。可以配置冗余接口来提高 ASA 的可靠性。此功能独立于设备级故障转移，但您可以在必要时配置冗余接口和故障转移。

本节介绍如何配置冗余接口。

- 第 10-10 页的配置冗余接口
- 第 10-11 页的更改主用接口

配置冗余接口

本节介绍如何创建冗余接口。默认情况下，冗余接口已启用。

准则和限制

- 最多可以配置 8 个冗余接口对。
- 冗余接口延迟值可配置，但在默认情况下，ASA 根据其成员接口的物理类型继承默认延迟值。
- 另请参阅第 10-7 页的冗余接口准则。

先决条件

- 两个成员接口必须为相同的物理类型。例如，两个都必须是千兆以太网接口。
- 不能将已配置了名称的物理接口添加到冗余接口。若要这样做，必须先使用 **no nameif** 命令移除名称。

注意事项　如果使用已在配置中的物理接口，移除该接口的名称将会清除引用该接口的任何配置。

详细步骤

	命令	用途
步骤 1	**interface redundant** *number* **示例：** `ciscoasa(config)# interface redundant 1`	添加逻辑冗余接口，其中 *number* 参数是介于 1 到 8 之间的整数。 **注**　如要配置冗余接口的逻辑参数（例如名称），需要先向该接口至少添加一个成员接口。
步骤 2	**member-interface** *physical_interface* **示例：** `ciscoasa(config-if)# member-interface gigabitethernet 0/0`	将第一个成员接口添加到冗余接口。添加该接口后，将移除其任何配置（例如 IP 地址）。
步骤 3	**member-interface** *physical_interface* **示例：** `ciscoasa(config-if)# member-interface gigabitethernet 0/1`	将第二个成员接口添加到冗余接口。 确保第二个接口的物理类型与第一个接口相同。 如要移除成员接口，请输入 **no member-interface** *physical_interface* 命令。您无法从冗余接口中删除两个成员接口；冗余接口至少需要一个成员接口。

示例

以下示例将创建两个冗余接口：

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

后续操作

可选任务：

- 配置 VLAN 子接口。请参阅第 10-11 页的配置 VLAN 子接口和 802.1Q 中继。
- 配置巨型帧支持。请参阅第 10-12 页的启用巨型帧支持。

必要任务：

- 完成接口配置。请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。

更改主用接口

默认情况下，主用接口 （如果有）是配置中列出的第一个接口。如要查看哪个接口是主用接口，请在 工具中输入以下命令：

```
ciscoasa# show interface redundantnumber detail | grep Member
```

例如：

```
ciscoasa# show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

如要更改主用接口，请输入以下命令：

```
ciscoasa# redundant-interface redundantnumber active-member physical_interface
```

其中，**redundant***number* 参数是冗余接口 ID，例如 **redundant1**。

physical_interface 是想激活的成员接口 ID。

配置 VLAN 子接口和 802.1Q 中继

子接口可将物理或冗余接口划分为用不同 VLAN ID 标记的多个逻辑接口。具有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 可将流量分开保持在特定的物理接口上，您可以增加网络可用的接口数，而无需添加额外的物理接口或 ASA。

准则和限制

- 最大子接口数 - 如要确定您的型号可使用多少个 VLAN 子接口，请参阅第 10-6 页的ASAv 接口的许可要求。
- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常也不想要物理接口传输流量，因为物理接口将传递未标记的数据包。该属性也适用于冗余接口对中的主用物理接口。由于必须启用物理或冗余接口才能使子接口传输流量，因此，请勿并忽略 **nameif** 命令，以确保物理或冗余接口不传输流量。如果要让物理或冗余接口传递未标记数据包，则可照常配置 **nameif** 命令。有关完成接口配置的详细信息，请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。

详细步骤

	命令	用途
步骤 1	**interface** {*physical_interface* | **redundant** *number*}.*subinterface* **示例：** `ciscoasa(config)# interface 千兆以太网 0/1.100`	指定新的子接口。有关物理接口 ID 的说明，请参阅第 10-8 页的启用物理接口并配置以太网参数。 **redundant** *number* 参数是冗余接口 ID，例如 **redundant 1**。 *子接口* ID 是介于 1 和 4294967293 之间的整数。
步骤 2	**vlan** *vlan_id* **示例：** `ciscoasa(config-subif)# vlan 101`	指定子接口的 VLAN。*vlan_id* 是介于 1 和 4094 之间的整数。某些 VLAN ID 可能保留在连接的交换机上，因此，请检查交换机文档了解详细信息。 一个子接口只能分配有一个 VLAN，且不能将同一个 VLAN 分配给多个子接口。无法将 VLAN 分配给物理接口。每个子接口必须有 VLAN ID 才能传输流量。如要更改 VLAN ID，无需移除带有 **no** 选项的旧 VLAN ID；可以输入带有不同 VLAN ID 的 **vlan** 命令，这样 ASA 就会更改旧 ID。

后续操作

可选任务：

- 配置巨型帧支持。请参阅第 10-12 页的启用巨型帧支持。

必要任务：

- 完成接口配置。请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。

启用巨型帧支持

巨型帧是指大于标准最大字节数 （1518 字节）的以太网数据包 （包括第 2 层报头和 FCS），最大可达 9216 字节。可通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配更多内存可能会限制对其他功能的最充分利用，如 ACL。有关详细信息，请参阅第 10-4 页的用最大传输单元、 TCP 最大分段大小控制分片。

先决条件

- 如果更改此设置，需要重新加载 ASA。
- 请务必不需要传输巨型帧的每个接口将 MTU 设为大于 1500 的值；例如，使用 **mtu** 命令将该值设置为 9000。请参阅第 11-7 页的配置 MAC 地址、 MTU 和 TCP MSS。
- 请务必调整 TCP MSS，或禁止将其用于非 VPN 流量 （使用 **sysopt connection tcpmss 0** 命令），或根据第 11-7 页的配置 MAC 地址、 MTU 和 TCP MSS按照 MTU 予将其递增。

详细步骤

命令	用途
jumbo-frame reservation **示例：** `ciscoasa(config)# jumbo-frame reservation`	启用巨型帧支持。如要禁用巨型帧，请使用此命令的 **no** 形式。

示例

以下示例启用巨型帧保留，保存配置并重新加载 ASA：

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted.Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload?[confirm] Y
```

后续操作

完成接口配置。请参阅第 11 章，“路由模式接口”或第 12 章，“透明模式接口”。

监控接口

如要监控接口，请输入以下命令之一：

命令	用途
show interface	显示接口统计信息。
show interface ip brief	显示接口的 IP 地址和状态。

ASAv 接口的配置示例

- 第 10-14 页的物理接口参数示例
- 第 10-14 页的子接口参数示例

物理接口参数示例

以下示例配置物理接口的参数：

```
interface gigabitethernet 0/1
    speed 1000
    duplex full
    no shutdown
```

子接口参数示例

以下示例配置子接口的参数：

```
interface gigabitethernet 0/1.1
    vlan 101
    no shutdown
```

后续操作

按照第 11 章，“路由模式接口”或第 12 章，“透明模式接口”中所述完成接口配置。

ASAv 接口的功能历史记录

表 10-1　接口的功能历史记录

功能名称	平台版本	功能信息
ASAv 支持	9.2(1)	引入了 ASAv。

路由模式接口

本章包含在路由防火墙模式中为所有型号完成接口配置的任务。

- 第 11-1 页的在路由模式中完成接口配置的相关信息
- 第 11-2 页的在路由模式中完成接口配置的许可要求
- 第 11-3 页的准则和限制
- 第 11-4 页的默认设置
- 第 11-5 页的在路由模式中完成接口配置
- 第 11-14 页的关闭和打开接口
- 第 11-14 页的监控接口
- 第 11-15 页的路由模式中接口的功能历史记录

注 对于多情景模式，请在情景执行空间完成本节中的任务。输入 **changeto context** *name* 命令以更改为要配置的情景。

在路由模式中完成接口配置的相关信息

- 第 11-1 页的安全级别
- 第 11-2 页的双堆栈 （IPv4 和 IPv6）

安全级别

每个接口必须有一个安全级别，范围为 0（最低）至 100（最高）。例如，应将最安全的网络（如内部主机网络）指定为级别 100。而连接到互联网的外部网络连接可指定为 0 级。其他网络（如 DMZ）可指定为中间的级别。可将多个接口分配至同一安全级别。有关详细信息，请参阅第 11-12 页的允许同一安全级别通信。

安全级别可控制以下行为：

- 网络访问 - 默认情况下，从安全性较高的接口到安全性较低的接口 （出站）有一个隐式许可。安全性较高接口上的主机可以访问安全性较低接口上的所有主机。可通过将 ACL 应用于接口来限制访问。

  如果为相同安全接口启用通信 （请参阅第 11-12 页的允许同一安全级别通信），则隐式许可就允许这些接口访问安全级别相同或较低的其他接口。

- 检查引擎 - 某些应用检查引擎取决于安全级别。对于相同安全接口，检查引擎适用于任何一个方向的流量。
  - NetBIOS 检查引擎 - 仅适用于出站连接。
  - SQL*Net 检查引擎 - 如果一个主机对之间存在 SQL*Net（以前称为 OraServ）端口的控制连接，则仅允许通过 ASA 进行入站数据连接。
- 过滤 - HTTP(S) 和 FTP 过滤仅适用于出站连接 （从较高级别到较低级别）。

  如果为相同安全接口启用通信，则可以过滤任何一个方向的流量。
- **established** 命令 - 如已建立从安全级别较高主机到安全级别较低主机的连接，则该命令允许连接从安全级别较低主机返回至安全级别较高主机。

  如果为相同安全接口启用通信，则可以为两个方向配置 **established** 命令。

双堆栈 （IPv4 和 IPv6）

思科 ASA 支持在同一接口上配置 IPv6 和 IPv4。您无需输入任何特殊命令来执行此操作；只需按通常的方式输入 IPv4 配置命令和 IPv6 配置命令即可。确保配置一条同时适用于 IPv4 和 IPv6 的默认路由。

在路由模式中完成接口配置的许可要求

型号	许可证要求
ASA 5512-X	VLAN： 基础许可证：50 增强型安全许可证：100 所有类型的接口： 基础许可证：716 增强型安全许可证：916
ASA 5515-X	VLAN： 基础许可证：100 所有类型的接口： 基础许可证：916
ASA 5525-X	VLAN： 基础许可证：200 所有类型的接口： 基础许可证：1316
ASA 5545-X	VLAN： 基础许可证：300 所有类型的接口： 基础许可证：1716

型号	许可证要求
ASA 5555-X	VLAN： 基础许可证：500 所有类型的接口： 基础许可证：2516
ASA 5585-X	VLAN： 基础许可证和增强型安全许可证：1024 SSP-10 和 SSP-20 的接口速度： 基础许可证 - 适用于光纤接口的 1 千兆以太网 10 GE I/O 许可证（增强型安全许可证）- 适用于光纤接口的 10 千兆以太网 （默认情况下，SSP-40 和 SSP-60 支持 10 千兆以太网。） 所有类型的接口： 基础许可证和增强型安全许可证：4612

注　对于根据 VLAN 限制计数的接口，您必须为它分配一个 VLAN。例如：
interface gigabitethernet 0/0.100
vlan 100

所有类型的接口构成最大数量的组合接口；例如，VLAN 接口、物理接口、冗余接口，桥组接口和 EtherChannel 接口。在配置中定义的每个 **interface** 命令均根据此限制进行计数。例如，以下两个接口都计入此限制，即使 GigabitEthernet 0/0 接口定义为 port-channel 1 的一部分：
interface gigabitethernet 0/0
和
interface port-channel 1

型号	许可证要求
ASASM	VLAN： 基础许可证：1000

准则和限制

本节包括此功能的准则和限制。

情景模式准则

- 对于多情景模式中的 ASA 5512-X 和更高版本，请根据第 9 章，“基本接口配置（ASA 5512-X 及更高版本）”在系统执行空间中配置物理接口。然后按照本章内容在情景执行空间中配置逻辑接口参数。对于多情景模式中的 ASASM，请按照第 3 章，“适用于思科 ASA 服务模块的交换机配置”配置交换机端口和交换机上的 VLAN，然后为 ASASM 分配 VLAN。

  ASAv 不支持多情景模式。

- 在多情景模式中，只能配置已根据第 6-14 页的配置多情景分配给系统配置中情景的情景接口。
- 多情景模式中不支持 PPPoE。

防火墙模式准则

支持路由防火墙模式。有关透明模式，请参阅第 12 章，“透明模式接口”。

故障转移准则

请勿采用本章中的操作步骤完成故障转移接口的配置。如要配置故障转移和状态链路，请参阅第 7 章，“通过故障转移实现高可用性”。在多情景模式中，故障转移接口在系统配置中进行配置。

IPv6 准则

支持 IPv6。

适合 ASASM 的 VLAN ID 准则

可向配置中添加任何 VLAN ID，但是，只有通过交换机分配至 ASA 的 VLAN 才能传输流量。如要查看分配至 ASA 的所有 VLAN，请使用 **show vlan** 命令。

如果为尚未通过交换机分配至 ASA 的 VLAN 添加接口，则该接口将处于关闭状态。将 VLAN 分配至 ASA 时，接口将更改为可用状态。如要获得有关接口状态的详细信息，请使用 **show interface** 命令。

默认设置

本节列出了接口的默认设置 （如果没有出厂默认配置）。有关出厂默认配置的信息，请参阅第 2-12 页的出厂默认配置。

默认安全级别

默认安全级别为 0。如将一个接口指定为“内部”，且未明确设置安全级别，则 ASA 将安全级别设置为 100。

注　如果更改接口的安全级别，且不想在使用新安全信息之前等待现有连接超时，则可使用 **clear local-host** 命令清除连接。

ASASM 接口的默认状态

- 在单情景模式或系统执行空间中，VLAN 接口默认启用。
- 在多情景模式中，所有分配的接口均默认启用，无论系统执行空间中接口的状态如何。但是，为使流量通过接口，还必须在系统执行空间中启用接口。如果关闭系统执行空间中的接口，则该接口将在共享它的所有情景中处于关闭状态。

巨型帧支持

默认情况下，ASASM 支持巨型帧。请根据第 11-7 页的配置 MAC 地址、MTU 和 TCP MSS为所需的数据包大小配置 MTU。

在路由模式中完成接口配置

- 第 11-5 页的用于完成接口配置的任务流
- 第 11-5 页的配置常规接口参数
- 第 11-7 页的配置 MAC 地址、 MTU 和 TCP MSS
- 第 11-10 页的配置 IPv6 寻址
- 第 11-12 页的允许同一安全级别通信

用于完成接口配置的任务流

步骤 1　根据型号设置接口：

- ASA 5512-X 和更高版本 - 第 9 章，“基本接口配置 （ASA 5512-X 及更高版本）”
- ASASM-第 3 章，“适用于思科 ASA 服务模块的交换机配置”
- ASAv-第 10 章，“基本接口配置 (ASAv)”

步骤 2　（多情景模式）根据第 6-14 页的配置多情景将接口分配给情景。

步骤 3　（多情景模式）输入 **changeto context** *name* 命令来更改为要配置的情景。配置通用接口参数，包括接口名称、安全级别和 IPv4 地址。请参阅第 11-5 页的配置常规接口参数。

步骤 4　（可选）配置 MAC 地址和 MTU。请参阅第 11-7 页的配置 MAC 地址、 MTU 和 TCP MSS。

步骤 5　（可选）配置 IPv6 寻址。请参阅第 11-10 页的配置 IPv6 寻址。

步骤 6　（可选）通过允许两个接口之间的通信，或通过允许流量进入和退出同一接口，来允许相同安全级别通信。请参阅第 11-12 页的允许同一安全级别通信。

配置常规接口参数

此操作步骤介绍如何设置名称、安全级别、 IPv4 地址和其他选项。

对于 ASA 5512-X 和更高版本及 ASAv，必须为以下接口类型配置接口参数：

- 物理接口
- VLAN 子接口
- 冗余接口
- EtherChannel 接口

对于 ASASM，必须为以下接口类型配置接口参数：

- VLAN 接口

准则和限制

如在使用故障转移，请勿使用此操作步骤命名为故障转移和 Stateful Failover 通信预留的接口。如要配置故障转移和状态链路，请参阅第 7 章，“通过故障转移实现高可用性”。

限制

- 多情景模式中不支持 PPPoE。
- PPPoE 和 DHCP 在 ASASM 上不受支持。

先决条件

- 根据型号设置接口：
  - ASA 5512-X 和更高版本 - 第 9 章，“基本接口配置 （ASA 5512-X 及更高版本）”
  - ASASM-第 3 章，“适用于思科 ASA 服务模块的交换机配置”
  - ASAv-第 10 章，“基本接口配置 (ASAv)”
- 在多情景模式中，只能配置已根据第 6-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。如要从系统切换至情景配置，请在输入 **changeto context** *name* 命令；双击有效设备 IP 地址下的情景名称。

详细步骤

	命令	用途
步骤 1	对于 ASA 5512-X 和更高版本及 ASAv： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[**.***subinterface*] | *mapped_name*} 对于 ASASM： ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **示例：** ciscoasa(config)# interface gigabithethernet 0/0	如果尚未处于接口配置模式，则可进入接口配置模式。 **redundant** *number* 参数是冗余接口 ID，例如 **redundant 1**。 **port-channel** *number* 参数是 EtherChannel 接口 ID，如 **port-channel 1**。 有关物理接口 ID 的说明，请参阅第 9-13 页的启用物理接口并配置以太网参数一节。 向以句点 (.) 分隔的物理或冗余接口 ID 附加 *子接口* ID。 在多情景模式中，如已使用 **allocate-interface** 命令分配一个接口，请输入 *mapped_name* 命令。
步骤 2	**nameif** *name* **示例：** ciscoasa(config-if)# nameif inside	为接口命名。 *name* 是文本字符串，最长 48 个字符且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致提及该名称的所有命令均被删除。
步骤 3	执行以下操作之一：	
	ip address *ip_address* [*mask*] [**standby** *ip_address*] **示例：** ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2	手动设置 IP 地址。 **注**　用于故障转移时，您必须手动设置 IP 地址和备用地址；不支持 DHCP 和 PPPoE。 *ip_address* 和 *mask* 参数设置接口 IP 地址和子网掩码。 **standby** *ip_address* 参数用于故障转移。有关详细信息，请参阅第 7-23 页的配置主用/备用故障转移或第 7-27 页的配置主用/主用故障转移。

	命令	用途
	ip address dhcp [**setroute**] **示例：** ciscoasa(config-if)# ip address dhcp	从 DHCP 服务器获取 IP 地址。 借助于关键字 **setroute**， ASA 可使用 DHCP 服务器提供的默认路由。 重新输入该命令，以重置 DHCP 租约并请求新租约。 如果在输入 **ip address dhcp** 命令之前不使用 **no shutdown** 命令启用接口，则可能不发送某些 DHCP 请求。
	如要从 PPPoE 服务器获取 IP 地址，请参阅 VPN 配置指南。	多情景模式中不支持 PPPoE。
步骤 4	**security-level** *number* **示例：** ciscoasa(config-if)# security-level 50	设置安全级别，其中，*number* 是 0（最低）至 100（最高）之间的整数。请参阅第 11-1 页的安全级别。
步骤 5	（可选） **management-only** **示例：** ciscoasa(config-if)# management-only	将接口设置为仅管理模式，使接口不传输直通流量。 默认情况下，管理接口配置为仅管理。如要禁用此设置，请输入 **no management-only** 命令。 （ASA 5512-X 至 ASA 5555-X）您无法在管理 0/0 接口上禁用 **management-only**。 **management-only** 命令不适用于冗余接口。

示例

以下示例为 VLAN 101 配置参数：

```
ciscoasa(config)# interface vlan 101
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

以下示例在多情景模式中为情景配置进行参数配置。接口 ID 为一个映射名称。

```
ciscoasa/contextA(config)# interface int1
ciscoasa/contextA(config-if)# nameif outside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

后续操作

- （可选）配置 MAC 地址和 MTU。请参阅第 11-7 页的配置 MAC 地址、 MTU 和 TCP MSS。
- （可选）配置 IPv6 寻址。请参阅第 11-10 页的配置 IPv6 寻址。

配置 MAC 地址、 MTU 和 TCP MSS

本节介绍如何为接口配置 MAC 地址及如何设置 MTU 和 TCP MSS。

有关 MAC 地址的信息

默认情况下，物理接口使用烧录 MAC 地址，物理接口的所有子接口均使用相同的烧录 MAC 地址。对于 ASASM，所有 VLAN 使用背板提供的同一个 MAC 地址。

冗余接口使用您添加的第一个物理接口的 MAC 地址。如果在配置中更改成员接口的顺序，则 MAC 地址发生更改，以匹配现第一个列出的接口的 MAC 地址。如果使用此命令将一个 MAC 地址分配给冗余接口，则无论成员接口 MAC 地址如何，均将使用该分配的 MAC 地址。

对于 EtherChannel，属于通道组的所有接口均共享相同 MAC 地址。该功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；他们不知道单个链路。端口通道接口使用编号最小的通道组接口 MAC 地址作为端口通道 MAC 地址。或者，您可以为端口通道接口手动配置 MAC 地址。在多情景模式中，可将唯一 MAC 地址自动分配给各个接口，包括 EtherChannel 端口接口。在组通道接口成员资格发生变化的情况下，我们建议手动或（在多情景模式中）自动配置唯一的 MAC 地址。如果移除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址更改至下一个编号最小的接口，从而导致流量中断。

在多情景模式中，如果在情景之间共享接口，则可将唯一 MAC 地址分配给每个情景的接口。借助于此功能，ASA 可轻松地将数据包分类到适当的情景中。可使用没有唯一 MAC 地址的共享接口，但受到一些限制。有关详细信息，请参阅第 6-2 页的ASA 如何对数据包分类。可手动分配每个 MAC 地址，或者也可为情景中共享接口自动生成 MAC 地址。如要自动生成 MAC 地址，请参阅第 6-22 页的自动为情景接口分配 MAC 地址。如果自动生成 MAC 地址，则可使用此操作步骤覆盖生成的地址。

对于单情景模式，或对于不在多情景模式中共享的接口，您可能要向子接口分配唯一 MAC 地址。例如，您的服务提供商可能根据 MAC 地址执行访问控制。

关于 MTU 和 TCP MSS 的信息

请参阅第 9-6 页的用最大传输单元、 TCP 最大分段大小控制分片。

先决条件

- 根据型号设置接口：
  - ASA 5512-X 和更高版本 - 第 9 章，“基本接口配置 （ASA 5512-X 及更高版本）”
  - ASASM-第 3 章，“适用于思科 ASA 服务模块的交换机配置”
  - ASAv-第 10 章，“基本接口配置 (ASAv)”
- 在多情景模式中，只能配置已根据第 6-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。如要从系统切换至情景配置，请在输入 **changeto context** *name* 命令；双击有效设备 IP 地址下的情景名称。
- 如要将 MTU 增加到 1500 以上，请按照第 9-21 页的启用巨型帧支持启用巨型帧。在 ASASM 上，巨型帧默认受支持；无需启用它们。

详细步骤

	命令	用途
步骤 1	对于 ASA 5512-X 和更高版本及 ASAv： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[**.***subinterface*] | *mapped_name*} 对于 ASASM： ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **示例：** ciscoasa(config)# interface vlan 100	如果尚未处于接口配置模式，则可进入接口配置模式。 **redundant** *number* 参数是冗余接口 ID，例如 **redundant 1**。 **port-channel** *number* 参数是 EtherChannel 接口 ID，如 **port-channel 1**。 有关物理接口 ID 的说明，请参阅第 9-13 页的启用物理接口并配置以太网参数一节。 向以句点 (.) 分隔的物理或冗余接口 ID 附加 *子接口* ID。 在多情景模式中，如已使用 **allocate-interface** 命令分配一个接口，请输入 *mapped_name* 命令。
步骤 2	**mac-address** *mac_address* [**standby** *mac_address*] **示例：** ciscoasa(config-if)# mac-address 000C.F142.4CDE	向该接口分配专用 MAC 地址。*mac_address* 的格式为 H.H.H，其中 H 是 16 位十六进制数字。例如，MAC 地址 00-0C-F1-42-4C-DE 需要输入 000C.F142.4CDE。 如果您还想使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。 如需与故障转移组合使用，请设置**备用** MAC 地址。如果主用设备发生故障转移，且备用设备变为主用设备，则新的主用设备开始使用有效 MAC 地址，以最大限度地减少网络中断，同时，原来的主用设备使用备用地址。
步骤 3	**mtu** *interface_name bytes* **示例：** ciscoasa(config)# mtu inside 9200	将 MTU 设置在 300 至 9198 字节之间 （对于 ASAv，设为 9000）。默认值为 1500 字节。 **注**　为冗余或端口通道接口设置 MTU 时，ASA 将设置应用于所有成员接口。 对于支持巨型帧的型号，如果为任何接口输入的值大于 1500，则需启用巨型帧支持。请参阅第 9-21 页的启用巨型帧支持。
步骤 4	**sysopt connection tcpmss** [**minimum**] *bytes* **示例：** ciscoasa(config)# sysopt connection tcpmss 8500 ciscoasa(config)# sysopt connection tcpmss minimum 1290	将最大 TCP 分段大小设置为介于 48 与任何最大数值之间的字节数。默认值为 1380 字节。可禁用此功能，只需将字节数设置为 **0**。 对于 **minimum** 关键字，请将最大分段大小设置为不小于 48 与 65535 之间的 *字节数*。最小功能默认处于禁用状态 （设置为 0）。

后续操作

（可选）配置 IPv6 寻址。请参阅第 11-10 页的配置 IPv6 寻址。

配置 IPv6 寻址

本节介绍如何配置 IPv6 寻址。

- 第 11-10 页的有关 IPv6 的信息
- 第 11-11 页的配置全局 IPv6 地址
- 第 11-12 页的配置 IPv6 邻居发现

有关 IPv6 的信息

本节包括有关如何配置 IPv6 的信息。

- 第 11-10 页的 IPv6 寻址
- 第 11-10 页的 Modified EUI-64 接口 ID

IPv6 寻址

可为 IPv6 配置两种类型的单播地址：

- 全局 - 全局地址是可在公用网络上使用的公用地址。
- 本地链路 - 本地链路地址是只能在直连网络上使用的专用地址。路由器不使用本地链路地址转发数据包；它们仅用于在特定物理网段上通信。它们可用于执行地址配置或 ND 功能，如地址解析和邻居发现。

至少需要配置本地链路地址，IPv6 才会起作用。如果您配置了全局地址，则接口上会自动配置本地链路地址，因此您无需专门配置本地链路地址。如果不配置全局地址，则需要自动或手动配置本地链路地址。

注　如果只想配置本地链路地址，请参阅命令参考中的 **ipv6 enable**（自动配置）或 **ipv6 address link-local**（手动配置）命令。

Modified EUI-64 接口 ID

RFC 3513：互联网协议第 6 版 (IPv6) 寻址架构要求所有单播 IPv6 地址 （以二进制值 000 开头的地址除外）的接口标识符部分长度为 64 位，结构格式为 Modified EUI-64 格式。ASA 可为连接到本地链路的主机强制执行该要求。

在接口上启用此功能时，该接口接收的 IPv6 数据包源地址将根据源 MAC 地址进行验证，以确保接口标识符使用 Modified EUI-64 格式。如果 IPv6 数据包不将 Modified EUI - 64 格式用于接口标识符，则将丢弃数据包，并生成以下系统日志消息：

```
%ASA-3-325003: EUI-64 source address check failed.
```

只有在创建流量时才能执行地址格式验证。不检查来自现有流量的数据包。此外，只能对本地链路上的主机执行地址验证。从路由器后面的主机接收的数据包将无法通过地址格式验证，且被丢弃，因为它们的源 MAC 地址将为路由器 MAC 地址，而不是主机 MAC 地址。

配置全局 IPv6 地址

如要配置全局 IPv6 地址，请执行以下步骤。

注　配置全局地址将自动配置本地链路地址，因此，无需另行配置它。

限制

ASA 不支持 IPv6 任播地址。

先决条件

- 根据型号设置接口：
  - ASA 5512-X 和更高版本 - 第 9 章，“基本接口配置 （ASA 5512-X 及更高版本）”
  - ASASM-第 3 章，“适用于思科 ASA 服务模块的交换机配置”
  - ASAv-第 10 章，“基本接口配置 (ASAv)”
- 在多情景模式中，只能配置已根据第 6-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。如要从系统切换至情景配置，请在输入 **changeto context** *name* 命令；双击有效设备 IP 地址下的情景名称。

详细步骤

	命令	用途
步骤 1	对于 ASA 5512-X 和更高版本及 ASAv： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[**.***subinterface*] | *mapped_name*} 对于 ASASM： ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **示例：** ciscoasa(config)# interface gigabithethernet 0/0	如果尚未处于接口配置模式，则可进入接口配置模式。 **redundant** *number* 参数是冗余接口 ID，例如 **redundant 1**。 **port-channel** *number* 参数是 EtherChannel 接口 ID，如 **port-channel 1**。 有关物理接口 ID 的说明，请参阅第 9-13 页的启用物理接口并配置以太网参数。 向以句点 (.) 分隔的物理或冗余接口 ID 附加 *子接口* ID。 在多情景模式中，如已使用 **allocate-interface** 命令分配一个接口，请输入 *mapped_name* 命令。
步骤 2	执行以下操作之一：	
	ipv6 address autoconfig **示例：** ciscoasa(config-if)# ipv6 address autoconfig	在接口上启用无状态自动配置。在接口上启用无状态自动配置时，将基于 Router Advertisement 消息中接收到的前缀来配置 IPv6 地址。启用无状态自动配置时，将基于修改的 EUI-64 接口 ID，自动生成接口的本地链路地址。 **注**　尽管 RFC 4862 明确要求配置为无状态自动配置的主机不发送 Router Advertisement 消息，但在此情况下，ASA 实际上会发送 Router Advertisement 消息。如要抑制消息，请查看 **ipv6 nd suppress-ra** 命令。

命令	用途
ipv6 address *ipv6-address/prefix-length* [**standby** *ipv6-address*] **示例：** `ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48`	向接口分配全局地址。分配全局地址时，将自动为接口创建本地链路地址。 **standby** 指定辅助设备使用的接口地址或故障转移对中的故障转移组。
ipv6 address *ipv6-prefix/prefix-length* **eui-64** **示例：** `ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98::/48 eui-64`	通过使用修改的 EUI-64 格式将指定的前缀与接口 MAC 地址生成的接口 ID 组合起来，为接口分配全局地址。分配全局地址时，将自动为接口创建本地链路地址。 您无需指定备用地址；接口 ID 将自动生成。
步骤 3　（可选） **ipv6 enforce-eui64** *if_name* **示例：** `ciscoasa(config)# ipv6 enforce-eui64 inside`	在本地链路上的 IPv6 地址中，强制使用 Modified EUI-64 格式的接口标识符。 *if_name* 参数是接口名称，由 **nameif** 命令指定，在该名称上可启用地址格式强制执行。 有关详细信息，请参阅第 11-10 页的 Modified EUI-64 接口 ID。

配置 IPv6 邻居发现

如要配置 IPv6 邻居发现，请参阅第 25 章，“IPv6 邻居发现”。

允许同一安全级别通信

默认情况下，同一个安全级别的接口不能相互通信，而且数据包无法进入和退出同一接口。本节介绍当接口为同一安全级别时如何启用接口间通信。

有关接口间通信的信息

允许同一安全级别的接口之间相互通信具有以下优势：

- 您可以配置超过 101 个通信接口。

  如果您为每个接口使用不同级别，而且不将任何接口分配到同一安全等级，则可以每个级别（0 到 100）仅配置一个接口。
- 您希望流量能够在同一安全级别的各接口之间自由流动而无需 ACL。

如果启用同一安全级别接口通信，则仍可照常配置不同安全级别的接口。

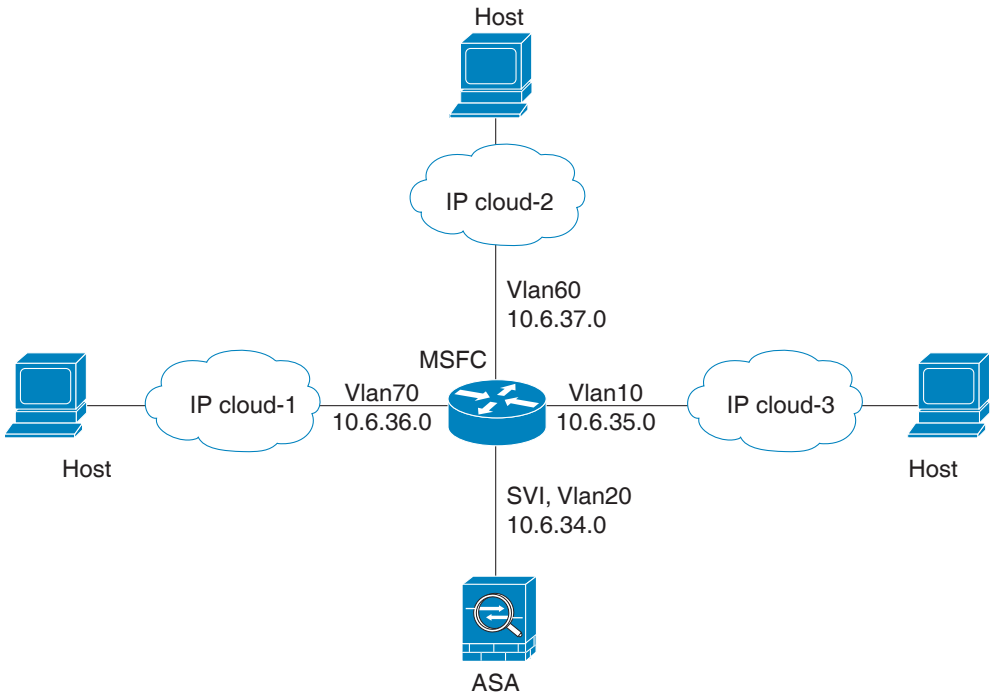
有关接口内通信的信息

接口内通信可能对从某一接口进入、却从同一接口流出的 VPN 流量有用。这种情况下， VPN 流量可能未加密，也可能被重新加密以用于另一个 VPN 连接。例如，如果有星型 VPN 网络，其中 ASA 为中心节点，远程 VPN 网络为分支节点，为使一个分支节点能与另一个分支节点进行通信，流量必须先进入 ASA，然后流出，再进入另一个分支节点。

注　此功能允许的所有流量仍将受到防火墙规则的制约。请勿创建可能导致回传流量不流经 ASA 的非对称路由情景。

对于 ASASM，在启动此功能之前，您首先必须正确配置 MSFC，以便将数据包发送到 ASA 的 MAC 地址，而不是直接通过交换机发送到目标主机。图 11-1 显示了同一接口上的主机需要通信的网络。

图 11-1　同一接口上的主机之间的通信



以下示例配置显示了思科 IOS **route-map** 命令，该命令用于在如图 11-1 中所示的网络中启用策略路由：

```
route-map intra-inter3 permit 0
    match ip address 103
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter2 permit 20
    match ip address 102
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter1 permit 10
    match ip address 101
    set interface Vlan20
    set ip next-hop 10.6.34.7
```

详细步骤

命令	用途
same-security-traffic permit inter-interface	启用同一安全级别的接口，使接口间可以互相通信。
same-security-traffic permit intra-interface	启用连接到同一接口的主机之间的通信。

关闭和打开接口

本节介绍如何关闭和打开接口。

默认情况下，所有接口均已启用。在多情景模式中，如果禁用或重新启用情景内的接口，则只有该情景接口受到影响。但是，如果禁用或重新启用系统执行空间中的接口，则将影响所有情景中的该接口。

详细步骤

	命令	用途
步骤 1	ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **示例：** ciscoasa(config)# interface vlan 100	如果尚未处于接口配置模式，则可进入接口配置模式。 在多情景模式中，如已使用 **allocate-interface** 命令分配一个接口，请输入 *mapped_name* 命令。
步骤 2	**shutdown** **示例：** ciscoasa(config-if)# shutdown	禁用接口。
步骤 3	**no shutdown** **示例：** ciscoasa(config-if)# no shutdown	重新启用接口。

监控接口

如要监控接口，请输入以下命令之一：

命令	用途
show interface	显示接口统计信息。
show interface ip brief	显示接口的 IP 地址和状态。

路由模式中接口的功能历史记录

表 11-1 列出了此功能的版本历史记录。

表 11-1　　接口的功能历史记录

功能名称	版本	功能信息
增加的 VLAN 数量	7.0(5)	增加了以下限制： • ASA5510 基础许可证的 VLAN 数从 0 增加到 10。 • ASA5510 增强型安全许可证的 VLAN 数从 10 增加到 25。 • ASA5520 的 VLAN 数从 25 增加到 100。 • ASA5540 的 VLAN 数从 100 增加到 200。
增加的 VLAN 数量	7.2(2)	ASA 5505 上增强型安全许可证 VLAN 的最大数量从 5（3 个全功能；1 个故障转移；一个限定于备用接口）增加至 20 个全功能接口。此外，中继端口数量从 1 增加到 8。现在已有 20 个全功能接口，无需使用备用接口命令削弱备用 ISP 接口的功能；可使用全功能接口替代它。备用接口命令对于 Easy VPN 配置仍非常有用。 以下型号的 VLAN 数量限制也有增加：ASA 5510（对于基础许可证，从 10 增加到 50，对于增强型安全许可证，从 25 增加到 100）、ASA 5520（从 100 增加到 150）和 ASA 5550（从 200 增加到 250）。
对于 ASA 5510 增强型安全许可证的千兆以太网支持	7.2(3)	ASA 5510 目前通过增强型安全许可证支持端口 0 和 1 的 GE（千兆以太网）。如果从基础许可证升级至增强型安全许可证，则外部 Ethernet 0/0 和 Ethernet0/1 端口的容量将从原始的 FE（快速以太网）(100 Mbps) 增加到 GE (1000 Mbps)。接口名称仍保持为 Ethernet 0/0 和 Ethernet0/1。使用 **speed** 命令更改接口上的速度，使用 **show interface** 命令查看当前为每个接口配置的速度。
对 ASA 5505 的本地 VLAN 支持	7.2(4)/8.0(4)	现在可将本地 VLAN 纳入 ASA 5505 中继端口。 我们引入了以下命令：**switchport trunk native vlan**。
对 ASA 5580 的巨型数据包支持	8.1(1)	思科 ASA 5580 支持巨型帧。巨型帧是一个以太网数据包，其大小大于标准的最大值 1518 字节 （包括第 2 层报头和 FCS），最大可达 9216 字节。可通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配更多内存可能会限制对其他功能的最充分利用，如 ACL。 我们引入了以下命令：**jumbo-frame reservation**。
为 ASA 5580 增加的 VLAN 数	8.1(2)	ASA 5580 支持的 VLAN 数量从 100 增加到 250。

表 11-1　　接口的功能历史记录（续）

功能名称	版本	功能信息
对透明模式的 IPv6 支持	8.2(1)	已为透明防火墙模式引入 IPv6 支持。
对 ASA 5580 10 千兆以太网接口上流量控制的暂停帧支持	8.2(2)	现可为流量控制启用暂停 (XOFF) 帧。 我们引入了以下命令：**flowcontrol**。

透明模式接口

本章包含的任务是在透明防火墙模式中为所有型号完成接口配置。

- 第 12-1 页的有关透明模式接口的信息
- 第 12-2 页的透明模式接口的许可要求
- 第 12-4 页的透明模式接口的准则和限制
- 第 12-5 页的透明模式接口的默认设置
- 第 12-5 页的在透明模式中完成接口配置
- 第 12-14 页的关闭和打开接口
- 第 12-15 页的监控接口
- 第 12-15 页的透明模式接口的配置示例
- 第 12-16 页的透明模式接口的功能历史

注 对于多情景模式，请在情景执行空间完成本节中的任务。输入 **changeto context** *name* 命令以更改为要配置的情景。

有关透明模式接口的信息

- 第 12-1 页的透明模式的网桥组
- 第 12-2 页的安全级别

透明模式的网桥组

如果不想产生安全情景开销，或者要最大限度地使用安全情景，请将接口一起组合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组的流量互为隔离；流量不会路由至 Cisco ASA 内的其他网桥组，而且，流量必须先退出 ASA，然后才能由外部路由器路由回 ASA 中的另一个网桥组。虽然每个网桥组的桥接功能互为独立，但许多其他功能可以供所有网桥组共享。例如，所有网桥组共享系统日志服务器或 AAA 服务器配置。如需完全分隔安全策略，请将安全情景与每个情景中的一个网桥组配合使用。每个情景或单个模式中至少需要一个网桥组。

每个网桥组均需要一个管理 IP 地址。有关另一种管理方法，请参阅第 9-2 页的管理接口。

注　ASA 不支持辅助网络上的流量；仅支持与管理 IP 地址相同的网络上的流量。

安全级别

每个接口必须有一个安全级别，范围为 0（最低）至 100（最高）。例如，应将最安全的网络（如内部主机网络）指定为级别 100。而连接到互联网的外部网络连接可指定为 0 级。其他网络（如 DMZ）可指定为中间的级别。可将多个接口分配至同一安全级别。有关详细信息，请参阅第 12-14 页的允许同一安全级别通信。

安全级别可控制以下行为：

- 网络访问 - 默认情况下，从安全性较高的接口到安全性较低的接口 （出站）有一个隐式许可。安全性较高接口上的主机可以访问安全性较低接口上的所有主机。可通过将 ACL 应用于接口来限制访问。

  如果为相同安全接口启用通信 （请参阅第 12-14 页的允许同一安全级别通信），则隐式许可就允许这些接口访问安全级别相同或较低的其他接口。

- 检查引擎 - 某些应用检查引擎取决于安全级别。对于相同安全接口，检查引擎适用于任何一个方向的流量。
  - NetBIOS 检查引擎 - 仅适用于出站连接。
  - SQL*Net 检查引擎 - 如果一个主机对之间存在 SQL*Net（以前称为 OraServ）端口的控制连接，则仅允许通过 ASA 进行入站数据连接。
- 过滤 - HTTP(S) 和 FTP 过滤仅适用于出站连接 （从较高级别到较低级别）。

  如果为相同安全接口启用通信，则可以过滤任何一个方向的流量。
- **established** 命令 - 如已建立从安全级别较高主机到安全级别较低主机的连接，则该命令允许连接从安全级别较低主机返回至安全级别较高主机。

  如果为相同安全接口启用通信，则可以为两个方向配置 **established** 命令。

透明模式接口的许可要求

型号	许可证要求
ASA 5512-X	VLAN： 基础许可证：50 增强型安全许可证：100 所有类型的接口： 基础许可证：716 增强型安全许可证：916
ASA 5515-X	VLAN： 基础许可证：100 所有类型的接口： 基础许可证：916

型号	许可证要求
ASA 5525-X	VLAN： 基础许可证：200 所有类型的接口： 基础许可证：1316
ASA 5545-X	VLAN： 基础许可证：300 所有类型的接口： 基础许可证：1716
ASA 5555-X	VLAN： 基础许可证：500 所有类型的接口： 基础许可证：2516
ASA 5585-X	VLAN： 基础许可证和增强型安全许可证：1024 SSP-10 和 SSP-20 的接口速度： 基础许可证 - 适用于光纤接口的 1 千兆以太网 10 GE I/O 许可证（增强型安全许可证）- 适用于光纤接口的 10 千兆以太网 （默认情况下，SSP-40 和 SSP-60 支持 10 千兆以太网。） 所有类型的接口： 基础许可证和增强型安全许可证：4612

注　对于根据 VLAN 限制计数的接口，您必须为它分配一个 VLAN。例如：

```
interface gigabitethernet 0/0.100
  vlan 100
```

所有类型的接口构成最大数量的组合接口；例如，VLAN 接口、物理接口、冗余接口，桥组接口和 EtherChannel 接口。在配置中定义的每个 **interface** 命令均根据此限制进行计数。例如，以下两个接口都计入此限制，即使 GigabitEthernet 0/0 接口定义为 port-channel 1 的一部分：

interface gigabitethernet 0/0

和

interface port-channel 1

型号	许可证要求
ASASM	VLAN： 基础许可证：1000

透明模式接口的准则和限制

本节包括此功能的准则和限制。

情景模式准则

- 对于多情景模式中的 ASA 5512-X 和更高版本，请根据第 9 章，“基本接口配置 （ASA 5512-X 及更高版本）”在系统执行空间中配置物理接口。然后按照本章内容在情景执行空间中配置逻辑接口参数。对于多情景模式中的 ASASM，请按照第 3 章，“适用于思科 ASA 服务模块的交换机配置”配置交换机端口和交换机上的 VLAN，然后为 ASASM 分配 VLAN。

  ASAv 不支持多情景模式。

- 您只能配置已使用 **allocate-interface** 命令分配给系统配置中情景的情景接口。

防火墙模式准则

- 可以在单情景模式或多情景模式的每个情景中配置多达 250 个网桥组。请注意，必须使用至少 1 个网桥组；数据接口必须属于网桥组。
- 每个网桥组最多可包括 4 个接口。
- 对于 IPv4，每个网桥组都需要一个管理 IP 地址以用于两个管理流量并供流量通过 ASA。

  与路由模式 （每个接口需要一个 IP 地址）不同，透明防火墙向整个网桥组分配一个 IP 地址。 ASA 使用此 IP 地址作为源自 ASA 的数据包 （如系统消息或 AAA 通信）的源地址。除网桥组管理地址外，还可以选择性地为某些型号配置管理接口；有关详细信息，请参阅第 9-2 页的管理接口。

  管理 IP 地址必须与所连接的网络位于相同的子网上。您不能将该子网设置为主机子网 (255.255.255.255)。 ASA 不支持辅助网络上的流量；仅支持与管理 IP 地址相同的网络上的流量。有关管理 IP 子网的详细信息，请参阅第 12-6 页的配置网桥组。

- 对于 IPv6，至少需要为直通流量的每个接口配置本地链路地址。为了实现完整功能，包括管理 ASA 的能力，需要为每个网桥组配置全局 IPv6 地址。
- 对于多情景模式，每个情景必须使用不同的接口；不能在情景之间共享接口。
- 对于多情景模式，每个情景通常使用不同的子网。可以使用重叠子网，但是网络拓扑需要路由器和 NAT 配置，以便从路由角度使用重叠子网。

故障转移准则

请勿采用本章中的操作步骤完成故障转移接口的配置。如要配置故障转移和状态链路，请参阅第 7 章，“通过故障转移实现高可用性”。在多情景模式中，故障转移接口在系统配置中进行配置。

IPv6 准则

透明模式中不支持 IPv6 任播地址。

适合 ASASM 的 VLAN ID 准则

可向配置中添加任何 VLAN ID，但是，只有通过交换机分配至 ASA 的 VLAN 才能传输流量。如要查看分配至 ASA 的所有 VLAN，请使用 **show vlan** 命令。

如果为尚未通过交换机分配至 ASA 的 VLAN 添加接口，则该接口将处于关闭状态。将 VLAN 分配至 ASA 时，接口将更改为可用状态。如要获得有关接口状态的详细信息，请使用 **show interface** 命令。

透明模式接口的默认设置

本节列出了接口的默认设置 （如果没有出厂默认配置）。有关出厂默认配置的信息，请参阅第 2-12 页的出厂默认配置。

默认安全级别

默认安全级别为 0。如将一个接口指定为“内部”，且未明确设置安全级别，则 ASA 将安全级别设置为 100。

注　如果更改接口的安全级别，且不想在使用新安全信息之前等待现有连接超时，则可使用 **clear local-host** 命令清除连接。

ASASM 接口的默认状态

- 在单情景模式或系统执行空间中，VLAN 接口默认启用。
- 在多情景模式中，所有分配的接口均默认启用，无论系统执行空间中接口的状态如何。但是，为使流量通过接口，还必须在系统执行空间中启用接口。如果关闭系统执行空间中的接口，则该接口将在共享它的所有情景中处于关闭状态。

巨型帧支持

默认情况下，ASASM 支持巨型帧。请根据第 12-10 页的配置 MAC 地址、MTU 和 TCP MSS为所需的数据包大小配置 MTU。

在透明模式中完成接口配置

- 第 12-5 页的用于完成接口配置的任务流
- 第 12-6 页的配置网桥组
- 第 12-7 页的配置常规接口参数
- 第 12-8 页的配置管理接口 （ASA 5512-X 和更高版本及 ASAv）
- 第 12-10 页的配置 MAC 地址、 MTU 和 TCP MSS
- 第 12-12 页的配置 IPv6 寻址
- 第 12-14 页的允许同一安全级别通信

用于完成接口配置的任务流

步骤 1　根据型号设置接口：

- ASA 5512-X 和更高版本 - 第 9 章，“基本接口配置 （ASA 5512-X 及更高版本）”
- ASASM-第 3 章，“适用于思科 ASA 服务模块的交换机配置”
- ASAv-第 10 章，“基本接口配置 (ASAv)”

步骤 2　（多情景模式）根据第 6-14 页的配置多情景将接口分配给情景。

步骤 3　（多情景模式）输入 **changeto context** ***name*** 命令以更改为要配置的情景。

步骤 4　配置一个或多个网桥组，包括 IPv4 地址。请参阅第 12-6 页的配置网桥组。

步骤 5　配置常规接口参数，包括其所属的网桥组、接口名称和安全级别。请参阅第 12-7 页的配置常规接口参数。

步骤 6　（可选）配置管理接口。请参阅第 12-8 页的配置管理接口 （ASA 5512-X 和更高版本及 ASAv）。

步骤 7　（可选）配置 MAC 地址和 MTU。请参阅第 12-10 页的配置 MAC 地址、 MTU 和 TCP MSS。

步骤 8　（可选）配置 IPv6 寻址。请参阅第 12-12 页的配置 IPv6 寻址。

步骤 9　（可选）通过允许两个接口之间的通信，或通过允许流量进入和退出同一接口，来允许相同安全级别通信。请参阅第 12-14 页的允许同一安全级别通信。

配置网桥组

每个网桥组均需要一个管理 IP 地址。 ASA 使用此 IP 地址作为源自网桥组的数据包的源地址。管理 IP 地址必须与所连接的网络位于相同的子网上。对于 IPv4 流量，传递任何流量均需要管理 IP 地址。对于 IPv6 流量，至少必须配置本地链路地址以传递流量，但要实现完整功能 （包括远程管理和其他管理操作），建议采用全局管理地址。

准则和限制

可以在单情景模式或多情景模式的每个情景中配置多达 250 个网桥组。请注意，必须使用至少 1 个网桥组；数据接口必须属于网桥组。

注　对于单独的管理接口 （对于受支持的型号），一个无法配置的网桥组 (ID 301) 将自动添加至您的配置。此网桥组未纳入网桥组限制中。

详细步骤

	命令	用途
步骤 1	**interface bvi** *bridge_group_number* **示例：** `ciscoasa(config)# interface bvi 1`	创建网桥组，其中 *bridge_group_number* 是介于 1 与 250 之间的整数。
步骤 2	**ip address** *ip_address* [*mask*] [**standby** *ip_address*] **示例：** `ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2`	指定网桥组的管理 IP 地址。 请勿将主机地址 （/32 或 255.255.255.255）分配给网桥组。此外，请勿使用主机地址不足 3 个的其他子网 （每个分别用于上游路由器、下游路由器和透明防火墙），如 /30 子网 (255.255.255.252)。 ASA 向子网中的第一个和最后一个地址或从其丢弃所有 ARP 数据包。因此，如果使用 /30 子网，且将已预留的地址从该子网分配给上游路由器，则 ASA 丢弃从下游路由器到上游路由器的 ARP 请求。 ASA 不支持辅助网络上的流量；仅支持与管理 IP 地址相同的网络上的流量。 **standby** 关键字和地址用于故障转移。

示例

以下示例设置网桥组 1 的管理地址和备用地址：

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

后续操作

配置常规接口参数。请参阅第 12-7 页的配置常规接口参数。

配置常规接口参数

本操作步骤介绍如何为每个透明接口设置名称、安全级别和网桥组。

如要配置单独的管理界面，请参阅第 12-8 页的配置管理接口 （ASA 5512-X 和更高版本及 ASAv）。

对于 ASA 5512-X 和更高版本及 ASAv，必须为以下接口类型配置接口参数：

- 物理接口
- VLAN 子接口
- 冗余接口
- EtherChannel 接口

对于 ASASM，必须为以下接口类型配置接口参数：

- VLAN 接口

准则和限制

- 可为每个网桥组配置多达四个接口。
- 有关安全级别的信息，请参阅第 12-2 页的安全级别。
- 如在使用故障转移，请勿使用此操作步骤命名为故障转移和 Stateful Failover 通信预留的接口。如要配置故障转移和状态链路，请参阅第 7 章，“通过故障转移实现高可用性”。

先决条件

- 根据型号设置接口：
  - ASA 5512-X 和更高版本 - 第 9 章，“基本接口配置 （ASA 5512-X 及更高版本）”
  - ASASM-第 3 章，“适用于思科 ASA 服务模块的交换机配置”
  - ASAv-第 10 章，“基本接口配置 (ASAv)”
- 在多情景模式中，只能配置已根据第 6-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。如要从系统切换至情景配置，请在输入 **changeto context** *name* 命令；双击有效设备 IP 地址下的情景名称。

详细步骤

	命令	用途
步骤 1	对于 ASA 5512-X 和更高版本及 ASAv： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[**.***subinterface*] | *mapped_name*} **示例：** `ciscoasa(config)# interface gigabitethernet 0/0`	如果尚未处于接口配置模式，则可进入接口配置模式。 **redundant** *number* 参数是冗余接口 ID，例如 **redundant 1**。 **port-channel** *number* 参数是 EtherChannel 接口 ID，如 **port-channel 1**。 有关物理接口 ID 的说明，请参阅第 9-13 页的启用物理接口并配置以太网参数一节。请勿对管理接口执行此操作步骤；如要配置管理接口，请参阅第 12-8 页的配置管理接口 （ASA 5512-X 和更高版本及 ASAv）。 向以句点 (.) 分隔的物理或冗余接口 ID 附加 *子接口* ID。 在多情景模式中，如已使用 **allocate-interface** 命令分配一个接口，请输入 *mapped_name* 命令。
步骤 2	**bridge-group** *number* **示例：** `ciscoasa(config-if)# bridge-group 1`	将该接口分配给网桥组，其中，*number* 是介于 1 与 100 之间的整数。最多可将四个接口分配到网桥组。不能将同一个接口分配到多个网桥组。
步骤 3	**nameif** *name* **示例：** `ciscoasa(config-if)# nameif inside`	为接口命名。 *name* 是文本字符串，最长 48 个字符且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致提及该名称的所有命令均被删除。
步骤 4	**security-level** *number* **示例：** `ciscoasa(config-if)# security-level 50`	设置安全级别，其中，*number* 是 0（最低）至 100（最高）之间的整数。

后续操作

- （可选）配置管理接口。请参阅第 12-8 页的配置管理接口 （ASA 5512-X 和更高版本及 ASAv）。
- （可选）配置 MAC 地址和 MTU。请参阅第 12-10 页的配置 MAC 地址、 MTU 和 TCP MSS。
- （可选）配置 IPv6 寻址。请参阅第 12-12 页的配置 IPv6 寻址。

配置管理接口 （ASA 5512-X 和更高版本及 ASAv）

可在单情景模式或每个情景中配置一个与网桥组接口分离的管理接口。有关详细信息，请参阅第 9-2 页的管理接口。

限制

- 请参阅第 9-2 页的管理接口。
- 请勿将此接口分配给网桥组；不可配置的网桥组 (ID 101) 将自动添加到您的配置中。此网桥组未纳入网桥组限制中。
- 如果您的型号不包括管理接口，则必须从数据接口管理透明防火墙；请跳过此操作步骤。（例如，在 ASASM 上。）

- 在多情景模式中，无法在情景之间共享任何接口，包括管理接口。如要为每个情景提供管理，可创建管理接口的子接口，然后向每个情景分配管理子接口。请注意，从 ASA 5512-X 到 ASA 5555-X 都不允许管理接口上有子接口，因此，对于每个情景管理，必须连接到数据接口。

先决条件

- 完成第 9 章，“基本接口配置 （ASA 5512-X 及更高版本）”中的操作步骤
- 在多情景模式中，只能配置已根据第 6-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。如要从系统切换至情景配置，请在输入 **changeto context** *name* 命令；双击有效设备 IP 地址下的情景名称。

详细步骤

	命令	用途
步骤 1	**interface** {{**port-channel** *number* | **management** *slot/port*}[**.***subinterface*] | *mapped_name*} **示例：** `ciscoasa(config)# interface management 0/0.1`	如果尚未处于接口配置模式，则可进入管理接口的接口配置模式。 **port-channel** *number* 参数是 EtherChannel 接口 ID，如 **port-channel 1**。 EtherChannel 接口只能拥有管理成员接口。 冗余接口不支持作为成员的管理*插槽/端口*接口。也不能将组成非管理接口的冗余接口设置为管理专属接口。 在多情景模式中，如已使用 **allocate-interface** 命令分配一个接口，请输入 *mapped_name* 命令。
步骤 2	**nameif** *name* **示例：** `ciscoasa(config-if)# nameif management`	为接口命名。 *name* 是文本字符串，最长 48 个字符且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致提及该名称的所有命令均被删除。
步骤 3	执行以下操作之一：	
	ip address *ip_address* [*mask*] [**standby** *ip_address*] **示例：** `ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2`	手动设置 IP 地址。 **注**　如需与故障转移组合使用，则必须手动设置 IP 地址和备用地址；DHCP 不受支持。 *ip_address* 和 *mask* 参数设置接口 IP 地址和子网掩码。 **standby** *ip_address* 参数用于故障转移。有关详细信息，请参阅第 7-23 页的配置主用/备用故障转移或第 7-27 页的配置主用/主用故障转移。
	ip address dhcp [**setroute**] **示例：** `ciscoasa(config-if)# ip address dhcp`	从 DHCP 服务器获取 IP 地址。 借助于关键字 **setroute**，ASA 可使用 DHCP 服务器提供的默认路由。 重新输入该命令，以重置 DHCP 租约并请求新租约。 如果在输入 **ip address dhcp** 命令之前不使用 **no shutdown** 命令启用接口，则可能不发送某些 DHCP 请求。
步骤 4	**security-level** *number* **示例：** `ciscoasa(config-if)# security-level 50`	设置安全级别，其中，*number* 是 0（最低）至 100（最高）之间的整数。

后续操作

- （可选）配置 MAC 地址和 MTU。请参阅第 12-10 页的配置 MAC 地址、 MTU 和 TCP MSS。
- （可选）配置 IPv6 寻址。请参阅第 12-12 页的配置 IPv6 寻址。

配置 MAC 地址、 MTU 和 TCP MSS

本节介绍如何为接口配置 MAC 地址及如何设置 MTU 和 TCP MSS。

有关 MAC 地址的信息

默认情况下，物理接口使用烧录 MAC 地址，物理接口的所有子接口均使用相同的烧录 MAC 地址。

对于 ASASM，所有 VLAN 使用背板提供的同一个 MAC 地址。

冗余接口使用您添加的第一个物理接口的 MAC 地址。如果在配置中更改成员接口的顺序，则 MAC 地址发生更改，以匹配现第一个列出的接口的 MAC 地址。如果使用此命令将一个 MAC 地址分配给冗余接口，则无论成员接口 MAC 地址如何，均将使用该分配的 MAC 地址。

对于 EtherChannel，属于通道组的所有接口均共享相同 MAC 地址。该功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；他们不知道单个链路。端口通道接口使用编号最小的通道组接口 MAC 地址作为端口通道 MAC 地址。或者，您可以为端口通道接口手动配置 MAC 地址。在多情景模式中，可将唯一 MAC 地址自动分配给各个接口，包括 EtherChannel 端口接口。在组通道接口成员资格发生变化的情况下，我们建议手动或（在多情景模式中）自动配置唯一的 MAC 地址。如果移除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址更改至下一个编号最小的接口，从而导致流量中断。

在多情景模式中，如果在情景之间共享接口，则可将唯一 MAC 地址分配给每个情景的接口。借助于此功能，ASA 可轻松地将数据包分类到适当的情景中。可使用没有唯一 MAC 地址的共享接口，但受到一些限制。有关详细信息，请参阅第 6-2 页的 ASA 如何对数据包分类。可手动分配每个 MAC 地址，或者也可为情景中共享接口自动生成 MAC 地址。如要自动生成 MAC 地址，请参阅第 6-22 页的自动为情景接口分配 MAC 地址。如果自动生成 MAC 地址，则可使用此操作步骤覆盖生成的地址。

对于单情景模式，或对于不在多情景模式中共享的接口，您可能要向子接口分配唯一 MAC 地址。例如，您的服务提供商可能根据 MAC 地址执行访问控制。

关于 MTU 和 TCP MSS 的信息

请参阅第 9-6 页的用最大传输单元、 TCP 最大分段大小控制分片。

先决条件

- 根据型号设置接口：
  - ASA 5512-X 和更高版本 - 第 9 章，“基本接口配置（ASA 5512-X 及更高版本）”
  - ASASM-第 3 章，“适用于思科 ASA 服务模块的交换机配置”
  - ASAv-第 10 章，“基本接口配置 (ASAv)”
- 在多情景模式中，只能配置已根据第 6-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。如要从系统切换至情景配置，请在输入 **changeto context** *name* 命令；双击有效设备 IP 地址下的情景名称。
- 如要将 MTU 增加到 1500 以上，请根据第 9-21 页的启用巨型帧支持在受支持的型号上启用巨型帧。在 ASASM 上，巨型帧默认受支持；无需启用它们。

详细步骤

	命令	用途
步骤 1	对于 ASA 5512-X 和更高版本及 ASAv： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[.*subinterface*] | *mapped_name*} 对于 ASASM： ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **示例：** ciscoasa(config)# interface vlan 100	如果尚未处于接口配置模式，则可进入接口配置模式。 **redundant** *number* 参数是冗余接口 ID，例如 **redundant 1**。 **port-channel** *number* 参数是 EtherChannel 接口 ID，如 **port-channel 1**。 有关物理接口 ID 的说明，请参阅第 9-13 页的启用物理接口并配置以太网参数一节。 向以句点 (.) 分隔的物理或冗余接口 ID 附加*子接口* ID。 在多情景模式中，如已使用 **allocate-interface** 命令分配一个接口，请输入 *mapped_name* 命令。
步骤 2	**mac-address** *mac_address* [**standby** *mac_address*] **示例：** ciscoasa(config-if)# mac-address 000C.F142.4CDE	向该接口分配专用 MAC 地址。*mac_address* 的格式为 H.H.H，其中 H 是 16 位十六进制数字。例如，MAC 地址 00-0C-F1-42-4C-DE 需要输入 000C.F142.4CDE。 如果您还想使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。 如需与故障转移组合使用，请设置**备用** MAC 地址。如果主用设备发生故障转移，且备用设备变为主用设备，则新的主用设备开始使用有效 MAC 地址，以最大限度地减少网络中断，同时，原来的主用设备使用备用地址。
步骤 3	**mtu** *interface_name bytes* **示例：** ciscoasa(config)# mtu inside 9200	将 MTU 设置在 300 至 9198 字节之间 （对于 ASAv，设为 9000）。默认值为 1500 字节。 **注**　为冗余或端口通道接口设置 MTU 时，ASA 将设置应用于所有成员接口。 对于支持巨型帧的型号，如果为任何接口输入的值大于 1500，则需启用巨型帧支持。请参阅第 9-21 页的启用巨型帧支持。
步骤 4	**sysopt connection tcpmss** [**minimum**] *bytes* **示例：** ciscoasa(config)# sysopt connection tcpmss 8500 ciscoasa(config)# sysopt connection tcpmss minimum 1290	将最大 TCP 分段大小设置为介于 48 与任何最大数值之间的字节数。默认值为 1380 字节。可禁用此功能，只需将字节数设置为 **0**。 对于 **minimum** 关键字，请将最大分段大小设置为不小于 48 与 65535 之间的*字节数*。最小功能默认处于禁用状态 （设置为 0）。

后续操作

（可选）配置 IPv6 寻址。请参阅第 12-12 页的配置 IPv6 寻址。

配置 IPv6 寻址

本节介绍如何配置 IPv6 寻址。

- 第 12-12 页的有关 IPv6 的信息
- 第 12-13 页的配置全局 IPv6 地址
- 第 12-14 页的配置 IPv6 邻居发现

有关 IPv6 的信息

本节包括有关如何配置 IPv6 的信息。

- 第 12-12 页的 IPv6 寻址
- 第 12-12 页的 Modified EUI-64 接口 ID
- 第 12-13 页的不受支持的命令

IPv6 寻址

可为 IPv6 配置两种类型的单播地址：

- 全局 - 全局地址是可在公用网络上使用的公用地址。需要为每个网桥组配置该地址，而不是每个接口。还可为管理接口配置全局 IPv6 地址。
- 本地链路 - 本地链路地址是只能在直连网络上使用的专用地址。路由器不使用本地链路地址转发数据包；它们仅用于在特定物理网段上通信。它们可用于执行地址配置或 ND 功能，如地址解析和邻居发现。由于本地链路地址仅在网段上可用，且与接口 MAC 地址绑定，因此，需要为每个接口配置本地链路地址。

至少需要配置本地链路地址，IPv6 才会起作用。如果配置全局地址，则会在每个接口上自动配置本地链路地址，因此，无需再特别配置本地链路地址。如果不配置全局地址，则需要自动或手动配置本地链路地址。

注　如果只想配置本地链路地址，请参阅命令参考中的 **ipv6 enable**（自动配置）或 **ipv6 address link-local**（手动配置）命令。

Modified EUI-64 接口 ID

RFC 3513：互联网协议第 6 版 (IPv6) 寻址架构要求所有单播 IPv6 地址 （以二进制值 000 开头的地址除外）的接口标识符部分长度为 64 位，结构格式为 Modified EUI-64 格式。ASA 可为连接到本地链路的主机强制执行该要求。

在接口上启用此功能时，该接口接收的 IPv6 数据包源地址将根据源 MAC 地址进行验证，以确保接口标识符使用 Modified EUI-64 格式。如果 IPv6 数据包不将 Modified EUI - 64 格式用于接口标识符，则将丢弃数据包，并生成以下系统日志消息：

```
%ASA-3-325003: EUI-64 source address check failed.
```

只有在创建流量时才能执行地址格式验证。不检查来自现有流量的数据包。此外，只能对本地链路上的主机执行地址验证。从路由器后面的主机接收的数据包将无法通过地址格式验证，且被丢弃，因为它们的源 MAC 地址将为路由器 MAC 地址，而不是主机 MAC 地址。

不受支持的命令

以下 IPv6 命令在透明防火墙模式中不支持，因为它们需要路由器功能：

- **ipv6 address autoconfig**
- **ipv6 nd prefix**
- **ipv6 nd ra-interval**
- **ipv6 nd ra-lifetime**
- **ipv6 nd suppress-ra**

配置全局 IPv6 地址

如要为网桥组或管理接口配置全局 IPv6 地址，请执行以下步骤。

注　配置全局地址将自动配置本地链路地址，因此，无需另行配置它。

限制

ASA 不支持 IPv6 任播地址。

先决条件

- 根据型号设置接口：
  - ASA 5512-X 和更高版本 - 第 9 章，“基本接口配置 （ASA 5512-X 及更高版本）”
  - ASASM-第 3 章，“适用于思科 ASA 服务模块的交换机配置”
  - ASAv-第 10 章，“基本接口配置 (ASAv)”
- 在多情景模式中，只能配置已根据第 6-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。如要从系统切换至情景配置，请在输入 **changeto context** *name* 命令；双击有效设备 IP 地址下的情景名称。

详细步骤

	命令	用途
步骤 1	对于网桥组： **interface bvi** *bridge_group_id* 对于管理接口： **interface** *management_interface_id* **示例：** `ciscoasa(config)# interface bvi 1`	如果尚未处于接口配置模式，则可进入接口配置模式。

	命令	用途
步骤 2	**ipv6 address** *ipv6-address/prefix-length* [**standby** *ipv6-address*] **示例：** `ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48`	向接口分配全局地址。分配全局地址时，将自动为接口 （为网桥组、为每个成员接口）创建本地链路地址。 **standby** 指定辅助设备使用的接口地址或故障转移对中的故障转移组。 **注**　在透明模式中，不支持要将 Modified EUI-64 接口 ID 用于接口 ID 的关键字 **eui-64**。
步骤 3	（可选） **ipv6 enforce-eui64** *if_name* **示例：** `ciscoasa(config)# ipv6 enforce-eui64 inside`	在本地链路上的 IPv6 地址中，强制使用 Modified EUI-64 格式的接口标识符。 *if_name* 参数是接口名称，由 **nameif** 命令指定，在该名称上可启用地址格式强制执行。 有关详细信息，请参阅第 12-12 页的 Modified EUI-64 接口 ID。

配置 IPv6 邻居发现

如要配置 IPv6 邻居发现，请参阅第 25 章，“IPv6 邻居发现”。

允许同一安全级别通信

默认情况下，同一个安全级别的接口不能相互通信，而且数据包无法进入和退出同一接口。本节介绍当接口为同一安全级别时如何启用接口间通信。

有关接口间通信的信息

如果想要流量不用 ACL 就能在所有同一安全级别接口之间自由流动，允许同一安全级别的接口间相互通信将非常有用。

如果启用同一安全级别接口通信，则仍可照常配置不同安全级别的接口。

详细步骤

命令	用途
same-security-traffic permit inter-interface	启用同一安全级别的接口，使接口间可以互相通信。

关闭和打开接口

本节介绍如何关闭和打开接口。

默认情况下，所有接口均已启用。在多情景模式中，如果禁用或重新启用情景内的接口，则只有该情景接口受到影响。但是，如果禁用或重新启用系统执行空间中的接口，则将影响所有情景中的该接口。

详细步骤

	命令	用途
步骤 1	ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **示例：** ciscoasa(config)# interface vlan 100	如果尚未处于接口配置模式，则可进入接口配置模式。 在多情景模式中，如已使用 **allocate-interface** 命令分配一个接口，请输入 *mapped_name* 命令。
步骤 2	**shutdown** **示例：** ciscoasa(config-if)# shutdown	禁用接口。
步骤 3	**no shutdown** **示例：** ciscoasa(config-if)# no shutdown	重新启用接口。

监控接口

命令	用途
show interface	显示接口统计信息。
show interface ip brief	显示接口的 IP 地址和状态。
show bridge-group	显示网桥组信息。

透明模式接口的配置示例

以下示例包括两个网桥组，每组三个接口，还有一个管理专属接口：

```
interface gigabitethernet 0/0
    nameif inside1
    security-level 100
    bridge-group 1
    no shutdown
interface gigabitethernet 0/1
    nameif outside1
    security-level 0
    bridge-group 1
    no shutdown
interface gigabitethernet 0/2
    nameif dmz1
    security-level 50
    bridge-group 1
    no shutdown
interface bvi 1
    ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
    nameif inside2
```

```
    security-level 100
    bridge-group 2
    no shutdown
interface gigabitethernet 1/1
    nameif outside2
    security-level 0
    bridge-group 2
    no shutdown
interface gigabitethernet 1/2
    nameif dmz2
    security-level 50
    bridge-group 2
    no shutdown
interface bvi 2
    ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
    nameif mgmt
    security-level 100
    ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
    no shutdown
```

透明模式接口的功能历史

表 12-1 列出了各种功能变更以及实施该等功能变更的平台版本。

表 12-1　透明模式接口的功能历史

功能名称	平台版本	功能信息
增加的 VLAN 数量	7.0(5)	增加了以下限制： • ASA5510 基础许可证的 VLAN 数从 0 增加到 10。 • ASA5510 增强型安全许可证的 VLAN 数从 10 增加到 25。 • ASA5520 的 VLAN 数从 25 增加到 100。 • ASA5540 的 VLAN 数从 100 增加到 200。
增加的 VLAN 数量	7.2(2)	ASA 5505 上增强型安全许可证 VLAN 的最大数量从 5（3 个全功能；1 个故障转移；一个限定于备用接口）增加至 20 个全功能接口。此外，中继端口数量从 1 增加到 8。现在已有 20 个全功能接口，无需使用备用接口命令削弱备用 ISP 接口的功能；可使用全功能接口替代它。备用接口命令对于 Easy VPN 配置仍非常有用。 以下型号的 VLAN 数量限制也有增加：ASA 5510（对于基础许可证，从 10 增加到 50，对于增强型安全许可证，从 25 增加到 100）、ASA 5520（从 100 增加到 150）和 ASA 5550（从 200 增加到 250）。
对于 ASA 5510 增强型安全许可证的千兆以太网支持	7.2(3)	ASA 5510 目前通过增强型安全许可证支持端口 0 和 1 的 GE（千兆以太网）。如果从基础许可证升级至增强型安全许可证，则外部 Ethernet 0/0 和 Ethernet0/1 端口的容量将从原始的 FE（快速以太网）(100 Mbps) 增加到 GE (1000 Mbps)。接口名称仍保持为 Ethernet 0/0 和 Ethernet0/1。使用 **speed** 命令更改接口上的速度，使用 **show interface** 命令查看当前为每个接口配置的速度。

表 12-1　　透明模式接口的功能历史（续）

功能名称	平台版本	功能信息
对 ASA 5505 的本地 VLAN 支持	7.2(4)/8.0(4)	现在可将本地 VLAN 纳入 ASA 5505 中继端口。 我们引入了以下命令：**switchport trunk native vlan**。
对 ASA 5580 的巨型数据包支持	8.1(1)	思科 ASA 5580 支持巨型帧。巨型帧是一个以太网数据包，其大小大于标准的最大值 1518 字节 （包括第 2 层报头和 FCS），最大可达 9216 字节。可通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配更多内存可能会限制对其他功能的最充分利用，如 ACL。 我们引入了以下命令：**jumbo-frame reservation**。
为 ASA 5580 增加的 VLAN 数	8.1(2)	ASA 5580 支持的 VLAN 数量从 100 增加到 250。
对透明模式的 IPv6 支持	8.2(1)	已为透明防火墙模式引入 IPv6 支持。
对 ASA 5580 10 千兆以太网接口上流量控制的暂停帧支持	8.2(2)	现可为流量控制启用暂停 (XOFF) 帧。 我们引入了以下命令：**flowcontrol**。
透明模式的网桥组	8.4(1)	如果不想产生安全情景开销，或者要最大限度地使用安全情景，请将接口一起组合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组流量与其他网桥组是隔离开的。在单情景模式或每个情景中可配置多达八个网桥组，每组四个接口。 我们引入了以下命令：**interface bvi**、 **show bridge-group**。
透明模式的网桥组最大数量增加到 250	9.3(1)	网桥组最大数量从 8 增加到 250。在单情景模式和多情景模式的每个情景中，最多可配置 250 个网桥组，每组最多 4 个接口。 我们修改了以下命令：**interface bvi**、 **bridge-group**。

第 4 部分

基本设置

第 13 章

基本设置

本章介绍如何在 ASA 上配置有效配置通常所需的基本设置。

- 第 13-1 页的设置主机名、域名及启用和 Telnet 密码
- 第 13-2 页的恢复启用和 Telnet 密码
- 第 13-7 页的设置日期和时间
- 第 13-10 页的配置主密码
- 第 13-13 页的配置 DNS 服务器
- 第 13-14 页的调整 ASP（加速安全路径）性能和行为

设置主机名、域名及启用和 Telnet 密码

如要设置主机名、域名及启用和 Telnet 密码，请执行以下步骤。

准备工作

- 在多情景模式中，可在系统和情景执行空间中配置主机名和域名。
- 启用和 Telnet 密码可在每个情景中设置；它们在系统中不可用。在多情景模式中发起从交换机到 ASASM 的会话时，ASASM 使用管理员情景中设置的登录密码。
- 如要从系统切换至情景配置，请输入 **changeto context** *name* 命令。

操作步骤

步骤 1 为 ASA 或情景指定主机名。默认主机名为“asa”。

hostname *name*

示例：

```
ciscoasa(config)# hostname myhostnamexample12345
```

此名称最多包含 63 个字符。主机名必须以字母或数字开头和结尾，并且只能包含字母、数字或连字符。

为 ASA 设置主机名后，该名称显示在命令行 提示符中。如果建立与多个设备的会话，则该主机名有助于跟踪命令输入位置。

对于多情景模式，在系统执行空间中设置的主机名均显示在所有情景的命令行提示符中。在情景内选择性设置的主机名不会显示在命令行中，但可供 **banner** 命令 **$(hostname)** 令牌使用。

步骤 2　为 ASA 指定域名。默认域名为 default.domain.invalid。

domain-name *name*

示例：

```
ciscoasa(config)# domain-name example.com
```

ASA 将域名作为后缀附加至非限定名称。例如，如果将域名设置为“example.com”，并以非限定名称“jupiter”指定系统日志服务器，则 ASA 将名称限定为“jupiter.example.com”。

步骤 3　如更改启用密码。默认情况下，启用密码为空。

如果不配置启用身份验证，则可使用启用密码进入特权 EXEC 模式。如果不配置 HTTP 身份验证，还可使用启用密码以空白用户名登录 ASDM。

enable password *password*

示例：

```
ciscoasa(config)# enable passwd Pa$$w0rd
```

password 参数为区分大小写的密码，最多由 16 个字母数字和特殊字符组成。密码中可使用除问号或空格外的任何字符。

该命令可更改最高权限级别 (15) 的密码。如果配置本地命令授权，则可使用以下语法，为从 0 到 15 的每个权限级别设置启用密码：

enable password *password* **level** *number*

该密码以加密形式保存在配置中，因此，输入后就无法查看原始密码。输入不含密码的 **enable password** 命令，将密码设置为默认的空值。

步骤 4　为 Telnet 访问设置登录密码。没有默认密码。

未配置 Telnet 身份验证时，该登录密码可用于 Telnet 访问。通过 **session** 命令从交换机访问 ASASM 时也可使用该密码。

{**passwd** | **password**} *password* [**encrypted**]

示例：

```
ciscoasa(config)# password cisco12345
```

可输入 **passwd** 或 **password**。*password* 为区分大小写的密码，最多由 16 个字母数字和特殊字符组成。密码中可使用除问号或空格外的任何字符。

该密码以加密形式保存在配置中，因此，输入后就无法查看原始密码。如果出于某种原因需要将密码复制到另一个 ASA，但不知道原始密码，则可随加密密码和关键字 **encrypted** 一起输入 **passwd** 命令。通常，只能在输入 **showing running-config passwd** 命令时查看该密码。

相关主题

第 35-16 页的配置访问特权 EXEC 模式 （enable 命令）的身份验证）

恢复启用和 Telnet 密码

忘记启用或 Telnet 密码时，可恢复它们。操作步骤因设备类型不同而异。必须使用 CLI 执行该任务。

- 第 13-3 页的恢复 ASA 上的密码
- 第 13-4 页的恢复 ASA 5506、 5506-W 和 ASA 5508 上的密码

- 第 13-5 页的恢复 ASAv 上的密码或映像
- 第 13-6 页的禁用密码恢复

恢复 ASA 上的密码

如要恢复 ASA 的密码，请执行以下步骤：

操作步骤

步骤 1　连接到 ASA 控制台端口。

步骤 2　关闭 ASA，然后再启动。

步骤 3　启动之后，在系统提示进入 ROMMON 模式时按下 **Escape** 键。

步骤 4　如要更新配置寄存器值，请输入以下命令：

```
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
```

步骤 5　如要将 ASA 设置为忽略启动配置，请输入以下命令：

```
rommon #1> confreg
```

ASA 显示当前配置寄存器值，并询问是否要更改它：

```
Current Configuration Register: 0x00000041
Configuration Summary:
boot default image from Flash
  ignore system configuration

Do you wish to change this configuration?y/n [n]: y
```

步骤 6　记录当前配置寄存器值，以便稍后恢复。

步骤 7　在提示符处输入 **Y** 以更改值。

ASA 提示输入新值。

步骤 8　接受所有设置的默认值，但“disable system configuration?”值除外。

步骤 9　在提示符处输入 **Y**。

步骤 10　通过输入以下命令重新加载 ASA：

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```

ASA 加载默认配置，而非启动配置。

步骤 11　通过输入以下命令访问特权 EXEC 模式：

```
ciscoasa# enable
```

步骤 12　系统提示输入密码时，按下 **Enter**。

密码为空。

步骤 13　通过输入以下命令加载启动配置：

```
ciscoasa# copy startup-config running-config
```

步骤 14　通过输入以下命令访问全局配置模式：

```
ciscoasa# configure terminal
```

步骤 15　通过输入以下命令，根据需要在默认配置中更改密码：

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

步骤 16　通过输入以下命令加载默认配置：

```
ciscoasa(config)# no config-register
```

默认配置寄存器值为 0x1。有关配置寄存器的详细信息，请参阅命令参考。

步骤 17　通过输入以下命令，将新密码保存至启动配置：

```
ciscoasa(config)# copy running-config startup-config
```

恢复 ASA 5506、 5506-W 和 ASA 5508 上的密码

如要恢复 ASA 5506、 5506-W 和 5508 的密码，请执行以下步骤：

操作步骤

步骤 1　连接到 ASA 控制台端口。

步骤 2　关闭 ASA，然后再启动。

步骤 3　启动之后，在系统提示进入 ROMMON 模式时按下 **Escape** 键。

步骤 4　如要更新配置寄存器值，请输入以下命令：

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

ASA 显示当前配置寄存器值和配置选项列表。记录当前配置寄存器值，以便稍后恢复。

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ..... auto-boot index 1 image in disks
```

步骤 5　通过输入以下命令重新加载 ASA：

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASA 加载默认配置，而非启动配置。

步骤 6　通过输入以下命令访问特权 EXEC 模式：

```
ciscoasa# enable
```

步骤 7　系统提示输入密码时，按下 **Enter**。

密码为空。

步骤 8　通过输入以下命令加载启动配置：

```
ciscoasa# copy startup-config running-config
```

步骤 9　通过输入以下命令访问全局配置模式：

```
ciscoasa# configure terminal
```

步骤 10　通过输入以下命令，根据需要在默认配置中更改密码：

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

步骤 11　通过输入以下命令加载默认配置：

```
ciscoasa(config)# no config-register
```

默认配置寄存器值为 0x1。有关配置寄存器的详细信息，请参阅 命令参考。

步骤 12　通过输入以下命令，将新密码保存至启动配置：

```
ciscoasa(config)# copy running-config startup-config
```

恢复 ASAv 上的密码或映像

如要恢复 ASAv 上的密码或映像，请执行以下步骤：

操作步骤

步骤 1　将运行的配置复制到 ASAv 上的备份文件：

```
copy running - config filename
```

示例：

```
ciscoasa# copy running-config backup.cfg
```

步骤 2　重新启动 ASAv：

```
reload
```

步骤 3　从 GNU GRUB 菜单，按向下箭头，选择 **<filename> with no configuration load** 选项，然后按下 **Enter**。文件名为 ASAv 上的默认启动映像文件名。默认启动映像永远不会通过 **fallback** 命令自动启动。然后加载选定的启动映像。

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

示例：

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

步骤 4　将备份配置文件复制至运行的配置。

copy *filename* **running-config**

示例：

```
ciscoasa (config)# copy backup.cfg running-config
```

步骤 5　重置密码。

enable password

示例：

```
ciscoasa(config)# enable password cisco123
```

步骤 6　保存新配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

禁用密码恢复

注　无法在 ASAv 上禁用密码恢复。

如要禁用密码恢复以确保未授权用户无法使用密码恢复机制危害 ASA，请执行以下步骤。

准备工作

在 ASA 上，**no service password-recovery** 命令可防止通过在配置完整无损的情况下进入 ROMMON 模式。进入 ROMMON 模式时，ASA 提示擦除所有闪存文件系统。不先执行该擦除操作就无法进入 ROMMON 模式。如果选择不擦除闪存文件系统，ASA 就会重新加载。因为密码恢复取决于使用 ROMMON 模式和维护现有配置，因此，该擦除可防止恢复密码。但是，禁用密码恢复会防止未授权用户查看配置或插入不同的密码。在此情况下，如要将系统恢复到操作状态，请加载新映像和备份配置文件（如可用）。

service password-recovery 命令显示在配置文件中仅供参考。在 CLI 提示符处输入命令时，设置保存在 NVRAM 中。更改该设置的唯一方式就是在 CLI 提示符处输入命令。通过不同版本的命令加载新配置不会更改设置。如在将 ASA 配置为在启动时忽略 （为密码恢复作准备）启动配置的情况下禁用密码恢复，则 ASA 就会更改设置，以照常加载启动配置。如果使用故障转移，且将备用设备配置为忽略启动配置，则在 **no service password recovery** 命令复制到备用设备时也对配置寄存器作出相同更改。

操作步骤

步骤 1　禁用密码恢复。

no service password-recovery

示例：

```
ciscoasa (config)# no service password-recovery
```

设置日期和时间

注　请勿设置 ASASM 的日期和时间；它可从主机交换机接收这些设置。

- 第 13-7 页的设置时区和夏令时日期
- 第 13-8 页的使用 NTP 服务器设置日期和时间
- 第 13-9 页的手动设置日期和时间

设置时区和夏令时日期

如要设置时区和日期范围，请执行以下步骤：

操作步骤

步骤 1　设置时区。默认情况下，时区是 UTC 时区，夏令时日期范围是从 2:00 a.m 开始。 on the first Sunday in April to 2:00 a.m.on the last Sunday in October.

clock TimeZone *zone* [**-**]*hours* [*minutes*]

示例：

```
ciscoasa(config)# clock timezone PST -8
```

zone 参数以字符串形式指定时区，例如，PST 表示 Pacific Standard Time（太平洋标准时间）。

[**-**]*hours* 值设置与 UTC 偏差的小时数。例如，PST 为 -8 小时。

minutes 值设置与 UTC 偏差的分钟数。

步骤 2　输入以下命令之一，以更改夏令时日期范围的默认值。默认周期性日期范围从三月第二个星期日 2:00 a.m 开始到十一月第一个星期日 2:00 a.m. 结束。

- 设置夏令时开始和结束日期作为特定年份中的特定日期。如果使用此命令，则需要每年重置日期。

  clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]

  示例：

  ```
  ciscoasa(config)# clock summer-time PDT 1 April 2010 2:00 60
  ```

  zone 参数以字符串形式指定时区，例如，PDT 表示 Pacific Daylight Time（太平洋夏季时间）。

  day 值设置一月中的第几天，从 1 到 31。例如，可用 April 1 或 1 April 形式输入月份和日，具体取决于标准日期格式。

  month 值以字符串形式设置月份。可用 April 1 或 1 April 形式输入月份和日，具体取决于标准日期格式。

  year 值以四位数字格式设置年份，例如， 2004。年份范围从 1993 至 2035。

  hh:*mm* 值以 24 小时制设置小时和分钟。

  offset 值设置要为夏令时更改的分钟数。默认情况下，此值为 60 分钟。

- 以某月某日某一时间，而非某年中的特定日期这种形式，指定夏令时的开始和结束日期。此命令可供您设置循环性日期范围，无需每年更改。

  clock summer-time *zone* **recurring** [*week weekday month hh:mm week weekday month hh:mm*] [*offset*]

  示例：

  ```
  ciscoasa(config)# clock summer-time PDT recurring first Monday April 2:00 60
  ```

  zone 参数以字符串形式指定时区，例如， PDT 表示 Pacific Daylight Time （太平洋夏季时间）。

  week 值用 1 到 4 的整数或“第一”或“最后”这样的词指定某月中的第几周。例如，如果某天刚好在跨在第五周，则用“最后”来指定。

  weekday 值指定周几：周一、周二、周三等。

  month 值以字符串形式设置月份。

  hh:mm 值以 24 小时制设置小时和分钟。

  offset 值设置要为夏令时更改的分钟数。默认情况下，此值为 60 分钟。

使用 NTP 服务器设置日期和时间

NTP 用于实施分层服务器系统，可在网络系统中提供精确的同步时间。时间敏感性操作需要这种精确度，如验证 CRL，包括精确时间戳。可配置多个 NTP 服务器。 ASA 选择层级最低的服务器，作为衡量数据可靠性的方式。

NTP 服务器生成的时间将覆盖手动设置的任何时间。

准备工作

在多情景模式中，只能在系统配置中设置时间。

操作步骤

步骤 1　启用 NTP 服务器身份验证。

ntp authenticate

示例：

```
ciscoasa(config)# ntp authenticate
```

步骤 2　指定要作为受信任密钥的身份验证密钥 ID，通过 NTP 服务器进行身份验证必须执行此操作。

ntp trusted-key *key_id*

示例：

```
ciscoasa(config)# ntp trusted-key 1
```

key_id 参数为介于 1 与 4294967295 之间的值。可输入多个受信任密钥，供多台服务器使用。

步骤 3　设置 NTP 服务器身份验证密钥。

ntp authentication-key *key_id* **md5** *key*

示例：

```
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
```

key_id 参数是使用 **ntp trusted - key** 命令在步骤 2 中设置的 ID，*key* 参数是一个最长达 32 个字符的字符串。

步骤 4　确定 NTP 服务器。

ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

示例：

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
```

key_id 参数是使用 **ntp trusted-key** 命令设置的 ID。

source *interface_name* 关键字参数对确定 NTP 数据包的传出接口 （如果不想使用路由表中的默认接口）。由于该系统不包括多情景模式中的任何接口，因此，请指定管理员情景中定义的接口名称。

如果多台服务器的准确度相似，则 **prefer** 关键字将 NTP 服务器设置为首选服务器。 NTP 使用一种算法确定最准确的服务器，然后与该服务器同步。如果多个服务器准确度相似，则 **prefer** 关键字指定使用这些服务器中的哪个服务器。但是，如果某台服务器的准确度明显高于首选服务器，则 ASA 将使用这个更准确的服务器。例如， ASA 使用 2 层服务器，而不使用 作为首选服务器的 3 层服务器。

可确定多台服务器；ASA 使用最准确的服务器。

手动设置日期和时间

如要手动设置日期和时间，请执行以下步骤。

准备工作

在多情景模式中，只能在系统配置中设置时间。

操作步骤

步骤 1　手动设置日期时间

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

示例：

```
ciscoasa# clock set 20:54:00 april 1 2004
```

hh:*mm*:*ss* 参数以 24 小时制 设置小时、分钟和秒。例如，输入 20:54:00 表示 8:54 pm。

day 值设置一月中的第几天，从 1 到 31。例如，可用 April 1 或 1 April 形式输入月份和日，具体取决于标准日期格式。

month 值设置月份。视乎标准日期格式，可用 april 1 或 1 april 形式输入月份和日。

year 值以四位数字格式设置年份，例如，2004。年份范围为 1993 至 2035。

默认时区为 UTC。如果在输入 **clock set** 命令后使用 **clock timezone** 命令更改时区，则时间将自动调整至新时区。

该命令在硬件芯片中设置时间，不将时间保存在配置文件中。该时间保持至重新启动为止。不同于其他 **clock** 命令，该命令属于特权 EXEC 命令。如要重置时钟，需要通过 **clock set** 命令设置新时间。

配置主密码

主密码可供您用加密格式安全地存储纯文本密码，并提供一个对所有密码进行加密或掩蔽的通用密钥，无需更改任何功能。使用主密码的功能包括：

- OSPF
- EIGRP
- VPN 负载均衡
- VPN（远程访问和站点对站点）
- 故障转移
- AAA 服务器
- 日志记录
- 共享许可证

注　如果已启用故障转移，但未设置故障转移共享密钥，则在更改主密码时就会显示错误消息，通知您必须输入故障转移共享密钥，以防主密码更改以纯文本形式发送。

添加或更改主密码

如要添加或更改主密码，请执行以下步骤。

准备工作

该操作步骤只能在安全会话中进行，例如通过控制台、 SSH 或通过 HTTPS 连接 ASDM。

操作步骤

步骤 1　设置用于生成加密密钥的密码。密码的长度必须介于 8 到 128 个字符之间。除退格符号和双引号之外的所有字符都可用于密码。如果不在命令中输入新密码，则系统将提示您输入。如要更改密码，必须输入原密码。

key config-key password-encryption [*new_passphrase* [*old_passphrase*]]

示例：

```
ciscoasa(config)# key config-key password-encryption
原密钥：bumblebee
新密钥：haverford
确认密钥：haverford
```

注　使用交互式提示输入密码，避免密码被记录在命令历史缓冲区。

请谨慎使用 **no key config-key password-encrypt** 命令，因为该命令会将加密密码更改为纯文本密码。降级至不支持密码加密的软件版本时，可使用该命令的 **no** 形式。

步骤 2　启用密码加密。

password encryption aes

示例：

```
ciscoasa(config)# password encryption aes
```

只要密码加密已启用且有主密码可用，所有用户密码将立即得以加密。运行的配置将以加密格式显示密码。

如果启用密码加密时未配置密码，则该命令将成功预期该密码在未来将可用。

如果稍后使用 **no password encryption aes** 命令禁用密码加密，所有的现有加密密码将保持不变，而且，只要主密码存在，加密密码就会根据应用要求被解密。

步骤 3　保存主密码的运行时值和生成的配置。

```
write memory
```

示例：

```
ciscoasa(config)# write memory
```

如果未输入此命令，启动配置中的密码可能仍然可见 （如果此前未加密保存）。此外，在多情景模式中，主密码在系统情景配置中将被更改。因此，所有情景中的密码都将受到影响。如果未在系统情景模式中输入 **write memory** 命令，而不是在所有用户情景中未输入该命令，则用户情景中的加密密码可能会过期。或者，在系统情景中使用 **write memory all** 命令以保存所有配置。

示例

以下示例显示不存在先前密钥：

```
ciscoasa(config)# key config-key password-encryption 12345678
```

以下示例显示已存在密钥：

```
ciscoasa(config)# key config-key password-encryption 23456789
原密钥：12345678
```

在以下示例中，输入不含参数的命令，以便系统将提示输入密钥。由于密钥已经存在，因此系统将提示输入。

```
ciscoasa(config)# key config-key password-encryption
原密钥：12345678
新密钥：23456789
确认密钥：23456789
```

在以下示例中，不存在密钥，因此系统不会提示您提供该信息。

```
ciscoasa(config)# key config-key password-encryption
新密钥：12345678
确认密钥：12345678
```

禁用主密码

禁用主密码可将加密密码恢复为纯文本密码。如果降级为不支持加密密码的以前软件版本，移除密码可能十分有用。

准备工作

- 只有知道当前主密码才能禁用它。如果不知道密码，请参阅第 13-12 页的移除主密码。
- 此操作步骤只能在安全会话中进行；如通过 Telnet、 SSH，或通过 HTTPS 连接 ASDM。

操作步骤

步骤 1　移除主密码。如果未在命令中输入密码，则系统将提示您输入。

no key config-key password-encryption [*old_passphrase*]]

示例：

```
ciscoasa(config)# no key config-key password-encryption
```

警告！您已选择将加密密码恢复为纯文本格式。此操作将在配置中暴露密码，因此，查看、存储和复制配置时需加小心。

原密钥：bumblebee

步骤 2　保存主密码的运行时值和生成的配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

包含密码的非挥发性内存将被 0xFF 模式擦除并覆盖。

在多情景模式中，主密码在系统情景配置中将被更改。因此，所有情景中的密码都将受到影响。如果在系统情景模式中输入 **write memory** 命令，而不是在所有用户情景中输入该命令，则用户情景中的加密密码可能会过期。或者，在系统情景中使用 **write memory all** 命令以保存所有配置。

移除主密码

无法恢复主密码。如果主密码丢失或未知，则可将其移除。

操作步骤

步骤 1　移除主密钥和包括加密密码的配置。

write erase

示例：

```
ciscoasa(config)# write erase
```

步骤 2　通过启动配置重新加载 ASA，无需任何主密钥或加密密码。

reload

示例：

```
ciscoasa(config)# reload
```

配置 DNS 服务器

需要配置 DNS 服务器，以便 ASA 能够将主机名解析为 IP 地址。

- 第 13-13 页的设置 DNS 服务器
- 第 13-14 页的监控 DNS 缓存

设置 DNS 服务器

某些 ASA 功能需要使用 DNS 服务器，以按域名访问外部服务器；例如，Botnet Traffic Filter 功能需要用 DNS 服务器访问动态数据库服务器并解析静态数据库中的条目。通过其他功能，如 **ping** 或 **traceroute** 命令，可输入要 ping 或 traceroute 的名称，而且，ASA 能够通过与 DNS 服务器进行通信来解析名称。许多 SSL VPN 和证书命令也支持名称。

还必须配置 DNS 服务器，以在访问规则中使用完全限定域名 (FQDN) 网络对象。

注　ASA 有限支持使用 DNS 服务器，具体取决于功能。例如，当手动配置 **name** 命令以将名称与 IP 地址相关联并通过 **name** 命令启用名称时，大多数命令要求您输入 IP 地址且只能使用名称。

准备工作

确保为启用 DNS 域名查找所在的任何接口配置合适的路由和访问规则，以便能够达到 DNS 服务器。

操作步骤

步骤 1　启用 ASA，发送 DNS 请求至 DNS 服务器，以对受支持的命令执行名称查找。

dns domain-lookup *interface_name*

示例：

```
ciscoasa(config)# dns domain-lookup inside
```

步骤 2　指定 ASA 用于传出请求的 DNS 服务器组。

dns server-group DefaultDNS

示例：

```
ciscoasa(config)# dns server-group DefaultDNS
```

可为 VPN 隧道组配置其他 DNS 服务器组。有关详细信息，请参阅命令参考中的 **tunnel-group** 命令。

步骤 3　指定一个或多个 DNS 服务器。可将六个 IP 地址全部输入同一命令中，用空格分隔，或者也可单独输入每个命令。 ASA 按顺序尝试每台 DNS 服务器，直至收到响应。

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

示例：

```
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

监控 DNS 缓存

ASA 对来自外部 DNS 查询的 DNS 信息提供本地缓存，这些查询是为某些无客户端 SSL VPN 和证书命令发送的。首先在本地缓存中查找每个 DNS 转换请求。如果本地缓存中有该信息，则将返回生成的 IP 地址。如果本地缓存无法解析该请求，则将 DNS 查询发送至已配置的各个 DNS 服务器。如果外部 DNS 服务器解析请求，则生成的 IP 地址与其相应的主机名一起存储在本地缓存中。

如需监控 DNS 缓存，请参阅以下命令：

- **show dns-hosts**

  此命令显示 DNS 缓存，包括从 DNS 服务器中动态获悉的条目，以及使用 **name** 命令手动输入的名称和 IP 地址。

调整 ASP（加速安全路径）性能和行为

ASP 是实现层，在此使策略和配置付诸实施。除了在通过思科技术支持中心进行故障排除期间，其他操作均与该层无直接关系。但是，可以调整几项与性能和可靠性相关的行为。

- 第 13-14 页的选择规则引擎事务提交模型
- 第 13-15 页的启用 ASP 负载均衡

选择规则引擎事务提交模型

默认情况下，更改基于规则的策略（如访问规则）时，更改会立即生效。但是，这种即时性将稍微降低性能。对于每秒连接速率较高的环境中超大型规则列表，性能降低更加显著，例如，在 ASA 每秒处理 18,000 次连接的同时更改拥有 25,000 条规则的策略。

由于规则引擎要编译规则以实现更快的规则查找，因此，性能将受到影响。默认情况下，系统在评估连接尝试时也搜索未编译规则，以便能够应用新规则；由于规则未编译，因此，搜索需要更长时间。

可更改此行为，以便规则引擎在执行规则更改、继续使用原规则直至新规则编译完成并可供使用时使用事务性模型。通过事务性模型，在规则编译期间性能应不会下降。下表阐明行为差异。

型号	编译前	编译中	编译后
默认值	匹配原规则。	匹配新规则。 （每秒连接速率降低。）	匹配新规则。
事务性	匹配原规则。	匹配原规则。 （每秒连接速率不受影响）	匹配新规则。

事务性模型的另一个优势是，替换接口上的 ACL 时，删除原 ACL 和应用新 ACL 之间无间隙。该功能减少了可接受连接在操作期间被断开的可能性。

提示　如果为某种规则类型启用事务性模型，则将生成系统日志以标记编译的开始和结束。这些系统日志的编号从 780001 到 780004。

如要为规则引擎启用事务提交模型，请使用以下命令：

asp rule-engine transactional-commit *option*

其中，选项包括：

- **access-group** - 全局应用或应用于接口的访问规则。
- **nat** - 网络地址转换规则。

示例：

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

启用 ASP 负载均衡

ASP 负载均衡机制有助于避免以下问题：

- 因偶发的流量高峰而造成溢出
- 因大量流量过度订用特定接口接收环而造成溢出
- 相对严重超载的接口接收环引起的超限，其中，单个核心无法承受负载。

asp load-balance per-packet 命令允许多个核心同时对接收自单个接口接收环的数据包施加作用。如果系统丢弃数据包，并且 **show cpu** 命令输出远远小于 100%，则此命令可能有助于您的吞吐量（如果数据包属于许多无关连接）。 **auto** 选项使 ASA 能够自动打开和关闭每数据包负载均衡。

如要启用自动打开和关闭每数据包负载均衡功能，请输入以下命令：

```
ciscoasa(config)# asp load-balance per-packet auto
```

基本设置历史

功能名称	平台版本	说明
主密码	8.3(1)	我们引入了此功能。主密码可供您用加密格式安全地存储纯文本密码，并提供一个对所有密码进行加密或掩蔽的通用密钥，无需更改任何功能。 我们引入了以下命令：**key config-key password-encryption**、**password encryption aes**、**clear configure password encryption aes**、**show running-config password encryption aes**、**show password encryption**。
密码加密可见性	8.4(1)	我们已修改 **show password encryption** 命令。

功能名称	平台版本	说明
默认 Telnet 密码的移除	9.0(2)/9.1(2)	为了提高 ASA 管理访问的安全性，已移除 Telnet 的默认登录密码；使用 Telnet 登录之前必须手动设置密码。 **注**　如果不配置 Telnet 用户身份验证，登录密码仅用于 Telent（**aaa authentication telnet console** 命令）。 以前清除密码时，ASA 恢复默认值“cisco”。现在清除密码时，密码即被移除。 登录密码还用于从交换机到 ASASM 的 Telnet 会话（请参阅 **session** 命令）。对于初始 ASASM 访问，必须使用 **service-module session** 命令，直到设置登录密码。 我们修改了以下命令：**passwd**。
ASP 负载均衡	9.3(2)	我们引入了此功能。ASP 负载均衡机制允许 CPU 的多个核心接收并独立处理来自接口接收环的数据包，从而降低丢包率和提高吞吐量。 我们引入了以下命令：**asp load-balance per-packet-auto**。

动态 DNS

本章介绍如何配置动态 DNS (DDNS) 更新方法。

- 第 14-1 页的关于 DDNS
- 第 14-2 页的 DDNS 准则
- 第 14-2 页的配置 DDNS
- 第 14-7 页的监控 DDNS
- 第 14-7 页的 DDNS 历史记录

关于 DDNS

DDNS 更新将 DNS 与 DHCP 相集成。这两种协议互为补充：DHCP 实现 IP 地址分配集中化和自动化；DDNS 更新按预定义时间间隔自动记录已分配地址与和主机名之间的关联。 DDNS 允许频繁更新不断变化的地址与主机名的关联。例如，移动主机可以自由地在网络中移动而无需用户或管理员干预。DDNS 在 DNS 服务器上为名称与地址之间的相互映射提供必需的动态更新和同步。

DDNS 名称与地址之间的映射以两种资源记录 (RR) 保留在 DHCP 服务器上：A RR 将名称映射至 IP 地址，而 PTR RR 将地址映射至名称。执行 DDNS 更新的两个方法中 - RFC 2136 定义的 IETF 标准和通用 HTTP 方法 - ASA 支持 IETF 方法。

相关主题

- 第 15-3 页的配置 DHCP 服务器

DDNS 更新配置

最常见的两种 DDNS 更新配置如下：

- DHCP 客户端更新 A RR，而 DHCP 服务器更新 PTR RR。
- DHCP 服务器既更新 A RR 也更新 PTR RR。

通常， DHCP 服务器代表客户端维护 DNS PTR RR。可将客户端配置为执行所有所需 DNS 更新。可将服务器配置为是否履行这些更新。 DHCP 服务器必须了解客户端的完全限定域名 (FQDN) 才能更新 PTR RR。客户端使用一个名为 Client FQDN 的 DHCP 选项向服务器提供 FQDN。

UDP 数据包大小

DDNS 允许 DNS 请求方通告其 UDP 数据包的大小并促进传输大于 512 八位字节的数据包。当一个 DNS 服务器收到通过 UDP 提出的请求时，它会从 OPT RR 识别 UDP 数据包的大小，并将其回应扩展为包含尽可能多的资源记录，但不能超过请求方指定的 UDP 数据包大小上限。对于 BIND，DNS 数据包的大小不得超过 4096 字节，对于 Windows 2003 DNS 服务器，则不得超过 1280 字节。有多个其他 **message-length maximum** 命令可用：

- 现有全局限制：**message-length maximum 512**
- 客户端或服务器特定限制：**message-length maximum client 4096 and message-length maximum server 4096**
- OPT RR 字段中指定的动态值：**message-length maximum client auto**

如果三个命令同时存在，则 ASA 允许自动配置的长度不超过已配置客户端或服务器最大支持数量。对于所有其他 DNS 流量，则使用 message - length maximum。

DDNS 准则

情景模式准则

仅在透明模式中支持 DNS Client 窗格。

配置 DDNS

本节介绍如何配置 DDNS。

为静态 IP 地址更新 A 和 PTR RR

如要配置客户端以请求其为静态 IP 地址更新 A 和 PTR RR，请执行以下步骤：

操作步骤

步骤 1　创建 DDNS 更新方法以动态更新 DNS RR。

ddns update method *name*

示例：

```
ciscoasa(config)# ddns update method ddns-2
```

步骤 2　指定客户端更新 DNS A 和 PTR RR。

ddns both

示例：

```
ciscoasa(DDNS-update-method)# ddns both
```

步骤 3　配置接口并输入接口配置模式。

interface *mapped_name*

示例：

```
ciscoasa(DDNS-update-method)# interface eth1
```

步骤 4　将 DDNS 方法与接口和一个更新主机名相关联。

ddns update [*method-name* | **hostname** *hostname*]

示例：

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

步骤 5　为接口配置静态 IP 地址。

ip address *ip_address* [*mask*] [**standby** *ip_address*]

示例：

```
ciscoasa(config-if)# ip address 10.0.0.40 255.255.255.0
```

更新 A 和 PTR RR

如要配置 DHCP 客户端以请求其更新 A 和 PTR RR 并且 DHCP 服务器履行这些请求，请执行以下步骤

操作步骤

步骤 1　配置 DHCP 客户端以请求 DHCP 服务器不执行更新。

dhcp-client update dns [**server** {**both** | **none**}]

示例：

```
ciscoasa(config)# dhcp-client update dns server none
```

步骤 2　创建 DDNS 更新方法以动态更新 DNS RR。

ddns update method *name*

示例：

```
ciscoasa(config)# ddns update method ddns-2
```

步骤 3　指定客户端更新 DNS A 和 PTR RR。

ddns both

示例：

```
ciscoasa(DDNS-update-method)# ddns both
```

步骤 4　配置接口并输入接口配置模式。

interface *mapped_name*

示例：

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

步骤 5　将 DDNS 方法与接口和一个更新主机名相关联。

ddns update [*method-name* | **hostname** *hostname*]

示例：

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

步骤 6　使用 DHCP 为接口获取一个 IP 地址。

ip address dhcp

示例：

```
ciscoasa(if-config)# ip address dhcp
```

步骤 7　配置 DHCP 服务器以执行 DDNS 更新。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

示例：

```
ciscoasa(if-config)# dhcpd update dns
```

忽略对任一 RR 的更新

如要将 DHCP 客户端配置为包括 FQDN 选项 （该选项指示 DHCP 服务器不履行 A 或 PTR 更新），请执行以下步骤：

操作步骤

步骤 1　创建 DDNS 更新方法以动态更新 DNS RR。

ddns update method *name*

示例：

```
ciscoasa(config)# ddns update method ddns-2
```

步骤 2　指定客户端更新 DNS A 和 PTR RR。

ddns both

示例：

```
ciscoasa(DDNS-update-method)# ddns both
```

步骤 3　配置接口并输入接口配置模式。

interface *mapped_name*

示例：

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

步骤 4　将 DDNS 方法与接口和一个更新主机名相关联。

ddns update [*method-name* | **hostname** *hostname*]

示例：

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

步骤 5　配置 DHCP 客户端以请求 DHCP 服务器不执行更新。

dhcp-client update dns [**server** {**both** | **none**}]

示例：

```
ciscoasa(config)# dhcp-client update dns server none
```

步骤 6　使用 DHCP 为接口获取一个 IP 地址。

ip address dhcp

示例：

```
ciscoasa(if-config)# ip address dhcp
```

步骤 7　配置 DHCP 服务器以覆盖客户端更新请求。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

示例：

```
ciscoasa(if-config)# dhcpd update dns both override
```

仅更新 PTR RR

如要配置服务器以默认仅执行 PTR RR 更新，请执行以下步骤：

操作步骤

步骤 1　配置一个接口。

interface *mapped_name*

示例：

```
ciscoasa(config)# interface Ethernet0
```

步骤 2　请求 DHCP 服务器更新 DNS A 和 PTR RR。

dhcp-client update dns [**server** {**both** | **none**}]

示例：

```
ciscoasa(config-if)# dhcp-client update dns both
```

步骤 3　在已配置的接口上配置 DHCP 客户端。

ddns update [*method-name* | **hostname** *hostname*]

示例：

```
ciscoasa(config-if)# ddns update hostname asa
```

步骤 4　配置 DHCP 服务器以执行 DDNS 更新。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

示例：

```
ciscoasa(config-if)# dhcpd update dns
```

步骤 5　为 DHCP 客户端定义 DNS 域名。

dhcpd domain *domain_name* [**interface** *if_name*]

示例：

```
ciscoasa(config-if)# dhcpd domain example.com
```

使用客户端更新 RR 并使用服务器更新 PTR RR

如要配置客户端以更新 A 资源记录，且配置服务器以更新 PTR 记录，请执行以下步骤：

操作步骤

步骤 1　创建 DDNS 更新方法以动态更新 DNS RR。

ddns update method *name*

示例：

```
ciscoasa(config)# ddns update method ddns-2
```

步骤 2　指定一个 DDNS 更新方法。

ddns both

示例：

```
ciscoasa(DDNS-update-method)# ddns both
```

步骤 3　配置一个接口。

interface *mapped_name*

示例：

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

步骤 4　配置 DHCP 客户端传递至 DHCP 服务器的更新参数。

dhcp-client update dns [**server** {**both** | **none**}]

示例：

```
ciscoasa(config-if)# dhcp-client update dns
```

步骤 5　将 DDNS 方法与接口和一个更新主机名相关联。

ddns update [*method-name* | **hostname** *hostname*]

示例：

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa
```

步骤 6　配置 DHCP 服务器以执行 DDNS 更新。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

示例：

```
ciscoasa(if-config)# dhcpd update dns
```

步骤 7　为 DHCP 客户端定义 DNS 域名。

dhcpd domain *domain_name* [**interface** *if_name*]

示例：

```
ciscoasa(config-if)# dhcpd domain example.com
```

监控 DDNS

如需监控 DDNS 状态，请参阅以下命令：

- **show running-config ddns**

  此命令显示当前 DDNS 配置。
- **show running-config dns server-group**

  此命令显示当前 DNS 服务器组的状态。

DDNS 历史记录

表 14-1　DDNS 历史记录

功能名称	版本	功能信息
DDNS	7.0(1)	我们引入了此功能。 我们添加了下列命令：**ddns**、**ddns update**、**dhcp client update dns**、**dhcpd update dns**、**show running-config ddns** 和 **show running-config dns server-group**。

DHCP 服务

本章介绍如何配置 DHCP 服务器或 DHCP 中继。

- 第 15-1 页的关于 DHCP 服务器
- 第 15-2 页的关于 DHCP 中继代理
- 第 15-2 页的 DHCP 服务的许可要求
- 第 15-2 页的 DHCP 服务准则
- 第 15-3 页的配置 DHCP 服务器
- 第 15-11 页的监控 DHCP 服务
- 第 15-11 页的 DHCP 服务的历史记录

关于 DHCP 服务器

DHCP 为 DHCP 客户端提供网络配置参数，如 IP 地址。Cisco ASA 可为连接到 ASA 接口的 DHCP 客户端提供 DHCP 服务器。 DHCP 服务器直接为 DHCP 客户端提供网络配置参数。

客户端使用预留的链路范围组播地址查找 DHCP 服务器，以请求分配配置信息，该地址表明客户端和服务器应连接到同一链路。但是，在某些情况下，关注的是易管理性、经济性或可扩展性，我们建议您允许 DHCP 客户端向未连接到同一链路的服务器发送消息。可能驻留在客户端网络的 DHCP 中继代理可在客户端与服务器之间中转消息。中继代理操作对客户端来说是透明的。

IPv4 DHCP 客户端使用广播而非组播地址到达服务器。DHCP 客户端侦听 UDP 端口 68 上的消息；DHCP 服务器侦听 UDP 端口 67 上的消息。

在 RFC 3315 中为 IPv6 指定的 DHCP (DHCPv6) 可使 IPv6 DHCP 服务器向 IPv6 节点 （即 DHCP 客户端）发送配置参数，如网络地址或前缀和 DNS 服务器地址。 DHCPv6 使用以下组播地址：

- All_DHCP_Relay_Agents_and_Servers (FF02::1:2) 是客户端与相邻的 （即在连的）中继代理和服务器进行通信所使用的链路范围组播地址。所有 DHCPv6 服务器和中继代理均为此组播组的成员。
- DHCPv6 中继服务和服务器侦听 UDP 端口 547 上的消息。 ASA DHCPv6 中继代理在 UDP 端口 547 和 All_DHCP_Relay_Agents_and_Servers 组播地址上侦听。

关于 DHCP 中继代理

可配置 DHCP 中继代理以向一个或多个 DHCP 服务器转发接口上收到的 DHCP 请求。DHCP 客户端使用 UDP 广播发送其初始 DHCPDISCOVER 消息，因为它们没有与其所连接网络有关的信息。如果客户端位于不包含服务器的网段，则通常 UDP 广播不会由 ASA 进行转发，因为它不转发广播流量。

可通过配置接收广播来将 DHCP 请求转发到另一个接口上 DHCP 服务器的 ASA 接口来对此情况做出补救。

DHCP 服务的许可要求

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

对于所有 ASA 型号，DHCP 客户端地址的最大数量因许可证而异。

- 如果上限是 10 台主机，则最大可用 DHCP 池为 32 个地址。
- 如果上限是 50 台主机，则最大可用 DHCP 池为 128 个地址。
- 如果主机数量无限制，则最大可用 DHCP 池为 256 个地址。

DHCP 服务准则

防火墙模式准则

在透明防火墙模式中不受支持。有关详细信息，请参阅第 15-3 页的 DHCP 中继准则。

IPv6 准则

不支持特定接口 DHCP 中继服务器的 IPv6。

DHCP 服务器准则

- 最大可用 DHCP 池为 256 个地址。
- 只能在 ASA 的每个接口配置一个 DHCP 服务器。每个接口均可使用其自己的地址池。但是，其他 DHCP 设置 （如 DNS 服务器、域名、选项、 ping 超时和 WINS 服务器）以全局方式配置，且供 DHCP 服务器在所有接口上使用。
- 无法在已启用服务器的接口上配置 DHCP 客户端或 DHCP 中继服务。此外， DHCP 客户端必须直接连接到已启用服务器的接口。
- ASA 不支持 QIP DHCP 服务器与 DHCP 代理服务组合使用。
- 如也启用 DHCP 服务器，则不能启用中继代理。
- ASA DHCP 服务器不支持 BOOTP 请求。在多情景模式中，不能在多个情景中所使用接口上启用 DHCP 服务器或 DHCP 中继服务。

- 在收到 DHCP 请求后，ASA 向 DHCP 服务器发送发现消息。此消息包括在组策略中已通过 **dhcp-network-scope** 命令配置的 IP 地址（在子网内）。如果服务器有属于该子网的地址池，则服务器将向 IP 地址 - 而非发现消息的源 IP 地址发送要约消息和池信息。
- 客户端连接后，ASA 向服务器列表中的所有服务器发送发现消息。此消息包括在组策略中已通过 **dhcp-network-scope** 命令配置的 IP 地址（在子网内）。ASA 选择收到的第一条要约并丢弃其他要约。如果服务器有属于该子网的地址池，则服务器将向 IP 地址 - 而非发现消息的源 IP 地址发送要约消息和池信息。如果需要更新地址，则其将尝试与租赁服务器（从其获得地址的服务器）更新地址。如果 DHCP 更新在指定次数的重试（四次尝试）后失败，则 ASA 将在过了预定时间段之后移至 DHCP 重新绑定阶段。在重新绑定阶段，ASA 向组中所有服务器同时发送请求。在高可用性环境中，租赁信息是共享的，因此，其他服务器可以确认租赁，并且 ASA 将返回到绑定状态。在重新绑定阶段，如未收到服务器列表中任何服务器的响应（三次重试后），则 ASA 将清除此类条目。

  例如，如果服务器有一个范围在 209.165.200.225 到 209.165.200.254 之间的池，掩码为 255.255.255.0，**dhcp-network-scope** 命令指定的 IP 地址为 209.165.200.1，则服务器将要约消息中的该池发送给 ASA。

  dhcp-network-scope 命令设置仅适用于 VPN 用户。

DHCP 中继准则

- 在单一模式和每个情景中，最多可以配置 10 台 DHCPv4 中继服务器，这些服务器为全局和特定接口服务器的组合，其中每个接口最多允许 4 台服务器。
- 在单一模式和每个情景中，最多可以配置 10 台 DHCPv6 中继服务器。不支持 IPv6 的特定接口服务器。
- 如也启用 DHCP 服务器功能，则不能启用中继代理。
- 如已启用 DHCP 中继服务，且定义了多台 DHCP 中继服务器，则 ASA 将向每个已定义的 DHCP 中继服务器转发客户端请求。来自服务器的回复也会转发到客户端，直到解除客户端 DHCP 中继绑定。如果 ASA 接收到以下任意 DHCP 消息：ACK、NACK、ICMP 不可达或拒绝，则绑定解除。
- 不能启用接口上作为 DHCP 代理服务运行的 DHCP 中继服务。必须首先移除 VPN DHCP 配置，否则将显示错误消息。在同时启用 DHCP 中继和 DHCP 代理服务后，将出现此错误。确保已启用 DHCP 中继或 DHCP 代理服务，但不能同时启用两者。
- 在透明防火墙模式中，DHCP 中继服务不可用。但是，可通过使用访问列表允许 DHCP 流量通过。如要在透明模式中允许 DHCP 请求和回复通过 ASA，则需要配置两个访问列表，一个允许从内部接口到外部接口的 DCHP 请求，另一个允许来自其他方向的服务器的回复。
- 对于 IPv4，客户端必须直接连接到 ASA 且不能通过另一个中继代理或路由器发送请求。对于 IPv6，ASA 支持来自另一个中继服务器的数据包。
- 对于多情景模式，不能在多个情景使用的接口上启用 DHCP 中继。
- DHCP 客户端必须与 ASA 中继请求的 DHCP 服务器位于不同接口。

配置 DHCP 服务器

本节介绍如何配置 ASA 提供的 DHCP 服务器。

步骤 1　启用 DHCP 服务器。请参阅第 15-4 页的启用 DHCP 服务器。

步骤 2　配置高级 DHCP 选项。请参阅第 15-5 页的配置高级 DHCP 选项。

步骤 3　配置 DHCPv4 中继代理或 DHCPv6 中继代理。请参阅第 15-9 页的配置 DHCPv4 中继代理或第 15-10 页的配置 DHCPv6 中继代理。

启用 DHCP 服务器

如要在 ASA 接口上启用 DHCP 服务器，请执行以下步骤：

操作步骤

步骤 1　创建 DHCP 地址池。ASA 向客户端分配来自该地址池的其中一个地址供其使用指定的一段时间。这些地址属于直接连接网络的本地未转换地址。

dhcpd address *ip_address if_name*

示例：

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
```

地址池必须与 ASA 接口位于相同的子网中。

步骤 2　（可选）指定 DNS 服务器的 IP 地址。

dhcpd dns *dns1* [*dns2*]

示例：

```
ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
```

步骤 3　（可选）指定 WINS 服务器的 IP 地址。最多可指定两台 WINS 服务器。

dhcpd wins *wins1* [*wins2*]

示例：

```
ciscoasa(config)# dhcpd wins 209.165.201.5
```

步骤 4　（可选）更改要授予客户端的租用时间。租用时间等于租赁到期之前客户端可以使用向其分配的 IP 地址的时间 （以秒为单位）。输入一个介于 0 与 1,048,575 之间的值。默认值为 3600 秒。

dhcpd lease *lease_length*

示例：

```
ciscoasa(config)# dhcpd lease 3000
```

步骤 5　（可选）配置域名。

dhcpd domain *domain_name*

示例：

```
ciscoasa(config)# dhcpd domain example.com
```

步骤 6　（可选）配置 ICMP 数据包的 DHCP ping 超时值。为避免地址冲突，ASA 会在将地址分配给 DHCP 客户端之前向该地址发送两个 ICMP ping 数据包。

dhcpd ping_timeout *milliseconds*

示例：

```
ciscoasa(config)# dhcpd ping timeout 20
```

步骤 7　定义发送给 DHCP 客户端的默认网关。如果不使用 **dhcpd option 3** 命令来定义默认网关，则 DHCP 客户端默认使用最接近 DHCP 客户端的 ASA 接口 IP 地址；ASA 将不使用管理接口 IP 地址。因此，DHCP ACK 不包括此选项。

dhcpd option 3 ip *gateway_ip*

示例：

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

步骤 8　在 ASA 中启用 DHCP 后台守护程序，以侦听已启用接口上的 DHCP 客户端请求。

dhcpd enable *interface_name*

示例：

```
ciscoasa(config)# dhcpd enable outside
```

配置高级 DHCP 选项

ASA 支持 RFC 2132、 RFC 2562 和 RFC 5510 中所列的DHCP 选项以发送信息。

可以使用高级 DHCP 选项向 DHCP 客户端提供 DNS、WINS 和域名参数。也可以使用 DHCP 自动配置设置获得这些值或手动定义这些值。如果使用多种方法定义此信息，则按以下序列将其传递给 DHCP 客户端：

1. 手动配置的设置。
2. 高级 DHCP 选项设置。
3. DHCP 自动配置设置。

例如，可以手动定义想要 DHCP 客户端接收的域名，然后启用 DHCP 自动配置。尽管 DHCP 自动配置要结合 DNS 和 WINS 服务器发现域，但手动定义的域名将与已发现的 DNS 和 WINS 服务器名称一起传递到 DHCP 客户端，因为手动定义的域名将取代通过 DHCP 自动配置过程发现的域名。

返回 IP 地址

如要配置返回一个或两个 IP 地址的 DHCP 选项，请执行以下步骤：

操作步骤

步骤 1　配置返回一个或两个 IP 地址的 DHCP 选项。

dhcpd option *code* **ip** *addr_1* [*addr_2*]

示例：

```
ciscoasa(config)# dhcpd option 2 ip 10.10.1.1 10.10.1.2
```

返回文本字符串

如要配置返回文本字符串的 DHCP 选项，请执行以下步骤：

操作步骤

步骤 1　配置返回文本字符串的 DHCP 选项。

dhcpd option *code* **ascii** *text*

示例：

```
ciscoasa(config)# dhcpd option 2 ascii examplestring
```

返回十六进制值

如要配置返回十六进制值的 DHCP 选项，请执行以下步骤：

操作步骤

步骤 1　配置返回十六进制值的 DHCP 选项。

dhcpd option *code* **hex** *value*

示例：

```
ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11
```

注　ASA 将不验证您提供的选项类型和值是否与 RFC 2132 中定义的选项代码的预期类型和值相匹配。例如，可输入 **dhcpd option 46 ascii hello** 命令，尽管 RFC 2132 中定义的选项 46 期望一位数十六进制值，但 ASA 仍将接受配置。有关选项代码及其关联的类型和期望值的详细信息，请参阅 RFC 2132。

表 15-1 显示 **dhcpd option** 命令不支持的 DHCP 选项。

表 15-1　不受支持的 DHCP 选项

选项代码	说明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER

表 15-1　不受支持的 DHCP 选项 （续）

选项代码	说明
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

DHCP 选项 3、66 和 150 用于配置 Cisco IP 电话。有关配置这些选项的详细信息，请参阅第 15-7 页的使用 DHCP 服务器配置 Cisco IP 电话。

使用 DHCP 服务器配置 Cisco IP 电话

Cisco IP 电话从 TFTP 服务器下载其配置。当 Cisco IP 电话启动时，如果其不让 IP 地址和 TFTP 服务器 IP 地址均得以预配置，则其将向 DHCP 服务器发送带有选项 150 或 66 的请求以获取此信息。

- DHCP 选项 150 提供 TFTP 服务器列表的 IP 地址。
- DHCP 选项 66 提供单一 TFTP 服务器的 IP 地址或主机名。

注　Cisco IP 电话也可在其请求中包含 DHCP 选项 3，该选项设置默认路由。

单一请求可能同时包括选项 150 和 66。在此情况下，如在 ASA 上已配置这两个选项，则 ASA DHCP 服务器将在响应中为两个选项提供值。

任何选项编号

如要发送用于任何选项编号的信息，请执行以下步骤：

操作步骤

步骤 1　为包含 RFC 2132 中指定的选项编号的 DHCP 请求提供信息。

dhcpd option *number value*

示例：

```
ciscoasa(config)# dhcpd option 2
```

选项 66

如要发送用于选项 66 的信息，请执行以下步骤：

操作步骤

步骤 1　为选项 66 提供一个 TFTP 服务器的 IP 地址或名称。

dhcpd option 66 ascii *server_name*

示例：

```
ciscoasa(config)# dhcpd option 66 ascii exampleserver
```

选项 150

如要发送用于选项 150 的信息，请执行以下步骤：

操作步骤

步骤 1　为选项 150 提供一个或两个 TFTP 服务器的 IP 地址或名称。

dhcpd option 150 ip *server_ip1* [*server_ip2*]

示例：

```
ciscoasa(config)# dhcpd option 150 ip 10.10.1.1
```

server_ip1 为主要 TFTP 服务器的 IP 地址或名称，而 *server_ip2* 为次要 TFTP 服务器的 IP 地址或名称。使用选项 150 最多可识别两个 TFTP 服务器。

选项 3

如要发送用于选项 3 的信息，请执行以下步骤：

操作步骤

步骤 1　设置默认路由。

dhcpd option 3 ip *router_ip1*

示例：

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

配置 DHCPv4 中继代理

在 DHCP 请求进入接口后，ASA 中继将请求转发到的 DHCP 服务器取决于您的配置。可以配置以下类型的服务器：

- 接口特定 DHCP 服务器 - DHCP 请求进入特定接口后，ASA 仅向接口特定服务器中继请求。
- 全局 DHCP 服务器 - DHCP 请求进入未让接口特定服务器得以配置的接口后，ASA 将向所有全局服务器中继请求。如果接口有接口特定服务器，则将不使用全局服务器。

操作步骤

步骤 1　执行以下两项操作之一或全部：

- 指定一个全局 DHCP 服务器 IP 地址及到达该地址所经过的接口。

  dhcprelay server *ip_address if_name*

  示例：

  ```
  ciscoasa(config)# dhcprelay server 209.165.201.5 outside
  ciscoasa(config)# dhcprelay server 209.165.201.8 outside
  ciscoasa(config)# dhcprelay server 209.165.202.150 it
  ```

- 指定连接到 DHCP 客户端网络的接口 ID 以及要用于进入该接口的 DHCP 请求的 DHCP 服务器 IP 地址。

  interface *interface_id*
  dhcprelay server *ip_address*

  示例：

  ```
  ciscoasa(config)# interface gigabitethernet 0/0
  ciscoasa(config)# dhcprelay server 209.165.201.6
  ciscoasa(config)# dhcprelay server 209.165.201.7
  ciscoasa(config)# interface gigabitethernet 0/1
  ciscoasa(config)# dhcprelay server 209.165.202.155
  ciscoasa(config)# dhcprelay server 209.165.202.156
  ```

  请注意，如同在全局 **dhcprelay server** 命令中，您未为请求指定输出接口；相反，ASA 将使用路由表确定输出接口。

步骤 2　在与 DHCP 客户端相连的接口上启用 DHCP 中继服务。可以在多个接口上启用 DHCP 中继。

dhcprelay enable *interface*

示例：

```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# dhcprelay enable dmz
ciscoasa(config)# dhcprelay enable eng1
ciscoasa(config)# dhcprelay enable eng2
ciscoasa(config)# dhcprelay enable mktg
```

步骤 3　（可选）设置为 DHCP 中继地址处理预留的秒数。

dhcprelay timeout *seconds*

示例：

```
ciscoasa(config)# dhcprelay timeout 25
```

步骤 4　（可选）将从 DHCP 服务器发送的数据包中第一个默认路由器地址更改为 ASA 接口的地址。

dhcprelay setroute *interface_name*

示例：

```
ciscoasa(config)# dhcprelay setroute inside
```

此操作使客户端能设置将指向 ASA 的其默认路由，即使 DHCP 服务器指定了另一个路由器。如果数据包内无默认路由器选项，则 ASA 将添加一个包含接口地址的选项。

步骤 5　（可选）请执行以下操作之一：

- 指定要信任的 DHCP 客户端接口。

  interface *interface_id*
  dhcprelay information trusted

  示例：

  ```
  ciscoasa(config)# interface gigabitethernet 0/0
  ciscoasa(config-if)# dhcprelay information trusted
  ```

  可将接口配置为受信任接口，以保留 DHCP 选项 82。下游交换机和路由器使用 DHCP 选项 82 进行 DHCP 探听和 IP 源保护。通常，如果 ASA DHCP 中继代理接收到一个已设置选项 82 的 DHCP 数据包，但是 giaddr 字段（在将数据包转发到服务器之前，指定由中继代理设置的 DHCP 中继代理地址）设置为 0，则 ASA 默认丢弃该数据包。现在可以保留选项 82 并通过将接口标识为受信任接口而转发数据包。

- 将所有客户端接口配置为受信任接口。

  dhcprelay information trust-all

  示例：

  ```
  ciscoasa(config)# dhcprelay information trust-all
  ```

配置 DHCPv6 中继代理

当 DHCPv6 请求进入接口时，ASA 将向所有 DHCPv6 全局服务器中继该请求。

操作步骤

步骤 1　指定客户端消息转发到的 IPv6 DHCP 服务器目标地址。

ipv6 dhcprelay server *ipv6_address* [*interface*]

示例：

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
```

ipv6-address 参数可能是接路范围的单播、组播、站点范围单播或全局 IPv6 地址。不允许将未指定、环回和本地节点组播地址用作中继目标。可选 *interface* 参数为目标指定输出接口。客户端消息通过输出接口连接的链路转发到目标地址。如果指定地址属于链路范围地址，则必须指定接口。

步骤 2　在客户端接口上启用 DHCPv6 中继服务。

ipv6 dhcprelay enable *interface*

示例：

```
ciscoasa(config)# ipv6 dhcprelay enable inside
```

步骤 3　（可选）以秒为单位指定响应通过中继地址处理中继绑定从 DHCPv6 服务器传递至 DHCPv6 客户端所允许的时间量。

ipv6 dhcprelay timeout *seconds*

示例：

```
ciscoasa(config)# ipv6 dhcprelay timeout 25
```

seconds 参数的有效值范围为 1 至 3600。默认值为 60 秒。

监控 DHCP 服务

有关如何监控 DHCP 服务，请参阅以下命令：

- **show running-config dhcpd**

  此命令显示当前 DHCP 配置。
- **show running-config dhcprelay**

  此命令显示当前 DHCP 中继服务状态。
- **show ipv6 dhcprelay binding**

  此命令显示中继代理创建的中继绑定条目。
- **show ipv6 dhcprelay statistics**

  此命令显示 IPv6 的 DHCP 中继代理统计信息。
- **clear config ipv6 dhcprelay**

  此命令清除 IPv6 DHCP 中继配置。

DHCP 服务的历史记录

表 15-2　　DHCP 服务的历史记录

功能名称	平台版本	说明
DHCP	7.0(1)	ASA 可以向连接到 ASA 接口的 DHCP 客户端提供 DHCP 服务器或 DHCP 中继服务。 我们引入了以下命令：**dhcp client update dns**、 **dhcpd address**、 **dhcpd domain**、 **dhcpd enable**、 **dhcpd lease**、 **dhcpd option**、 **dhcpd ping timeout**、 **dhcpd update dns**、 **dhcpd wins**、 **dhcp-network-scope**、 **dhcprelay enable**、 **dhcprelay server**、 **dhcprelay setroute** 和 **dhcp-server**。 **show running-config dhcpd** 和 **show running-config dhcprelay**。

表 15-2　DHCP 服务的历史记录（续）

功能名称	平台版本	说明
DHCP for IPv6 (DHCPv6)	9.0(1)	已添加对 IPv6 的支持。 我们引入了以下命令：**ipv6 dhcprelay server**、 **ipv6 dhcprelay enable**、 **ipv6 dhcprelay timeout**、 **clear config ipv6 dhcprelay**、 **ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag**、**debug ipv6 dhcp**、**debug ipv6 dhcprelay**、**show ipv6 dhcprelay binding**、**clear ipv6 dhcprelay binding**、**show ipv6 dhcprelay statistics** 和 **clear ipv6 dhcprelay statistics**。
每个接口的 DHCP 中继服务器 （仅限 IPv4）	9.1(2)	现在可以配置单个接口的 DHCP 中继服务器，因此仅将进入指定接口的请求中继给为该接口指定的服务器。 IPv6 不受单个接口 DHCP 中继之支持。 我们引入或修改了以下命令：**dhcprelay server**（接口配置模式）、**clear configure dhcprelay**、**show running-config dhcprelay**。
DHCP 受信任接口	9.1(2)	现可将接口配置为受信任接口，以保留 DHCP 选项 82。下游交换机和路由器使用 DHCP 选项 82 进行 DHCP 探听和 IP 源保护。通常，如果 ASA DHCP 中继代理接收到一个已设置选项 82 的 DHCP 数据包，但是 giaddr 字段 （在将数据包转发到服务器之前，指定由中继代理设置的 DHCP 中继代理地址）设置为 0，则 ASA 默认丢弃该数据包。现在可以保留选项 82 并通过将接口标识为受信任接口而转发数据包。 我们引入或修改了以下命令：**dhcprelay information trusted**、 **dhcprelay information trust-all**、 **show running-config dhcprelay**。
DHCP 重新绑定功能	9.1(4)	在 DHCP 重新绑定阶段，客户端尝试重新绑定到隧道组列表中的其他 DHCP 服务器。在此版本之前，当 DHCP 租约未能更新时，客户端不重新绑定到备用服务器。 我们未引入或修改任何命令。

第 5 部分

对象和 ACL

访问控制对象

对象指配置中可重用的组件。您可以在思科 ASA 配置中定义和使用对象来代替内联 IP 地址、服务、名称等。您可以使用对象轻松维护配置，因为您只需要修改某一位置的对象，便可以使该对象在引用它的所有其他位置显示出来。如未使用对象，必要时您必须逐一修改每项功能的参数，而不是一次性修改完成。例如，如果网络对象定义了 IP 地址和子网掩码，当您要更改地址时，您只需要在对象定义中进行更改，而无需在引用该 IP 地址的各项功能中逐一更改。

- 第 16-1 页的对象准则
- 第 16-2 页的配置对象
- 第 16-9 页的监控对象
- 第 16-10 页的对象的历史记录

对象准则

IPv6 准则

在以下限制条件下支持 IPv6：

- ASA 不支持 IPv6 嵌套网络对象组，因此您无法将含有 IPv6 条目的对象划分在另一个 IPv6 对象组下。
- 您可以将 IPv4 和 IPv6 条目混合在同一网络对象组中；但您无法使用混合对象组进行 NAT。

附加准则和限制

- 由于对象和对象组共享同一命名空间，因此对象名称必须唯一。当您可能要创建名为“Engineering”的网络对象组以及名为“Engineering”的服务对象组时，您需要在至少其中一个对象组名称的末尾添加一个标识符（或“标记”），使其名称唯一。例如，可以使用名称“Engineering_admins”和“Engineering_hosts”，使对象组名称保持唯一，同时有助于进行识别。
- 对象名称限于 64 个字符，包括字母、数字和如下字符：.!@#$%^&()-_{}。对象名称区分大小写。
- 如果在命令中使用对象，您无法将对象移除或留空，除非启用 前向引用（**forward-reference enable** 命令）。

配置对象

以下各节介绍了如何配置主要用于访问控制的对象。

- 第 16-2 页的配置网络对象和组
- 第 16-4 页的配置服务对象和服务组
- 第 16-6 页的配置本地用户组
- 第 16-7 页的配置安全组对象组
- 第 16-8 页的配置时间范围

配置网络对象和组

网络对象和组可以识别 IP 地址或主机名。您可以使用访问控制列表中的这些对象来简化规则。

- 第 16-2 页的配置网络对象
- 第 16-3 页的配置网络对象组

配置网络对象

网络对象可以包含主机、网络 IP 地址、 IP 地址范围或完全限定域名 (FQDN)。

您也可以启用对象的 NAT 规则 （FQDN 对象除外）。有关配置对象 NAT 的详细信息，请参阅防火墙配置指南。

操作步骤

步骤 1 使用对象名称创建或编辑网络对象。

```
ciscoasa(config)# object network object_name
```

示例

```
ciscoasa(config)# object network email-server
```

步骤 2 使用下列命令之一将地址添加到对象。使用命令的 **no** 形式来移除对象。

- **host** {*IPv4_address* | *IPv6_address*} - 单台主机的 IPv4 或 IPv6 地址。例如， 10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} - 网络的地址。对于 IPv4 子网，请在空格后添加掩码，例如， 10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个单元添加 （不带空格），例如 2001:DB8:0:CD30::/60。
- **range** *start_address end_address* - 地址的范围。您可以指定 IPv4 或 IPv6 范围。请勿添加掩码和前缀。
- **fqdn** [**v4** | **v6**] *fully_qualified_domain_name* - 完全限定域名，即主机的名称，例如 www.example.com。指定 **v4** 将地址限定于 IPv4，**v6** 将地址限定于 IPv6。如果未指定地址类型，则假定为 IPv4。

示例

```
ciscoasa(config-network-object)# host 10.2.2.2
```

步骤 3 （可选）添加说明。

```
ciscoasa(config-network-object)# description string
```

配置网络对象组

网络对象组可以包含多个网络对象以及内联网络或主机。网络对象组可以同时包含 IPv4 和 IPv6 地址。

但是，你无法使用包含 IPv4 和 IPv6 的混合对象组进行 NAT，也无法使用包含 FQDN 对象的对象组。

操作步骤

步骤 1 使用对象名称创建或编辑网络对象组。

```
ciscoasa(config)# object-group network group_name
```

示例

```
ciscoasa(config)# object-group network admin
```

步骤 2 使用以下一个或多个命令将对象和地址添加到网络对象组。使用命令的 **no** 形式来移除对象。

- **network-object host** {*IPv4_address* | *IPv6_address*} - 单台主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **network-object** {*IPv4_address IPv4_mask* | *IPv6_address*/*IPv6_prefix*} - 网络或主机的地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个单元添加（不带空格），例如 2001:DB8:0:CD30::/60。
- **network-object object** *object_name* - 现有网络对象的名称。
- **group-object** *object_group_name* - 现有网络对象组的名称。

示例

```
ciscoasa(config-network-object-group)# network-object 10.1.1.0 255.255.255.0
ciscoasa(config-network-object-group)# network-object 2001:db8:0:cd30::/60
ciscoasa(config-network-object-group)# network-object host 10.1.1.1
ciscoasa(config-network-object-group)# network-object host 2001:DB8::0DB8:800:200C:417A
ciscoasa(config-network-object-group)# network-object object existing-object-1
ciscoasa(config-network-object-group)# group-object existing-network-object-group
```

步骤 3 （可选）添加说明。

```
ciscoasa(config-network-object-group)# description string
```

示例

如要创建包含三个管理员 IP 地址的网络组，请输入以下命令：

```
hostname (config)# object-group network admins
hostname (config-protocol)# description Administrator Addresses
hostname (config-protocol)# network-object host 10.2.2.4
hostname (config-protocol)# network-object host 10.2.2.78
hostname (config-protocol)# network-object host 10.2.2.34
```

输入下列命令，为来自各部门的特权用户创建网络对象组：

```
hostname (config)# object-group network eng
hostname (config-network)# network-object host 10.1.1.5
hostname (config-network)# network-object host 10.1.1.9
hostname (config-network)# network-object host 10.1.1.89

hostname (config)# object-group network hr
hostname (config-network)# network-object host 10.1.2.8
hostname (config-network)# network-object host 10.1.2.12

hostname (config)# object-group network finance
hostname (config-network)# network-object host 10.1.4.89
hostname (config-network)# network-object host 10.1.4.100
```

然后按下述方法对所有三个组进行嵌套：

```
hostname (config)# object-group network admin
hostname (config-network)# group-object eng
hostname (config-network)# group-object hr
hostname (config-network)# group-object finance
```

配置服务对象和服务组

服务对象和组可标识协议和端口。您可以使用访问控制列表中的这些对象来简化规则。

- 第 16-4 页的配置服务对象
- 第 16-5 页的配置服务组

配置服务对象

服务对象可包含单一协议、 ICMP、 ICMPv6、 TCP 或 UDP 端口或端口范围。

操作步骤

步骤 1 使用对象名称创建或编辑服务对象。

```
ciscoasa(config)# object service object_name
```

示例

```
ciscoasa(config)# object service web
```

步骤 2 使用下列命令之一将服务添加到对象。使用命令的 **no** 形式来移除对象。

- **service** *protocol* - IP 协议的名称或编号 (0 - 255)。指定 **ip** 将应用于所有协议。有关受支持关键字的列表，请参阅第 43-9 页的协议和应用。
- **service** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]] - 适用于 ICMP 或 ICMP 第 6 版消息。或者，您可以按名称或编号 (0 - 255) 指定 ICMP 类型，以便将对象限于该消息类型。如果指定类型，则可以选择为该类型指定一个 ICMP 代码 (1-255)。如果不指定代码，则将使用所有代码。有关 ICMP 类型的列表，请参阅第 43-14 页的 ICMP 类型。
- **service** {**tcp** | **udp**} [**source** *operator port*] [**destination** *operator port*] - 适用于 TCP或 UDP。或者，您可以指定源端口、目标端口或两者。可以按名称或编号指定端口 （有关列表，请参阅第 43-10 页的 TCP 和 UDP 端口）。操作符可以是以下任意一项：
  - **lt** - 小于。
  - **gt** - 大于。

- **eq** - 等于。
- **neq** - 不等于。
- **range** - 值的包含范围。使用该操作符时，请指定两个端口编号，例如，**range 100 200**。

示例

```
ciscoasa(config-service-object)# service tcp destination eq http
```

步骤 3 （可选）添加说明。

```
ciscoasa(config-service-object)# description string
```

配置服务组

服务对象组可以包括协议组合，必要时包括适用于 TCP 或 UDP 的可选源端口和目标端口。

准备工作

您可以使用通用服务对象组来建立所有服务的模型（如本节所介绍）。不过，您仍然可以配置 ASA 8.3(1) 版本之前可用的服务组对象的类型。上述旧版对象包括 TCP/UDP/TCP-UDP 端口组、协议组和 ICMP 组。这些组的内容与通用服务对象组中的关联配置等效，ICMP 组除外，因为这些组不支持 ICMP6 和 ICMP 代码。如果您仍要使用这些旧版对象，请参阅 Cisco.com 网站上命令参考中的 **object-service** 命令说明以了解详细说明。

操作步骤

步骤 1 使用对象名称创建或编辑服务对象组。

```
ciscoasa(config)# object-group service group_name
```

示例

```
ciscoasa(config)# object-group service general-services
```

步骤 2 使用以下一个或多个命令将对象和服务添加到服务对象组。使用命令的 **no** 形式来移除对象。

- **service-object** *protocol* - IP 协议的名称或编号 (0 - 255)。指定 **ip** 将应用于所有协议。有关受支持关键字的列表，请参阅第 43-9 页的协议和应用。
- **service-object** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]] - 适用于 ICMP 或 ICMP 第 6 版消息。或者，您可以按名称或编号 (0 - 255) 指定 ICMP 类型，以便将对象限于该消息类型。如果指定类型，则可以选择为该类型指定一个 ICMP 代码 (1-255)。如果不指定代码，则将使用所有代码。有关 ICMP 类型的列表，请参阅第 43-14 页的 ICMP 类型。
- **service-object** {**tcp** | **udp** | **tcp-udp**} [**source** *operator port*] [**destination** *operator port*] - 适用于 TCP、 UDP 或两者。或者，您可以指定源端口、目标端口或两者。可以按名称或编号指定端口（有关列表，请参阅第 43-10 页的 TCP 和 UDP 端口）。操作符可以是以下任意一项：
  - **lt** - 小于。
  - **gt** - 大于。
  - **eq** - 等于。
  - **neq** - 不等于。
  - **range** - 值的包含范围。使用该操作符时，请指定两个端口编号，例如，**range 100 200**。
- **service-object object** *object_name* - 现有服务对象的名称。
- **group-object** *object_group_name* - 现有服务对象组的名称。

示例

```
ciscoasa(config-service-object-group)# service-object ipsec
ciscoasa(config-service-object-group)# service-object tcp destination eq domain
ciscoasa(config-service-object-group)# service-object icmp echo
ciscoasa(config-service-object-group)# service-object object my-service
ciscoasa(config-service-object-group)# group-object Engineering_groups
```

步骤 3 （可选）添加说明。

```
ciscoasa(config-service-object-group)# description string
```

示例

以下示例显示了如何同时将 TCP 和 UDP 服务添加到服务对象组：

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

以下示例显示了如何将多个服务对象添加到服务对象组：

```
ciscoasa(config)# object service SSH
ciscoasa(config-service-object)# service tcp destination eq ssh
ciscoasa(config)# object service EIGRP
ciscoasa(config-service-object)# service eigrp
ciscoasa(config)# object service HTTPS
ciscoasa(config-service-object)# service tcp source range 1 1024 destination eq https
ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# service-object object SSH
ciscoasa(config-service-object-group)# service-object object EIGRP
ciscoasa(config-service-object-group)# service-object object HTTPS
```

配置本地用户组

您可以创建本地用户组，通过将组列入扩展 ACL 中，在支持身份防火墙的功能中使用本地用户组，进而用于访问规则等。

ASA 为 Active Directory 域控制器中全局定义的用户组将 LDAP 查询发送到 Active Directory 服务器。ASA 会导入这些组，将其用于基于身份的规则。但是，ASA 可能已将未全局定义的网络资源本地化，这些网络资源需要具有本地化安全策略的本地用户组。本地用户组可包含嵌套组和从 Active Directory 导入的用户组。ASA 可整合本地和 Active Directory 组。

用户可以属于本地用户组和从 Active Directory 导入的用户组。

由于您能够在 ACL 中直接使用用户名和用户组，因此只有在以下情况下您才需配置本地用户组：

- 如要创建 LOCAL 数据库中定义的一组用户。
- 如要创建在 AD 服务器定义的单一用户组中未捕获的一组用户或用户组。

有关如何启用身份防火墙的详细信息，请参阅第 31 章，“身份防火墙”。

操作步骤

步骤 1 使用对象名称创建或编辑用户对象组。

```
ciscoasa(config)# object-group user group_name
```

示例

```
ciscoasa(config)# object-group user admins
```

步骤 2 使用以下一个或多个命令将用户和组添加到用户对象组。使用命令的 **no** 形式来移除对象。

- **user** [*domain_NETBIOS_name*\]*username* - 用户名。如果域名或用户名中有空格，您必须用引号将域名和用户引起来。域名可以是 LOCAL（适用于本地数据库中定义的用户）或如 **user-identity domain** *domain_NetBIOS_name* **aaa-server** *aaa_server_group_tag* 命令中所指定的 Active Directory (AD) 域名。添加 AD 域中定义的用户时，*user_name* 必须是 Active Directory sAMAccountName（唯一），而非公用名 (cn)（可能不唯一）。如果您未指定域名，则使用默认域名，即 LOCAL 或 **user-identity default-domain** 命令中定义的域名。
- **user-group** [*domain_NETBIOS_name*\\]*username* - 用户组。如果域名或组名中有空格，您必须用引号将域名和组引起来。请注意分隔域名和组名的双斜号 \\。
- **group-object** *object_group_name* - 现有用户对象组的名称。

示例

```
ciscoasa(config-user-object-group)# user EXAMPLE\admin
ciscoasa(config-user-object-group)# user-group EXAMPLE\\managers
ciscoasa(config-user-object-group)# group-object local-admins
```

步骤 3 （可选）添加说明。

```
ciscoasa(config-user-object-group)# description string
```

配置安全组对象组

您可以创建安全组对象组，通过将组列入扩展 ACL 中，在支持 思科 TrustSec 的功能中使用安全组对象组，进而用于访问规则等。

与思科 TrustSec 集成后，ASA 可以从 ISE 下载安全组信息。ISE 可以提供思科 TrustSec 标记到用户的身份映射以及思科 TrustSec 标记到服务器的资源映射，从而充当身份储存库。您可以在 ISE 上集中部署和管理安全组 ACL。

但是， ASA 可能已将未全局定义的网络资源本地化，这些网络资源需要具有本地化安全策略的本地安全组。本地安全组可以包含从 ISE 下载的嵌套安全组。 ASA 可以整合本地和中央安全组。

如要在 ASA 上创建本地安全组，请创建一个本地安全对象组。本地安全对象组可以包含一个或多个嵌套安全对象组、安全 ID 或安全组名称。您还可以创建 ASA 中不存在的 新安全 ID 或安全组名称。

您可以使用在 ASA 中创建的安全对象组来控制对网络资源的访问。您可以将安全对象组作为访问组或服务策略的一部分。

有关如何集成 ASA 和 Trustsec 的详细信息，请参阅第 32 章，“ASA 和思科 TrustSec”。

提示 如果使用 ASA 未知的标记和名称来创建组，则使用该组的任何规则都将处于非活动状态，直到您使用 ISE 对标记或名称解析成功为止。

操作步骤

步骤 1 使用对象名称来创建或编辑安全组对象组。

```
ciscoasa(config)# object-group security group_name
```

示例

```
ciscoasa(config)# object-group security mktg-sg
```

步骤 2 使用以下一个或多个命令将对象添加到服务组对象组。使用命令的 **no** 形式来移除对象。

- **security-group** {**tag** *sgt_number* | **name** *sg_name*} - 安全组标记 (SGT) 或名称。标记为一个介于 1 和 65533 之间的数字，由 ISE 通过 IEEE 802.1X 身份验证、网络身份验证或 MAC 身份验证旁路 (MAB) 分配给设备。安全组名称在 ISE 上创建，为安全组提供用户友好的名称。此安全组表将 SGT 映射到安全组名称。有关有效标记和名称，请查阅 ISE 配置。
- **group-object** *object_group_name* - 现有安全组对象组的名称。

示例

```
ciscoasa(config-security-object-group)# security-group tag 1
ciscoasa(config-security-object-group)# security-group name mgkt
ciscoasa(config-security-object-group)# group-object local-sg
```

步骤 3 （可选）添加说明。

```
ciscoasa(config-security-object-group)# description string
```

配置时间范围

时间范围对象定义了由起始时间、结束时间和可选循环条目组成的特定时间。您可以将这些对象用于 ACL 规则，从而提供对特定功能或资产基于时间的访问。例如，您可以创建一条仅允许在工作时间对特定服务器进行访问的访问规则。

注 您可以在时间范围对象中列入多个定期条目。如果时间范围规定了绝对值和周期值，则只有在达到绝对起始时间后才开始评估周期值，而且在绝对结束时间到达后便不再对其进行评估。

创建时间范围并不会限制对设备的访问。该操作步骤仅定义时间范围。您随后必须在访问控制规则中使用该对象。

操作步骤

步骤 1 创建时间范围。

```
time-range name
```

步骤 2 （可选。）为时间范围添加起始或结束时间 （或两者）。

```
absolute [start time date] [end time date]
```

如果未指定起始时间，则默认当前时间为起始时间。

time 采用 24 小时格式 *(hh*:*mm*)。例如，8.00 是上午 8:00，而 20:00 是下午 8:00

date 采用 *day month year* 的格式，例如，**1 January 2014**。

步骤 3 （可选。）添加循环时间周期。

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

您可以为 *days-of-the-week* 指定以下值。请注意，只有当您为第一个参数指定了某一天时，您才可以指定一个星期中的第二天。

- **Monday**、**Tuesday**、**Wednesday**、**Thursday**、**Friday**、**Saturday** 或 **Sunday**。您可以为第一个 *days-of-the-week* 参数指定上述其中多个值 （用空格隔开）。
- **每天**
- **工作日**
- **周末**

time 采用 24 小时格式 *(hh*:*mm*)。例如，8.00 是上午 8:00，而 20:00 是下午 8:00

您可以重复该命令来配置多个循环时间段。

示例

以下是 2006 年 1 月 1 日上午 8:00 开始的绝对时间范围 的示例。由于未指定结束时间和日期，因此该时间范围无限期有效。

```
ciscoasa(config)# time-range for2006
ciscoasa(config-time-range)# absolute start 8:00 1 january 2006
```

以下是工作日从上午 8:00 到 下午 6:00 的每周定期时间范围的示例：

```
ciscoasa(config)# time-range workinghours
ciscoasa(config-time-range)# periodic weekdays 8:00 to 18:00
```

以下示例确定时间范围的结束日期，并设置从上午 8 点 到下午 5 点，以及星期一、星期三、星期五 （相比于星期二和星期四） 5 点后的不同时段的工作日周期。

```
asa4(config)# time-range contract-A-access
asa4(config-time-range)# absolute end 12:00 1 September 2025
asa4(config-time-range)# periodic weekdays 08:00 to 17:00
asa4(config-time-range)# periodic Monday Wednesday Friday 18:00 to 20:00
asa4(config-time-range)# periodic Tuesday Thursday 17:30 to 18:30
```

监控对象

如要监控对象和组，请输入以下命令：

- **show access-list**

  显示访问列表条目。包括对象的条目也会基于对象内容展开显示单独的条目。
- **show running-config object** [**id** *object_id*]

  显示所有的当前对象。使用关键字 **id** 按名称查看单个对象。
- **show running-config object** *object_type*

  按类型 （**网络**或**服务**）显示当前对象。
- **show running-config object-group** [**id** *group_id*]

  显示所有的当前对象组。使用关键字 **id** 按名称查看单个对象组。
- **show running-config object-group** *grp_type*

  按组类型显示当前对象组。

对象的历史记录

功能名称	平台版本	说明
对象组	7.0(1)	对象组可简化 ACL 的创建和维护。 我们引入或修改了以下命令：**object-group** *protocol*、**object-group** *network*、**object-group** *service* 和 **object-group** *icmp_type*。
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，将其用于检查策略映射下。引入了以下命令：**class-map type regex**、**regex** 和 **match regex**。
对象	8.3(1)	引入了对象支持功能。 我们引入或修改了以下命令：**object-network**、**object-service**、**object-group** *network*、**object-group** *service*、**network object**、**access-list extended**、**access-list webtype** 和 **access-list remark**。
用于身份防火墙的用户对象组	8.4(2)	引入了用于身份防火墙的用户对象组。 我们引入了以下命令：**object-network user** 和 **user**。
用于思科 TrustSec 的安全组对象组	8.4(2)	引入了用于思科 TrustSec 的安全组对象组 我们引入了以下命令：**object-network security** 和 **security**。
IPv4 和 IPv6 混合网络对象组	9.0(1)	之前，网络对象组只能包含全 IPv4 地址或全 IPv6 地址。现在网络对象组可以同时包含 IPv4 和 IPv6 地址。 **注** 您无法使用混合对象组进行 NAT。 我们修改了以下命令：**object-group network**。
用于按 ICMP 代码过滤 ICMP 流量的扩展 ACL 和对象增强	9.0(1)	现在您可以根据 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** 和 **service**。

访问控制列表

访问控制列表 (ACL) 在许多不同的功能中使用。作为访问规则应用到接口或全局应用时，这些列表可允许或拒绝通过设备的流量。对于其他功能，ACL 可选择功能所适用的流量，执行匹配服务而非控制服务。

以下各节介绍了 ACL 的基本信息以及如何配置和监控 ACL。在 防火墙配置指南 中详细介绍了作为访问规则全局应用或应用到接口的 ACL。

- 第 17-1 页的关于 ACL
- 第 17-4 页的 ACL 准则
- 第 17-5 页的配置 ACL
- 第 17-16 页的监控 ACL
- 第 17-17 页的 ACL 功能历史

关于 ACL

访问控制列表 (ACL) 通过一个或多个特征识别流量，包括源和目标 IP 地址、 IP 协议、端口、EtherType 及其他参数，视 ACL 类型而定。ACL 可用于各种功能。ACL 由一个或多个访问控制条目 (ACE) 组成。

ACL 类型

ASA 使用以下类型的 ACL：

- 扩展 ACL - 扩展 ACL 是您将使用的主要类型。这些 ACL 用于访问规则以允许和拒绝通过设备的流量，并在许多功能中用于流量匹配，包括服务策略、 AAA 规则、 WCCP、僵尸网络流量过滤器、 VPN 组和 DAP 策略。请参阅第 17-6 页的配置扩展 ACL。
- EtherType ACL - EtherType ACL 适用于透明防火墙的第 2 层非 IP 流量。您可以使用这些规则，根据第 2 层数据包中的 EtherType 值允许或丢弃流量。通过 EtherType ACL，您可以控制设备上的非 IP 流量。请参阅第 17-15 页的配置 EtherType ACL。
- Webtype ACL - Webtype ACL 用于过滤无客户端 SSL VPN 流量。这些 ACL 可基于 URL 或目标地址拒绝访问。请参阅第 17-12 页的配置 Webtype ACL。
- 标准 ACL - 标准 ACL 只能基于目标地址识别流量。使用这种 ACL 的功能较少：路由映射和 VPN 过滤器。由于 VPN 过滤器还允许扩展访问列表，因此限制将标准 ACL 用于路由映射。请参阅第 17-12 页的配置标准 ACL。

下表列出了 ACL 的一些常见用途及使用的类型。

表 17-1　ACL 类型和常见用途

ACL 用途	ACL 类型	说明
控制 IP 流量的网络访问 （路由和透明模式）	扩展	ASA 不允许任何从低安全性接口到高安全性接口的流量，除非扩展 ACL 明确允许。 **注**　如要访问 ASA 接口以进行管理访问，您无需 ACL 允许主机 IP 地址。您只需要根据第 35 章，“管理访问”配置管理访问。
识别 AAA 规则的流量	扩展	AAA 规则使用 ACL 识别流量。
为给定用户增强 IP 流量的网络访问控制	扩展，按用户从 AAA 服务器下载	您可以配置 RADIUS 服务器以下载要应用于用户的动态 ACL，或服务器可以发送您已在 ASA 上配置的 ACL 名称。
VPN 访问和过滤	扩展 标准	用于远程访问和站点到站点 VPN 的组策略使用标准或扩展 ACL 进行过滤。远程访问 VPN 还将扩展 ACL 用于客户端防火墙配置和动态访问策略。
为模块化策略框架识别流量类映射中的流量	扩展	ACL 可用于识别类映射中的流量，该用途用于支持模块化策略框架的功能。支持模块化策略框架的功能包括 TCP 和常规连接设置，以及检查。
对于透明防火墙模式，控制非 IP 流量的网络访问	EtherType	您可以配置一个基于其 EtherType 来控制流量的 ACL。
识别路由过滤和重分布	标准 扩展	各种路由协议将标准 ACL 用于 IPv4 地址 （扩展 ACL 用于 IPv6 地址）的路由过滤和重分布 （通过路由映射）。
无客户端 SSL VPN 过滤	Webtype	您可以配置 Webtype ACL 以过滤 URL 和目标。

ACL 名称

每个 ACL 都有一个名称或数字 ID，如 outside_in、OUTSIDE_IN 或 101。名称限于不超过 241 个字符。请考虑全部使用大写字母，以便在查看运行配置时时更方便地查找名称。

制定一个可帮助您识别 ACL 的预期用途的命名约定。例如，ASDM 使用约定 *interface-name_purpose_direction*，例如，outside_access_in，用于在入站方向应用于“外部”接口的 ACL。

一般来说，ACL ID 为数字。标准 ACL 的范围为 1 - 99 或 1300 - 1999。扩展 ACL 的范围为 100 - 199 或 2000 - 2699。 ASA 不强制执行这些范围，但如果您要使用编号，可能要遵守这些约定以便与运行 IOS 软件的路由器保持一致。

访问控制条目顺序

ACL 由一个或多个 ACE 组成。除非您明确将 ACE 插入给定行，否则您为给定 ACL 名称输入的每个 ACE 都将附加到 ACL 的末尾。

ACE 的顺序非常重要。当 ASA 决定是转发还是丢弃数据包时，ASA 会按照条目所列顺序对每个 ACE 测试数据包。找到匹配项后，不会再检查 ACE。

因此，如果将一条更具体的规则放在一条更通用的规则之后，则该更具体的规则可能永远不会被命中。例如，如果要允许网络 10.1.1.0/24，但要丢弃该子网上来自主机 10.1.1.15 的流量，则拒绝 10.1.1.15 的 ACE 必须排在允许 10.1.1.0/24 的 ACE 之前。如果允许 10.1.1.0/24 的 ACE 排在前面，则将允许 10.1.1.15，并且用以拒绝的 ACE 将永远不会被匹配。

在扩展 ACL 中，使用 **access-list** 命令上的 **line** *number* 参数将规则插入正确位置。使用 **show access-list** *name* 命令查看 ACL 条目及其行号以帮助确定要使用的行号。对于其他类型的 ACL，您必须重新创建 ACL（或最好使用 ASDM）以更改 ACE 的顺序。

允许/拒绝与 匹配/不匹配

访问控制条目“允许”或“拒绝”与规则匹配的流量。将 ACL 应用到确定是允许流量通过 ASA 还是丢弃流量的功能时，例如全局和接口访问规则，“允许”和“拒绝”即表示实际的允许和拒绝。

对于其他功能，例如服务策略规则，“允许”和“拒绝”实际上表示“匹配”或“不匹配”。在这些情况下， ACL 选择的是应接收该功能服务的流量，例如，应用检查或重定向到服务模块。“被拒绝”流量即不匹配 ACL 的流量，因而将不会接收该服务。

访问控制隐式拒绝

所有 ACL 的末尾都有一条隐式拒绝语句。因此，对于那些应用于接口的流量控制 ACL，如果未明确允许某个类型的流量，则该流量将被丢弃。例如，如果您要允许所有用户通过 ASA 访问网络，某个或多个特定地址除外，则需要拒绝那些特定地址并允许其他地址。

对于用于为某项服务选择流量的 ACL，您必须明确“允许”流量；对于该服务，任何未被“允许的”流量都将不会被匹配接受服务；“被拒绝”流量将绕过该服务。

对于 EtherType ACL，ACL 末尾的隐式拒绝不会影响 IP 流量或 ARP；例如，如果您允许 EtherType 8037，则 ACL 末尾的隐式拒绝语句不会立即阻止之前使用扩展 ACL 允许的任何 IP 流量（或隐性允许从高安全性接口到低安全性接口的流量）。但是，如果您通过 EtherType ACE *明确*拒绝所有流量，则 IP 和 ARP 流量将被拒绝；仅仍然允许物理协议流量，如自动协商。

使用 NAT 时用于扩展 ACL 的 IP 地址

使用 NAT 或 PAT 时，您将转换地址或端口，通常是在内部和外部地址之间进行映射。如果您需要创建适用于已转换的地址或端口的扩展 ACL，则需要确定是要使用实际 （未转换）地址或端口，还是要使用已映射地址或端口。具体要求因功能而异。

使用实际地址和端口意味着如果 NAT 配置发生更改，您无需更改 ACL。

使用实际 IP 地址的功能

以下命令和功能可以在 ACL 中使用实际 IP 地址，即使接口上所示的地址是映射地址：

- 访问规则 （由 **access-group** 命令引用的扩展 ACL）
- 服务策略规则 （模块化策略框架 **match access-list** 命令）
- 僵尸网络流量过滤器流量分类 （**dynamic-filter enable classify-list** 命令）
- AAA 规则 （**aaa ... match** 命令）
- WCCP（**wccp redirect-list group-list** 命令）

例如，如果您为内部服务器 10.1.1.5 配置了 NAT，以便其在外部 209.165.201.5 上具有公开可路由的 IP 地址，则允许外部流量访问内部服务器的访问规则需要引用服务器的实际 IP 地址 (10.1.1.5)，而不是映射地址 (209.165.201.5)。

```
ciscoasa(config)# object network server1
ciscoasa(config-network-object)# host 10.1.1.5
ciscoasa(config-network-object)# nat (inside,outside) static 209.165.201.5

ciscoasa(config)# access-list OUTSIDE extended permit tcp any host 10.1.1.5 eq www
ciscoasa(config)# access-group OUTSIDE in interface outside
```

使用映射 IP 地址的功能

以下功能使用 ACL，但这些 ACL 使用接口上所示的映射值：

- IPsec ACL
- **capture** 命令 ACL
- 每用户 ACL
- 路由协议 ACL
- 所有其他功能 ACL

基于时间的 ACE

您可以将时间范围对象应用到扩展 ACE 和 Webtype ACE，以便规则仅在特定时期内处于活动状态。通过这些类型的规则，您可以区分在一天中某些时间点可接受但在其他时间点不可接受的活动。例如，您可以在工作时间内提供附加限制，而在下班后或在午餐时间则不限制。相反，您基本上可以在非工作时间关闭网络。有关创建时间范围对象的详细信息，请参阅第 16-8 页的配置时间范围。

注 用户可能会在指定结束时间后遇到约 80 至 100 秒的延迟，以使 ACL 处于非活动状态。例如，如果指定的结束时间是 3:50，因为结束时间包含在内，因此将在 3:51:00 与 3:51:59 之间的任何时间点选取命令。选取命令后，ASA 将完成所有当前运行的任务，然后执行命令以停用 ACL 服务。

ACL 准则

防火墙模式准则

扩展 ACL 和标准 ACL 均支持路由和透明防火墙模式。

Webtype ACL 仅支持路由模式。

EtherType ACL 仅支持透明模式。

IPv6 准则

扩展 ACL 和 Webtype ACL 允许 IPv4 和 IPv6 地址混合使用。

标准 ACL 不允许 IPv6 地址。

EtherType ACL 不包含 IP 地址。

（仅限扩展 ACL。）不支持身份防火墙、 FQDN 和思科 TrustSec ACL 的功能

以下功能使用 ACL，但无法接受带身份防火墙（指定用户或组名称）、FQDN（完全限定域名），或思科 TrustSec 值的 ACL：

- **route-map** 命令
- VPN **crypto map** 命令

- VPN **group-policy** 命令，**vpn-filter** 除外
- WCCP
- DAP

附加准则和限制

- 指定网络掩码的方法与思科 IOS 软件 **access-list** 命令不同。ASA 使用网络掩码（例如，255.255.255.0 用于 C 类掩码）。思科 IOS 掩码使用通配位（例如，0.0.0.255）。

配置 ACL

以下各节介绍了如何配置各种类型的 ACL。请阅读有关 ACL 基本信息的章节以了解总体情况，然后阅读有关特定类型 ACL 的章节了解详细信息。

- 第 17-5 页的基本 ACL 配置和管理选项
- 第 17-6 页的配置扩展 ACL
- 第 17-12 页的配置标准 ACL
- 第 17-12 页的配置 Webtype ACL
- 第 17-15 页的配置 EtherType ACL

基本 ACL 配置和管理选项

ACL 由一个或多个具有相同 ACL ID 或名称的访问控制条目 (ACE) 组成。如要创建新的 ACL，您只需使用新的 ACL 名称创建 ACE 即可，它将成为新 ACL 中的第一条规则。

使用 ACL 时，您可进行下列操作：

- **检查 ACL 内容并确定行号和命中次数** - 使用 **show access-list** *name* 命令查看 ACL 的内容。每一行是一个 ACE，并且包括行号，如果您想将新条目插入扩展 ACL 中，则需要了解这些信息。信息还包括每个 ACE 的命中次数，即为流量匹配规则的次数。例如：

```
ciscoasa# show access-list outside_access_in
access-list outside_access_in; 3 elements; name hash: 0x6892a938
access-list outside_access_in line 1 extended permit ip 10.2.2.0 255.255.255.0 any
(hitcnt=0) 0xcc48b55c
access-list outside_access_in line 2 extended permit ip host
2001:DB8::0DB8:800:200C:417A any (hitcnt=0) 0x79797f94
access-list outside_access_in line 3 extended permit ip user-group LOCAL\\usergroup
any any (hitcnt=0) 0xb0f5b1e1
```

- **添加 ACE** - 用于添加 ACE 的命令是 **access-list** *name* [**line** *line-num*] *type parameters*。行号参数仅适用于扩展 ACL。如果在命令中包含行号，ACE 将插入 ACL 中的该位置，而且该位置的 ACE 及剩余 ACE 将向下移动（即，在行号处插入 ACE 不会取代该行上的旧 ACE）。如果不包含行号，ACE 将被添加到 ACL 末尾。可用参数因 ACL 类型而异；请参阅每个 ACL 类型的特定主题以了解详细信息。
- **将注释添加到 ACL（所有类型，Webtype 除外）** - 使用 **access-list** *name* [**line** *line-num*] **remark** *text* 命令将备注添加到 ACL，以便帮助说明 ACE 的用途。最好是在 ACE 之前插入备注；如果您在 ASDM 中查看配置，备注将与备注后面的ACE 关联。您可以在 ACE 之前输入多个备注以包含一个扩展注释。每条备注限制在 100 个字符以内。您可以包含前导空格以帮助引出备注。如果不包含行号，备注将被添加到 ACL 末尾。例如，您可以在添加每个 ACE 之前添加备注：

```
ciscoasa(config)# access-list OUT remark - this is the inside admin address
ciscoasa(config)# access-list OUT extended permit ip host 209.168.200.3 any
```

```
ciscoasa(config)# access-list OUT remark - this is the hr admin address
ciscoasa(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

- **编辑或移动 ACE 或备注** - 您无法编辑或移动 ACE 或备注。相反，您必须使用所需的值在正确位置创建新的 ACE 或备注（使用行号），然后删除旧的 ACE 或备注。由于您只能将 ACE 插入扩展 ACL，如果需要编辑或移动 ACE，则需要重新建立标准 ACL、 Webtype ACL 或 EtherType ACL。使用 ASDM 能更容易地重新组织较长的 ACL。
- **删除 ACE 或备注** - 使用 **no access-list** *parameters* 命令移除 ACE 或备注。使用 **show access-list** 命令查看您必须输入的参数字符串: 字符串必须完全匹配 ACE 或备注才能将其删除，**line** *line-num* 参数除外，该参数对于 **no access-list** 命令为可选参数。
- **删除整个 ACL，包括备注** - 使用 **clear configure access-list** *name* 命令。务必要谨慎使用该命令！命令不会要求您进行确认。如果不包含名称，则 ASA 上的每个访问列表都将被移除。
- **重命名 ACL** - 使用 **access-list** *name* **rename** *new_name* 命令。
- **将 ACL 应用到策略** - 在其内部创建或创建自己的 ACL 对流量毫无用处。您必须将 ACL 应用到策略。例如，您可以使用 **access-group** 命令将扩展 ACL 应用到接口，从而拒绝或允许通过接口的流量。有关 ACL 某些用途的详细信息，请参阅第 17-1 页的 ACL 类型。

配置扩展 ACL

扩展 ACL 由具有相同 ACL ID 或名称的所有 ACE 组成。扩展 ACL 是最复杂且功能丰富的一类 ACL，可以用于许多功能。扩展 ACL 最显著用途是作为访问组被全局应用或应用到接口，以确定将被拒绝或允许通过设备的流量。但是，扩展 ACL 还可用于确定要向其提供其他服务的流量。

由于扩展 ACL 非常复杂，以下各节集中描述了创建 ACE 以提供特定类型的流量匹配。前几节介绍了关于基于地址的基本 ACE 以及 TCP/UDP ACE 的基本信息，给剩余各节提供了基础。

- 第 17-6 页的添加扩展 ACE 以进行基于 IP 地址或完全限定域名的匹配
- 第 17-8 页的添加扩展 ACE 以进行基于 TCP 或 UDP 的匹配 （含端口）
- 第 17-8 页的添加扩展 ACE 以进行基于 ICMP 的匹配
- 第 17-9 页的添加扩展 ACE 以进行基于用户的匹配 （身份防火墙）
- 第 17-10 页的添加扩展 ACE 以进行基于安全组的匹配(思科 TrustSec)
- 第 17-10 页的扩展 ACL 的示例
- 第 17-11 页的示例 （为扩展 ACL 将地址转换为对象）

添加扩展 ACE 以进行基于 IP 地址或完全限定域名的匹配

基本的扩展 ACE 基于源地址和目标地址 （包括 IPv4 和 IPv6 地址及完全限定域名 (FQDN)，如 www.example.com）来匹配流量。事实上，每种类型的扩展 ACE 都必须包含源地址和目标地址的一些规格，因此，本主题介绍了最基本的扩展 ACE。

提示　如果要基于 FQDN 匹配流量，则必须为每个 FQDN 创建一个网络对象。

如要添加 ACE 以进行 IP 地址或 FQDN 匹配，请使用以下命令：

```
access-list access_list_name [line line_number] extended {deny | permit}
protocol_argument source_address_argument dest_address_argument
[log [[level] [interval secs] | disable | default]]
[time-range time_range_name]
[inactive]
```

示例：

```
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

选项如下：

- *access_list_name* - 新的或现有 ACL 的名称。
- Line number - **line** *line_number* 选项指定插入 ACE 的行号，否则，ACE 将添加到 ACL 末尾。
- Permit or Deny - 关键字 **deny** 在条件匹配的情况下拒绝或免除数据包。关键字 **permit** 在条件匹配的情况下允许或包含数据包。
- Protocol - *protocol_argument* 指定 IP 协议：
  - *name* 或 *number* - 指定协议名称或编号。指定 **ip** 将应用于所有协议。有关受支持关键字的列表，请参阅第 43-9 页的协议和应用。
  - **object-group** *protocol_grp_id* - 指定使用 **object-group protocol** 命令创建的协议对象组。请参阅第 16-4 页的配置服务对象和服务组。
  - **object** *service_obj_id* - 指定使用 **object service** 命令创建的服务对象。TCP、UDP 或 ICMP 服务对象可以包含一个协议以及一个源或目标端口或 ICMP 类型和代码。
  - **object-group** *service_grp_id* - 指定使用 **object-group service** 命令创建的服务对象组。
- Source Address, Destination Address - *source_address_argument* 指定将从其发送数据包的 IP 地址或 FQDN，*dest_address_argument* 指定将向其发送数据包的 IP 地址或 FQDN：
  - **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，例如 10.100.10.0 255.255.255.0。
  - *ipv6-address/prefix-length* - 指定 IPv6 主机或网络地址和前缀。
  - **any**、**any4** 和 **any6** - **any** 同时指定 IPv4 和 IPv6 流量；**any4** 仅指定 IPv4 流量；**any6** 仅指定 IPv6 流量。
  - **interface** *interface_name* - 指定 ASA 接口的名称。使用接口名称 （而非 IP 地址）基于哪个接口是流量的源或目标来匹配流量。
  - **object** *nw_obj_id* - 指定使用 **object network** 命令创建的网络对象。请参阅第 16-2 页的配置网络对象和组。
  - **object-group** *nw_grp_id* - 指定使用 **object-group network** 命令创建的网络对象组。
- Logging - **log** 参数为网络访问设置当 ACE 匹配数据包时的记录选项（使用 **access-group** 命令应用的 ACL）。如果您未在 **log** 选项中输入任何参数，则将以默认间隔 （300 秒）启用默认级别 (6) 的系统日志消息 106100。日志选项包括：
  - *level* - 介于 0 与 7 之间的严重性级别。默认值为 6（仅供参考）。如果您为某个活动 ACE 更改此级别，则新级别将应用到新连接；现有连接将继续以之前的级别进行记录。
  - **interval** *secs* - 系统日志消息之间的时间间隔（以秒为单位），范围为 1 至 600。默认值为 300。此值还被用作从收集丢弃统计信息的缓存删除非活动流的超时值。
  - **disable** - 禁用所有 ACE 记录。
  - **default** - 为被拒绝的数据包启用消息 106023 记录。此设置与不包含 **log** 选项的作用相同。
- Time Range - **time-range** *time_range_name* 选项指定时间范围对象，可以确定 ACE 在一天中某些时间或一周中某些天处于活动状态。如果不包含时间范围，规则将始终处于活动状态。
- Activation - 使用 **inactive** 选项以在不删除 ACE 的情况下禁用 ACE。如要重新启用 ACE，请输入完整的 ACE，无需含 inactive 关键字。

添加扩展 ACE 以进行基于 TCP 或 UDP 的匹配 （含端口）

TCP/UDP 扩展 ACE 只是基本的地址匹配 ACE，其中协议为 **tcp** 或 **udp**。由于这些协议使用端口，您可以将端口规格添加到 ACE。例如，您可以将 TCP 端口 80 上的 HTTP 流量作为目标。

要添加 ACE 以进行 IP 地址或 FQDN 匹配 （其中协议为 TCP 或 UDP），请使用以下命令：

```
access-list access_list_name [line line_number] extended {deny | permit}
{tcp | udp} source_address_argument [port_argument] dest_address_argument [port_argument]
[log [[level] [interval secs] | disable | default]]
[time-range time_range_name]
[inactive]
```

示例：

```
ciscoasa(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
```

port_argument 选项指定源或目标端口。如果不指定端口，则将匹配所有端口。可用参数包括：

- *operator port* - *操作符*可以是以下任意一项：
  - **lt** - 小于
  - **gt** - 大于
  - **eq** - 等于
  - **neq** - 不等于
  - **range** - 值的包含范围。使用此运算符时，需指定两个端口号，例如：

    ```
    range 100 200
    ```

  port 可以是整数或 TCP 或 UDP 端口的名称。对于 DNS、 Discard、 Echo、 Ident、 NTP、 RPC、 SUNRPC 和 Talk，每一项都要求一个针对 TCP 的定义和一个针对 UDP 的定义。TACACS+ 要求一个针对 TCP 上端口 49 的定义。
- **object** *service_obj_id* - 指定使用 **object service** 命令创建的服务对象。请参阅第 16-4 页的配置服务对象和服务组。
- **object-group** *service_grp_id* - 指定使用 **object-group service** 命令创建的服务对象组。

有关其他关键字的说明，请参阅第 17-6 页的添加扩展 ACE 以进行基于 IP 地址或完全限定域名的匹配。

添加扩展 ACE 以进行基于 ICMP 的匹配

ICMP 扩展 ACE 只是基本的地址匹配 ACE，其中协议为 **icmp** 或 **icmp6**。由于这些协议具有类型和代码值，您可以将类型和代码规格添加到 ACE。例如，您可以将 ICMP 回应请求流量 (ping) 作为目标。

如要添加 ACE 以进行 IP 地址或 FQDN 匹配 （其中协议为 ICMP 或 ICMP6），请使用以下命令：

```
access-list access_list_name [line line_number] extended {deny | permit}
{icmp | icmp6} source_address_argument dest_address_argument [icmp_argument]
[log [[level] [interval secs] | disable | default]]
[time-range time_range_name]
[inactive]
```

示例：

```
ciscoasa(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
ciscoasa(config)# access-list abc extended permit icmp any any echo
```

icmp_argument 选项指定 ICMP 类型和代码。

- *icmp_type* [*icmp_code*] - 按名称或编号指定 ICMP 类型，以及该类型的可选 ICMP 代码。如果不指定代码，则将使用所有代码。有关 ICMP 类型的列表，请参阅第 43-14 页的 ICMP 类型。
- **object-group** *icmp_grp_id* - 为 ICMP/ICMP6 指定使用 **object-group service** 或 （弃用的） **object-group icmp** 命令创建的对象组。

有关其他关键字的说明，请参阅第 17-6 页的添加扩展 ACE 以进行基于 IP 地址或完全限定域名的匹配。

添加扩展 ACE 以进行基于用户的匹配 （身份防火墙）

基于用户的扩展 ACE 只是基本的地址匹配 ACE，您可以在源匹配条件中包含用户名或用户组。通过基于用户身份创建规则，您可以避免将规则与静态主机或网络地址相关联。例如，如果您为 user1 定义规则，且身份防火墙功能将该用户映射到某一天分配 10.100.10.3 但下一天分配 192.168.1.5 的主机，则基于用户的规则将仍然适用。

由于您仍必须提供源地址和目标地址，因此请扩展源地址以包含将分配给用户 （通常通过 DHCP） 的可能地址。例如，无论分配什么 IP 地址，用户“LOCAL\user1 any”都将匹配 LOCAL\user1 用户，而“LOCAL\user1 10.100.1.0 255.255.255.0”仅在地址处于 10.100.1.0/24 网络上时匹配该用户。

通过使用组名称，您可以基于整个类别的用户 （如学生、教师、管理人员、工程师等）定义规则。

如要添加 ACE 以进行用户或组匹配，请使用以下命令：

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument
[user_argument] source_address_argument [port_argument]
dest_address_argument [port_argument]
[log [[level] [interval secs] | disable | default]]
[time-range time_range_name]
[inactive]
```

示例：

```
ciscoasa(config)# access-list v1 extended permit ip user LOCAL\idfw
any 10.0.0.0 255.255.255.0
```

user_argument 选项指定除源地址之外还要为其匹配流量的用户或组。可用参数包括以下各项：

- **object-group-user** *user_obj_grp_id* - 指定使用 **object-group user** 命令创建的用户对象组。
- **user** {[*domain_nickname*\]*name* | **any** | **none**} - 指定用户名。指定 **any** 以匹配所有具有用户凭据的用户，或指定 **none** 以匹配未映射到用户名的地址。这些选项对于合并 **access-group** 和 **aaa authentication match** 策略尤其有用。
- **user-group** [*domain_nickname*\\]*user_group_name* - 指定用户组名称。注意分隔域名和组名称的双斜号 \\。

有关其他关键字的说明，请参阅第 17-6 页的添加扩展 ACE 以进行基于 IP 地址或完全限定域名的匹配。

提示 您可以在给定 ACE 中同时包含用户和思科 TrustSec 安全组。请参阅第 17-10 页的添加扩展 ACE 以进行基于安全组的匹配(思科 TrustSec)。

添加扩展 ACE 以进行基于安全组的匹配（思科 TrustSec）

安全组 （思科 TrustSec）扩展 ACE 只是基本的地址匹配 ACE，您可在源或目标匹配条件中包含安全组或标记。通过基于安全组创建规则，您可以避免将规则与静态主机或网络地址相关联。由于您仍必须提供源地址和目标地址，因此请扩展地址以包含将分配给用户 （通常通过 DHCP）的可能地址。

提示　在添加此类型的 ACE 之前，请按 第 32 章，“ASA 和思科 TrustSec” 中所述配置思科 TrustSec。

如要添加 ACE 以进行安全组匹配，请使用以下命令：

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument
[security_group_argument] source_address_argument [port_argument]
[security_group_argument] dest_address_argument [port_argument] [log [[level]
[interval secs] | disable | default]] [inactive | time-range time_range_name]
```

示例：

```
ciscoasa(config)# access-list INSIDE_IN extended permit ip
security-group name my-group any any
```

security_group_argument 选项指定除源地址或目标地址之外还要为其匹配流量的安全组。可用参数包括以下各项：

- **object-group-security** *security_obj_grp_id* - 指定使用 **object-group security** 命令创建的安全对象组。
- **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*} - 指定安全组名称或标记。

有关其他关键字的说明，请参阅第 17-6 页的添加扩展 ACE 以进行基于 IP 地址或完全限定域名的匹配。

提示　您可以在给定 ACE 中同时包含用户和思科 TrustSec 安全组。请参阅第 17-9 页的添加扩展 ACE 以进行基于用户的匹配 （身份防火墙）。

扩展 ACL 的示例

以下 ACL 允许所有主机 （位于应用 ACL 的接口上）通过 ASA：

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

以下 ACL 为基于 TCP 的流量防止 192.168.1.0/24 上的主机访问 209.165.201.0/27 网络。但允许所有其他地址。

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

如果要仅限制对特定主机的访问，则输入一个受限制的允许 ACE。默认情况下，所有其他流量都将被拒绝，除非流量被明确允许。

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

以下 ACL 限制了所有主机 （位于要向其应用 ACL 的接口）访问 209.165.201.29 地址的网站。但允许所有其他流量。

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
```

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

以下使用对象组的 ACL 限制了内部网络上的多台主机访问若干网络服务器。但允许所有其他流量。

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

以下示例临时禁用了一个 ACL，该 ACL 允许从一组网络对象 (A) 到另一组网络对象 (B) 的流量：

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

如要实施基于时间的 ACE，请使用 **time-range** 命令定义一天中或一周中的特定时间，然后使用 **access-list extended** 命令将时间范围绑定到 ACE。以下示例将“Sales”ACL 中的 ACE 绑定到名为“New_York_Minute”的时间范围。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

以下示例显示了同时包含 IPv4 和 IPv6 的 ACL：

```
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 10.2.2.0
255.255.255.0
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 2001:DB8:2::/64
hostname(config)# access-list demoacl extended permit ip host 10.3.3.3 host 10.4.4.4
```

示例（为扩展 ACL 将地址转换为对象）

以下未使用对象组的正常 ACL 限制了内部网络上的多台主机访问若干网络服务器。但允许所有其他流量。

```
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78
eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
ciscoasa(config)# access-group ACL_IN in interface inside
```

如果您建立两个网络对象组，一个用于内部主机，一个用于网络服务器，则可以简化配置并轻松地修改配置以添加更多主机：

```
ciscoasa(config)# object-group network denied
ciscoasa(config-network)# network-object host 10.1.1.4
ciscoasa(config-network)# network-object host 10.1.1.78
ciscoasa(config-network)# network-object host 10.1.1.89

ciscoasa(config-network)# object-group network web
```

```
ciscoasa(config-network)# network-object host 209.165.201.29
ciscoasa(config-network)# network-object host 209.165.201.16
ciscoasa(config-network)# network-object host 209.165.201.78

ciscoasa(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
ciscoasa(config)# access-group ACL_IN in interface inside
```

配置标准 ACL

标准 ACL 由具有相同 ACL ID 或名称的所有 ACE 组成。标准 ACL 用于有限数量的功能，如路由映射或 VPN 过滤器。标准 ACL 仅使用 IPv4 地址，并且仅定义目标地址。

如要添加标准访问列表条目，请使用以下命令：

```
ciscoasa(config)# access-list access_list_name standard {deny | permit}
{any4 | host ip_address | ip_address mask}
```

示例：

```
ciscoasa(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

选项如下：

- Name - *access_list_name* 参数可指定 ACL 的编号名称。标准 ACL 的传统编号是 1 - 99 或 1300 - 1999，但您可以使用任意名称或编号。如果 ACL 不存在，则创建新的 ACL，否则，将条目添加到 ACL 末尾。
- Permit or Deny - 关键字 **deny** 在条件匹配的情况下拒绝或免除数据包。关键字 **permit** 在条件匹配的情况下允许或包含数据包。
- Destination Address - 关键字 **any4** 匹配所有 IPv4 地址。**host** *ip_address* 参数匹配主机 IPv4 地址。*ip_address ip_mask* 参数匹配 IPv4 子网，例如，10.1.1.0 255.255.255.0。

配置 Webtype ACL

Webtype ACL 用于过滤无客户端 SSL VPN 流量，限制用户对特定网络、子网、主机和网络服务器的访问。如果不定义过滤器，将允许所有连接。 Webtype ACL 由具有相同 ACL ID 或名称的所有 ACE 组成。

通过 Webtype ACL，您可以基于 URL 或目标地址来匹配流量。单个 ACE 不能混用这些规格。以下各节介绍了每种类型的 ACE。

- 第 17-12 页的添加 Webtype ACE 以进行 URL 匹配
- 第 17-14 页的添加 Webtype ACE 以进行 IP 地址匹配
- 第 17-14 页的 Webtype ACL 的示例

添加 Webtype ACE 以进行 URL 匹配

如要基于用户正尝试访问的 URL 匹配流量，请使用以下命令：

```
access-list access_list_name webtype {deny | permit} url {url_string | any}
[log [[level] [interval secs] | disable | default]]
[time_range time_range_name]]
[inactive]
```

示例：

```
ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com
```

选项如下：

- *access_list_name* - 新的或现有 ACL 的名称。如果 ACL 已经存在，则 ACE 将添加到 ACL 末尾。
- Permit or Deny - 关键字 **deny** 在条件匹配的情况下拒绝或免除数据包。关键字 **permit** 在条件匹配的情况下允许或包含数据包。
- URL - 关键字 **url** 指定要匹配的 URL。使用 **url any** 匹配所有基于 URL 的流量。否则，输入一个 URL 字符串，可含通配符。以下是一些有关指定 URL 的提示和限制：
  - 指定 **any** 将匹配所有 URL。
  - Permit url any 将允许所有具有 protocol://server-ip/path 格式的 URL 并将阻止不匹配该模式的流量，如端口转发。应该有一个 ACE 允许连接至所需端口 （如果是 Citrix，为端口 1494），以避免发生隐式拒绝。
  - 智能隧道和 ica 插件不会受带 permit url any 值的 ACL 的影响，因为它们仅匹配 smart-tunnel:// 和 ica:// types。
  - 您可以使用以下协议：cifs://、citrix://、citrixs://、ftp://、http://、https://、imap4://、nfs://、pop3://、smart-tunnel:// 和 smtp://。您还可以在协议中使用通配符；例如，htt* 匹配 http 和 https，星号“*”匹配所有协议。例如，*://*.example.com 会将任何类型的基于 URL 的流量匹配到 example.com 网络。
  - 如果您指定一个 smart-tunnel:// URL，则仅可以包含服务器名称。URL 不能包含路径。例如， smart-tunnel://www.example.com 可以接受，但 smart-tunnel://www.example.com/index.html 却不可接受。
  - 星号“*”匹配 none 或任意数量的字符。如要匹配任意 http URL，请输入 http://*/*。
  - 问号 ?与任意一个字符完全匹配。
  - 方括号“[]”为范围运算符，匹配范围中的任意字符。例如，如要同时匹配 http://www.cisco.com:80/ 和 http://www.cisco.com:81/，请输入 **http://www.cisco.com:8[01]/**。
- Logging - **log** 参数可设置当 ACE 匹配数据包时的记录选项。如果您未在 **log** 选项中输入任何参数，则将以默认间隔 （300 秒）启用默认级别 (6) 的系统日志消息 106102。日志选项包括：
  - *level* - 介于 0 与 7 之间的严重性级别。默认值为 6。
  - **interval** *secs* - 系统日志消息之间的时间间隔（以秒为单位），范围为 1 至 600。默认值为 300。
  - **disable** - 禁用所有 ACL 记录。
  - **default** - 启用消息 106103 记录。此设置与不包含 **log** 选项的作用相同。
- Time Range - **time-range** *time_range_name* 选项指定时间范围对象，可以确定 ACE 在一天中某些时间或一周中某些天处于活动状态。如果不包含时间范围，规则将始终处于活动状态。
- Activation - 使用 **inactive** 选项以在不删除 ACE 的情况下禁用 ACE。如要重新启用 ACE，请输入完整的 ACE，无需含 inactive 关键字。

添加 Webtype ACE 以进行 IP 地址匹配

您可以基于用户正尝试访问的目标地址来匹配流量。除了 URL 规格之外，Webtype ACL 可以同时包含 IPv4 和 IPv6 地址。

如要添加 Webtype ACE 以进行 IP 地址匹配，请使用以下命令：

```
access-list access_list_name webtype {deny | permit}
tcp dest_address_argument [operator port]
[log [[level] [interval secs] | disable | default]]
[time_range time_range_name]]
[inactive]]
```

示例：

```
ciscoasa(config)# access-list acl_company webtype permit tcp any
```

有关此处未说明的关键字的说明，请参阅第 17-12 页的添加 Webtype ACE 以进行 URL 匹配。此类型 ACE 的特定关键字和参数包括以下各项：

- **tcp** - TCP 协议。 Webtype ACL 仅匹配 TCP 流量。
- Destination Address - *dest_address_argument* 指定将向其发送数据包的 IP 地址。
  - **host** *ip_address* - 指定 IPv4 主机地址。
  - *dest_ip_address mask* - 指定 IPv4 网络地址和子网掩码，如 10.100.10.0 255.255.255.0。
  - *ipv6-address/prefix-length* - 指定 IPv6 主机或网络地址和前缀。
  - **any**、**any4** 和 **any6** - **any** 同时指定 IPv4 和 IPv6 流量；**any4** 仅指定 IPv4 流量；**any6** 仅指定 IPv6 流量。
- *operator port* - 目标端口。如果不指定端口，则将匹配所有端口。*操作符*可以是以下任意一项：
  - **lt** - 小于
  - **gt** - 大于
  - **eq** - 等于
  - **neq** - 不等于
  - **range** - 值的包含范围。使用此运算符时，需指定两个端口号，例如：

    ```
    range 100 200
    ```

  port 可以是整数或 TCP 端口的名称。

Webtype ACL 的示例

以下示例显示了如何拒绝访问特定的公司 URL：

```
ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com
```

以下示例显示了如何拒绝访问特定的网页：

```
ciscoasa(config)# access-list acl_file webtype deny url
https://www.example.com/dir/file.html
```

以下示例显示了如何拒绝通过端口 8080 以 HTTP 方式访问特定服务器上的任意 URL：

```
ciscoasa(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

以下示例显示了如何在 Webtype ACL 中使用通配符。

- 以下示例匹配 http://www.example.com/layouts/1033 等 URL：

```
access-list VPN-Group webtype permit url http://www.example.com/*
```

- 以下示例匹配 http://www.example.com/ 和 http://www.example.net/ 等 URL：

```
access-list test webtype permit url http://www.example.*
```

- 以下示例匹配 http://www.example.com 和 ftp://wwz.example.com 等 URL：

```
access-list test webtype permit url *://ww?.e*co*/
```

- 以下示例匹配 http://www.cisco.com:80 和 https://www.cisco.com:81 等 URL：

```
access-list test webtype permit url *://ww?.c*co*:8[01]/
```

上例中的范围运算符“[]”指定字符 **0** 或 **1** 可以出现在该位置。

- 以下示例匹配 http://www.example.com 和 http://www.example.net 等 URL：

```
access-list test webtype permit url http://www.[a-z]xample?*/
```

上例中的范围运算符“[]”指定可出现从 **a** 至 **z** 中的任意字符。

- 以下示例匹配文件名或路径中包含“cgi”的 http 或 https URL。

```
access-list test webtype permit url htt*://*/*cgi?*
```

注　如要匹配任意 http URL，您必须输入 **http://*/***，而非 http://*。

以下示例显示了如何强制 Webtype ACL 禁用对特定 CIFS 共享的访问。

在本示例中，我们有一个包含名为“Marketing_Reports” 和“Sales_Reports”的两个子文件夹的“shares”根文件夹。我们希望明确拒绝访问“shares/Marketing_Reports”文件夹。

```
access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.
```

但是，由于 ACL 末尾有一个隐式语句“deny all”，上述 ACL 使得所有子文件夹都不可访问（“shares/Sales_Reports”和“shares/Marketing_Reports”），包括根文件夹 （“shares”)。

如要解决此问题，请添加新的 ACL 以允许访问根文件夹和其余子文件夹：

```
access-list CIFS_Allow webtype permit url cifs://172.16.10.40/shares*
```

配置 EtherType ACL

EtherType ACL 适用于透明防火墙模式中的第 2 层非 IP 流量。您可以使用这些规则，根据第 2 层数据包中的 EtherType 值允许或丢弃流量。通过 EtherType ACL，您可以控制 ASA 上的非 IP 流量。请注意，802.3 格式的帧不是由 ACL 处理，因为这些帧使用的是长度字段，而非类型字段。

如要添加 EtherType ACE，请使用以下命令：

access-list *access_list_name* **ethertype** {**deny** | **permit**}
{**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **isis** | **any** | *hex_number*}

示例：

```
ciscoasa(config)# access-list ETHER ethertype deny ipx
```

选项如下：

- *access_list_name* - 新的或现有 ACL 的名称。如果 ACL 已经存在，则 ACE 将添加到 ACL 末尾。

- Permit or Deny - 关键字 **deny** 在条件匹配的情况下拒绝数据包。关键字 **permit** 在条件匹配的情况下允许数据包。
- Traffic Matching Criteria - 您可以使用以下选项匹配流量：
  - **ipx** - 互联网数据包交换 (IPX).
  - **bpdu** - 桥接协议数据单元，默认情况下允许。
  - **mpls-multicast -** MPLS 组播。
  - **mpls-unicast** - MPLS 单播。
  - **isis** - 中间系统到中间系统 (IS-IS)。
  - **any** - 匹配所有流量。
  - *hex_number* - 任意可通过 16 位十六进制数字 （0x600 至 0xffff）识别的 EtherType。请参阅 http://www.ietf.org/rfc/rfc1700.txt 上的 RFC 1700“分配的编号”，以获取 EtherType 列表。

EtherType ACL 的示例

以下示例显示了如何配置 EtherType ACL，包括如何将 ACL 应用到接口。

以下示例 ACL 允许源自内部接口的公用流量：

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

以下 ACL 允许一些 EtherType 通过 ASA，但拒绝 IPX：

```
ciscoasa(config)# access-list ETHER ethertype deny ipx
ciscoasa(config)# access-list ETHER ethertype permit 1234
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
ciscoasa(config)# access-group ETHER in interface outside
```

以下 ACL 拒绝带 EtherType 0x1256 的流量，但允许两个接口上的所有其他流量：

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

监控 ACL

如要监控 ACL，请输入以下其中一个命令：

命令	用途
show access-list [*name*]	显示访问列表，包括每个 ACE 的行号和命中次数。包含 ACL 名称或您将看到所有访问列表。
show running-config access-list [*name*]	显示当前正在运行的访问列表配置。包含 ACL 名称或您将看到所有访问列表。

ACL 功能历史

功能名称	版本	说明
扩展 ACL、标准 ACL、 Webtype ACL	7.0(1)	ACL 用于控制网络访问或为多项功能指定要采取操作的流量。扩展访问控制列表用于通过设备的访问控制和其他几种功能。标准 ACL 用于路由映射和 VPN 过滤器。Webtype ACL 用于无客户端 SSL VPN 过滤。 EtherType ACL 控制第 2 层非 IP 流量。 我们引入了以下命令：**access-list extended**、 **access-list standard**、 **access-list webtype** 和 **access-list ethertype**。
扩展 ACL 中的实际 IP 地址	8.3(1)	使用 NAT 或 PAT 时，对于几种功能，ACL 中不再使用映射地址和端口。您必须为这些功能使用实际、未转换的地址和端口。使用实际地址和端口意味着如果 NAT 配置发生更改，您无需更改 ACL。有关详细信息，请参阅第 17-3 页的使用 NAT 时用于扩展 ACL 的 IP 地址。
支持在扩展 ACL 中使用身份防火墙	8.4(2)	您现在可以将身份防火墙用户和组用于源和目标。您可以将身份防火墙 ACL 与访问规则、AAA 规则配合使用，并可将其用于 VPN 身份验证。 我们修改了以下命令：**access-list extended**。
IS-IS 流量的 EtherType ACL 支持	8.4(5)、9.1(2)	在透明防火墙模式中，ASA 现在可以使用 EtherType ACL 控制 IS-IS 流量。 我们修改了以下命令：**access-list ethertype** {**permit** | **deny**} **isis**。
支持在扩展 ACL 中使用思科 TrustSec	9.0(1)	您现在可以将思科 TrustSec 安全组用于源和目标。您可以将身份防火墙 ACL 与访问规则配合使用。 我们修改了以下命令：**access-list extended**。
为 IPv4 和 IPv6 统一扩展 ACL 和 Webtype ACL	9.0(1)	扩展 ACL 和 Webtype ACL 现在支持 IPv4 和 IPv6 地址。您甚至可以为源和目标同时指定 IPv4 和 IPv6 地址。已更改关键字 **any** 以代表 IPv4 和 IPv6 流量。已添加 **any4** 和 **any6** 关键字以分别表示仅 IPv4 和仅 IPv6 流量。 IPv6 特定 ACL 已废弃。现有 IPv6 ACL 已迁移到扩展 ACL。请参阅版本说明以了解有关迁移的详细信息。 我们修改了以下命令：**access-list extended** 和 **access-list webtype**。 我们移除了以下命令：**ipv6 access-list**、 **ipv6 access-list webtype** 和 **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)	现在您可以根据 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** 和 **service**。

第 6 部分

IP 路由

路由概述

本章介绍有关路由如何在思科 ASA 内部运行的基本概念以及支持的路由协议。

- 第 18-1 页的有关路由
- 第 18-3 页的路由如何在 ASA 中运行
- 第 18-4 页的支持的路由互联网协议
- 第 18-5 页的有关路由表
- 第 18-9 页的禁用代理 ARP 请求

有关路由

所谓路由就是指通过互联网络把信息从源地点移到目标地点的活动。在途中，经常至少遇到一个中间节点。路由包含两项基本活动：确定最佳路由路径和通过互联网络传输信息组 （通常称为数据包）。在路由进程情景中，后者称为分组交换。尽管数据包交换相对简单，路径的确定过程却可能非常复杂。

- 第 18-1 页的交换
- 第 18-2 页的路径确定
- 第 18-2 页的支持的路由类型

交换

交换算法相对简单；大多数路由协议都采用相同的算法。在大多数情况下，主机确定必须将数据包发送到另一台主机。源主机通过某种方式获取路由器地址后，将带有具体地址的数据包发送到一个指定路由器物理 （媒体访问控制 [MAC] 层）地址，此时带有目标主机的协议 （网络层）地址。

路由器检查数据包的目标协议地址时，确定是否知道如何将数据包转发到下一跳。如果路由器不知道如何转发数据包，通常会丢失数据包。但是，如果路由器知道如何转发数据包，则将目标物理地址更改为下一跳的物理地址并发送数据包。

下一跳可能是最终目标主机。如果不是，下一跳通常是另一条路由器，该路由器也执行同样的交换决策进程。当数据包通过互联网络传输时，其物理地址会发生更改，但是，其协议地址保持不变。

路径确定

路由协议使用尺度来评估数据包传输的最佳路径。尺度为度量的标准 （例如路径带宽，路由算法使用路径带宽来确定到达目标地址的最佳路径。）为帮助确定路径进程，路由算法初始化和维护诸多包含路由信息的路由表。路由信息取决于所使用的路由算法。

路由算法用多种信息来填充路由表。目标或下一跳关联告知路由器，通过将数据包发送到到达终端目标途中代表下一跳的特定路由器，便可以最优路径到达特定目标。当路由器收到传入数据包时，会检查目标地址并尝试将此地址与下一跳关联。

路由表还包含其他信息，例如有关路径可取性的数据。路由器通过比较尺度确定最佳路径，而尺度又取决于所使用路由算法的设计。

路由器之间互相通信，并通过传输各种消息来维护路由表。路由更新消息通常包括路由表全部或部分内容。通过分析来自所有其他路由器的路由更新，路由器可以创建一份详细的网络拓扑图。链路状态通告为路由器之间发送的另一种消息，用以将发送方链路的状态告知其他路由器。链路信息还可用于创建完整网络拓扑图，使路由器能够确定到达网络目标的最佳路径。

注　非对称路由仅能用于多情景模式中的主用/主用故障转移。

支持的路由类型

路由器可以使用多种路由类型。 ASA 使用以下类型的路由：

- 第 18-2 页的静态与动态
- 第 18-2 页的单路径与多路径
- 第 18-3 页的平面结构与层次结构
- 第 18-3 页的链路状态与距离向量

静态与动态

静态路由算法几乎算不上是算法，而是网络管理员在路由开始之前建立的表映射。除非网络管理员对这些映射进行修改，否则映射不会发生改变。使用静态路由的算法易于设计，适合用于网络流量相对可预测和网络设计相对简单的环境。

静态路由系统无法对网络更改作出反应，因而通常被认为不适合大型且不断变化的网络。大多数主要的路由算法为动态路由算法，这些算法通过分析传入的路由更新消息来适应变化的网络环境。如果有消息表明网络发生更改时，路由软件将重新计算路由并发出新的路由更新消息。这些消息渗入网络中，促使路由器重新运行自身的算法并相应地更改路由表

您可以酌情使用静态路由对动态路由算法进行补充。例如，将默认路由器 （所有无法路由的数据包都被发送到该路由器）指定为所有无法路由的数据包的储存地，以确保所有消息都至少以某种方式进行处理。

单路径与多路径

某些综合路由协议支持指向同一目标的多条路径。与单路径算法不同，多路径算法允许流量在多条线路上多路复用。多路径算法的优势是完全在于较高的吞吐量和可靠性，通常称为负载共享。

平面结构与层次结构

某些路由算法在平面结构中运行而其他算法则使用路由层次结构。在平面路由系统中，路由器是所有其他路由器的对等体。在层次结构路由系统中，某些路由器形成了实际上的路由选择主干。来自非主干路由器的数据包可以传输到主干路由器，在此数据包通过主干传输直到到达目标的大致区域。此时，数据包通过一个或者多个非主干路由器，从最后一个主干路由器传输到终端目标。

路由系统常常指定逻辑节点组，称为域、自治系统或者区域。在层次结构系统中，某个域中的一些路由器可以和其他域的路由器通信，而其他路由器只可以同本域中的路由器通信。在大型网络中，还可能存在其他的层次结构级别，其中位于最高层次结构级别的路由器形成路由主干。

层次结构路由的主要优点在于，它优化了大多数公司的体系结构，从而可以很好地支持这些公司的流量模式。大多数网络通信发生在小型公司组 （域）中。由于域内路由器只需要知道该域中的其他路由器，所以可以简化这些路由器的路由算法，并根据所使用的路由算法相应地减少路由更新流量。

链路状态与距离向量

链路状态算法 （也称最短路径优先算法）在互联网络中将路由信息以泛洪形式发送给所有节点。然而，每台路由器只发送说明其自身链路状态的路由表部分内容。在链路状态算法中，每台路由器在其路由表中构建整个网络的情景。距离向量算法 （也称为 Bellman-Ford 算法）要求每台路由器只向其相邻的路由器发送其路由表的全部或部分内容。实质上，链路状态算法将小的更新发送到各处，而距离向量算法只将较大的更新发送给相邻的路由器。距离向量算法仅知道其相邻路由器。通常，链路状态算法会配合 OSPF 路由协议使用。

路由如何在 ASA 中运行

ASA 使用路由表和 XLATE 表来决定路由。为了处理目标 IP 转换流量，即反向转换流量，ASA 搜索现有的 XLATE 或静态转换来选择传出接口。

- 第 18-3 页的传出接口选择进程
- 第 18-4 页的下一跳选择进程

传出接口选择进程

选择进程按以下操作进行：

1. 如果已经存在目标 IP 转换 XLATE，则数据包的传出接口由 XLATE 表而非路由表来确定。
2. 如果不存在目标 IP 转换 XLATE，但是存在匹配的静态转换，则传出接口由静态 NAT 规则确定并创建一个 XLATE，不会使用路由表。
3. 如果不存在目标 IP 转换 XLATE，并且不存在匹配的静态转换，则不对数据包进行目标 IP 转换。 ASA 通过查询路由选择传出接口来处理该数据包，然后执行源 IP 转换 （必要时）。

   对于常规的动态出站 NAT，使用路由表对初始传出数据包进行路由然后创建 XLATE。仅使用现有 XLATE 转发传入的返回数据包。对于静态 NAT，始终使用现有 XLATE 或静态转换规则来传输目标转换传入数据包。

下一跳选择进程

在使用之前描述的任一方法选择传出接口之后，如要进行附加的路由查询，以找到合适的下一跳，该下一跳属于之前选择的传出接口。如果路由表中没有明确属于所选接口的路由，则数据包会被丢失并生成等级 6 系统日志消息 110001 (no route to host)，即使存在另有一条用于既定目标网络但属于不同传出接口的路由。如果找到属于所选传出接口的路由，数据包将被转发到相应的下一跳。

只有对可以使用单个传出接口访问的多个下一跳， ASA 才能实现负载共享。负载共享无法共享多个传出接口。

如果在 ASA 中使用动态路由，并且路由表在 XLATE 创建后发生变化 （例如路由摆动），则使用原先的 XLATE 而非路由表转发目标转换流量，直至 XLATE 超时。如果原先的路由被从原先的接口移除并通过路由进程挂接到另一个接口，则流量要么被转发到错误的接口，要么被丢谟并生成等级 6 系统日志消息 110001 (no route to host)。

当 ASA 自身没有路由摆动但是某条路由进程在其周围摆动，并使用不同接口通过 ASA 发送属于相同流量的源转换数据包时，同样的问题也可能发生。目标转换的返回数据包可能被通过错误的传出接口转发回来。

在某些安全流量配置中，任何流量可能根据流量里起始数据包的方向被进行源转换或目标转换，因此该问题很有可能发生。当在路由摆动后发生该问题时，可使用 **clear xlate** 命令手动解决或等待 XLATE 超时自动解决该问题。可以减少 XLATE 超时 （必要时）。为了保证该问题极少出现，请确保 ASA 上及其周围不存在路由摆动。即确保属于同一流量的目标转换数据包始终以相同的方式通过 ASA 转发。

支持的路由互联网协议

ASA 支持多种用于路由的互联网协议。本节对每个协议只做简单介绍。

- 增强型内部网关路由协议 (EIGRP)

  作为思科的专利协议，EIGRP 实现和 IGRP 路由的兼容性和无缝互操作性。自动再分配机制允许将 IGRP 路由导入到增强型 IGRP，反之亦然，因此，能够逐渐将增强型 IGRP 添加到现有的 IGRP 网络。

  有关配置 EIGRP 的详细信息，请参阅第 23-3 页的配置 EIGRP。

- 开放最短路径优先 (OSPF)

  OSPF 是由互联网工程任务小组 (IETF) 的内部网关协议 (IGP) 工作小组开发、面向互联网络协议 (IP) 网络的路由协议。 OSPF 使用链路状态算法构建和计算到所有已知目标的最短路径。OSPF 区域中的每台路由器包含相同的链路状态数据库，该数据库是由每台路由器可使用的接口和可到达的邻居组成的列表。

  有关配置 OSPF 的详细信息，请参阅第 22-5 页的配置 OSPFv2。

- 路由信息协议 (RIP)

  RIP 是一种使用跳数作为尺度的距离向量协议。RIP 被广泛用于路由全局互联网中的流量，并且作为一种内部网关协议 (IGP)，该协议在单个自动系统里进行路由。

  有关配置 RIP 的详细信息，请参阅旧版功能指南。

- 边界网关协议 (BGP)

  BGP 是一种自治系统间路由协议。BGP 用于交换互联网的路由信息，是在互联网服务提供商 (ISP) 之间使用的协议。客户连接到 ISP，ISP 使用 BGP 交换客户和 ISP 路由。在自治系统 (AS) 之间使用时，BGP 称为外部 BGP (EBGP)。如果服务提供商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

  有关配置 BGP 的详细信息，请参阅第 21-3 页的配置 BGP。

有关路由表

- 第 18-5 页的显示路由表
- 第 18-5 页的如何填充路由表
- 第 18-7 页的如何制定转发决策
- 第 18-7 页的动态路由和故障转移
- 第 18-8 页的动态路由和集群
- 第 18-9 页的多情景模式中的动态路由

显示路由表

操作步骤

步骤 1　查看路由表中的条目：

```
ciscoasa# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

S    10.1.1.0 255.255.255.0 [3/0] via 10.86.194.1, outside
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

如何填充路由表

ASA 路由表可由静态定义的路由、直连路由以及 RIP、EIGRP、OSPF 和 BGP 路由协议发现的路由来填充。除了路由表内的静态和连接路由，ASA 还可以运行多条路由协议，因此同一条路由可能被以不同方式发现或输入。当到达同一目标的两条路由都被添加到路由表中，将按以下方法确定哪条路由将被保留在路由表中：

- 如果两条路由有不同的网络前缀长度 （网络掩码），则两条路由都被视为唯一的路由并被输入到路由表中。然后由数据包转发逻辑确定使用哪一条路由。

  例如，如果 RIP 和 OSPF 进程发现以下路由：

  – RIP：192.168.32.0/24

  – OSPF：192.168.32.0/19

即使 OSPF 路由具有更好的管理距离，但是因为两条路由有不同的前缀长度 （子网掩码），两条路由都将被添加到路由表中。这两条路由被视为不同目标，并且由数据包转发逻辑确定采用哪一个路由。

- 如果 ASA 从单个协议获悉到达同一目标的多条路径，例如 RIP，则具有更优尺度的 RIP（由路由协议确定）将被输入到路由表中。

  尺度为关联具体路由的值，路由从最高优先到最低优先进行排序。用于确定尺度的参数取决于路由协议。尺度最低的路径被选为最佳路径并添加到路由表中。如果存在多条相等尺度的路径到达同一目标，则在这些等价路径上进行负载均衡。

- 如果 ASA 从多条路由协议获悉目标，则比较路由的管理距离，管理距离更短的路由将被输入到路由表中。

路由的管理距离

您可以更改由路由协议发现或被重新分配到路由协议的路由的管理距离。如果来自两个不同路由协议的两条路由具有相同的管理距离，则具有较低*默认*管理距离的路由将被输入到路由表中。对于 EIGRP 和 OSPF 路由，如果 EIGRP 路由和 OSPF 路由具有相同的管理距离，则默认选择 EIGRP 路由。

当存在来自不同协议的两条或更多不同的路由到达同一目标，ASA 使用管理距离作为路由参数来选择最佳路径。由于路由协议基于算法的尺度和其他协议不同，因此有时无法为不同路由协议生成的到达同一目标的两条路由确定最佳路径。

每个路由协议通过使用管理距离值来进行优先级排序。表 18-1 显示了 ASA 支持的路由协议的默认管理距离。

表 18-1　　支持的路由协议的默认管理距离

路由源	默认管理距离
已连接的接口	0
静态路由	1
EIGRP 汇总路由	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部路由	170
内部 BGP	200
未知	255

管理距离值越小，协议的优先等级越高。例如，如果 ASA 同时接收来自 OSPF 路由进程（默认管理距离 - 110）和 RIP 路由进程（默认管理距离 - 120）到达某个网络的路由，ASA 将选择 OSPF 路由，因为 OSPF 具有更高的优先级。在这种情况下，路由器将路由的 OSPF 版本添加到路由表。

在本示例中，如果 OSPF 派生路由的源丢失（例如，由于电源关闭），ASA 将使用 RIP 派生路由，直到 OSPF 派生路由再次出现。

管理距离为本地设置项。例如，如果您使用 **distance-ospf** 命令改变通过 OSPF 获取路由的路由管理距离，该更改只会影响输入了该命令的 ASA 上的路由表。管理距离不会在路由更新中被通告。

管理距离不会影响路由进程。EIGRP、OSPF、RIP 和 BGP 路由进程只通告被路由进程发现或被重新分配到路由进程的路由。例如，即使 OSPF 路由进程发现的路由被用于 ASA 路由表，RIP 路由进程也会通告 RIP 路由。

备用路由

当由于另一条路由被添加导致初始尝试将路由添加到路由表失败时，则注册一条备用路由。如果添加到路由表的路由发生故障，路由表维护进程呼叫所有注册了备用路由的路由协议进程并要求它们重新在路由表中添加此路由。如果存在多条协议为该故障路由注册了备用路由，则根据管理距离选择优先路由。

鉴于以上进程，当动态路由协议发现的路由发生故障时，您可以创建添加到路由表的浮动静态路由。浮动静态路仅仅为比 ASA 上运行的动态路由协议配置有更大管理距离的静态路由。当动态路由进程发现的相应路由发生故障时，静态路由将被添加到路由表。

如何制定转发决策

传输决策按以下方式来制定：

- 如果目标不匹配路由表中的任何条目，将通过为默认路由指定的接口转发数据包。如果尚未配置默认路由，数据包将被丢弃。
- 如果目标匹配路由表中的单个条目，将通过与该路由关联的接口转发数据包。
- 如果目标匹配路由表中的多个条目，并且所有条目具有相同的网络前缀长度，则具有相同网络前缀却有不同接口的两个条目无法同时存在路由表中。
- 如果目标匹配路由表中的多个条目，并且这些条目具有不同的网络前缀长度，则将通过与具有较长网络前缀长度的路由相关联的接口转发数据包。

例如，发往 192.168.32.1 的数据包到达路由表中拥有以下路由的 ASA 接口：

```
ciscoasa# show route
        ....
        R   192.168.32.0/24 [120/4] via 10.1.1.2
        O   192.168.32.0/19 [110/229840] via 10.1.1.3
        ....
```

在这种情况下，发往 192.168.32.1 的数据包将被直接发送到 10.1.1.2，因为 192.168.32.1 属于 192.168.32.0/24 网络。它也属于路由表中的其他路由，但 192.168.32.0/24 在路由表中的前缀最长（24 位 VS 19 位）。在转发数据包时，较长前缀始终优先于较短的前缀。

动态路由和故障转移

静态路由系统无法对网络更改作出反应，因而通常被认为不适合大型且不断变化的网络。大多数主要的路由算法为动态路由算法，这些算法通过分析传入的路由更新消息来适应变化的网络环境。如果有消息表明网络发生更改时，路由软件将重新计算路由并发出新的路由更新消息。这些消息渗入网络中，促使路由器重新运行自身的算法并相应地更改路由表

您可以酌情使用静态路由对动态路由算法进行补充。例如，将默认路由器（所有无法路由的数据包都被发送到该路由器）指定为所有无法路由的数据包的储存地，以确保所有消息都至少以某种方式进行处理。

当路由表在主用设备上发生改变时，备用设备上的动态路由同步变化，也就是说，主用设备上的所有添加、删除或更改会被立即传送到备用设备。如果在主设备进入主用状态有一段时间之后，备用设备也进入主用状态，则路由在故障转移批量同步进程中会被同步，因此，在主用/备用故障转移对上的路由表应该显示为一样的。

关于静态路由以及如何配置静态路由的详细信息，请参阅第 19-2 页的静态路由配置。

动态路由和集群

在集群中，动态路由被充分集成，不同设备之间共享路由 （每个集群最多允许 8 台设备）。路由表条目也在集群中的设备之间被复制。

当设备从从设备过渡到主设备时，RIB 表初始序号（32 位序列号）也相应增加。完成过渡后，新的主设备最初拥有的 RIB 表条目为之前主设备的镜像。此外，在新的主设备上启动再收敛计时器。当 RIB 表的初始序号增加时，所有的现有条目将被视为过时。IP 数据包转发继续正常进行。在新的主设备上，动态路由开始用新的初始序号更新现有的路由条目或创建新路由条目。带有当前初始序号的已修改条目或新创建条目表明它们已经被更新且与所有从设备同步。在再收敛计时器超时后，RIB 表中的旧条目被移除。OSPF 路由、RIP 路由以及 EIGRP 路由的 RIB 表条目也和从设备同步。

只有当某台设备加入集群时，才会从主设备到加入的设备进行批量同步。

对于动态路由更新，当主设备通过 OSPF、RIP、EIGRP 获悉新的路由时，主设备通过可靠的消息发送将更新消息发送给所有从设备。从设备在接收集群路由更新消息之后更新 RIB 表。

对于支持的动态路由协议 （OSPF、RIP 和 EIGRP），来自从设备上第 2 层负载均衡接口的路由数据包被转发给主设备。只有主设备才能发现和处理动态路由协议数据包。当从设备请求执行批量同步时，所有通过第 2 层负载均衡接口获悉的路由条目都将被复制。

当通过主设备上第 2 层负载均衡接口获悉新的路由条目时，新条目被广播到所有从设备。当网络拓扑变化导致现有路由条目被修改时，被修改的条目被同步到所有从设备。当网络拓扑变化导致现有路由条目被移除时，被移除的条目被同步到所有从设备。

当为动态路由同时部署和配置了第 2 层以及第 3 层负载均衡接口时，从设备仅拥有路由进程中部分的拓扑和相邻信息 （包括从第 3 层负载均衡接口获得的详细信息），因为对于第 2 层负载均衡接口来说，只有 RIB 表条目和主设备同步。您必须将网络的第 2 层和第 3 层配置为属于不同的路由进程，并且重新分配来自每个路由进程的负载。

表 18-2 提供了对支持配置的概述。Yes 表明两个进程构成的组合（到第 2 层的进程和到第 3 层的进程）起作用，No 表明两个进程构成的组合不起作用。

表 18-2　　支持配置概述

第 2 层或第 3 层	OSPF（第 3 层）	EIGRP（第 3 层）	RIP（第 3 层）
OSPF（第 2 层）	是	是	是
EIGRP（第 2 层）	是	否	是
RIP（第 2 层）	是	是	否

集群中的所有设备必须处于同一模式：单情景模式或多情景模式。在多情景模式中，主从同步在同步消息中包含所有情景和所有情景中的 RIB 条目。

在集群中，如果您已配置第 3 层接口，还必须配置路由器地址池设置。

有关动态路由和集群的详细信息，请参阅第 8 章，“ASA 集群”。

多情景模式中的动态路由

在多情景模式中，每个情景维护一个独立的路由表和路由协议数据库。因而您可以在每个情景中单独配置 OSPFv2 和 EIGRP。您可以在某些情景中配置 EIGRP 以及在相同或不同的情景中配置 OSPFv2。在混合情景模式中，您可以在路由模式的情景中启用任何动态路由协议。多情景模式不支持 RIP 和 OSPFv3。

下表列出了 EIGRP 及 OSPFv2 的属性、用于给 OSPFv2 和 EIGRP 进程分配路由的路由映射、以及在 OSPFv2 中用于过滤路由更新 （多情景模式中进入或离开某个区域）的前缀列表：

EIGRP	OSPFv2	路由映射和前缀列表
每个情景支持一个实例。	每个情景支持两个实例。	不适用
在系统情景中禁用。		不适用
两个情景可能使用相同的或不同的自治系统编号。	两个情景可能使用相同或不同的区域 ID。	不适用
两个情景的共享接口可能会运行多个 EIGRP 实例。	两个情景的共享接口可能会运行多个 OSPF 实例。	不适用
支持共享接口间 EIGRP 实例的交互。	支持共享接口间 OSPFv2 实例的交互。	不适用
在单模式中可用的所有 CLI 在多情景模式中也可用。		
每个 CLI 仅对其被使用的情景起作用。		

路由资源管理

我们已经介绍过名叫 *routes* 的资源类，该资源类指定了能够存在于某个情景中的路由表条目的最大数量。因而解决了一个情景影响另一个情景中可用的路由表条目的问题，您也可以对每个情景中的路由条目最大数量进行更好的控制。

由于没有明确的系统限制，您只能为该资源限制指定一个绝对值，不能使用百分比限制。此外，每个情景中没有最小限制和最大限制，因此，默认类不会进行更改。如果您在某个情景中为静态或动态路由协议 （连接、静态、 OSPF、 EIGRP 和 RIP）添加新的路由但情景的资源限制已被耗尽，则路由添加失败，并且生成系统日志消息。

禁用代理 ARP 请求

将 IP 流量发送到同一以太网网络上的其他设备时，主机需要知道该设备的 MAC 地址。ARP 是将 IP 地址解析为 MAC 地址的第 2 层协议。主机发送 ARP 请求 “Who is this IP address?”，拥有 IP 地址的设备回答 “I own that IP address; here is my MAC address”。

当设备使用自身的 MAC 地址响应 ARP 请求时，会使用代理 ARP，即使该设备不具有 IP 地址。当您配置 NAT 并指定与 ASA 接口处于相同网络里的映射地址时，ASA 使用代理 ARP。流量能到达主机的唯一方法为，ASA 使用代理 ARP 来声称 MAC 地址已被分配到目标映射地址。

在极少数情况下，您可能想要为 NAT 地址禁用代理 ARP。

如果您的 VPN 客户端地址池与现有网络重叠， ASA 默认在所有接口上发送代理 ARP 请求。如果您在同一个第 2 层域上有另一个接口，它将看到 ARP 请求，并以其接口的 MAC 地址来回应。结果是，通往内部主机的 VPN 客户端的返回流量将流向错误的接口，然后被丢弃。在这种情况下，您需要在不需要的接口上禁用代理 ARP 请求。

操作步骤

步骤 1　禁用代理 ARP 请求

sysopt noproxyarp *interface*

示例：

```
ciscoasa(config)# sysopt noproxyarp exampleinterface
```

静态路由和默认路由

本章介绍如何在思科 ASA 上配置静态路由和默认路由。

- 第 19-1 页的有关静态路由和默认路由
- 第 19-2 页的静态路由和默认路由准则
- 第 19-2 页的静态路由配置
- 第 19-3 页的配置默认静态路由
- 第 19-4 页的配置 IPv6 默认和静态路由
- 第 19-5 页的监控静态路由或默认路由
- 第 19-7 页的静态路由或默认路由的示例
- 第 19-7 页的静态路由和默认路由的功能历史

有关静态路由和默认路由

如要将流量路由到无连接主机或网络，您必须定义一条到主机或网络的静态路由，或至少定义一条默认路由到不直接与 ASA 连接的任意网络，例如，网络和 ASA 之间有一台路由器。

如果没有定义静态路由或默认路由，流向无连接主机或网络的流量将生成以下系统日志消息：

```
%ASA-6-110001: No route to dest_address from source_address
```

在以下情况下，您可能想要在单情景模式中使用静态路由：

- 网络使用 EIGRP、 RIP 或 OSPF 中不同的路由器发现协议。
- 网络规模小，您可以轻松管理静态路由。
- 您不希望流量或 CPU 开销与路由协议相关联。

最简单的方法是配置一条默认路由，将所有流量发送到上游路由器，由路由器确定如何路由流量。但是，在某些情况下，默认网关可能无法到达目标网络，因此，您还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法直接将流量发送到不直接与 ASA 连接的任何内部网络。

在透明防火墙模式中，对于源自 ASA 并且要发往非直接相连的网络的流量，您需要配置一条默认路由或静态路由，以便 ASA 知道通过哪个接口发送流量。源自 ASA 的流量可能包括与系统日志服务器、Websense 或 N2H2 服务器或 AAA 服务器的通信。如果有服务器无法通过单条默认路由进行访问，则必须配置静态路由。此外，对于同一负载均衡接口，ASA 最多支持 3 条等价路由。

静态路由和默认路由准则

故障转移准则

支持动态路由协议的状态故障转移。

其他指导原则

- ASDM 透明模式不支持 IPv6 静态路由。
- 在集群中，只有主设备支持静态路由监控。有关集群的详细信息，请参阅第 8 章，“ASA 集群”。

静态路由配置

静态路由算法基本上是指网络管理员在路由开始之前建立的表映射。除非网络管理员对这些映射进行修改，否则映射不会发生改变。使用静态路由的算法易于设计，适合用于网络流量相对可预测和网络设计相对简单的环境。鉴于此，静态路由系统无法对网络更改作出反应。

即使指定的网关变得不可用，静态路由仍然保留在路由表中。如果指定的网关变得不可用，您需要手动从路由表移除静态路由。然而，如果指定接口发生故障，静态路由将从路由表移除，并且当接口恢复时再复原到路由表。

注　如果您创建静态路由比 ASA 上运行的路由协议具有更大的管理距离，则到达该路由协议发现的指定目标的路由优先于静态路由。只有当动态发现路由从路由表移除时，才使用静态路由。

您最多可以为每个接口定义 3 个等价路由到达同一目标。多个接口上间不支持等价多路径 (ECMP)。有了 ECMP，路由之间的流量没必要平均分配，流量基于散列源和目标 IP 地址的算法被分配到指定网关。

静态 Null0 路由配置

通常，使用 ACL 来过滤流量，您可以根据报头包含的信息、过滤数据包。在数据包过滤过程中，ASA 防火墙检查数据包报头做出过滤决策，由此增加一些数据包处理开销并影响性能。

静态 Null0 路由是过滤的补充解决方案。静态 Null0 路由用于将不必要或不想要的流量转发到黑洞。空接口 Null0 用于创建黑洞。静态路由是为不想要的目标而创建，静态路由配置指向空接口。对于任何流量，如果其目标地址和黑洞静态路由具有最佳匹配，都将被自动丢弃。不同于 ACL，静态 Null0 不会导致任何性能降级。

静态 Null0 路由配置用于防止路由环路。 BGP 利用静态 Null0 配置用于远程触发黑洞路由。

例如：

```
route null0 192.168.2.0 255.255.255.0
```

如要配置静态路由，请参阅以下章节：

- 第 19-3 页的添加或编辑静态路由

添加或编辑静态路由

操作步骤

步骤 1　添加或编辑静态路由：

route *if_name dest_ip mask gateway_ip* [*distance*]

示例：

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 [1]
```

参数 *dest_ip* 和 *mask 表明*目标网络的 IP 地址，参数 *gateway_ip* 为下一跳路由器的地址。为静态路由指定的地址是在进入 ASA 和执行 NAT 之前的数据包内的地址。

参数 *distance 为*路由的管理距离。如果未指定值，默认值为 1。管理距离是一个用来比较不同路由协议之间路由的参数。静态路由的默认管理距离为 1，使静态路由优先于动态路由协议发现的路由，但不优先于直接连接的路由。

OSPF 发现路由的默认管理距离为 110。如果静态路由与动态路由的管理距离相同，静态路由将优先。直连路由始终优先于静态路由或动态发现路由。

示例

以下示例显示作为等价路由的静态路由将流量定向到外部接口上的三个不同的网关。ASA 在指定网关间分配流量。

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.2
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.3
```

配置默认静态路由

默认路由对网关 IP 地址进行标识，ASA 将所有不具有已获悉或静态路由的数据包发送到该网关地址。默认静态路由是指将 0.0.0.0/0 作为目标 IP 地址的静态路由。标识具体目标的路由优先于默认路由。

注　在 7.0(1) 版本及更高版本中，如果您在具有不同尺度的不同接口上同时配置两条默认路由，则从具有更高尺度的接口到 ASA 的连接将发生故障，但是，从具有有较尺度的低口到 ASA 的连接则会成功，如同预期结果一样。

您最多可以为每台设备定义 3 个等价默认路由条目。如果定义多个等价默认路由条目，会导致发送到默认路由的流量被在指定网关间进行分配。定义多条默认路由时，您必须为每个条目指定同一接口。

如果您尝试定义不止 3 条等价默认路由或定义与先前定义的默认路由有不同接口的默认路由，您将收到以下消息：

```
"ERROR: Cannot add route entry, possible conflict with existing routes."
```

您可以为隧道流量定义单独的默认路由以及标准默认路由。当您创建了一条带有**隧道** 选项的默认路由时，来自终止于无法使用已获悉或静态路由进行路由的 ASA 的隧道的所有流量都将被发送到该路由。对于来自隧道的流量，该路由覆盖任何其他的已配置的或已获悉的默认路由。

默认静态路由配置的限制

以下限制应用于带有隧道选项的默认路由：

- 请勿在隧道路由的传出接口上启用单播 RPF（**ip verify reverse - path** 命令），因为该设置会导致会话失败。
- 请勿在隧道路由的传出接口上启用 TCP 拦截，因为该设置会导致会话失败。
- 请勿使用带有隧道路由的 VoIP 检测引擎 (CTIQBE、 H.323、 GTP、 MGCP、 RTSP、 SIP、 SKINNY)、 DNS 检测引擎或 DCE RPC 检测引擎，因为这些检测引擎会忽略隧道路由。
- 您无法定义多 条带有隧道选项的默认路由。
- 不支持隧道流量 ECMP。

操作步骤

步骤 1　添加或编辑隧道默认静态路由：

route *if_name* 0.0.0.0 0.0.0.0 *gateway_ip* [*distance* | *tunneled*]

示例：

```
ciscoasa(config)# route outside 0 0 192.168.2.4 tunneled
```

参数 *dest_ip* 和 *mask* 表明目标网络的 IP 地址，参数 *gateway_ip* 为下一跳路由器的地址。为静态路由指定的地址是在进入 ASA 和执行 NAT 之前的数据包内的地址。

参数 *distance* 为路由的管理距离。如果未指定值，默认值为 1。管理距离是一个用来比较不同路由协议之间路由的参数。静态路由的默认管理距离为 1，使静态路由优先于动态路由协议发现的路由，但不优先于直接连接的路由。OSPF 发现路由的默认管理距离为 110。如果静态路由与动态路由的管理距离相同，静态路由将优先。直连路由始终优先于静态路由或动态发现路由。

提示　您可以为目标网络地址和子网掩码输入 0 0 而非 0.0.0.0 0.0.0.0，如下例所示：

```
ciscoasa(config)# route outside 0 0 192.168.1 1
```

配置 IPv6 默认和静态路由

如果已为 IPv6 启用直连主机连接的接口并且 IPv6 ACLs 允许流量通过，ASA 将自动在这些主机之间路由 IPv6 流量。

操作步骤

步骤 1　添加默认 IPv6 路由：

ipv6 route *if_name* **::/0** *next_hop_ipv6_addr*

示例：

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1
```

示例为网络 7fff::0/32 将数据包路由到 3FFE:1100:0:CC00::1 内部接口的网络设备

地址 ::/0 是任何 IPv6 对等体。

步骤 2　将 IPv6 静态路由添加到 IPv6 路由表：

ipv6 route *if_name destination next_hop_ipv6_addr* [*admin_distance*]

示例：

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 [110]
```

示例为网络 7fff::0/32 将数据包路由到 3FFE:1100:0:CC00::1 内部接口的网络设备，管理距离为 110。

注　**ipv6 route** 命令和用于定义 IPv4 静态路由的 **route** 命令具有相同的工作原理。

监控静态路由或默认路由

使用静态路由的其中一个问题是，没有内在机制确定路由处于打开还是关闭状态。即使下一跳网关变得不可用，这些路由依然保留在路由表中。只有 ASA 上的关联接口发生故障时，静态路由才会从路由表中移除。

如果主要路由发生故障，静态路由跟踪功能可以用来跟踪静态路由的可用性和添加备用路由。例如，您可以定义一条到 ISP 网关的默认路由和一条到辅助 ISP的备用默认路由，以防主要 ISP 变得不可用。

ASA 通过将静态路由与您定义的监控目标相关联来实施该功能，并使用 ICMP 回应请求监控目标。如果在指定时间内没有收到回应回复，对象将被视为关闭并且将从路由表移除相关联的路由。先前配置的备用路由将代替被移除的路由。

选择监控目标时，您需要确保该目标可回应 ICMP 回应请求。该目标可能是您选择的任何网络对象，但是，您应考虑使用以下各项：

- ISP 网关 （双 ISP 支持）地址
- 下一跳网关地址 （如果您关注网关的可用性）
- 目标网络上的服务器通信，例如 AAA 服务器，ASA 需要与该服务器进行通信。
- 目标网络上的持久网络对象

注　最好不要用台式或笔记本电脑，因为您可能会在晚上关闭这些电脑。

您可以为静态定义路由或通过 DHCP 或 PPPoE 获取的默认路由配置静态路由跟踪。您只能在配置了路由跟踪的多个接口上启用 PPPoE 客户端。

操作步骤

步骤 1　定义监控进程，以配置跟踪对象监控参数：

sla monitor *sla_id*

示例：

```
ciscoasa(config)# sla monitor 5
```

如果您更改已定义类型的计划外监控进程的监控参数，您将自动进入 sla 协议配置模式。

步骤 2　指定监控协议：

type echo protocol ipIcmpEcho *target_ip* **interface** *if_name*

示例：

```
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 172.29.139.134
```

如果您更改已定义类型的计划外监控进程的监控参数，您将自动进入 sla 协议配置模式并无法更改设置。

参数 *target_ip* 为网络对象的 IP 地址，跟踪进程监控其可用性。当该对象可用时，跟踪进程被添加到路由表。当该对象变得不可用时，跟踪进程移除该路由，并且启用备用路由。

步骤 3　安排监控进程：

sla monitor schedule *sla_id* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | *pending* | *now* | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]

示例：

```
ciscoasa(config)# sla monitor schedule 5 start-time now
```

通常，您可以使用 **sla monitor schedule** *sla_id* **life forever start-time now** 命令执行监控时间表，并且允许监控配置决定多久进行检测。

然而，您可以将监控进程安排为未来时间开始并只以指定次数进行。

步骤 4　将被跟踪的静态路由关联到 SLA 监控进程：

track *track_id* **rtr** *sla_id* **reachability**

示例：

```
ciscoasa(config)# track 6 rtr 5 reachability
```

参数 *track_id* 为使用该命令分配的跟踪号。参数 *sla_id* 为 SLA 进程的 ID 号。

步骤 5　跟踪静态路由：

route *if_name dest_ip mask gateway_ip* [*admin_distance*] **track** *track_id*

示例：

```
ciscoasa(config)# route if_name dest_ip mask gateway_ip [admin_distance] track track_id
```

您无法在静态路由跟踪中使用 **route** 命令来使用 **tunneled** 选项。

步骤 6　跟踪通过 DHCP 获取的默认路由：

```
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# dhcp client route track track_id
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config-if)# exit
```

请记住，您必须使用关键字 **setroute** 结合 **ip address dhcp** 命令来通过 DHCP 获取默认路由。

步骤 7　跟踪通过 PPPoE 获取的默认路由：

```
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# pppoe client route track track_id
```

```
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config-if)# exit
```

请记住，您必须使用关键字 **setroute** 结合 **ip address pppoe** 命令来通过 PPPoE 获取默认路由。

静态路由或默认路由的示例

以下示例展示如何创建一条静态路由，该路由将以 10.1.1.0/24 为目标的所有流量发送到与内部接口连接的路由器 10.1.2.45，定义 3 条将流量定向到外部接口的 3 个不同网关的等价静态路由，并将默认路由添加到隧道流量。然后 ASA 在指定网关间分配流量。

```
ciscoasa(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.1
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.2
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.3
ciscoasa(config)# route outside 0 0 192.168.2.4 tunneled
```

ASA 收到的未加密流量没有静态或可获悉的路由，将使用 IP 地址 192.168.2.1、 192.168.2.2 和 192.168.2.3 在网关间进行分配。 ASA 收到的加密流量没有静态或可获悉的路由，将使用 IP 地址 192.168.2.4 传送到网关。

以下示例创建一条静态路由，该路由将以 10.1.1.0/24 为目标的所有流量发送到与内部接口连接的路由器 (10.1.2.45)。

```
ciscoasa(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
```

静态路由和默认路由的功能历史

表 19-1　静态路由和默认路由的功能历史

功能名称	平台版本	功能信息
路由	7.0(1)	引入了静态路由和默认路由。 引入了 **route** 命令。
集群	9.0(1)	仅在主设备上支持静态路由监控。
静态 Null0 路由配置	9.2(1)	向 Null0 接口发送流量会导致发往指定网络的数据包被丢弃。此功能对于配置 BGP 的远程触发黑洞 (RTBH) 作用甚大。 修改了以下命令：**route**。

路由映射

- 第 20-1 页的有关路由映射
- 第 20-3 页的路由映射准则
- 第 20-4 页的定义路由映射
- 第 20-4 页的自定义路由映射
- 第 20-6 页的路由映射的配置示例
- 第 20-6 页的路由映射的功能历史记录

有关路由映射

在将路由重新分发给 OSPF、 RIP、 EIGRP 或 BGP 路由进程时使用路由映射。为 OSPF 路由进程生成默认路由时也使用路由映射。路由映射定义允许将源自指定路由协议的哪些路由重新分发给目标路由进程。

路由映射与广为人知的 ACL 有许多相同功能。以下是两者共有的一些特征：

- 它们都是个别语句的有序序列，各有一个允许或拒绝结果。 ACL 或路由映射的评估包括采用预先确定顺序的列表扫描，以及每条语句匹配条件的评估。一旦找到第一个语句匹配即中止列表扫描，并且会执行与语句匹配关联的操作。
- 它们都是通用机制 - 条件匹配和匹配解释由应用的方式决定。应用于不同任务的相同路由映射可能以不同方式进行解释。

以下是路由映射与 ACL 之间的一些差异：

- 路由映射经常使用 ACL 作为匹配条件。
- ACL 评估的主要结果为肯定或否定回答 - 即 ACL 允许或拒绝输入数据。应用于重新分发时，ACL 确定特定路由能 （路由匹配 ACL Permit 语句）否 （路由匹配 Deny 语句）重新分发。重新分发到另一协议时，典型的路由映射不仅允许 （部分）重新分发的路由，而且还修改与路由关联的信息。
- 路由映射比 ACL 更加灵活，可以根据 ACL 无法验证的条件对路由进行验证。例如，路由映射可以验证路由的类型是否为内部。
- 根据设计约定，每个 ACL 以隐式 Deny 语句结尾；路由映射没有类似约定。如果在匹配尝试期间达到路由映射的结尾，则结果取决于路由映射的特定应用。幸运的是，应用于重新分发的路由映射与 ACL 的行为方式相同：如果路由与路由映射中的任何子句均不匹配，则路由重新分发会被拒绝，如同路由映射末尾包含 Deny 语句一样。

动态协议 **redistribute** 命令可供您应用路由映射。在 Cisco ASDM 中，当添加或编辑新的路由映射时，可以找到用于重新分发的此功能（请参阅第 20-4 页的定义路由映射）。如果要在重新分发期间修改路由信息或者如果需要比 ACL 能够提供的功能更强大的匹配功能，路由映射是首选。如果只是需要根据路由的前缀或掩码选择性地允许一些路由，我们建议您使用路由映射直接在 **redistribute** 命令中映射到 ACL（或等效前缀列表）。如果根据路由的前缀或掩码使用路由映射选择性地允许一些路由，通常可以使用更多配置命令来实现相同目标。

注　必须使用标准 ACL 作为路由映射的匹配条件。使用扩展式 ACL 将不起作用，且将永不重新分发路由。我们建议您以 10 为间隔对子句编号以保留编号空间，以便将来需要插入子句。

- 第 20-2 页的 Permit 和 Deny 子句
- 第 20-2 页的 Match 和 Set 子句值
- 第 20-3 页的 BGP Match 和 BGP Set 子句

Permit 和 Deny 子句

路由映射可以有 Permit 和 Deny 子句。在 **route-map ospf-to-eigrp** 命令中，有一个 Deny 子句（序号为 10）和两个 Permit 子句。 Deny 子句可拒绝来自重新分发的路由匹配。因此，请遵守以下规则：

- 如果在使用 Permit 子句的路由映射中使用 ACL，则将重新分发 ACL 允许的路由。
- 如在路由映射 Deny 子句中使用 ACL，则将不重新分发 ACL 允许的路由。
- 如果在路由映射 Permit 或 Deny 子句中使用 ACL，并且 ACL 拒绝路由，则找不到路由映射子句匹配，并将评估下一个路由映射子句。

Match 和 Set 子句值

每个路由映射子句均有两种类型的值：

- 匹**配**值**选择**应将此子句应用到的路由。
- 设定值修改将重新分发到目标协议的信息。

对于要重新分发的每个路由，路由器首先评估路由映射中子句的匹配条件。如果匹配条件成功，则将根据 Permit 或 Deny 子句的指示重新分发或拒绝路由，其某些属性可能被从 ASDM 中 Set Value 选项卡或从 **set** 命令设定的值修改。如果匹配条件失败，则此子句不适用于路由，软件会根据路由映射中下一个子句继续评估路由。路由映射的扫描会继续进行，直到 **match** 命令找到子句，或者 ASDM 中的 Match Clause 选项卡中设置的 Match 子句与路由匹配，或者到达路由映射的末尾。

如果存在以下条件之一，则每个子句中的匹配或设定值会缺少或重复多次：

- 如果子句中存在多个 **match** 命令或 ASDM 中的 Match Clause 值，则一切必须针对给定路由成功才能使该路由与子句匹配 （换句话说，逻辑 AND 算法适用于多个匹配命令）。
- 如果 **match** 命令或 ASDM 中的 Match Clause 值在一个命令中引用多个对象，则其中之一应匹配（应用逻辑 OR 算法）。例如，在 **match ip address 101 121** 命令中，如果 ACL 101 或 ACL 121 允许路由，则路由即被允许。
- 如果 **match** 命令或 ASDM 中的 Match Clause 值不存在，则所有路由均与子句匹配。在上述示例中，到达子句 30 的所有路由均匹配；因此，永远不会到达路由映射的结尾。
- 如果 **set** 命令或 ASDM 中的 Set Value 在路由映射 Permit 子句中不存在，则将重新分发路由，而不会修改其当前属性。

注　请勿在路由映射 Deny 子句中配置 **set** 命令，因为 Deny 子句禁止路由重新分发 - 将不修改信息。

没有 **match** 或 **set** 命令或 ASDM 中的 Match Value 或 Set Value 选项卡中设置的值，路由映射子句会执行操作 空 permit 子句允许重新分发剩余路由，而不会做出修改。空 deny 子句不允许重新分发其他路由 （如果路由映射完成扫描但未找到显式匹配，此为默认操作）。

BGP Match 和 BGP Set 子句

除了如上所述的匹配和设定值之外，BGP 还为路由映射提供其他匹配和设置功能。

BGP 目前支持以下新的路由映射 Match 子句：

- match as-path
- match community
- match policy-list
- match tag

BGP 目前支持以下新的路由映射 Set 子句：

- set as-path
- set automatic-tag
- set community
- set local-preference
- set origin
- set weight

对于要重新分发的每个 BGP 路由，ASA 首先评估路由映射中子句的 BGP 匹配条件。如果 BGP 匹配条件成功，则将根据 Permit 或 Deny 子句的指示重新分发或拒绝路由，其某些属性可能被从 ASDM 中 BGP Set Clause 选项卡或从 **set** 命令设定的值修改。如果匹配条件失败，则此子句不适用于路由，软件会根据路由映射中下一个子句继续评估路由。路由映射的扫描会继续进行，直到 **match** 命令找到子句、ASDM 中的 BGP Match Clause 选项卡中的设置与路由匹配，或者到达路由映射的末尾。

路由映射准则

防火墙模式

仅在路由防火墙模式中受支持。透明防火墙模式不受支持。

其他指导原则

路由映射不支持包括用户、用户组和完全限定域名对象的 ACL。

定义路由映射

当指定允许将源自指定路由协议的哪些路由重新分发到目标路由进程时，必须定义路由映射。

操作步骤

步骤 1　创建路由映射条目：

route-map *name* {**permit** | **deny**} [*sequence_number*]

示例：

```
ciscoasa(config)# route-map name {permit} [12]
```

路由映射条目按顺序读取。您可以使用 *sequence_number* 参数标识顺序，否则 ASA 会使用您添加路由映射条目的顺序。

自定义路由映射

本节说明如何自定义路由映射。

- 第 20-4 页的定义路由以匹配特定目标地址
- 第 20-5 页的为路由操作配置度量值

定义路由以匹配特定目标地址

操作步骤

步骤 1　创建路由映射条目：

route-map *name* {**permit** | **deny**} [*sequence_number*]

示例：

```
ciscoasa(config)# route-map name {permit} [12]
```

路由映射条目按顺序读取。您可以使用 *sequence_number* 选项标识顺序，否则 ASA 会使用您添加路由映射条目的顺序。

步骤 2　匹配包含目标网络且匹配标准 ACL 或前缀列表的所有路由：

match ip address *acl_id* [*acl_id*] [...] [prefix-list]

示例：

```
ciscoasa(config-route-map)# match ip address acl1
```

如果指定多个 ACL，则路由可以匹配任何 ACL。

步骤 3　匹配拥有指定度量的任何路由：

match metric *metric_value*

示例：

```
ciscoasa(config-route-map)# match metric 200
```

metric_value 范围在 0 到 4294967295 之间。

步骤 4　匹配包含下一跳路由器地址且匹配标准 ACL 的任何路由：

match ip next-hop *acl_id* [*acl_id*] [...]

示例：

```
ciscoasa(config-route-map)# match ip next-hop acl2
```

如果指定多个 ACL，则路由可以匹配任何 ACL。

步骤 5　匹配带有指定下一跳接口的任何路由：

match interface *if_name*

示例：

```
ciscoasa(config-route-map)# match interface if_name
```

如果指定多个接口，则路由可以匹配任一接口。

步骤 6　匹配由匹配标准 ACL 的路由器已通告的任何路由：

match ip route-source *acl_id* [*acl_id*] [...]

示例：

```
ciscoasa(config-route-map)# match ip route-source acl_id [acl_id] [...]
```

如果指定多个 ACL，则路由可以匹配任何 ACL。

步骤 7　匹配路由类型：

match route-type {**internal** | **external** [**type-1** | **type-2**]}

为路由操作配置度量值

如果路由与 **match** 命令匹配，则以下 **set** 命令会确定在重新分发路由之前对路由执行的操作。

如要为路由操作配置度量值，请执行以下步骤：

操作步骤

步骤 1　创建路由映射条目：

route-map *name* {**permit** | **deny**} [*sequence_number*]

示例：

```
ciscoasa(config)# route-map name {permit} [12]
```

路由映射条目按顺序读取。您可以使用 *sequence_number* 参数标识顺序，否则 ASA 会使用您添加路由映射条目的顺序。

步骤 2　为路由映射设置度量值：

set metric *metric_value*

示例：

```
ciscoasa(config-route-map)# set metric 200
```

metric_value 参数的范围在 0 到 294967295 之间。

步骤 3　为路由映射设置度量类型：

set metric-type {**type-1** | **type-2**}

示例：

```
ciscoasa(config-route-map)# set metric-type type-2
```

metric-type 参数可能是 type-1 或 type-2。

路由映射的配置示例

以下示例显示如何将跳数等于 1 的路由重新分发到 OSPF。

ASA 将这些路由作为度量为 5 且度量类型为 1 类的外部 LSA 重新分发。

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

以下示例显示如何使用配置的度量值将 10.1.1.0 静态路由重新分发到 eigrp 进程 1：

```
ciscoasa(config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config-router)# redistribute static metric 250 250 1 1 1 route-map mymap2
```

路由映射的功能历史记录

表 20-1　　路由映射的功能历史记录

功能名称	平台版本	功能信息
路由映射	7.0(1)	我们引入了此功能。 我们引入了以下命令：**route-map**。
对静态和动态路由映射的增强支持	8.0(2)	增加了对动态和静态路由映射的增强支持。
支持动态路由协议（EIGRP、OSPF 和 RIP）有状态故障转移以及一般路由操作的调试	8.4(1)	我们引入了以下命令：**debug route**、 **show debug route**。 我们修改了以下命令：**show route**。
多情景模式中的动态路由	9.0(1)	路由映射在多情景模式中受支持。

表 20-1　　路由映射的功能历史记录（续）

功能名称	平台版本	功能信息
支持 BGP	9.2(1)	我们引入了此功能。 我们引入以下命令：**router bgp**
		我们引入了以下命令：

BGP

本章节介绍如何配置思科 ASA，以使用边界网关协议 (BGP) 来路由数据、执行身份验证以及重新分发路由信息。

- 第 21-1 页的关于 BGP
- 第 21-3 页的 BGP 准则
- 第 21-3 页的配置 BGP
- 第 21-18 页的监控 BGP
- 第 21-20 页的 BGP 配置示例
- 第 21-21 页的 BGP 历史记录

关于 BGP

BGP 是一种自治系统间的路由协议。自治系统是一个或一组接受共同管理并采用共同路由策略的网络。 BGP 用于交换互联网的路由信息，是在互联网服务提供商 (ISP) 之间使用的协议。

- 第 21-1 页的何时使用 BGP
- 第 21-1 页的路由表更改

何时使用 BGP

客户网络（例如，大学和公司）通常使用 OSPF 等内部网关协议 (IGP) 在它们的网络内部交换路由信息。客户连接到 ISP，ISP 使用 BGP 交换客户和 ISP 路由。在自治系统 (AS) 之间使用时，BGP 称为外部 BGP (EBGP)。如果服务提供商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

路由表更改

在 BGP 邻居之间首次建立 TCP 连接时，BGP 邻居会交换完整路由信息。当检测到对路由表所做的更改时，BGP 路由器向它们的邻居仅发送已更改的路由。BGP 路由器不发送定期路由更新，BGP 路由更新仅通告到达目标网络的最佳路径。

当存在多个到达某个特定目标的路由时，通过 BGP 学习的路由的属性可用于确定到达该目标的最佳路径。这些属性称为 BGP 属性，可用于路由选择过程：

- 权重 - 这是思科定义的路由器本地属性。权重属性不通告给相邻路由器。如果路由器获悉有多个到达同一目标的路由，则首选权重最高的路由。

- 本地首选项 - 本地首选项属性用于从本地 AS 中选择出口点。与权重属性不同，本地首选项属性在整个本地 AS 中传播。如果有多个来自 AS 的出口点，本地首选项属性最高的出口点用作特定路由的出口点。
- 多出口鉴别器 - 多出口鉴别器 (MED) 或度量属性可用作对外部 AS 关于进入正在通告此度量的 AS 的首选路径的建议。因为正在接收 MED 的外部 AS 也可能正在使用其他 BGP 选择路由，所以它被称作建议。首选 MED 度量较低的路由。
- 源 - 源属性指示 BGP 获悉某个特定路由的方式。源属性可能拥有三个可能值其中之一，并用于路由选择。
  - IGP - 此路由是源 AS 的内部路由。当使用网络路由器配置命令向 BGP 注入路由时，设置该值。
  - EGP - 此路由通过外部边界网关协议 (EBGP) 获悉。
  - 不完整 - 路由源未知或通过其他方式获悉。当路由被重新分发到 BGP 时，会出现不完整源。
- AS_path - 当路由通告通过自治系统时，将 AS 编号添加到此路由通告已经穿越的 AS 编号有序列表。仅拥有最短 AS_path 列表的路由安置在 IP 路由表中。
- 下一跳 - EBGP 下一跳属性是用于到达通告路由器的 IP 地址。对于 EBGP 对等体，下一跳地址是对等体之间的连接 IP 地址。对于 IBGP，EBGP 下一跳地址将携带至本地 AS 中。
- 社区 - 社区属性提供一种目标 （称为社区）的分组方式，可对社区应用路由决策 （例如，接受、首选项和重新分发）。路由映射用于设定社区属性。预定义的社区属性如下所示：
  - no-export - 不向 EBGP 对等体通告此路由。
  - no-advertise - 不向任何对等体通告此路由。
  - internet - 向互联网社区通告此路由；网络中的所有路由器均属于它。

BGP 路径选择

BGP 可能从不同来源接收同一路由的多个通告。BGP 仅选择一个路径作为最佳路径。选择此路径时，BGP 将选定的路径放在 IP 路由表中，并将此路径传播给其邻居。BGP 按列出的顺序使用以下条件选择某个目标的路径：

- 如果路径指定的下一跳不可访问，则放弃此次更新。
- 首选权重最高的路径。
- 如果权重相同，则首选本地首选项最高的路径。
- 如果本地首选项相同，则首选此路由器上运行的 BGP 发起的路径。
- 如果未发起路由，则首选 AS_path 最短的路由。
- 如果所有路径的 AS_path 长度相同，则首选源类型最低的路径（其中，IGP 低于 EGP，EGP 低于不完整路径）。
- 如果源代码相同，则首选 MED 属性最低的路径。
- 如果路由的 MED 相同，则首选外部路径而非内部路径。
- 如果路径依然相同，则首选穿过最近的 IGP 邻居的路径。
- 如果两个路径都是外部路径，则首选第一个接收的路径 （最早的路径）。
- 首选拥有由 BGP 路由器 ID 指定的最低 IP 地址的路径。
- 如果多条路径的发起方或路由器 ID 相同，则首选集群列表长度最短的路径。
- 首选来自最低邻居地址的路径。

BGP 准则

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

不支持透明防火墙模式。 BGP 仅在路由器模式中受支持。

故障转移准则

在单情景模式和多情景模式中支持有状态故障转移。

注　启用集群时，不支持故障转移。

集群准则

BGP 仅在 L2（以太网信道类型）和 L3（单个接口类型）集群模式中受支持。

注　在用户情景中删除和重新应用 BGP 配置时，允许 60 秒的延迟，使从/备用 ASA 装置同步。

IPv6 准则

支持 IPv6。优雅重启不受 IPv6 地址系列支持。

配置 BGP

本节介绍如何在系统上启用和配置 BGP 进程。

操作步骤

步骤 1　在 CLI 中，启用 BGP，配置一般 BGP 参数。

步骤 2　为 BGP 路由进程定义最佳路径，并配置最佳路径配置参数。

步骤 3　添加和配置策略列表。

步骤 4　添加和配置 AS 路径过滤器。

步骤 5　添加和配置社区规则。

步骤 6　配置 IPv4 地址系列设置。

启用 BGP

本节介绍启用 BGP 路由、建立 BGP 路由进程和配置一般 BGP 参数所需的步骤。

操作步骤

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp *autonomous-num*

示例：

```
ciscoasa(config)# router bgp 2
```

autonomous-num 的有效值范围为 1-4294967295 至 1.0-XX.YY。

步骤 2 丢弃 as-path 分段超出指定值的路由。

bgp maxas-limit *number*

示例：

```
ciscoasa(config-router)# bgp maxas-limit 15
```

此 *number* 参数指定允许的最大自治系统分段数。有效值范围为 1 至 254。

步骤 3 日志 BGP 邻居重置：

bgp log-neighbor-changes

步骤 4 使 BGP 自动发现每个 BGP 会话的最佳 TCP 路径 MTU：

bgp transport path-mtu-discovery

步骤 5 在用于到达对等体的链接中断时，使 BGP 终止任何直接相邻对等体的外部 BGP 会话；无需等待抑制计时器过期：

bgp fast-external-fallover

步骤 6 如果外部 BGP (eBGP) 对等体未在传入路径的 AS_PATH 属性中将其自治系统 (AS) 编号列为首个 AS 路径分段，则允许 BGP 路由进程放弃从这些外部 BGP 接收的更新。

bgp enforce-first-as

步骤 7 将 BGP 4 字节自治系统编号的默认显示和正则表达式匹配格式从 asplain（十进制值）更改为点表示法。

bgp asnotation dot

步骤 8 调整 BGP 网络计时器：

timers bgp *keepalive holdtime* [*min-holdtime*]

示例：

```
ciscoasa(config-router)# timers bgp 80 120
```

- *keepalive* - ASA 向其对等体发送 keepalive 消息的频率 （单位：秒）。默认值为 60 秒。
- *holdtime* - ASA 在未接收到 keepalive 消息后宣布对等体无效的时间间隔 （单位：秒）。默认值为 180 秒。
- （可选） *min-holdtime* - ASA 未从邻居接收到 keepalive 消息后宣布邻居无效的时间间隔（单位：秒）。

步骤 9　启用 BGP 优雅重启功能：

bgp graceful-restart [**restart-time** *seconds*|**stalepath-time** *seconds*][**all**]

示例：

```
ciscoasa(config-router)# bgp graceful-restart restart-time 200
```

- **restart-time** - ASA 等待能够优雅重启的邻居在重启事件发生后恢复正常操作的最大时间段（单位：秒）。默认值为 120 秒。有效值范围为 1 至 3600 秒。
- **stalepath-time** - ASA 为重启对等体保留过时路径的最大时间段 （单位：秒）。此计时器过期后，将删除所有过时路径。默认值为 360 秒。有效值范围为 1 至 3600 秒。

定义 BGP 路由进程的最佳路径

本节介绍配置 BGP 最佳路径所需的步骤。有关最佳路径的更多信息，请参阅第 21-2 页的 BGP 路径选择。

操作步骤

步骤 1　启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp *autonomous-num*

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2　更改默认本地首选项值：

bgp default local-preference *number*

示例：

```
ciscoasa(config-router)# bgp default local-preference 500
```

此 *number* 参数是介于 0 与 4294967295 之间的任意值。值越高，表示首选项更高。

默认值为 100。

步骤 3　启用从不同自治系统中的不同邻居获悉的路径之间的多出口鉴别器 (MED) 比较：

bgp always-compare-med

步骤 4　在最佳路径选择过程中，比较从外部 BGP (eBGP) 接收的类似路径，将最佳路径切换到路由器 ID 最低的路由：

bgp bestpath compare-routerid

步骤 5　选择从相邻 AS 通告的最佳 MED 路径：

bgp deterministic-med

步骤 6　将拥有缺失 MED 属性的路径设置为最不受欢迎的路径：

bgp bestpath med missing-as-worst

配置策略列表

当在路径映射中引用策略列表时，将评估和处理此策略列表中的所有匹配语句。通过一个路由映射可以配置两个或更多策略列表。策略列表也可以与任何其他早已存在的匹配共存，并设置在同一路径映射内部、策略列表外部配置的语句。本节介绍配置策略列表所需的步骤。

操作步骤

步骤 1 启用策略映射配置模式，在该模式中可创建 BGP 策略列表：

policy-list *policy_list_name* {**permit** | **deny**}

示例：

```
ciscoasa(config)# policy-list Example-policy-list1 permit
```

关键字 **permit** 允许访问匹配条件。

关键字 **deny** 拒绝访问匹配条件。

步骤 2 分发让其下一跳脱离一个指定接口的路由：

match interface [*...interface_name*]

示例：

```
ciscoasa(config-policy-list)# match interface outside
```

步骤 3 通过匹配以下某个或所有项重新分发路由：目标地址、下一跳路由器地址和路由器/接入服务器来源：

match ip {**address** | **next-hop** | **route-source**}

步骤 4 匹配 BGP 自治系统路径：

match as-path

步骤 5 匹配 BGP 社区：

match community {*community-list_name* | **exact-match**}

示例：

```
ciscoasa(config-policy-list)# match community ExampleCommunity1
```

- *community-list_name* - 一个或多个社区列表。
- **exact-match** - 指示需要精确匹配 所有社区以及仅指定社区必须存在。

步骤 6 重新分发带指定度量的路由：

match metric

步骤 7 重新分发路由表中匹配指定标记的路由：

match tag

配置 AS 路径过滤器

AS 路径过滤器可供您使用访问列表过滤路由更新消息，查看更新消息中的单个前缀。如果更新消息中的前缀匹配过滤条件，则该单个前缀将被过滤掉或接受，具体取决于已将过滤器条目配置为执行什么操作。本节介绍配置 AS 路径过滤器所需的步骤。

注　**as-path 访问列表**不**同于**常规防火墙 ACL。

操作步骤

步骤 1　在全局配置模式中，使用正则表达式配置自治系统路径过滤器：

as-path access-list *acl-number* {**permit**|**deny**} *regexp*

示例：

```
ciscoasa(config)# as-path access-list 35 permit testaspath
```

- *acl-number* - AS 路径访问列表号。有效值范围为 1 至 500。
- *regexp* - 定义 AS 路径过滤器的正则表达式。自治系统号表示为从 1 至 65535 的值。

配置社区规则

社区指的是一组共享某个通用属性的目标。您可以使用社区列表，创建要在路由映射中的匹配子句中使用的社区组。像访问列表一样，可以创建一系列的社区列表。系统将检查语句，直至找到匹配为止。只要满足一个语句，测试即可结束。本节介绍配置社区规则所需的步骤。

操作步骤

步骤 1　创建或配置 BGP 社区列表，并控制对它的访问：

community-list {**standard**| *community list-name* {**deny**|**permit**} [*community-number*] [*AA:NN*] [**internet**] [**no-advertise**][**no-export**]}| {**expanded**|*expanded list-name* {**deny**| **permit**}*regexp*}

示例：

```
ciscoasa(config)# community-list standard excomm1 permit 100 internet no-advertise
no-export
```

- **standard** - 使用 1 至 99 的数字配置标准社区列表，以识别社区的一个或多个允许或拒绝组。
- （可选） *community-number* - 作为从 1 至 4294967200 的32 位数字的社区。可输入一个社区，也可输入多个社区，用空格隔开。
- *AA:NN* - 以 4 字节新社区格式输入的自治系统号和网络号。此值使用 2 个用冒号隔开的 2 字节数字配置。为每个 2 字节号输入 1 至 65535 的数字。可输入一个社区，也可输入多个社区，用空格隔开。
- （可选）**internet** - 指定互联网社区。向所有对等体（内部和外部）通告带此社区的路由。
- （可选）**no-advertise** - 指定无通告社区。不向任何对等体（内部或外部）通告带此社区的路由。
- （可选）**no-export** - 指定无导出社区。仅向同一自治系统中的对等体或者仅向联盟中的其他子自治系统通告带此社区的路由。不向外部对等体通告这些路由。

- （可选）**expanded**- 配置一个从 100 至 500 的已扩展社区列表号，以识别社区的一个或多个允许或拒绝组。
- *regexp* - 定义 AS 路径过滤器的正则表达式。自治系统号表示为从 1 至 65535 的值。

注 正则表达式只能与已扩展社区列表一起使用。

配置 IPv4 地址系列设置

BGP 的 IPv4 设置可以从 BGP 配置设置中的 IPv4 系列选项设定。IPv4 系列部分包括以下子部分：一般设置、汇聚地址设置、过滤设置和邻居设置。每一这些子部分均可供您自定义 IPv4 系列专用参数。

本节介绍如何自定义 BGP IPv4 系列设置。

- 第 21-8 页的配置 IPv4 系列一般设置
- 第 21-10 页的配置 IPv4 系列汇聚地址设置
- 第 21-11 页的配置 IPv4 系列过滤设置
- 第 21-12 页的配置 IPv4 系列 BGP 邻居设置
- 第 21-16 页的配置 IPv4 网络设置
- 第 21-17 页的配置重新分发设置
- 第 21-18 页的配置路由注入设置

配置 IPv4 系列一般设置

本节介绍配置一般 IPv4 设置所需的步骤。

操作步骤

步骤 1 启用 BGP 路由进程，使路由器进入路由器配置模式：

router bgp *autonomous-num*

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IPv4 地址前缀配置路由会话：

address-family ipv4 [**unicast**]

关键字 **unicast** 指定 IPv4 单播地址前缀。这是默认设置，即使未指定。

步骤 3 （可选）为本地 BGP 路由进程配置固定路由器 ID：

bgp router-id *A.B.C.D*

示例：

```
ciscoasa(config-router-af)# bgp router-id 10.86.118.3
```

参数 *A.B.C.D* 以 IP 地址形式指定路由器标识符。如果不指定路由器 ID，系统将自动分配路由器 ID。

步骤 4　（可选）在单个接口 (L3) 模式中配置 IP 地址集群池：

bgp router-id *cluster-pool*

示例：

```
ciscoasa(config-router-af)# bgp router-id cp
```

注　在 L3 集群中，不能将 BGP 邻居定义为其中一个集群池 IP 地址。

步骤 5　配置 BGP 路由的管理距离：

distance bgp *external-distance internal-distance local-distance*

示例：

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- *external-distance* - 外部 BGP 路由的管理距离。从外部自治系统获悉的路由为外部路由。此参数的值范围为 1 至 255。
- *internal-distance* - 内部 BGP 路由的管理距离。从本地自治系统中对等体获悉的路由为内部路由。此参数的值范围为 1 至 255。
- *local-distance* - 本地 BGP 路由的管理距离。本地路由指的是通过网络路由器配置命令列出的网络，通常作为正在从其他进程重新分发的路由器或网络的后门。此参数的值范围为 1 至 255。

步骤 6　使用 BGP 获悉的路由更新 IP 路由表时，修改度量和标记值。

table-map {**WORD**|*route-map_name*}

示例：

```
ciscoasa(config-router-af)# table-map example1
```

参数 *route-map_name* 指定来自 **route-map** 命令的路由映射名称。

步骤 7　配置 BGP 路由进程，以分发默认路由 （网络 0.0.0.0）：

default-information originate

步骤 8　将子网路由自动摘要配置进网络层路由：

auto-summary

步骤 9　抑制未安置在路由信息库 (RIB) 中的路由的通告：

bgp suppress-inactive

步骤 10　在 BGP 与内部网关协议 (IGP) 系统之间实现同步：

synchronization

步骤 11　将 iBGP 重新分发配置进 IGP，例如 OSPF：

bgp redistribute-internal

步骤 12　为下一跳验证配置 BGP 路由器扫描时间间隔：

bgp scan-time *scanner-interval*

示例：

```
ciscoasa(config-router-af)# bgp scan-time 15
```

参数 *scanner-interval* 指定 BGP 路由信息的扫描时间间隔。有效值范围为 5 至 60 秒。默认值为 60 秒。

步骤 13 配置 BGP 下一跳地址跟踪：

bgp nexthop trigger {**delay** *seconds*|**enable**}

示例：

```
ciscoasa(config-router-af)# bgp nexthop trigger delay 15
```

- **trigger** - 指定使用 BGP 下一跳地址跟踪。使用此关键字与关键字 **delay** 更改下一跳跟踪延迟。使用此关键字与关键字 **enable** 启用下一跳地址跟踪。
- **delay** - 更改路由表中安置的更新下一跳路由上的检查延迟时间间隔。
- *seconds* - 指定以秒为单位的延迟。范围为 0 至 100。默认值为 5。
- **enable** - 立即启用 BGP 下一跳地址跟踪。

步骤 14 控制可以安置在路由表中的并行 iBGP 路由的最大数量：

maximum-paths {*number_of_paths*|ibgp *number_of_paths*}

示例：

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

注 参数 *number_of_paths* 指定安置到路由表中的路由的数量。在 ASA 9.3(1) 中，有效值范围介于 1 与 3 之间。
如果未使用关键字 **ibgp**，则参数 *number_of_paths* 将控制并行 EBGP 路由的最大数量。

配置 IPv4 系列汇聚地址设置

本节介绍将特定路由汇聚定义为一个路由所需的步骤。

操作步骤

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp *autonomous-num*

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IPv4 地址前缀配置路由会话：

address-family ipv4 [**unicast**]

关键字 **unicast** 指定 IPv4 单播地址前缀。这是默认设置，即使未指定。

步骤 3 在 BGP 数据库中创建汇聚条目：

aggregate-address *address mask* [**as-set**][**summary-only**][**suppress-map** *map-name*][**advertise-map** *map-name*][**attribute-map** *map-name*]

示例：

```
ciscoasa(config-router-af) aggregate-address 10.86.118.0 255.255.255.0 as-set summary-only
suppress-map example1 advertise-map example1 attribute-map example1
```

- *address* - 汇聚地址。
- *mask* - 汇聚掩码。
- *map-name* - 路由映射。
- （可选）**as-set -** 生成自治系统集路径信息。
- （可选）**summary-only** - 过滤来自更新的所有更具体的路由。
- （可选）**Suppress-map *map-name* -** 指定用于选择要抑制的路由的路由映射的名称。
- （可选）**Advertise-map *map-name* -** 指定用于选择创建 AS_SET 源社区所需的路由的路由映射的名称。
- （可选）**Attribute-map *map-name* -** 指定用于设置汇聚路由属性的路由映射的名称。

配置 IPv4 系列过滤设置

本节介绍过滤在传入 BGP 更新中接收的路由或网络所需的步骤。

操作步骤

步骤 1　启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp *autonomous-num*

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2　进入地址系列配置模式，以使用标准 IPv4 地址前缀配置路由会话：

address-family ipv4 [**unicast**]

关键字 **unicast** 指定 IPv4 单播地址前缀。这是默认设置，即使未指定。

步骤 3　过滤在传入 BGP 更新中接收的或在传出 BGP 更新中通告的路由或网络：

distribute-list *acl-number* **in**|**out**[]

示例：

```
ciscoasa(config-router-af)# distribute-list ExampleAcl in bgp 2
```

参数 *acl-number* 指定 IP 访问列表号。此访问列表定义要在路由更新中接收的网络和要抑制的网络。关键字 **in** 指定过滤器必须应用于传入 BGP 更新，关键字 **out** 指定过滤器必须应用于传出 BGP 更新。

配置 IPv4 系列 BGP 邻居设置

本节介绍定义 BGP 邻居和邻居设置所需的步骤。

操作步骤

步骤 1 启用 BGP 路由进程，使路由器进入路由器配置模式：

router bgp *autonomous-num*

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IPv4 地址前缀配置路由会话：

address-family ipv4 [**unicast**]

关键字 **unicast** 指定 IPv4 单播地址前缀。这是默认设置，即使未指定。

步骤 3 向 BGP 邻居表添加条目：

neighbor *ip-address* **remote-as** *autonomous-number*

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remote-as 3
```

步骤 4 （可选）禁用邻居或对等组：

neighbor *ip-address* **shutdown**

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 shutdown 3
```

步骤 5 与 BGP 邻居交换信息：

neighbor *ip-address* **activate**

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 activate
```

步骤 6 为 BGP 邻居启用或禁用边界网关协议 (BGP) 优雅重启功能：

neighbor *ip-address* **ha-mode graceful-restart** [**disable**]

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ha-mode graceful-restart
```

（可选）关键字 **disable 为邻居禁用** BGP 优雅重启功能。

步骤 7 按访问列表中的指定分发 BGP 邻居信息：

neighbor {*ip-address*} **distribute-list** {*access-list-name*}{**in**|**out**}

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 distribute-list ExampleAcl in
```

- *access-list-number* - 标准或扩展访问列表的编号。标准访问列表号的范围为 1 至 99。扩展访问列表号的范围为 100 至 199。

- *expanded-list-number* - 已扩展访问列表的编号。已扩展访问列表的范围为 1300 至 2699。
- *access-list-name* - 标准或扩展访问列表的名称。
- *prefix-list-name* - BGP 前缀列表的名称。
- **in** - 访问列表应用于传入到此邻居的通告。
- **out** - 访问列表应用于传出到此邻居的通告。

步骤 8 将路由映射应用于传入或传出路由：

neighbor {*ip-address*} **route-map** *map-name* {**in**|**out**}

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 route-map example1 in
```

关键字 **in** 将路由映射应用于传入路由。

关键字 **out** 将路由映射应用于传出路由。

步骤 9 按前缀列表中的指定分发 BGP 邻居信息：

neighbor {*ip-address*} **prefix-list** *prefix-list-name* {**in**|**out**}

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 prefix-list NewPrefixList in
```

关键字 **in** 意味着前缀列表应用于从此邻居传入的通告。

关键字 **out** 意味着前缀列表应用于传出到此邻居的通告。

步骤 10 设置过滤器列表：

neighbor {*ip-address*} **filter-list** *access-list-number* {**in**|**out**}

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 filter-list 5 in
```

- *access-list-name* - 指定自治系统路径访问列表的编号。您可以使用 **ip as-path access-list** 命令定义此访问列表。
- **in** - 访问列表应用于从此邻居传入的通告。
- **out** - 访问列表应用于传出到此邻居的通告。

步骤 11 控制可以从邻居接收的前缀的数量：

neighbor {*ip-address*} **maximum-prefix** *maximum* [*threshold*][**restart** *restart interval*][**warning-only**]

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 maximum-prefix 7 75 restart 12
```

- *maximum* - 从此邻居允许的前缀的最大数量。
- （可选）*threshold* - 指定路由器在达到最大值的多少百分比时开始生成警告消息的整数。范围为 1 至 100；默认值为 75 (%)。
- （可选）*restart interval* - 指定 BGP 邻居重新启动前的时间间隔的整数值（单位：分钟）。
- （可选）**warning-only** - 允许路由器在超出前缀最大数时生成日志消息，而不是终止对等。

步骤 12 允许 BGP 发言者 （本地路由器）将默认路由 0.0.0.0 发送到邻居，用作默认路由：

neighbor {*ip-address*} **default-originate** [**route-map** *map-name*]

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 default-originate route-map example1
```

参数 *map-name* 是路由映射的名称。路由映射允许有条件地注入路由 0.0.0.0。

步骤 13 设置发送 BGP 路由更新的最小时间间隔：

neighbor {*ip-address*} **advertisement-interval** *seconds*

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 advertisement-interval 15
```

参数 *seconds* 是时间 （单位：秒）。有效值范围为 0 至 600。

步骤 14 通告 BGP 表中匹配已配置的路由映射的路由。

neighbor {*ip-address*} **advertise-map** *map-name* {**exist-map** *map-name* |**non-exist-map** *map-name*}[**check-all-paths**]

示例：

```
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

- **advertise-map** *map name* - 将在达到存在映射或非存在映射的条件时通告的路由映射的名称。
- **exist-map** *map name* - 与 BGP 表中的路由进行比较，以确定通告映射路由是否被通告的存在映射的名称。
- **non-exist-map** *map name* - 与 BGP 表中的路由进行比较，以确定通告映射路由是否被通告的非存在映射的名称
- （可选）**check all paths** - 让拥有 BGP 表中的前缀的存在映射检查所有路径。

步骤 15 从出站路由更新中删除专用自治系统号：

neighbor {*ip-address*} **remove-private-as**

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remove-private-as
```

步骤 16 为特定 BGP 对等体或对等组设置计时器。

neighbor {*ip-address*} **timers** *keepalive holdtime min holdtime*

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 timers 15 20 12
```

- *keepalive* - ASA 向其对等体发送 keepalive 消息的频率（单位：秒）。默认值为 60 秒。有效值范围为 0 至 65535。
- *holdtime* - ASA 在未接收到 keepalive 消息后宣布对等体无效的时间间隔 （单位：秒）。默认值为 180 秒。
- *min holdtime* - ASA 在未接收到 keepalive 消息后宣布对等体无效的最小时间间隔 （单位：秒）。

步骤 17 在两个 BGP 对等体之间的 TCP 连接上启用 Message Digest 5 (MD5) 身份验证：

neighbor {*ip-address*} **password** *string*

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 password test
```

参数 *string* 是区分大小写的密码，启用 **service password-encryption** 命令时，最多 25 个字符；不启用 **service password-encryption** 命令时，最多 81 个字符。此字符串包含任意字母数字字符，包括空格。

注　第一个字符不能为数字。您不能指定 number-space-anything 格式的密码。数字后的空格会导致身份验证失败。

步骤 18　指定应将社区属性发送至 BGP 邻居：

neighbor {*ip-address*} **send-community**[**both**|**standard**|**extended**]

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 send-community
```

- （可选）关键字 **both** - 将发送标准社区和扩展社区。
- （可选）关键字 **standard** - 仅发送标准社区。
- （可选）关键字 **extended** - 仅发送扩展社区。

步骤 19　配置路由器作为 BGP 发言邻居或对等组的下一跳：

neighbor {*ip-address*}**next-hop-self**

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 next-hop-self
```

步骤 20　接受并尝试到驻留在未直接连接的网络上的外部对等体的 BGP 连接：

neighbor {*ip-address*} **ebgp-multihop** [*ttl*]

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ebgp-multihop 5
```

参数 *ttl* 指定生存时间，范围为 1 到 255 跳。

步骤 21　禁用连接验证，与使用环回接口的单跳对等体建立 eBGP 对等会话：

neighbor {*ip-address*} **disable-connected-check**

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 disable-connected-check
```

步骤 22　保护 BGP 对等会话，配置分隔两个外部 BGP (eBGP) 对等体的最大跳数。

neighbor {*ip-address*} **ttl-security hops** *hop-count*

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

参数 *hop-count* 指的是分隔 eBGP 对等体的跳数。 TTL 值由路由器使用已配置的跳数参数计算得出。有效值范围为 1 至 254。

步骤 23 向邻居连接分配权重：

neighbor {*ip-address*} **weight** *number*

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 weight 30
```

参数 *number* 指的是分配给邻居连接的权重。有效值范围为 0 至 65535。

步骤 24 配置 ASA 仅接受某个特定 BGP 版本：

neighbor {*ip-address*} **version** *number*

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 version 4
```

参数 *number* 指定 BGP 版本号。版本可以设为 2，强制软件仅使用第 2 版与指定邻居。默认情况下使用第 4 版，如有要求，可以动态地协商降级至第 2 版本。

步骤 25 为 BGP 会话启用 TCP 传输会话选项：

neighbor {*ip-address*} **transport** {**connection-mode**{**active**|**passive**}|
path-mtu-discovery[**disable**]}

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 transport path-mtu-discovery
```

- **connection-mode** - 连接类型 （**主动**或**被动**）。
- **path-mtu-discovery** - 启用 TCP 传输路径最大传输单位 (MTU) 发现。 TCP 路径 MTU 发现已默认启用。
- （可选）**disable -** 禁用 TCP 路径 MTU 发现。

步骤 26 为从边界网关协议 (eBGP) 邻居接收的路由自定义 AS_PATH 属性：

neighbor {*ip-address*} **local-as** [*autonomous-system-number*[**no-prepend**]]

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- （可选）*autonomous-system-number* - 向 AS_PATH 属性预置的自治系统号。此参数的值范围为从 1 至 4294967295 或 1.0 至 XX.YY 的任意有效自治系统号。
- （可选）**no-prepend** - 不向从 eBGP 邻居接收的任何路由预置本地自治系统号。

配置 IPv4 网络设置

本节介绍定义将由 BGP 路由进程通告的网络所需的步骤。

操作步骤

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp *autonomous-num*

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2　进入地址系列配置模式，以使用标准 IPv4 地址前缀配置路由会话：

address-family ipv4 [unicast]

关键字 **unicast** 指定 IPv4 单播地址前缀。这是默认设置，即使未指定。

步骤 3　指定将由 BGP 路由进程通告的网络：

network {*network-number* *[***mask** *network-mask]}[***route-map** *map-tag]*

示例：

```
ciscoasa(config-router-af)# network 10.86.118.13 mask 255.255.255.255 route-map example1
```

- *network-number* - BGP 将通告的网络。
- （可选）*network-mask* - 带掩码地址的网络或子网掩码。
- （可选）*map-tag* - 已配置的路由映射的标识符。应当检查路由映射，以过滤要通告的网络。如果未指定，则通告所有网络。

配置重新分发设置

本节介绍定义将路由从另一个路由域重新分发到 BGP 的条件所需的步骤。

操作步骤

步骤 1　启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp *autonomous-num*

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2　进入地址系列配置模式，以使用标准 IPv4 地址前缀配置路由会话：

address-family ipv4 [unicast]

示例：

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

关键字 **unicast** 指定 IPv4 单播地址前缀。这是默认设置，即使未指定。

步骤 3　将路由从另一个路由域重新分发到 BGP 自治系统：

redistribute *protocol [process-id] [metric] [***route-map [map-tag]]**

示例：

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- *protocol* - 从其中重新分发路由的源协议。它可能是以下某项：Connected、 EIGRP、 OSPF、 RIP 或 Static。
- （可选）*process-id* - 特定路由协议的名称。
- （可选）*metric* - 已重新分发的路由的度量。
- （可选）*map-tag* - 已配置的路由映射的标识符。

注 应当检查路由映射，以过滤要重新分发的网络。如果未指定，则重新分发所有网络。

配置路由注入设置

本节介绍定义有条件地注入 BGP 路由表中的路由所需的步骤。

操作步骤

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp *autonomous-num*

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IPv4 地址前缀配置路由会话：

```
address-family ipv4 [unicast]
```

示例：

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

关键字 **unicast** 指定 IPv4 单播地址前缀。这是默认设置，即使未指定。

步骤 3 配置有条件的路由注入，将更具体的路由注入 BGP 路由表：

bgp inject-map *inject-map* **exist-map** *exist-map* [**copy-attributes**]

示例：

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- *inject-map* - 指定要注入本地 BGP 路由表的前缀的路由映射的名称。
- *exist-map* - 包含 BGP 发言者将跟踪的前缀的路由映射的名称。
- （可选）**copy-attributes** - 将已注入的路由配置为继承汇聚路由的属性。

监控 BGP

您可以使用以下命令监控 BGP 路由进程。有关命令输出的示例和说明，请参阅命令参考。此外，您可以禁用邻居变更消息和邻居警告消息的日志记录。

如要监控各种 BGP 路由统计信息，请输入以下命令之一：

- **show bgp** [*ip-address* [*mask* [*longer-prefixes* [*injected*] | *shorter-prefixes* [*length*]]]| **prefix-list** *name* | **route-map** *name*]

  显示 BGP 路由表中的条目。
- **show bgp cidr-only**

显示带非自然网络掩码的路由 （即，无类别域间路由，或 CIDR）。

- **show bgp community** *community-number* [**exact-match**][**no-advertise**][**no-export**]

  显示属于指定的 BGP 社区的路由。
- **show bgp community-list** *community-list-name* [**exact-match**]

  显示 BGP 社区列表允许的路由。
- **show bgp filter-list** *access-list-number*

  显示符合指定的过滤器列表的路由。
- **show bgp injected-paths**

  显示 BGP 路由表中所有注入的路径。
- **show bgp ipv4 unicast**

  显示 IPv4 BGP 路由表中的单播会话条目。
- **show bgp neighbors** *ip_address*

  显示有关到邻居的 BGP 和 TCP 连接的信息。
- **show bgp paths** [LINE]

  显示数据库中的所有 BGP 路径。
- **show bgp pending-prefixes**

  显示有待删除的前缀。
- **show bgp prefix-list** *prefix_list_name* [WORD]

  显示匹配已指定前缀列表的路由。
- **show bgp regexp** *regexp*

  显示匹配自治系统路径正则表达式的路由。
- **show bgp replication** [*index-group* | *ip-address*]

  显示 BGP 更新组的更新复制统计信息。
- **show bgp rib-failure**

  显示无法安置在路由信息库 (RIB) 表中的 BGP 路由。
- **show bgp route-map** *map-name*

  根据已指定的路由映射显示 BGP 路由表中的条目。
- **show bgp summary**

  显示所有 BGP 连接的状态。
- **show bgp system-config**

  显示多情景模式中的系统情景专用 BGP 配置。

  此命令在多情景模式中的所有用户情景中可用。
- **show bgp update-group**

  显示有关 BGP 更新组的信息。

注　如要禁用 BGP Log 消息，请在路由器配置模式中输入 **no bgp log-neighbor-changes** 命令。这会禁用邻居变更消息的日志记录。在 BGP 路由进程的路由器配置模式中输入此命令。
默认情况下，已记录邻居变更。

BGP 配置示例

本示例显示如何通过各种可选进程启用和配置 BGPv4。

步骤 1 定义从一个路由协议向另一个路由协议重新分发路由的条件，或者启用策略路由：

```
ciscoasa(config)# route-map mymap2 permit 10
```

步骤 2 重新分发有路由地址或匹配已指定的某个访问列表传输的数据包的任何路由：

```
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

步骤 3 指示从何处输出为策略路由传递路由映射匹配子句的数据包：

```
ciscoasa(config-route-map)# set ip next-hop peer address
```

步骤 4 从全局配置模式启用 BGP 路由进程：

```
ciscoasa(config)# router bgp 2
```

步骤 5 在地址系列配置模式中，为本地边界网关协议 (BGP) 路由进程配置固定路由器 ID：

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

步骤 6 向 BGP 邻居表添加条目：

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 remote-as 65
```

步骤 7 将路由映射应用于传入或传出路由：

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 route-map mymap2 in
```

BGP 历史记录

表 21-1 列出了各种功能变更以及实施该等功能变更的平台版本。

表 21-1 BGP 功能历史

功能名称	平台版本	功能信息
BGP 支持	9.2(1)	添加了以下支持：可以使用边界网关协议路由数据、执行身份验证以及重新分发和监控路由信息。 我们引入了以下命令：**router bgp**、**bgp maxas-limit**、 **bgp log-neighbor-changes**、 **bgp transport path-mtu-discovery**、 **bgp fast-external-fallover**、 **bgp enforce-first-as**、 **bgp asnotation dot**、**timers bgp**、 **bgp default local-preference**、 **bgp always-compare-med**、**bgp bestpath compare-routerid**、**bgp deterministic-med**、**bgp bestpath med missing-as-worst**、 **policy-list**、 **match as-path**、 **match community**、 **match metric**、 **match tag**、 **as-path access-list**、**community-list**、 **address-family ipv4**、 **bgp router-id**、 **distance bgp**、**table-map**、 **bgp suppress-inactive**、 **bgp redistribute-internal**、 **bgp scan-time**、 **bgp nexthop**、 **aggregate-address**、 **neighbor**、 **bgp inject-map**、**show bgp**、**show bgp cidr-only**、**show bgp all community**、**show bgp all neighbors**、 **show bgp community**、 **show bgp community-list**、 **show bgp filter-list**、 **show bgp injected-paths**、 **show bgp ipv4 unicast**、 **show bgp neighbors**、 **show bgp paths**、 **show bgp pending-prefixes**、 **show bgp prefix-list**、 **show bgp regexp**、 **show bgp replication**、 **show bgp rib-failure**、 **show bgp route-map**、 **show bgp summary**、 **show bgp system-config**、 **show bgp update-group**、 **clear route network**、 **maximum-path**、 **network**。 我们修改了以下命令：**show route**、**show route summary**, **show running-config router**、**clear config router**、**clear route all**、**timers lsa arrival**、**timers pacing**、**timers throttle**、**redistribute bgp**。
ASA 集群的 BGP 支持	9.3(1)	我们添加了对 L2 和 L3 集群的支持。 我们引入了以下新命令：**bgp router-id clusterpool**
不间断转发的 BGP 支持	9.3(1)	我们添加了对不间断转发的支持。 我们引入了以下新命令：**bgp graceful-restart**、**neighbor ha-mode graceful-restart**
通告映射的 BGP 支持	9.3(1)	我们添加了对 BGPv4 通告映射的支持。 我们引入了以下新命令：**neighbor advertise-map**

OSPF

本章描述如何配置思科 ASA 以使用开放式最短路径优先 (OSPF) 路由协议来路由数据，执行身份验证和重新分发路由信息。

本章包含以下各节：

- 第 22-1 页的关于 OSPF
- 第 22-4 页的 OSPF 准则
- 第 22-5 页的配置 OSPFv2
- 第 22-6 页的配置 OSPF 快速呼叫数据包
- 第 22-7 页的定制 OSPFv2
- 第 22-17 页的配置 OSPFv3
- 第 22-34 页的配置无中断重新启动
- 第 22-38 页的 OSPFv2 的配置示例
- 第 22-39 页的 OSPFv3 的配置示例
- 第 22-40 页的监控 OSPF
- 第 22-42 页的附加参考资料
- 第 22-42 页的 OSPF 功能历史记录

关于 OSPF

OSPF 是一种使用链路状态而非距离矢量进行路径选择的内部网关路由协议。OSPF 传播链路状态通告而非路由表更新。由于仅交换 LSA 而不是整个路由表，因此 OSPF 网络比 RIP 网络更快收敛。

OSPF 使用链路状态算法构建和计算到所有已知目标的最短路径。OSPF 区域中的每台路由器包含相同的链路状态数据库，该数据库是由每台路由器可使用的接口和可到达的邻居组成的列表。

OSPF 相比于 RIP 包括以下优点：

- OSPF 链路状态数据库更新的发送频率低于 RIP 更新，并且随着过时信息的超时，链路状态数据库即时而非逐步更新。
- 路由决策基于成本，它表明通过特定接口发送数据包所需的开销。 ASA 根据链路带宽而非到目标的跃点数计算接口的成本。可以配置成本来指定首选路径。

最短路径优先算法的缺点是需要大量 CPU 周期和内存。

ASA 可以在不同接口集上同时运行 OSPF 协议的两个进程。如果您具有使用相同 IP 地址的接口（NAT 允许这些接口共存，但是 OSPF 不允许重叠的地址），则可以要运行两个进程。或者，可能要在内部运行一个进程，在外部运行另一个进程，并且在两个进程之间重新分发路由的子集。同样，可能需要将专用地址与公用地址分离。

可以将路由从一个 OSPF 路由进程、 RIP 路由进程或从在启用了 OSPF 的接口上配置的静态路由和已连接路由重新分发到另一个 OSPF 路由进程中。

ASA 支持以下 OSPF 功能：

- 区域内、区域间和外部 （I 类和 II 类）路由。
- 虚拟链路。
- LSA 泛洪。
- OSPF 数据包身份验证 （密码和 MD5 身份验证）。
- 将 ASA 配置为指定路由器或指定备用路由器。 ASA 也可以设置为 ABR。
- 末节区域和次末节区域。
- 区域边界路由器 3 类 LSA 过滤。

OSPF 支持 MD5 和明文邻居身份验证。如有可能，应该将身份验证与所有路由协议配合使用，因为在 OSPF 和其他协议 （如 RIP）之间的路由重新分发可能会被攻击者用于破坏路由信息。

如果使用 NAT，如果 OSPF 是在公共和专用区域上运行，并且如果要求地址过滤，则需要运行两个 OSPF 进程，一个进程对应于公共区域，一个进程对应于专用区域。

在多个区域中具有接口的路由器称为区域边界路由器 (ABR)。充当网关以在使用 OSPF 的路由器之间与使用其他路由协议的路由器之间重新分发流量的路由器称为自治系统边界路由器 (ASBR)。

ABR 使用 LSA 将有关可用路由的信息发送到其他 OSPF 路由器。使用 ABR 3 类 LSA 过滤，可以具有单独的以 ASA 为 ABR 的专用和公共区域。可以将 3 类 LSA（区域间路由）从一个区域过滤到另一个区域，借此能够将 NAT 和 OSPF 一起使用而不通告专用网络。

注　只能过滤 3 类 LSA。如果在专用网络中将 ASA 配置为 ASBR，它将发送描述专用网络的 5 类 LSA，后者会泛洪至整个 AS，包括公共区域。

如果采用 NAT 但 OSPF 仅在公共区域中运行，则可以在专用网络内将公共网络的路由作为默认或 5 类 AS 外部 LSA 重新分发。但是，需要为受 ASA 保护的专用网络配置静态路由。此外，不应在同一 ASA 接口上混用公用和专用网络。

可以同时在 ASA 上运行两个 OSPF 路由进程、一个 RIP 路由进程和一个 EIGRP 路由进程。

快速呼叫数据包 OSPF 支持

快速呼叫数据包 OSPF 支持功能提供在小于 1 秒的间隔内发送呼叫数据包的配置方法。此类配置在开放式最短路径优先 (OSPF) 网络中会导致更快的收敛。

快速呼叫数据包 OSPF 支持的先决条件

OSPF 必须已在网络中进行配置或与快速呼叫数据包 OSPF 支持功能同时配置。

有关快速呼叫数据包 OSPF 支持的信息。

以下各节描述与快速呼叫数据包 OSPF 支持相关的概念：

- OSPF 呼叫间隔和停顿间隔
- OSPF 快速呼叫数据包
- OSPF 快速呼叫数据包的好处

OSPF 呼叫间隔和停顿间隔

OSPF 呼叫数据包是 OSPF 进程向其 OSPF 邻居发送以保持与这些邻居的连接的数据包。呼叫数据包按照可配置间隔 （以秒为单位）进行发送。对于以太网链路，默认值为 10 秒；对于非广播链路，默认值为 30 秒。呼叫数据包包含在停顿间隔内为其接收到呼叫数据包的所有邻居的列表。停顿间隔也是可配置间隔 （以秒为单位），并且默认为呼叫间隔值的四倍。所有呼叫间隔的值在网络中都必须相同。同样，所有停顿间隔的值在网络中也必须都相同。

这两种间隔通过表明链路可运行来保持连接。如果路由器在停顿间隔内没有从邻居接收到呼叫数据包，它将声明该邻居关闭。

OSPF 快速呼叫数据包

OSPF 快速呼叫数据包是指按照小于 1 秒的间隔发送的呼叫数据包。如要了解快速呼叫数据包，您应该已经了解 OSPF 呼叫数据包与停顿间隔之间的关系。请参阅第 22-3 页的 OSPF 呼叫间隔和停顿间隔。

通过使用 **ospf dead-interval** 命令来获取 OSPF 快速呼叫数据包。停顿间隔设置为 1 秒，并且 hello-multiplier 值设置为在该 1 秒期间要发送的呼叫数据包的数量，从而提供亚秒或“快速”呼叫数据包。

当在接口上配置了快速呼叫数据包时，此接口发出的呼叫数据包中通告的呼叫间隔设置为 0。系统将忽略通过此接口接收到的呼叫数据包中的呼叫间隔。

无论停顿间隔设置为 1 秒 （对于快速呼叫数据包）还是设置为任何其他值，它在分段上都必须一致。只要在停顿间隔内发送了至少一个呼叫数据包，呼叫乘数对于整个分段便无需相同。

OSPF 快速呼叫数据包的好处

OSPF 快速呼叫数据包功能的好处是 OSPF 网络将比没有快速呼叫数据包的情况更快收敛。通过此功能可在 1 秒内检测丢失的邻居。它在开放式系统互连 (OSI) 物理层和数据链路层可能未检测到邻居丢失的 LAN 分段中尤其有用。

OSPFv2 与 OSPFv3 之间的实施差异

OSPFv3 不与 OSPFv2 向后兼容。如要使用 OSPF 路由 IPv4 和 IPv6 流量，必须同时运行 OSPFv2 和 OSPFv3。它们会共存但不相互交互。

OSPFv3 提供的其他功能包括：

- 逐条链路进行协议处理。
- 移除寻址语义。
- 添加泛洪范围。
- 支持每条链路多个实例。
- 使用 IPv6 链路本地地址执行网络发现和其他功能。

- 以前缀和前缀长度表示 LSA。
- 添加两种 LSA 类型。
- 处理未知 LSA 类型。
- 使用 OSPFv3 路由协议流量的 IPsec ESP 标准支持身份验证，如 RFC-4552 所指定。

OSPF 准则

情景模式准则

OSPFv2 支持单情景和多情景模式。

OSPFv3 仅支持单情景模式。

防火墙模式准则

OSPF 仅支持路由防火墙模式。 OSPF 不支持透明防火墙模式。

故障转移准则

OSPFv2 和 OSPFv3 支持有状态故障转移。

IPv6 准则

- OSPFv2 不支持 IPv6。
- OSPFv3 支持 IPv6。
- OSPFv3 使用 IPv6 进行身份验证。
- ASA 将 OSPFv3 路由安装到 IPv6 RIB 中，前提是它是最佳路由。
- 可以在 **capture** 命令中使用 IPv6 ACL 滤除 OSPFv3 数据包。

集群准则

- OSPFv2 和 OSPFv3 支持集群。
- 不支持 OSPFv3 加密。如果尝试在集群环境中配置 OSPFv3 加密，系统将显示错误消息。
- 在跨接口模式中，在管理专属接口上不支持动态路由。
- 在单个接口模式中，请确保将主单元和从属单元建立为 OSPFv2 或 OSPFv3 邻居。
- 当配置 OSPFv2 和 EIGRP 时，可以使用跨接口模式或单个接口模式；不能同时使用这两种模式。
- 在单个接口模式中，只能在主单元的共享接口上的两个情景之间建立 OSPFv2 邻接。仅在点对点链路上支持配置静态邻居；因此，在接口上仅允许一个邻居声明。
- 路由器 ID 在 OSPFv2、OSPFv3 和 EIGRP 路由器配置模式中是可选的。如果没有显式设置路由器 ID，则会自动生成路由器 ID 并将其设置为各集群单元中任意数据接口上的最高 IPv4 地址。
- 如果尚未配置集群接口模式，则仅允许将单个点分十进制 IPv4 地址作为路由器 ID，并会禁用 **cluster pool** 选项。
- 如果集群接口模式设置为跨接口配置，则仅允许将单个点分十进制 IPv4 地址作为路由器 ID，并会禁用 **cluster pool** 选项。
- 如果集群接口模式设置为单个接口配置，则必需 **cluster pool** 选项，并且不允许将单个点分十进制 IPv4 地址作为路由器 ID。
- 将集群接口模式从跨接口配置更改为单个接口配置 （反之亦然）而不指定 **check-detail** 或 **nocheck** 选项时，将移除整个配置，包括路由器 ID。

- 如果任何动态路由协议路由器 ID 与新接口模式不兼容，则控制台上会显示错误消息，并且接口模式 CLI 失败。该错误消息中对应于每个动态路由协议（OSPFv2、OSPFv3 和 EIGRP）包含一行内容，并会列出出现不兼容配置时所处的每个情景的名称。
- 如果为 **cluster interface mode** 命令指定 **nocheck** 选项，即使所有路由器 ID 配置可能与新模式不兼容，也允许更改接口模式。
- 启用集群后，将重复路由器 ID 兼容性检查。如果检测到任何不兼容情况，则 **cluster enable** 命令会失败。管理员需要先更正不兼容的路由器 ID 配置，然后才能启用集群。
- 当某个单元作为从属单元进入集群时，建议为 **cluster interface mode** 命令指定 **nocheck** 选项，以避免任何路由器 ID 兼容性检查失败。从属单元仍然从主单元继承路由器配置。
- 当集群中发生主身份角色更改时，将出现以下行为：
  - 在跨接口模式中，路由器进程仅在主单元上处于活动状态，在从属单元上处于挂起状态。各集群单元具有同一路由器 ID，因为已从主单元对配置进行同步。因此，在角色更改期间，相邻路由器不会注意到集群的路由器 ID 发生的任何更改。
  - 在单个接口模式中，路由器进程在所有单个集群单元上都处于活动状态。各集群单元从已配置的集群池中选择其自己独特的路由器 ID。集群中的主身份角色更改不会以任何方式更改路由拓扑。

其他指导原则

- OSPFv2 和 OSPFv3 在接口上支持多个实例。
- OSPFv3 在非集群环境中通过 ESP 头支持加密。
- OSPFv3 支持非负载加密。
- OSPFv2 根据 RFC 4811、4812 和 3623 定义分别支持思科 NSF 无中断重新启动和 IETF NSF 无中断重新启动机制。
- OSPFv3 根据 RFC 5187 定义支持无中断重新启动机制。

配置 OSPFv2

本节描述如何在 ASA 上启用 OSPFv2 进程。

启用 OSPFv2 后，需要定义路由映射。有关详细信息，请参阅第 20-4 页的定义路由映射。然后，生成默认路由。有关详细信息，请参阅第 19-2 页的静态路由配置。

为 OSPFv2 进程定义路由映射后，可以根据特定需要对其进行定制。如要了解任何在 ASA 上定制 OSPFv2 进程，请参阅第 22-7 页的定制 OSPFv2。

如要启用 OSPFv2，需要创建 OSPFv2 路由进程，指定与该路由进程关联的 IP 地址的范围，然后指定与 IP 地址范围关联的区域 ID。

可以启用最多两个 OSPFv2 进程实例。每个 OSPFv2 进程具有其自己的关联区域和网络。

如要启用 OSPFv2，请执行以下步骤：

操作步骤

步骤 1　创建 OSPF 路由进程：

```
router ospf process_id
```

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。可以使用最多两个进程。

如果仅在 ASA 上启用了一个 OSPF 进程，则默认情况下会选择该进程。编辑现有区域时，无法更改 OSPF 进程 ID。

步骤 2 定义 OSPF 运行所在的 IP 地址和该接口的区域 ID：

network *ip_address mask* **area** *area_id*

示例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

添加新区域时，输入区域 ID。可以将区域 ID 指定为十进制数字或 IP 地址。有效十进制值范围为 0 至 4294967295。编辑现有区域时，无法更改区域 ID。

配置 OSPF 快速呼叫数据包

本节描述如何配置 OSPF 快速呼叫数据包。

操作步骤

步骤 1 配置接口：

interface port-channel *number*

示例：

```
ciscoasa(config)# interface port-channel 10
```

number 参数表明端口通道接口号。

步骤 2 设置在其期间必须接收至少一个呼叫数据包，否则会将邻居视为关闭的间隔：

ospf dead-interval minimal hello-multiplier *no.of times*

示例：

```
ciscoasa(config-if)# ospf dead-interval minimal hell0-multiplier 5
ciscoasa
```

no.of times 参数表明每秒要发送的呼叫数据包的数量。有效值介于 3 和 20 之间。

在本示例中，通过指定 minimal 关键字以及 hello-multiplier 关键字和值启用了快速呼叫数据包 OSPF 支持。由于乘数设置为 5，因此每秒将发送五个呼叫数据包。

定制 OSPFv2

本节说明如何定制 OSPFv2 进程。

- 第 22-7 页的将路由重新分发到 OSPFv2 中
- 第 22-9 页的将路由重新分发到 OSPFv2 中时配置路由摘要
- 第 22-10 页的配置 OSPFv2 区域之间的路由摘要
- 第 22-10 页的配置 OSPFv2 接口参数
- 第 22-13 页的配置 OSPFv2 区域参数
- 第 22-13 页的配置 OSPFv2 NSSA
- 第 22-15 页的为集群配置 IP 地址池 （OSPFv2 和 OSPFv3）
- 第 22-15 页的定义静态 OSPFv2 邻居
- 第 22-16 页的配置路由计算计时器
- 第 22-16 页的记录邻居启动或关闭

将路由重新分发到 OSPFv2 中

ASA 可以控制路由在 OSPFv2 路由进程之间的重新分发。

注　如果要通过定义允许将来自指定路由协议的哪些路由重新分发到目标路由进程中来重新分发路由，必须首先生成默认路由。请参阅第 19-2 页的静态路由配置，然后根据第 20-4 页的定义路由映射定义路由映射。

如要将静态、已连接、 RIP 或 OSPFv2 路由重新分发到 OSPFv2 进程中，请执行以下步骤：

操作步骤

步骤 1　创建 OSPF 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。可以使用最多两个进程。

步骤 2　将已连接路由重新分发到 OSPF 路由进程中：

redistribute connected [[**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

示例：

```
ciscoasa(config)# redistribute connected 5 type-1 route-map-practice
```

步骤 3　将静态路由重新分发到 OSPF 路由进程中：

redistribute static [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*

示例：

```
ciscoasa(config)# redistribute static 5 type-1 route-map-practice
```

步骤 4　将路由从一个 OSPF 路由进程重新分发到另一个 OSPF 路由进程中：

redistribute ospf *pid* [**match {internal** | **external** [**1** | **2]** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

示例：

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

可以在此命令中使用 **match** 选项来匹配和设置路由属性，也可以使用路由映射。 **subnets** 选项在 **route-map** 命令中没有等效项。如果在 **redistribute** 命令中同时使用路由映射和 **match** 选项，则其必须匹配。

示例通过将路由与等于 1 的度量相匹配来显示从 OSPF 进程 1 到 OSPF 进程 2 中的路由重新分发。ASA 将这些路由作为度量为 5 且度量类型为 1 类的外部 LSA 重新分发。

步骤 5　将路由从 RIP 路由进程重新分发到 OSPF 路由进程中：

redistribute rip [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

示例：

```
ciscoasa(config)# redistribute rip 5
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

步骤 6　将路由从 EIGRP 路由进程重新分发到 OSPF 路由进程中：

redistribute eigrp *as-num* [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

示例：

```
ciscoasa(config)# redistribute eigrp 2
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

将路由重新分发到 OSPFv2 中时配置路由摘要

将来自其他协议的路由重新分发到 OSPF 中时，将在外部 LSA 中单独通告每个路由。但是，可以将 ASA 配置为对于为指定网络地址和掩码包含的所有重新分发的路由通告单个路由。此配置可减小 OSPF 链路状态数据库的大小。

可以抑制与指定 IP 地址/掩码对相匹配的路由。标记值可用作用于通过路由映射控制重新分发的值。

如要配置路由摘要，可以执行以下操作：

- 第 22-9 页的添加路由摘要地址

添加路由摘要地址

如要在一个摘要路由上配置适用于为网络地址和掩码包含的所有重新分发的路由的软件通告，请执行以下步骤：

操作步骤

步骤 1　创建 OSPF 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。可以使用最多两个进程。

步骤 2　设置摘要地址：

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

示例：

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

在本示例中，摘要地址 10.1.0.0 包含地址 10.1.1.0、10.1.2.0、10.1.3.0，依此类推。在外部链路状态通告中仅通告地址 10.1.0.0。

配置 OSPFv2 区域之间的路由摘要

路由摘要是通告地址的整合。此功能导致通过区域边界路由器向其他区域通告单个摘要路由。在 OSPF 中，区域边界路由器将一个区域中的网络通告到另一个区域中。如果以某种方式分配区域中的网络号来使其连续，则可以将区域编辑路由器配置为通告摘要路由，包括该区域内属于指定范围的所有单独网络。

如要定义摘要路由的地址范围，请执行以下步骤：

操作步骤

步骤 1　创建 OSPF 路由进程并进入此 OSPF 进程的路由器配置模式：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符。它可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。可以使用最多两个进程。

步骤 2　设置地址范围：

area *area-id* range *ip-address mask* [**advertise** | **not-advertise**]

示例：

```
ciscoasa(config-rtr)# area 17 range 12.1.0.0 255.255.0.0
```

在本示例中，地址范围设置在 OSPF 区域之间。

配置 OSPFv2 接口参数

如有必要，可以更改某些特定于接口的 OSPFv2 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：**ospf hello-interval**、**ospf dead-interval**、**ospf authentication-key**。如果配置其中任何参数，请确保网络上所有路由器的配置都具有兼容值。

要配置 OSPFv2 接口参数，请执行以下步骤：

操作步骤

步骤 1　创建 OSPF 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。可以使用最多两个进程。

步骤 2　定义 OSPF 运行所在的 IP 地址和该接口的区域 ID：

network *ip_address mask* **area** *area_id*

示例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

步骤 3　进入接口配置模式：

interface *interface_name*

示例：

```
ciscoasa(config)# interface my_interface
```

步骤 4　指定接口的身份验证类型：

ospf authentication [**message-digest** | **null**]

示例：

```
ciscoasa(config-interface)# ospf authentication message-digest
```

步骤 5　分配要供相邻 OSPF 路由器在使用 OSPF 简单密码身份验证的网段上使用的密码：

ospf authentication-key *key*

示例：

```
ciscoasa(config-interface)# ospf authentication-key cisco
```

key 参数可以是长度最多为 8 字节的任何连续字符串。

当 ASA 软件发出路由协议数据包时，此命令创建的密码用作直接插入到 OSPF 标头中的密钥。可以逐个接口向每个网络分配单独的密码。同一网络上的所有相邻路由器都必须具有同一密码才能交换 OSPF 信息。

步骤 6　明确指定在 OSPF 接口上发送数据包的成本：

ospf cost *cost*

示例：

```
ciscoasa(config-interface)# ospf cost 20
```

cost 是从 1 至 65535 的整数。

在本示例中，cost 设置为 20。

步骤 7　设置设备在因未接收到呼叫数据包而声明邻居 OSPF 路由器关闭之前必须等待的秒数：

ospf dead-interval *seconds*

示例：

```
ciscoasa(config-interface)# ospf dead-interval 40
```

该值必须对于网络上的所有节点都相同。

步骤 8　指定 ASA 在 OSPF 接口上发送呼叫数据包间隔的时间长度：

ospf hello-interval *seconds*

示例：

```
ciscoasa(config-interface)# ospf hello-interval 10
```

该值必须对于网络上的所有节点都相同。

步骤 9 启用 OSPF MD5 身份验证：

ospf message-digest-key *key_id* **md5** *key*

示例：

```
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
```

可以设置以下参数值：

key_id - 范围在 1 至 255 内的标识符。

key - 最多为 16 字节的字母数字密码。

通常，每个接口使用一个密钥在发送数据包时生成身份验证信息并对传入数据包进行身份验证。邻居路由器上的同一密钥标识符必须具有相同密钥值。

我们建议不要每个接口保留多个密钥。每次添加新密钥时，应该移除旧密钥以防止本地系统继续与知道旧密钥的恶意系统进行通信。移除旧密钥还会减少滚动更新期间的开销。

步骤 10 设置优先级以帮助确定网络的 OSPF 指定的路由器：

ospf priority *number_value*

示例：

```
ciscoasa(config-interface)# ospf priority 20
```

number_value 参数范围为 0 至 255。

步骤 11 指定属于 OSPF 接口的邻接的 LSA 重新传输间隔秒数：

ospf retransmit-interval *seconds*

示例：

```
ciscoasa(config-interface)# ospf retransmit-interval seconds
```

seconds 的值必须大于连接的网络上任意两个路由器之间的预期往返延迟。范围为 1 至 8192 秒。默认值为 5 秒。

步骤 12 设置在 OSPF 接口上发送链路状态更新数据包所需的估计秒数。

ospf transmit-delay *seconds*

示例：

```
ciscoasa(config-interface)# ospf transmit-delay 5
```

seconds 值的范围为 1 至 8192 秒。默认值为 1 秒。

步骤 13 设置在 1 秒内发送的呼叫数据包的数量。

ospf dead-interval minimal hello-interval *multiplier*

示例：

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 6
```

有效值是介于 3 和 20 之间的整数。

步骤 14 将接口指定为点对点非广播网络：

```
ospf network point-to-point non-broadcast
```

示例：

```
ciscoasa(config-interface)# ospf network point-to-point non-broadcast
```

将接口指定为点对点和非广播时，必须手动定义 OSPF 邻居；无法实现动态邻居发现。有关详细信息，请参阅第 22-15 页的定义静态 OSPFv2 邻居。此外，在该接口上只能定义一个 OSPF 邻居。

配置 OSPFv2 区域参数

可以配置多个 OSPF 区域参数。这些区域参数 （显示在以下任务列表中）包括设置身份验证，定义末节区域以及向默认摘要路由分配特定成本。身份验证提供基于密码的区域非授权访问防御。

末节区域是有关外部路由的信息未发送到的区域。相反，ABR 生成了到自治系统外部目标的末节区域中的默认外部路由。如要利用 OSPF 末节区域支持，必须在末节区域中使用默认路由。如要进一步减少发送到末节区域中的 LSA 数量，可以在 ABR 上使用 **area stub** 命令的 **no-summary** 关键字，以防止其将摘要链路通告 （3 类 LSA）发送到该末节区域中。

操作步骤

步骤 1　创建 OSPF 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。可以使用最多两个进程。

步骤 2　为 OSPF 区域启用身份验证：

area *area-id* **authentication**

示例：

```
ciscoasa(config-rtr)# area 0 authentication
```

步骤 3　为 OSPF 区域启用 MD5 身份验证：

area *area-id* **authentication message-digest**

示例：

```
ciscoasa(config-rtr)# area 0 authentication message-digest
```

配置 OSPFv2 NSSA

NSSA 的 OSPFv2 实施类似于 OSPFv2 末节区域。 NSSA 不会将 5 类外部 LSA 从核心泛洪至该区域中，但是可在区域内以有限的方法导入自治系统外部路由。

NSSA 通过重新分发在 NSSA 区域内导入 7 类自治系统外部路由。这些 7 类 LSA 由 NSSA ABR 转换为在整个路由域中泛洪的 5 类 LSA。在转换期间支持摘要和过滤。

如果您是必须将使用 OSPFv2 的中心站点连接到对 NSSA 使用其他路由协议的远程站点的 ISP 或网络管理员，则可以简化管理。

在 NSSA 实施前，企业站点边界路由器和远程路由器之间的连接不能作为 OSPFv2 末节区域运行，因为远程站点的路由无法重新分发到末节区域中，并且需要保持两种路由协议。通常会运行简单协议 （如 RIP）并使用其处理重新分发。在使用 NSSA 的情况下，可以通过将企业路由器和远程路由器之间的区域定义为 NSSA 来将 OSPFv2 扩展至覆盖远程连接。

使用此功能之前，请遵循以下准则：

- 可以设置用于到达外部目标的 7 类默认路由。配置时，路由器会生成到 NSSA 或 NSSA 区域边界路由器中的 7 类默认路由。
- 同一区域内的每个路由器都必须同意区域为 NSSA；否则，路由器无法相互通信。

操作步骤

步骤 1　创建 OSPF 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是此路由进程的内部使用的标识符。它可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。可以使用最多两个进程。

步骤 2　定义 NSSA 区域：

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate**]

示例：

```
ciscoasa(config-rtr)# area 0 nssa
```

步骤 3　设置摘要地址，帮助减小路由表的大小：

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

示例：

```
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

对 OSPF 使用此命令会导致 OSPF ASBR 将一个外部路由通告为该地址覆盖的所有重新分发的路由的聚合。

在本示例中，摘要地址 10.1.0.0 包含地址 10.1.1.0、10.1.2.0、10.1.3.0，依此类推。在外部链路状态通告中仅通告地址 10.1.0.0。

注　OSPF 不支持摘要地址 0.0.0.0 0.0.0.0。

为集群配置 IP 地址池 （OSPFv2 和 OSPFv3）

如果使用的是单个接口集群，则可以为路由器 ID 集群池分配 IPv4 地址范围。

操作步骤

如要为 OSPFv2 和 OSPFv3 的单个接口集群中的路由器 ID 集群池分配 IPv4 地址范围，请输入以下命令：

步骤 1　指定单个接口集群的路由器 ID 集群池：

router-id cluster-pool hostname | **A.B.C.D** *ip_pool*

示例：

```
hostname(config)# ip local pool rpool 1.1.1.1-1.1.1.4
hostname(config)# router ospf 1
hostname(config-rtr)# router-id cluster-pool rpool
hostname(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
hostname(config-rtr)# log-adj-changes
```

在配置了单个接口集群时，**cluster-pool** 关键字会启用 IP 地址池的配置。**hostname** | **A.B.C.D.**关键字指定此 OSPF 进程的 OSPF 路由器 ID。 *ip_pool* 参数指定 IP 地址池的名称。

注　如果使用的是集群，则无需指定路由器 ID 的 IP 地址池。如果未配置 IP 地址池，则 ASA 使用自动生成的路由器 ID。

定义静态 OSPFv2 邻居

需要定义静态 OSPFv2 邻居来通过点对点非广播网络通告 OSPFv2 路由。通过此功能，可以跨现有 VPN 连接广播 OSPFv2 通告，而不必将通告封装在 GRE 隧道中。

开始之前，必须创建到 OSPFv2 邻居的静态路由。有关创建静态路由的详细信息，请参阅第 19 章，“静态路由和默认路由”。

操作步骤

详细步骤

	步骤 2	用途	命令
步骤 1	**步骤 3** **步骤 4**	创建 OSPFv2 路由进程并进入此 OSPFv2 进程的路由器配置模式： *process_id* 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。可以使用最多两个进程。	**router ospf** *process_id* `ciscoasa(config)# router ospf 2`

	步骤 2	用途	命令
步骤 2	步骤 5 步骤 6	定义 OSPFv2 邻近区域： *addr* 参数是 OSPFv2 邻居的 IP 地址。*if_name* 参数是用于与邻居进行通信的接口。如果 OSPFv2 邻居与任何直接连接的接口不在同一网络上，则必须指定接口。	**neighbor** *addr* [**interface** *if_name*] ciscoasa(config-rtr)# neighbor 255.255.0.0 [interface my_interface]

配置路由计算计时器

可以配置 OSPFv2 接收拓扑更改时与其启动 SPF 计算时之间的延迟时间。您还可以配置两次连续 SPF 计算之间的保持时间。

如要配置路由计算计时器，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router ospf** *process_id* **示例：** ciscoasa(config)# router ospf 2	创建 OSPFv2 路由进程并进入此 OSPFv2 进程的路由器配置模式。 *process_id* 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。可以使用最多两个进程。
步骤 2	**timers throttle spf** *spf-start spf-hold spf-maximum* **示例：** ciscoasa(config-router)# timers throttle spf 500 500 600	配置路由计算时间。 *spf-start* 参数是 OSPF 接收拓扑更改时和其启动 SPF 计算时之间的延迟时间 （以毫秒为单位）。它可以是介于 0 和 600000 之间的整数。 *spf-hold* 参数是两次连续 SPF 计算间隔的最短时间 （以毫秒为单位）。它可以是介于 0 和 600000 之间的整数。 *spf-maximum* 参数是两次连续 SPF 计算间隔的最长时间 （以毫秒为单位）。它可以是介于 0 和 600000 之间的整数。

记录邻居启动或关闭

默认情况下，在 OSPFv2 邻居启动或关闭时会生成系统日志消息。

如果要知道 OSPFv2 邻居是启动还是关闭而不开启 **debug ospf adjacency** 命令，请配置 **log-adj-changes** 命令。 **log-adj-changes** 命令使用更少的输出提供对等关系的高级视图。如果要查看各状态更改的消息，请配置 **log-adj-changes detail** 命令。

如要记录 OSPFv2 邻居启动或关闭，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router ospf** *process_id* **示例：** `ciscoasa(config)# router ospf 2`	创建 OSPFv2 路由进程并进入此 OSPFv2 进程的路由器配置模式。 *process_id* 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。可以使用最多两个进程。
步骤 2	**log-adj-changes** [**detail**] **示例：** `ciscoasa(config-rtr)# log-adj-changes [detail]`	为启动或关闭的邻居配置日志记录。

配置 OSPFv3

本部分描述如何配置 OSPFv3 路由进程。

- 第 22-18 页的启用 OSPFv3
- 第 22-18 页的配置 OSPFv3 接口参数
- 第 22-23 页的配置 OSPFv3 路由器参数
- 第 22-25 页的配置 OSPFv3 区域参数
- 第 22-26 页的配置 OSPFv3 被动接口
- 第 22-27 页的配置 OSPFv3 管理距离
- 第 22-27 页的配置 OSPFv3 计时器
- 第 22-30 页的定义静态 OSPFv3 邻居
- 第 22-31 页的重置 OSPFv3 默认参数
- 第 22-31 页的发送系统日志消息
- 第 22-32 页的抑制系统日志消息
- 第 22-32 页的计算摘要路由成本
- 第 22-32 页的生成到 OSPFv3 路由域中的默认外部路由
- 第 22-33 页的配置 IPv6 摘要前缀
- 第 22-34 页的重新分发 IPv6 路由

启用 OSPFv3

如要启用 OSPFv3，需要创建 OSPFv3 路由进程，创建 OSPFv3 的区域，启用 OSPFv3 的接口，然后将路由重新分发到目标 OSPFv3 路由进程中。

如要启用 OSPFv3，输入以下命令或执行以下步骤：

命令	用途
ipv6 router ospf *process-id* **示例：** `ciscoasa(config)# ipv6 router ospf 10`	创建 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process_id* 参数是此路由进程的内部使用的标记，可以是任何正整数。此标记不必与任何其他设备上的标记匹配；它仅供内部使用。可以使用最多两个进程。

	命令	用途
步骤 1	**interface** *interface_name* **示例：** `ciscoasa(config)# interface Gigabitethernet0/0`	启用接口。
步骤 2	**ipv6 ospf** *process-id* **area** *area_id* **示例：** `ciscoasa(config)# ipv6 ospf 200 area 100`	创建具有指定进程 ID 的 OSPFv3 路由进程和具有指定区域 ID 的 OSPFv3 区域。

配置 OSPFv3 接口参数

如有必要，可以更改某些特定于接口的 OSPFv3 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：**ipv6 ospf hello-interval** 和 **ipv6 ospf dead-interval**。如果配置其中任何参数，请确保网络上所有路由器的配置都具有兼容值。

如要为 IPv6 配置 OSPFv3 接口参数，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 10`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process_id* 参数是此路由进程的内部使用的标记，可以是任何正整数。此标记不必与任何其他设备上的标记匹配；它仅供内部使用。可以使用最多两个进程。

	命令	用途
步骤 2	**ipv6 ospf area** [*area-num*] [**instance**] **示例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200	创建 OSPFv3 区域。 *area-num* 参数是要为其启用身份验证的区域，可以是十进制值或 IP 地址。 **instance** 关键字指定要分配给接口的区域实例 ID。接口只能有一个 OSPFv3 区域。可以在多个接口上使用同一区域，并且每个接口可以使用不同的区域实例 ID。
步骤 3	执行下列操作之一以配置 OSPFv3 接口参数：	
	ipv6 ospf cost *interface-cost* **示例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200	显式指定在接口上发送数据包的成本。 *interface-cost* 参数指定表示为链路状态度量的无符号整数值，其值的范围可以为 1 至 65535。默认成本基于带宽。
	ipv6 ospf database-filter all out **示例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf database-filter all out	过滤到 OSPFv3 接口的传出 LSA。默认情况下，所有传出 LSA 都泛洪至该接口。

命令	用途
ipv6 ospf dead-interval *seconds* **示例：** `ciscoasa(config-if)# interface GigabitEthernet3/2.200` `vlan 200` `nameif outside` `security-level 100` `ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31` `ipv6 address 3001::1/64 standby 3001::8` `ipv6 address 6001::1/64 standby 6001::8` `ipv6 enable` `ospf priority 255` `ipv6 ospf cost 100` `ipv6 ospf 100 area 10 instance 200` `ipv6 ospf dead-interval 60`	设置在邻居表明路由器关闭之前不得查看呼叫数据包的时间段 （以秒为单位）。该值必须对于同一网络上的所有节点都相同，并且范围可以是 1 至 65535。默认值是 **ipv6 ospf hello-interval** 命令设置的间隔的四倍。
ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [[*key-encryption-type*] *key* | **null**} **示例：** `ciscoasa(config-if)# interface GigabitEthernet3/2.200` `vlan 200` `nameif outside` `security-level 100` `ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31` `ipv6 address 3001::1/64 standby 3001::8` `ipv6 address 6001::1/64 standby 6001::8` `ipv6 enable` `ospf priority 255` `ipv6 ospf cost 100` `ipv6 ospf 100 area 10 instance 200` `ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D`	指定接口的加密类型。**ipsec** 关键字指定 IP 安全协议。**spi** *spi* 关键字参数对指定安全策略索引，它必须在范围 256 至 42949667295 内并以十进制形式输入。 **esp** 关键字指定封装安全负载。 *encryption-algorithm* 算法参数指定要与 ESP 配合使用的加密算法。有效值包括： • aes-cdc - 启用 AES-CDC 加密。 • 3des - 启用 3DES 加密。 • des - 启用 DES 加密。 • null - 指定不带加密的 ESP。 *key-encryption-type* 参数可以是以下两个值之一： • 0 - 密钥未加密。 • 7 - 密钥已加密。 *key* 参数指定消息摘要计算中使用的数字。该数字长度为 32 个十六进制数字 （16 字节）。密钥的大小取决于使用的加密算法。通过某些协议 （如 AES-CDC）可以选择密钥的大小。 *authentication-algorithm* 参数指定要使用的加密身份验证算法，可以是以下之一： • md5 - 启用消息摘要 5 (MD5)。 • sha1 - 启用 SHA-1。 **null** 关键字覆盖区域加密。 **注** 如果在接口上启用了 OSPFv3 加密且邻居位于其他区域（例如，区域 0）上，并且您希望 ASA 与该区域形成邻接，则必须更改 ASA 上的区域。将 ASA 上的区域更改为 0 之后，在 OSPFv3 邻接形成之前有一个两分钟的延迟。

命令	用途
ipv6 ospf flood-reduction **示例：** `ciscoasa(config-if)# interface GigabitEthernet3/2.200` `vlan 200` `nameif outside` `security-level 100` `ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31` `ipv6 address 3001::1/64 standby 3001::8` `ipv6 address 6001::1/64 standby 6001::8` `ipv6 enable` `ospf priority 255` `ipv6 ospf cost 100` `ipv6 ospf 100 area 10 instance 200` `ipv6 ospf flood reduction`	指定减少到接口的 LSA 泛洪。
ipv6 ospf hello-interval *seconds* **示例：** `ciscoasa(config-if)# interface GigabitEthernet3/2.200` `vlan 200` `nameif outside` `security-level 100` `ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31` `ipv6 address 3001::1/64 standby 3001::8` `ipv6 address 6001::1/64 standby 6001::8` `ipv6 enable` `ospf priority 255` `ipv6 ospf cost 100` `ipv6 ospf 100 area 10 instance 200` `ipv6 ospf hello-interval 15`	指定接口上发送的呼叫数据包之间的间隔 （以秒为单位）。该值必须对于特定网络上的所有节点都相同，并且范围可以是 1 至 65535。默认间隔对于以太网接口为 10 秒，对于非广播接口为 30 秒。
ipv6 ospf mtu-ignore **示例：** `ciscoasa(config-if)# interface GigabitEthernet3/2.200` `vlan 200` `nameif outside` `security-level 100` `ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31` `ipv6 address 3001::1/64 standby 3001::8` `ipv6 address 6001::1/64 standby 6001::8` `ipv6 enable` `ospf priority 255` `ipv6 ospf cost 100` `ipv6 ospf 100 area 10 instance 200` `ipv6 ospf mtu-ignore`	接收到 DBD 数据包后，禁用 OSPF MTU 不匹配检测。默认情况下，会启用 OSPF MTU 不匹配检测。

命令	用途
ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**} **示例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf network point-to-point non-broadcast	将 OSPF 网络类型设置为除默认以外的其他类型，具体取决于网络类型。 **point-to-point non-broadcast** 关键字将网络类型设置为点对点非广播。 **broadcast** 关键字将网络类型设置为广播。
ipv6 ospf priority *number-value* **示例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf priority 4	设置路由器优先级，这有助于为网络确定指定的路由器。有效值范围为 0 至 255。
ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**] **示例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01	配置与非广播网络的 OSPFv3 路由器互连。

命令	用途
ipv6 ospf retransmit-interval *seconds* **示例：** `ciscoasa(config-if)# interface GigabitEthernet3/2.200` `vlan 200` `nameif outside` `security-level 100` `ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31` `ipv6 address 3001::1/64 standby 3001::8` `ipv6 address 6001::1/64 standby 6001::8` `ipv6 enable` `ospf priority 255` `ipv6 ospf cost 100` `ipv6 ospf 100 area 10 instance 200` `ipv6 ospf retransmit-interval 8`	指定属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）。该时间必须大于连接的网络上任意两个路由器之间的预期往返延迟。有效值范围为 1 至 65535 秒。默认值为 5 秒。
ipv6 ospf transmit-delay *seconds* **示例：** `ciscoasa(config-if)# interface GigabitEthernet3/2.200` `vlan 200` `nameif outside` `security-level 100` `ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31` `ipv6 address 3001::1/64 standby 3001::8` `ipv6 address 6001::1/64 standby 6001::8` `ipv6 enable` `ospf priority 255` `ipv6 ospf cost 100` `ipv6 ospf 100 area 10 instance 200` `ipv6 ospf retransmit-delay 3`	设置在接口上发送链路状态更新数据包所需的估计时间（以秒为单位）。有效值范围为 1 至 65535 秒。默认值为 1 秒。

配置 OSPFv3 路由器参数

如要为 IPv6 配置 OSPFv3 路由器参数，请执行以下步骤：

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config)# ipv6 router ospf 10`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	执行下列操作之一以配置可选 OSPFv3 接口参数：	
	`area` **示例：** `ciscoasa(config-rtr)# area 10`	配置 OSPFv3 区域参数。支持的参数包括从 0 至 4294967295 的十进制值形式的区域 ID 和 IP 地址格式 **A.B.C.D** 的区域 ID。

命令	用途
default **示例：** `ciscoasa(config-rtr)# default originate`	将命令设置为其默认值。 **originate** 参数分发默认路由。
default-information **示例：** `ciscoasa(config-rtr)# default-information`	控制默认信息的分发。
distance **示例：** `ciscoasa(config-rtr)# distance 200`	根据路由类型定义 OSPFv3 路由管理距离。支持的参数包括值为 1 至 254 的管理距离和 OSPFv3 距离的 **ospf**。
`exit` **示例：** `ciscoasa(config-rtr)# exit`	从 IPv6 路由器配置模式中退出。
ignore **示例：** `ciscoasa(config-rtr)# ignore lsa`	当路由器接收 6 类多播 OSPF (MOSPF) 数据包的链路状态通告 (LSA) 时，抑制使用 **lsa** 参数发送系统日志消息。
log-adjacency-changes **示例：** `ciscoasa(config-rtr)#` `log-adjacency-changes detail`	将路由器配置为在 OSPFv3 邻居启动或关闭时发送系统日志消息。通过 **detail** 参数，将会记录所有状态更改。
passive-interface [*interface_name*] **示例：** `ciscoasa(config-rtr)# passive-interface` `inside`	抑制在接口上发送和接收路由更新。*interface_name* 参数指定 OSPFv3 进程运行所在的接口的名称。
redistribute **示例：** `ciscoasa(config-rtr)# redistribute ospf`	根据以下参数配置从一个路由域到另一个路由域的路由的重新分发： • **connected** - 指定连接的路由。 • **ospf** - 指定 OSPFv3 路由。 • **static** - 指定静态路由。
router-id **示例：** `ciscoasa(config-rtr)# router-id 10.1.1.1`	使用以下参数为指定进程创建固定路由器 ID： • **A.B.C.D** - 以 IP 地址格式指定 OSPF 路由器 ID。 • **cluster-pool** - 在配置了单个接口集群时配置 IP 地址池。有关集群中使用的 IP 地址池的详细信息，请参阅第 22-15 页的为集群配置 IP 地址池（OSPFv2 和 OSPFv3）。

命令	用途
summary-prefix **示例：** `ciscoasa(config-if)# ipv6 router ospf 1` `ciscoasa(config-router)# router-id 192.168.3.3` `ciscoasa(config-router)# summary-prefix FECO::/24` `ciscoasa(config-router)# redistribute static`	配置有效值为 0 至 128 的 IPv6 地址摘要。 **X:X:X:X::X/** 参数指定 IPv6 前缀。
timers **示例：** `ciscoasa(config)# ipv6 router ospf 10` `ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000`	调整路由计时器。路由计时器参数如下： • **lsa** - 指定 OSPFv3 LSA 计时器。 • **pacing** - 指定 OSPFv3 步调设置计时器。 • **throttle** - 指定 OSPFv3 调速计时器。

配置 OSPFv3 区域参数

如要配置 OSPFv3 区域参数，请执行以下步骤：

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	执行下列操作之一以配置可选 OSPFv3 区域参数：	
	area *area-id* **default-cost** *cost* **示例：** `ciscoasa(config-rtr)# area 1 default-cost nssa`	设置 NSSA 区域或末节区域的摘要默认成本。
	area *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise** | **not advertise**] [**cost** *cost*] **示例：** `ciscoasa(config-rtr)# area 1 range FE01:1::1/64`	仅汇总与边界路由器的地址和掩码匹配的路由。 *area-id* 参数标识要为其汇总路由的区域。值可以指定为十进制或 IPv6 前缀。*ipv6-prefix* 参数指定 IPv6 前缀。*prefix-length* 参数指定前缀长度。 **advertise** 关键字将地址范围状态设置为已通告并生成 3 类摘要 LSA。 **not-advertise** 关键字将地址范围状态设置为 DoNotAdvertise。系统会抑制 3 类摘要 LSA，并且组件网络对于其他网络保持隐藏状态。 **cost** *cost* 关键字/参数对指定摘要路由的度量或成本，它在 OSPF SPF 计算期间用于确定目标的最短路径。有效值范围为 0 至 16777215。
	area *area-id* **nssa** **示例：** `ciscoasa(config-rtr)# area 1 nssa`	指定 NSSA 区域。

命令	用途
area *area-id* **stub** **示例：** `ciscoasa(config-rtr)# area 1 stub`	指定末节区域。
area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*] **示例：** `ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello-interval 5`	定义虚拟链路及其参数。 *area-id* 参数标识要为其汇总路由的区域。 **virtual link** 关键字指定创建虚拟链路邻居。 *router-id* 参数指定与虚拟链路邻居关联的路由器 ID。输入 **show ospf** or **show ipv6 ospf** 命令以显示路由器 ID。没有默认值。 **hello-interval** 关键字指定在接口上发送的呼叫数据包的间隔时间 （以秒为单位）。呼叫数据包间隔是将在呼叫数据包中通告的无符号整数。该值必须对于连接到公用网络的所有路由器和接入服务器都相同。有效值范围为 1 至 8192。默认值为 10。 **retransmit-interval** *seconds* 关键字/参数对指定属于接口的邻接的 LSA 重新传输的间隔时间 （以秒为单位）。重新传输间隔是连接的网络上任意两个路由器之间的预期往返延迟。该值必须大于预期往返延迟，并且范围可以为 1 至 8192。默认值为 5。 **transmit-delay** *seconds* 关键字/参数对指定在接口上发送链路状态更新数据包所需的估计时间 （以秒为单位）。整数值必须大于零。更新数据包中的 LSA 在传输之前会按此数量递增其自己的年龄。值的范围可以是从 1 至 8192。默认值为 1。 **dead-interval** *seconds* 关键字/参数对指定在邻居表明路由器关闭之前不得查看呼叫数据包的时间 （以秒为单位）。停顿间隔是无符号整数。默认值是呼叫间隔的四倍 （或 40 秒）。该值必须对于连接到公用网络的所有路由器和接入服务器都相同。有效值范围为 1 至 8192。 **ttl-security hops** 关键字在虚拟链路上配置生存时间 (TTL) 安全。 *hop-count* 参数值范围可以为 1 至 254。

配置 OSPFv3 被动接口

如要配置 OSPFv3 被动接口，请执行以下步骤：

	命令	用途
步骤 1	**ipv6 router ospf** *process_id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	**passive-interface** [*interface_name*] **示例：** `ciscoasa(config-rtr)# passive-interface inside`	抑制在接口上发送和接收路由更新。*interface_name* 参数指定 OSPFv3 进程运行所在的接口的名称。如果指定了 *no interface_name* 参数，则 OSPFv3 进程 *process_id* 的所有接口都变为被动接口。

配置 OSPFv3 管理距离

如要为 IPv6 路由配置 OSPFv3 管理距离，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process_id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	**distance** [**ospf** {**external** | **inter-area** | **intra-area**}] *distance* **示例：** `ciscoasa(config-rtr)# distance ospf external 200`	设置 OSPFv3 路由的管理距离。 **ospf** 关键字指定 OSPFv3 路由。**external** 关键字指定 OSPFv3 的外部 5 类和 7 类路由。**inter-area** 关键字指定 OSPVv3 的区域间路由。 **intra-area** 关键字指定 OSPFv3 的区域内路由。*distance* 参数指定管理距离，它是从 10 至 254 的整数。

配置 OSPFv3 计时器

可以为 OSPFv3 设置 LSA 到达计时器、 LSA 步调设置计时器和调速计时器。

如要设置 ASA 接受来自 OSPFv3 邻居的同一 LSA 的最短间隔，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	**timers lsa arrival** *milliseconds* **示例：** `ciscoasa(config-rtr)# timers lsa arrival 2000`	设置 ASA 接受来自 OSPF 邻居的同一 LSA 的最小间隔。 *milliseconds* 参数指定前后两次接受从邻居到达的同一 LSA 之间必须经过的最小延迟 （以毫秒为单位）。范围为 0 至 6,000,000 毫秒。默认值为 1000 毫秒。

如要配置 LSA 泛洪数据包步调设置，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	**timers pacing flood** *milliseconds* **示例：** `ciscoasa(config-rtr)# timers lsa flood 20`	配置 LSA 泛洪数据包步调设置。 *milliseconds* 参数指定在前后两次更新之间泛洪队列中的 LSA 设置步调的间隔时间 （以毫秒为单位）。可配置范围为 5 至 100 毫秒。默认值为 33 毫秒。

如要更改将 OSPFv3 LSA 收集到组中并刷新、校验和或老化的间隔，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	**timers pacing lsa-group** *seconds* **示例：** `ciscoasa(config-rtr)# timers pacing lsa-group 300`	更改将 OSPFv3 LSA 收集到组中并刷新、校验和或老化的间隔。 *seconds* 参数指定将 LSA 分组、刷新、校验和或老化的间隔秒数。范围为 10 至 1800 秒。默认值为 240 秒。

如要配置 LSA 重新传输数据包步调设置，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	**timers pacing retransmission** *milliseconds* **示例：** `ciscoasa(config-rtr)# timers pacing retransmission 100`	配置 LSA 重新传输数据包步调设置。 *milliseconds* 参数指定重新传输队列中的 LSA 设置步调的间隔时间 （以毫秒为单位）。可配置范围为 5 至 200 毫秒。默认值为 66 毫秒。

LSA 和 SPF 调速提供一种动态机制在网络不稳定期间降低 OSPFv3 中的 LSA 更新速度，并通过提供 LSA 速率限制 （以毫秒为单位）允许更快的 OSPFv3 收敛。

如要配置 LSA 和 SPF 调速计时器，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	选择以下选项之一：	
	timers throttle lsa *milliseconds1 milliseconds2 milliseconds3* **示例：** `ciscoasa(config-rtr)# timers throttle lsa 500 6000 8000`	配置 OSPFv3 LSA 调速。 *milliseconds1* 参数指定生成 LSA 的第一次出现所需的延迟（以毫秒为单位）。*milliseconds2* 参数指定发起同一 LSA 所需的最大延迟 （以毫秒为单位）。 *milliseconds3* 参数指定发起同一 LSA 所需的最小延迟 （以毫秒为单位）。 对于 LSA 调速，如果最小时间或最大时间小于第一次出现值，则 OSPFv3 会自动更正为第一次出现值。同样，如果指定的最大延迟小于最小延迟，则 OSPFv3 会自动更正为最小延迟值。 LSA 调速的默认值如下： • 对于 *milliseconds1*，默认值为 0 毫秒。 • 对于 *milliseconds2* 和 *milliseconds3*，默认值为 5000 毫秒。

命令	用途
timers throttle spf *milliseconds1 milliseconds2 milliseconds3* **示例：** `ciscoasa(config-rtr)# timers throttle spf 5000 12000 16000`	配置 OSPFv3 SPF 调速。 *milliseconds1* 参数指定接收对 SPF 计算的更改所需的延迟（以毫秒为单位）。 *milliseconds2* 参数指定第一次和第二次 SPF 计算之间的延迟 （以毫秒为单位）。 *milliseconds3* 参数指定 SPF 计算的最长等待时间 （以毫秒为单位）。 对于 SPF 调速，如果 *milliseconds2* 或 *milliseconds3* 小于 *milliseconds1*，则 OSPFv3 会自动更正为 *milliseconds1* 值。同样，如果 *milliseconds3* 小于 *milliseconds2*，则 OSPFv3 自动更正为 *milliseconds2* 值。 SPF 调速的默认值如下： • 对于 *milliseconds1*，默认值为 5000 毫秒。 • 对于 *milliseconds2* 和 *milliseconds3*，默认值为 10000 毫秒。

定义静态 OSPFv3 邻居

需要定义静态 OSPFv3 邻居来通过点对点非广播网络通告 OSPF 路由。通过此功能，可以跨现有 VPN 连接广播 OSPFv3 通告，而不必将通告封装在 GRE 隧道中。

开始之前，必须创建到 OSPFv3 邻居的静态路由。有关创建静态路由的详细信息，请参阅第 19 章，“静态路由和默认路由”。

如要定义静态 OSPFv3 邻居，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	**ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**] **示例：** `ciscoasa(config-if)# interface ethernet0/0` `ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01`	配置与非广播网络的 OSPFv3 路由器互连。

重置 OSPFv3 默认参数

如要将 OSPFv3 参数还原为其默认值，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	**default** [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **discard-route** | **distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**] **示例：** `ciscoasa(config-rtr)# default metric 5`	将可选参数还原为其默认值。 **area** 关键字指定 OSPFv3 区域参数。**auto-cost** 关键字根据带宽指定 OSPFv3 接口成本。 **default-information** 关键字分发默认信息。 **default-metric** 关键字指定重新分发的路由的度量。**discard-route** 关键字启用或禁用丢弃安装路由。 **distance** 关键字指定管理距离。 **distribute-list** 关键字过滤路由更新中的网络。 **ignore** 关键字忽略特定事件。 **log-adjacency-changes** 关键字记录邻接状态中的记录。 **maximum-paths** 关键字通过多个路径转发数据包。**passive-interface** 关键字在接口上抑制路由更新。 **redistribute** 关键字重新分发来自其他路由协议的 IPv6 前缀。 **router-id** 关键字指定所指定路由进程的路由器 ID。 **summary-prefix** 关键字指定 IPv6 摘要前缀。 **timers** 关键字指定 OSPFv3 计时器。

发送系统日志消息

如要将路由器配置为在 OSPFv3 邻居启动或关闭时发送系统日志消息，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	**log-adjacency-changes** [**detail**] **示例：** `ciscoasa(config-rtr)# log-adjacency-changes detail`	将路由器配置为在 OSPFv3 邻居启动或关闭时发送系统日志消息。 **detail** 关键字为每个状态发送系统日志消息，而不只是在 OSPFv3 启动或关闭时才发送系统日志消息。

抑制系统日志消息

如要在路由器接收不受支持的 LSA 6 类多播 OSPF (MOSPF) 数据包时抑制发送系统日志消息，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router ospf** *process_id* **示例：** `ciscoasa(config-if)# router ospf 1`	启用 OSPFv2 路由进程并进入路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	**ignore lsa mospf** **示例：** `ciscoasa(config-rtr)# ignore lsa mospf`	当路由器接收不受支持的 LSA 6 类 MOSPF 数据包时，抑制发送系统日志消息。

计算摘要路由成本

如要根据 RFC 1583 计算摘要路由成本，请输入以下命令：

命令	用途
compatible rfc1583 **示例：** `ciscoasa (config-rtr)# compatible rfc1583`	还原用于根据 RFC 1583 计算摘要路由成本的方法。

生成到 OSPFv3 路由域中的默认外部路由

如要生成到 OSPFv3 路由域中的默认路由，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。

	命令	用途
步骤 2	**default-information originate** [**always**] **metric** *metric-value* [**metric-type** *type-value*] [**route-map** *map-name*] **示例：** `ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2`	生成到 OSPFv3 路由域中的默认外部路由。 **always** 关键字通告默认路由（无论默认路由是否存在）。**metric** *metric-value* 关键字/参数对指定用于生成默认路由的度量。如果不使用 **default - metric** 命令指定值，则默认值为 10。有效度量值范围为 0 至 16777214。 **metric-type** *type-value* 关键字/参数对指定与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。有效值可以是以下之一： • 1 - 1 类外部路由 • 2 - 2 类外部路由 默认为 2 类外部路由。**route-map** *map-name* 关键字/参数对指定在满足路由映射的情况下生成默认路由的路由进程。

配置 IPv6 摘要前缀

如要配置 IPv6 摘要前缀，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	**summary-prefix** *prefix* [**not-advertise** | **tag** *tag-value*] **示例：** `ciscoasa(config-if)# ipv6 router ospf 1` `ciscoasa(config-rtr)# router-id 192.168.3.3` `ciscoasa(config-rtr)# summary-prefix FECO::/24` `ciscoasa(config-rtr)# redistribute static`	配置 IPv6 摘要前缀。 *prefix* 参数是目标的 IPv6 路由前缀。 **not-advertise** 关键字抑制与指定前缀/掩码对匹配的路由。此关键字仅适用于 OSPFv3。 **tag** *tag-value* 关键字/参数对指定可用作通过路由映射控制重新分发的匹配值的标记值。此关键字仅适用于 OSPFv3。

重新分发 IPv6 路由

如要将已连接路由重新分发到 OSPFv3 进程中，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ipv6 router ospf** *process-id* **示例：** `ciscoasa(config-if)# ipv6 router ospf 1`	启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。 *process-id* 参数是此路由进程的内部使用的标识符，以本地方式分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。可以使用最多两个进程。
步骤 2	**redistribute** *source-protocol* [*process-id*] [**include-connected** {[**level-1** | **level-2**}] [*as-number*] [**metric** [*metric-value* | **transparent**}] **[metric-type** *type-value*] [**match** {**external** [**1**|**2**] | **internal** | **nssa-external** [**1**|**2**]}] [**tag** *tag-value*] [**route-map** *map-tag*] **示例：** `ciscoasa(config-rtr)# redistribute connected 5 type-1`	将 IPv6 路由从一个 OSPFv3 进程重新分发到另一个 OSPFv3 进程中。 *source-protocol* 参数指定从其重新分发路由的源协议，可以为 static、connected 或 OSPFv3。*process-id* 参数是在启用了 OSPFv3 路由进程时以管理方式分配的数字。**include-connected** 关键字允许目标协议重新分发源协议获知的路由以及源协议运行所在的接口上的已连接前缀。**level-1** 关键字指定对于中间系统对中间系统 (IS-IS)，1 级路由独立重新分发到其他 IP 路由协议中。**level-1-2** 关键字指定对于 IS-IS，1 级和 2 级路由均重新分发到其他 IP 路由协议中。**level-2** 关键字指定对于 (IS-IS)，2 级路由独立重新分发到其他 IP 路由协议中。对于 **metric** *metric-value* 关键字参数对，当在同一路由器上将路由从一个 OSPFv3 进程重新分发到另一个 OSPFv3 进程时，如果未指定度量值，则会将度量从一个进程携带至另一个进程。将其他进程重新分发到 OSPFv3 进程时，如果未指定度量值，则默认度量值为 20。**metric transparent** 关键字导致 RIP 使用重新分发的路由的路由表度量为 RIP 度量。**metric-type** *type-value* 关键字/参数对指定与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。有效值可以是以下之一：1（表示 1 类外部路由）或 2（表示 2 类外部路由）。如果没有为 **metric-type** 关键字指定任何值，则 ASA 采用 2 类外部路由。对于 IS-IS，链路类型可以是以下之一：内部（适用于小于 63 的 IS-IS 度量）或外部（适用于大于 64 且小于 128 的 IS-IS 度量）。默认为内部。**match** 关键字将路由重新分发到其他路由域中并与以下选项之一配合使用：**external [1|2]**，表示自治系统的外部路由，但会作为 1 类或 2 类外部路由导入到 OSPFv3 中；**internal**，表示特定自治系统的内部路由；**nssa-external [1|2]**，表示自治系统的外部路由，但会在 IPv6 的 NSSA 中作为 1 类或 2 类外部路由导入到 OSPFv3 中。**tag** *tag-value* 关键字/参数对指定连接到每个外部路由的 32 位十进制值，它可用于在 ASBR 之间传达信息。如果未指定任何内容，则对来自 BGP 和 EGP 的路由使用远程自治系统编号。对于其他协议，将会使用零。有效值范围为 0 至 4294967295。**route-map** 关键字指定路由映射来检查对从源路由协议到当前路由协议的路由的导入的过滤。如果未指定此关键字，则会重新分发所有路由。如果已指定此关键字，但未列出路由映射标记，则不会导入任何路由。*map-tag* 参数标识已配置的路由映射。

配置无中断重新启动

ASA 可能会遇到一些已知的故障情况，这些故障情况不应影响跨交换平台转发的数据包。不间断转发 (NSF) 功能允许在还原路由协议信息的同时沿已知路由继续转发数据。此功能在以下情况下有用：存在组件故障 （即，在故障转移 (HA) 模式中主用单元崩溃而备用单元接管，在集群模式中主要单元崩溃而从属单元被选为新的主要单元），或者已计划无中断软件升级。

在 OSPFv2 和 OSPFv3 上均支持无中断重新启动。通过使用 NSF Cisco（RFC 4811 和 RFC 4812）或 NSF IETF (RFC 3623)，可以在 OSPFv2 上配置无中断重新启动。可以使用 graceful-restart (RFC 5187) 在 OSPFv3 上配置无中断重新启动。

配置 NSF 无中断重新启动功能涉及两个步骤；配置功能和将设备配置为具有 NSF 功能或可感知 NSF。具有 NSF 功能的设备可以向邻居表明其自己的重新启动活动，而可感知 NSF 的设备可以帮助重新启动邻居。

根据某些条件，可以将设备配置为具有 NSF 功能或可感知 NSF：

- 设备可以配置为可感知 NSF，而与其所处的模式无关。
- 设备必须处于 Failover 或 Spanned Etherchannel (L2) 集群模式中才能配置为具有 NSF 功能。
- 为使设备可感知 NSF 或具有 NSF 功能，应将其配置为能够根据需要处理不透明链路状态通告 (LSA)/本地链路信令 (LLS) 块。

注　如果为 OSPFv2 配置了快速呼叫，则在主用单元重新加载且备用单元激活时不会发生无中断重新启动。这是因为角色更改所需的时间超过配置的停顿间隔。

配置功能

Cisco NSF 无中断重新启动机制取决于 LLS 功能，因为它会发送含有呼叫数据包中设置的 RS 位的 LLS 块来表示重新启动活动。IETF NSF 机制取决于不透明 LSA 功能，因为它会发送不透明 9 类 LSA 来表示重新启动活动。如要配置功能，请输入以下命令：

命令	用途
router ospf *process_id* **示例：** `ciscoasa(config)# router ospf 2`	创建 OSPF 路由进程并进入要重新分发的 OSPF 进程的路由器配置模式。 *process_id* 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。可以使用最多两个进程。
capability {**lls**|**opaque**} **示例：** `ciscoasa(config-router)# capability lls`	支持使用 LLS 数据块或不透明 LSA 来启用 NSF。 **lls** 关键字用于启用 Cisco NSF 无中断重新启动机制的 LLS 功能。 **opaque** 关键字用于启用 IETF NSF 无中断重新启动机制的不透明 LSA 功能。

为 OSPFv2 配置无中断重新启动

对于 OSPFv2、Cisco NSF 和 IETF NSF，存在两种无中断重新启动机制。一次只能为 ospf 实例配置其中一种无中断重新启动机制。可感知 NSF 的设备既可以配置为 Cisco NSF 助手，也可以配置为 IETF NSF 助手，但是一次只能在 Cisco NSF 或 IETF NSF 模式中为 ospf 实例配置具有 NSF 功能的设备。

为 OSPFv2 配置 Cisco NSF 无中断重新启动

如要为 OSPFv2 配置 Cisco NSF 无中断重新启动（适用于具有 NSF 功能或可感知 NSF 的设备），输入以下命令：

命令	用途
nsf cisco [**enforce global**] **示例：** ciscoasa(config-router)# nsf cisco	在具有 NSF 功能的设备上启用 Cisco NSF。 **enforce global** 关键字在检测到无法感知 NSF 的邻居设备时会取消 NSF 重新启动。
capability {**lls**|**opaque**} **示例：** ciscoasa(config-router)# capability lls	（可选）在可感知 NSF 的设备上启用 Cisco NSF 助手模式。 默认情况下会启用此命令。使用命令的 no 形式可禁用该命令。

为 OSPFv2 配置 IETF NSF 无中断重新启动

如要为 OSPFv2 配置 IETF NSF 无中断重新启动（适用于具有 NSF 功能或可感知 NSF 的设备），输入以下命令：

命令	用途
nsf ietf [**restart interval** *seconds*] **示例：** ciscoasa(config-router)# nsf ietf restart interval 80	在具有 NSF 功能的设备上启用 IETF NSF。 （可选）**restart interval** *seconds* 指定无中断重新启动间隔的长度（以秒为单位）。有效值范围为 1 至 1800 秒。默认值为 120 秒。 **注** 使用小于邻接启动所需的时间的值来配置重新启动间隔时，可能会终止无中断重新启动。例如，不支持低于 30 秒的重新启动间隔。
nsf ietf helper [**strict-lsa-checking**] **示例：** ciscoasa(config-router)# nsf ietf helper	（可选）在可感知 NSF 的设备上启用 IETF NSF 助手模式。 （可选）**strict-LSA-checking** 关键字指示如果助手路由器在以下情况下将终止重新启动路由器的过程：它检测到会泛洪至正在重新启动的路由器的 LSA 发生更改，或者如果在启动无中断重新启动过程后正在重新启动的路由器的重新传输列表中有已更改的 LSA。 **注** 默认情况下会启用此命令。使用命令的 no 形式可禁用该命令。

为 OSPFv3 配置无中断重新启动

为 OSPFv3 配置 NSF 无中断重新启动功能涉及两个步骤：将一个设备配置为具有 NSF 功能，然后将另一个设备配置为可感知 NSF。如要为 OSPFv3 配置无中断重新启动，输入以下命令：

命令	用途
interface *physical_interface* **ipv6 enable** **示例：** ciscoasa(config)# interface ethernet 0/0 ciscoasa(config-if)# ipv6 enable	在未配置有显式 IPv6 地址的接口上启用 IPv6 处理。 *physical_interface* 参数标识参与 OSPFv3 NSF 的接口。
graceful-restart [**restart interval** *seconds*] **示例：** ciscoasa(config-router)# graceful-restart restart interval 80	在具有 NSF 功能的设备上为 OSPFv3 启用 graceful-restart。 （可选）**restart interval** *seconds* 指定无中断重新启动间隔的长度（以秒为单位）。有效值范围为 1 至 1800 秒。默认值为 120 秒。 **注**　使用小于邻接启动所需的时间的值来配置重新启动间隔时，可能会终止无中断重新启动。例如，不支持低于 30 秒的重新启动间隔。
graceful-restart helper [**strict-lsa-checking**] **示例：** ciscoasa(config-router)# graceful-restart helper strict-lsa-checking	在可感知 NSF 的设备上为 OSPFv3 启用 graceful-restart。 （可选）**strict-LSA-checking** 关键字指示如果助手路由器在以下情况下将终止重新启动路由器的过程：它检测到会泛洪至正在重新启动的路由器的 LSA 发生更改，或者如果在启动无中断重新启动过程后正在重新启动的路由器的重新传输列表中有已更改的 LSA。 **注**　默认情况下会启用无中断重新启动助手模式。

移除 OSPF 配置

如要移除已启用的整个 OSPFv2 配置，请输入以下命令：

命令	用途
clear configure router ospf *pid* **示例：** ciscoasa(config)# clear configure router ospf 1000	移除已启用的整个 OSPFv2 配置。清除配置后，必须使用 **router ospf** 命令重新配置 OSPF。

如要移除已启用的整个 OSPFv3 配置，请输入以下命令：

命令	用途
clear configure ipv6 router ospf *process-id* **示例：** ciscoasa(config)# clear configure ipv6 router ospf 1000	移除已启用的整个 OSPFv3 配置。清除配置后，必须使用 **ipv6 router ospf** 命令重新配置 OSPFv3。

OSPFv2 的配置示例

以下示例显示如何使用各种可选进程启用和配置 OSPFv2：

步骤 1　要启用 OSPFv2，请输入以下命令：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

步骤 2　（可选）要将路由从一个 OSPFv2 进程重新分发到另一个 OSPFv2 进程，请输入以下命令：

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

步骤 3　（可选）要配置 OSPFv2 接口参数，请输入以下命令：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
ciscoasa(config-rtr)# interface inside
ciscoasa(config-interface)# ospf cost 20
ciscoasa(config-interface)# ospf retransmit-interval 15
ciscoasa(config-interface)# ospf transmit-delay 10
ciscoasa(config-interface)# ospf priority 20
ciscoasa(config-interface)# ospf hello-interval 10
ciscoasa(config-interface)# ospf dead-interval 40
ciscoasa(config-interface)# ospf authentication-key cisco
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
ciscoasa(config-interface)# ospf authentication message-digest
```

步骤 4　（可选）要配置 OSPFv2 区域参数，请输入以下命令：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# area 0 authentication
ciscoasa(config-rtr)# area 0 authentication message-digest
ciscoasa(config-rtr)# area 17 stub
ciscoasa(config-rtr)# area 17 default-cost 20
```

步骤 5　（可选）要配置路由计算计时器并显示邻居启动和关闭日志消息，请输入以下命令：

```
ciscoasa(config-rtr)# timers spf 10 120
ciscoasa(config-rtr)# log-adj-changes [detail]
```

步骤 6　（可选）要显示当前 OSPFv2 配置设置，请输入 **show ospf** 命令。

以下是来自 **show ospf** 命令的样本输出：

```
ciscoasa(config)# show ospf

Routing Process "ospf 2" with ID 10.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs.Minimum LSA arrival 1 secs
Number of external LSA 5.Checksum Sum 0x 26da6
Number of opaque AS LSA 0.Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1.1 normal 0 stub 0 nssa
External flood list length 0
    Area BACKBONE(0)
```

```
Number of interfaces in this area is 1
Area has no authentication
SPF algorithm executed 2 times
Area ranges are
Number of LSA 5.Checksum Sum 0x 209a3
Number of opaque link LSA 0.Checksum Sum 0x     0
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

步骤 7　如要清除 OSPFv2 配置，请输入以下命令：

```
ciscoasa(config)# clear configure router ospf pid
```

OSPFv3 的配置示例

以下示例显示如何在接口级别启用和配置 OSPFv3：

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf 1 area 1
```

以下是来自 **show running-config ipv6** 命令的样本输出：

```
ciscoasa (config)# show running-config ipv6
ipv6 router ospf 1
 log-adjacency-changes
```

以下是来自 **show running-config interface** 命令的样本输出：

```
ciscoasa (config-if)# show running-config interface GigabitEthernet3/1
interface GigabitEthernet3/1
 nameif fda
 security-level 100
 ip address 1.1.11.1 255.255.255.0 standby 1.1.11.2
 ipv6 address 9098::10/64 standby 9098::11
 ipv6 enable
 ipv6 ospf 1 area 1
```

以下示例显示如何配置特定于 OSPFv3 的接口：

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# nameif fda
ciscoasa (config-if)# security-level 100
ciscoasa (config-if)# ip address 10.1.11.1 255.255.255.0 standby 10.1.11.2
ciscoasa (config-if)# ipv6 address 9098::10/64 standby 9098::11
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf cost 900
ciscoasa (config-if)# ipv6 ospf hello-interval 20
ciscoasa (config-if)# ipv6 ospf network broadcast
ciscoasa (config-if)# ipv6 ospf database-filter all out
ciscoasa (config-if)# ipv6 ospf flood-reduction
ciscoasa (config-if)# ipv6 ospf mtu-ignore
ciscoasa (config-if)# ipv6 ospf 1 area 1 instance 100
ciscoasa (config-if)# ipv6 ospf encryption ipsec spi 890 esp null md5
123456789012345678901234567890 12

ciscoasa (config)# ipv6 router ospf 1
ciscoasa (config)# area 1 nssa
```

```
ciscoasa (config)# distance ospf intra-area 190 inter-area 100 external 100
ciscoasa (config)# timers lsa arrival 900
ciscoasa (config)# timers pacing flood 100
ciscoasa (config)# timers throttle lsa 900 900 900
ciscoasa (config)# passive-interface fda
ciscoasa (config)# log-adjacency-changes
ciscoasa (config)# redistribute connected metric 100 metric-type 1 tag 700
```

有关如何配置 OSPFv3 虚拟链路的示例，请参阅以下 URL：

http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080b8fd06.shtml

监控 OSPF

您可以显示特定统计，如 IP 路由表、缓存和数据库的内容。您还可以使用所提供的信息确定资源利用率和解决网络问题。您也可以显示有关节点可达性的信息并发现设备数据包通过网络所采用的路由路径。

如要监控或显示各种 OSPFv2 路由统计，请输入以下命令之一：

命令	用途
show ospf [*process-id* [*area-id*]]	显示有关 OSPFv2 路由进程的一般信息。
show ospf border-routers	向 ABR 和 ASBR 显示内部 OSPFv2 路由表条目。
show ospf [*process-id* [*area-id*]] **database**	显示与特定路由器的 OSPFv2 数据库相关的信息列表。
show ospf flood-list *if-name*	显示等待通过接口泛洪的 LSA 的列表 （以观察 OSPFv2 数据包步调设置）。 OSPFv2 更新数据包自动设置步调，因此其不会以小于 33 毫秒的间隔进行发送。如果没有步调设置，则在链路速度缓慢，邻居无法足够快速地接收更新或者路由器可能会用尽缓冲区空间的情况下，某些更新数据包可能会丢失。例如，如果没有步调设置，则在存在以下任一拓扑的情况下，可能会丢弃数据包： • 快速路由器通过点对点链路连接到速度较慢的路由器。 • 在泛洪期间，多个邻居同时向单个路由器发送更新。 在重新发送的间隔内也会使用步调设置，以提高效率并尽量减少重新传输丢失。您还可以显示等待从接口发出的 LSA。通过步调设置，可以更高效地发送 OSPFv2 更新数据包和重新传输数据包。 此功能没有配置任务；它自动进行配置。
show ospf interface [*if_name*]	显示与 OSPFv2 相关的接口信息。
show ospf neighbor [*interface-name*] [*neighbor-id*] [**detail**]	逐个接口显示 OSPFv2 邻居信息。
show ospf request-list *neighbor if_name*	显示路由器请求的所有 LSA 的列表。
show ospf retransmission-list *neighbor if_name*	显示等待重新发送的所有 LSA 的列表。

命令	用途
show ospf [*process-id*] **summary-address**	显示在 OSPFv2 进程下配置的所有摘要地址重新分发信息的列表。
show ospf [*process-id*] **traffic**	显示由特定 OSPFv2 实例发送或接收的不同类型的数据包的列表。
show ospf [*process-id*] **virtual-links**	显示与 OSPFv2 相关的虚拟链路信息。
show route cluster	显示集群中的其他 OSPFv2 路由同步信息。

如要监控或显示各种 OSPFv3 路由统计，请输入以下命令之一：

命令	用途
show ipv6 ospf [*process-id* [*area-id*]]	显示有关 OSPFv3 路由进程的一般信息。
show ipv6 ospf [*process-id*] **border-routers**	向 ABR 和 ASBR 显示内部 OSPFv3 路由表条目。
show ipv6 ospf [*process-id* [*area-id*]] **database** [**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] | **self-originate**] [**internal**] [**database-summary**]	显示与特定路由器的 OSPFv3 数据库相关的信息列表。
show ipv6 ospf [*process-id* [*area-id*]] **events**	显示 OSPFv3 事件信息。
show ipv6 ospf [*process-id*] [*area-id*] **flood-list** *interface-type interface-number*	显示等待通过接口泛洪的 LSA 的列表 （以观察 OSPFv3 数据包步调设置）。 OSPFv3 更新数据包自动设置步调，因此其不会以小于 33 毫秒的间隔进行发送。如果没有步调设置，则在链路速度缓慢，邻居无法足够快速地接收更新或者路由器可能会用尽缓冲区空间的情况下，某些更新数据包可能会丢失。例如，如果没有步调设置，则在存在以下任一拓扑的情况下，可能会丢弃数据包： • 快速路由器通过点对点链路连接到速度较慢的路由器。 • 在泛洪期间，多个邻居同时向单个路由器发送更新。 在重新传输的间隔内也会使用步调设置，以提高效率并尽量减少重新传输丢失。您还可以显示等待从接口发出的 LSA。通过步调设置，可以更高效地发送 OSPFv3 更新数据包和重新传输数据包。 此功能没有配置任务；它自动进行配置。
show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]	显示与 OSPFv3 相关的接口信息。
show ipv6 ospf neighbor [*process-id*] [*area-id*] [*interface-type interface-number*] [*neighbor-id*] [**detail**]	逐个接口显示 OSPFv3 邻居信息。

命令	用途
show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]	显示路由器请求的所有 LSA 的列表。
show ipv6 ospf [*process-id*] [*area-id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]	显示等待重新发送的所有 LSA 的列表。
show ipv6 ospf statistic [*process-id*] [**detail**]	显示各种 OSPFv3 统计。
show ipv6 ospf [*process-id*] **summary-prefix**	显示在 OSPFv3 进程下配置的所有摘要地址重新分发信息的列表。
show ipv6 ospf [*process-id*] **timers** [**lsa-group** | **rate-limit**]	显示 OSPFv3 计时器信息。
show ipv6 ospf [*process-id*] **traffic** [*interface_name*]	显示与 OSPFv3 流量相关的统计。
show ipv6 ospf virtual-links	显示与 OSPFv3 相关的虚拟链路信息。
show ipv6 route cluster [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]	显示集群中的 IPv6 路由表序号、 IPv6 重新收敛计时器状态和 IPv6 路由条目序号。

附加参考资料

RFC

RFC	标题
2328	OSPFv2
4552	OSPFv3 Authentication
5340	OSPF for IPv6

OSPF 功能历史记录

表 22-1 列出了各种功能变更以及实施该等功能变更的平台版本。

表 22-1 OSPF 功能历史记录

功能名称	平台版本	功能信息
OSPF 支持	7.0(1)	添加了对使用开放式最短路径优先 (OSPF) 路由协议来路由数据、执行身份验证以及重新分发和监控路由信息的支持。 我们引入了以下命令：**route ospf**

表 22-1　　OSPF 功能历史记录（续）

功能名称	平台版本	功能信息
多情景模式中的动态路由	9.0(1)	在多情景模式中支持 OSPFv2 路由。
集群		对于 OSPFv2 和 OSPFv3，在集群环境中支持批量同步、路由同步和跨网络 EtherChannel 负载均衡。 我们引入或修改了以下命令：**show route cluster**、 **show ipv6 route cluster**、 **debug route cluster**、 **router-id cluster-pool**。
IPv6 的 OSPFv3 支持		IPv6 支持 OSPFv3 路由。 我们引入或修改了以下命令：**ipv6 ospf**、 **ipv6 ospf area**、 **ipv6 ospf cost**、 **ipv6 ospf database-filter all out**、 **ipv6 ospf dead-interval**、 **ipv6 ospf encryption**、 **ipv6 ospf hello-interval**、 **ipv6 ospf mtu-ignore**、 **ipv6 ospf neighbor**、 **ipv6 ospf network**、 **ipv6 ospf flood-reduction**、 **ipv6 ospf priority**、 **ipv6 ospf retransmit-interval**、 **ipv6 ospf transmit-delay**、 **ipv6 router ospf**、**ipv6 router ospf area**、**ipv6 router ospf default**、**ipv6 router ospf default-information**、 **ipv6 router ospf distance**、 **ipv6 router ospf exit**、 **ipv6 router ospf ignore**、 **ipv6 router ospf log-adjacency-changes**、 **ipv6 router ospf no**、**ipv6 router ospf passive-interface**、**ipv6 router ospf redistribute**、 **ipv6 router ospf router-id**、 **ipv6 router ospf summary-prefix**、**ipv6 router ospf timers**、**area encryption**、**area range**、 **area stub**、 **area nssa**、 **area virtual-link**、 **default**、 **default-information originate**、 **distance**、 **ignore lsa mospf**、 **log-adjacency-changes**、 **redistribute**、 **router-id, summary-prefix**、 **timers lsa arrival**、 **timers pacing flood**、 **timers pacing lsa-group**、 **timers pacing retransmission**、 **timers throttle**、 **show ipv6 ospf**、 **show ipv6 ospf border-routers**、 **show ipv6 ospf database**、 **show ipv6 ospf events**、 **show ipv6 ospf flood-list**、 **show ipv6 ospf graceful-restart**、**show ipv6 ospf interface**、**show ipv6 ospf neighbor**、 **show ipv6 ospf request-list**、 **show ipv6 ospf retransmission-list**、 **show ipv6 ospf statistic**、 **show ipv6 ospf summary-prefix**、 **show ipv6 ospf timers**、 **show ipv6 ospf traffic**、 **show ipv6 ospf virtual-links**、 **show ospf**、 **show running-config ipv6 router**、 **clear ipv6 ospf**、 **clear configure ipv6 router**、 **debug ospfv3**、 **ipv6 ospf neighbor**。

表 22-1　　OSPF 功能历史记录（续）

功能名称	平台版本	功能信息
OSPF 支持快速呼叫	9.2(1)	OSPF 支持快速呼叫数据包功能，从而产生在 OSPF 网络中导致更快收敛的配置。 我们修改了以下命令：**ospf dead-interval**
计时器		添加了新 OSPF 计时器；启用了旧 OSPF 计时器。 我们引入了以下命令：**timers lsa arrival**、 **timers pacing**、 **timers throttle** 我们移除了以下命令：**Timers spf**、 **timers lsa-grouping-pacing**
使用访问列表过滤路由		现在支持使用 ACL 过滤路由。 我们引入了以下命令：**distribute-list** 我们引入了以下屏幕：
OSPF 监控增强功能		添加了其他 OSPF 监控信息。 我们修改了以下命令：**show ospf events**、 **show ospf rib**、 **show ospf statistics**、 **show ospf border-routers [detail]**、 **show ospf interface brief**
OSPF 重新分发 BGP		添加了 OSPF 重新分发功能。 我们添加了以下命令：**redistribute bgp**
对不间断转发 (NSF) 的 OSPF 支持	9.3(1)	添加了对 NSF 的 OSPFv2 和 OSPFv3 支持。 我们添加了以下命令：**capability**、 **nsf cisco**、 **nsf cisco helper**、 **nsf ietf**、 **nsf ietf helper**、 **nsf ietf helper strict-lsa-checking**、 **graceful-restart**、 **graceful-restart helper**、 **graceful-restart helper strict-lsa-checking**

EIGRP

本章介绍如何使用增强型内部网关路由协议 (EIGRP) 配置 Cisco ASA，以路由数据、执行身份验证和重新分发路由信息。

- 第 23-1 页的有关 EIGRP 的信息
- 第 23-2 页的 EIGRP 许可要求
- 第 23-2 页的准则和限制
- 第 23-3 页的配置 EIGRP
- 第 23-4 页的自定义 EIGRP
- 第 23-15 页的监控 EIGRP
- 第 23-16 页的 EIGRP 的配置示例
- 第 23-17 页的 EIGRP 的功能历史记录

有关 EIGRP 的信息

EIGRP 是思科开发的 IGRP 增强版。与 IGRP 和 RIP 不同，EIGRP 不发送定期路由更新。仅在网络拓扑发生变化时才会发送 EIGRP 更新。将 EIGRP 与其他路由协议区分开来的主要功能包括快速聚合、支持可变长度子网掩码、支持部分更新以及支持多个网络层协议。

运行 EIGRP 的路由器存储所有的邻居路由表，以便迅速适应备用路由。如果不存在合适的路由，则 EIGRP 会查询其邻居以发现备用路由。这些查询会一直传播，直到找到备用路由。支持可变长度子网掩码功能允许在网络号边界自动摘要路由。此外，可以将 EIGRP 配置为在任何接口的任何位边界摘要。EIGRP 不会定期发送更新。而仅在路由度量发生变化时才发送部分更新。部分更新的传播是自动绑定的，以便仅更新需要该信息的路由器。得益于这两项功能，EIGRP 与 IGRP 相比可显著减少占用的带宽。

邻居发现是 ASA 用于动态获悉直接连接的网络中其他路由器的过程。EIGRP 路由器发送组播 Hello 数据包，通告其在网络中的存在状态。当 ASA 收到来自新邻居的 Hello 数据包时，会将其包含初始化位集的拓扑表发送至邻居。当邻居收到包含初始化位集的拓扑更新时，邻居将其拓扑表发回到 ASA。

Hello 数据包作为组播消息发送。预期不对 Hello 消息作出响应。但对静态定义的邻居除外。如果您使用 **neighbor** 命令或在 ASDM 中配置 Hello 时间间隔以配置邻居，则发送到该邻居的 Hello 消息将作为单播消息发送。路由更新和确认作为单播消息发送。

此邻居关系建立之后，除非网络拓扑发生变化，否则不会交换路由更新。邻居关系通过 Hello 数据包来维护。从邻居收到的每个 Hello 数据包均包括保持时间。这是 ASA 预期收到来自该邻居的 Hello 数据包的时间。如果 ASA 在保持时间内未收到由该邻居通告的 Hello 数据包，则 ASA 会将该邻居视为不可用。

EIGRP 协议使用四种关键算法技术，包括邻居发现/恢复、可靠的传输协议 (RTP) 和对于路由计算非常重要的 DUAL。DUAL 将所有路由保存至拓扑表中的目标，而不仅是最低成本路由。最低成本路由会插入路由表。其他路由保留在拓扑表中。如果主路由发生故障，可以从可行后继路由中选择另一个路由。后继路由是指用于具有到达目标的最低成本路径的数据包转发的邻居路由器。可行性计算可确保路径不是路由环路的一部分。

如果未在拓扑表中找到可行后继路由，则必须进行路由重新计算。路由重新计算期间，DUAL 会查询 EIGRP 邻居获取路由，该邻居反过来查询其邻居。没有用于路由的可行后继路由的路由器会返回不可达消息。

路由重新计算期间，DUAL 会将路由标记为活动状态。默认情况下，ASA 等待三分钟接收来自其邻居的响应。如果 ASA 未收到来自邻居的响应，则路由会标记为陷入活动状态。拓扑表中指向无响应邻居的所有路由均作为可行性后继路被移除。

注 如果无 GRE 隧道，EIGRP 邻居关系就不会通过 IPSec 隧道得以支持。

使用集群

有关集群与 EIGRP 配合使用的信息，请参阅第 18-8 页的动态路由和集群。

EIGRP 许可要求

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

仅在路由防火墙模式中受支持。透明防火墙模式不受支持。

故障转移准则

在单情景模式和多情景模式中支持有状态故障转移。

IPv6 准则

不支持 IPv6。

集群准则

- 当配置为同时使用 EIGRP 和 OSPFv2 时，支持跨越式 EtherChannel 和单个接口集群。
- 在单个接口集群设置中，EIGRP 邻接关系只能在主要设备共享接口上的两个情景之间建立。分别手动配置对应每个集群节点的多个邻居语句，即可解决此问题。

其他指导原则

- 由于组播流量的情景间交换不受支持，因此 EIGRP 实例不能跨共享接口彼此建立邻接关系。
- 最多支持一个 EIGRP 进程。

配置 EIGRP

如要介绍如何在系统中启用 EIGRP 进程。启用 EIGRP 之，请参阅以下各节了解如何在系统中自定义 EIGRP 进程。

- 第 23-3 页的启用 EIGRP
- 第 23-4 页的启用 EIGRP 末节路由

启用 EIGRP

仅能在 ASA 中启用一个 EIGRP 路由进程。

如要启用 EIGRP，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router eigrp** *as-num* **示例：** `ciscoasa(config)# router eigrp 2`	创建 EIGRP 路由进程，并输入此 EIGRP 进程的路由器配置模式。 *as-num* 参数是 EIGRP 路由进程的自治系统编号。
步骤 2	**network** *ip-addr* [*mask*] **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`	配置参与 EIGRP 路由的接口和网络。可以使用此命令配置一个或多个**网络**语句。 已定义网络内的直接连接和静态网络由 ASA 通告。此外，已定义网络内只有带有 IP 地址的接口才参与 EIGRP 路由进程。 如果不希望接口参与 EIGRP 路由，但是该接口连接到希望通告的网络，请参阅第 23-5 页的配置 EIGRP 的接口。

启用 EIGRP 末节路由

可以启用 ASA，并将其配置为 EIGRP 末节路由器。末节路由可降低 ASA 上的内存和处理要求。作为末节路由器，ASA 不需要维护完整的 EIGRP 路由表，因为它将所有非本地流量转发到分布式路由器。一般而言，除了发送末节路由器的默认路由，分布式路由器不需要发送任何其他信息。

仅指定的路由从末节路由器传播到分布式路由器。作为末节路由器，ASA 以“不可达”消息响应对摘要、已连接路由、重新分发的静态路由、外部路由和内部路由的所有查询。当 ASA 配置为末节时，它会发送特殊对等信息数据包到所有邻居路由器，报告其作为末节路由器的状态。收到通知其末节状态之数据包的任何邻居都将不会查询末节路由器是否存在任何路由，且具有末节对等体的路由器也将不查询该对等体。末节路由器依赖于分布式路由器发送正确的更新到所有对等体。

如要启用 ASA 作为 EIGRP 末节路由进程，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router eigrp** *as-num* **示例：** `ciscoasa(config)# router eigrp 2`	创建 EIGRP 路由进程，并输入此 EIGRP 进程的路由器配置模式。 *as-num* 参数是 EIGRP 路由进程的自治系统编号。
步骤 2	**network** *ip-addr* [*mask*] **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`	配置参与 EIGRP 路由的接口和网络。可以使用此命令配置一个或多个**网络**语句。 已定义网络内的直接连接和静态网络由 ASA 通告。此外，已定义网络内只有带有 IP 地址的接口才参与 EIGRP 路由进程。 如果不希望接口参与 EIGRP 路由，但是该接口连接到希望通告的网络，请参阅第 23-7 页的配置被动接口 节。
步骤 3	**eigrp stub** {**receive-only** | [**connected**] [**redistributed**] [**static**] [**summary**]} **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0` `ciscoasa(config-router)# eigrp stub {receive-only | [connected] [redistributed] [static] [summary]}`	配置末节路由进程。必须指定哪些网络由末节路由进程通告到分布式路由器。静态和已连接网络不会自动重新分发到末节路由进程。

注 末节路由进程不维护完整的拓扑表。至少，末节路由需要分布式路由器的默认路由，以此做出路由决定。

自定义 EIGRP

本节说明如何自定义 EIGRP 路由。

- 第 23-5 页的为 EIGRP 路由进程定义网络
- 第 23-5 页的配置 EIGRP 的接口

- 第 23-7 页的在接口上配置摘要汇聚地址
- 第 23-8 页的更改接口延迟值
- 第 23-8 页的在接口上启用 EIGRP 身份验证
- 第 23-9 页的定义 EIGRP 邻居
- 第 23-10 页的将路由重新分发到 EIGRP 中
- 第 23-11 页的。在 EIGRP 中过滤网络
- 第 23-12 页的自定义 EIGRP Hello 时间间隔和保持时间
- 第 23-13 页的禁用自动路由摘要
- 第 23-14 页的在 EIGRP 中配置默认信息
- 第 23-14 页的禁用 EIGRP 水平分割
- 第 23-15 页的重新启动 EIGRP 进程

为 EIGRP 路由进程定义网络

网络表可供您指定 EIGRP 路由进程所用的网络。对于参与 EIGRP 路由的接口，它必须在网络条目定义的地址范围内。对于要通告的直接连接和静态网络，它们也必须位于网络条目的范围内。

网络表显示为 EIGRP 路由进程配置的网络。表的每一行显示为指定的 EIGRP 路由进程配置的网络地址和关联的掩码。

如要添加或定义网络，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router eigrp** *as-num* **示例：** `ciscoasa(config)# router eigrp 2`	创建 EIGRP 路由进程，并输入此 EIGRP 进程的路由器配置模式。 *as-num* 参数是 EIGRP 路由进程的自治系统编号。
步骤 2	**network** *ip-addr* [*mask*] **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`	配置参与 EIGRP 路由的接口和网络。可以使用此命令配置一个或多个**网络**语句。 已定义网络内的直接连接和静态网络由 ASA 通告。此外，已定义网络内只有带有 IP 地址的接口才参与 EIGRP 路由进程。 如果不希望接口参与 EIGRP 路由，但是该接口连接到希望通告的网络，请参阅第 23-7 页的配置被动接口。

配置 EIGRP 的接口

如果您具有不希望其参与 EIGRP 路由但连接到要播发的网络的接口，则可以配置其中包含该接口连接到的网络的ASA a **network** 命令，并且使用 **passive-interface** 命令阻止该接口发送或接收 EIGRP 更新。

如要配置 EIGRP 的接口，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router eigrp** *as-num* **示例：** `ciscoasa(config)# router eigrp 2`	创建 EIGRP 路由进程，并输入此 EIGRP 进程的路由器配置模式。 *as-num* 参数是 EIGRP 路由进程的自治系统编号。
步骤 2	`ciscoasa(config-router)#` **network** *ip-addr* [*mask*] **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`	配置参与 EIGRP 路由的接口和网络。可以使用此命令配置一个或多个网络语句。 已定义网络内的直接连接和静态网络由 ASA 通告。此外，已定义网络内只有带有 IP 地址的接口才参与 EIGRP 路由进程。 如果不希望接口参与 EIGRP 路由，但是该接口连接到希望通告的网络，请参阅第 23-5 页的为 EIGRP 路由进程定义网络。
步骤 3	（可选）执行以下操作之一，自定义要参与 EIGRP 路由的接口：	
	no default-information {**in** | **out** | **WORD**} **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0` `ciscoasa(config-router)# no default-information {in | out | WORD}`	允许控制发送或接收候选默认路由信息。 输入 **no default-information in** 命令会导致候选默认路由位在已收到路由中被拦截。输入 **no default-information out** 命令会禁用已通告路由中默认路由位的设置。 有关此特殊选项的详细信息，请参阅第 23-14 页的在 EIGRP 中配置默认信息。
	authentication mode eigrp *as-num* **md5** **示例：** `ciscoasa(config)# authentication mode eigrp 2 md5`	启用 EIGRP 数据包的 MD5 身份认证。 *as-num* 参数是在 ASA 中配置的 EIGRP 路由进程的自治系统编号。如果 EIGRP 未启用或者如果输入错误编号，则 ASA 将返回以下错误消息： `指定的 % Asystem(100) 不存在` 有关此特殊选项的详细信息，请参阅第 23-8 页的在接口上启用 EIGRP 身份验证。
	延迟*值* **示例：** `ciscoasa(config-if)# delay 200`	输入的 *value* 参数为数十微秒。如要设置延迟 2000 毫秒，请输入*值* 200。 要查看分配给接口的延迟值，请使用 **show interface** 命令。 有关此特殊选项的详细信息，请参阅第 23-8 页的更改接口延迟值。
	hello-interval eigrp *as-num seconds* **示例：** `ciscoasa(config)# hello-interval eigrp 2 60`	允许更改 Hello 时间间隔。有关此特殊选项的详细信息，请参阅第 23-12 页的自定义 EIGRP Hello 时间间隔和保持时间。
	hold-time eigrp *as-num seconds* **示例：** `ciscoasa(config)# hold-time eigrp 2 60`	允许更改保持时间。有关此特殊选项的详细信息，请参阅第 23-12 页的自定义 EIGRP Hello 时间间隔和保持时间。

配置被动接口

可以将一个或多个接口配置为被动接口。在 EIGRP 中，被动接口既不发送也不接收路由更新。

如要配置被动接口，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router eigrp** *as-num* **示例：** `ciscoasa(config)# router eigrp 2`	创建 EIGRP 路由进程，并输入此 EIGRP 进程的路由器配置模式。 *as-num* 参数是 EIGRP 路由进程的自治系统编号。
步骤 2	`ciscoasa(config-router)#` **network** *ip-addr* [*mask*] **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`	配置参与 EIGRP 路由的接口和网络。可以使用此命令配置一个或多个**网络**语句。 已定义网络内的直接连接和静态网络由 ASA 通告。此外，已定义网络内只有带有 IP 地址的接口才参与 EIGRP 路由进程。 如果不希望接口参与 EIGRP 路由，但是该接口连接到希望通告的网络，请参阅第 23-5 页的为 EIGRP 路由进程定义网络。
步骤 3	**passive-interface** {**default** | *if-name*} **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0` `ciscoasa(config-router)# passive-interface {default}`	阻止接口发送或接收 EIGRP 路由消息。 使用**默认**关键字可禁用所有接口上的 EIGRP 路由更新。如 **nameif** 命令所定义，指定接口名称可以禁用指定接口上的 EIGRP 路由更新。可以在 EIGRP 路由器配置中使用多个 **passive-interface** 命令。

在接口上配置摘要汇聚地址

可逐一为每个接口上配置摘要地址。如果要创建不发生在网络号边界上的摘要地址，或者想要在自动路由摘要禁用的情况下在 ASA 上使用摘要地址，则需要手动定义摘要地址。如果路由表中有更具体的路由，则 EIGRP 将用相当于所有更上体路由最小值的度量将摘要地址通告出接口。

如要创建摘要地址，请执行以下操作：

详细步骤

	命令	用途
步骤 1	**interface** *phy_if* **示例：** `ciscoasa(config)# interface inside`	为正在其上面更改 EIGRP 所用延迟值的接口输入接口配置模式。

	命令	用途
步骤 2	**summary-address eigrp** *as-num address mask* [*distance*] **示例：** `ciscoasa(config-if)# summary-address eigrp 2 address mask [20]`	创建摘要地址。 默认情况下，定义的 EIGRP 摘要地址的管理距离为 5。可以通过在 *summary-address* 命令中指定可选 **distance** 参数来更改此值。

更改接口延迟值

接口延迟值用于 EIGRP 距离计算。可以逐一为每个接口修改此值。

如要更改接口延迟值，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**interface** *phy_if* **示例：** `ciscoasa(config)# interface inside`	为正在其上面更改 EIGRP 所用延迟值的接口输入接口配置模式。
步骤 2	**延迟***值* **示例：** `ciscoasa(config-if)# delay 200`	输入的 *value* 参数为数十微秒。要设置延迟 2000 毫秒，请输入*值* 200。 如要查看分配给接口的延迟值，请使用 **show interface** 命令。

在接口上启用 EIGRP 身份验证

EIGRP 路由身份验证提供来自 EIGRP 路由协议的路由更新 MD5 身份验证。每个 EIGRP 数据包中的 MD5 密钥摘要可防止从未批准的来源引入未经授权或虚假的路由消息。

将逐一为每个接口配置 EIGRP 路由身份验证。必须使用相同的身份验证模式和密钥配置接口上为 EIGRP 消息身份验证配置的所有 EIGRP 邻居，才能建立邻接关系。

注 必须先启用 EIGRP 路由身份验证，然后才能启用 EIGRP。

如要在接口上启用 EIGRP 身份验证，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router eigrp** *as-num* **示例：** `hostname(config)# router eigrp 2`	创建 EIGRP 路由进程，并输入此 EIGRP 进程的路由器配置模式。 *as-num* 参数是 EIGRP 路由进程的自治系统编号。

	命令	用途
步骤 2	**network** *ip-addr* [*mask*] **示例：** hostname(config)# router eigrp 2 hostname(config-router)# network 10.0.0.0 255.0.0.0	配置参与 EIGRP 路由的接口和网络。可以使用此命令配置一个或多个网络语句。 已定义网络内的直接连接和静态网络由 ASA 通告。此外，仅带有属于已定义网络内的 IP 地址的接口才参与 EIGRP 路由进程。 如果不希望接口参与 EIGRP 路由，但是该接口连接到希望通告的网络，请参阅第 23-3 页的配置 EIGRP。
步骤 3	**interface** *phy_if* **示例：** hostname(config)# interface inside	为正在其上面配置 EIGRP 消息身份验证的接口输入接口配置模式。
步骤 4	**authentication mode eigrp** *as-num* **md5** **示例：** hostname(config)# authentication mode eigrp 2 md5	启用 EIGRP 数据包的 MD5 身份认证。 *as-num* 参数是在 ASA 上配置的 EIGRP 路由进程的自治系统编号。如果 EIGRP 未启用或者如果输入错误编号，则 ASA 将返回以下错误消息： 指定的 % Asystem(100) 不存在
步骤 5	**authentication key eigrp** *as-num key* **key-id** *key-id* **示例：** hostname(config)# authentication key eigrp 2 cisco key-id 200	配置 MD5 算法使用的密钥。 *as-num* 参数是在 ASA 上配置的 EIGRP 路由进程的自治系统编号。如果 EIGRP 未启用或者如果输入错误编号，则 ASA 将返回以下错误消息： 指定的 % Asystem(100) 不存在 % *key* 参数最多可以包括 16 个字符，包括字母、数字和特殊字符。 **注**　key 参数中不允许有空格。 *key-id* 参数可能是范围为 0 至 255 范围内的数字。

定义 EIGRP 邻居

EIGRP Hello 数据包以组播数据包的形式发送。如果 EIGRP 邻居位于非广播网络内，如隧道，则必须手动定义该邻居。当手动定义 EIGRP 邻居时，Hello 数据包作为单播消息发送至该邻居。

如要手动定义 EIGRP 邻居，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router eigrp** *as-num* **示例：** ciscoasa(config)# router eigrp 2	创建 EIGRP 路由进程，并输入此 EIGRP 进程的路由器配置模式。 *as-num* 参数是 EIGRP 路由进程的自治系统编号。

	命令	用途
步骤 2	**neighbor** *ip-addr* **interface** *if_name* **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1`	定义静态邻居。 *ip-addr* 参数是邻居的 IP 地址。 *if-name* 参数是接口的名称，根据 **nameif** 命令指定，邻居通过该接口变得可用。可以为 EIGRP 路由进程定义多个邻居。

将路由重新分发到 EIGRP 中

可以将 RIP 和 OSPF 发现的路由重新分发到 EIGRP 路由进程中。您还可以将静态路由和已连接路由重新分发到 EIGRP 路由进程中。如果已连接路由位于 EIGRP 配置中**网络**语句范围内，则不需要进行重新分发它们。

注　仅适用于 RIP：开始此操作步骤之前，必须创建路由映射，以进一步定义将指定路由协议中哪些路由重新分发到 RIP 路由进程。有关创建路由映射的详细信息，请参阅第 20 章，“路由映射”。

如要将路由重新分发到 EIGRP 路由进程，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router eigrp** *as-num* **示例：** `ciscoasa(config)# router eigrp 2`	创建 EIGRP 路由进程，并输入此 EIGRP 进程的路由器配置模式。 *as-num* 参数是 EIGRP 路由进程的自治系统编号。
步骤 2	**default-metric** *bandwidth delay reliability loading mtu* **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# default-metric bandwidth delay reliability loading mtu`	（可选）指定应应用于已重新分发到 EIGRP 路由进程的路由的默认度量。 如果未在 EIGRP 路由器配置中指定默认度量，则必须在每个 **redistribute** 命令中指定度量值。如果在 **redistribute** 命令中指定 EIGRP 度量且 EIGRP 路由器配置中有 **default-metric** 命令，则将使用 **redistribute** 命令中的度量。
步骤 3	执行以下操作之一，以将选定的路由类型重新分发到 EIGRP 路由进程：	
	redistribute connected [**metric** *bandwidth delay reliability loading mtu*] [**route-map** *map_name*] **示例：** `ciscoasa(config-router): redistribute connected [metric bandwidth delay reliability loading mtu] [route-map map_name]`	将已连接路由重新分发到 EIGRP 路由进程。 如果 EIGRP 路由器配置中没有 **default-metri** 命令，则必须在**重新分配**命令中指定 EIGRP 度量值。

命令	用途
redistribute static [**metric** *bandwidth delay reliability loading mtu*] [**route-map** *map_name*] **示例：** ciscoasa(config-router): redistribute static [metric *bandwidth delay reliability loading mtu*] [route-map *map_name*]	将静态路由重新分发到 EIGRP 路由进程。
redistribute ospf *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** *bandwidth delay reliability loading mtu*] [**route-map** *map_name*] **示例：** ciscoasa(config-router): redistribute ospf *pid* [match {internal | external [1 | 2] | nssa-external [1 | 2]}] [metric *bandwidth delay reliability loading mtu*] [route-map *map_name*]	将源自 OSPF 路由进程的路由重新分发到 EIGRP 路由进程。
redistribute rip [**metric** bandwidth delay reliability load mtu] [**route-map map_name**] **示例：** (config-router): redistribute rip [metric bandwidth delay reliability load mtu] [route-map map_name]	将源自 RIP 路由进程的路由重新分发到 EIGRP 路由进程。

在 EIGRP 中过滤网络

注　开始此过程之前，必须创建标准 ACL，以定义要通告的路由。也就是说，创建标准 ACL，以定义要从发送或接收更新中过滤的路由。

如要在 EIGRP 中过滤网络，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router eigrp** *as-num* **示例：** `ciscoasa(config)# router eigrp 2`	创建 EIGRP 路由进程，并输入此 EIGRP 进程的路由器配置模式。 *as-num* 参数是 EIGRP 路由进程的自治系统编号。
步骤 2	`ciscoasa(config-router)#` **network** *ip-addr* [*mask*] **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`	配置参与 EIGRP 路由的接口和网络。可以使用此命令配置一个或多个网络语句。 已定义网络内的直接连接和静态网络由 ASA 通告。此外，已定义网络内只有带有 IP 地址的接口才参与 EIGRP 路由进程。 如果不希望接口参与 EIGRP 路由，但是该接口连接到希望通告的网络，请参阅第 23-5 页的配置 EIGRP 的接口。
步骤 3	执行以下操作之一，过滤 EIGRP 路由更新中发送或接收的网络：	
	distribute-list *acl* **out** [**connected** | **ospf** | **rip** | **static** | **interface** *if_name*] **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0` `ciscoasa(config-router): distribute-list acl out [connected]`	过滤 EIGRP 路由更新中发送的网络。 可以指定接口，将过滤器仅应用于该特定接口发送的更新。 可以在 EIGRP 路由器配置中输入多个 **distribute-list** 命令。
	distribute-list *acl* **in** [**interface** *if_name*] **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0` `ciscoasa(config-router): distribute-list acl in [interface interface1]`	过滤 EIGRP 路由更新中收到的网络。 可以指定接口，将过滤器仅应用于该接口收到的更新。

自定义 EIGRP Hello 时间间隔和保持时间

ASA 定期发送 Hello 数据包，用于发现邻居以及获悉邻居何时变得不可达或不起作用。默认情况下，每 5 秒发送一次 Hello 数据包。

Hello 数据包通告 ASA 保持时间。保持时间向 EIGRP 邻居指示应将邻居视为 ASA 可达的时间长度。如果邻居在通告的保持时间内未收到 Hello 数据包，则 ASA 将被视为不可达。默认情况下，通告的保持时间是 15 秒 （Hello 时间间隔的三倍）。

Hello 时间间隔和通告的保持时间均按每个接口逐一进行配置。我们建议将保持时间设置为至少相当于 Hello 时间间隔的三倍。

如要配置 Hello 时间间隔和通告的保持时间，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**interface** *phy_if* **示例：** `ciscoasa(config)# interface inside`	为正在其上面配置 Hello 时间间隔或通告保持时间的接口输入接口配置模式。
步骤 2	**hello-interval eigrp** *as-num seconds* **示例：** `ciscoasa(config)# hello-interval eigrp 2 60`	更改 Hello 时间间隔。
步骤 3	**hold-time eigrp** *as-num seconds* **示例：** `ciscoasa(config)# hold-time eigrp 2 60`	更改保持时间。

禁用自动路由摘要

默认情况下已启用自动路由摘要。 EIGRP 路由进程在网络号边界摘要。如果存在非邻接网络，这可能引起路由问题。

例如，如果路由器同时连接到 192.168.1.0、 192.168.2.0 和 192.168.3.0 网络，且这些网络全部参与 EIGRP，则 EIGRP 路由进程会为这些路由创建摘要地址 192.168.0.0。如果另一个路由器添加到网络 192.168.10.0 和 192.168.11.0，且这些网络均参与 EIGRP，则它们也会摘要为 192.168.0.0。为防止流量路由到错误位置的可能性，应在创建冲突性摘要地址的路由器上禁用自动路由摘要。

如要禁用自动路由摘要，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router eigrp** *as-num* **示例：** `ciscoasa(config)# router eigrp 2`	创建 EIGRP 路由进程，并输入此 EIGRP 进程的路由器配置模式。 *as-num* 参数是 EIGRP 路由进程的自治系统编号。
步骤 2	**no auto-summary** **示例：** `ciscoasa(config-router)# no auto-summary`	无法对此值进行配置。自动摘要地址的管理距离为 5。

在 EIGRP 中配置默认信息

可以控制 EIGRP 更新中默认路由信息的发送和接收。默认情况下，将发送并接受默认路由。如将 ASA 配置为禁止接收默认信息，则将导致候选默认路由位在收到的路由中被拦截。如将 ASA 配置为禁止发送默认信息，则可禁用通告路由中默认路由位的设置。

如要配置默认路由信息，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**router eigrp** *as-num* **示例：** `ciscoasa(config)# router eigrp 2`	创建 EIGRP 路由进程，并输入此 EIGRP 进程的路由器配置模式。 *as-num* 参数是 EIGRP 路由进程的自治系统编号。
步骤 2	`ciscoasa(config-router)#` **network** *ip-addr* [*mask*] **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`	配置参与 EIGRP 路由的接口和网络。可以使用此命令配置一个或多个网络语句。 已定义网络内的直接连接和静态网络由 ASA 通告。此外，已定义网络内只有带有 IP 地址的接口才参与 EIGRP 路由进程。 如果不希望接口参与 EIGRP 路由，但是该接口连接到希望通告的网络，请参阅第 23-5 页的配置 EIGRP 的接口。
步骤 3	**no default-information** {**in** | **out** | **WORD**} **示例：** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0` `ciscoasa(config-router)# no default-information {in | out | WORD}`	控制候选默认路由信息的发送或接收。 输入 **no default-information in** 命令会导致候选默认路由位在已收到路由中被拦截。输入 **no default-information out** 命令会禁用已通告路由中默认路由位的设置。

禁用 EIGRP 水平分割

水平分割控制 EIGRP 更新和查询数据包的发送。在接口上启用水平分割时，不会为此接口是下一跳的目标发送更新和查询数据包。以这种方式控制更新和查询数据包可减少路由环路的可能性。

默认情况下，水平分割在所有接口上均已启用。

水平分割可阻止路由器通告的路由信息从产生该信息的所有接口传出。此行为通常可优化多个路由设备之间的通信，尤其是在链路中断时。但是，使用非广播网络时，可能存在此行为不令人意的的情况。对于这些情况，包括配置了 EIGRP 的网络，可能需要禁用水平分割。

如果在某一接口上禁用水平分割，则必须也为该接口上所有路由器和接入服务器禁用水平分割。

如要禁用 EIGRP 水平分割，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**interface** *phy_if* **示例：** `ciscoasa(config)# interface phy_if`	为正在其上面更改 EIGRP 所用延迟值的接口输入接口配置模式。
步骤 2	**no split-horizon eigrp** *as-number* **示例：** `ciscoasa(config-if)# no split-horizon eigrp 2`	禁用水平分割。

重新启动 EIGRP 进程

如要重新启动 EIGRP 进程或清除重新分发或计数器，请输入以下命令：

命令	用途
clear eigrp pid {**1-65535** | **neighbors** | **topology** | **events)**} **示例：** `ciscoasa(config)# clear eigrp pid 10 neighbors`	重新启动 EIGRP 进程或清除重新分发或计数器。

监控 EIGRP

可以使用以下命令监控 EIGRP 路由进程。有关命令输出的示例和说明，请参阅命令参考。此外，您可以禁用邻居变更消息和邻居警告消息的日志记录。

如要监控或禁用多个 EIGRP 路由统计信息，请输入以下命令之一：

命令	用途
监控 EIGRP 路由	
router-id	显示此 EIGRP 进程的 router-id。
show eigrp [*as-number*] **events** [{*start end*} | **type**]	显示 EIGRP 事件日志。
show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]	显示参与 EIGRP 路由的接口。
show eigrp [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]	显示 EIGRP 邻居表。
show eigrp [*as-number*] **topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]	显示 EIGRP 拓扑表。

命令（续）	用途（续）
show eigrp [*as-number*] **traffic**	显示 EIGRP 流量统计信息。
show mfib cluster	显示转发条目和接口方面的 MFIB 信息。
show route cluster	显示用于集群的附加路由同步详细信息。
禁用 EIGRP 日志记录消息	
no eigrp log-neighbor-changes	禁用邻居更改消息的日志记录。在路由器配置模式中为 EIGRP 路由进程输入此命令。
no eigrp log-neighbor-warnings	禁用邻居警告消息的日志记录。

注 默认情况下，邻居更改消息和邻居警告消息均已记录。

EIGRP 的配置示例

以下示例显示如何通过多个可选进程启用和配置 EIGRP：

步骤 1 如要启用 EIGRP，请输入以下命令：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

步骤 2 如要配置从中发送或接收 EIGRP 路由消息的接口，请输入以下命令：

```
ciscoasa(config-router)# passive-interface {default}
```

步骤 3 如要定义 EIGRP 邻居，请输入以下命令：

```
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

步骤 4 如要配置参与 EIGRP 路由的接口和网络，请输入以下命令：

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

步骤 5 如要更改用于 EIGRP 距离计算的接口延迟值，请输入以下命令：

```
ciscoasa(config-router)# exit
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# delay 200
```

EIGRP 的功能历史记录

表 23-1 列出了各种功能变更以及实施该等功能变更的平台版本。

表 23-1 EIGRP 的功能历史记录

功能名称	平台版本	功能信息
EIGRP 支持	7.0(1)	增加了使用增强型内部网关路由协议 (EIGRP) 对路由数据、执行身份验证和重新分发及监控路由信息的支持。 我们引入了以下命令：**route eigrp**。
多情景模式中的动态路由	9.0(1)	EIGRP 路由在多情景模式中受支持。
集群	9.0(1)	对于 EIGRP，在集群环境中支持批量同步、路由同步和第 2 层负载均衡。 我们引入或修改了以下命令：**show route cluster**、**debug route cluster**、 **show mfib cluster**、 **debug mfib cluster**。
EIGRP 自动摘要	9.2(1)	默认情况下，Auto-Summary 字段现已禁用。

组播路由

本章介绍如何将思科 ASA 配置为使用组播路由协议。

- 第 24-1 页的有关组播路由的信息
- 第 24-3 页的组播路由的许可要求
- 第 24-3 页的准则和限制
- 第 24-3 页的启用组播路由
- 第 24-4 页的自定义组播路由
- 第 24-14 页的组播路由的配置示例
- 第 24-14 页的附加参考资料
- 第 24-15 页的组播路由的功能历史记录

有关组播路由的信息

组播路由是一种带宽节省技术，通过同时向数千个公司收件人和家庭传送单一信息流来减少流量。使用组播路由的应用包括视频会议、公司通信、远程教育以及软件、股票报价和新闻的分发。

组播路由协议将源流量传送给多个接收者，而不会对源或接收者造成任何额外负担，而且是同类技术当中占用网络带宽最少的。组播数据包通过启用了协议无关组播 (PIM) 及其他支持性组播协议的思科路由器在网络中复制，是目前为止向多个接收者传输数据的最高效方式。

ASA 支持末节组播路由和 PIM 组播路由。但是，不能在一个 ASA 上都配置这两种路由。

注 UDP 和非 UDP 传输均支持组播路由。但是，非 UDP 传输没有进行快速路径优化。

- 第 24-2 页的末节组播路由
- 第 24-2 页的 PIM 组播路由
- 第 24-2 页的组播组概念
- 第 24-2 页的集群

末节组播路由

末节组播路由提供动态主机注册并促进组播路由。如果针对末节组播路由进行了配置， ASA 将用作 IGMP 受托代理。ASA 将 IGMP 消息转发到上游组播路由器（上游组播路由器设置组播数据的传输），而不是完全参加组播路由。如果 ASA 针对末节组播路由进行了配置，则不能针对 PIM 进行配置。

ASA 支持 PIM-SM 和双向 PIM。PIM-SM 是一个组播路由协议，它使用基础单播路由信息库或支持组播的独立路由信息库。它为每个组播组构建以单一交汇点为根的单向共享树，或者为每个组播源创建最短路径树。

PIM 组播路由

双向 PIM 是 PIM-SM 的一种变体，用于构建连接组播源和接收者的双向共享树。双向树使用在每个组播拓扑链路上运行的 DF 选择进程来构建。在 DF 的帮助下，组播数据从源转发到交汇点，再从那里沿着共享树发送到接收者，而无需源特定状态。 DF 选择在交汇点发现过程中发生，并向交汇点提供默认路由。

注　如果 ASA 是 PIM 交汇点，请将 ASA 的逆向转换外部地址用作交汇点地址。

组播组概念

组播基于组概念。任意一组接收者对接收特定数据流表现出兴趣。这样的组没有任何物理边界或地理边界 - 主机可位于互联网上的任何位置。有兴趣接收流向特定组的数据的主机必须使用 IGMP 加入该组。如要接收数据流，主机必须是该组的成员。

组播地址

组播地址指定已加入某个组的任意一组 IP 主机，并希望接收发送到该组的流量。

集群

组播路由支持集群。在第 2 层集群中，在快速路径转发建立之前，主设备会发送所有的组播数据包和数据包。在建立快速路径转发后，从设备可能会转发组播数据包。所有数据流都是全流量。同时还支持末节转发流。由于第 2 层集群中仅有一台设备接收组播数据包，因此，常常会重定向到主设备。在第 3 层集群中，设备不会独立工作。所有的数据和路由数据包均由主设备处理和转发。从设备会丢弃已发送的所有数据包。

有关集群的更多信息，请参阅第 8 章，“ASA 集群”。

组播路由的许可要求

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景模式中受支持。在多情景模式中，非共享接口和共享接口不受支持。

防火墙模式准则

仅在路由防火墙模式中受支持。透明防火墙模式不受支持。

IPv6 准则

不支持 IPv6。

其他指导原则

在集群中，对于 IGMP 和 PIM，此功能仅在主设备上受支持。

启用组播路由

通过启用组播路由，可以在 ASA 上启用组播路由。默认情况下，启用组播路由可以在所有接口上启用 IGMP 和 PIM。 IGMP 用于了解直连子网上是否存在组成员。主机通过发送 IGMP 报告消息加入组播组。 PIM 用于维护转发表，以转发组播数据报。

注　组播路由仅支持 UDP 传输层。

如要启用组播路由，请输入以下命令：

命令	用途
multicast-routing **示例：** `ciscoasa(config)# multicast-routing`	启用组播路由。 组播路由表中的条目数量受限于 ASA 的 RAM 容量。

表 24-1 根据 ASA 的 RAM 容量列出了特定组播表的最大条目数。一旦达到这些限制，将会放弃所有新条目。

表 24-1　　组播表的条目限制

表	16 MB	128 MB	128+ MB
MFIB	1000	3000	30000
IGMP 组	1000	3000	30000
PIM 路由	3000	7000	72000

自定义组播路由

本节介绍如何自定义组播路由。

- 第 24-4 页的配置末节组播路由和转发 IGMP 消息
- 第 24-5 页的配置静态组播路由
- 第 24-5 页的配置 IGMP 功能
- 第 24-9 页的配置 PIM 功能
- 第 24-12 页的配置双向邻居过滤器
- 第 24-13 页的配置组播边界

配置末节组播路由和转发 IGMP 消息

注　末节组播路由和 PIM 不能同时受支持。

用作末节区域网关的 ASA 不需要加入到 PIM。相反，可以将该 ASA 配置为 IGMP 受托代理，并使其会从连接到一个接口的主机将 IGMP 消息转发到另一个接口上的上游组播路由器。如要将 ASA 配置为 IGMP 受托代理，请从末节区域将有关主机加入和离开的消息转发到上游接口

如要转发有关主机加入和离开的消息，请从连接到末节区域的接口输入以下命令：

命令	用途
igmp forward interface *if_name* **示例：** `ciscoasa(config-if)# igmp forward interface interface1`	配置末节组播路由并转发 IGMP 消息。

配置静态组播路由

配置静态组播路由可以将组播流量与单播流量分隔开。例如，如果源和目标之间的路由不支持组播路由，可以通过如下方法来解决这个问题：使用 GRE 隧道在它们之间配置两个组播设备，并通过该隧道发送组播数据包。

使用 PIM 时，ASA 期望用于接收数据包的接口和用于将单播数据包发送回到源的接口是同一个接口。在某些情况下（例如，绕过不支持组播路由的路由），您可能希望单播数据包和组播数据包使用不同的路径。

静态组播路由不能通告或重分布。

如要配置静态组播路由或末节区域的静态组播路由，请输入以下命令之一：

命令	用途
mroute *src_ip src_mask* {*input_if_name* | *rpf_neighbor*} [*distance*] **示例：** ciscoasa(config)# mroute *src_ip src_mask* {*input_if_name* | *rpf_neighbor*} [*distance*]	配置静态组播路由。
mroute *src_ip src_mask input_if_name* [**dense** *output_if_name*] [*distance*] **示例：** ciscoasa(config)# mroute *src_ip src_mask input_if_name* [dense *output_if_name*] [*distance*]	配置末节区域的静态组播路由。 末节组播路由仅支持 **dense** *output_if_name* 关键字-参数对。

配置 IGMP 功能

IP 主机使用互联网组管理协议 (IGMP) 将其组成员报告给直连组播路由器。

IGMP 用于在特定 LAN 上的一个组播组中动态注册单个主机。主机通过向其本地组播路由器发送 IGMP 消息来识别组成员。在 IGMP 下，路由器监听 IGMP 消息，并定期发出查询以发现特定子网上哪些组处于活动状态还是非活动状态。

IGMP 将组地址 （D 类 IP 地址）用作组标识符。主机组地址的范围可以是 224.0.0.0 到 239.255.255.255。地址 224.0.0.0 不分配给任何组。地址 224.0.0.1 分配给子网上的所有系统。地址 224.0.0.2 分配给子网上的所有路由器。

如果在 ASA 上启用组播路由，IGMP V2 将会在所有接口上自动启用。

注　使用 **show run** 命令时，接口配置中只会显示 **no igmp** 命令。如果设备配置中显示 **multicast-routing** 命令，则 IGMP 会在所有接口上自动启用。

本节介绍如何逐个接口配置可选的 IGMP 设置。

- 第 24-6 页的禁用接口上的 IGMP
- 第 24-6 页的配置 IGMP 组成员
- 第 24-6 页的配置静态加入的 IGMP 组
- 第 24-7 页的控制对组播组的访问

- 第 24-8 页的限制接口上的 IGMP 状态数量
- 第 24-8 页的修改发送到组播组的查询消息
- 第 24-9 页的更改 IGMP 版本

禁用接口上的 IGMP

可以禁用特定接口上的 IGMP。如果知道特定接口上没有组播接口，并且想要防止 ASA 通过该接口发送主机查询消息，则此信息很有用。

如要禁用接口上的 IGMP，请输入以下命令：

命令	用途
no igmp **示例：** `ciscoasa(config-if)# no igmp`	禁用接口上的 IGMP。 如要重新启用接口上的 IGMP，请使用 **igmp** 命令。

注　接口配置中仅显示 **no igmp** 命令。

配置 IGMP 组成员

可以将 ASA 配置为组播组的成员。配置 ASA 加入组播组会使上游路由器维护该组的组播路由表信息，并保持该组的路径处于活动状态。

注　如果要将特定组的组播数据包转发给接口，且无需 ASA 将这些数据包接受为该组的一部分，请参阅第 24-6 页的配置静态加入的 IGMP 组。

如要使 ASA 加入组播组，请输入以下命令：

命令	用途
igmp join-group *group-address* **示例：** `ciscoasa(config-if)# igmp join-group mcast-group`	将 ASA 配置为组播组的成员。 *group-address* 参数是该组的 IP 地址。

配置静态加入的 IGMP 组

有时候，由于某些配置，组成员无法报告其在组中的成员身份，或网段上的组可能没有成员。但是，您仍希望将该组的组播流量发送到该网段。可以通过配置静态加入的 IGMP 组将该组的组播流量发送到网段。

请输入 **igmp static-group** 命令。ASA 不接受组播数据包，而是将它们转发到指定的接口。

如要在接口上配置静态加入的组播组请输入以下命令：

命令	用途
igmp static-group **示例：** ciscoasa(config-if)# **igmp static-group** *group-address*	将 ASA 配置为静态加入到接口上的组播组。 *group-address* 参数是该组的 IP 地址。

控制对组播组的访问

如要控制 ASA 上的主机可加入的组播组，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	执行以下操作之一来创建标准或扩展 ACL：	
	access-list *name* **standard** [**permit** | **deny**] *ip_addr mask* **示例：** ciscoasa(config)# access-list *acl1* standard permit *192.52.662.25*	为组播流量创建标准 ACL。 可以为一个 ACL 创建多个条目。可以使用扩展或标准 ACL。 *ip_addr mask* 参数是被允许或拒绝的组播组的 IP 地址。
	access-list *name* **extended** [**permit** | **deny**] *protocol src_ip_addr src_mask dst_ip_addr dst_mask* **示例：** ciscoasa(config)# access-list *acl2* extended permit *protocol* src_*ip_addr* src_*mask dst_ip_addr dst_mask*	创建扩展 ACL。 *dst_ip_addr* 参数是被允许或拒绝的组播组的 IP 地址。
步骤 2	**igmp access-group** *acl* **示例：** ciscoasa(config-if)# igmp access-group *acl*	将 ACL 应用于接口。 *acl* 参数是标准或扩展 IP ACL 的名称。

限制接口上的 IGMP 状态数量

可以对每个接口限制 IGMP 成员报告造成的 IGMP 状态数量。超出所配置限制的成员报告不会输入到 IGMP 缓存中，多余成员报告的流量不会转发。

如要限制接口上的 IGMP 状态数量，请输入以下命令：

命令	用途
igmp limit *number* **示例：** `ciscoasa(config-if)# igmp limit 50`	限制接口上的 IGMP 状态数量。 有效值范围为 0 到 500，默认值是 500。将此值设置为 0 可防止获悉的组被添加，但仍允许手动定义成员（使用 **igmp join-group** 和 **igmp static-group** 命令）。此命令的 **no** 形式将恢复默认值。

修改发送到组播组的查询消息

注　**igmp query-timeout** 和 **igmp query-interval** 命令需要 IGMP V2。

ASA 发送查询消息，以发现哪些组播组有成员位于与接口连接的网络上。成员以 IGMP 报告消息作出响应，以表明自己想要接收特定组的组播数据包。查询消息会发送到全系统组播组，该组的地址为 224.0.0.1，生存时间值为 1。

这些消息会定期发送，从而刷新 ASA 上存储的成员信息。如果 ASA 发现组播组中没有本地成员仍与接口相连接，它会停止向连接的网络转发该组的组播数据包，并会向数据包源发送回删除消息。

默认情况下，子网上的 PIM 指定路由器负责发送查询消息。默认情况下，每 125 秒发送一次消息。

默认情况下，更改查询响应时间时，IGMP 查询中通告的最大查询响应时间为 10 秒。如果 ASA 不在此时间内接收对于主机查询的响应，它就会删除该组。

如要更改查询间隔时间、查询响应时间和查询超时值，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**igmp query-interval** *seconds* **示例：** `ciscoasa(config-if)# igmp query-interval 30`	设置查询间隔时间，以秒为单位。 有效值范围为 0 到 500；默认值是 125。 如果 ASA 不能在指定超时值（默认值是 255 秒）内在接口上收到查询消息，ASA 将会成为指定路由器并开始发送查询消息。
步骤 2	**igmp query-timeout** *seconds* **示例：** `ciscoasa(config-if)# igmp query-timeout 30`	更改查询的超时值。 有效值范围为 0 到 500；默认值是 225。
步骤 3	**igmp query-max-response-time** *seconds* **示例：** `ciscoasa(config-if)# igmp query-max-response-time 30`	更改最大查询响应时间。

更改 IGMP 版本

默认情况下，ASA 运行 IGMP V2；此版本启用了多项附加功能，例如 **igmp query-timeout** 和 **igmp query-interval** 命令。

子网上所有的组播路由器必须支持同一版本的 IGMP。ASA 不会自动检测 IGMP V1 路由器并切换到 IGMP V1。但是，可以在子网上结合使用 IGMP V1 和 IGMP V2 主机；当存在 IGMP V1 主机时，运行 IGMP V2 的 ASA 可正常工作。

要控制哪个版本的 IGMP 在接口上运行，请输入以下命令：

命令	用途
igmp version {**1** | **2**} **示例：** `ciscoasa(config-if)# igmp version 2`	控制要在接口上运行的 IGMP 版本。

配置 PIM 功能

路由器使用 PIM 来维护转发表，以便用于转发组播图。如果在 ASA 上启用组播路由，PIM 和 IGMP 将会在所有接口上自动启用。

注　PAT 不支持 PIM。PIM 协议不使用端口，PAT 只能与使用端口的协议配合使用。

本节介绍如何配置可选的 PIM 设置。

- 第 24-10 页的在接口上启用和禁用 PIM
- 第 24-10 页的配置静态交汇点地址
- 第 24-11 页的配置指定路由器优先级
- 第 24-11 页的配置和过滤 PIM 注册消息
- 第 24-11 页的配置 PIM 消息间隔时间
- 第 24-12 页的过滤 PIM 邻居

在接口上启用和禁用 PIM

可以在特定接口上启用或禁用 PIM。要在接口上启用或禁用 PIM，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**pim** **示例：** `ciscoasa(config-if)# pim`	在特定接口上启用或重新启用 PIM。
步骤 2	**no pim** **示例：** `ciscoasa(config-if)# no pim`	在特定接口上禁用 PIM。

注　接口配置中仅显示 **no pim** 命令。

配置静态交汇点地址

常见 PIM 稀疏模式中或 bidir 域中的所有路由器均需要了解 PIM RP 地址。该地址使用 **pim rp-address** 命令进行静态配置。

注　ASA 不支持 Auto-RP 或 PIM BSR。必须使用 **pim rp-address** 命令来指定 RP 地址。

可以将 ASA 配置为用作多个组的 RP。 ACL 中指定的组范围确定 PIM RP 组映射。如果未指定 ACL，则一个组的 RP 将应用于整个组播组范围 (224.0.0.0/4)。

如要配置 PIM PR 的地址，请输入以下命令：

命令	用途
pim rp-address *ip_address* [*acl*] [**bidir**] **示例：** `ciscoasa(config)# pim rp-address` `10.86.75.23 [acl1] [bidir]`	在特定接口上启用或重新启用 PIM。 *ip_address* 参数是分配为 PIM RP 的路由器的单播 IP 地址。 *acl* 参数是定义应与 RP 一起使用的组播组的标准 ACL 的名称或编号。请勿将主机 ACL 与此命令配合使用。 排除 **bidir** 关键字会使组在 PIM 稀疏模式中运行。

注　ASA 始终会在 PIM hello 消息中通告双向功能，无论实际的双向配置如何。

配置指定路由器优先级

指定路由器 (DR) 负责将 PIM 注册消息、加入消息和删除消息发送到 RP。如果网段上有多个组播路由器，将会根据 DR 优先级来选择 DR。如果多台设备具有同样的 DR 优先级，则具有最高 IP 地址的设备将会成为 DR。

默认情况下，ASA 的 DR 优先级为 1。要更改此值，请输入以下命令：

命令	用途
pim dr-priority *num* **示例：** `ciscoasa(config-if)# pim dr-priority 500`	配置指定路由器优先级。 *num* 参数可以是介于 1 到 4294967294 之间的任意数字。

配置和过滤 PIM 注册消息

当 ASA 作为 RP 时，您可以禁止特定的组播源注册到 ASA，从而防止未授权的源注册到 RP。Request Filter 窗格可用于定义 ASA 将会接受 PIM 注册消息的组播源。

如要过滤 PIM 注册消息，请输入以下命令：

命令	用途
pim accept-register {**list** *acl* | **route-map** *map-name*} **示例：** `ciscoasa(config)# pim accept-register {list acl1 | route-map map2}`	配置 ASA 以过滤 PIM 注册消息。 在此示例中，ASA 过滤 PIM 注册消息 *acl1* 和路由映射 *map2*。

配置 PIM 消息间隔时间

路由器查询消息用于选择 PIM DR。PIM DR 负责发送路由器查询消息。默认情况下，每隔 30 秒发送一次路由器查询消息。此外，ASA 每隔 60 秒发送一次 PIM 加入消息或删除消息。

如要更改这些间隔时间，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**pim hello-interval** *seconds* **示例：** `ciscoasa(config-if)# pim hello-interval 60`	发送路由器查询消息。 *seconds* 参数的有效值范围为 1 到 3600 秒。
步骤 2	**pim join-prune-interval** *seconds* **示例：** `ciscoasa(config-if)# pim join-prune-interval 60`	更改 ASA 会发送 PIM 加入消息或删除消息的时间段（以秒为单位）。 *seconds* 参数的有效值范围为 10 到 600 秒。

过滤 PIM 邻居

可以定义可成为 PIM 邻居的路由器。通过过滤可成为 PIM 邻居的路由器，可以实现以下目的：

- 防止未授权的路由器成为 PIM 邻居。
- 防止连接的末节路由器加入到 PIM。

如要定义可成为 PIM 邻居的邻居，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**access-list pim_nbr deny** *router-IP_addr PIM neighbor* **示例：** `ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255`	使用标准 ACL 定义要加入到 PIM 的路由器。 在此示例中，以下 ACL 与 **pim neighbor-filter** 命令配合使用可防止 10.1.1.1 路由器成为 PIM 邻居。
步骤 2	**pim neighbor-filter pim_nbr** **示例：** `ciscoasa(config)# interface GigabitEthernet0/3` `ciscoasa(config-if)# pim neighbor-filter pim_nbr`	过滤邻居路由器。 此示例防止 10.1.1.1 路由器在接口 GigabitEthernet0/3 上成为 PIM 邻居。

配置双向邻居过滤器

Bidirectional Neighbor Filter 窗格显示在 ASA 上配置的 PIM 双向邻居过滤器（如果有）。 PIM 双向邻居过滤器是定义可参与 DF 选择的邻居设备的 ACL。如果接口未配置 PIM 双向邻居过滤器，则没有限制。如果配置了 PIM 双向邻居过滤器，则只有 ACL 允许的邻居可参加 DF 选择进程。

如果 PIM 双向邻居过滤器配置应用于 ASA，名称为 *interface-name*_multicast 的运行配置中会显示 ACL，其中，*interface-name* 是应用组播边界过滤器的接口的名称。如果已存在使用该名称的 ACL，将会给名称加上一个数字（例如，inside_multicast_1）。此 ACL 定义哪些设备可成为 ASA 的 PIM 邻居。

双向 PIM 使组播路由器可以保留减少的状态信息。如要选择 DF，必须为 bidir 双向启用分段中的所有组播路由器。

PIM 双向邻居过滤器允许指定应参与 DF 选择的路由器，同时仍允许所有路由器加入到稀疏模式域，从而实现从纯稀疏模式网络到 bidir 网络的过渡。支持 bidir 的路由器可以从它们本身当中选择 DF，即使分段上有非 bidir 路由器。非 bidir 路由器上的组播边界可防止 bidir 组中的 PIM 消息和数据泄漏到 bidir 子集云中或从 bidir 子集云泄漏出去。

如果启用了 PIM 双向邻居过滤器，ACL 允许的路由器将被视为具有双向功能。因此，以下说法均是正确的：

- 如果一个获允许的邻居不支持 bidir，将不会发生 DF 选择。
- 如果一个被拒绝的邻居支持 bidir，将不会发生 DF 选择。
- 如果一个被拒绝的邻居不支持 bidir，可能会发生 DF 选择。

如要定义可成为 PIM 双向邻居过滤器的邻居，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**access-list pim_nbr deny** *router-IP_addr PIM neighbor* **示例：** `ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255`	使用标准 ACL 定义要加入到 PIM 的路由器。 在此示例中，以下 ACL 与 **pim neighbor-filter** 命令配合使用可防止 10.1.1.1 路由器成为 PIM 邻居。
步骤 2	**pim bidirectional-neighbor-filter pim_nbr** **示例：** `ciscoasa(config)# interface GigabitEthernet0/3` `ciscoasa(config-if)# pim bidirectional neighbor-filter pim_nbr`	过滤邻居路由器。 此示例防止 10.1.1.1 路由器在接口 GigabitEthernet0/3 上成为 PIM 双向邻居。

配置组播边界

地址范围定义域边界，从而使具有 IP 地址相同的 RP 的域不会相互泄漏。可在大型域内的子网边界以及域与互联网之间的边界上执行范围界定。

可以通过以下做法在接口上为组播组地址设置使用管理权限界定的边界：**Configuration > Routing > Multicast > MBoundary** 输入 **multicast boundary** 命令。 IANA 已将 239.0.0.0 到 239.255.255.255 的组播地址范围指定为可使用管理权限界定的地址。此地址范围可在不同组织管理的域中重用。此类地址被视为本地地址，而不是全局唯一地址。

标准 ACL 定义受影响地址的范围。设置边界后，不允许组播数据包从任一方向流经边界。边界允许同一个组播组地址在不同的管理域中重用。

可以通过输入 **filter-autorp** 关键字在使用管理权限界定的边界配置、检查和过滤 Auto-RP 发现消息和通知消息。Auto-RP 数据包中被边界 ACL 拒绝的任意 Auto-RP 组范围通知都会被移除。仅在 Auto-RP 组范围中的所有地址获边界 ACL 允许的情况下，Auto-RP 组范围通知才可以通过边界。如果有任何地址未获允许，在 Auto-RP 消息被转发前，将会过滤整个组范围并将其从 Auto-RP 消息中移除。

如要配置组播边界，请输入以下命令：

命令	用途
multicast boundary *acl* [**filter-autorp**] **示例：** `ciscoasa(config-if)# multicast boundary acl1 [filter-autorp]`	配置组播边界。

组播路由的配置示例

以下示例显示如何使用各个可选过程启用和配置组播路由：

步骤 1　启用组播路由：

```
ciscoasa(config)# multicast-routing
```

步骤 2　配置静态组播路由：

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
ciscoasa(config)# exit
```

步骤 3　将 ASA 配置为组播组的成员：

```
ciscoasa(config)# interface
ciscoasa(config-if)# igmp join-group group-address
```

附加参考资料

有关路由的其他信息，请参阅以下各节：

- 第 24-14 页的相关文档
- 第 24-14 页的 RFC

相关文档

相关主题	文档标题
用于实施 SMR 功能的 IGMP 和组播路由标准的技术详细信息	IETF draft-ietf-idmr-igmp-proxy-01.txt

RFC

RFC	标题
RFC 2113	IP 路由器告警选项
RFC 2236	IGMPv2
RFC 2362	PIM-SM
RFC 2588	IP 组播和防火墙

组播路由的功能历史记录

表 24-2 列出了各种功能变更以及实施该等功能变更的平台版本。

表 24-2　　组播路由的功能历史记录

功能名称	平台版本	功能信息
组播路由支持	7.0(1)	增加了对于组播路由数据、身份验证以及使用组播路由协议重发布和监控路由信息的支持。 引入了 **multicast-routing** 命令。
集群支持	9.0(1)	增加了集群支持。 引入了以下命令：**debug mfib cluster**、**show mfib cluster**。

IPv6 邻居发现

- 第 25-1 页的有关 IPv6 邻居发现的信息
- 第 25-3 页的 IPv6 邻居发现的许可要求
- 第 25-3 页的 IPv6 邻居发现的先决条件
- 第 25-4 页的准则和限制
- 第 25-5 页的 IPv6 邻居发现的默认设置
- 第 25-5 页的配置 IPv6 邻居发现
- 第 25-11 页的监控 IPv6 邻居发现
- 第 25-11 页的附加参考资料
- 第 25-12 页的 IPv6 邻居发现的功能历史记录

有关 IPv6 邻居发现的信息

IPv6 邻居发现过程使用 ICMPv6 消息和请求节点组播地址，确定同一网络 （本地链路）中邻居的链路层地址、验证邻居的可读性及跟踪相邻路由器。

节点 （主机）使用邻居发现确定已知驻留在连接的链路上邻居的链路层地址并快速清除变为无效的缓存值。主机还使用邻居发现查找愿意代表自己转发数据包的邻居路由器。此外，节点使用协议主动跟踪哪些邻居可到达及哪些邻居不可达，并检测已更改的链路层地址。当路由器或路由器的路径发生故障时，主机会主动搜索起作用的替代项。

- 第 25-2 页的邻居请求消息
- 第 25-2 页的邻居可到达时间
- 第 25-2 页的重复地址检测
- 第 25-2 页的路由器通告消息
- 第 25-3 页的静态 IPv6 邻居

邻居请求消息

邻居请求消息 （ICMPv6 类型 135）由尝试发现本地链路上其他节点的链路层地址的节点在本地链路上发送。邻居请求消息发送到请求的节点组播地址。邻居请求消息的源地址是发送邻居请求消息的节点的 IPv6 地址。邻居请求消息还包括源节点的链路层地址。

在收到邻居请求消息后，目标节点通过在本地链路上发送邻居通告消息 （ICPMv6 类型 136）作出应答。邻居通告消息的源地址是发送邻居通告消息的节点的 IPv6 地址；目标地址是发送邻居请求消息的节点的 IPv6 地址。邻居通告消息的数据部分包括发送邻居通告消息的节点的链路层地址。

源节点接收邻居通告后，源节点与目标节点即可通信。

识别邻居的链路层地址后，邻居请求消息也用于验证邻居的可达性。当节点要验证邻居的可达性时，邻居请求消息中的目标地址是邻居的单播地址。

本地链路中一个节点的链路层地址发生变化时，也会发送邻居通告消息。当发生此类变化时，邻居通告的目标地址是所有节点组播地址。

邻居可到达时间

邻居可到达时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快，但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。

重复地址检测

在无状态自动配置过程中，重复地址检测可在新的单播 IPv6 地址被分配给接口之前验证该地址的唯一性 （执行重复地址检测时，新地址保持暂定状态）。重复地址检测首先在新的链路本地地址上执行。当链路本地地址经过验证为唯一时，重复地址检测在接口上所有其他 IPv6 单播地址上执行。

重复地址检测在处于管理性关闭状态的接口上暂停。当接口处于管理性关闭状态时，单播 IPv6 地址将分配给设置为处于挂起状态的接口。恢复管理性打开状态的接口将重新启动对接口上所有单播 IPv6 地址的重复地址检测。

识别出重复地址后，该地址的状态会设置为 DUPLICATE，且不会使用该地址并生成以下错误消息：

```
%ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface
```

如果重复地址是接口的链接本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。但是，地址的状态设置为 DUPLICATE 时，与重复地址关联的所有配置命令均持为已配置。

如果接口的链路本地地址发生变化，则会将新的链路本地地址执行重复地址检测，并将重新生成与接口关联的所有其他 IPv6 地址 （重复地址检测仅在新的链路本地地址上执行）。

ASA 使用邻居请求消息执行重复地址检测。默认情况下，接口执行重复地址检测的次数为 1。

路由器通告消息

思科 ASA 可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。路由器通告消息（ICMPv6 类型 134）定期被发送出 ASA 的每个 IPv6 配置接口。路由器通告消息发送到所有节点组播地址。

路由器通告消息通常包括以下信息：

- 可供本地链路上节点用于自动配置其 IPv6 地址的一个或多个 IPv6 前缀。

- 通告中包括的每个前缀的有效期信息。
- 标志集，指示可以完成的自动配置的类型 （无状态或有状态）。
- 默认路由器信息 （发送通告的路由器是否应作为默认路由器，以及如果是，路由器应用作默认路由器的持续时间 [秒]）。
- 主机的其他信息，如主机在其发送的数据包中应使用的跳数限制和 MTU。
- 给定链路上邻居请求消息重新传输之间的时间。
- 节点将邻居视为可到达的时间。

也会发送路由器通告，以响应路由器请求消息 （ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。由于路由器请求消息通常由主机在系统启动时发送，而主机没有配置的单播地址，因此，路由器请求消息的源地址通常是未指定的 IPv6 地址 (0:0:0:0:0:0:0:0)。如果主机有一个配置的单播地址，则发送路由器请求消息的接口的单播地址将用作消息的源地址。路由器请求消息的目标地址是链路范围内所有路由器组播地址。当发送路由器通告以响应路由器请求时，路由器通告消息的目标地址是路由器请求消息的源的单播地址。

可以为路由器通告消息配置以下设置：

- 定期路由器通告消息之间的时间间隔。
- 路由器有效期值，指示 IPv6 节点应将 ASA 视为默认路由器的时间。
- 链路中使用的 IPv6 网络前缀。
- 接口是否传输路由器通告消息。

除非另有说明，否则路由器通告消息设置特定于接口并在接口配置模式中输入。

静态 IPv6 邻居

可以在 IPv6 邻居缓存中手动定义一个邻居。如果指定 IPv6 地址的条目在邻居发现缓存中已存在（已通过 IPv6 邻居发现过程获悉），则该条目会自动转换为静态条目。邻居发现过程不会修改 IPv6 邻居发现缓存中的静态条目。

IPv6 邻居发现的许可要求

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

IPv6 邻居发现的先决条件

请根据第 11-10 页的配置 IPv6 寻址配置 IPv6 地址。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

仅在路由模式中受支持。透明模式不受支持。

附加准则和限制

- 时间间隔值包括在发送出该接口的所有 IPv6 路由器通告中。
- 配置的时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快，但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。
- 如果使用 **ipv6 nd ra-lifetime** 命令将 ASA 配置为默认路由器，则传输之间的时间间隔应小于或等于 IPv6 路由器通告的有效期。为防止与其他 IPv6 节点的同步，请将所用的实际值随机调整为指定值的 20% 以内。
- **ipv6 nd prefix** 命令可按前缀控制各个参数，包括是否应该通告前缀。
- 默认情况下，接口上使用 **ipv6 addres** 命令配置为地址的前缀在路由器通告中通告。如果使用 **ipv6 nd prefix** 命令为通告配置前缀，则仅通告这些前缀。
- **default** 关键字可用于为所有前缀设置默认参数。
- 可以设置日期来指定前缀的过期日期。实时倒计时有效有效期和首选有效期。到达过期日期后，将不再会通告前缀。
- 在链路上打开 （默认情况下）时，指定的前缀会分配给该链路。向包含指定前缀的此类地址发送流量的节点会将目标视为在链路上本地可到达。
- 当自动配置启用 （默认情况下）时，它向本地链路上的主机指示可将指定前缀用于 IPv6 自动配置。
- 为使无状态自动配置正常运行，路由器通告消息中通告的前缀长度必须始终为 64 位。
- 路由器有效期值包括在发送出接口的所有 IPv6 路由器通告中。值表示作为该接口上默认路由器的 ASA 用途。
- 将值设置为非零值表示应将 ASA 视为该接口的默认路由器。路由器有效期值的非零值不能小于路由器通告间隔时间。

以下准则和限制适用于配置静态 IPv6 邻居：

- **ipv6 neighbor** 命令类似于 **arp** 命令。如果指定 IPv6 地址的条目在邻居发现缓存中已存在（已通过 IPv6 邻居发现过程获悉），则该条目会自动转换为静态条目。当使用复制命令存储配置时，这些条目存储在配置中。
- 使用 **show ipv6 neighbor** 命令可查看 IPv6 邻居发现缓存中的静态条目。
- **clear ipv6 neighbor** 命令可删除 IPv6 邻居发现缓存中除静态条目之外的所有条目。 **no ipv6 neighbor** 命令可从邻居发现缓存中删除指定的静态条目；该命令不会从缓存中移除动态条目，这些条目从 IPv6 邻居发现过程中获悉。使用 **no ipv6 enabl** 命令在接口上禁用 IPv6 可删除为该接口配置的所有 IPv6 邻居发现缓存条目，静态条目 （条目的状态更改为 INCMP [Incomplete]）之外。
- 邻居发现过程不会修改 IPv6 邻居发现缓存中的静态条目。
- **clear ipv6 neighbor** 命令不会从 IPv6 邻居发现缓存中移除静态条目；仅会清除动态条目。

- IPv6 邻居条目的定期刷新生成了 ICMP 系统日志。 IPv6 邻居条目的 ASA 默认计时器为 30 秒，因此，ASA 将大约每 30 秒生成 ICMPv6 邻居发现和响应数据包。如果 ASA 拥有用 IPv6 地址配置的故障转移 LAN 和状态接口，则 ASA 将每 30 秒为配置的和链路本地的 IPv6 地址生成 ICMPv6 邻居发现和响应数据包。此外，由于每个数据包将生成多个系统日志 （ICMP 连接和本地主机创建或拆卸），因此，似乎一直在不断生成 ICMP 系统日志。可以在常规数据接口上配置 IPv6 邻居条目的刷新时间，但是，不可在故障转移接口上配置。但是，此 ICMP 邻居发现流量对 CPU 的影响最小。

IPv6 邻居发现的默认设置

表 25-1 列出 IPv6 邻居发现的默认设置。

表 25-1　　默认的 IPv6 邻居发现参数

参数	默认值
value for the neighbor solicitation transmission message interval	邻居请求传输之间为 1000 秒。
value for the neighbor reachable time	默认值为 0。
value for the router advertisement transmission interval	默认值为 200 秒。
value for the router lifetime	默认值为 1800 秒。
value for the number of consecutive neighbor solicitation messages sent during DAD	默认值为一条消息。
prefix lifetime	默认有效期为 2592000 秒 （30 天），首选有效期为 604800 秒 （7 天）。
on-link flag	该标志已默认打开，表示前缀用于通告接口上。
autoconfig flag	该标志已默认打开，表示前缀用于自动配置。
static IPv6 neighbor	静态条目不在 IPv6 邻居发现缓存中配置。

配置 IPv6 邻居发现

- 第 25-6 页的进入接口配置模式
- 第 25-6 页的配置邻居请求消息间隔
- 第 25-7 页的配置邻居可到达时间
- 第 25-7 页的配置路由器通告传输时间间隔
- 第 25-8 页的配置路由器有效期值
- 第 25-8 页的配置 DAD 设置
- 第 25-9 页的抑制路由器通告消息
- 第 25-9 页的为 IPv6 DHCP 中继配置地址配置标志
- 第 25-10 页的配置路由器通告中的 IPv6 前缀
- 第 25-11 页的配置静态 IPv6 邻居

进入接口配置模式

配置每个接口的邻居发现设置。如要进入接口配置模式，请执行以下步骤。

详细步骤

命令	用途
接口 *名称* **示例：** `hostname(config)# interface gigabitethernet 0/0` `hostname(config-if)#`	进入接口配置模式。

配置邻居请求消息间隔

如要在接口上配置 IPv6 邻居请求重新传输之间的时间间隔，请输入以下命令。

详细步骤

命令	用途
ipv6 nd ns-interval *value* **示例：** `hostname (config-if)# ipv6 nd ns-interval 9000`	设置接口上 IPv6 邻居请求重新传输之间的时间间隔。 值参数的有效值范围为 1000 至 3600000 毫秒。 此信息也在路由器通告消息中发送。

示例

以下示例为千兆以太网 0/0 配置 9000 毫秒的 IPv6 邻居请求传输时间间隔：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ns-interval 9000
```

配置邻居可到达时间

如要配置可访问性确认事件发生后远程 IPv6 节点被视为可到达的时间，请输入以下命令。

详细步骤

命令	用途
ipv6 nd reachable-time *value* **示例：** `hostname (config-if)# ipv6 nd reachable-time 1700000`	设置远程 IPv6 节点可到达的时间。 *value* 参数的有效值范围为 0 至 3600000 毫秒。 当该值为 0 时，将发送未确定的可到达时间 由接收设备来设置和跟踪可到达时间的值。

示例

以下示例为选定的接口千兆以太网 0/0 配置 1700000 毫秒的 IPv6 可到达时间：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd reachable-time 1700000
```

配置路由器通告传输时间间隔

如要在接口上配置 IPv6 路由器通告传输之间的时间间隔，请输入以下命令。

详细步骤

命令	用途
ipv6 nd ra-interval [**msec**] *value* **示例：** `hostname (config-if)# ipv6 nd ra-interval 201`	设置 IPv6 路由器通告传输之间的时间间隔。 可选 **msec** 关键字表示所提供的值以毫秒为单位。如果此关键字不存在，则提供的值以秒为单位。 如果提供了 **msec** 关键字，则 *value* 参数的有效值范围为 3 至 1800 秒或 500 至 1800000 毫秒。 如将 ASA 配置为默认路由器，则传输之间的时间间隔应小于或等于 IPv6 路由器通告的有效期。有关详细信息，请参阅第 25-8 页的配置路由器有效期值。为防止与其他 IPv6 节点的同步，请将所用的实际值随机调整为所需值的 20% 以内。

示例

以下示例为选定的接口千兆以太网 0/0 配置 201 秒的 IPv6 路由器通告时间间隔：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-interval 201
```

配置路由器有效期值

如要在接口上配置 IPv6 路由器通告的路由器有效期值，请输入以下命令。

详细步骤

命令	用途
ipv6 nd ra-lifetime [**msec**] *value* **示例：** `hostname (config-if)# ipv6 nd ra-lifetime 2000`	指定本地链路上的节点应将 ASA 视为链路上默认路由器的时间长度。 可选 **msec** 关键字表示所提供的值以毫秒为单位。如果此关键字不存在，则提供的值以秒为单位。 *value* 参数的有效值范围为 0 至 9000 秒。 输入 0 表示不应将 ASA 被视为选定接口的默认路由器。

示例

以下示例为选定的接口千兆以太网 0/0 配置 2000 秒的 IPv6 路由器有效期值：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-lifetime 2000
```

配置 DAD 设置

如要在接口上指定 DAD 设置，请输入以下命令。

详细步骤

命令	用途
ipv6 nd dad attempts *value* **示例：** `hostname (config-if)# ipv6 nd dad attempts 20`	在分配新的单播 IPv6 地址之前指定其唯一性，并确保在链路基础上检测网络中的重复 IPv6 地址。 *value* 参数的有效值范围为 0 至 600。零值可在指定的接口上禁用 DAD 处理。

示例

以下示例为选定的接口千兆以太网 0/0 配置 DAD 尝试值 20：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd dad attempts 20
```

抑制路由器通告消息

路由器通告消息将自动发送，以响应路由器请求消息。在不想要 ASA 提供 IPv6 前缀的所有接口（例如，外部接口）上，您可能想要禁用这些消息。

如要在接口上抑制 IPv6 路由器通告中路由器有效期值，请输入以下命令。

详细步骤

命令	用途
ipv6 nd suppress-ra *seconds* **示例：** `hostname (config-if)# ipv6 nd suppress-ra 900`	抑制路由器有效期值 *seconds* 参数将 ASA 的有效性指定为该接口的默认路由器。有效值范围为 0 到 9000 秒。零值表示不应将 ASA 视为指定接口的默认路由器。 输入此命令会导致 ASA 显示为链路上的常规 IPv6 邻居，而不是显示为 IPv6 路由器。

示例

以下示例抑制指定的接口千兆以太网 0/0 的 IPv6 路由器通告传输：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd suppress-ra 900
```

为 IPv6 DHCP 中继配置地址配置标志

可以向 IPv6 路由器通告添加标志，以通知 IPv6 自动配置客户端使用 DHCPv6 来获取 IPv6 地址和/或其他信息，如 DNS 服务器地址。

详细步骤

命令	用途
ipv6 nd managed-config-flag **示例：** `hostname (config-if)# ipv6 nd managed-config-flag`	在 IPv6 路由器通告数据包中设置受管地址配置标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 来获取相关地址以及派生的无状态自动配置地址。
ipv6 nd other-config-flag **示例：** `hostname (config-if)# ipv6 nd other-config-flag`	在 IPv6 路由器通告数据包中设置其他地址配置标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。

配置路由器通告中的 IPv6 前缀

如要配置哪些 IPv6 前缀包括在 IPv6 路由器通告中，请输入以下命令。

详细步骤

命令	用途
ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**] **示例：** `hostname (config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900`	配置哪些 IPv6 前缀包括在 IPv6 路由器通告中。前缀通告可供邻居设备用于自动配置其接口地址。无状态自动配置使用路由器通告消息中提供的 IPv6 前缀从链路本地地址创建全局单播地址。 **at** *valid-date preferred-date* 语法表示有效期和首选项到期的日期和时间。到达该指定的日期和时间之前，前缀均有效。日期的表示格式为 *date-valid-expire month-valid-expire hh:mm-valid-expire* *date-prefer-expire month-prefer-expire hh:mm-prefer-expire*。 **default** 关键字表示使用的默认值。 可选 **infinite** 关键字指定有效的有效期不过期。 *ipv6-prefix* 参数指定路由器通告中要包括的 IPv6 网络号。此参数必须采用 RFC 2373 中记录的形式，其中地址是用冒号分隔的十六进制 16 位值。 可选 **no-advertise** 关键字向本地链路上的主机指示不将指定的前缀用于 IPv6 自动配置。 可选 **no-autoconfig** 关键字向本地链路上的主机指示指定的前缀无法用于 IPv6 自动配置。 可选 **off-link** 关键字表示指定的前缀将不用于非链路确定。 *preferred-lifetime* 参数指定将指定的 IPv6 前缀作为首选前缀进行通告的时间（以秒为单位）。有效值范围为 0 到 4294967295 秒。最大值代表无穷大，还可以使用无限指定。默认值为 604800 秒 （7 天）。 *prefix-length* 参数指定 IPv6 前缀的长度。该值表示组成前缀网络部分的地址高位、连续位的数量。斜线 (/) 必须在前缀长度前。 *valid-lifetime* 参数指定将指定的 IPv6 前缀通告为有效的持续时间 （以秒为单位）。有效值范围为 0 到 4294967295 秒。最大值代表无穷大，还可以使用无限指定。默认值为 2592000 秒 （30 天）。

示例

以下示例包括 IPv6 prefix 2001:DB8::/32，其中已指定接口千兆以太网 0/0 发出的路由器通告的有效有效期为 1000 秒，首选有效期为 900 秒：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

配置静态 IPv6 邻居

如要在 IPv6 邻居发现缓存中配置静态条目，请输入以下命令。

详细步骤

命令	用途
ipv6 neighbor *ipv6_address if_name mac_address* **示例：** `hostname(config-if)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472`	在 IPv6 邻居发现缓存中配置静态条目。 *ipv6_address* 参数是邻居的链路本地 IPv6 地址，*if_name* 参数是邻居借以可用的接口，*mac_address* 参数是邻居接口的 MAC 地址。

示例

以下示例将 IPv6 地址为 3001:1::45A 且 MAC 地址为 002.7D1a.9472 的内部主机的静态条目添加到邻居发现缓存：

```
hostname(config-if)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

监控 IPv6 邻居发现

如要监控 IPv6 邻居发现参数，请输入以下命令：

命令	用途
show ipv6 interface	显示为 IPv6 配置的接口的可用性状态。包括接口名称，例如“outside”，并显示指定接口的设置。从命令排除名称并显示已启用 IPv6 的所有接口的设置。命令输出显示以下信息： • 接口的名称和状态。 • 链路本地和全局单播地址。 • 接口所属的组播组。 • ICMP 重新定向和错误消息设置。 • 邻居发现设置。 • 命令设置为 0 时的实际时间。 • 正在使用的邻居发现可到达时间。

附加参考资料

有关实施 IPv6 前缀的其他信息，请参阅以下主题：

- 第 25-12 页的 IPv6 前缀的相关文档
- 第 25-12 页的 IPv6 前缀的 RFC 和文档

IPv6 前缀的相关文档

相关主题	文档标题
ipv6 命令	*命令参考*

IPv6 前缀的 RFC 和文档

RFC	标题
RFC 2373 包含完整文档，显示如何在路由器通告中必须显示 IPv6 网络地址编号。命令参数 *ipv6-prefix* 指示此网络号，其中地址必须以十六进制格式指定，冒号之间使用 16 位值。	IPv6 寻址架构
RFC 3849 指定在文档中使用 IPv6 地址前缀的要求。预留用于文档中的 IPv6 单播地址前缀为 2001:DB8::/32。	预留给文档的 IPv6 地址前缀

IPv6 邻居发现的功能历史记录

表 25-2 列出了各种功能变更以及实施该等功能变更的平台版本。

表 25-2　　IPv6 邻居发现的功能历史记录

功能名称	版本	功能信息
IPv6 邻居发现	7.0(1)	我们引入了此功能。 我们引入了以下命令：**ipv6 nd ns-interval**、 **ipv6 nd ra-lifetime**、**ipv6 nd suppress-ra**、**ipv6 neighbor**、**ipv6 nd prefix**、 **ipv6 nd dad-attempts**、 **ipv6 nd reachable-time**、 **ipv6 address**、**ipv6 enforce-eui64**。
IPv6 DHCP 中继的地址配置标志	9.0(1)	我们引入了以下命令：**ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag**、

第 7 部分

AAA 服务器和本地数据库

关于 AAA 的信息

本章介绍身份验证、授权和记帐（AAA，也称为“3A”）。AAA 是一组服务，用于控制对计算机资源的访问、强制实施策略、评估使用情况并提供对服务进行计费所需的信息。这些过程对于高效进行网络管理和安全性而言至关重要。

- 第 26-1 页的身份验证
- 第 26-2 页的授权
- 第 26-2 页的记帐
- 第 26-2 页的身份验证、授权和记帐之间的交互
- 第 26-2 页的 AAA 服务器
- 第 26-2 页的 AAA 服务器组
- 第 26-2 页的本地数据库支持

身份验证

身份验证提供了一种标识用户的方法，这种方法通常先请用户输入有效用户名和有效密码，然后再授予访问权限。AAA 服务器将用户的身份验证凭证与数据库中存储的其他用户凭证进行比较。如果凭证匹配，则允许用户访问网络。如果凭证不匹配，则身份验证失败，并拒绝网络访问。

您可以配置思科 ASA，以便对下列各项进行身份验证：

- 所有与 ASA 建立的管理连接，包括下列会话：
  - Telnet
  - SSH
  - 串行控制台
  - 使用 HTTPS 的 ASDM
  - VPN 管理访问
- **enable** 命令
- 网络访问
- VPN 访问

授权

授权是强制实施策略的过程：确定允许用户访问哪些类型的活动、资源或服务。对用户进行身份验证后，可能会授权该用户执行各种类型的访问或活动。

您可以配置 ASA 以便对下列各项进行授权：

- 管理命令
- 网络访问
- VPN 访问

记帐

记帐用于测量用户在访问期间使用的资源量，这可以包括系统时间长度或者用户在会话期间发送或接收的数据量。记帐是通过记录会话统计信息和使用量信息来执行的，这些信息用于进行授权控制、计费、趋势分析、资源利用和容量规划活动。

身份验证、授权和记帐之间的交互

您可以单独使用身份验证功能，也可以将其与授权和记帐功能配合使用。授权始终要求先对用户进行身份验证。您可以单独使用记帐功能，也可以将其与身份验证和授权功能配合使用。

AAA 服务器

AAA 服务器是用于进行访问控制的网络服务器。身份验证用于标识用户。授权实现策略，这些策略确定经过身份验证的用户能够访问哪些资源和服务。记帐对时间和数据资源进行追踪，这些资源用于计费和分析。

AAA 服务器组

如果要使用外部 AAA 服务器进行身份验证、授权或记帐，您必须先为每种 AAA 协议创建至少一个 AAA 服务器组，并向每个组添加一个或多个服务器。您通过名称来标识 AAA 服务器组。每个服务器组都专门用于一种类型的服务器或服务。

本地数据库支持

ASA 维护一个本地数据库，您可以将用户配置文件填入其中。您可以使用本地数据库代替 AAA 服务器来提供用户身份验证、授权和记帐。

用于 AAA 的本地数据库

本章介绍如何配置用于 AAA 的本地服务器。

- 第 27-1 页的关于本地数据库
- 第 27-2 页的本地数据库准则
- 第 27-3 页的向本地数据库添加用户帐户
- 第 27-6 页的监控本地数据库
- 第 27-7 页的本地数据库的历史

关于本地数据库

您可以使用本地数据库实现下列功能：

- ASDM 每用户访问
- 控制台身份验证
- Telnet 和 SSH 身份验证
- **enable** 命令身份验证

  此设置仅适用于 CLI 访问，而不会影响思科 ASDM 登录。
- 命令授权

  如果您使用本地数据库开启命令授权，思科 ASA 将根据用户的权限级别来确定可用的命令。否则，通常不使用权限级别。默认情况下，所有命令的权限级别均为 0 或 15。
- 网络访问身份验证
- VPN 客户端身份验证

对于多情景，您可以在系统执行空间中配置用户名，以便在 CLI 中使用 **login** 命令提供个人登录；但是，您不能在系统执行空间中配置任何使用本地数据库的 AAA 规则。

注 您不能使用本地数据库进行网络访问授权。

回退支持

本地数据库可以充当多项功能的回退方法。此行为旨在帮助您避免意外被锁定而无法登录 ASA。

用户登录时，将从配置中指定的第一个服务器开始逐个访问组中的服务器，直到有服务器作出响应为止。如果组中的所有服务器都不可用，并且您已将本地数据库配置为回退方法（仅用于管理身份验证和授权），则 ASA 将尝试使用本地数据库。如果未配置任何回退方法，则 ASA 将继续尝试使用 AAA 服务器。

对于需要回退支持的用户，我们建议您确保本地数据库中的用户名和密码与 AAA 服务器上的用户名和密码匹配。这种做法将提供透明的回退支持。由于用户无法确定是 AAA 服务器还是本地数据库正在提供服务，因此，如果 AAA 服务器上使用的用户名和密码与本地数据库中的用户名和密码不同，用户将无法确定应该提供哪个用户名和密码。

本地数据库支持下列回退功能：

- 控制台和启用密码身份验证 - 如果组中的服务器全部不可用，则 ASA 将使用本地数据库对管理访问进行身份验证，这还可以包括启用密码身份验证。
- 命令授权 - 如果组中的 TACACS+ 服务器全部不可用，则使用本地数据库根据权限级别进行命令授权。
- VPN 身份验证和授权 - 支持 VPN 身份验证和授权，以便在通常支持这些 VPN 服务的 AAA 服务器不可用时，启用对 ASA 的远程访问。如果管理员的 VPN 客户端指定了配置为回退到本地数据库的隧道组，只要本地数据库配置了必要的属性，即使 AAA 服务器组不可用，也可以建立 VPN 隧道。

组中存在多个服务器时的回退方式

如果在服务器组中配置了多个服务器，并且对于该服务器组允许回退到本地数据库，则该组中没有任何服务器对来自 ASA 的身份验证请求作出响应时，将会进行回退。为了说明这一点，请考虑以下场景：

您配置了一个 LDAP 服务器组，其中依次包含两个 Active Directory 服务器，即服务器 1 和服务器 2。当远程用户登录时，ASA 将尝试向服务器 1 进行身份验证。

如果服务器 1 作出了身份验证失败响应（例如*找不到用户*），则 ASA 不会尝试向服务器 2 进行身份验证。

如果服务器 1 在超时期限内未作出响应（或者尝试进行身份验证的次数超过配置的最大值），则 ASA 尝试服务器 2。

如果该组中的两个服务器均未作出响应，并且 ASA 配置为回退到本地数据库，则 ASA 将尝试向本地数据库进行身份验证。

本地数据库准则

在使用本地数据库进行身份验证或授权时，请确保避免被锁定而无法登录 ASA。

相关主题

第 35-29 页的从锁定中恢复

向本地数据库添加用户帐户

如要向本地数据库添加用户，请执行以下步骤：

操作步骤

步骤 1　创建用户帐户。

username *username* {**nopassword** | **password** *password*} [**privilege** *priv_level*]

示例：

```
ciscoasa(config)# username exampleuser1 privilege 1
```

username *user*name 关键字是长度为 4 到 64 个字符的字符串。 **password** *password* 关键字是长度为 3 到 32 个字符的字符串。**privilege** *priv_level* 关键字用于设置范围为 0 到 15 的权限级别。默认值为 2。此权限级别用于命令授权。

注意事项　如果未使用命令授权（**AAA 授权控制台的 LOCAL** 命令），则默认级别 2 允许对特权 EXEC 模式进行管理访问。如果要限制对特权 EXEC 模式的访问，请将权限级别设置为 0 或 1，或者使用 **service-type** 命令。

nopassword 关键字用于创建没有密码的用户帐户。**encrypted** 关键字表示密码已加密。如果在 **username** 命令中定义了密码，则 ASA 在将该密码保存到配置时会对其进行加密，以确保安全。当您输入 **show running-config** 命令时，**username** 命令不会显示实际密码，而是显示已加密的密码，后跟 **encrypted** 关键字。例如，如果您输入了密码“test”，则 **show running-config** 输出将显示类似于以下的内容：

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

只有在剪切并粘贴配置文件以便在另一个 ASA 中使用，并且要使用同一个密码时，才真正需要在 CLI 中输入 **encrypted** 关键字。

步骤 2　（可选）配置用户名属性。

username *username* **attributes**

示例：

```
ciscoasa(config)# username exampleuser1 attributes
```

username 参数是您在第一步中创建的用户名。

默认情况下，使用此命令添加的 VPN 用户不具有任何属性或组策略关联。您必须使用 **username attributes** 命令明确配置所有的值。有关详细信息，请参阅 《VPN 配置指南》。

步骤 3　（或者）如果使用 **aaa authorization exec** 命令配置了管理授权，请配置用户级别。

service-type {**admin** | **nas-prompt** | **remote-access**}

示例：

```
ciscoasa(config-username)# service-type admin
```

admin 关键字允许对 **aaa authentication console LOCAL** 命令指定的任何服务进行完全访问。**admin** 关键字是默认值。

nas-prompt 关键字允许访问 CLI（如果您配置了 **aaa authentication {telnet | ssh | serial} console** 命令），但拒绝 ASDM 配置访问 （如果您配置了 **aaa authentication http console** 命令）。允许进行 ASDM 监控访问。如果您使用 **aaa authentication enable console** 命令启用了身份验证，则用户无法使用 **enable** 命令 （或 **login** 命令）访问特权 EXEC 模式。

remote-access 关键字用于拒绝管理访问。您无法使用 **aaa authentication console** 命令指定的任何服务 （不包括 **serial** 关键字；允许进行串行访问）。

步骤 4　对于与 ASA 的 SSH 连接，按每个用户启用公钥身份验证。

ssh authentication {**pkf** | **publickey** *key* [**hashed**]}

示例：

```
ciscoasa(config-username)# ssh authentication pkf

输入 SSH 公钥格式文件。
请以 "quit" 一词结尾 （独占一行）：
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config-username)#
```

您可以指定公钥文件 (PKF) 格式的密钥 （**pkf** 关键字）或 Base64 密钥 （**publickey** 关键字）。对于 **publickey**，*key* 是 Base64 编码的公钥。您可以使用任何能够生成 SSH-RSA 原始密钥（不含证书）的 SSH 密钥生成软件 （例如 ssh keygen）来生成密钥。

对于 **pkf** 密钥，系统将会提示您粘贴 PKF 格式的密钥，其长度可达 4096 位。对于由于过长而无法以 Base64 格式粘贴内联的密钥，请使用此格式。例如，您可以使用 ssh keygen 生成一个 4096 位的密钥，然后将其转换为 PKF，并使用 **pkf** 关键字让系统提示您输入该密钥。

注　您可以将 **pkf** 选项用于故障转移，但 PKF 密钥不会自动复制到备用系统。必须输入 **write standby** 命令对 PKF 密钥进行同步。

在 ASA 上使用 **show running-config username** 命令查看密钥时，密钥将使用 SHA-256 哈希算法进行加密。即使您输入了 **pkf** 形式的密钥，ASA 也会对该密钥进行哈希处理，并将其显示为经过哈希处理的 **publickey**。如果需要从 **show** 的输出中复制密钥，请指定 **publickey** 类型和 **hashed** 关键字。

步骤 5　（可选）如果要使用此用户名进行 VPN 身份验证，则可以为用户配置许多 VPN 属性。有关详细信息，请参阅 《VPN 配置指南》。

示例

以下示例向管理员用户帐户分配权限级别 15：

```
ciscoasa(config)# username admin password password privilege 15
```

以下示例创建没有密码的用户帐户。

```
ciscoasa(config)# username user34 nopassword
```

以下示例启用管理授权，创建具有密码的用户帐户，进入用户名配置模式，并指定 **service-type** 为 **nas-prompt**：

```
ciscoasa(config)# aaa authorization exec authentication-server
ciscoasa(config)# username user1 password gOgeOus
ciscoasa(config)# username user1 attributes
ciscoasa(config-username)# service-type nas-prompt
```

以下示例在 Linux 或 Macintosh 系统上生成用于 SSH 的共享密钥，并将其导入到 ASA 中：

步骤 1　在计算机上生成 4096 位的 ssh-rsa 公钥和私钥：

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)?y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + .E          |
|  o o            |
| ooooo           |
+-----------------+
```

步骤 2　将该密钥转换为 PKF 格式：

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by ramona@rboersma-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

步骤 3　将该密钥复制到剪贴板。

步骤 4　连接到 ASA CLI，并将该公钥添加到您的用户名：

```
ciscoasa(config)# username test attributes
ciscoasa(config-username)# ssh authentication pkf
输入 SSH 公钥格式文件。
请以 "quit" 一词结尾 (独占一行)：
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by ramona@rboersma-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+561+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file completed successfully.
```

步骤 5　验证用户 (test) 是否能够与 ASA 建立 SSH 连接：

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

系统将显示以下对话框，以供您输入口令：

同时，终端会话将显示以下内容：

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

监控本地数据库

请查看下列命令以监控本地数据库：

- **show aaa-server**

此命令显示已配置的数据库的统计信息。要清除 AAA 服务器配置，请输入 **clear aaa-server statistics** 命令。

- **show running-config aaa-server**

  此命令显示 AAA 服务器运行配置。要清除 AAA 服务器统计信息，请输入 **clear configure aaa-server** 命令。

本地数据库的历史

表 27-1　　本地数据库的历史

功能名称	平台版本	功能信息
AAA 的本地数据库配置	7.0(1)	讨论如何配置本地数据库以供 AAA 使用。 我们引入了以下命令： **username**、 **aaa authorization exec authentication-server**、 **aaa authentication console LOCAL**、 **aaa authorization exec LOCAL**、 **service-type**、 **aaa authentication {telnet | ssh | serial} console LOCAL**、 **aaa authentication http console LOCAL**、 **aaa authentication enable console LOCAL**、 **show running-config aaa-server**、 **show aaa-server**、 **clear configure aaa-server** 和 **clear aaa-server statistics**。
对 SSH 公钥身份验证的支持	9.1(2)	现在，对于与 ASA 的 SSH 连接，您可以按每个用户启用公钥身份验证。您可以指定公钥文件 (PKF) 格式的密钥或 Base64 密钥。PKF 密钥的长度可达 4096 位。对于由于过长而导致 ASA 不支持使用 Base64 格式 （限长 2048 位）的密钥，请使用 PKF 格式。 我们引入了以下命令：**ssh authentication**。 *在 8.4(4.1) 中也可用；PKF 密钥格式支持仅在 9.1(2) 中提供。*

AAA RADIUS 服务器

本章介绍如何配置 AAA RADIUS 服务器。

- 第 28-1 页的有关 RADIUS 服务器
- 第 28-13 页的 RADIUS 服务器许可要求
- 第 28-13 页的准则和限制
- 第 28-14 页的配置 RADIUS 服务器
- 第 28-19 页的监控 RADIUS 服务器
- 第 28-19 页的附加参考资料
- 第 28-20 页的 RADIUS 服务器功能历史

有关 RADIUS 服务器

思科 ASA 支持以下兼容 RFC 的 AAA RADIUS 服务器：

- 思科安全 ACS 3.2、 4.0、 4.1、 4.2 和 5.x
- 思科身份服务引擎 (ISE)
- RSA 身份验证管理器 5.2、 6.1 和 7.x 中的 RSA RADIUS
- Microsoft

- 第 28-1 页的支持的身份验证方法
- 第 28-2 页的 VPN 连接的用户身份验证
- 第 28-2 页的支持的 RADIUS 属性集
- 第 28-2 页的支持的 RADIUS 授权属性
- 第 28-12 页的支持的 IETF RADIUS 授权属性
- 第 28-12 页的 RADIUS 记账断开原因代码

支持的身份验证方法

ASA 使用 RADIUS 服务器支持以下身份验证方法：

- PAP - 适用于所有连接类型。
- CHAP 和 MS-CHAPv1 - 适用于 L2TP-over-IPsec 连接。

- MS-CHAPv2 - 适用于 L2TP-over-IPsec 连接和常规 IPsec 远程访问连接（当密码管理功能被启用时）。您也可以通过无客户端连接使用 MS-CHAPv2。
- 身份验证代理模式 - 适用于 RADIUS-to Active-Directory、 RADIUS-to-RSA/SDI、RADIUS-to-Token 服务器和 RSA/SDI-to-RADIUS 连接。

注　为了将 MS-CHAPv2 启用为 ASA 与 RADIUS 服务器之间使用的协议以实现 VPN 连接，您必须在隧道组常规属性里启用密码管理。启用密码管理将生成一个从 ASA 到 RADIUS 服务器的 MS-CHAPv2 身份验证请求。有关详细信息，请参阅 **password-management** 命令说明。

如果在隧道组中使用双重身份验证并启用密码管理，则主要身份验证请求和辅助身份验证请求包含 MS-CHAPv2 请求属性。如果 RADIUS 服务器不支持 MS-CHAPv2，您可以使用 **no mschapv2-capable** 命令，将该服务器配置为发送非 MS CHAPv2 的身份验证请求。

VPN 连接的用户身份验证

ASA 可以使用 RADIUS 服务器进行 VPN 远程访问和防火墙直接转发代理会话的用户验证（按用户使用动态 ACL 或 ACL 名称）。如要实施动态 ACL，您必须将 RADIUS 服务器配置为支持动态 ACL。在用户进行身份验证时，RADIUS 服务器向 ASA 发送可下载的 ACL 或 ACL 名称。ACL 允许或拒绝对指定服务的访问。当身份验证会话超时的时候，ASA 将删除 ACL。

除了 ACL，ASA 还支持许多其他的授权属性和 VPN 远程访问以及防火墙直接转发代理会话的权限设置。

支持的 RADIUS 属性集

ASA 支持以下 RADIUS 属性集：

- RFC 2138 定义的身份验证属性。
- RFC 2139 定义的记账属性。
- RFC 2868 定义的用于隧道协议支持的 RADIUS 属性。
- RADIUS 供应商 ID 9 确定的思科 IOS 供应商特定属性 (VSA)。
- RADIUS 供应商 ID 3076 确定的思科 VPN 相关 VSA。
- RFC 2548 定义的 Microsoft VSA。
- Cisco VSA (Cisco-Priv-Level) 提供 0 至15 级标准数字权限等级，最低等级 1，最高等级 15。等级 0 表示没有权限。等级 1（登录）对该等级可用的命令允许执行特权执行模式。等级 2（启用）允许 CLI 配置权限。

支持的 RADIUS 授权属性

授权指的是实施权限或属性的进程。如果已配置权限或属性，被定义为身份验证服务器的 RADIUS 服务器可以实施权限或属性。这些属性具有供应商 ID 3076。

表 28-1 列出了受支持的 RADIUS 属性，这些属性可用于用户授权。

注　RADIUS 属性名称不包含 cVPN3000 前缀。思科安全 ACS 4.x 支持这一新的命名法，但是， ACS 4.0 之前版本中的属性名仍然包含 cVPN3000 前缀。 ASA 基于属性数字 ID 而非属性名来实施 RADIUS 属性。

表 28-1 列出的所有属性都是从 RADIUS 服务器发送到 ASA 的下行属性，以下编号的属性除外：146、150、151 和 152。这些编号的属性是从 ASA 发送到 RADIUS 服务器的上行属性。RADIUS 属性 146 和 150 是从 ASA 发送到 RADIUS 服务器用于身份验证和授权请求的属性。以上所列的四个属性都是从 ASA 发送到 RADIUS 服务器用于记账开始请求、临时更新请求和停止请求的属性。 8.4(3) 版本引入了上行 RADIUS 属性 146、 150、 151 和 152。

在版本 9.0(1) 中，对于使用 RADIUS 身份验证进行的 IP 地址分配，思科 ACS 5.x 和思科 ISE 不支持 IPv6 框架 IP 地址。

表 28-1　　支持的 RADIUS 授权属性

属性名	ASA	属性编号	语法/类型	单值或多值	说明或值
Access-Hours	有	1	字符串	单值	时间范围名称，例如工作时间
Access-List-Inbound	有	86	字符串	单值	ACL ID
Access-List-Outbound	有	87	字符串	单值	ACL ID
Address-Pools	有	217	字符串	单值	IP 本地地址池名称
Allow-Network-Extension-Mode	有	64	布尔值	单值	0 = 禁用 1 = 启用
Authenticated-User-Idle-Timeout	有	50	整数	单值	1 - 35791394 分钟
Authorization-DN-Field	有	67	字符串	单值	可能值：UID、 OU、 O、 CN、 L、 SP、 C、 EA、 T、 N、 GN、 SN、 I、 GENQ、 DNQ、 SER、 use-entire-name
Authorization-Required		66	整数	单值	0 = 否 1 = 是
Authorization-Type	有	65	整数	单值	0 = 无 1 = RADIUS 2 = LDAP
Banner1	有	15	字符串	单值	为思科 VPN 远程访问会话显示的横幅字符串：IPsec IKEv1、AnyConnect SSL TLS/DTLS/IKEv2 和 Clientless SSL。
Banner2	有	36	字符串	单值	为思科 VPN 远程访问会话显示的横幅字符串：IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2 和 Clientless SSL。如果进行了相应的配置，Banner2 字符串将被与 Banner1 字符串联系在一起。
Cisco-IP-Phone-Bypass	有	51	整数	单值	0 = 禁用 1 = 启用

表 28-1　　支持的 RADIUS 授权属性（续）

属性名	ASA	属性编号	语法/类型	单值或多值	说明或值
Cisco-LEAP-Bypass	有	75	整数	单值	0 = 禁用 1 = 启用
Client Type	有	150	整数	单值	1 = Cisco VPN 客户端 (IKEv1) 2 = AnyConnect 客户端 SSL VPN 3 = 无客户端 SSL VPN 4 = 直接转发代理 5 = L2TP/IPsec SSL VPN 6 = AnyConnect 客户端 IPsec VPN (IKEv2)
Client-Type-Version-Limiting	有	77	字符串	单值	IPsec VPN 版本号字符串
DHCP-Network-Scope	有	61	字符串	单值	IP 地址
Extended-Authentication-On-Rekey	有	122	整数	单值	0 = 禁用 1 = 启用
Group-Policy	有	25	字符串	单值	为远程访问 VPN 会话设置组策略。对于 8.2.x 版本和更高版本，使用该属性而非 IETF-Radius-Class。您可以使用以下任一格式： • *组策略名称* • OU = *组策略名称* • OU = *组策略名称*;
IE-Proxy-Bypass-Local		83	整数	单值	0 = 无 1 = 本地
IE-Proxy-Exception-List		82	字符串	单值	新行 (\n) 分隔 DNS 域列表
IE-Proxy-PAC-URL	有	133	字符串	单值	PAC 地址字符串
IE-Proxy-Server		80	字符串	单值	IP 地址
IE-Proxy-Server-Policy		81	整数	单值	1 = 不修改 2 = 不使用代理服务器 3 = 自动检测 4 = 使用集中器设置
IKE-KeepAlive-Confidence-Interval	有	68	整数	单值	10 - 300 秒
IKE-Keepalive-Retry-Interval	有	84	整数	单值	2 - 10 秒
IKE-Keep-Alives	有	41	布尔值	单值	0 = 禁用 1 = 启用
Intercept-DHCP-Configure-Msg	有	62	布尔值	单值	0 = 禁用 1 = 启用
IPsec-Allow-Passwd-Store	有	16	布尔值	单值	0 = 禁用 1 = 启用

表 28-1　　支持的 RADIUS 授权属性（续）

属性名	ASA	属性编号	语法/类型	单值或多值	说明或值
IPsec-Authentication		13	整数	单值	0 = 无 1 = RADIUS 2 = LDAP（仅限授权） 3 = NT 域 4 = SDI 5 = 内部 6 = 支持有效期的 RADIUS 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	有	42	布尔值	单值	0 = 禁用 1 = 启用
IPsec-Backup-Server-List	有	60	字符串	单值	服务器地址 （空格分隔）
IPsec-Backup-Servers	有	59	字符串	单值	1 = 使用客户端配置的列表 2 = 禁用并清除客户端列表 3 = 使用备份服务器列表
IPsec-Client-Firewall-Filter-Name		57	字符串	单值	指定要被推入客户端 （作为防火墙策略）的过滤器的名称
IPsec-Client-Firewall-Filter-Optional	有	58	整数	单值	0 = 要求 1 = 可选
IPsec-Default-Domain	有	28	字符串	单值	指定要发送到客户端的单个默认域名 （1 - 255 个字符）。
IPsec-IKE-Peer-ID-Check	有	40	整数	单值	1 = 要求 2 = 对等证书是否支持 3 = 不检测
IPsec-IP-Compression	有	39	整数	单值	0 = 禁用 1 = 启用
IPsec-Mode-Config	有	31	布尔值	单值	0 = 禁用 1 = 启用
IPsec-Over-UDP	有	34	布尔值	单值	0 = 禁用 1 = 启用
IPsec-Over-UDP-Port	有	35	整数	单值	4001 - 49151 默认值为 10000。
IPsec-Required-Client-Firewall-Capability	有	56	整数	单值	0 = 无 1 = 远程防火墙 Are-You-There (AYT) 定义的策略 2 = 策略推送的 CPP 4 = 来自服务器的策略
IPsec-Sec-Association		12	字符串	单值	安全关联的名称
IPsec-Split-DNS-Names	有	29	字符串	单值	指定要发送到客户端的辅助域名列表 （1 - 255 个字符）。
IPsec-Split-Tunneling-Policy	有	55	整数	单值	0 = 无分割隧道 1 = 分割隧道 2 = 获准的本地 LAN
IPsec-Split-Tunnel-List	有	27	字符串	单值	指定描述隧道包含列表的网络或 ACL 名称。

表 28-1　　支持的 RADIUS 授权属性（续）

属性名	ASA	属性编号	语法/类型	单值或多值	说明或值
IPsec-Tunnel-Type	有	30	整数	单值	1 = LAN 对 LAN 2 = 远程访问
IPsec-User-Group-Lock		33	布尔值	单值	0 = 禁用 1 = 启用
IPv6-Address-Pools	有	218	字符串	单值	IP 本地地址池 IPv6 的名称
IPv6-VPN-Filter	有	219	字符串	单值	ACL 值
L2TP-Encryption		21	整数	单值	位图： 1 = 要求加密 2 = 40 位 4 = 128 位 8 = 要求无状态 15= 40/128 要求加密/无状态
L2TP-MPPC-Compression		38	整数	单值	0 = 禁用 1 = 启用
Member-Of	有	145	字符串	单值	逗号分隔的字符串，例如： `Engineering, Sales` 可在动态访问策略里使用的管理属性。不设置组策略。
MS-Client-Subnet-Mask	有	63	布尔值	单值	IP 地址
NAC-Default-ACL		92	字符串		ACL
NAC-Enable		89	整数	单值	0 = 否 1 = 是
NAC-Revalidation-Timer		91	整数	单值	300 - 86400 秒
NAC-Settings	有	141	字符串	单值	NAC 策略名称
NAC-Status-Query-Timer		90	整数	单值	30 - 1800 秒
Perfect-Forward-Secrecy-Enable	有	88	布尔值	单值	0 = 否 1 = 是
PPTP-Encryption		20	整数	单值	位图： 1 = 要求加密 2 = 40 位 4 = 128 位 8 = 要求无状态 15= 40/128 要求加密/无状态
PPTP-MPPC-Compression		37	整数	单值	0 = 禁用 1 = 启用
Primary-DNS	有	5	字符串	单值	IP 地址
Primary-WINS	有	7	字符串	单值	IP 地址
Privilege-Level	有	220	整数	单值	介于 0 和 15 之间的整数。

表 28-1　　支持的 RADIUS 授权属性（续）

属性名	ASA	属性编号	语法/类型	单值或多值	说明或值
Required-Client- Firewall-Vendor-Code	有	45	整数	单值	1 = 思科系统 （带思科集成客户端） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = 思科系统 （带思科入侵防御安全代理）
Required-Client-Firewall-Description	有	47	字符串	单值	字符串
Required-Client-Firewall-Product-Code	有	46	整数	单值	思科系统产品： 1 = 思科入侵防御安全代理或思科集成客户端 (CIC) Zone Labs 产品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 产品： 1 = BlackIce Defender/代理 Sygate 产品： 1 = 个人防火墙 2 = 个人防火墙专业版 3 = 安全代理
Required-Individual-User-Auth	有	49	整数	单值	0 = 禁用 1 = 启用
Require-HW-Client-Auth	有	48	布尔值	单值	0 = 禁用 1 = 启用
Secondary-DNS	有	6	字符串	单值	IP 地址
Secondary-WINS	有	8	字符串	单值	IP 地址
SEP-Card-Assignment		9	整数	单值	未使用
Session Subtype	有	152	整数	单值	0 = 无 1 = 无客户端 2 = 客户端 3 = 仅客户端 会话子类型仅限于Session Type (151) 属性为以下值时：1、 2、 3 和 4。

表 28-1　　支持的 RADIUS 授权属性（续）

属性名	ASA	属性编号	语法/类型	单值或多值	说明或值
Session Type	有	151	整数	单值	0 = 无 1 = AnyConnect 客户端 SSL VPN 2 = AnyConnect 客户端 IPSec VPN (IKEv2) 3 = 无客户端 SSL VPN 4 = 无客户端邮件代理 5 = Cisco VPN 客户端 (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN 负载均衡
Simultaneous-Logins	有	2	整数	单值	0 - 2147483647
Smart-Tunnel	有	136	字符串	单值	智能隧道的名称
Smart-Tunnel-Auto	有	138	整数	单值	0 = 禁用 1 = 启用 2 = 自动启动
Smart-Tunnel-Auto-Signon-Enable	有	139	字符串	单值	域名附加的智能隧道自动登录列表名称
Strip-Realm	有	135	布尔值	单值	0 = 禁用 1 = 启用
SVC-Ask	有	131	字符串	单值	0 = 禁用 1 = 启用 3 = 启用默认服务 5 = 启用默认无客户端 （未使用 2 和 4）
SVC-Ask-Timeout	有	132	整数	单值	5 - 120 秒
SVC-DPD-Interval-Client	有	108	整数	单值	0 = 关闭 5 - 3600 秒
SVC-DPD-Interval-Gateway	有	109	整数	单值	0 = 关闭 5 - 3600 秒
SVC-DTLS	有	123	整数	单值	0 = 假 1 = 真
SVC-Keepalive	有	107	整数	单值	0 = 关闭 15 - 600 秒
SVC-Modules	有	127	字符串	单值	字符串 （模块名）
SVC-MTU	有	125	整数	单值	MTU 值 256 - 1406 个字节
SVC-Profiles	有	128	字符串	单值	字符串 （文件名）
SVC-Rekey-Time	有	110	整数	单值	0 = 禁用 1 - 10080 分钟
Tunnel Group Name	有	146	字符串	单值	(1 - 253 个字符)
Tunnel-Group-Lock	有	85	字符串	单值	隧道组名或“无”

表 28-1　　支持的 RADIUS 授权属性（续）

属性名	ASA	属性编号	语法/类型	单值或多值	说明或值
Tunneling-Protocols	有	11	整数	单值	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 和 4 相互排斥。 0 - 11、16 - 27、32 - 43、48 - 59 为合法值。
Use-Client-Address		17	布尔值	单值	0 = 禁用 1 = 启用
VLAN	有	140	整数	单值	0 - 4094
WebVPN-Access-List	有	73	字符串	单值	访问列表名称
WebVPN ACL	有	73	字符串	单值	设备上的 WebVPN ACL 名称
WebVPN-ActiveX-Relay	有	137	整数	单值	0 = 禁用 Otherwise = 启用
WebVPN-Apply-ACL	有	102	整数	单值	0 = 禁用 1 = 启用
WebVPN-Auto-HTTP-Signon	有	124	字符串	单值	保留
WebVPN-Citrix-Metaframe-Enable	有	101	整数	单值	0 = 禁用 1 = 启用
WebVPN-Content-Filter-Parameters	有	69	整数	单值	1 = Java ActiveX 2 = Java 脚本 4 = 映像 8 = 映像内的 Cookie
WebVPN-Customization	有	113	字符串	单值	定制名称
WebVPN-Default-Homepage	有	76	字符串	单值	URL（例如 http://example-example.com）
WebVPN-Deny-Message	有	116	字符串	单值	有效字符串 （500 个字符）
WebVPN-Download_Max-Size	有	157	整数	单值	0x7fffffff
WebVPN-File-Access-Enable	有	94	整数	单值	0 = 禁用 1 = 启用
WebVPN-File-Server-Browsing-Enable	有	96	整数	单值	0 = 禁用 1 = 启用
WebVPN-File-Server-Entry-Enable	有	95	整数	单值	0 = 禁用 1 = 启用
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	有	78	字符串	单值	带可选通配符 (*) 的逗号分隔的 DNS/IP （例如 *.cisco.com, 192.168.1.*, wwwin.cisco.com）
WebVPN-Hidden-Shares	有	126	整数	单值	0 = 无 1 = 可见

表 28-1　支持的 RADIUS 授权属性（续）

属性名	ASA	属性编号	语法/类型	单值或多值	说明或值
WebVPN-Home-Page-Use-Smart-Tunnel	有	228	布尔值	单值	启用 （无客户端主页将通过智能隧道呈现时）。
WebVPN-HTML-Filter	有	69	位图	单值	1 = Java ActiveX 2 = 脚本 4 = 映像 8 = Cookie
WebVPN-HTTP-Compression	有	120	整数	单值	0 = 关闭 1 = 解压压缩
WebVPN-HTTP-Proxy-IP-Address	有	74	字符串	单值	逗号分隔的 DNS/IP:端口，带 http= 或 https= 前缀 （例如 http=10.10.10.10:80, https=11.11.11.11:443）
WebVPN-Idle-Timeout-Alert-Interval	有	148	整数	单值	0 - 30。 0 = 禁用。
WebVPN-Keepalive-Ignore	有	121	整数	单值	0 - 900
WebVPN-Macro-Substitution	有	223	字符串	单值	无限制。例如，请在以下 URL 中参阅 *《SSL VPN 部署指南》*： http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Macro-Substitution	有	224	字符串	单值	无限制。例如，请在以下 URL 中参阅 *《SSL VPN 部署指南》*： http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Port-Forwarding-Enable	有	97	整数	单值	0 = 禁用 1 = 启用
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	有	98	整数	单值	0 = 禁用 1 = 启用
WebVPN-Port-Forwarding-HTTP-Proxy	有	99	整数	单值	0 = 禁用 1 = 启用
WebVPN-Port-Forwarding-List	有	72	字符串	单值	端口转发列表名称
WebVPN-Port-Forwarding-Name	有	79	字符串	单值	字符串名称 （例如，Corporate-Apps）。 此文本将取代无客户端门户主页上默认的字符串“Application Access”。
WebVPN-Post-Max-Size	有	159	整数	单值	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	有	149	整数	单值	0 - 30。 0 = 禁用。
WebVPN Smart-Card-Removal-Disconnect	有	225	布尔值	单值	0 = 禁用 1 = 启用

表 28-1　　支持的 RADIUS 授权属性（续）

属性名	ASA	属性编号	语法/类型	单值或多值	说明或值
WebVPN-Smart-Tunnel	有	136	字符串	单值	智能隧道的名称
WebVPN-Smart-Tunnel-Auto-Sign-On	有	139	字符串	单值	域名附加的智能隧道自动登录列表名称
WebVPN-Smart-Tunnel-Auto-Start	有	138	整数	单值	0 = 禁用 1 = 启用 2 = 自动启动
WebVPN-Smart-Tunnel-Tunnel-Policy	有	227	字符串	单值	“e networkname”、“i networkname”或“a”中的某一项，其中 networkname 是指智能隧道网络列表的名称，e 表示不包含的通道，i 表示指定的隧道，a 则表示所有隧道。
WebVPN-SSL-VPN-Client-Enable	有	103	整数	单值	0 = 禁用 1 = 启用
WebVPN-SSL-VPN-Client-Keep-Installation	有	105	整数	单值	0 = 禁用 1 = 启用
WebVPN-SSL-VPN-Client-Required	有	104	整数	单值	0 = 禁用 1 = 启用
WebVPN-SSO-Server-Name	有	114	字符串	单值	有效字符串
WebVPN-Storage-Key	有	162	字符串	单值	
WebVPN-Storage-Objects	有	161	字符串	单值	
WebVPN-SVC-Keepalive-Frequency	有	107	整数	单值	15 - 600 秒，0 = 关闭
WebVPN-SVC-Client-DPD-Frequency	有	108	整数	单值	5 - 3600 秒，0 = 关闭
WebVPN-SVC-DTLS-Enable	有	123	整数	单值	0 = 禁用 1 = 启用
WebVPN-SVC-DTLS-MTU	有	125	整数	单值	MTU 值为 256 - 1406 字节。
WebVPN-SVC-Gateway-DPD-Frequency	有	109	整数	单值	5 - 3600 秒， 0 = 关闭
WebVPN-SVC-Rekey-Time	有	110	整数	单值	4 - 10080 分钟， 0 = 关闭
WebVPN-SVC-Rekey-Method	有	111	整数	单值	0（关闭）、1 (SSL)、2（新隧道）
WebVPN-SVC-Compression	有	112	整数	单值	0（关闭），1（解压压缩）
WebVPN-UNIX-Group-ID (GID)	有	222	整数	单值	有效 UNIX 组 ID
WebVPN-UNIX-User-ID (UIDs)	有	221	整数	单值	有效 UNIX 用户 ID
WebVPN-Upload-Max-Size	有	158	整数	单值	0x7fffffff
WebVPN-URL-Entry-Enable	有	93	整数	单值	0 = 禁用 1 = 启用
WebVPN-URL-List	有	71	字符串	单值	URL 列表名称
WebVPN-User-Storage	有	160	字符串	单值	
WebVPN-VDI	有	163	字符串	单值	设置列表

支持的 IETF RADIUS 授权属性

表 28-2 列出了支持的 IETF RADIUS 属性。

表 28-2　支持的 IETF RADIUS 授权属性

属性名	ASA	属性编号	语法/类型	单值或多值	说明或值
IETF-Radius-Class	有	25		单值	对于 8.2.x 版本及更高版本，建议使用表 28-1中所述的 Group-Policy 属性 (VSA 3076, #25)。 • *组策略名称* • OU = *组策略名称* • OU = *组策略名称*
IETF-Radius-Filter-Id	有	11	字符串	单值	在 ASA 中定义的 ACL 名称，仅适用于全隧道 IPsec 和 SSL VPN 客户端。
IETF-Radius-Framed-IP-Address	有	不适用	字符串	单值	IP 地址
IETF-Radius-Framed-IP-Netmask	有	不适用	字符串	单值	IP 地址掩码
IETF-Radius-Idle-Timeout	有	28	整数	单值	秒
IETF-Radius-Service-Type	有	6	整数	单值	秒。业务类型可能值： • .Administrative - 允许用户访问配置提示符。 • .NAS-Prompt - 允许用户访问执行提示符。 • .remote-access - 允许用户访问网络。
IETF-Radius-Session-Timeout	有	27	整数	单值	秒

RADIUS 记账断开原因代码

如果 ASA 在发送数据包时断开，将返回这些代码。

断开原因代码
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11

断开原因代码（续）
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

RADIUS 服务器许可要求

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

IPv6 准则

支持 IPv6。

其他指导原则

- 您可以在单情景模式中使用 100 个服务器组或在多情景模式的每个情景中使用 4 个服务器组。
- 单情景模式中每组可支持 16 台服务器，多情景模式中每组可支持 4 台服务器。
- 如果您想要使用本地数据库来配置回退支持，请参阅第 27-2 页的回退支持和第 27-2 页的组中存在多个服务器时的回退方式。
- 为防止使用 RADIUS 身份验证时从 ASA 中锁定，请参阅第 35-29 页的从锁定中恢复。

配置 RADIUS 服务器

- 第 28-14 页的配置 RADIUS 服务器任务流程
- 第 28-14 页的配置 RADIUS 服务器组
- 第 28-17 页的将 RADIUS 服务器添加到组

配置 RADIUS 服务器任务流程

步骤 1 将 ASA 属性加载到 RADIUS 服务器。加载属性采用的方法取决于您所使用的 RADIUS 服务器类型：

- 思科 ACS：该服务器已集成这些属性。您可以跳过此步骤。
- 来自其他供应商的 RADIUS 服务器（例如，Microsoft 互联网身份验证服务）：您必须手动定义每个ASA 属性。您可以使用属性名或编号、类型、值和供应商代码 (3076) 来定义属性。

步骤 2 添加 RADIUS 服务器组。请参阅第 28-14 页的配置 RADIUS 服务器组。

步骤 3 对于某个服务器组，将一台服务器添加至该服务器组。请参阅第 28-17 页的将 RADIUS 服务器添加到组。

配置 RADIUS 服务器组

如果您想要使用一台外部 RADIUS 服务器进行身份验证、授权或记账，则必须首先为每个 AAA 协议创建至少一个 RADIUS 服务器组并为每个组添加一台或多台服务器。您通过名称来标识 AAA 服务器组。

如要添加 RADIUS 服务器组，请执行以下操作：

详细步骤

	命令	用途
步骤 1	**aaa-server** *server_tag* **protocol radius** **示例：** `ciscoasa(config)# aaa-server servergroup1 protocol radius` `ciscoasa(config-aaa-server-group)#`	确定服务器组名称和协议。 输入 **aaa-server protocol** 命令时，即可进入 AAA 服务器组配置模式。

	命令	用途
步骤 2	**merge-dacl** {**before-avpair** | **after-avpair**} **示例：** ciscoasa(config)# aaa-server servergroup1 protocol radius ciscoasa(config-aaa-server-group)# merge-dacl before-avpair	将可下载的 ACL 和来自 RADIUS 包的思科 AV pair 中接收的 ACL 合并。默认设置为 **no merge dacl**，指定不将可下载 ACL 和思科 AV pair 的 ACL 合并。如果同时收到 AV pair ACL 和可下载 ACL， AV pair 优先被使用。 **before-avpair** 选项指定应该将可下载 ACL 条目放在思科 AV Pair 条目之前。 **before-avpair** 选项指定应该将可下载 ACL 条目放在思科 AV Pair 条目之后。此选项仅适用于 VPN 连接。对于 VPN 用户， ACL 形式包括思科 AV Pair ACL、可下载的 ACL 和在 ASA 上配置的 ACL。该选项确定是否合并可下载 ACL 和 AV Pair ACL，不适用于在 ASA 上配置的任何 ACL。
步骤 3	**max-failed-attempts** *number* **示例：** ciscoasa(config-aaa-server-group)# max-failed-attempts 2	指定在尝试下一台服务器之前，发送到组中某台 RADIUS 服务器的请求的最大数目。 *number* 参数的取值范围为 1 至 5。默认值为 3。 如果您配置了使用本地数据库的回退方法 （仅用于管理访问），并且组中的所有服务器都未能响应，则该服务器组会被视为无响应，系统将会尝试回退方法。服务器组在 10 分钟 （默认情况下）期间内仍然标记为无响应，那么，以便该期间的附加 AAA 请求不尝试与服务器组联系，且立即使用回退方法。如要更改默认的无响应期间，请参阅下一步中的 **reactivation-mode** 命令。 如果没有回退方法，则 ASA 将继续重试该组中的服务器。
步骤 4	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} **示例：** ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20	指定重新激活组内故障服务器的方法 （重新激活策略）。 关键字 **depletion** 只有在组内的所有服务器均处于非活动状态后才会重新激活故障服务器。 关键字-参数对 **deadtime** *minutes* 指定禁用组内最后一个服务器与随后重新启用所有服务器之间的时间，以分钟计量，在 0 至 1440 之间。默认时间为 10 分钟。 关键字 **timed** 在停机 30 秒后重新激活故障服务器。
步骤 5	**accounting-mode simultaneous** **示例：** ciscoasa(config-aaa-server-group)# accounting-mode simultaneous	将记账消息发送到组中的所有服务器。 如果只在活动服务器上恢复发送消息的默认设置，请输入 **accounting-mode single** 命令。
步骤 6	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **示例：** ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1	确定服务器及其所属的 AAA 服务器组。 输入 **aaa-server host** 命令时，即可进入 AAA 服务器主机配置模式。

	命令	用途
步骤 7	**dynamic-authorization** {port *port-number*} **示例：** (config-aaa-server-group)# dynamic-authorization port 1700	为 AAA 服务器组启用 RADIUS 动态授权 (CoA) 服务。 定义完成后，将注册相应的 RADIUS 服务器组以获取 CoA 通知，并且 ASA 会侦听端口以从 ISE 获取 CoA 策略更新。 CoA 侦听 *port-number* 的有效范围为 1 至 65535。 如果该命令以“no”形式指定的端口编号或接口与当前配置的任意行都不匹配，则会显示错误消息。
步骤 8	**authorize-only** **示例：** (config-aaa-server-group)# authorize-only	为 RADIUS 服务器组启用仅授权模式。表示该服务器组被用于进行授权时， RADIUS 访问请求消息将被创建为“Authorize Only”请求，与目前可用的已配置的密码方法相反。 Authorize-Only 请求在 Access-Request 中包含带 Authorize-Only 值 (17) 的 Service-Type 属性以及消息验证器。 仅授权模式无需在 Access-Request 中包含 RADIUS 通用密码。因此，无需在 AAA 服务器主机模式中使用 radius-common-pw CLI 来配置通用密码。 **注**　仅授权模式针对服务器组而配置，而通用密码特定于主机。因此，一旦配置了仅授权模式，针对单台 AAA 服务器配置的通用密码将被忽略。
步骤 9	**without-csd** {**anyconnect**} **示例：** (config-tunnel-webvpn)# without-csd anyconnect	为连到特定隧道组的连接关闭 hostscan 进程。目前，该设置适用于无客户端和 L3 连接。此命令已被修改，该设置仅应用于 AnyConnect 连接。
步骤 10	**interim-accounting-update** {periodic *interval*} **示例：** (config-aaa-server-group)# interim-accounting-update periodic 12	启用生成 RADIUS interim-accounting-update 消息。目前，只有在无客户端 VPN 会话中加入了 VPN 隧道连接时，才会生成这些消息。该情况下，将会生成记账更新，以将新分配的 IP 地址通知到 RADIUS 服务器。已将关键字添加到此命令，可以配置该关键字，以允许当前功能或允许为所有（被配置为向指定服务器组发送记账消息的）会话生成定期临时记账更新。 *periodic* - 此可选关键字允许为每个 （被配置为向相关服务器组发送记账记录的）VPN 会话定期生成和发送记账记录。 *interval* - 代表定期记账更新的间隔时间的数值，以小时为单位。有效值范围为 1 至 120，默认值为 24。

示例

以下示例显示如何添加一个带单台服务器的 RADIUS 组：

```
ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key RadUauthKey
ciscoasa(config-aaa-server-host)# exit
```

以下示例显示如何针对仅授权、动态授权 (CoA) 更新和每小时定期记账来配置 ISE 服务器对象：

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
```

```
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
```

以下示例显示如何通过 ISE 为密钥身份验证配置隧道组：

```
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

以下示例显示如何通过 ISE 为本地证书验证和授权配置隧道组：

```
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

将 RADIUS 服务器添加到组

如要将 RADIUS 服务器添加到组，请执行以下操作：

详细步骤

	命令	用途
步骤 1	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **示例：** `ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1`	确定 RADIUS 服务器及其所属的 AAA 服务器组。 输入 **aaa-server host** 命令时，即可进入 AAA 服务器主机配置模式。
步骤 2	**acl-netmask-convert** {**auto-detect** | **standard** | **wildcard**} **示例：** `ciscoasa(config-aaa-server-host)#` **acl-netmask-convert standard**	指定 ASA 如何处理来自使用 **aaa-server host** 命令访问的 RADIUS 服务器的可下载 ACL 包含的网络掩码。 关键字 **auto-detect** 指定 ASA 应该尝试确定所使用的网络掩码表达式的类型。如果 ASA 检测到通配符网络掩码表达式，则将其转换为标准的网络掩码表达式。 关键字 **standard** 指定 ASA 假定来自 RADIUS 服务器的可下载 ACL 只包含标准的网络掩码表达式。因而不会对通配符网络掩码表达式进行转换。 关键字 **wildcard** 指定 ASA 假定来自 RADIUS 服务器的可下载 ACL 只包含通配符网络掩码表达式，并且在下载 ACL 后会将它们全部转换为标准的网络掩码表达式。

	命令	用途
步骤 3	**radius-common-pw** *string* **示例：** ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc	为所有通过 ASA 访问 RADIUS 授权服务器的用户指定一个通用密码。 参数 *string* 为一个区分大小写的字母数字关键字 （最多 127 个字符），将作为与 RADIUS 服务器进行的所有授权事务的通用密码。
步骤 4	**mschapv2-capable** **示例：** ciscoasa(config-aaa-server-host)# mschapv2-capable	对 RADIUS 服务器启用 MS-CHAPv2 身份验证请求。
步骤 5	**timeout** *hh:mm:ss* **示例：** ciscoasa(config-aaa-server-host)# timeout 15	指定在将请求发送到备用服务器之前， ASA 等待来自主用服务器的响应的时间，以秒为单位。
步骤 6	**retry-interval** *seconds* **示例：** ciscoasa(config-aaa-server-host)# retry-interval 8	为上一个 **aaa-server host** 命令指定的特定 AAA 服务器配置重试尝试间隔时间。 参数 *seconds* 指定请求的重试间隔时间（1 - 10 秒）。这是 ASA 在重试连接请求之前等待的时间。 **注**　无论您输入了何种重试间隔设置，随后的重试间隔时间始终为 50 或 100 毫秒。这属于预期行为。
步骤 7	**accounting-mode simultaneous** **示例：** ciscoasa(config-aaa-server-group)# accounting-mode simultaneous	将记账消息发送到组中的所有服务器。 如果只在活动服务器上恢复发送消息的默认设置，请输入 **accounting-mode single** 命令。
步骤 8	**authentication-port** *port* **示例：** ciscoasa(config-aaa-server-host)# authentication-port 1645	将身份验证端口指定为端口 1645 或者指定用于用户身份验证的服务器端口。
步骤 9	**accounting-port** *port* **示例：** ciscoasa(config-aaa-server-host)# accounting-port 1646	将记账端口指定为端口 1646 或者指定用于主机记账的服务器端口。
步骤 10	**密钥** **示例：** ciscoasa(config-aaa-host)# key myexamplekey1	指定用于向 ASA 对 RADIUS 服务器进行身份验证的服务器密钥值。您配置的服务器密钥应该与在 RADIUS 服务器中配置的密钥相匹配。如果您不知道服务器密钥值，请询问 RADIUS 服务器管理员。最大长度为 64 个字符。

示例

以下示例显示如何将 RADIUS 服务器添加到现有的 RADIUS 服务器组：

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
```

```
ciscoasa(config-aaa-server-host)# radius-common-pw myexaplepasswordabc123
ciscoasa(config-aaa-server-host)# mschapv2-capable
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# accounting-mode simultaneous
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# authorization-port 1645
ciscoasa(config-aaa-server-host)# key mysecretkeyexampleiceage2
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

监控 RADIUS 服务器

如要监控 RADIUS 服务器，请输入以下任一命令：

命令	用途
show aaa-server	显示已配置 RADIUS 服务器统计信息。 如要清除 RADIUS 服务器配置，请输入 **clear aaa-server statistics** 命令。
show running-config aaa-server	显示 RADIUS 服务器运行配置。 如要清除 RADIUS 服务器统计信息，请输入 **clear configure aaa - server** 命令。

附加参考资料

有关通过 RADIUS 服务器实施 AAA 的附加信息，请参阅 第 28-19 页的 RFC。

RFC

RFC	标题
2138	*远程身份验证拨入用户服务 (RADIUS)*
2139	*RADIUS 记帐*
2548	*Microsoft 供应商特定 RADIUS 属性*
2868	*用于隧道协议支持的 RADIUS 属性*

RADIUS 服务器功能历史

表 28-3 列出了各种功能变更以及实施该等功能变更的平台版本。

表 28-3 RADIUS 服务器功能历史

功能名称	平台版本	功能信息
AAA RADIUS 服务器	7.0(1)	描述如何配置 AAA RADIUS 服务器。 我们引入了以下命令： **aaa-server protocol**、 **max-failed-attempts**、**reactivation-mode**、 **accounting-mode simultaneous**、**aaa-server host**、 **show aaa-server**、 **show running-config aaa-server**、 **clear aaa-server statistics**、**authentication-port**、**accounting-port**、**retry-interval**、**acl-netmask-convert**、 **clear configure aaa-server**、**merge-dacl**、 **radius-common-pw, key**。
从 ASA 在 RADIUS 访问请求和记账请求数据包中发送的关键供应商特定属性 (VSA)。	8.4(3)	从 ASA 在 RADIUS 访问请求数据包中发送四个新 VSA - Tunnel Group Name (146) 和 Client Type (150)。从 ASA 在 RADIUS 记账请求数据包中发送 Session Type (151) 和 Session Subtype (152)。为所有类型的记账请求数据包发送所有这四个属性：Start、Interim-Update 和 Stop。RADIUS 服务器（例如，ACS 和 ISE）可以实施授权和策略属性或者利用它们进行记账和收费。

用于 AAA 的 TACACS+ 服务器

本章介绍如何配置在 AAA 中使用的 TACACS+ 服务器。

- 第 29-1 页的有关 TACACS+ 服务器的信息
- 第 29-2 页的 TACACS+ 服务器的许可要求
- 第 29-2 页的准则和限制
- 第 29-3 页的配置 TACACS+ 服务器
- 第 29-5 页的监控 TACACS+ 服务器
- 第 29-6 页的 TACACS+ 服务器的功能历史记录

有关 TACACS+ 服务器的信息

ASA 支持使用以下协议执行 TACACS+ 服务器身份验证：ASCII、PAP、CHAP 和 MS-CHAPv1。

使用 TACACS+ 属性

思科 ASA 可支持 TACACS+ 属性。TACACS+ 属性可用于分隔身份验证、授权和记帐功能。该协议支持两种类型的属性：必需和可选。服务器和客户端都必须能够理解必需属性，而且必须将必需属性应用至用户。可选属性是否能被理解，或是否会被使用不作要求。

注 如要使用 TACACS+ 属性，请确保您已在 NAS 上启用 AAA 服务。

表 29-1 列出了适用于直通代理连接的受支持的 TACACS+ 授权响应属性。表 29-2 列出了受支持的 TACACS+ 记帐属性。

表 29-1 受支持的 TACACS+ 授权响应属性

属性	说明
acl	确定要应用至连接的本地配置的 ACL。
idletime	指定经过身份验证的用户会话会被终止前，可以有的非活动时长，以分钟为单位。
timeout	指定经过身份验证的用户会话会被终止前，身份验证凭据可以保持活动状态的时长，以分钟为单位。

表 29-2　受支持的 TACACS+ 记帐时间

属性	说明
bytes_in	指定连接过程中，传输的输入字节的数量（仅停止记录）
bytes_out	指定连接过程中，传输的输出字节的数量（仅停止记录）
cmd	定义会被执行的命令（仅命令记帐）。
disc-cause	指定标识断开原因的数值代码（仅停止记录）。
elapsed_time	定义连接的运行时间（仅停止记录）。
foreign_ip	指定隧道连接的客户端的 IP 地址。定义用于直通代理连接的最低安全性接口上的地址。
local_ip	指定对于隧道连接，客户端已连接到的 IP 地址。定义用于直通代理连接的最高安全性接口上的地址。
NAS port	包含连接的会话 ID。
packs_in	指定在连接期间传输的输入数据包的数量。
packs_out	指定在连接期间传输的输出数据包的数量。
priv-level	设置为命令记帐请求的用户权限级别，否则设置为 1。
rem_iddr	指定客户端的 IP 地址。
service	指定所使用的服务。对于仅进行命令记帐的情况，始终设置为“shell”。
task_id	指定记帐事务的唯一任务 ID。
username	指定用户的名称。

TACACS+ 服务器的许可要求

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

IPv6 准则

支持 IPv6。

其他指导原则

- 您可以在单情景模式中使用 100 个服务器组或在多情景模式的每个情景中使用 4 个服务器组。
- 单情景模式中每组可支持 16 台服务器，多情景模式中每组可支持 4 台服务器。
- 如果您想要使用本地数据库来配置回退支持，请参阅第 27-2 页的回退支持和第 27-2 页的组中存在多个服务器时的回退方式。
- 要在使用 TACACS+ 身份验证或授权时，防止来自 ASA 的锁定，请参阅第 35-29 页的从锁定中恢复。

配置 TACACS+ 服务器

- 第 29-3 页的配置 TACACS+ 服务器任务流程
- 第 29-3 页的配置 TACACS+ 服务器组
- 第 29-5 页的将 TACACS+ 服务器添加至服务器组

配置 TACACS+ 服务器任务流程

步骤 1　添加 TACACS+ 服务器组。请参阅第 29-3 页的配置 TACACS+ 服务器组。

步骤 2　对于某个服务器组，将一台服务器添加至该服务器组。请参阅第 29-5 页的将 TACACS+ 服务器添加至服务器组。

配置 TACACS+ 服务器组

如果您想要将 TACACS+ 服务器用于身份验证、授权或记帐，必须先创建至少一个 TACACS+ 服务器组，然后向每个服务器组添加一台或多台服务器。您可以通过名称标识 TACACS+ 服务器组。

如要添加 TACACS+ 服务器组，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**aaa-server** *server_tag* **protocol tacacs+** **示例：** `ciscoasa(config)# aaa-server servergroup1 protocol tacacs+` `ciscoasa(config-aaa-server-group)#`	确定服务器组名称和协议。 输入 **aaa-server protocol** 命令时，即可进入 AAA 服务器组配置模式。

	命令	用途
步骤 2	**max-failed-attempts** *number* **示例：** `ciscoasa(config-aaa-server-group)# max-failed-attempts 2`	指定在尝试下一服务器前，会向组中 AAA 服务器发送的请求的最大数量。*number* 参数的取值范围为 1 至 5。默认值为 3。 如果您配置了使用本地数据库的回退方法（仅用于管理访问），并且组中的所有服务器都未能响应，则该服务器组会被视为无响应，系统将会尝试回退方法。服务器组在 10 分钟（默认情况下）期间内仍然标记为无响应，那么，以便该期间的附加 AAA 请求不尝试与服务器组联系，且立即使用回退方法。要更改默认的无响应期间，请参阅下一步中的 **reactivation-mode** 命令。 如果没有回退方法，则 ASA 将继续重试该组中的服务器。
步骤 3	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} **示例：** `ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20`	指定重新激活组内故障服务器的方法（重新激活策略）。 关键字 **depletion** 只有在组内的所有服务器均处于非活动状态后才会重新激活故障服务器。 关键字-参数对 **deadtime** *minutes* 指定禁用组内最后一个服务器与随后重新启用所有服务器之间的时间，以分钟计量，在 0 至 1440 之间。默认时间为 10 分钟。 关键字 **timed** 在停机 30 秒后重新激活故障服务器。
步骤 4	**accounting-mode simultaneous** **示例：** `ciscoasa(config-aaa-server-group)# accounting-mode simultaneous`	将记账消息发送到组中的所有服务器。 如果只在活动服务器上恢复发送消息的默认设置，请输入 **accounting-mode single** 命令。

示例

以下示例显示，如何添加拥有一台主用服务器和一台备用服务器的一个 TACACS+ 组。

```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.2
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey2
ciscoasa(config-aaa-server-host)# exit
```

将 TACACS+ 服务器添加至服务器组

如要将 TACACS+ 服务器添加至服务器组，请执行以下操作：

详细步骤

	命令	用途
步骤 1	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **示例：** `ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1`	确定 TACACS+ 服务器，以及该服务器所属的服务器组。 输入 **aaa-server host** 命令时，即可进入 AAA 服务器主机配置模式。
步骤 2	**timeout** *hh:mm:ss* **示例：** `ciscoasa(config-aaa-server-host)# timeout 15`	指定在将请求发送到备用服务器之前，ASA 等待来自主用服务器的响应的时间，以秒为单位。
步骤 3	**server-port** *port_number* **示例：** `ciscoasa(config-aaa-server-host)# server-port 49`	将服务器端口指定为端口号 49，或者指定为 ASA 用于与 TACACS+ 服务器通信的 TCP 端口号。
步骤 4	**密钥** **示例：** `ciscoasa(config-aaa-host)# key myexamplekey1`	指定服务器密钥值，该密钥值会用于面向 TACACS+ 服务器对 NAS 进行身份验证。该密钥值是一个区分大小写的字母数字关键字，最大长度为 127 个字符，它的值与 TACACS+ 服务器上的密钥相同。超出 127 个字符后的所有字符都会被忽略。该密钥会在客户端和服务器之间使用，用于加密它们之间传送的数据，该密钥在客户端和服务器系统上必须相同。该密钥不能包含空格，但允许包含其他的特殊字符。

监控 TACACS+ 服务器

要监控 TACACS+ 服务器，请输入以下任一命令：

命令	用途
show aaa-server	显示配置的 TACACS+ 服务器的统计信息。 如要清除 TACACS+ 服务器配置，请输入 **clear aaa-server statistics** 命令。
show running-config aaa-server	显示 TACACS+ 服务器的运行配置。 如要清除 TACACS+ 服务器的统计信息，请输入 **clear configure aaa-server** 命令。

TACACS+ 服务器的功能历史记录

表 29-3 列出了各种功能变更以及实施该等功能变更的平台版本。

表 29-3　TACACS+ 服务器的功能历史记录

功能名称	平台版本	功能信息
TACACS+ 服务器	7.0(1)	介绍如何配置用于 AAA 的 TACACS+ 服务器。 我们引入了以下命令： **aaa-server protocol**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**aaa authorization exec authentication-server**、**server-port**、**key**、**clear aaa-server statistics**、**clear configure aaa-server**、**show aaa-server**、**show running-config aaa-server**、**username**、**service-type**、**timeout**。

AAA 中的 LDAP 服务器

本章介绍如何配置 AAA 的 LDAP 服务器。

- 第 30-1 页的有关 LDAP 和 ASA 的信息
- 第 30-4 页的 LDAP 服务器许可要求
- 第 30-4 页的准则和限制
- 第 30-4 页的配置 LDAP 服务器
- 第 30-10 页的监控 LDAP 服务器
- 第 30-10 页的 LDAP 服务器的功能历史记录

有关 LDAP 和 ASA 的信息

思科 ASA 兼容于大多数 LDAPv3 目录服务器，包括：

- Sun Microsystems JAVA System Directory Server，目前是 Oracle Directory Server Enterprise Edition 的一部分，以前称为 Sun ONE Directory Server
- Microsoft Active Directory
- Novell
- OpenLDAP

默认情况下，ASA 会自动检测其是否连接到 Microsoft Active Directory、Sun LDAP、Novell、OpenLDAP 或通用 LDAPv3 目录服务器。但是，如果自动检测无法确定 LDAP 服务器类型，则可以手动配置它。

LDAP 服务器准则

配置 LDAP 服务器时，请注意以下准则：

- 为访问 Sun 目录服务器而在 ASA 上配置的 DN 必须能够访问该服务器上的默认密码策略。我们建议将目录管理员或具有目录管理员权限的用户用作 DN。或者，可将 ACL 放在默认密码策略上。
- 您必须通过 SSL 配置 LDAP，以便对 Microsoft Active Directory 和 Sun 服务器启用密码管理。
- ASA 不支持对 Novell、OpenLDAP 和其他 LDAPv3 目录服务器启用密码管理。
- VPN 3000 集中器和 ASA/PIX 7.0 软件需要思科 LDAP 模式进行授权操作。从 V 7.1.x 开始，ASA 使用本地 LDAP 模式执行身份验证和授权，而不再需要思科模式。

如何用 LDAP 进行身份验证

执行身份验证期间，ASA 将充当用户的 LDAP 服务器的客户端代理，并以纯文本或使用 SASL 协议对 LDAP 服务器执行身份验证。默认情况下，ASA 以纯文本将身份验证参数，通常为用户名和密码传递至 LDAP 服务器。

ASA 支持以下 SASL 机制，按强度递增的顺序列示：

- Digest-MD5 - ASA 以一个由用户名和密码计算的 MD5 值响应 LDAP 服务器。
- Kerberos - ASA 通过使用 GSSAPI Kerberos 机制发送用户名和领域响应 LDAP 服务器。

ASA 和 LDAP 服务器支持这些 SASL 机制的任意组合。如果配置多个机制，则 ASA 将检索服务器上配置的 SASL 机制的列表，并将身份验证机制设置为 ASA 和服务器上配置的最强机制。例如，如果 LDAP 服务器和 ASA 支持这两种机制，则 ASA 将选择两者中的较强者 Kerberos。

对用户成功执行 LDAP 身份验证后，LDAP 服务器将返回已通过身份验证的用户的属性。对于 VPN 身份验证，这些属性通常包括已应用于 VPN 会话的授权数据。在此情况下，使用 LDAP 即可一步完成身份验证和授权。

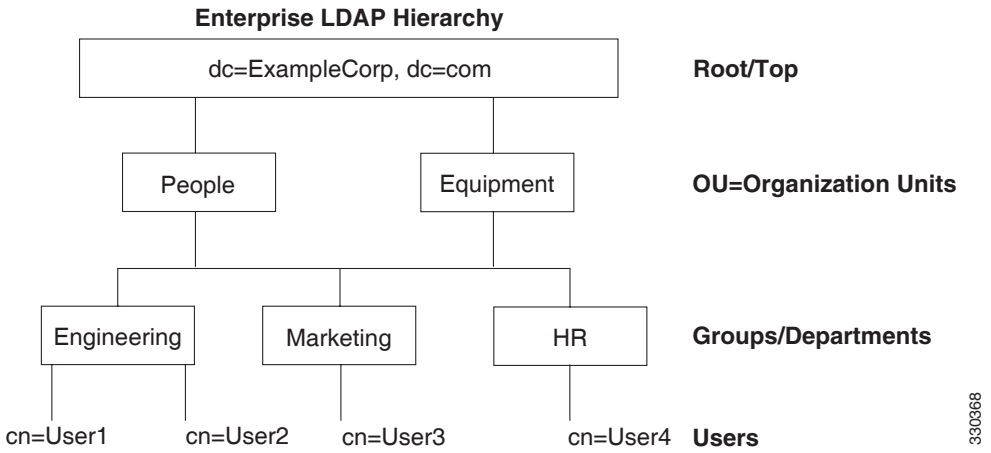
注　有关 LDAP 协议的详细信息，请参阅 RFC 1777、 2251 和 2849。

关于 LDAP 层次结构

您的 LDAP 配置应反映贵组织的逻辑层次结构。例如，假设贵公司 Example Corporation 的一名员工叫 Employee1。 Employee1 在工程组工作。您的 LDAP 层次结构可能有一个或多个级别。您可能决定设置一个单级别层次结构，在其中 Employee1 被视为 Example Corporation 的一名成员。您也可以设置一个多级别层次结构，在其中 Employee1 被视为工程部门的一名成员，该部门是一个称为 People 的组织单位的成员，而该组织单位则是 Example Corporation 的成员。请参阅图 30-1，了解多级别层次结构的示例。

多级别层次结构的信息比较详细，但是，在单级别层次结构中搜索结果的速度更快。

图 30-1　　多级别 LDAP 层次结构



搜索 LDAP 层次结构

ASA 可供您在 LDAP 层次结构中定制搜索。您在 ASA 上配置以下三个字段，定义在 LDAP 层次结构中开始搜索的位置、搜索范围和所搜索信息的类型。这些字段共同将层次结构的搜索仅限于包含用户权限的部分。

- LDAP Base DN 将定义服务器自 ASA 收到授权请求后开始在 LDAP 层次结构中搜索用户信息的位置。
- Search Scope 将定义在 LDAP 层次结构中的搜索范围。搜索继续在层次结构中 LDAP Base DN 下方的多个级别中进行。您可以选择让服务器仅搜索紧接其下方的那个级别，否则，它可能搜索整个子树。单级别搜索比较快，但子树搜索更加广泛。
- Naming Attribute 定义唯一识别 LDAP 服务器中条目的 RDN。常用的命名属性可能包括 cn (Common Name)、 sAMAccountName 和 userPrincipalName。

图 30-1 显示了 Example Corporation 的一个 LDAP 层次结构示例。鉴于该层次结构，您可以不同的方式定义您的搜索。表 30-1 显示了两个搜索配置示例。

在第一个配置示例中，如果 Employee1 用所需 LDAP 授权建立 IPsec 隧道，则 ASA 将向 LDAP 服务器发送一个搜索请求，指明其应在工程组中搜索 Employee1。这种搜索速度很快。

在第二个配置示例中，ASA 发送一个搜索请求，指明服务器应在 Example Corporation 中搜索 Employee1。这种搜索需时较长。

表 30-1　搜索配置示例

编号	LDAP Base DN	搜索范围	命名属性	结果
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	一级	cn=Employee1	搜索速度较快
2	dc=ExampleCorporation,dc=com	子树	cn=Employee1	搜索时间较长

关于绑定到 LDAP 服务器

ASA 使用登录 DN 和登录密码与 LDAP 服务器建立信任（绑定）。执行 Microsoft Active Directory 只读操作（例如身份验证、授权或组搜索）时，ASA 可绑定登录 DN 与较少权限。例如，登录 DN 可能是 AD “Member Of”名称为 Domain Users 一部分的用户。对于 VPN 密码管理操作，登录 DN 需要较高的权限，而且必须为 Account Operators AD 组的一部分。

以下是登录 DN 的一个示例：

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA 支持以下身份验证方法：

- 使用未加密密码对端口 389 执行的简单 LDAP 身份验证
- 对端口 636 执行的安全 LDAP (LDAP-S)
- 简单身份验证和安全层 (SASL) MD5
- SASL Kerberos

ASA 不支持匿名身份验证。

注　作为一个 LDAP 客户端， ASA 不支持匿名绑定或请求的传输。

LDAP 服务器许可要求

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

IPv6 准则

支持 IPv6。

配置 LDAP 服务器

- 第 30-4 页的用于配置 LDAP 服务器的任务流
- 第 30-4 页的配置 LDAP 属性映射
- 第 30-7 页的配置 LDAP 服务器组第 30-9 页的用 LDAP 为 VPN 配置身份验证

用于配置 LDAP 服务器的任务流

步骤 1　添加 LDAP 服务器组。请参阅第 30-7 页的配置 LDAP 服务器组。

步骤 2　（可选）从与身份验证机制分离而且不同的 LDAP 服务器配置授权。请参阅第 30-9 页的用 LDAP 为 VPN 配置身份验证。

步骤 3　配置 LDAP 属性映射。请参阅第 30-4 页的配置 LDAP 属性映射。
将 LDAP 服务器添加至 LDAP 服务器组之前，必须添加属性映射。

配置 LDAP 属性映射

ASA 可为以下项使用 LDAP 目录对用户进行身份验证：

- VPN 远程访问用户
- 防火墙网络访问/直通代理会话

- 设置策略权限（也称为授权属性），如 ACL、书签列表、DNS 或 WINS 设置，以及会话计时器。
- 在本地组策略中设置关键属性

ASA 使用 LDAP 属性映射将本地 LDAP 用户属性转换为思科 ASA 属性。您可以将这些属性映射与 LDAP 服务器进行绑定或删除它们。您还可以显示或清除属性映射。

准则

LDAP 属性映射不支持多值属性。例如，如果用户是多个 AD 组的成员，而且 LDAP 属性映射与多个组匹配，则根据匹配条目的字母顺序选择值。

如要正确使用属性映射功能，您需了解 LDAP 属性名称和值，以及用户定义的属性名称和值。

频繁映射的 LDAP 属性的名称以及经常将其映射到的用户定义属性的类型包括：

- IETF-Radius-Class（ASA V 8.2 或更高版本中的 Group_Policy）- 根据目录部门或用户组（例如，Microsoft Active Directory memberOf）属性值设置组策略。组策略属性用 ASDM V 6.2/ASA V 8.2 或更高版本替换 IETF-Radius-Class 属性。
- IETF-Radius-Filter-Id - 将访问控制列表或 ACL 应用于 VPN 客户端、 IPsec 和 SSL。
- IETF-Radius-Framed-IP-Address - 将已分配的静态 IP 地址分配到 VPN 远程访问客户端、IPsec 和 SSL。
- Banner1 - 在 VPN 远程访问用户登录时显示文本标题。
- Tunneling-Protocols - 根据访问类型，允许或拒绝 VPN 远程访问会话。

注　单一 LDAP 属性映射可以包含一个或多个属性。只能从一个特定 LDAP 服务器映射一个 LDAP 属性。

如要映射 LDAP 功能，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**ldap attribute-map** *map-name* **示例：** `ciscoasa(config)# ldap attribute-map att_map_1`	创建未填充 LDAP 属性映射表。
步骤 2	**map-name** *user-attribute-name Cisco-attribute-name* **示例：** `ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class`	将用户定义的属性名称部门映射到思科属性。
步骤 3	**map-value** *user-attribute-name Cisco-attribute-name* **示例：** `ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1`	将用户定义的映射值部门映射到用户定义的属性值和思科属性值。

	命令	用途
步骤 4	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **示例：** `ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4`	确定服务器及其所属的 AAA 服务器组。
步骤 5	**ldap-attribute-map** *map-name* **示例：** `ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1`	将属性映射绑定到 LDAP 服务器。

示例

以下示例展示如何根据称为 accessType 的 LDAP 属性将管理会话限定于 ASA。accessType 属性可能有下列值之一：

- VPN
- admin
- helpdesk

以下示例展示如果将每个值映射到 ASA 支持的有效 IETF-Radius-Service-Type 属性之一：remote-access (Service-Type 5) Outbound、 admin (Service-Type 6) Administrative 和 nas-prompt (Service-Type 7) NAS Prompt。

```
ciscoasa(config)# ldap attribute-map MGMT
ciscoasa(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
ciscoasa(config-ldap-attribute-map)# map-value accessType VPN 5
ciscoasa(config-ldap-attribute-map)# map-value accessType admin 6
ciscoasa(config-ldap-attribute-map)# map-value accessType helpdesk 7

ciscoasa(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
ciscoasa(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password test
ciscoasa(config-aaa-server-host)# ldap-login-dn
CN=Administrator,CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# server-type auto-detect
ciscoasa(config-aaa-server-host)# ldap-attribute-map MGMT
```

以下示例展示如何显示思科 LDAP 属性名称的完整列表：

```
ciscoasa(config)# ldap attribute-map att_map_1
ciscoasa(config-ldap-attribute-map)# map-name att_map_1?

ldap mode commands/options:
cisco-attribute-names:
Access-Hours
  Allow-Network-Extension-Mode
  Auth-Service-Type
  Authenticated-User-Idle-Timeout
  Authorization-Required
  Authorization-Type
   :
   :
  X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

配置 LDAP 服务器组

如要使用外部 LDAP 服务器执行身份验证、授权和/或记帐，首先必须至少创建一个 LDAP 服务器组，且向每个组添加一个或多个服务器。按名称标识 LDAP 服务器组。每个服务器组对应于一个服务器类型。

准则

- 在单模式中，最多可以有 100 个 LDAP 服务器组；在多模式中，每个情景可以有 4 个 LDAP 服务器组。
- 在单模式中，每组最多可以有 16 个 LDAP 服务器；在多模式中，每组可以有 4 个 LDAP 服务器。
- 用户登录时，从您在配置中指定的第一个服务器开始，一次访问一个 LDAP 服务器，直到服务器响应为止。如果该组中的所有服务器均不可用，如将 ASA 配置为回退方法（仅管理身份验证和授权），则其将尝试本地数据库。如果没有回退方法，则 ASA 将继续尝试 LDAP 服务器。

详细步骤

以下步骤说明如何创建和配置 LDAP 服务器组，并将 LDAP 服务器添加到该组。

	命令	用途
步骤 1	**aaa-server** *server_tag* **protocol ldap** **示例：** `ciscoasa(config)# aaa-server servergroup1 protocol ldap` `ciscoasa(config-aaa-server-group)#`	确定服务器组名称和协议。输入 **aaa-server protocol** 命令时，即可进入 AAA 服务器组配置模式。
步骤 2	**max-failed-attempts** *number* **示例：** `ciscoasa(config-aaa-server-group)# max-failed-attempts 2`	指定在尝试下一个 LDAP 服务器之前发送到组中某个 LDAP 服务器的最大请求数。*number* 参数的取值范围为 1 至 5。默认值为 3。 如已使用本地数据库（仅用于管理访问）配置了回退方法，以配置回退机制，且组中所有服务器均未能响应，则该组被视为无响应，并尝试回退方法。服务器组在 10 分钟（默认情况下）期间内仍然标记为无响应，那么，以便该期间的附加 AAA 请求不尝试与服务器组联系，且立即使用回退方法。如要更改默认的无响应期间，请参阅下一步中的 **reactivation-mode** 命令。 如果没有回退方法，则 ASA 将继续重试该组中的服务器。

	命令	用途
步骤 3	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} **示例：** `ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20`	指定重新激活组内故障服务器的方法 （重新激活策略）。 关键字 **depletion** 只有在组内的所有服务器均处于非活动状态后才会重新激活故障服务器。 关键字-参数对 **deadtime** *minutes* 指定禁用组内最后一个服务器与随后重新启用所有服务器之间的时间，以分钟计量，在 0 至 1440 之间。默认时间为 10 分钟。 关键字 **timed** 在停机 30 秒后重新激活故障服务器。
步骤 4	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **示例：** `ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1` 移至将服务器添加到组这一新操作步骤	识别 LDAP 服务器以及其所属的 AAA 服务器组。 输入 **aaa-server host** 命令时，即可进入 AAA 服务器主机配置模式。根据需要，使用主机配置模式命令进一步配置 AAA 服务器。 表 30-2 列出了可用于 LDAP 服务器的命令，以及新的 LDAP 服务器定义是否有该命令的默认值。如果未提供默认值 （以“-”表示），请使用命令指定该值。

表 30-2　　主机模式命令和默认值

命令	默认值	说明
ldap-attribute-map	-	分开 **aa server host** 命令下操作步骤中的步骤
ldap-base-dn	-	-
ldap-login-dn	-	-
ldap-login-password	-	-
ldap-naming-attribute	-	-
ldap-over-ssl	636	如果未设置，则 ASA 将 sAMAccountName 用于 LDAP 请求。无论是使用 SASL 还是纯文本，都可以用 SSL 保护 ASA 与 LDAP 服务器之间的通信。如果未配置 SASL，我们强烈建议您用 SSL 保护 LDAP 通信。
ldap-scope	-	-
sasl-mechanism	-	-
server-port	389	-
server-type	autodiscovery	如果自动检测未能确定 LDAP 服务器类型，并且您知道服务器为 Microsoft、 Sun 或通用 LDAP 服务器，则可以手动配置服务器类型。
timeout	10 秒	-

示例

以下示例说明如何配置名为 watchdogs 的 LDAP 服务器组并将 LDAP 服务器添加到该组。由于示例未定义重试间隔或 LDAP 服务器侦听的端口，ASA 使用这两个服务器特定参数的默认值。

```
ciscoasa(config)# aaa-server watchdogs protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

用 LDAP 为 VPN 配置身份验证

如果为 VPN 访问对用户执行的 LDAP 身份验证已成功，ASA 将查询 LDAP 服务器，且服务器会返回 LDAP 属性。这些属性通常包括适用于 VPN 会话的授权数据。以这种方式使用 LDAP 一步可完成身份验证和授权。

然而，可能需要获得与身份验证机制分开而且不同的 LDAP 目录服务器的授权。例如，如果使用 SDI 或证书服务器执行身份验证，则不返回授权信息。对于此情况下的用户授权，可以在身份验证成功后查询 LDAP 目录，分两步完成身份验证和授权。

如要用 LDAP 设置 VPN 用户授权，请执行以下步骤。

详细步骤

	命令	用途
步骤 1	**tunnel-group** *groupname* **示例：** `ciscoasa(config)# tunnel-group remotegrp`	创建名为 remotegrp 的 IPsec 远程访问隧道组。
步骤 2	**tunnel-group** *groupname* **general-attributes** **示例：** `ciscoasa(config)# tunnel-group remotegrp general-attributes`	将服务器组与隧道组相关联。
步骤 3	**authorization-server-group** *group-tag* **示例：** `ciscoasa(config-general)# authorization-server-group ldap_dir_1`	将新隧道组分配给以前创建的 AAA 服务器组进行授权。

示例

虽然有其他授权相关命令和选项可用于特定要求，但以下示例显示可用于通过 LDAP 启用用户授权的命令。然后，该示例然后创建名为 remote-1 的 IPsec 远程访问隧道组，并将该新隧道组分配给以前创建的 ldap_dir_1 AAA 服务器组进行授权：

```
ciscoasa(config)# tunnel-group remote-1 type ipsec-ra
ciscoasa(config)# tunnel-group remote-1 general-attributes
ciscoasa(config-general)# authorization-server-group ldap_dir_1
ciscoasa(config-general)#
```

完成此配置工作后，可以通过输入以下命令配置额外的 LDAP 授权参数，例如目录密码、目录搜索起点和目录搜索范围：

```
ciscoasa(config)# aaa-server ldap_dir_1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
ciscoasa(config-aaa-server-host)# ldap-login-dn obscurepassword
ciscoasa(config-aaa-server-host)# ldap-base-dn starthere
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)#
```

监控 LDAP 服务器

如要监控 LDAP 服务器，并输入以下命令之一：

命令	用途
show aaa-server	显示已配置的 AAA 服务器的统计信息。 要清除 AAA 服务器配置，请输入 **clear aaa-server statistics** 命令。
show running-config aaa-server	显示 AAA 服务器运行配置。 要清除 AAA 服务器统计信息，请输入 **clear configure aaa-server** 命令。

LDAP 服务器的功能历史记录

表 30-3 列出了各种功能变更以及实施该等功能变更的平台版本。

表 30-3　　AAA 服务器的功能历史记录

功能名称	平台版本	功能信息
AAA 中的 LDAP 服务器	7.0(1)	LDAP Servers 将介绍对 AAA 的支持以及如何配置 LDAP 服务器。 我们引入了以下命令： **username**、 **aaa authorization exec authentication-server**、 **aaa authentication console LOCAL**、 **aaa authorization exec LOCAL**、 **service-type**、 **ldap attribute-map**、 **aaa-server protocol**、 **aaa authentication {telnet | ssh | serial} console LOCAL**、**aaa authentication http console LOCAL**、 **aaa authentication enable console LOCAL**、 **max-failed-attempts**、 **reactivation-mode**、 **accounting-mode simultaneous**、 **aaa-server host**、 **authorization-server-group**、 **tunnel-group**、**tunnel-group general-attributes**、**map-name**、**map-value** 和 **ldap-attribute-map**。

身份防火墙

本章介绍如何为身份防火墙配置 ASA。

- 第 31-1 页的关于身份防火墙的信息
- 第 31-6 页的身份防火墙许可
- 第 31-6 页的准则和限制
- 第 31-8 页的先决条件
- 第 31-8 页的配置身份防火墙
- 第 31-19 页的监控身份防火墙
- 第 31-21 页的身份防火墙的功能历史记录

关于身份防火墙的信息

- 第 31-1 页的身份防火墙概述
- 第 31-2 页的身份防火墙部署的架构
- 第 31-3 页的身份防火墙功能
- 第 31-4 页的部署方案

身份防火墙概述

在企业中，用户通常需要访问一个或多个服务器资源。通常，防火墙不知道用户的身份，因此也就无法基于身份应用安全策略。如要配置每个用户的访问策略，则您必须配置用户身份验证代理，其要求用户交互 （用户名/密码查询）。

ASA 内的身份防火墙基于用户身份提供更细粒度的访问控制。您可以基于用户名和用户组名，而不是通过源 IP 地址配置访问规则和安全策略。ASA 基于 IP 地址与 Windows Active Directory 登录信息的关联应用安全策略，并基于映射的用户名，而不是基于网络 IP 地址报告事件。

身份防火墙与提供实际身份映射的外部 Active Directory (AD) 代理配合，与 Microsoft Active Directory 相集成。ASA 将 Windows Active Directory 用作检索特定 IP 地址的当前用户身份信息的源，并允许 Active Directory 用户的透明身份验证。

通过允许指定用户或组来代替源 IP 地址，基于身份的防火墙服务增强现有访问控制和安全策略机制。基于身份的安全策略可以交错，无传统的基于 IP 地址的规则之间的限制。

身份防火墙的主要优点包括：

- 将网络拓扑从安全策略解耦
- 简化安全策略创建
- 能够轻松识别用户在网络资源上的活动
- 简化用户活动监控

身份防火墙部署的架构

身份防火墙与提供实际身份映射的外部 Active Directory (AD) 代理配合，与 Window Active Directory 相集成。

身份防火墙由三个组件组成：

- ASA
- Microsoft Active Directory

  虽然 Active Directory 是 ASA 中身份防火墙的一部分，但是 Active Directory 管理员对其进行管理。数据可靠性和准确性取决于 Active Directory 中的数据。

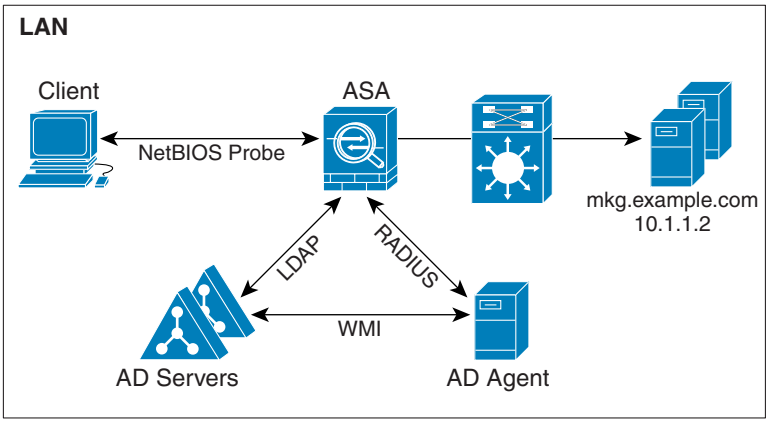
  支持的版本包括 Windows Server 2003、 Windows Server 2008 和 Windows Server 2008 R2 服务器。
- Active Directory (AD) 代理

  AD 代理在 Windows 服务器上运行。支持的 Windows 服务器包括 Windows 2003、 Windows 2008 和 Windows 2008 R2。

注　对于 AD 代理服务器来说，不支持 Windows 2003 R2。

图 31-1 显示身份防火墙的组件。随后的表格介绍这些组件的角色，以及它们如何互相通信。

图 31-1　身份防火墙组件



1	**在 ASA 上**：管理员配置本地用户组和身份防火墙策略。	4	**客户端 <-> ASA**：客户端通过 Microsoft Active Directory 登录网络。 AD 服务器对用户进行身份验证并生成用户登录安全日志。 或者，客户端可以通过直接转发代理或 VPN 登录网络。

2	**ASA <-> AD 服务器**：ASA 发送对在 AD 服务器上配置的 Active Directory 组的 LDAP 查询。 ASA 整合本地和 Active Directory 组，并基于用户身份应用访问规则和模块化策略框架安全策略。	5	**ASA <-> 客户端**：基于在 ASA 上配置的策略，它许可或拒绝客户端访问。 如果已进行配置，ASA 则探测客户端的 NetBIOS 来通过非活动和无响应用户。
3	**ASA <-> AD 代理**：根据身份防火墙配置，ASA 下载 IP - 用户数据库或向 AD 代理发送 RADIUS 请求来要求提供用户的 IP 地址。 ASA 将从网络身份验证和 VPN 会话所了解到的新映射的条目转发到 AD 代理。	6	**AD 代理 <-> AD 服务器**：AD 代理维护用户 ID 和 IP 地址映射条目的缓存，并将更改通知给 ASA。 AD 代理向系统日志服务器发送日志。

身份防火墙功能

身份防火墙包括以下主要功能。

灵活性

- 通过向 AD 代理查询每个新 IP 地址或通过维护整个用户身份和 IP 地址数据库的本地副本，ASA 可以从 AD 代理检索用户身份和 IP 地址映射。
- 支持用户身份策略目标的主机组、子网或 IP 地址。
- 支持用户身份策略源和目标的完全限定域名 (FQDN)。
- 支持基于 ID 策略的五元组策略组合。基于身份的功能与现有五元组解决方案配套使用。
- 支持使用 IPS 和应用检查策略。
- 从远程访问 VPN、AnyConnect VPN、L2TP VPN 和直接转发代理检索用户身份信息。所有检索到的用户填充到与 AD 代理连接的所有 ASA。

可扩展性

- 每个 AD 代理支持 100 个 ASA。多个 ASA 能够与单个 AD 代理通信，以在更大型网络部署中提供扩展性。
- 假如 IP 地址在所有域中保持唯一，则支持 30 个 Active Directory 服务器。
- 在域中的每个用户身份可以包含多达 8 个 IP 地址。
- 在 ASA 5500 系列型号的有效策略中支持多达 64,000 个用户身份 - IP 地址映射条目。此限制控制应用了策略的用户最大数量。用户总数是在所有不同情景中配置的所有用户合计数量。
- 在有效 ASA 策略中支持多达 256 个用户组。
- 单个访问规则可以包含一个或多个用户组或用户。
- 支持多个域。

可用性

- 当 AD 代理无法将源 IP 地址映射到用户身份时，ASA 从 Active Directory 中检索组信息，回退到 IP 地址网络身份验证。
- 如果任何 Active Directory 服务器或 ASA 不响应，AD 代理会继续运行。
- 支持在 ASA 上配置一个主要 AD 代理和一个辅助 AD 代理。如果主要 AD 代理停止响应，ASA 可以切换到辅助 AD 代理。

- 如果 AD 代理不可用，ASA 可以回退到现有身份源，比如直接转发代理和 VPN 身份验证。
- AD 代理运行监视器进程，在服务关闭时自动重新启动服务。
- 允许在 ASA 之间使用分布式 IP 地址/用户映射数据库。

部署方案

根据环境要求，您能够以下列方式部署身份防火墙组件。

图 31-2 显示如何部署身份防火墙组件以允许冗余。方案 1 显示无组件冗余的简单安装。方案 2 也显示无冗余的简单安装。但是，在此部署方案中，Active Directory 服务器和 AD 代理共同位于同一 Windows 服务器上。

图 31-2　　无冗余部署方案

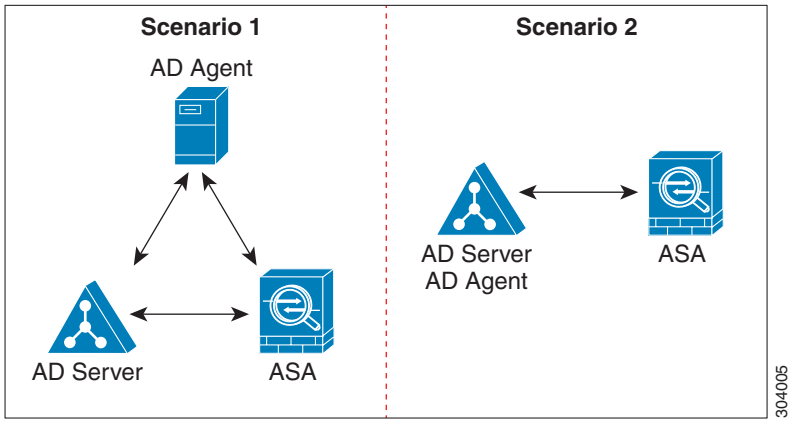


图 31-3 显示如何部署身份防火墙组件以支持冗余。方案 1 显示一种部署，其中有多个 Active Directory 服务器和单个安装在单独 Windows 服务器上的 AD 代理。方案 2 显示一个部署，其中有多个 Active Directory 服务器和多个安装在单独 Windows 服务器上的 AD 代理。

图 31-3　　具有冗余组件的部署方案

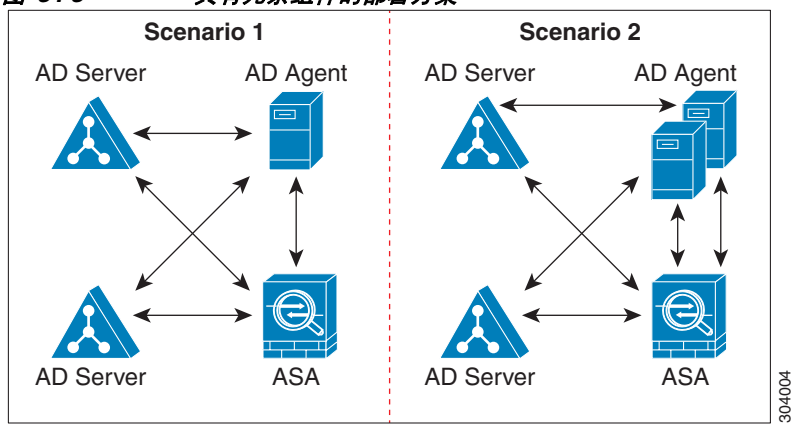


图 31-4 显示所有身份防火墙组件（Active Directory 服务器、AD 代理和客户端）如何进行安装以及如何在局域网上进行通信。

图 31-4　基于局域网的部署

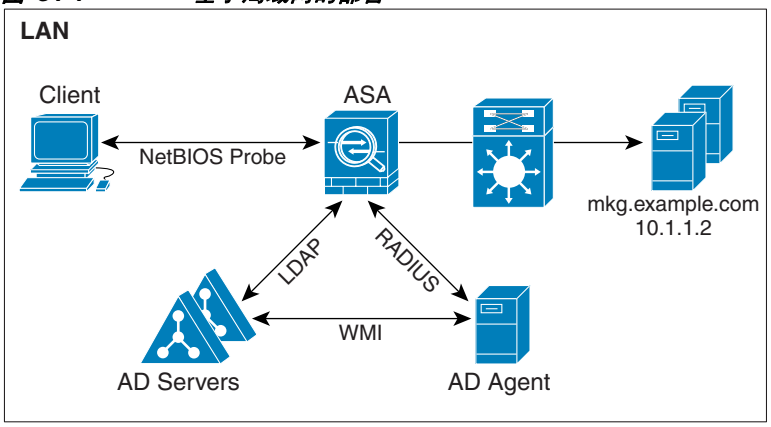


图 31-5 显示支持远程站点的基于广域网的部署。Active Directory 服务器和 AD 代理安装在主站点局域网中。客户端位于远程站点，并通过广域网连接至身份防火墙组件。

图 31-5　基于广域网的部署

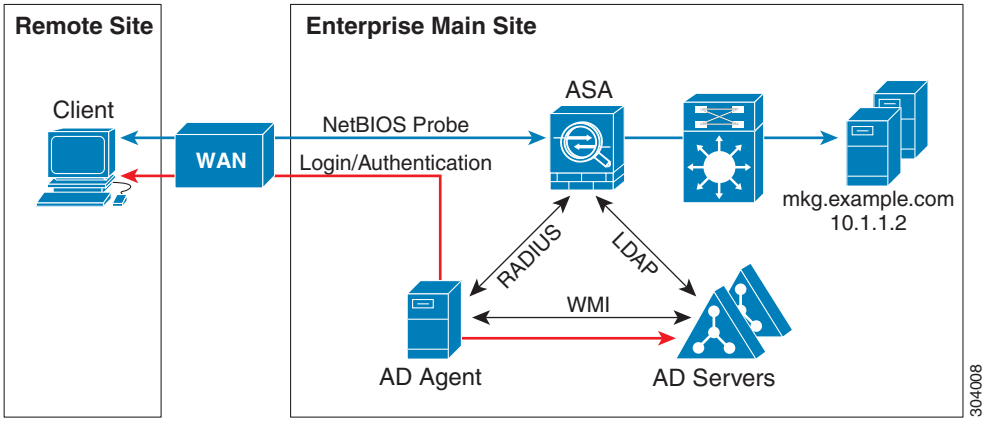


图 31-6 也显示支持远程站点的基于广域网的部署。Active Directory 服务器安装在主站点局域网中。但是，AD 代理通过远程站点的客户端进行安装和访问。远程客户端通过广域网连接至主站点的 Active Directory 服务器。

图 31-6　具有远程 AD 代理的基于广域网的部署

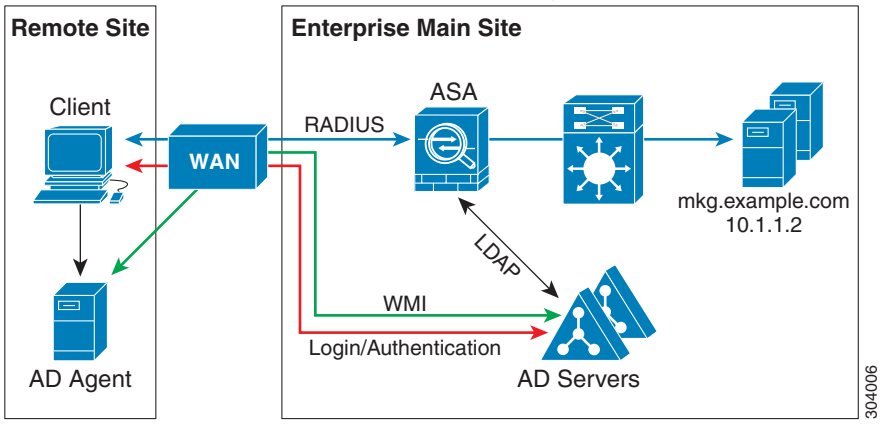
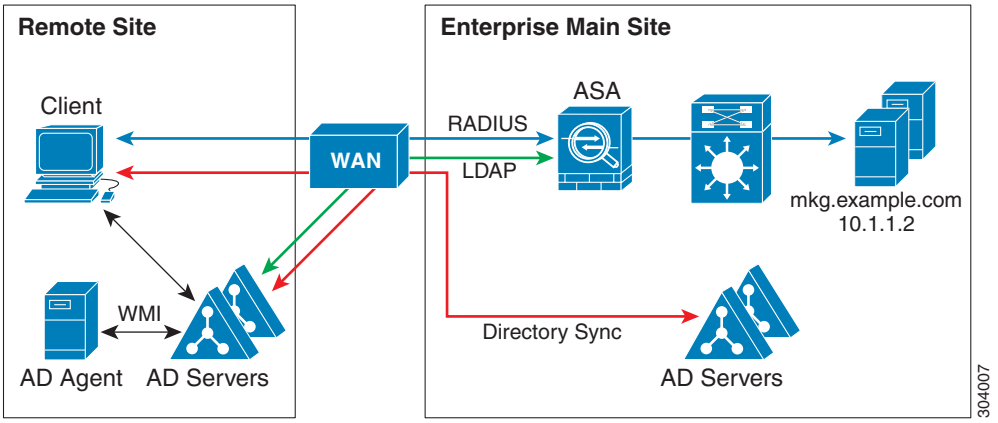


图 31-7 显示扩展的远程站点安装。AD 代理和 Active Directory 服务器安装在远程站点。客户端登录位于主站点的网络资源时，在本地访问这些组件。远程 Active Directory 服务器必须与位于主站点的中央 Active Directory 服务器同步其数据。

图 31-7　具有远程 AD 代理和 AD 服务器的基于广域网的部署



身份防火墙许可

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

故障转移准则

- 当启用状态故障转移时，身份防火墙支持从主用设备到备用设备的用户身份 - IP 地址映射和 AD 代理状态复制。但是，仅复制用户身份 - IP 地址映射、 AD 代理状态和域状态。用户和用户组记录不会复制到备用 ASA。
- 配置故障转移后，也必须配置备用 ASA 以直接连接至 AD 代理来检索用户组。即使当已为身份防火墙配置 NetBIOS 探测选项，备用 ASA 也不会向客户端发送 NetBIOS 数据包。

- 当主用 ASA 确定客户端处于非活动状态时，信息传播到备用 ASA。用户统计信息不会传播到备用 ASA。
- 配置故障转移后，必须将 AD 代理配置为与主用和备用 ASA 通信。有关在 AD 代理服务器上配置 ASA 的步骤，请参阅 《*Active Directory 代理安装和设置指南*》。

IPv6 准则

- 支持 IPv6。
- AD 代理支持具有 IPv6 地址的终端。它可以接收日志事件中的 IPv6 地址，将其置于缓存中，并通过 RADIUS 消息进行发送。
- 不支持 IPv6 上的 NetBIOS。

附加准则和限制

- 不支持将完整 URL 用作目标地址。
- 对于要运行的 NetBIOS 探测，在 ASA、 AD 代理和客户端之间的网络必须支持 UDP 封装的 NetBIOS 流量。
- 当存在干预路由器时，身份防火墙的 MAC 地址检查不起作用。登录同一路由器之后的客户端的用户具有相同的 MAC 地址。通过使用此实现，来自同一路由器的所有数据包都可以通过检查，这是因为 ASA 无法确定路由器之后的实际 MAC 地址。
- 以下 ASA 功能不支持在扩展 ACL 中使用基于身份的对象和 FQDN：
  - 路由映射
  - 加密映射
  - WCCP
  - NAT
  - 组策略 （除 VPN 过滤器外）
  - DAP
- 您可以使用 **user-identity update active-user-database** 命令主动发起从 AD 代理进行的用户 - IP 地址下载。

  根据设计，如果以前的下载会话已完成，ASA 将不允许再次发出此命令。

  因此，如果用户 - IP 数据库非常大，以前的下载会话仍未完成，并且，您发出另一个 **user-identity update active-user-database** 命令，系统将显示以下错误消息：

  ```
  "ERROR: one update active-user-database is already in progress."
  ```

  您需要等到上次会话完全结束，然后才可以发出另一个 **user-identity update active-user-database** 命令。

  此行为另一个示例的发生是由于从 AD 代理到 ASA 的数据包丢失。

  当发出 **user-identity update active-user-database** 命令时，ASA 要求提供要下载的用户 - IP 映射条目的总数。然后，AD 代理发起与 ASA 的 UDP 连接，并发送授权请求数据包的更改信息。

  如果由于某种原因导致数据包丢失，ASA 也就无法识别这一点。因此，ASA 会保持会话 4 到 5 分钟。在此期间，如果您已发出 **user-identity update active-user-database** 命令，系统将继续显示错误消息。
- 将 Cisco Context Directory Agent (CDA) 与 ASA 或 Cisco Ironport Web Security Appliance (WSA) 配合时，请确保打开以下端口：
  - UDP 身份验证端口 - 1645
  - UDP 记帐端口 - 1646

  - UDP 侦听端口 - 3799

    侦听端口用于从 CDA 向 ASA 或 WSA 发送授权更改请求。

- 对于域名，以下字符无效：\:*?"<>|。有关命名约定，请参阅 http://support.microsoft.com/kb/909264。
- 对于用户名，以下字符无效：\[]:;=,+*?"<>|@。
- 对于用户组名，以下字符无效：\[]:;=,+*?"<>|。

先决条件

在 ASA 中配置身份防火墙之前，必须满足 AD 代理和 Microsoft Active Directory 的先决条件。

AD 代理

- AD 代理必须安装在可通过 ASA 访问的 Windows 服务器上。此外，您必须将 AD 代理配置为从 Active Directory 服务器获取信息并与 ASA 通信。
- 支持的 Windows 服务器包括 Windows 2003、 Windows 2008 和 Windows 2008 R2。

注　对于 AD 代理服务器来说，不支持 Windows 2003 R2。

- 关于安装和配置 AD 代理的步骤，请参阅 《*Active Directory 代理安装和设置指南*》。
- 在 ASA 中配置 AD 代理之前，请获取 AD 代理和 ASA 用于通信的密钥值。该值必须在 AD 代理和 ASA 上均匹配。

Microsoft Active Directory

- Microsoft Active Directory 必须安装在 Windows 服务器上，并且可通过 ASA 访问。支持的版本包括 Windows 2003、 2008 和 2008 R2 服务器。
- 在 ASA 上配置 Active Directory 服务器之前，请在 Active Directory 中创建用于 ASA 的用户帐户。
- 此外，ASA 通过使用在 LDAP 上启用的 SSL 向 Active Directory 服务器发送加密的登录信息。在 Active Directory 服务器上必须启用 SSL。有关如何启用 Active Directory 的 SSL，请参阅 Microsoft Active Directory 的文档。

注　在运行 AD 代理安装程序之前，必须在 AD 代理监控的每个 Microsoft Active Directory 服务器上安装 *README First for the Cisco Active Directory Agent* 中列出的补丁。即使当 AD 代理直接安装在域控制器服务器上时，这些补丁也是必需的。

配置身份防火墙

本节包含以下主题：

- 第 31-9 页的配置身份防火墙任务流程
- 第 31-9 页的配置 Active Directory 域
- 第 31-11 页的配置 Active Directory 代理
- 第 31-12 页的配置身份选项

- 第 31-16 页的配置基于身份的安全策略
- 第 31-17 页的收集用户统计信息

配置身份防火墙任务流程

如要配置身份防火墙，请执行以下任务：

步骤 1　在 ASA 中配置 Active Directory 域。

请参阅第 31-9 页的配置 Active Directory 域。

关于部署 Active Directory 服务器以满足环境要求的方式，另请参阅第 31-4 页的部署方案。

步骤 2　在 ASA 中配置 AD 代理。

请参阅第 31-11 页的配置 Active Directory 代理。

关于部署 AD 代理以满足环境要求的方式，另请参阅第 31-4 页的部署方案。

步骤 3　配置身份选项。

请参阅第 31-12 页的配置身份选项。

步骤 4　配置基于身份的安全策略。在配置 AD 域和 AD 代理后，您可以创建将用在许多功能中的基于身份的对象组和 ACL。

请参阅第 31-16 页的配置基于身份的安全策略。

配置 Active Directory 域

为使 ASA 在从 AD 代理接收 IP - 用户映射时可以从特定域下载 Active Directory 组和接受用户身份，在 ASA 上的 Active Directory 域配置是必需的。

先决条件

- Active Directory 服务器 IP 地址
- LDAP 基础 DN 的可分辨名称
- 身份防火墙用于连接 Active Directory 域控制器的 Active Directory 用户的可分辨名称和密码

如要配置 Active Directory 域，请执行以下步骤：

	命令	用途
步骤 1	**aaa-server** *server-tag* **protocol ldap** **示例：** `ciscoasa(config)# aaa-server adserver protocol ldap`	创建 AAA 服务器组并为 AAA 服务器配置 Active Directory 服务器参数。

	命令	用途
步骤 2	**aaa-server** *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*] **示例：** `ciscoasa(config-aaa-server-group)# aaa-server adserver (mgmt) host 172.168.224.6`	对于 Active Directory 服务器，将 AAA 服务器配置为主机特定的 AAA 服务器组和 AAA 服务器参数的一部分。
步骤 3	**ldap-base-dn** *string* **示例：** `ciscoasa(config-aaa-server-host)# ldap-base-dn DC=SAMPLE,DC=com`	在 LDAP 层次结构中指定当服务器接收到授权请求时应开始搜索的位置。 指定 **ldap-base-dn** 命令为可选操作。如果不指定此命令，ASA 从 Active Directory 检索 defaultNamingContext，并将其作为基础 DN。
步骤 4	**ldap-scope subtree** **示例：** `ciscoasa(config-aaa-server-host)# ldap-scope subtree`	在 LDAP 层次结构中指定当服务器接收到授权请求时应执行的搜索范围。
步骤 5	**ldap-login-password** *string* **示例：** `ciscoasa(config-aaa-server-host)# ldap-login-password obscurepassword`	为 LDAP 服务器指定登录密码。
步骤 6	**ldap-login-dn** *string* **示例：** `ciscoasa(config-aaa-server-host)# ldap-login-dn SAMPLE\user1`	指定系统应将其绑定的目录对象名称。 ASA 通过向用户身份验证请求添加 Login DN 字段来标识自己，实现经过身份验证的绑定。 Login DN 字段介绍 ASA 的身份验证特征。 *string* 参数是多达 128 个字符的区分大小写的字符串，在 LDAP 层次结构中指定目录对象名称。该字符串中不允许使用空格，但是允许使用其他特殊字符。 您可以指定传统或简化的格式。 典型的 **ldap-login-dn** 命令格式包括：CN=username,OU=Employees,OU=Sample Users,DC=sample,DC=com。
步骤 7	**server-type microsoft** **示例：** `ciscoasa(config-aaa-server-host)# server-type microsoft`	配置 Microsoft Active Directory 服务器的 LDAP 服务器模式。
步骤 8	**ldap-group-base-dn** *string* **示例：** `ciscoasa(config-aaa-server-host)# ldap-group-base-dn OU=Sample Groups,DC=SAMPLE,DC=com`	指定 Active Directory 组配置在 Active Directory 域控制器中的位置。如果未指定，则使用 **ldap-group-base-dn** 命令中的值。 指定 **ldap-group-base-dn** 命令为可选操作。

	命令	用途
步骤 9	**ldap-over-ssl enable** **示例：** `ciscoasa(config-aaa-server-host)# ldap-over-ssl enable`	允许 ASA 通过 SSL 访问 Active Directory 域控制器。如要支持 SSL 上的 LDAP，需要将 Active Directory 服务器配置为具有此支持。 默认情况下，Active Directory 没有配置 SSL。如果未在 Active Directory 上配置 SSL，则不需要在 ASA 上为身份防火墙配置 SSL。
步骤 10	**server-port** *port-number* **示例：** `ciscoasa(config-aaa-server-host)# server-port 389` `ciscoasa(config-aaa-server-host)# server-port 636`	默认情况下，如果 **ldap-over-ssl** 命令未启用，默认服务器端口为 389；如果 **ldap-over-ssl** 命令已启用，默认服务器端口为 636。
步骤 11	**group-search-timeout** *seconds* **示例：** `ciscoasa(config-aaa-server-host)# group-search-timeout 300`	设置在 LDAP 查询超时前的时间量。

配置 Active Directory 代理

为 AD 代理服务器组配置主要和辅助 AD 代理。当 ASA 检测到主要 AD 代理不响应，并已指定辅助代理，ASA 将切换到辅助 AD 代理。AD 代理的 Active Directory 服务器将 RADIUS 用作通信协议；因此，您应该指定 ASA 和 AD 代理间共享密钥的关键属性。

先决条件

确保在配置 AD 代理之前具备以下信息：

- AD 代理 IP 地址
- ASA 和 AD 代理之间的共享密钥

如要配置 AD 代理，请执行以下步骤：

	命令	用途
步骤 1	**aaa-server** *server-tag* **protocol radius** **示例：** `ciscoasa(config)# aaa-server adagent protocol radius`	创建 AAA 服务器组并为 AD 代理配置 AAA 服务器参数。
步骤 2	**ad-agent-mode** **示例：** `ciscoasa(config)# ad-agent-mode`	启动 AD 代理模式。

	命令	用途
步骤 3	**aaa-server** *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*] **示例：** `ciscoasa(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101`	对于 AD 代理，将 AAA 服务器配置为主机特定的 AAA 服务器组和 AAA 服务器参数的一部分。
步骤 4	**key** *key* **示例：** `ciscoasa(config-aaa-server-host)# key mysecret`	指定用于对到 AD 代理服务器的 ASA 进行身份验证的服务器密钥值。
步骤 5	**user-identity ad-agent aaa-server** *aaa_server_group_tag* **示例：** `ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent`	定义 AD 代理的服务器组。 在 *aaa_server_group_tag* 参数中定义的第一个服务器是主要 AD 代理，定义的第二个服务器是辅助 AD 代理。 身份防火墙仅支持定义两个 AD 代理主机。 当 ASA 检测到主要 AD 代理关闭，并已指定备用代理时，它将切换到辅助 AD 代理。 AD 代理的 AAA 服务器将 RADIUS 用作通信协议；因此，您应该指定 ASA 和 AD 代理之间的共享密钥的关键属性。
步骤 6	**test aaa-server ad-agent** **示例：** `ciscoasa(config-aaa-server-host)# test aaa-server ad-agent`	测试 ASA 和 AD 代理服务器之间的通信。

后续操作

配置身份防火墙的访问规则。请参阅第 31-16 页的配置基于身份的安全策略。

配置身份选项

执行此操作步骤来添加或编辑身份防火墙功能；选中 **Enable** 复选框启用此功能。默认情况下，身份防火墙功能被禁用。

先决条件

在为身份防火墙配置身份选项之前，满足 AD 代理和 Microsoft Active Directory 的先决条件。有关 AD 代理和 Microsoft Active Directory 安装的要求，请参阅第 31-8 页的先决条件。

如要配置身份防火墙的身份选项，请执行以下步骤：

	命令	用途
步骤 1	**user-identity enable** **示例：** `ciscoasa(config)# user-identity enable`	启用身份防火墙功能。
步骤 2	**user-identity default-domain** *domain_NetBIOS_name* **示例：** `ciscoasa(config)# user-identity default-domain SAMPLE`	指定身份防火墙的默认域。 对于 *domain_NetBIOS_name* 参数，请输入用户名（最多 32 个字符，由 [a-z]、[A-Z]、[0-9]、[!@#$%^&()-_=+[]{};,.] 组成，第一个字符不能为 . 和空格）。如果域名包含空格，请确保使用引号将整个名称引起来。域名不区分大小写。 当没有为所有用户或用户组明确配置域时，所有用户和用户组都使用默认域。当未指定默认域时，用户和组的默认域是 LOCAL。对于多情景模式，您可以为每个情景以及在系统执行空间中设置一个默认域名。 **注**　指定的默认域名必须与在 Active Directory 域控制器上配置的 NetBIOS 域名相匹配。如果域名不匹配，AD 代理会错误地将用户身份 - IP 地址映射的条目与在配置 ASA 时输入的域名相关联。要查看 NetBIOS 域名，请在任意文本编辑器中打开 Active Directory 用户事件安全日志。 身份防火墙将 LOCAL 域用于所有本地定义的用户组或本地定义的用户。通过网络门户（直接转发代理）登录的用户指定为属于用于身份验证的 Active Directory 域。除非使用 Active Directory 通过 LDAP 对 VPN 进行身份验证，否则，通过 VPN 登录的用户指定为属于 LOCAL 域。在这种情况下，身份防火墙可以将用户与其 Active Directory 域相关联。
步骤 3	**user-identity domain** *domain_nickname* **aaa-server** *aaa_server_group_tag* **示例：** `ciscoasa(config)# user-identity domain SAMPLE aaa-server ds`	将为导入用户组查询而为 AAA 服务器定义的 LDAP 参数与域名相关联。 对于 *domain_nickname* 参数，请输入名称（最多 32 个字符，由 [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,.] 组成，第一个字符不能为 . 和空格）。如果域名包含空格，则必须用引号将该空格字符引起来。域名不区分大小写。
步骤 4	**user-identity logout-probe netbios local-system probe-time** *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed** | **match-any** | **exact-match**] **示例：** `ciscoasa(config)# user-identity logout-probe netbios local-system probe-time minutes 10 retry-interval seconds 10 retry-count 2 user-not-needed`	启用 NetBIOS 探测。启用此选项可以配置 ASA 探测用户客户端 IP 地址以确定客户端是否仍处于活动状态的频率。默认情况下，NetBIOS 探测被禁用。 为了最小化 NetBIOS 数据包，当用户已空闲超过指定的分钟数时，ASA 仅向客户端发送一个 NetBIOS 探测。 • **Exact-match** - 分配到 IP 地址的用户的用户名在 NetBIOS 响应中必须唯一。否则，该 IP 地址的用户身份就被视为无效。 • **User-not-needed** - 只要 ASA 接收到来自客户端的 NetBIOS 响应，用户身份就被视为有效。 身份防火墙仅为那些处于活动状态且存在于至少一个安全策略中的用户执行 NetBIOS 探测。 ASA 不为用户通过直接转发代理登录或通过使用 VPN 登录的客户端执行 NetBIOS 探测。

	命令	用途
步骤 5	**user-identity inactive-user-timer minutes** *minutes* **示例：** `ciscoasa(config)# user-identity inactive-user-timer minutes 120`	指定用户在被认为空闲之前的时间量，这意味着 ASA 在指定的时间量内没有接收到来自用户 IP 地址的流量。 当计时器到期时，用户 IP 地址标记为非活动并从本地缓存的用户身份 - IP 地址映射数据库中移除，并且 ASA 不再通知有关该 IP 地址的 AD 代理。仍然允许现有流量通过。指定此命令后，即使当 NetBIOS Logout Probe 已配置时， ASA 也运行非活动计时器。 默认情况下，空闲超时设置为 60 分钟。 **注**　Idle Timeout 选项不适用于 VPN 或直接转发代理用户。
步骤 6	**user-identity poll-import-user-group-timer hours** *hours* **示例：** `ciscoasa(config)# user-identity poll-import-user-group-timer hours 1`	指定在 ASA 查询 Active Directory 服务器有关用户组信息之前的时间量。 如果向 Active Directory 组添加用户或从其删除用户， ASA 会在导入组计时器运行后收到更新的用户组。 默认情况下，**poll-import-user-group-timer hours** 的值为 8 小时。 如要立即更新用户组信息，请输入 **user-identity update import-user** 命令。
步骤 7	**user-identity action netbios-response-fail remove-user-ip** **示例：** `ciscoasa(config)# user-identity action netbios-response-fail remove-user-ip`	指定客户端不响应 NetBIOS 探测时的操作。例如，到该客户端的网络连接可能阻塞或客户端处于非活动状态。 配置 **user-identity action remove-user-ip** 命令后，ASA 将为该客户端移除用户身份 - IP 地址映射。 默认情况下，此命令被禁用。
步骤 8	**user-identity action domain-controller-down** *domain_nickname* **disable-user-identity-rule** **示例：** `ciscoasa(config)# user-identity action domain-controller-down SAMPLE disable-user-identity-rule`	指定当域因为 Active Directory 域控制器未响应而关闭时的操作。 当域关闭，并且已配置 **disable-user-identity-rule** 关键字时，ASA 将为该域禁用用户身份 - IP 地址映射。此外，该域内所有用户 IP 地址的状态在通过 **show user-identity user** 命令显示的输出内容中都标记为禁用。 默认情况下，此命令被禁用。
步骤 9	**user-identity user-not-found enable** **示例：** `ciscoasa(config)# user-identity user-not-found enable`	启用未找到的用户的跟踪。仅跟踪最后 1024 个 IP 地址。 默认情况下，此命令被禁用。
步骤 10	**user-identity action ad-agent-down disable-user-identity-rule** **示例：** `ciscoasa(config)# user-identity action ad-agent-down disable-user-identity-rule`	指定当 AD 代理不响应时的操作。 当 AD 代理关闭，并且已配置 **user-identity action ad-agent-down** 命令时，ASA 将禁用与该域内用户关联的用户身份规则。此外，该域内所有用户 IP 地址的状态在通过 **show user-identity user** 命令显示的输出内容中都标记为禁用。 默认情况下，此命令被禁用。
步骤 11	**user-identity action mac-address-mismatch remove-user-ip** **示例：** `ciscoasa(config)# user-identity action mac-address-mismatch remove-user-ip`	指定当发现用户的 MAC 地址与当前映射到该 MAC 地址的 ASA IP 地址不一致时的操作。 配置 **user-identity action mac-address-mismatch** 命令后， ASA 将为该客户端移除用户身份 - IP 地址映射。 默认情况下，指定此命令后，ASA 将使用 **remove-user-ip** 关键字。

	命令	用途
步骤 12	**user-identity ad-agent active-user-database** {**on-demand** | **full-download**} **示例：** ciscoasa(config)# user-identity ad-agent active-user-database full-download	定义 ASA 如何从 AD 代理检索用户身份 - IP 地址映射信息： • **Full-download** - 指定 ASA 向 AD 代理发送请求以在 ASA 开始时下载整个 IP - 用户映射表，然后在用户登录和注销时接收递增的 IP - 用户映射信息。 • **On-demand** - 指定当 ASA 接收到要求新连接的数据包并且其源 IP 地址的用户没有位于用户身份数据库中时，ASA 将从 AD 代理检索 IP 地址的用户映射信息。 默认情况下，ASA 使用完全下载选项。 完全下载是事件驱动，意味着当有后续下载数据库请求时，将只发送用户身份 - IP 地址映射数据库的更新。 当 ASA 在 AD 代理上注册更改请求时，AD 代理向 ASA 发送新事件。
步骤 13	**user-identity ad-agent hello-timer seconds** *seconds* **retry-times** *number* **示例：** ciscoasa(config)# user-identity ad-agent hello-timer seconds 20 retry-times 3	定义 ASA 和 AD 代理之间的 hello 计时器。 在 ASA 与 AD 代理之间的 hello 计时器定义 ASA 交换 hello 数据包的频率。 ASA 使用 hello 数据包来获取 ASA 复制状态 （保持同步或失去同步）和域状态 （运行或关闭）。如果 ASA 未收到来自 AD 代理的响应，则会在指定的时间间隔后重新发送 hello 数据包。 默认情况下，hello 计时器设置为 30 秒和 5 次重试。
步骤 14	**user-identity ad-agent event-timestamp-check** **示例：** ciscoasa(config)# user-identity ad-agent event-timestamp-check	使 ASA 能够持续跟踪它收到的用于每个标识符的上一个事件时间戳，并能够在事件时间戳晚于 ASA 的时钟至少 5 分钟的情况下，或者，如果其时间戳早于最后事件时间戳时，丢弃任何消息。 对于最近启动的不知道上一个事件时间戳的 ASA，ASA 会将事件时间戳与自己的时钟进行比较。如果事件至少是在 5 分钟之前，ASA 将不接受该消息。 我们建议您将 ASA、 Active Directory 和 Active Directory 代理配置为使用 NTP 来同步它们之间的时钟。
步骤 15	**user-identity ad-agent aaa-server** *aaa_server_group_tag* **示例：** ciscoasa(config)# user-identity ad-agent aaa-server adagent	定义 AD 代理的服务器组。 对于 *aaa_server_group_tag* 参数，请输入通过 **aaa-server** 命令定义的值。

后续操作

配置 Active Directory 域和服务器组。请参阅第 31-9 页的配置 Active Directory 域。

配置 AD 代理。请参阅第 31-11 页的配置 Active Directory 代理。

配置基于身份的安全策略

您可以在许多 ASA 功能中纳入基于身份的策略。任何使用扩展 ACL 的功能（除了在第 31-6 页的准则和限制中列为不支持的 ACL）都可以利用身份防火墙。现在，您可以将用户身份参数添加到扩展 ACL 中，并添加基于网络的参数。

- 如要配置扩展 ACL，请参阅第 17 章，“访问控制列表”
- 如要配置在 ACL 中可以使用的 本地用户组，请参阅第 16-6 页的配置本地用户组。

可以使用身份的功能包括以下内容：

- 访问规则 - 访问规则利用网络信息允许或拒绝接口上的流量。借助身份防火墙，您可以基于用户身份控制访问。请参阅防火墙配置指南。
- AAA 规则 - 身份验证规则（也称为直接转发代理）基于用户控制网络访问。由于此功能非常类似于访问规则加上身份防火墙，因此 AAA 规则现在可以用作用户 AD 登录超时情况下的身份验证备份方法。例如，对于无有效登录的任何用户，您可以触发 AAA 规则。如要确保 AAA 规则仅对无有效登录的用户触发，您可以在用于访问规则和 AAA 规则的扩展 ACL 中指定特殊用户名：None（无有效登录的用户）和 Any（有有效登录的用户）。在访问规则中，请照常为用户和组配置策略，但是，包括允许所有 None 用户的 AAA 规则；必须允许这些用户，以便他们以后可以触发 AAA 规则。然后，配置拒绝 Any 用户的 AAA 规则（这些用户将不受 AAA 规则的限制，并已由访问规则处理），但是 AAA 规则允许所有 None 用户。例如：

```
access-list 100 ex permit ip user CISCO\xyz any any
access-list 100 ex deny ip user CISCO\abc any any
access-list 100 ex permit ip user NONE any any
access-list 100 ex deny any any
access-group 100 in interface inside

access-list 200 ex deny ip user ANY any any
access-list 200 ex permit user NONE any any
aaa authenticate match 200 inside user-identity
```

  有关详细信息，请参阅 旧版功能指南。

- 云网络安全 - 可以控制将哪些用户发送给云网络安全代理服务器。此外，您可以在基于用户组 （包含在发送到云网络安全的 ASA 流量报头中）的云网络安全 ScanCenter 上配置策略。请参阅 《防火墙配置指南》。
- VPN 过滤器 - 虽然 VPN 一般不支持身份防火墙 ACL，但您可以将 ASA 配置为在 VPN 流量上执行基于身份的访问规则。默认情况下，VPN 流量不受访问规则限制。您可以强制 VPN 客户端遵守使用身份防火墙 ACL 的访问规则（使用 **no sysopt connection permit-vpn** 命令）。还可以使用具有 VPN 过滤器功能的身份防火墙 ACL；VPN 过滤器一般实现与访问规则相似的效果。

收集用户统计信息

如要通过模块化策略框架激活用户统计信息的收集并匹配身份防火墙的查询操作，请输入以下命令：

命令	用途
user-statistics [**accounting** | **scanning**] **示例：** ciscoasa**(config)#** class-map c-identity-example-1 ciscoasaciscoasa(config-cmap)# match access-list identity-example-1 ciscoasaciscoasa(config-cmap)# exit ciscoasaciscoasa(config)# policy-map p-identity-example-1 ciscoasaciscoasa(config-pmap)# class c-identity-example-1 ciscoasaciscoasa(config-pmap)# user-statistics accounting ciscoasaciscoasa(config-pmap)# exit ciscoasaciscoasa(config)# service-policy p-identity-example-1 interface outside	通过模块化策略框架激活用户统计信息的收集并匹配身份防火墙的查询操作。 **accounting** 关键字指定 ASA 收集已发送数据包计数、已发送丢弃计数和已接收的数据包计数。 **scanning** 关键字指定 ASA 仅收集已发送丢弃计数。 当配置策略映射以收集用户统计信息时，ASA 收集选定用户的详细统计信息。当指定无 **accounting** 或 **scanning** 关键字的 **user-statistics** 命令时，ASA 收集记帐和扫描统计信息。

配置示例

- 第 31-17 页的 AAA 规则和访问规则示例 1
- 第 31-18 页的 AAA 规则和访问规则示例 2
- 第 31-18 页的 VPN 过滤器示例

AAA 规则和访问规则示例 1

此示例显示允许用户通过 ASA 登录的典型直接转发代理配置。在本示例中，应用以下条件：

- ASA IP 地址为 172.1.1.118。
- Active Directory 域控制器的 IP 地址为 71.1.2.93。
- 终端用户客户端的 IP 地址为 172.1.1.118，并通过网络门户使用 HTTPS 登录。
- 用户通过 LDAP 由 Active Directory 域控制器进行身份验证。
- ASA 使用内部接口连接公司网络中的 Active Directory 域控制器。

```
ciscoasa(config)# access-list AUTH extended permit tcp any 172.1.1.118 255.255.255.255 eq http
ciscoasa(config)# access-list AUTH extended permit tcp any 172.1.1.118 255.255.255.255 eq https
ciscoasa(config)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 171.1.2.93
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-group-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-dn cn=kao,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-login-password *****
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)# server-type microsoft
ciscoasa(config-aaa-server-host)# aaa authentication match AUTH inside LDAP
ciscoasa(config)#
```

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 0.0.0.0 0.0.0.0 inside
ciscoasa(config)#
ciscoasa(config)# auth-prompt prompt Enter Your Authentication
ciscoasa(config)# auth-prompt accept You are Good
ciscoasa(config)# auth-prompt reject Goodbye
```

AAA 规则和访问规则示例 2

在本示例中，应用以下准则：

- 在 **access list** 命令中，应在输入 **access-list 100 ex deny any any** 命令之前写入允许用户 NONE 的规则，从而允许未经身份验证的传入用户触发 AAA 直接转发代理。
- 在 **auth access-list** 命令中，允许用户 NONE 规则仅确保未经身份验证的触发直接转发代理。理想情况下，他们应该是最后几行。

```
ciscoasa(config)# access-list listenerAuth extended permit tcp any any
ciscoasa(config)# aaa authentication match listenerAuth inside ldap
ciscoasa(config)# aaa authentication listener http inside port 8888
ciscoasa(config)# access-list 100 ex permit ip user SAMPLE\user1 any any
ciscoasa(config)# access-list 100 ex deny ip user SAMPLE\user2 any any
ciscoasa(config)# access-list 100 ex permit ip user NONE any any
ciscoasa(config)# access-list 100 ex deny any any
ciscoasa(config)# access-group 100 in interface inside
ciscoasa(config)# aaa authenticate match 200 inside user-identity
```

VPN 过滤器示例

某些流量可能需要绕过身份防火墙。

ASA 向 AD 代理报告通过 VPN 身份验证或网络门户 （直接转发代理）登录的用户， AD 代理将用户信息分发给所有注册的 ASA 设备。具体来说，通过身份验证的用户的 IP - 用户映射将转发到所有 ASA 情景中，这些情景包括接收 HTTP/HTTPS 数据包并进行身份验证的输入接口。 ASA 指定通过 VPN 登录的用户属于 LOCAL 域。

有两种不同的方式可以对 VPN 用户应用身份防火墙 (IDFW) 规则：

- 应用禁用绕过访问列表检查的 VPN 过滤器
- 应用启用绕过访问列表检查的 VPN 过滤器

使用 IDFW 规则的 VPN - 示例 1

默认情况下，**sysopt connection permit-vpn** 命令已启用，VPN 流量免除访问列表检查。要对 VPN 流量应用基于接口的 ACL 规则，则需要禁用 VPN 流量访问列表绕过。

在本示例中，如果用户从外部接口登录，IDFW 规则控制可以访问哪些网络资源。所有 VPN 用户存储在 LOCAL 域下。因此，只有向 LOCAL 用户或包含 LOCAL 用户的对象组应用规则才有意义。

```
! Apply VPN-Filter with bypassing access-list check disabled
no sysopt connection permit-vpn
access-list v1 extended deny ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v1 extended permit ip user LOCAL\idfw any 20.0.0.0 255.255.255.0
access-group v1 in interface outside
```

使用 IDFW 规则的 VPN - 示例 2

默认情况下，**sysopt connection permit-vpn** 命令已启用，VPN 流量访问绕过已启用。VPN 过滤器可用于向 VPN 流量应用 IDFW 规则。可以在 CLI 用户名和组策略中定义使用 IDFW 规则的 VPN 过滤器。

在此示例中，当用户 idfw 登录时，该用户可以访问 10.0.00/24 子网中的网络资源。但是，当用户 user1 登录时，则被拒绝访问 10.0.00/24 子网中的网络资源。请注意，所有 VPN 用户都存储在 LOCAL 域下。因此，只有向 LOCAL 用户或包含 LOCAL 用户的对象组应用规则才有意义。

注　IDFW 规则仅可以应用于组策略下 VPN 过滤器，并不是在所有其他组策略功能中都提供。

```
! Apply VPN-Filter with bypassing access-list check enabled
sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v2 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0
username user1 password QkBIIYVi6IFLEsYv encrypted privilege 0 username user1 attributes
    vpn-group-policy group1 vpn-filter value v2
username idfw password eEm2dmjMaopcGozT encrypted
username idfw attributes
    vpn-group-policy testgroup vpn-filter value v1

sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0 access-list
v1 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0 group-policy group1
internal
group-policy group1 attributes

    vpn-filter value v1
    vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless
```

监控身份防火墙

- 第 31-19 页的监控 AD 代理
- 第 31-20 页的监控组
- 第 31-20 页的监控身份防火墙的内存使用情况
- 第 31-20 页的监控身份防火墙用户

监控 AD 代理

如要获得 AD 代理的故障排除信息，请使用以下命令之一：

- **show user-identity ad-agent**
- **show user-identity ad-agent statistics**

这些命令显示有关主要和辅助 AD 代理的以下信息：

- AD 代理状态
- 域状态
- AD 代理统计信息

监控组

如要获取为身份防火墙配置的用户组的故障排除信息，请使用 **show user-identity group** 命令。

监控身份防火墙的内存使用情况

如要获取身份防火墙的内存使用情况的故障排除信息，请使用 **show user-identity memory** 命令。

此命令显示身份防火墙中各种模块的内存使用情况 （以字节为单位）：

- 用户
- 组
- 用户状态
- LDAP

  ASA 发送对在 Active Directory 服务器中配置的 Active Directory 组的 LDAP 查询。 Active Directory 服务器对用户进行身份验证并生成用户登录安全日志。
- AD 代理
- 其他
- 总内存使用情况

注　如何配置身份防火墙以从 AD 代理检索用户信息会影响功能所使用的内存量。您可以指定 ASA 是使用按需检索还是全部下载检索。选择按需检索的优点是使用较少的内存，因为只查询和存储接收到的数据包的用户。有关详细信息，请参阅第 31-12 页的配置身份选项。

监控身份防火墙用户

如要获取 AD 代理的故障排除信息，请输入以下命令之一：

- **show user-identity user all list**
- **show user-identity user active user** *domain\user-name* **list detail**

这些命令显示用户的以下信息：

domain\user_name　状态 （活动或非活动）　连接数　空闲分钟数

domain\user_name　活动连接　空闲分钟数

默认域名可以是实时域名、特殊保留词或 LOCAL。对于所有本地定义的用户组或本地定义的用户 （通过使用 VPN 或网络门户登录和进行身份验证的用户），身份防火墙使用 LOCAL 域名。当未指定默认域时，默认域名为 LOCAL。

基于每个用户而不是使用用户的 IP 地址存储空闲时间。

如果 **user-identity action domain-controller-down** *domain_name* **disable-user-identity-rule** 命令已配置且指定域已关闭，或者如果 **user-identity action ad-agent-down disable-user-identity-rule** 命令已配置且 AD 代理已关闭，所有已登录用户的状态都为禁用。

身份防火墙的功能历史记录

表 31-1 列出了此功能的版本历史记录。

表 31-1　身份防火墙的功能历史记录

功能名称	版本	功能信息
身份防火墙	8.4(2)	我们引入了身份防火墙功能。 我们引入或修改了以下命令：**user-identity enable**、**user-identity default-domain**、 **user-identity domain**、**user-identity logout-probe**、 **user-identity inactive-user-timer**、 **user-identity poll-import-user-group-timer**、 **user-identity action netbios-response-fail**、 **user-identity user-not-found**、**user-identity action ad-agent-down**、**user-identity action mac-address-mismatch**、 **user-identity action domain-controller-down**、 **user-identity ad-agent active-user-database**、 **user-identity ad-agent hello-timer**、 **user-identity ad-agent aaa-server**、**user-identity update import-user**、 **user-identity static user**、 **dns domain-lookup**、 **dns poll-timer**、 **dns expire-entry-timer**、 **object-group user**、 **show user-identity**、 **show dns**、 **clear configure user-identity**、**clear dns**、 **debug user-identity**。

ASA 和思科 TrustSec

- 第 32-1 页的关于集成思科 TrustSec 的 ASA
- 第 32-9 页的思科 TrustSec 的许可要求
- 第 32-9 页的使用思科 TrustSec 的先决条件
- 第 32-11 页的准则和限制
- 第 32-12 页的为思科 TrustSec 集成配置 ASA
- 第 32-24 页的配置示例
- 第 32-25 页的面向思科 TrustSec 的 AnyConnect VPN 支持
- 第 32-26 页的附加参考资料
- 第 32-27 页的思科 TrustSec 集成的功能历史

关于集成思科 TrustSec 的 ASA

- 第 32-2 页的关于思科 TrustSec
- 第 32-2 页的思科 TrustSec 中的 SGT 和 SXP 支持
- 第 32-2 页的思科 TrustSec 功能中的角色
- 第 32-3 页的安全组策略实施
- 第 32-4 页的 ASA 如何实施基于安全组的策略
- 第 32-5 页的安全组更改对 ISE 产生的影响
- 第 32-6 页的关于 ASA 上的 Speaker 和 Listener 角色
- 第 32-7 页的 SXP 通信速率
- 第 32-7 页的 SXP 计时器
- 第 32-7 页的 IP-SGT 管理器数据库
- 第 32-8 页的 ASA-思科 TrustSec 集成的功能

关于思科 TrustSec

通常，防火墙等安全功能根据预定义的 IP 地址、子网和协议执行访问控制。然而，随着企业不断向无边界网络过渡，用于连接人员和公司的技术以及对数据和网络保护的安全要求有了长足的发展。同时，终端变得越来越具流动性，而且用户通常利用各种终端 （例如，笔记本电脑 （而非台式机）、智能手机或平板电脑），这样用户属性结合终端属性一起提供了关键特征 （除了现有的基于 6 元组的规则以外），带防火墙功能的交换机和路由器或专用防火墙等实施设备能够可靠地利用这些关键特征制定访问控制决策。

因此，对于支持跨客户网络、在网络的接入层、分发层和核心层以及在数据中心实现安全性，终端属性或客户端身份属性的可用性和传送性已经成为越来越重要的要求。

思科 TrustSec 可以提供基于现有的身份感知基础设施的访问控制，确保网络设备之间的数据保密性，并集成平台上的安全访问服务。在思科 TrustSec 功能中，实施设备结合用户属性和终端属性制定基于角色和基于身份的访问控制决策。此信息的可用性和传送性支持在网络的接入层、分发层和核心层实现跨网络安全性。

在环境中实施思科 TrustSec 具备以下优势：

- 支持越来越具移动性和复杂的劳动力可以从任意设备进行适当并更安全的访问
- 针对正在连接有线或无线网络的人员和设备提供全面的可视性，降低安全风险
- 针对访问物理或云计算型的 IT 资源的网络用户的活动提供优越控制
- 通过集中化、高度安全的访问策略管理和可扩展的实施机制降低总体拥有成本

有关在各种思科产品上使用思科 TrustSec 功能的详细信息，请参阅第 32-26 页的附加参考资料。

思科 TrustSec 中的 SGT 和 SXP 支持

在思科 TrustSec 功能中，安全组访问可以将拓扑感知网络转换为基于角色的网络，支持在基于角色的访问控制 (RBAC) 的基础上实施端到端策略。在身份验证期间获得的设备和用户凭证用于按安全组对数据包进行分类。每个进入思科 TrustSec 云的数据包被标记有安全组标记 (SGT)。这种标记有助于可信的中间设备识别数据包的源身份，沿着数据路径实施安全策略。当 SGT 被用于定义安全组 ACL 时，SGT 可以指明域上的权限级别。

SGT 通过 IEEE 802.1X 身份验证、网络身份验证或 MAC 身份验证旁路 (MAB) 被分配到设备，被分配的同时带有 RADIUS 供应商特定属性。SGT 可以被静态地分配给特定 IP 地址或交换机接口。在成功进行身份验证之后，SGT 可以被动态地传送到交换机或访问点。

安全组交换协议 (SXP) 一种为思科 TrustSec 开发的协议，用以在不具有（支持 SGT 的）硬件支持的网络设备上将 IP--to-SGT 映射数据库传送到支持 SGT 和安全组 ACL 的硬件。SXP 为一种控制层面协议，可以将 IP-SGT 映射从身份验证点（例如，旧版接入层交换机）传送到网络中的上游设备。

SXP 连接为点到点的连接，使用 TCP 作为底层传输协议。SXP 使用众所周知的 TCP 端口号 64999 发起连接。此外，SXP 连接唯一可通过源 IP 地址和目标 IP 地址被识别。

思科 TrustSec 功能中的角色

为了提供基于身份和策略的访问实施，思科 TrustSec 功能包含以下角色：

- 访问请求者 (AR) - 访问请求者指的是请求访问网络中受保护资源的终端设备。它们是架构的主要主体，其访问权限视身份凭证而定。

  访问请求者包括终端设备，例如 计算机、笔记本电脑、移动电话、打印机、摄像机和支持 MACsec 功能的 IP 电话。

- 策略决定点 (PDP) - 策略决定点负责制定访问控制决策。PDP 可以提供 802.1x、MAB 和网络身份验证等功能。 PDP 通过 VLAN、 DACL 和安全组访问 (SGACL/SXP/SGT) 支持身份验证和实施。

  在思科 TrustSec 功能中，思科身份服务引擎 (ISE) 可充当 PDP。思科 ISE 提供身份和访问控制策略功能。

- 策略信息点 (PIP) - 策略信息点是向策略决策点提供外部信息 （例如，信誉、位置和 LDAP 属性）的源。

  策略信息点包括 Session Directory、 Sensor IPS 和 通信管理器等设备。

- 策略管理点 (PAP) - 策略管理点定义策略并将策略插入授权系统。PAP 提供思科 TrustSec 标记到用户身份映射和思科 TrustSec 标记到服务器资源映射，充当一个身份资源库。

  在思科 TrustSec 功能中，思科安全访问控制系统 （带集成式 802.1x 和 SGT 支持的策略服务器）充当 PAP。

- 策略实施点 (PEP) - 策略实施点是实施 PDP 为每个 AR 制定的决策（策略规则和操作）的实体。PEP 设备通过网络上的主要通信路径获悉身份信息。PEP 设备从多个来源获悉每个 AR 的身份属性，例如终端代理、授权服务器、对等实施设备和网络流量。反过来，PEP 设备使用 SXP 将 IP-SGT 映射传送到网络上相互信任的对等设备。

  策略实施点包括多种网络设备，例如 Catalyst 交换机、路由器、防火墙（具体是指 ASA）、服务器、VPN 设备和 SAN 设备。

思科 ASA 在身份架构中为 PEP 角色提供服务。 ASA 采用 SXP 直接从身份验证点获悉身份信息，并利用这些信息实施基于身份的策略。

安全组策略实施

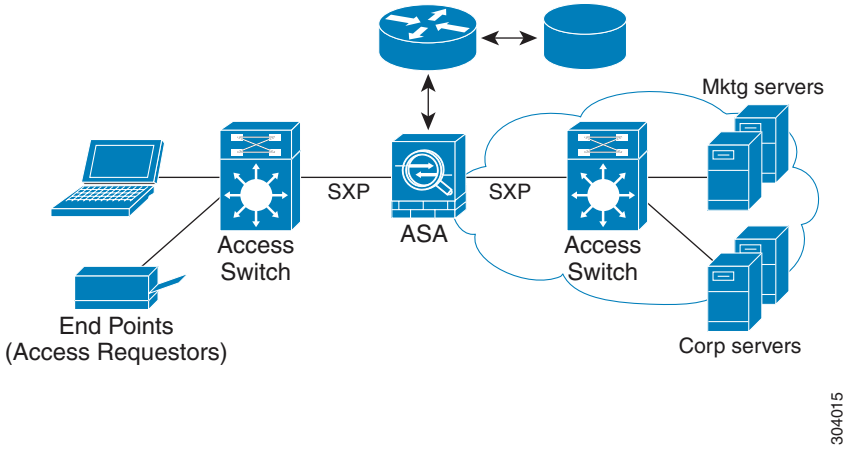
安全策略实施基于安全组名称进行。终端设备尝试访问数据中心中的资源。与在防火墙上配置的基于 IP 的传统策略相比，基于身份的策略基于用户和设备身份配置。例如，允许市场营销承包商访问市场营销服务器；允许市场营销公司用户访问市场营销服务器和公司服务器。

此类部署的优点包括：

- 使用单一对象 (SGT) 简化策略管理定义和实施用户组与资源。
- 在支持思科 TrustSec 的交换机基础设施中保留用户身份和资源身份。

图 32-1 显示了基于安全组名称的策略实施部署。

图 32-1　　基于安全组名称的策略实施部署



通过实施思科 TrustSec，您可以配置支持服务器分类的安全策略，并且实现以下功能：

- 可以将 SGT 分配给服务器池，以简化策略管理。
- SGT 信息保留在支持思科 TrustSec 的交换机的基础设施中。
- ASA 可以使用 IP-SGT 映射，在思科 TrustSec 域上实施策略。
- 服务器强制要求 802.1x 授权，由此可能简化部署。

ASA 如何实施基于安全组的策略

注　ASA 上同时允许基于用户的安全策略和基于安全组的策略。网络属性、基于用户的属性和基于安全组的属性的任意组合都能够在安全策略中配置。有关配置基于用户的安全策略的详细信息，请参阅第 31 章，“身份防火墙”。

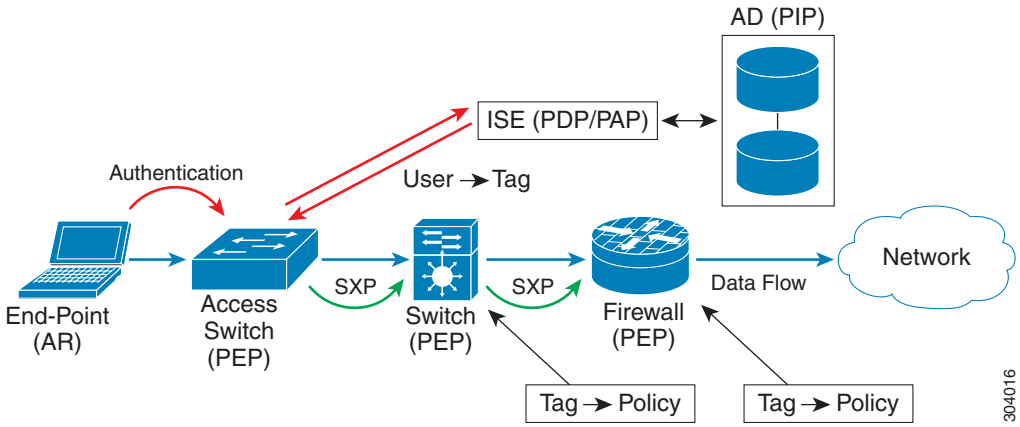
如要配置 ASA 与思科 TrustSec 配合使用，您必须从 ISE 导入受保护访问凭证 (PAC) 文件。有关详细信息，请参阅第 32-14 页的导入 PAC 文件。

将 PAC 文件导入 ASA，在 ASA 与 ISE 之间建立安全的通信信道。信道建立之后，ASA 发起与 ISE 之间的 PAC 安全 RADIUS 事务，下载思科 TrustSec 环境数据（即安全组表）。此安全组表将 SGT 映射到安全组名称。安全组名称在 ISE 上创建，为安全组提供用户友好的名称。

首次下载安全组表时，ASA 会浏览表中的所有条目，解析已在 ASA 上配置的安全策略包含的所有安全组名称；然后，ASA 在本地激活这些安全策略。如果无法解析安全组名称，ASA 会为未知安全组名称生成一条系统日志消息。

图 32-2 显示如何在思科 TrustSec 中实施安全策略。

图 32-2　　安全策略实施



1. 终端设备直接或通过远程访问连接到接入层设备，并使用思科 TrustSec 进行身份验证。
2. 通过使用 802.1X 或网络身份验证等身份验证方法，接入层设备可以利用 ISE 对终端设备进行身份验证。终端设备传送角色和组成员信息，将此设备划分至相应的安全组。
3. 接入层设备使用 SXP，将 IP-SGT 映射传送到上游设备。
4. ASA 接收数据包，并利用 SXP 传送的 IP -SGT 映射在 SGT 中查找源 IP 地址和目标 IP 地址。

   如果映射是新映射，ASA 则将其记录在本地 IP-SGT 管理器数据库中。IP-SGT 管理器数据库在控制层面中运行，为每个 IPv4 或 IPv6 地址跟踪 IP-SGT 映射。此数据库记录映射被获悉的源。SXP 连接的对等 IP 地址可用作映射源。每个 IP-SGT 映射条目都可以有多个源。

   如果 ASA 被配置为 Speaker，ASA 则将所有 IP-SGT 映射条目传输到其 SXP 对等体。有关详细信息，请参阅第 32-6 页的关于 ASA 上的 Speaker 和 Listener 角色。
5. 如果在 ASA 上使用此 SGT 或安全组名称配置安全策略，ASA 则实施此策略。（您可以在 ASA 上创建包含 SGT 或安全组名称的安全策略。为了基于安全组名称实施策略，ASA 需要一个安全组表，以将安全组名称映射到 SGT。）

   如果 ASA 在安全组表中找不到安全组名称，并且安全组名称包含在安全策略中，ASA 则认为此安全组名未知，并生成一条系统日志消息。在 ASA 刷新来自 ISE 的安全组表并获悉安全组名称之后，ASA 会生成一条系统日志消息，指明安全组名称已知。

安全组更改对 ISE 产生的影响

通过从 ISE 下载更新的表，ASA 定期刷新安全组表。在不同的下载之间，ISE 上的安全组会发生更改。直到 ASA 刷新安全组表，这些更改才会在 ASA 上体现出来。

提示　我们建议您在维护窗口期间安排 ISE 上的策略配置更改，然后在 ASA 上手动刷新安全组表，确保安全组更改包含在内。

按这种方式处理策略配置更改，可以最大限度增加安全组名称获得解析和安全策略立即进入活动状态的几率。

当环境数据计时器过期时，系统会自动刷新安全组表。您也可以按需触发安全组表刷新。

如果安全组在 ISE 上发生更改，当 ASA 刷新安全组表时，会发生以下事件：

- 只有使用安全组名称配置的安全组策略才需要通过安全组表进行解析。包含策略组标记的策略始终处于活动状态。
- 当安全组表首次可用时，浏览所有包含安全组名称的策略，解析安全组名称，激活策略。浏览所有包含标记的策略，并为未知标记生成系统日志。
- 如果安全组表已过期，将继续根据最新下载的安全组表实施策略，直到您清楚此表有新表变得可用为止。
- 当解析的安全组名称在 ASA 上变成未知时，它会停用安全策略；然而，此安全策略依然存在于 ASA 运行配置中。
- 如果在 PAP 上删除某个现有安全组，以前已知的安全组标记会变成未知，但在 ASA 上不会发生策略状态更改。以前已知的安全组名称会变成未解析，然后策略被停用。如果安全组名称被重用，则使用新标记重新编译策略。
- 如果在 PAP 上添加新安全组，以前未知的安全组标记会变成已知，会生成系统日志消息，但策略状态不会发生更改。以前未知的安全组名称变成已解析，然后相关联的策略被激活。
- 如果已在 PAP 上重命名标记，使用标记配置的策略会显示新的标记名称，策略状态不会发生更改。使用此新标记值重新编译使用安全组名称配置的策略。

关于 ASA 上的 Speaker 和 Listener 角色

ASA 支持 SXP 向其他网络设备发送和从这些设备接收 IP-SGT 映射条目。SXP 允许安全设备和防火墙从访问交换机获悉身份信息，无需硬件升级或更改。 SXP 还能够用来将上游设备 （例如，数据中心设备）的 IP-SGT 映射条目重新传送到下游设备。 ASA 能够接收来自上游和下游方向的信息。

当在 ASA 上配置到 SXP 对等体的 SXP 连接时，您必须将 ASA 指定为此连接的说话者或收听者，以便它能够交换身份信息：

- 说话者模式 - 配置 ASA，以便它能够将在 ASA 上收集的所有活动 IP-SGT 映射条目转发给上游设备，进行策略实施。
- 收听者模式 - 配置 ASA，以便可以从下游设备 （具备 SGT 功能的交换机）接收 IP-SGT 映射条目，并使用这些信息创建策略定义。

如果将 SXP 连接的一端配置为说话者，必须将另一端配置为 收听者，反之亦然。如果 SXP 连接的两端设备都配置同一角色（说话者或收听者），SXP 连接将失败，同时ASA 将生成一条系统日志消息。

多个 SXP 连接能够获悉已从 IP-SGT 映射数据库下载的 IP-SGT 映射条目。在 ASA 上建立到 SXP 对等体的 SXP 连接后，收听者从说话者下载整个 IP-SGT 映射数据库。此后发生的所有更改仅在网络上出现新设备时被发送。因此，SXP 信息流速率与终端主机对网络进行身份验证的速率成比例。

已通过 SXP 连接获悉的 IP-SGT 映射条目在 SXP IP-SGT 映射数据库中进行维护。可以通过不同 SXP 连接获悉相同映射条目。此映射数据库为每个已获悉的映射条目维护一个副本。同一 IP-SGT 映射值的多个映射条目按获悉映射的连接的对等 IP 地址进行识别。SXP 请求 IP-SGT 管理器在首次获悉新映射时添加映射条目，并在移除 SXP 数据库中的最后副本时移除映射条目。

无论 SXP 连接何时被配置为说话者，SXP 都请求 IP-SGT 管理器将在设备上收集的所有映射条目转发给对等体。当在本地获悉新映射时，IP-SGT 管理器请求 SXP 通过已配置为说话者的连接转发此映射。

将 ASA 配置为 SXP 连接的说话者和收听者会形成 SXP 环路，这意味着，SXP 数据能够被最初传输它的 SXP 对等体接收。

SXP 通信速率

SXP 信息流速率与终端主机对网络进行身份验证的速率成比例。建立 SXP 对等之后，收听者设备从说话者设备下载整个 IP-SGT 数据库。之后，所有更改仅在新设备出现在网络中或者离开网络时被增量发送。另请注意，只有挂接到新设备的访问设备才能对上游设备发起这种增量更新。

换句话说，SXP 协议的通信速率不会高于受限于身份验证服务器能力的身份验证速率。因此，SXP 通信速率不是主要问题。

SXP 计时器

- 重试打开计时器 - 如果设备上有一个 SXP 连接未建立，则触发重试打开计时器。在重试打开计时器过期后，设备浏览整个连接数据库，如果有任何连接处于关闭或“待定”状态，重试打开计时器将重新启动。计时器默认值为 120 秒。 0 值意味着重试计时器不会启动。重试打开计时器继续，直到所有 SXP 连接都建立或重试打开计时器值已被设为 0 为止。
- 删除抑制计时器 - 当收听者上的某个连接被中断时，触发连接特定删除抑制计时器。已获悉的映射条目不会被立即删除，而是一直保留到删除抑制计时器过期。此计时器过期后，这些映射条目将被删除。删除抑制计时器的值被设为 120 秒，该值不可配置。
- 协调计时器 - 如果在删除抑制计时器期间建立 SXP 连接，则对此连接实施批量更新。这意味着，最新映射条目已被获悉，并且被关联到新的连接实例化标识符。定期的连接特定协调计时器在后台启动。当此协调计时器过期时，它将扫描整个 SXP 映射数据库，识别当前连接会话中所有未被获悉的映射条目 （即带有不匹配连接实例化标识符的映射条目），并对这些条目进行标记，以便将它们删除。这些条目在后续协调审核中被删除。协调计时器默认值为 120 秒。 ASA 上不允许设为 0 值，以防止过时条目的停留时间超出指定范围，给策略实施造成意外结果。
- HA 协调计时器 - 启用 HA 时，主用和备用装置的 SXP 映射数据库保持同步。新的主用装置尝试建立到其所有对等体的新 SXP 连接，并获取最新映射条目。HA 协调计时器可以提供一种识别和移除旧映射条目的方法。该计时器在故障转移后启动，使 ASA 有时间获取最新映射条目。在 HA 协调计时器过期后，ASA 将扫描整个 SXP映射数据库，识别当前连接会话中所有未被获悉的映射条目。标记有不匹配实例化标识符的映射条目以便删除。此协调机制与协调计时器的协调机制相同。时间值与协调计时器的时间值相同，并且可配置。

在 SXP 对等体终止其 SXP 连接后，ASA 启动删除抑制计时器。只有被指定为收听者的 SXP 对等体才能够终止连接。如果 SXP 对等体在删除抑制计时器运行期间连接，ASA 将启动协调计时器；然后，ASA 更新 IP-SGT 映射数据库，以获悉最新映射。

IP-SGT 管理器数据库

IP-SGT 管理器数据库不会将任何条目从主用装置同步到备用装置。 IP-SGT 管理器数据库接收 IP-SGT 映射条目的每个源都会将其数据库从主用装置同步到备用装置，然后向备用装置上的 IP-SGT 管理器提供最终 IP-SGT 映射。

对于 9.0(1) 版本，IP-SGT 管理器数据库仅从 SXP 源接收 IP-SGT 映射更新。

ASA-思科 TrustSec 集成的功能

ASA 将思科 TrustSec 作为其基于身份的防火墙功能的一部分。思科 TrustSec 可以提供以下功能：

灵活性

- ASA 可被配置为 SXP 说话者或收听者，或两者。
- ASA 支持将 SXP 用于 IPv6 和支持 IPv6 的网络设备。
- SXP 能够为 IPv4 和 IPv6 地址更改映射条目。
- SXP 终端支持 IPv4 和 IPv6 地址。
- ASA 仅支持 SXP 第 2 版本。
- ASA 可以与支持 SXP 的不同网络设备协商 SXP 版本。 SXP 版本协商消除了对静态版本配置的需求。
- 您可以配置 ASA，使其在 SXP 协调计时器过期时刷新安全组表，您也可以按需下载安全组表。从 ISE 更新 ASA 上的安全组表时，更改将在相应的安全策略中体现出来。
- ASA 根据源字段或目标字段或两者中的安全组名称支持安全策略。您可以根据安全组、 IP 地址、 Active Directory 组/用户名和 FQDN 构成的组合，在 ASA 上配置安全策略。

可用性

- 在 ASA 上，您可以在主用/主用和主用/备用配置中配置基于安全组的策略。
- ASA 可以与专为实现高可用性 (HA) 配置的 ISE 进行通信。
- 您可以在 ASA 上配置多台 ISE 服务器，如果第一台服务器无法访问，它将继续访问第二台服务器，以此类推。然而，如果服务器列表被下载为思科 TrustSec 环境数据的一部分，它将被忽略。
- 如果 ASA 上从 ISE 下载的 PAC 文件过期，并且它无法下载更新的安全组表，ASA 将继续根据最后下载的安全组表实施安全策略，直到ASA 下载更新的安全组表为止。

集群

- 对于第 2 层网络，所有装置共享同一 IP 地址。当您更改接口地址时，更改的配置将被发送到所有其他装置。当 IP 地址从特定装置的接口更新时，系统会发送一份通知，以更新此装置上的 IP-SGT 本地数据库。
- 对于第 3 层网络，为主装置上的每个接口配置地址池，并将此配置同步到从装置。在主装置上，发送表示 IP 地址已分配给接口的通知，并且更新 IP-SGT 本地数据库。通过利用已同步到从装置的地址池配置 （池中每个接口的第一个地址始终属于主装置），每个从装置上的 IP-SGT 数据库可以使用主装置的 IP 地址来更新。

  当从装置启动时，它会通知主装置。然后，主装置浏览每个接口上的地址池，为向其发送通知的新从装置计算 IP 地址，并更新主装置上的 IP-SGT 本地数据库。此外，主装置还将有关新从装置的信息通知其他从装置。在通知处理过程中，每个从装置都会为新从装置计算 IP 地址，并将此条目添加到每个从装置上的 IP-SGT 本地数据库。所有从装置都具有地址池配置，以此确定 IP 地址值。对于每个接口，按以下方法确定值：

  Master IP + (M-N)，其中：

  M - 最大装置数量 （最多允许 8 个）

  N - 发送通知的从装置号

  当任何接口上的 IP 地址池发生更改时，需要在主装置以及每个其他从装置上的 IP-SGT 本地数据库中重新计算和更新所有从装置和主装置的 IP 地址。需要删除旧 IP 地址，并添加新 IP 地址。

当发生更改的地址池配置被同步到从装置时，在配置更改处理过程中，每个从装置为主装置和每个其他 IP 地址已更改的从装置重新计算 IP 地址，然后删除旧 IP 地址的条目，并添加新 IP 地址。

可扩展性

表 32-1 显示 ASA 支持的 IP-SGT 映射条目数。

表 32-1　IP-SGT 映射条目的容量数

ASA 型号	IP-SGT 映射条目数
带 SSP-10 的 5585-X	18,750
带 SSP-20 的 5585-X	25,000
带 SSP-40 的 5585-X	50,000
带 SSP-60 的 5585-X	100,000

表 32-2 显示 ASA 支持的 SXP 连接数。

表 32-2　SXP 连接

ASA 型号	SXP TCP 连接数
带 SSP-10 的 5585-X	150
带 SSP-20 的 5585-X	250
带 SSP-40 的 5585-X	500
带 SSP-60 的 5585-X	1000

思科 TrustSec 的许可要求

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

使用思科 TrustSec 的先决条件

配置 ASA 使用思科 TrustSec 之前，您必须执行以下任务：

- 第 32-10 页的通过 ISE 注册 ASA
- 第 32-10 页的在 ISE 上创建安全组
- 第 32-10 页的生成 PAC 文件

通过 ISE 注册 ASA

在 ASA 能够成功导入 PAC 文件之前，您必须将 ASA 配置为 ISE 中可识别的思科 TrustSec 网络设备。如要通过 ISE 注册 ASA，请执行以下步骤：

1. 登录 ISE。
2. 选择 **Administration > Network Devices > Network Devices**。
3. 点击 **Add**。
4. 输入 ASA 的 IP 地址。
5. 当 ISE 被用于进行用户身份验证时，请在 Authentication Settings 区域输入一个共享密钥。

   在 ASA 上配置 AAA 服务器时，请提供您在 ISE 上创建的共享密钥。 ASA 上的 AAA 服务器使用此共享密钥与 ISE 进行通信。
6. 指定 ASA 的设备名、设备 ID、密码和下载时间间隔。有关如何执行这些任务的详细信息，请参阅 ISE 文档。

在 ISE 上创建安全组

配置 ASA 与 ISE 进行通信时，您需指定 AAA 服务器。在 ASA 上配置 AAA 服务器时，您必须指定服务器组。必须配置安全组，使其使用 RADIUS 协议。如要在 ISE 上创建安全组，请执行以下步骤：

1. 登录 ISE。
2. 选择 **Policy > Policy Elements > Results > Security Group Access > Security Group**。
3. 为 ASA 添加安全组。（安全组是全局性的，而非特定于 ASA。）

   ISE 在 Security Groups 下创建带有标记的条目。
4. 在 Security Group Access 区域，为 ASA 配置设备 ID 凭证和密码。

生成 PAC 文件

生成 PAC 文件之前，您必须已通过 ISE 注册 ASA。如要生成 PAC 文件，请执行以下步骤：

1. 登录 ISE。
2. 选择 **Administration > Network Resources > Network Devices**。
3. 从设备列表中，选择 ASA。
4. 在 Security Group Access (SGA) 下方，点击 **Generate PAC**。
5. 如要加密 PAC 文件，请输入密码。

   为加密 PAC 文件而输入的密码（或加密密钥）独立于在 ISE 上被配置为设备凭证的一部分的密码。

ISE 生成 PAC 文件。ASA 能够通过 TFTP、FTP、HTTP、HTTPS 或 SMB，从闪存或远程服务器导入 PAC 文件。（导入之前，PAC 文件不必驻留在 ASA 闪存上。）

有关 PAC 文件的详细信息，请参阅第 32-14 页的导入 PAC 文件。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

IPv6 准则

支持 IPv6 用于 SXP 终端。

集群准则

支持集群环境中的主装置和从装置。

故障转移准则

通过配置支持服务器列表。如果第一台服务器无法访问，ASA 则尝试连接列表中的第二台服务器，以此类推。然而，被下载为思科 TrustSec 环境数据的一部分的服务器列表将被忽略。

支持主用/备用和主用/主用情境。接管之后，所有 SXP 数据将被从主用装置复制到备用装置。

其他指导原则

思科 TrustSec 在单一情景和多情景模式中支持智能报障服务功能，但在系统情景模式中不支持此功能。

限制

- ASA 只能配置为在单一思科 TrustSec 域中进行互操作。
- ASA 不支持设备上的静态 SGT 名称映射配置。
- SXP 消息不支持 NAT。
- SXP 在网络中将 IP-SGT 映射传送到实施点。如果接入层交换机与实施点分属不同的 NAT 域，它上传的 IP-SGT 映射则无效，而且在实施设备上进行的 IP-SGT 映射数据库查找不会显示有效的结果。因此，ASA 无法在实施设备上应用安全组感知安全策略。
- 您可以为 ASA 配置用于 SXP 连接的默认密码，或者选择不使用密码；然而，不支持将连接特定密码用于 SXP 对等体。配置的默认 SXP 密码应当在部署网络中保持一致。如果配置连接特定密码，连接可能会失败，并且显示警告消息。如果使用默认密码配置连接，但未配置默认密码，则结果与不使用密码配置连接时的结果相同。
- 当设备拥有到对等体的双向连接，或者设备是单向连接设备链的一部分时，会形成 SXP 连接环路。（ASA 可以从数据中心的接入层为资源获悉 IP-SGT 映射。 ASA 可能需要将这些标记传送到下游设备。）SXP 连接环路会导致 SXP 消息传输出现意外行为。在 ASA 配置为说话者和收听者的情况下，会发生 SXP 连接回路，使 SXP 数据会被最初传输它的对等体接收。
- 更改 ASA 本地 IP 地址时，您必须确保所有 SXP 对等体已更新其对等体列表。此外，如果 SXP 对等体更改其 IP 地址，您必须确保这些更改在 ASA 上体现出来。
- 不支持自动 PAC 文件配置。 ASA 管理员必须从 ISE 管理界面请求 PAC 文件，并将其导入 ASA。有关 PAC 文件的详细信息，请参阅第 32-10 页的生成 PAC 文件和第 32-14 页的导入 PAC 文件。
- PAC 文件有过期日期。您必须在当前 PAC 文件过期之前导入更新的 PAC 文件；否则，ASA 将无法检索环境数据更新。

- 当安全组在 ISE 上发生更改（例如，被重命名或删除）时，ASA 不会更改任何包含与已更改安全组相关联的 SGT 或安全组名称的 ASA 安全组策略的状态；然而，ASA 会生成系统日志消息，指明这些安全策略已更改。

  请参阅，有关在 ASA 上手动更新安全组表以包含来自 ISE 的更改的详细信息，请参阅第 32-18 页的刷新环境数据。
- 在 ISE 1.0 中不支持组播类型。
- SXP 连接在两个被 ASA 互联的 SXP 对等体之间保持正在初始化状态，如以下示例所示。

  （SXP 对等体 A）- - - - (ASA) - - - （SXP 对等体 B）

  因此，当配置 ASA 与思科 TrustSec 集成时，您必须在 ASA 上启用 no-NAT、no-SEQ-RAND 和 MD5-AUTHENTICATION TCP 选项，配置 SXP 连接。为 SXP 对等体之间以 SXP 端口 TCP 64999 为目标的流量创建 TCP 状态旁路策略。然后，在相应的接口上应用该策略。

  例如，以下命令集显示如何为 TCP 状态旁路策略配置 ASA：

```
access-list SXP-MD5-ACL extended permit tcp h 支持路由和透明防火墙模式。 ost peerA host
peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

- ASA 5585-X 的硬件架构专门用于以最佳方式加载平衡正则数据包，但采用第 2 层安全组标记实施的内联已标记数据包例外。当 ASA 5585-X 处理传入的内联已标记数据包时，可能会出现明显的性能降级。其他 ASA 平台上的内联已标记数据包以及 ASA 5585-X 上的未标记数据包不会出现这种问题。一种解决方法是卸载访问策略，最大限度地减少进入 ASA 5585-X 的内联已标记数据包，允许交换机处理已标记策略实施。另一种解决方法是使用 SXP，使 ASA 5585-X 能够将 IP 地址映射到安全组标记，无需接收已标记数据包。
- ASASM 不支持第 2 层安全组标记实施。

为思科 TrustSec 集成配置 ASA

- 第 32-13 页的为思科 TrustSec 集成配置 AAA 服务器
- 第 32-14 页的导入 PAC 文件
- 第 32-16 页的配置安全交换协议
- 第 32-18 页的添加 SXP 连接对等体
- 第 32-18 页的刷新环境数据
- 第 32-19 页的配置安全策略
- 第 32-20 页的配置第 2 层安全组标记实施

- 第 32-22 页的启用 SGT plus Ethernet Tagging
- 第 32-23 页的在接口上传送安全组标记
- 第 32-23 页的将策略应用到手动配置的思科 TrustSec 链路
- 第 32-24 页的手动配置 IP-SGT 绑定

为思科 TrustSec 集成配置 AAA 服务器

在配置 ASA 集成思科 TrustSec 的过程中，您必须配置 ASA，使其能够与 ISE 进行通信。

先决条件

- 必须配置参考服务器组，使其使用 RADIUS 协议。如果您将非 RADIUS 服务器组添加到 ASA，配置将失败。
- 如果 ISE 也用于进行用户身份验证，则获取您在通过 ISE 注册 ASA 时在 ISE 上输入的共享密钥。请联系 ISE 管理员，以获取此信息。

如要在 ASA 上为 ISE 配置 AAA 服务器组，请执行以下步骤：

	命令	用途
步骤 1	`ciscoasa(config)# aaa-server server-tag protocol radius` **示例：** `ciscoasa(config)# aaa-server ISEserver protocol radius`	创建 AAA 服务器组并配置 AAA 服务器参数，以便 ASA 与 ISE 服务器进行通信。 *server-tag* specifies the server group name. 有关详细信息，请参阅第 32-10 页的在 ISE 上创建安全组。
步骤 2	`ciscoasa(config-aaa-server-group)# exit`	从 aaa 服务器组配置模式中退出。
步骤 3	`ciscoasa(config)# aaa-server server-tag (interface-name) host server-ip` **示例：** `ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1`	将 AAA 服务器配置为 AAA 服务器组的一部分，设置主机特定连接数据。 *interface-name* 指定 ISE 服务器驻留的网络接口。需要在此参数中使用圆括号。 *server-tag* 为 AAA 服务器组的名称。 *server-ip* 指定 ISE 服务器的 IP 地址。
步骤 4	`ciscoasa(config-aaa-server-host)# key key` **示例：** `ciscoasa(config-aaa-server-host)# key myexclusivemumblekey`	指定用于通过 ISE 服务器对 ASA 进行身份验证的服务器密钥值。 *key* 为一个字母数字关键字，最大长度为 127 个字符。 如果 ISE 也用于进行用户身份验证，则输入您在通过 ISE 注册 ASA 时在 ISE 上输入的共享密钥。 有关详细信息，请参阅第 32-10 页的通过 ISE 注册 ASA。
步骤 5	`ciscoasa(config-aaa-server-host)# exit`	从 aaa 服务器主机配置模式中退出。
步骤 6	`ciscoasa(config)# cts server-group AAA-server-group-name` **示例：** `ciscoasa(config)# cts server-group ISEserver`	识别被思科 TrustSec 用于环境数据检索的 AAA 服务器组。 *AAA-server-group-name* 为您在第 1 步在参数 *server-tag* 中指定的 AAA 服务器组名称。 在 ASA 上，只能为思科 TrustSec 配置一个服务器组实例。

示例

以下示例显示如何为思科 TrustSec 集成配置 ASA 与 ISE 服务器进行通信：

```
ciscoasa(config)# aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

导入 PAC 文件

将受保护的访问凭证 (PAC) 文件导入 ASA，与 ISE 建立连接。信道建立之后，ASA 发起与 ISE 之间的安全 RADIUS 事务，下载思科 TrustSec 环境数据 （即安全组表）。此安全组表将 SGT 映射到安全组名称。安全组名称在 ISE 上创建，为安全组提供用户友好的名称。

更具体地说，在 RADIUS 事务之前没有建立信道。 ASA 使用 PAC 文件进行身份验证，通过 ISE 发起 RADIUS 事务。

提示　PAC 文件包含一个共享密钥，允许 ASA 和 ISE 保证它们之间的 RADIUS 事务安全可靠。考虑到此密钥的敏感性质，您必须将其安全地存储在 ASA 上。

成功导入此文件后，ASA 从 ISE 下载思科 TrustSec 环境数据，无需在 ISE 中配置的设备密码。

先决条件

- 在 ASA 能够成功生成 PAC 文件之前，您必须将 ASA 配置为 ISE 中可识别的思科 TrustSec 网络设备。虽然 ASA 能够导入任何 PAC 文件，但 PAC 文件只在被正确配置的 ISE 生成时才能在 ASA 上运行。有关详细信息，请参阅第 32-10 页的通过 ISE 注册 ASA。
- 在 ISE 上生成 PAC 文件时，请获取用于加密此文件的密码。

  ASA 要求此密码，以导入并解密 PAC 文件。
- 访问 ISE 生成的 PAC 文件。ASA 能够通过 TFTP、FTP、HTTP、HTTPS 或 SMB，从闪存或远程服务器导入 PAC 文件。（导入之前，PAC 文件不必驻留在 ASA 闪存上。）
- 已为 ASA 配置了服务器组。

限制

- 当 ASA 成为故障转移配置的一部分时，您必须将 PAC 文件导入主 ASA 设备。
- 当 ASA 成为集群配置的一部分时，您必须将 PAC 文件导入主设备。

如要导入 PAC 文件，请输入以下命令：

命令	用途
ciscoasaciscoasa(config)# **cts import-pac** *filepath* **password** *value* **示例：** ciscoasaciscoasa(config)# cts import-pac disk0:/xyz.pac password IDFW-pac99	将导入思科 TrustSec PAC 文件。 *filepath* 作为以下执行模式命令和选项之一被输入： **单一模式** • **disk0**：disk0 上的路径和文件名 • **disk1**：disk1 上的路径和文件名 • **flash**：闪存上的路径和文件名 • **ftp**：FTP 上的路径和文件名 • **http**：HTTP 上的路径和文件名 • **https**：HTTPS 上的路径和文件名 • **smb**：SMB 上的路径和文件名 • **tftp**：TFTP 上的路径和文件名 **多模式** • **http**：HTTP 上的路径和文件名 • **https**：HTTPS 上的路径和文件名 • **smb**：SMB 上的路径和文件名 • **tftp**：TFTP 上的路径和文件名 *value* 指定用于加密 PAC 文件的密码。此密码独立于在 ISE 上配置为设备凭证的一部分的密码。

示例

以下示例显示如何将 PAC 文件导入 ASA：

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC 文件已成功导入
```

以下示例显示如何使用终端将 PAC 文件导入 ASA：

```
ciscoasa(config)# cts import-pac terminal password A9875Za551
以 ASCII 十六进制格式输入 PAC 文件数据
以单词 "quit" 结尾，并独占一行。
ciscoasa(exec_pac_hex)# 0100290405000001000000000000000
ciscoasa(exec_pac_hex)# 00000000000000001111111111111111
ciscoasa(exec_pac_hex)# 11111111111111112222222222222222
ciscoasa(exec_pac_hex)# 222222222222222276d7d64b6be4804b
ciscoasa(exec_pac_hex)# 0b4fdca3aeee11950ecd0e47c34157e5
ciscoasa(exec_pac_hex)# 25f4964ed75835cde0adb7e198e0bcdb
ciscoasa(exec_pac_hex)# 6aa8e363b0e4f9b4ac241be9ab576d0b
ciscoasa(exec_pac_hex)# a1fcd34e5dd05dbe1312cbfea072fdb9
ciscoasa(exec_pac_hex)# ee356fb61fe987d2d8f0ac3ef0467627
ciscoasa(exec_pac_hex)# 7f8b137da2b840e16da520468b039bae
ciscoasa(exec_pac_hex)# 36a4d844acc85cdefd7cb2cc58787590
ciscoasa(exec_pac_hex)# ef123882a69b6c37bdbc9320e403024f
ciscoasa(exec_pac_hex)# 354d42f404ec2d67ef3606575014584b
ciscoasa(exec_pac_hex)# 2796e65ccd6e6c8d14d92448a8b24f6e
ciscoasa(exec_pac_hex)# 47015a21f4f66cf6129d352bdfd4520f
```

```
ciscoasa(exec_pac_hex)# 3f0c6f340a80715df4498956efe15dec
ciscoasa(exec_pac_hex)# c08bb9a58cb6cb83ac91a3c40ce61de0
ciscoasa(exec_pac_hex)# 284b743e52fd68e848685e2d78c33633
ciscoasa(exec_pac_hex)# f2b4c5824138fc7bac9d9b83ac58ff9f
ciscoasa(exec_pac_hex)# 1dbc84c416322f1f3c5951cf2132994a
ciscoasa(exec_pac_hex)# a7cf20409df1d0d6621eba2b3af83252
ciscoasa(exec_pac_hex)# 70d0130650122bdb13a83b2dae55533a
ciscoasa(exec_pac_hex)# 4a394f21b441e164
ciscoasa(exec_pac_hex)# quit
PAC 已成功导入
ciscoasa(config)#
```

配置安全交换协议

配置安全交换协议 (SXP) 包括在 ASA 中启用此协议，并为 SXP 设置以下默认值：

- SXP 连接的源 IP 地址
- SXP 对等体之间的身份验证密码
- SXP 连接的重试间隔
- 思科 TrustSec SXP 协调期

注　如要让 SXP 在 ASA 上运行，至少要有一个接口处于 UP/UP 状态。

目前，当 SXP 已启用且所有接口都关闭时，ASA 不会显示一条指明 SXP 未工作或无法启用的消息。如果您通过输入 **show running-config** 命令来检查配置，此命令输出则显示以下消息：

```
"WARNING: SXP configuration in process, please wait for a few moments and try again."
```

此消息是通用的，不会指出 SXP 不运行的原因。

如要配置 SXP，请执行以下步骤：

	命令	用途
步骤 1	`ciscoasa(config)# cts sxp enable`	如有必要，在 ASA 上启用 SXP。默认情况下，SXP 被禁用。 在多情景模式中，在用户情景中启用 SXP。
步骤 2	`ciscoasa(config)# cts sxp default source-ip` *ipaddress* **示例：** `ciscoasa(config)# cts sxp default source-ip 192.168.1.100`	为 SXP 连接配置默认源 IP 地址。 *ipaddress* 为一个 IPv4 或 IPv6 地址。 为 SXP 连接配置默认源 IP 地址时，您必须将同一地址指定为 ASA 出站接口。如果源 IP 地址不匹配出站接口的地址，SXP 连接将失败。 在不为 SXP 连接配置源 IP 地址的情况下，ASA 会执行路由/ARP 查询，以确定 SXP 连接的出站接口。有关详细信息，请参阅第 32-18 页的添加 SXP 连接对等体。

	命令	用途
步骤 3	ciscoasa(config)# **cts sxp default password** [**0** | **8**] *password* **示例：** ciscoasa(config)# cts sxp default password 8 IDFW-TrustSec-99	配置用于对 SXP 对等体进行 TCP MD5 身份验证的默认密码。默认情况下，不为 SXP 连接设置密码。 配置密码的加密级别为可选操作。如果配置加密级别，您只能设置一个级别： • Level 0 - 未加密纯文本 • Level 8 - 已加密文本 *password* 指定一个最多 162 个字符的加密字符串，或者最多 80 个字符的 ASCII 密钥字符串。
步骤 4	ciscoasa(config)# **cts sxp retry period** *timervalue* **示例：** ciscoasa(config)# cts sxp retry period 60	指定 ASA 尝试在 SXP 对等体之间建立新 SXP 连接的默认时间间隔。ASA 继续尝试连接，直到连接成功为止。只要 ASA 上有一个未建立的 SXP 连接，就会触发重试计时器。 *timervalue* 的范围为 0 至 64000 秒。默认情况下，*timervalue*为 120 秒。 如果指定为 0 秒，该计时器永远不会过期，ASA 也不会尝试连接 SXP 对等体。 当重试计时器过期时，ASA 会浏览连接数据库，如果数据库包含任何已关闭或处于“待处理”状态的连接，ASA 会重新启动重试计时器。 我们建议您将重试计时器配置为不同于其 SXP 对等体的值。
步骤 5	ciscoasa(config)# **cts sxp reconciliation period** *timervalue* **示例：** ciscoasa(config)# cts sxp reconciliation period 60	指定默认协调计时器的值。在 SXP 对等体终止其 SXP 连接后， ASA 启动抑制计时器。 如果 SXP 对等体在抑制计时器运行期间连接，ASA 将启动协调计时器；然后，ASA 更新 SXP 映射数据库，以获悉最新映射。 当协调计时器过期时，ASA 将扫描 SXP 映射数据库，以识别旧映射条目（在上一连接会话中获悉的条目）。ASA 将这些连接标记为过时条目。当协调计时器过期时，ASA 从 SXP 映射数据库移除这些过时条目。 *timervalue* 的范围为 1 至 64000 秒。默认情况下，*timervalue*为 120 秒。 您无法将协调计时器值指定为 0 秒，因为该值会阻止计时器启动。不允许协调计时器运行的话，会使旧条目保留时间不确定，导致策略实施出现意外结果。

示例

以下示例显示如何为 SXP 设置默认值：

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

添加 SXP 连接对等体

对等体间的 SXP 连接为点到点的连接，使用 TCP 作为底层传输协议。

如要添加 SXP 连接对等体，请执行以下步骤：

	命令	用途
步骤 1	`ciscoasa(config)# cts sxp enable`	如有必要，在 ASA 上启用 SXP。默认情况下，SXP 被禁用。
步骤 2	`ciscoasa(config)# cts sxp connection peer peer_ip_address [source source_ip_address] password {default | none} [mode {local | peer}] {speaker | listener}` **示例：** `ciscoasaciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker`	建立到 SXP 对等体的 SXP 连接。SXP 连接按 IP 地址设置；单一设备对能够服务多个 SXP 连接。 *peer_ip_address* 为 SXP 对等体的 IPv4 或 IPv6 地址。对等体 IP 地址必须可从 ASA 传出接口进行访问。 *source_ip_address* 为 SXP 连接的 IPv4 或 IPv6 地址。源 IP 地址必须与 ASA 出站接口的 IP 地址相同，否则，连接将失败。 我们建议您不要为 SXP 连接配置源 IP 地址，并允许 ASA 执行路由/ARP 查找，以确定 SXP 连接的源 IP 地址。 指定是否使用 SXP 连接的身份验证密钥： • **default** - 使用为 SXP 连接配置的默认密码。请参阅第 32-16 页的配置安全交换协议。 • **none** - 不使用 SXP 连接的密码。 指定 SXP 连接模式： • **local** - 使用本地 SXP 设备。 • **peer** - 使用对等 SXP 设备。 指定 ASAASA 用作 SXP 的说话者还是 收听者。请参阅第 32-6 页的关于 ASA 上的 Speaker 和 Listener 角色。 • **说话者** - ASAASA 可以将 IP-SGT 映射转发到上游设备。 • **收听者** - ASAASA 可以从下游设备接收 IP-SGT 映射。

示例

以下示例显示如何在 ASA 上配置 SXP 对等体：

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
ciscoasa(config)# cts sxp connection peer 192.168.1.101 password default mode peer
ciscoasa(config)# no cts sxp connection peer 192.168.1.100
ciscoasa(config)# cts sxp connection peer 192.168.1.100 source 192.168.1.1 password default mode peer speaker
ciscoasa(config)# no cts sxp connection peer 192.168.1.100 source 192.168.1.1 password default mode peer speaker
```

刷新环境数据

ASA 可以从 ISE 下载环境数据，其中包括安全组标记 (SGT) 名称表。当您在 ASA 上完成以下任务时，ASA 会自动刷新从 ISE 获取的环境数据。

- 配置 AAA 服务器与 ISE 进行通信。
- 从 ISE 导入 PAC 文件。

- 识别 ASA 将用于检索思科 TrustSec 环境数据的 AAA 服务器组。

通常，您无需手动刷新来自 ISE 的环境数据；然而，安全组会在 ISE 上发生更改。这些更改不会在 ASA 上体现出来，直到您刷新 ASA 安全组表中的数据，所以您需要刷新 ASA 上的数据，以确保在 ISE 上所做的任何安全组更改都能在 ASA 上体现出来。

提示　我们建议您在维护窗口期间在 ISE 上安排策略配置更改，并在 ASA 上安排手动刷新数据。按这种方式处理策略配置更改，可以最大限度增加安全组名称获得解析和安全策略在 ASA 上立即进入活动状态的几率。

先决条件

必须将 ASA 配置为 ISE 中可识别的思科 TrustSec 网络设备，而且 ASA 必须已成功导入 PAC 文件，确保对思科 TrustSec 所做的更改已应用到 ASA。

限制

- 当 ASA 成为 HA 配置的一部分时，您必须刷新主 ASA 设备上的环境数据。
- 当 ASA 成为集群配置的一部分时，您必须刷新主设备上的环境数据。

如要刷新环境数据，请输入以下命令

命令	用途
cts refresh environment-data **示例：** `ciscoasaciscoasa(config)# cts refresh environment-data`	刷新来自 ISE 的环境数据，将协调计时器重置为已配置的默认值。

配置安全策略

您可以将思科 TrustSec 策略纳入多项 ASA 功能中。任何使用扩展 ACL（除非在本章节被列为不支持）的功能都能够利用思科 TrustSec。现在，您可以将安全组参数添加到扩展 ACL 以及基于网络的传统参数中。

- 要配置扩展 ACL，请参阅防火墙配置指南。
- 要配置可在 ACL 中使用的安全组对象组，请参阅第 16-7 页的配置安全组对象组。

例如，访问规则通过网络信息允许或拒绝接口上的流量。通过思科 TrustSec，您可以根据安全组控制访问。例如，您可以为 sample_securitygroup1 10.0.0.0 255.0.0.0 创建访问规则，这意味着，安全组可以拥有 10.0.0.0/8 子网上的任何 IP 地址。

您可以根据安全组名称 （服务器、用户、非受管设备等等）、基于用户的属性和基于 IP 地址的传统对象 （IP 地址、 Active Directory 对象和 FQDN）构成的组合配置安全策略。安全组成员能够扩展到角色以外，将设备和位置属性包含在内，并且不受用户组成员约束。

示例

以下示例显示如何创建一个使用在本地定义的安全对象组的 ACL：

```
object-group security objgrp-it-admin
   security-group name it-admin-sg-name
   security-group tag 1
object-group security objgrp-hr-admin
```

```
   security-group name hr-admin-sg-name  // single sg_name
   group-object it-admin     // locally defined object-group as nested object
object-group security objgrp-hr-servers
    security-group name hr-servers-sg-name
object-group security objgrp-hr-network
    security-group tag 2
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
```

在上例中配置的 ACL 可以通过配置访问组或模块化策略框架来激活。

附加示例：

```
!match src hr-admin-sg-name from any network to dst host 172.23.59.53
    access-list idw-acl permit ip security-group name hr-admin-sg-name any host 172.23.59.53
!match src hr-admin-sg-name from host 10.1.1.1 to dst any
    access-list idfw-acl permit ip security-group name hr-admin-sg-name host 10.1.1.1 any
!match src tag 22 from any network to dst hr-servers-sg-name any network
    access-list idfw-acl permit ip security-group tag 22 any security-group name hr-servers-sg-name any
!match src user mary from any host to dst hr-servers-sg-name any network
    access-list idfw-acl permit ip user CSCO\mary any security-group name hr-servers-sg-name any
!match src objgrp-hr-admin from any network to dst objgrp-hr-servers any network
    access-list idfw-acl permit ip object-group-security objgrp-hr-admin any object-group-security
    objgrp-hr-servers any
!match src user Jack from objgrp-hr-network and ip subnet 10.1.1.0/24 to dst objgrp-hr-servers any network
    access-list idfw-acl permit ip user CSCO\Jack object-group-security objgrp-hr-network 10.1.1.0
    255.255.255.0 object-group-security objgrp-hr-servers any
!match src user Tom from security-group mktg any google.com
object network net-google
    fqdn google.com
    access-list sgacl permit ip sec name mktg any object net-google
! If user Tom or object_group security objgrp-hr-admin needs to be matched, multiple ACEs can be defined as
follows:
    access-list idfw-acl2 permit ip user CSCO\Tom 10.1.1.0 255.255.255.0 object-group-security
    objgrp-hr-servers any
    access-list idfw-acl2 permit ip object-group-security objgrp-hr-admin 10.1.1.0 255.255.255.0
    object-group-security objgrp-hr-servers any
```

配置第 2 层安全组标记实施

思科 TrustSec 可以对每个网络用户和资源进行识别和身份验证，并分配一个称为安全组标记 (SGT) 的 16 位数字。反过来，此标识符可以在网络跳段之间传送，允许任何中间设备 （例如 ASA、交换机和路由器）根据此身份标记实施策略。

SGT plus Ethernet Tagging，也称作第 2 层 SGT 实施，使 ASA 能够使用思科专有以太网帧 (EtherType 0x8909) 在以太网接口上发送和接收安全组标记，其允许将源安全组标记插入纯文本以太网帧。 ASA 可以根据手动每接口配置，在传出数据包上插入安全组标记并在传入数据包上处理安全组标记。此功能允许跨网络设备对终端身份进行内联逐跳传送，在每个跳段之间提供无缝的第 2 层 SGT 实施。

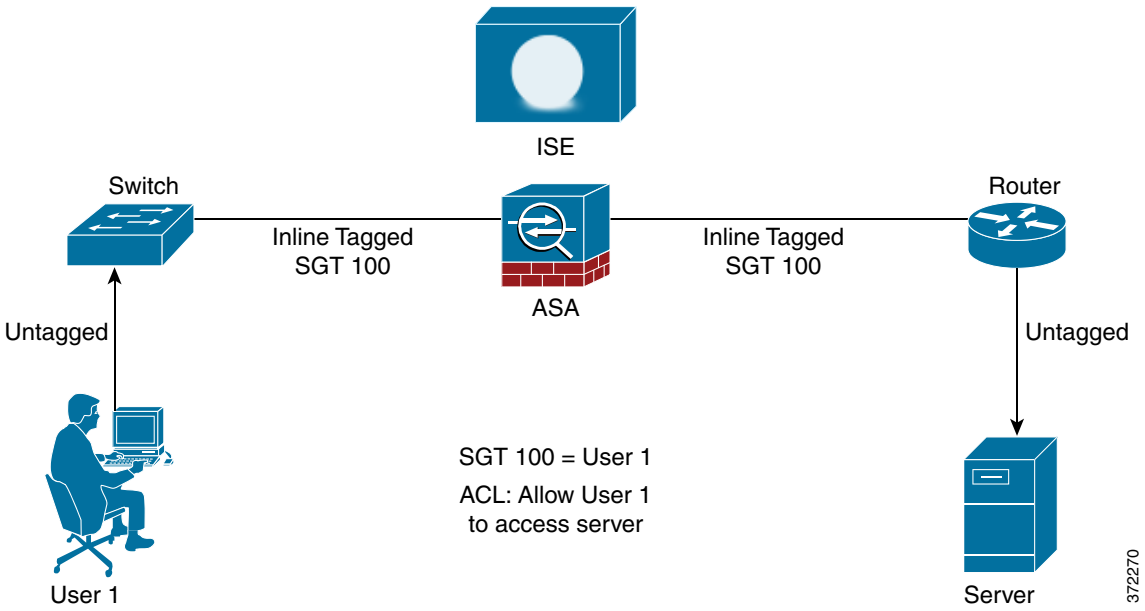
限制

- 仅支持物理接口、 VLAN 接口、端口通道接口和冗余接口。
- 不支持逻辑接口或虚拟接口，例如 BVI。
- 不支持采用 SAP 协商和 MACsec 的链路加密。
- 不支持故障转移链路。
- 不支持集群控制链路。

- 如果 SGT 已更改，ASA 不会对现有流量进行重新分类。任何根据以前 SGT 指定的策略决定对流量寿命依然有效。然而，ASA 能够立即体现出口数据包上的 SGT 更改，即使这些数据包属于根据以前 SGT 进行分类的流量。

图 32-3 显示了典型的第 2 层 SGT 实施示例。

图 32-3　　第 2 层 SGT 实施



使用情境

表 32-3 描述了配置此功能时进口流量的预期行为。

表 32-3　　进口流量

接口配置	收到的已标记数据包	收到的未标记数据包
未发布命令。	数据包被丢弃。	SGT 值来自 IP-SGT 管理器。
cts manual 命令被发布。	SGT 值来自 IP-SGT 管理器。	SGT 值来自 IP-SGT 管理器。
cts manual 命令和 **policy static sgt** *sgt_number* 命令都被发布。	SGT 值来自 **policy static sgt** *sgt_number* 命令。	SGT 值来自 **policy static sgt** *sgt_number* 命令。
cts manual 命令和 **policy static sgt** *sgt_number* **trusted** 命令都被发布。	SGT 值来自数据包中的内联 SGT。	SGT 值来自 **policy static sgt** *sgt_number* 命令。

注　如果没有来自 IP-SGT 管理器的匹配 IP-SGT 映射，则为“Unknown”使用预留 SGT 值“0x0”。

表 32-4 描述了配置此功能时出口流量的预期行为。

表 32-4　　出口流量

接口配置	发送的已标记或未标记数据包
未发布命令。	未标记
cts manual 命令被发布。	已标记
cts manual 命令和 **propagate sgt** 命令都被发布。	已标记
The **cts manual** 命令和 **no propagate sgt** 命令都被发布。	未标记

表 32-5 描述了配置此功能时流向设备的流量和流出设备的流量的预期行为。

表 32-5　　流向设备的流量和流出设备的流量

接口配置	接收的已标记或未标记数据包
未在进口接口上为流向设备的流量发布命令。	数据包被丢弃。
在进口接口上为流向设备的流量发布了 **cts manual** 命令。	数据包已被接受，但没有策略实施或 SGT 传送。
未发布 **cts manual** 命令，或者在出口接口上为流出设备的流量发布了 **cts manual** 命令和 **no propagate sgt** 命令。	未标记数据包被发送，但没有策略实施。 SGT 号来自 IP-SGT 管理器。
发布了 **cts manual** 命令，或者在出口接口上为流出设备的流量发布了 **cts manual** 命令和 **propagate sgt** 命令。	已标记数据包被发送。 SGT 号来自 IP-SGT 管理器。

注　如果没有来自 IP-SGT 管理器的匹配 IP-SGT 映射，则为“Unknown”使用预留 SGT 值“0x0”。

启用 SGT plus Ethernet Tagging

如要启用 SGT plus Ethernet Tagging，请输入以下命令：

命令	用途
`ciscoasa(config-if)# cts manual` **示例：** `ciscoasaciscoasa(config-if)# cts manual` `ciscoasa(config-if-cts-manual)#`	启用第 2 层 SGT 实施，并进入 CTS 手动接口配置模式。 如要禁用第 2 层 SGT 实施，请输入 **no cts manual** 命令。

在接口上传送安全组标记

如要在接口上启用或禁用安全标记传送，请执行以下步骤：

	命令	用途
步骤 1	`ciscoasa(config-if)# cts manual` **示例：** `ciscoasa(config-if)# cts manual` `ciscoasa(config-if-cts-manual)#`	启用第 2 层 SGT 实施，并进入 CTS 手动接口配置模式。
步骤 2	`ciscoasa(config-if-cts-manual)# propagate sgt` **示例：** `ciscoasa(config-if-cts-manual)# propagate sgt`	在接口上启用安全组标记 （称作 **sgt**）传送。默认情况下，传送被启用。要在接口上禁用安全组标记 （称作 **sgt**）传送，请使用 **no propagate sgt** 命令。

将策略应用到手动配置的思科 TrustSec 链路

如要将策略应用到手动配置的 CTS 链路，请执行以下步骤：

	命令	用途
步骤 1	`ciscoasa(config-if)# cts manual` **示例：** `ciscoasa(config-if)# cts manual` `ciscoasa(config-if-cts-manual)#`	启用第 2 层 SGT 实施，并进入 CTS 手动接口配置模式。
步骤 2	`ciscoasa(config-if-cts-manual)# policy static sgt` *sgt_number* [**trusted**] **示例：** `ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted`	将策略应用到手动配置的 CTS 链路。 **static** 指定应用到链路上的传入流量的 SGT 策略。 **sgt** *sgt_number* specifies the SGT number to apply to incoming traffic from the peer.有效值为 2 至 65519。 **trusted** 指明接口上具有在命令中指定的 SGT 的进口流量不应使其 SGT 被覆盖。默认设置为 Untrusted。

示例

以下示例为第 2 层 SGT 实施启用接口并定义此接口是否可信：

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# propagate sgt
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

手动配置 IP-SGT 绑定

如要手动配置 IP-SGT 绑定，请输入以下命令：

命令	用途
ciscoasa(config)# **cts role-based sgt-map** [*IPv4_addr* | *IPv6_addr*] **sgt** *sgt_value* **示例：** ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50	允许手动配置 IP-SGT 绑定。 **sgt** *sgt_value* 指定 SGT 号。有效值为 2 至 65519。

故障排除提示

使用 **packet-tracer** 命令确定为何特定会话被允许或被拒绝，正在使用哪个 SGT 值 （来自数据包中的 SGT，来自 IP-SGT 管理器，或来自在接口上配置的 **policy static sgt** 命令），以及应用了哪些基于安全组的安全策略。

以下示例显示了 **packet-tracer** 命令的输出，以显示到 IP 地址的安全组标记映射：

```
ciscoasa# packet-tracer input inside tcp inline-tag 100 security-group name alpha 30
security-group tag 31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
----------------More---------------------
```

使用 **capture** *capture-name* **type inline-tag** *tag* 命令仅捕获带或不带特定 SGT 值的思科 CMD 数据包 (EtherType 0x8909)。

以下示例显示了 **show capture** 命令针对指定的 SGT 值的输出：

```
ciscoasa# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
```

配置示例

以下示例显示了如何配置 ASA 使用思科 TrustSec：

```
// Import an encrypted CTS PAC file
    cts import-pac asa.pac password Cisco
// Configure ISE for environment data download
    aaa-server cts-server-list protocol radius
```

```
    aaa-server cts-server-list host 10.1.1.100 cisco123
    cts server-group cts-server-list
// Configure SXP peers
    cts sxp enable
    cts sxp connection peer 192.168.1.100 password default mode peer speaker
//Configure security-group based policies
    object-group security objgrp-it-admin
          security-group name it-admin-sg-name
          security-group tag 1
    object-group security objgrp-hr-admin
        security-group name hr-admin-sg-name
        group-object it-admin
    object-group security objgrp-hr-servers
        security-group name hr-servers-sg-name
    access-list hr-acl permit ip object-group-security objgrp-hr-admin any
    object-group-security objgrp-hr-servers
//Configure security group tagging plus Ethernet tagging
   interface gi0/1
   cts manual
   propagate sgt
   policy static sgt 100 trusted10.1.1.100 sgt 50
```

面向思科 TrustSec 的 AnyConnect VPN 支持

ASA 9.3(1) 版本完全支持 VPN 会话的安全组标记。可以使用外部 AAA 服务器或者通过配置本地用户数据库，向 VPN 会话分配安全组标记 (SGT)。然后，可以在第 2 层以太网上通过思科 TrustSec 系统传送此标记。当 AAA 服务器无法提供 SGT 时，安全组标记对于组策略和本地用户非常有用。

如果 AAA 服务器属性中没有用以分配给 VPN 用户的 SGT，ASA 则使用默认组策略中的 SGT。如果组策略中没有 SGT，则分配标记 0x0。

远程用户连接到服务器的典型步骤

1. 用户连接到 ASA。
2. ASA 从 ISE 请求 AAA 信息，其中可能包含 SGT。 ASA 还为用户的隧道流量分配 IP 地址。
3. ASA 使用 AAA 信息进行身份验证并创建隧道。
4. ASA 使用来自 AAA 信息的 SGT 和已分配的 IP 地址，在第 2 层标头中添加 SGT。
5. 包含 SGT 的数据包被传送到思科 TrustSec 网络中的下一个对等设备。

将 SGT 添加到本地用户和组

如要在本地用户数据库上和组策略中配置 SGT 属性，请输入以下命令：

命令	用途
`ciscoasa(config-group-policy)# [no] security-group-tag value sgt` **示例：** `ciscoasa(config-group-policy)# security-group-tag value 101`	在已命名的组策略或本地用户名的属性集上配置 SGT 属性。 此命令的默认格式为 **security-group-tag none**，这意味着，此属性集中没有安全组标记。 **[no] security-group-tag value** *sgt* 命令将配置返回为默认值。

监控思科 TrustSec

如要在 ASA 上监控思科 TrustSec，请输入以下一个或多个命令：

命令	用途
show running-config cts	显示为思科 TrustSec 基础设施和 SXP 命令配置的默认值。
show running-config [all] cts role-based [sgt-map]	显示用户定义的 IP-SGT 绑定表条目。
show cts sxp connections	采用多情景模式时为特定用户情景显示 ASA 上的 SXP 连接。
show conn security-group	显示所有 SXP 连接的数据。
show cts environment-data	显示包含在 ASA 上的安全组表中的思科 TrustSec 环境信息。
show cts sgt-map	显示控制路径中的 IP 地址安全组表管理器条目。
show asp table cts sgt-map	显示在数据路径中维护的 IP 地址安全组表映射数据库中的 IP 地址安全组表映射条目。
show cts pac	显示有关从 ISE 导入 ASA 的 PAC 文件的信息。当 PAC 文件已过期或将 30 天内过期时，显示一条警告消息。

附加参考资料

参考网站	说明
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html	介绍面向企业的思科 TrustSec 系统和架构。
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_DesignZone_TrustSec.html	提供有关在企业中部署思科 TrustSec 解决方案的指导说明，包含到组件设计指南的链接。
http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/solution_overview_c22-591771.pdf	提供有关与 ASA、交换机、无线 LAN (WLAN) 控制器和路由器配合使用的思科 TrustSec 解决方案的概述。
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html	提供思科 TrustSec 平台支持矩阵，其中列出了支持思科 TrustSec 解决方案的思科产品。

思科 TrustSec 集成的功能历史

表 32-6 列出了各种功能变更以及实施该等功能变更的平台版本。

表 32-6　思科 TrustSec 集成的功能历史

功能名称	平台版本	功能信息
思科 TrustSec 集成	9.0(1)	思科 TrustSec 可以提供基于现有的身份感知基础设施的访问控制，确保网络设备之间的数据保密性，并集成平台上的安全访问服务。在思科 TrustSec 功能中，实施设备结合用户属性和终端属性制定基于角色和基于身份的访问控制决策。 在此版本中，ASA 与思科 TrustSec 集成以提供基于安全组的策略实施。思科 TrustSec 域中的访问策略不受拓扑影响，基于源和目标设备的角色，而非基于网络 IP 地址。 ASA 可以将此项思科 TrustSec 功能用于其他类型的基于安全组的策略（例如应用检查）；例如，您可以根据安全组配置包含访问策略的类映射。 引入或修改了以下命令：**access-list extended**、**cts sxp enable**、**cts server-group**、**cts sxp default**、**cts sxp retry period**、**cts sxp reconciliation period**、 **cts sxp connection peer**、 **cts import-pac**、 **cts refresh environment-data**、 **object-group security**、 **security-group**、 **show running-config cts**、 **show running-config object-group**、 **clear configure cts**、 **clear configure object-group**、 **show cts pac**、 **show cts environment-data**、 **show cts environment-data sg-table**、 **show cts sxp connections**、 **show object-group**、 **show configure security-group**、 **clear cts environment-data**、 **debug cts** 和 **packet-tracer**。
第 2 层安全组标记施加	9.3(1)	现在，您可以使用结合了以太网标记的安全组标记来实施策略。 SGT plus Ethernet Tagging，也称作第 2 层 SGT 实施，使 ASA 能够使用思科专有以太网帧 (EtherType 0x8909) 在以太网接口上发送和接收安全组标记，其允许将源安全组标记插入纯文本以太网帧。 引入或修改了以下命令：**cts manual**、 **policy static sgt**、 **propagate sgt**、**cts role-based sgt-map**、**show cts sgt-map**、**packet-tracer**、**capture**、**show capture**、 **show asp drop**、 **show asp table classify**、 **show running-config all**、 **clear configure all** 和 **write memory**。

ASA 和思科移动支持

- 关于 ASA 和思科移动支持
- ASA MDM 代理准则和限制
- 将 ASA 配置为 MDM 代理
- 监控 Mobile Enablement Proxy 活动
- ASA Mobile Enablement Proxy 的功能历史记录

关于 ASA 和思科移动支持

思科 ASA 是边缘设备，可对受思科移动支持 (ME) （思科身份服务引擎 (ISE) 的一个组件）管理的移动设备提供对于公司网络的外部访问权限。作为适用于 ISE ME 的网络访问设备 (NAD)， ASA 可用作移动设备授权、注册和定期登记的代理。它在外部远程移动设备 （AnyConnect 设备管理客户端）与移动设备管理器 （ISE 移动支持服务器）之间提供安全通信路径。这样一来，运行 AnyConnect 客户端应用的外部移动设备就可以完全像内部移动设备一样参与移动设备管理。

本节仅介绍 ASA 特定配置及行为。

可通过指定以下各项在 ASA 上配置 ME 代理功能：

- AnyConnect ME 客户端用于注册和登记请求的 ASA 接口和端口。
- 用于对客户端进行身份验证的 AAA 服务器。通常是 Radius 服务器 （该服务器是 ISE 移动支持解决方案的一个组成部分）。
- 用于向移动支持服务器对 ASA 进行识别和身份验证的信任点

ASA MDM 代理准则和限制

- ME 代理功能仅在单情景路由器模式中受支持。
- ME 代理没有 ASA 许可要求。 ME 的许可在 ISE 上执行。
- 在移动设备上运行的 AnyConnect ME 客户端使用同一个 URI 与 ME 服务器通信，无论用户是在内部 （位于公司网络上）还是在外部 （位于公用网络上）。如要支持这一行为，网络的 DNS 配置必须将 ME URI 解析到 ASA 网关（以实现外部支持）和 ISE 策略服务器节点 (PSN)（以实现内部支持）。

- 对于 AnyConnect ME 客户端与 ASA 之间的身份验证以及 ASA 与 ISE ME 服务器之间的身份验证，需要数字证书。为纳入了 ASA ME 代理的移动支持解决方案计划和配置证书时，请注意以下几点：
  - 对 ISE 策略服务节点进行 ASA 身份验证的证书必须允许同时代表多个代理设备。
  - 对于注册期间作为 SCEP 的结果而在移动设备上接收的 AnyConnect 客户端证书，应将其定义为在外部时对 ASA 进行身份验证，在内部时对 ISE 进行身份验证。同样，以相同的方式在 Apple iOS 移动设备上接收的其他 Applie iOS 客户端证书也应具有这种行为。
  - 可如下定义单一证书：在 Subject Alternative Name (SAN) 字段中指定两个服务器的 FQDN，从而将证书定义为会向移动设备上的客户端进行 ASA 和 ISE 身份验证。
- 外部受管移动设备不能访问“ISE 我的设备”门户。如要访问此门户，移动设备用户必须是内部用户。

将 ASA 配置为 MDM 代理

准备工作

- 必须配置 Radius 服务器组，使其能够访问 ISE AAA Radius 服务器以进行授权和记帐。
- 必须配置信任点，用于代表 AnyConnect 客户端向 ISE MDM 服务器进行 ASA 身份验证。

操作步骤

步骤 1　从配置模式进入 config-mdm-proxy 模式，以配置和启用 MDM 代理功能：

```
asa(config)# mdm-proxy
```

步骤 2　配置用于 AnyConnect 设备管理注册和登记的端口：

默认注册端口是 443。必须指定用于 MDM 登记请求的端口。这两个端口的范围都必须是 1 到 65535。

```
asa (config-mdm-proxy)# port enrollment 443 checkin 8906
```

步骤 3　为 MDM 代理会话配置之前定义的身份验证和记帐服务器组：

```
asa (config-mdm-proxy)# accounting-server-group ISE-AAA
asa (config-mdm-proxy)# authentication-server-group ISE-AAA
```

步骤 4　代表所有 AnyConnect 设备管理会话配置之前为 ISE MDM 服务器的 MDM 代理访问定义的信任点：

```
asa (config-mdm-proxy)# trustpoint ASAtoISEMDM
```

步骤 5　（可选）指定在密码到期之前多少天发出警告：

```
asa (config-mdm-proxy)# password-management 5
```

步骤 6　（可选）指定 MDM 代理会话限制：

a. 设置并发 MDM 会话的数量 （1 到 10000，默认值为 1000）：

```
asa (config-mdm-proxy)# session-limit 5000
```

b. 设置注册和登记的会话最长持续时间 （默认值为 300）：

```
asa (config-mdm-proxy)# session-timeout enrollment 600 checkin 600
```

步骤 7　在外部接口上启用 MDM 代理配置：

```
asa (config-mdm-proxy)# enable outside
```

监控 Mobile Enablement Proxy 活动

如要查看 ASA 的移动支持统计信息，请输入以下命令：

show mdm-proxy statistics

如要查看当前的移动支持配置，请输入以下命令：

show running-config mdm-proxy

ASA Mobile Enablement Proxy 的功能历史记录

功能名称	平台版本	功能信息
Mobile Enablement Proxy	9.3(1)	Mobile Enablement Proxy 是 ISE Mobile Enablement 解决方案的组件，允许外部移动设备以与内部移动设备完全相同的方式参与移动设备管理。 我们引入了 **mdm-proxy** 命令，以进入 config-mdm-proxy 模式。在此新模式中，以下命令适用：**authentication-server-group**、 **accounting-server-group**、 **password-management**、 **trusttpoint**、 **port**、 **session-limit**、 **session-timeout** 和 **enable**。

第 34 章

数字证书

本章介绍了如何配置数字证书。

- 第 34-1 页的关于数字证书
- 第 34-7 页的本地证书的先决条件
- 第 34-8 页的数字证书准则
- 第 34-9 页的配置数字证书
- 第 34-34 页的监控数字证书
- 第 34-36 页的证书管理的功能历史

关于数字证书

CA 负责管理证书请求和颁发数字证书。数字证书包括识别用户或的设备信息，如名称、序列号、公司、部门或 IP 地址。数字证书还包括用户或设备的公钥副本。 CA 可以是可信的第三方，如 VeriSign，或公司内建立的私有 （内部） CA。

提示 有关包括证书配置和负载均衡的情景示例，请参阅以下 URL：https://supportforums.cisco.com/docs/DOC-5964。

公钥加密

由公钥加密支持的数字签名提供了一种验证设备和用户身份的方法。在 RSA 加密系统等公钥加密中，每个用户都具有一个包含公钥和私钥的密钥对。密钥对互为补充，采用其中一个密钥加密的任何东西均可使用另一个密钥解密。

简单来说，使用私钥加密数据时，将形成签名。签名附于数据中并发送给接收方。接收方将发送方的公钥应用于数据。如果随数据一起发送的签名与将公钥应用于数据的结果相匹配，则验证了消息的有效性。

此过程依赖于，接收方具有发送方公钥的副本，且高度肯定此密钥属于发送方，而非冒充发送方的其他人。

获取发送方公钥通常是在外部处理或通过安装时执行的操作处理。例如，默认情况下，大多数网络浏览器都是使用几个 CA 的根证书进行配置。对于 VPN，作为 IPsec 一部分的 IKE 协议可使用数字签名在设置安全关联之前验证对等设备身份。

证书可扩展性

在没有数字证书的情况下，必须手动为每个与其通信的对等体配置各自的 IPSec 对等体；因此，每个添加到网络的新对等体都会要求对需要与其安全通信的每个对等体进行配置更改。

使用数字证书时，系统将向 CA 注册每个对等体。两个对等体试图进行通信时，它们将交换证书并以数字方式签署数据以进行相互身份验证。新对等体添加到网络时，向 CA 注册该对等体，其他任何对等体都不需要修改。新对等体尝试进行 IPSec 连接时，证书将自动交换并且对等体可进行身份验证。

通过 CA，对等体可将证书发送到远程对等体并进行一些公钥加密，从而自行向远程对等体进行身份验证。每个对等体将发送由 CA 颁发的唯一证书。之所以执行此过程，是因为每个证书会封装关联对等体的公钥，每个证书由 CA 进行身份验证，且所有参与对等体都将 CA 视为身份验证机构。此过程称为带 RSA 签名的 IKE。

对等体可继续为多个 IPsec 会话发送其证书，并可向多个 IPSec 对等体发送证书，直到证书过期。证书过期后，对等体管理员必须从 CA 获取新的证书。

CA 还可以为不再参与 IPsec 的对等体撤销证书。撤销的证书无法被其他对等体识别为有效证书。撤销的证书列于 CRL 中，每个对等体都可能会在从其他对等体接受证书之前检查这些证书。

有些 CA 会在实施过程中使用 RA。RA 是一种用作 CA 的代理的服务器，因此，CA 功能可以在 CA 不可用时继续使用。

密钥对

密钥对是 RSA 密钥，具有以下特征：

- RSA 密钥可用于 SSH 或 SSL。
- SCEP 注册支持 RSA 密钥的认证。
- 为了生成密钥，RSA 密钥的最大密钥模值为 2048 位。默认长度为 1024 位。许多使用含超过 1024 位 RSA 密钥对的身份证书的 SSL 连接可能会导致 ASA 上的 CPU 使用率较高，并导致无客户端登录被拒绝。
- 对于签名操作，支持的最大密钥长度为 4096 位。我们建议使用至少为 2048 位的密钥长度。
- 您可以生成一个通用 RSA 密钥对，用于签名和加密，也可以为每种用途生成单独的 RSA 密钥对。单独的签名和加密密钥有助于减少密钥泄露的机会，因为 SSL 使用密钥进行加密，但不签名。但是，IKE 使用密钥进行签名，但不加密。通过为每种用途使用单独的密钥，泄露密钥的风险降至最低。

信任点

信任点可让您管理和跟踪 CA 与证书。信任点是一种 CA 或身份对的表现。信任点包括 CA 的身份、 CA 特定配置参数，以及与一个注册的身份证书的关联。

定义信任点之后，可以在要求指定 CA 的命令中根据名称来引用它。您可以配置多个信任点。

注　如果 Cisco ASA 具有多个共享相同 CA 的信任点，则只有其中一个共享 CA 的信任点可用于验证用户证书。如要控制将哪个共享 CA 的信任点用于验证由该 CA 颁发的用户证书，请使用 **support-user-cert-validation** 命令。

对于自动注册，信任点必须使用注册 URL 进行配置，并且信任点代表的 CA 必须在网络中可用且必须支持 SCEP。

您可以 PKCS12 格式导出和导入密钥对，以及与某个信任点关联的已颁发证书。此格式有助于在不同的 ASA 上手动复制信任点配置。

证书注册

ASA 需要每个信任点都有一个 CA 证书，它自己也需要一个或两个证书，具体取决于信任点使用的密钥的配置。如果信任点使用单独的 RSA 密钥进行签名和加密，则 ASA 需要两个证书，每种用途一个。在其他密钥配置中，只需要一个证书。

ASA 支持使用 SCEP 自动注册和手动注册，这样可将 base-64 编码的证书直接粘贴到终端。对于站点到站点 VPN，必须注册每个 ASA。对于远程访问 VPN，必须注册每个 ASA 和每个远程访问 VPN 客户端。

SCEP 请求的代理

ASA 可代理 AnyConnect 和第三方 CA 之间的 SCEP 请求。如果 ASA 用作代理，则 CA 只需要允许它访问。如果要 ASA 提供此服务，用户必须在 ASA 发送注册请求之前使用任意受 AAA 支持的方法进行身份验证。您还可以使用主机扫描和动态访问策略强制注册资格规则。

ASA 只在 AnyConnect SSL 或 IKEv2 VPN 会话中支持此功能。它支持所有符合 SCEP 的 CA，包括 Cisco IOS CS、 Windows Server 2003 CA 和 Windows Server 2008 CA。

无客户端（基于浏览器）访问不支持 SCEP 代理，但 WebLaunch（无客户端启动 AnyConnect）支持它。

ASA 不支持证书的轮询。

ASA 支持此功能的负载均衡。

撤销检查

证书颁发后，在固定时期内有效。有时，CA 会在此时期到期前撤销证书，例如，因为安全问题或名称变化或关联等原因而撤销。CA 会定期发布签署的撤销证书列表。启用撤销检查可强制 ASA CA 在每次使用证书进行身份验证时检查并确定其未撤销该证书。

启用撤销检查后，ASA 会在 PKI 证书验证过程中使用 CRL 检查、OCSP 或同时使用两者检查证书撤销状态。只有在第一种方法返回错误时（例如，指示服务器不可用时）才使用 OCSP。

通过 CRL 检查，ASA 可检索、分析、缓存 CRL，从而提供完整的撤销（和未撤销）证书及其证书序列号列表。ASA 根据 CRL（也称为权限撤销列表）评估证书，从身份证书一直到从属证书颁发机构链。

OCSP 提供了一种更具可扩展性的撤销状态检查方法。此方法通过验证机构对证书状态进行本地化，验证机构会查询特定证书的状态。

支持的 CA 服务器

ASA 支持以下 CA 服务器：

Cisco IOS CS、 ASA 本地 CA 和符合 X.509 的第三方 CA 供应商，包括但不限于：

- Baltimore Technologies
- Entrust

- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

CRL 为 ASA 提供了一种方法来确定某个有效期内的证书是否已被证书颁发机构 (CA) 撤销。CRL 配置是信任点配置的一部分。

进行证书身份验证时，可使用 **revocation-check crl** 命令配置 ASA 以将 CRL 检查设为强制性检查。也可以使用 **revocation-check crl none** 命令将 CRL 检查设为可选检查，这种情况下，在 CA 无法提供更新的 CRL 数据时，证书身份验证也会成功。

ASA 可使用 HTTP、SCEP 或 LDAP 从 CA 检索 CRL。为每个信任点检索的 CRL 会在为每个信任点配置的时间内一直缓存。

当 ASA 缓存 CRL 的时间长于配置用于缓存 CRL 的时间时，ASA 会认为 CRL 太陈旧（因而也就不太可靠）或“过时”。 ASA 会在下一次证书身份验证需要检查过时 CRL 时尝试检索更新版本的 CRL。

ASA 缓存 CRL 的时间由以下两个因素决定：

- 使用 **cache-time** 命令指定的分钟数。默认值为 60 分钟。
- 检索的 CRL 中的 NextUpdate 字段，CRL 中可能没有该字段。可使用 **enforcenextupdate** 命令控制 ASA 是否需要和使用 NextUpdate 字段。

ASA 通过以下方式利用这两个因素：

- 如果不需要 NextUpdate 字段，ASA 会在由 **cache-time** 命令定义的时间过后将 CRL 标记为“过时”。
- 如果需要 NextUpdate 字段，ASA 会在由 **cache-time** 命令和 NextUpdate 字段指定的两个时间中较早的那个时间点将 CRL 标记为“过时”。例如，如果 **cache-time** 命令设置为 100 分钟，而 NextUpdate 字段指定下一次更新是在 70 分钟后，则 ASA 会将 CRL 标记为“在 70 分钟后过时”。

如果 ASA 的内存不足以存储为给定信任点缓存的所有 CRL，它将删除最近最少使用的 CRL 以为新检索的 CRL 腾出空间。

OCSP

OCSP 为 ASA 提供了一种方法来确定某个有效期内的证书是否已被证书颁发机构 (CA) 撤销。OCSP 配置是信任点配置的一部分。

OCSP 在验证机构（一种 OCSP 服务器，也称为 *响应方*）上对证书状态进行本地化，这样 ASA 就可查询特定证书的状态。相比 CRL 检查，此方法可提供更好的可扩展性和更新的撤销状态，并且可帮助装有大型 PKI 的公司部署和扩展安全网络。

注　ASA 允许 OCSP 响应有五秒钟的时间偏差。

在进行证书身份验证时，可使用 **revocation-check ocsp** 命令配置 ASA 以将 OCSP 检查设为强制性检查。也可以使用 **revocation-check ocsp none** 命令将 OCSP 检查设为可选检查，这种情况下，在验证机构无法提供更新的 OCSP 数据时，证书身份验证也会成功。

OCSP 提供三种定义 OCSP 服务器 URL 的方法。 ASA 按以下顺序使用这些服务器：

1. 使用 **match certificate** 命令在匹配证书覆盖规则中定义的 OCSP URL。
2. 使用 **ocsp url** 命令配置的 OCSP URL。
3. 客户端证书的 AIA 字段。

注　如要将信任点配置为验证自签名 OCSP 响应方证书，请将自签名响应方证书作为可信 CA 证书导入其自己的信任点。之后，在客户端证书验证信任点配置 **match certificate** 命令以使用包括自签名 OCSP 响应方证书的信任点验证响应方证书。使用相同操作步骤在客户端证书的验证路径外部配置验证响应方证书。

OCSP 服务器（响应方）证书通常会签署 OCSP 响应。在收到响应后，ASA 将尝试验证响应方证书。CA 通常会将 OCSP 响应方证书的有效期设置为相对较短的时间以将受危害的可能性降至最低。CA 通常还会在响应方证书中包含 ocsp-no-check 扩展，表明此证书不需要进行撤销状态检查。但是，如果此扩展不存在，ASA 将尝试使用信任点中指定的同一方法检查撤销状态。如果响应方证书无法验证，则撤销检查失败。如要避免这种可能性，请使用 **revocation-check none** 命令配置响应方证书验证信任点，并使用 **revocation-check ocsp** 命令配置客户端证书。

本地 CA

本地 CA 执行以下任务：

- 在 ASA 上集成基本证书授权操作。
- 部署证书。
- 为已颁发的证书提供安全的撤销检查。
- 在 ASA 上提供一个证书授权功能以便与基于浏览器和基于客户端的 SSL VPN 连接配合使用。
- 为用户提供可信数字证书，而无需依赖于外部证书授权。
- 提供安全的内部机构进行证书身份验证，并提供通过网站登录进行的直接用户注册。

本地 CA 文件的存储

ASA 可使用本地 CA 数据库访问和实施用户信息、已颁发的证书和撤销列表。默认情况下，此数据库驻留在本地闪存中，也可以配置为驻留在已安装且允许 ASA 访问的外部文件系统上。

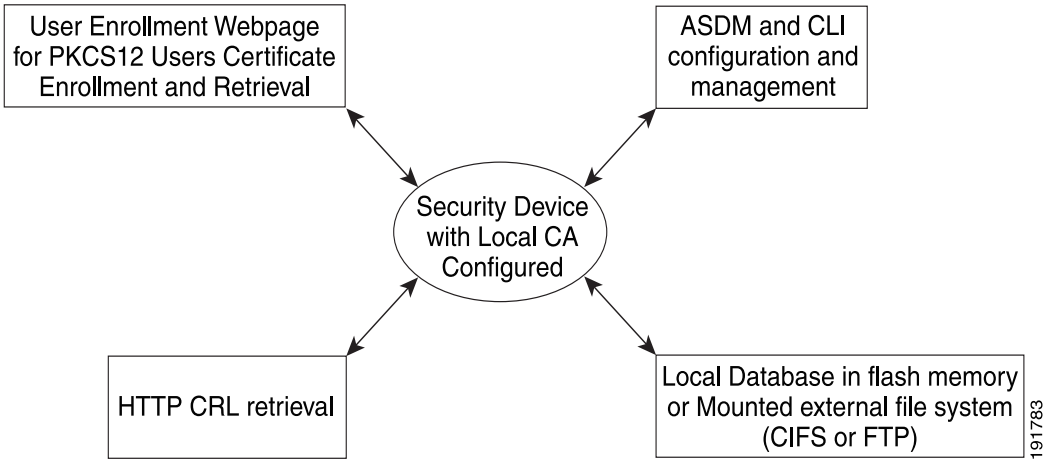
可存储在本地 CA 用户数据库中的用户数量不受限制；但是，如果出现闪存存储问题，将生成系统日志以提示管理员采取行动，并且本地 CA 可能会被禁用，直到存储问题得到解决。闪存可存储不超过 3500 个用户的数据库；但是，超过 3500 个用户的数据库需要外部存储器。

本地 CA 服务器

在 ASA 上配置本地 CA 服务器后，用户可为每个证书进行注册，方法如下：登录网站并输入用户名及由本地 CA 管理员提供的一次性密码以验证其注册资格。

图 34-1 显示本地 CA 服务器驻留在 ASA 上并处理来自网站用户的注册请求，以及来自其他证书验证设备和 ASA 的 CRL 查询。本地 CA 数据库和配置文件保存在 ASA 闪存（默认存储器）或单独的存储设备上。

图 34-1　本地 CA



证书和用户登录凭证

下一节介绍了使用证书和用户登录凭证 （用户名和密码）进行身份验证和授权的不同方法。这些方法适用于 IPsec、 AnyConnect 和无客户端 SSL VPN。

在任何情况下，LDAP 授权都不会使用密码作为凭证。RADIUS 授权对所有用户使用公用密码或使用用户名作为密码。

用户登录凭证

身份验证和授权的默认方法是使用用户登录凭证。

- 身份验证
  - 通过隧道组 （也称为 ASDM 连接配置文件）中的身份验证服务器组设置启用
  - 使用用户名和密码作为凭证
- 授权
  - 通过隧道组 （也称为 ASDM 连接配置文件）中的授权服务器组设置启用
  - 使用用户名作为凭证

证书

如果已配置用户数字证书，ASA 会先验证证书。但是，它不会使用证书的任意 DN 作为用户名进行身份验证。

如果身份验证和授权均已启用，ASA 将使用用户登录凭证同时进行用户身份验证和授权。

- 身份验证
  - 通过身份验证服务器组设置启用
  - 使用用户名和密码作为凭证
- 授权
  - 通过授权服务器组设置启用
  - 使用用户名作为凭证

如果身份验证禁用，而授权启用，ASA 将使用主要 DN 字段进行授权。

- 身份验证
  - 通过身份验证服务器组设置禁用 （设置为 None）
  - 未使用凭证
- 授权
  - 通过授权服务器组设置启用
  - 使用证书主要 DN 字段的用户名作为凭证

注　如果证书中不存在主要 DN 字段，ASA 将使用次要 DN 字段值作为授权请求的用户名。

以包含以下 Subject DN 字段和值的用户证书为例：

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

如果主要 DN = EA（邮件地址）并且次要 DN = CN（公用名称），则授权请求中使用的用户名是 anyuser@example.com。

本地证书的先决条件

本地证书有以下先决条件要求：

- 确保正确配置 ASA 以支持证书。配置不正确的 ASA 可能会导致注册失败或请求包含不准确信息的证书。
- 确保正确配置 ASA 的主机名和域名。如要查看当前配置的主机名和域名，请输入 **show running - config** 命令。
- 确保在配置 CA 之前准确设置 ASA 时钟。证书具有有效和到期的日期和时间。当 ASA 向 CA 注册并获取证书时，ASA 会检查当前时间是否在证书的有效范围内。如果超出范围，注册失败。

SCEP 代理支持的先决条件

将 ASA 配置为代理以提交对第三方证书的请求时，具有以下要求：

- 终端中必须运行的是 AnyConnect 安全移动客户端 3.0 或更高版本。
- 在组策略的连接配置文件中配置的身份验证方法必须设置为同时使用 AAA 和证书身份验证。
- 对于 IKEv2 VPN 连接，SSL 端口必须处于打开状态。
- CA 必须处于自动授予模式。

数字证书准则

情景模式准则

- 对于第三方 CA，只在单情景模式中受支持。

故障转移准则

- 在带状态的故障转移中不支持复制会话。
- 对于本地 CA，不支持故障转移。

IPv6 准则

不支持 IPv6。

其他指导原则

- 对于配置为 CA 服务器或客户端的 ASA，将证书的有效期限制为不超过建议的结束日期，2038 年 1 月 19 日凌晨 3:14:08 (UTC)。本准则还适用于从第三方供应商导入的证书。
- 启用故障转移时，无法配置本地 CA。您只能为无故障转移的独立 ASA 配置本地 CA 服务器。有关详细信息，请参阅 CSCty43366。
- 证书注册完成后，ASA 将存储包含用户的密钥对和证书链的 PKCS12 文件，每次注册需要约 2 KB 的闪存或磁盘空间。实际的磁盘空间容量取决于已配置的 RSA 密钥长度和证书字段。在可用闪存容量有限的 ASA 上添加大量待处理的证书注册时，请记住此准则，因为这些 PKCS12 文件在配置的注册检索超时期间存储在闪存中。我们建议使用至少为 2048 位的密钥长度。
- 本地 CA 服务器证书第一次生成时 （即，最初配置本地 CA 服务器并发出 **no shutdown** 命令时），**lifetime ca-certificate** 命令生效。CA 证书到期时，配置的有效期值用于生成新的 CA 证书。您不能更改现有 CA 证书的有效期值，
- 而应配置 ASA 以使用身份证书保护流向管理接口的 ASDM 流量和 HTTPS 流量。使用 SCEP 自动生成的身份证书会在每次重新启动后重新生成，因此请确保手动安装您自己的身份证书。本操作步骤仅适用于 SSL，有关示例，请参阅以下 URL：http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml。
- ASA 和 AnyConnect 客户端只可验证其中 X520Serialnumber 字段 （使用者名称中的序列号）使用 PrintableString 格式的证书。如果序列号格式使用编码 （如 UTF8），证书授权将失败。
- 如果在 ASA 上导入证书参数时，只对证书参数使用有效的字符和值。

- 如要使用通配符 (*) 符号，请确保在允许在字符串值中使用此字符的 CA 服务器上使用编码。虽然 RFC 5280 建议使用 UTF8String 或 PrintableString，但您应使用 UTF8String，因为 PrintableString 无法将通配符识别为有效字符。如果在导入过程中发现无效的字符或值，ASA 将拒绝导入的证书。例如：

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read
162*H÷ytes as CA certificate:0U0= \Ivr"phÕV°3é¼þ0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

配置数字证书

本节介绍了如何配置本地 CA 证书。确保按照所列任务的顺序正确配置此类型的数字证书。

- 第 34-10 页的配置密钥对
- 第 34-10 页的移除密钥对
- 第 34-11 页的配置信任点
- 第 34-13 页的为信任点配置 CRL
- 第 34-15 页的导出信任点配置
- 第 34-15 页的导入信任点配置
- 第 34-16 页的配置 CA 证书映射规则
- 第 34-17 页的手动获取证书
- 第 34-18 页的使用 SCEP 自动获取证书
- 第 34-19 页的为 SCEP 请求配置代理支持
- 第 34-20 页的启用本地 CA 服务器
- 第 34-21 页的配置本地 CA 服务器
- 第 34-22 页的自定义本地 CA 服务器
- 第 34-23 页的调试本地 CA 服务器
- 第 34-24 页的禁用本地 CA 服务器
- 第 34-24 页的删除本地 CA 服务器
- 第 34-24 页的配置本地 CA 证书特征

配置密钥对

如要生成密钥对，请执行以下步骤：

	命令	用途
步骤 1	**crypto key generate rsa** **示例：** `ciscoasa/contexta(config)# crypto key generate rsa`	系统将生成一个通用 RSA 密钥对。默认密钥模值为 1024 位。要指定其他模值大小，请使用 **modulus** 关键字。 **注**　很多使用含超过 1024 位 RSA 密钥对的身份证书的 SSL 连接都可能会导致 ASA 上的 CPU 使用率较高，并导致无客户端登录被拒绝。
步骤 2	**crypto key generate rsa label** *key-pair-label* **示例：** `ciscoasa/contexta(config)# crypto key generate rsa label exchange`	（可选）向每个密钥对分配标签。该标签由使用密钥对的信任点引用。如果未分配标签，密钥对将自动标记为 *Default-RSA-Key*。
步骤 3	**show crypto key** *name of key* **示例：** `ciscoasa/contexta(config)# show crypto key examplekey`	验证已生成的密钥对。
步骤 4	**write memory** **示例：** `ciscoasa(config)# write memory`	保存已生成的密钥对。

移除密钥对

如要移除密钥对，请执行以下步骤：

命令	用途
crypto key zeroize rsa **示例：** `ciscoasa(config)# crypto key zeroize rsa`	移除密钥对。

示例

以下示例显示了如何移除密钥对：

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All device certs issued using these keys will also be removed.

Do you really want to remove these keys?[yes/no] y
```

配置信任点

如要配置信任点，请执行以下步骤：

	命令	用途
步骤 1	**crypto ca trustpoint** *trustpoint-name* **示例：** `ciscoasa/contexta(config)# crypto ca trustpoint Main`	创建对应于 ASA 需要从其接收证书的 CA 的信任点。进入 crypto ca trustpoint 配置模式，该模式控制可从第 3 步开始配置的 CA 特定信任点参数。 **注**　尝试连接时，如果尝试从信任点检索 ID 证书，系统将发出警告，指示信任点不包含 ID 证书。
步骤 2	选择以下选项之一：	
	enrollment url *url* **示例：** `ciscoasa/contexta(config-ca-trustpoint)# enrollment url http://10.29.67.142:80/certsrv/mscep/mscep.dll`	使用指定信任点请求使用 SCEP 的自动注册并配置注册 URL。
	enrollment terminal **示例：** `ciscoasa/contexta(config-ca-trustpoint)# enrollment terminal`	将从 CA 收到的证书粘贴到终端，请求使用指定信任点手动注册。
步骤 3	**revocation-check crl none** `revocation-check crl` `revocation-check none` **示例：** `ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl none` `ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl` `ciscoasa/contexta(config-ca-trustpoint)# revocation-check none`	指定可用的 CRL 配置选项。 **注**　要启用必要的或可选的 CRL 检查，请确保在获得证书后配置 CRL 管理的信任点。
步骤 4	**crl configure** **示例：** `ciscoasa/contexta(config-ca-trustpoint)# crl configure`	进入 crl 配置模式。
步骤 5	**email** *address* **示例：** `ciscoasa/contexta(config-ca-trustpoint)# email example.com`	在注册过程中，要求 CA 在证书的“使用者备用名称”扩展中包含指定的邮件地址。
步骤 6	**enrollment retry period** **示例：** `ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 5`	（可选）指定重试时间 （以分钟为单位），且仅应用于 SCEP 注册。

	命令	用途
步骤 7	**enrollment retry count** **示例：** `ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 2`	（可选）指定允许的最大重试次数，且仅应用于 SCEP 注册。
步骤 8	**fqdn** *fqdn* **示例：** `ciscoasa/contexta(config-ca-trustpoint)# fqdn example.com`	在注册过程中，要求 CA 在证书的“使用者备用名称”扩展中包含指定的完全限定域名。
步骤 9	**ip-address** *ip-address* **示例：** `ciscoasa/contexta(config-ca-trustpoint)# ip-address 10.10.100.1`	在注册过程中，要求 CA 在证书中包含 ASA 的 IP 地址。
步骤 10	**keypair** *name* **示例：** `ciscoasa/contexta(config-ca-trustpoint)# keypair exchange`	指定要认证其公钥的密钥对。
步骤 11	**match certificate map-name override ocsp** **示例：** `ciscoasa/contexta(config-ca-trustpoint)# match certificate examplemap override ocsp`	配置 OCSP URL 覆盖和信任点以用于验证 OCSP 响应方证书。
步骤 12	**ocsp disable-nonce** **示例：** `ciscoasa/contexta(config-ca-trustpoint)# ocsp disable-nonce`	禁用 OCSP 请求上的 nonce 扩展。 nonce 扩展以加密方式将请求与响应绑定在一起以避免重放攻击。
步骤 13	**ocsp url** **示例：** `ciscoasa/contexta(config-ca-trustpoint)# ocsp url`	为 ASA 配置 OCSP 服务器以用于检查与信任点关联的所有证书，而不是使用客户端证书的 AIA 扩展中指定的服务器。
步骤 14	**password** *string* **示例：** `ciscoasa/contexta(config-ca-trustpoint)# password mypassword`	指定在注册过程中向 CA 注册的质询短语。CA 通常使用此短语对随后的撤销请求进行身份验证。
步骤 15	**revocation check** **示例：** `ciscoasa/contexta(config-ca-trustpoint)# revocation check`	设置一种或多种撤销检查方法：CRL、 OCSP 和 none。

	命令	用途
步骤 16	**subject-name** *X.500 name* **示例：** `ciscoasa/contexta(config-ca-trustpoint)# myname X.500 examplename`	在注册过程中，要求 CA 在证书中包含指定的使用者 DN。如果 DN 字符串包含逗号，可用双引号将值字符串引起来（例如，O="Company, Inc."）。
步骤 17	**serial-number** **示例：** `ciscoasa/contexta(config-ca-trustpoint)# serial number JMX1213L2A7`	在注册过程中，要求 CA 在证书中包含 ASA 序列号。
步骤 18	**write memory** **示例：** `ciscoasa/contexta(config)# write memory`	保存运行配置。

为信任点配置 CRL

如要在证书身份验证过程中使用强制性或可选 CRL 检查，您必须为每个信任点配置 CRL。如要为信任点配置 CRL，请执行以下步骤：

	命令	用途
步骤 1	**crypto ca trustpoint** *trustpoint-name* **示例：** `ciscoasa (config)# crypto ca trustpoint Main`	进入要修改其 CRL 配置的信任点的 crypto ca trustpoint 配置模式。 **注**　确保在输入此命令之前已启用 CRL。此外，CRL 必须可用才能成功进行身份验证。
步骤 2	**crl configure** **示例：** `ciscoasa (config-ca-trustpoint)# crl configure`	进入当前信任点的 crl 配置模式。 **提示**　如要将所有 CRL 配置参数设置为默认值，请使用 **default** 命令。在 CRL 配置过程中，任何时候重新输入此命令即可重启操作步骤。
步骤 3	执行以下操作之一：	
	policy cdp **示例：** `ciscoasa (config-ca-crl)# policy cdp`	配置检索策略。 CRL 是只从已通过身份验证的证书中指定的 CRL 分发点检索。 **注**　证书中指定的分发点不支持 SCEP 检索。 如要继续，请转至第 5 步。
	policy static **示例：** `ciscoasa (config-ca-crl)# policy static`	配置检索策略。 CRL 是只从您配置的 URL 中检索。 如要继续，请转至第 4 步。
	policy both **示例：** `ciscoasa (config-ca-crl)# policy both`	配置检索策略。 CRL 是从已通过身份验证的证书中指定的 CRL 分发点和您配置的 URL 中检索。 如要继续，请转至第 4 步。

	命令	用途
步骤 4	**url** *n url* **示例：** ciscoasa (config-ca-crl)# url 2 http://www.example.com	如果在配置 CRL 策略时使用关键字 **static** 或 **both**，则必须为 CRL 检索配置 URL。最多可以输入五个 URL，级别为 1 到 5。*n* 是分配给 RUL 的级别。如要移除 URL，请使用 **no url** *n* 命令。
步骤 5	**protocol http | ldap | scep** **示例：** ciscoasa (config-ca-crl)# protocol http	配置检索方法。指定 HTTP、LDAP 或 SCEP 作为 CRL 检索方法。
步骤 6	**cache-time** *refresh-time* **示例：** ciscoasa (config-ca-crl)# cache-time 420	为当前信任点配置 ASA 缓存 CRL 的时间。*refresh-time* 是 ASA 将 CRL 视为“过时”前等待的分钟数。
步骤 7	执行以下操作之一：	
	enforcenextupdate **示例：** ciscoasa (config-ca-crl)# enforcenextupdate	CRL 中需要 NextUpdate 字段。这是默认设置。
	no enforcenextupdate **示例：** ciscoasa (config-ca-crl)# no enforcenextupdate	允许 CRL 中没有 NextUpdate 字段。
步骤 8	**ldap-defaults** *server* **示例：** ciscoasa (config-ca-crl)# ldap-defaults ldap1	如果 LDAP 被指定为检索协议，可找出 ASA 的 LDAP 服务器。您可以按 DNS 主机名或 IP 地址指定服务器。如果服务器侦听端口上的 LDAP 查询，则还可以提供端口号，而不是使用默认端口号 389。 **注**　如果使用主机名而非 IP 地址来指定 LDAP 服务器，请确保您已配置 ASA 以使用 DNS。
步骤 9	**ldap-dn** *admin-DN password* **示例：** ciscoasa (config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering c00lRunZ	如果 LDAP 服务器需要凭证，则允许 CRL 检索。
步骤 10	**crypto ca crl request** *trustpoint* **示例：** ciscoasa (config-ca-crl)# crypto ca crl request Main	从指定信任点所代表的 CA 检索当前的 CRL 并为当前信任点测试 CRL 配置。
步骤 11	**write memory** **示例：** ciscoasa (config)# write memory	保存运行配置。

导出信任点配置

要导出信任点配置，请输入以下命令：

命令	用途
crypto ca export *trustpoint* **示例：** ciscoasa(config)# crypto ca export Main	以 PKCS12 格式导出带所有关联密钥和证书的信任点配置。 ASA 将在终端中显示 PKCS12 数据。您可以复制该数据。信任点数据受密码保护；但是，如果将信任点数据保存在文件中，请确保文件处于安全的位置。

示例

以下示例显示了使用密码 Wh0zits 导出信任点 Main 的 PKCS12 数据：

```
ciscoasa (config)# crypto ca export Main pkcs12 Wh0zits

Exported pkcs12 follows:

[ PKCS12 data omitted ]

---End - This line not part of the pkcs12---
```

导入信任点配置

如要导入信任点配置，请输入以下命令：

命令	用途
crypto ca import *trustpoint* **pkcs12** **示例：** ciscoasa(config)# crypto ca import Main pkcs12	导入与信任点配置关联的密钥对和已颁发证书。 ASA 提示您以 base64 格式将文本粘贴到终端上。系统将向与信任点一起导入的密钥对分配一个与所创建的信任点名称相匹配的标签。 **注**　如果 ASA 具有共享相同 CA 的信任点，则只能使用其中一个共享 CA 的信任点来验证用户证书。要控制将哪个共享 CA 的信任点用于验证由该 CA 颁发的用户证书，请使用 **support-user-cert-validation** 关键字。

示例

以下示例显示了使用密码 Wh0zits 将 PKCS12 数据手动导入信任点 Main：

```
ciscoasa (config)# crypto ca import Main pkcs12 Wh0zits

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
```

以下示例显示了手动导入信任点 Main 的证书：

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com
```

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

配置 CA 证书映射规则

您可以根据证书的 Issuer 和 Subject 字段配置规则。使用创建的规则，您可以使用 **tunnel-group-map** 命令将 IPsec 对等体证书映射到隧道组。 ASA 支持一个 CA 证书映射，该映射可包含多个规则。

如要配置 CA 证书映射规则，请执行以下步骤：

	命令	用途
步骤 1	**crypto ca certificate map** *sequence-number* **示例：** `ciscoasa(config)# crypto ca certificate map 1`	进入要配置的规则的 CA 证书映射配置模式并指定规则索引编号。
步骤 2	**issuer-name** *DN-string* **示例：** `ciscoasa(config-ca-cert-map)# issuer-name cn=asa.example.com`	指定所有已颁发证书的可分辨名称，此名称同样也是自签名 CA 证书的使用者名称 DN。使用逗号来分隔属性值对。使用引号将任何包含逗号的值引起来。颁发者名称必须少于 500 个字母数字字符。默认颁发者名称是 cn=*hostame.domain-name*。
步骤 3	**subject-name attr** *tag* **eq | co | ne | nc** *string* **示例：** `ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert`	指定 ASA 可应用于证书 Subject 字段中找到的值的测试。测试可以应用于特定属性或整个字段。您可以为每个规则配置多个测试，并且使用这些命令指定的所有测试都必须适用于与证书相匹配的规则。以下是有效的操作符： • eq - 字段或属性必须与给定的值相同。 • ne - 字段或属性不能与给定的值相同。 • co - 部分或所有字段或属性必须与给定的值相匹配。 • nc - 字段或属性的任何部分都不能与给定的值相匹配。
步骤 4	**write memory** **示例：** `ciscoasa (config)# write memory`	保存运行配置。

手动获取证书

如要手动获取证书，请执行以下步骤：

	命令	用途
步骤 1	**crypto ca authenticate** *trustpoint* **示例：** ciscoasa(config)# crypto ca authenticate Main Enter the base 64 encoded CA certificate. End with a blank line or the word "quit" on a line by itself MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB *[certificate data omitted]* /7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ== **quit** INFO: Certificate has the following attributes: Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34 Do you accept this certificate?[yes/no]: **y** Trustpoint CA certificate accepted. % Certificate successfully imported	导入配置的信任点的 CA 证书。 **注**　此步骤假设您已从信任点所代表的 CA 获取 base-64 编码的 CA 证书。 信任点是否要求手动获取证书由配置信任点时是否使用 **enrollment terminal** 命令而定。有关详细信息，请参阅第 34-11 页的配置信任点。
步骤 2	**crypto ca enroll** *trustpoint* **示例：** ciscoasa(config)# crypto ca enroll Main % Start certificate enrollment .. % The fully-qualified domain name in the certificate will be: securityappliance.example.com % Include the device serial number in the subject name?[yes/no]: **n** Display Certificate Request to terminal?[yes/no]: **y** Certificate Request follows: MIIBoDCCAQkCAQAwIzEhMB8GCSqGSIb3DQEJAhYSRmVyYWxQaXguY2lzY28uY29t *[certificate request data omitted]* jF4waw68eOxQxVmdgMWeQ+RbIOYmvt8g6hnBTrd0GdqjjVLt ---End - This line not part of the certificate request--- Redisplay enrollment request?[yes/no]: **n**	使用信任点注册 ASA。生成用于签署数据和根据已配置的密钥类型加密数据的证书。 如果对签署和加密使用单独的 RSA 密钥，**crypto ca enroll** 命令会显示两个证书请求，每个密钥各一个。如果对签名和加密使用通用 RSA 密钥，则 **crypto ca enroll** 命令会显示一个证书请求。 如要完成注册，请从适用信任点所代表的 CA 获取由 **crypto ca enroll** 命令生成的所有证书请求的证书。确保证书是采用 base-64 格式。

	命令	用途
步骤 3	**crypto ca import** *trustpoint* **certificate** **示例：** ciscoasa (config)# crypto ca import Main certificate % The fully-qualified domain name in the certificate will be: securityappliance.example.com Enter the base 64 encoded certificate. End with a blank line or the word "quit" on a line by itself *[certificate data omitted]* quit INFO: Certificate successfully imported	导入从 CA 收到的每个证书。请求您以 base-64 格式将证书粘贴到终端上。
步骤 4	**show crypto ca server certificate** **示例：** ciscoasa(config)# show crypto ca server certificate Main	显示为 ASA 颁发的证书详细信息和信任点的 CA 证书，验证注册过程已成功。
步骤 5	**write memory** **示例：** ciscoasa(config)# write memory	保存运行配置。 对为手动注册配置的每个信任点重复上述步骤。

使用 SCEP 自动获取证书

如要使用 SCEP 自动获取证书，请执行以下步骤：

	命令	用途
步骤 1	**crypto ca authenticate** *trustpoint* **示例：** ciscoasa/contexta(config)# crypto ca authenticate Main	为配置的信任点获取 CA 证书。 **注**　此步骤假设您已从信任点所代表的 CA 获取 base-64 编码的 CA 证书。 配置信任点时，使用 **enrollment url** 命令确定是否必须通过 SCEP 自动获取证书。有关详细信息，请参阅第 34-11 页的配置信任点。
步骤 2	**crypto ca enroll** *trustpoint* **示例：** ciscoasa/contexta(config)# crypto ca enroll Main	使用信任点注册 ASA。检索用于签署数据和根据已配置的密钥类型加密数据的证书。在输入此命令前，请与 CA 管理员联系，其可能需要在 CA 授予证书之前手动对注册请求进行身份验证。 如果 ASA 未在发送证书请求后一分钟 （默认值）内从 CA 收到证书，它将重新发送证书请求。 ASA 会继续每分钟发送一次证书请求，直到收到证书。 如果为信任点配置的完全限定域名与 ASA 的完全限定域名不相同，包括字符的大小写，系统将显示一条警告。如要解决此问题，请退出注册过程，进行任何必要的更正，并重新输入 **crypto ca enroll** 命令。 **注**　如果 ASA 在您发出 **crypto ca enroll** 命令后但在您收到证书前重新启动，则重新输入 **crypto ca enroll** 命令并通知 CA 管理员。

	命令	用途
步骤 3	**show crypto ca server certificate** **示例：** `ciscoasa/contexta(config)# show crypto ca server certificate Main`	显示为 ASA 颁发的证书详细信息和信任点的 CA 证书，验证注册过程已成功。
步骤 4	**write memory** **示例：** `ciscoasa/contexta(config)# write memory`	保存运行配置。

为 SCEP 请求配置代理支持

如要使用第三方 CA 配置 ASA 以对远程访问终端进行身份验证，请执行以下步骤：

	命令	用途
步骤 1	**crypto ikev2 enable outside client-services port** *portnumber* **示例：** `ciscoasa(config-tunnel-ipsec)# crypto ikev2 enable outside client-services`	启用客户端服务。 **注**　仅在支持 IKEv2 时需要。 在隧道组 ipsec 属性配置模式中输入此命令。 默认端口号为 443。
步骤 2	**scep-enrollment enable** **示例：** `ciscoasa(config-tunnel-general)# scep-enrollment enable` `INFO: 'authentication aaa certificate' must be configured to complete setup of this option.`	为隧道组启用 SCEP 注册。 在隧道组常规属性配置模式中输入此命令。
步骤 3	**scep-forwarding-url value** *URL* **示例：** `ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/`	为组策略注册 SCEP CA。 为每个组策略输入一次此命令以支持第三方数字证书。在组策略常规属性配置模式中输入命令。 *URL* 为 CA 上的 SCEP URL。
步骤 4	**secondary-pre-fill-username clientless hide use-common-password** *password* **示例：** `ciscoasa(config)# tunnel-group remotegrp webvpn-attributes` `ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide use-common-password secret`	证书不可用于 SCEP 代理的 WebLaunch 支持时，提供公用的二级密码。 您必须使用 **hide** 关键字支持 SCEP 代理。 例如，某个证书不可用于某个请求证书的终端。终端获得证书后，AnyConnect 断开连接，然后重新连接到 ASA 以对提供内部网络资源访问权限的 DAP 策略进行限定。

	命令	用途
步骤 5	**secondary-pre-fill-username ssl-client hide use-common-password** *password* **示例：** ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide use-common-password secret	隐藏 AnyConnect VPN 会话的二级预填写用户名。 尽管从更早版本继承了 **ssl-client** 关键字，但请使用此命令支持使用 IKEv2 或 SSL 的 AnyConnect 会话。 您必须使用 **hide** 关键字支持 SCEP 代理。
步骤 6	**secondary-username-from-certificate** {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**] **示例：** ciscoasa(config-tunnel-webvpn)# secondary-username-from-certificate CN no-certificate-fallback cisco-secure-desktop machine-unique-id	证书不可用时，提供用户名。

启用本地 CA 服务器

启用本地 CA 服务器之前，必须先创建至少七个字符的密码以对包含要生成的本地 CA 证书和密钥对的 PKCS12 文件进行编码和存档。如果 CA 证书或密钥对丢失，该密码可解锁 PKCS12 档案。

如要启用本地 CA 服务器，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server** **示例：** ciscoasa (config)# crypto ca server	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**no shutdown** **示例：** ciscoasa (config-ca-server)# no shutdown	启用本地 CA 服务器。生成本地 CA 服务器证书、密钥对和必要的数据库文件，并存档本地 CA 服务器证书和密钥对以存储在 PKCS12 文件中。需要一个 8-65 个字母数字字符的密码。初始启动后，可以禁用本地 CA，无需提示输入密码。 **注**　启用本地 CA 服务器后，保存配置以确保本地 CA 证书和密钥对在重新启动后不会丢失。

示例

以下示例显示了启用本地 CA 服务器：

```
hostname (config)# crypto ca server
ciscoasa (config-ca-server)# no shutdown

% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password: caserver
```

```
Re-enter password: caserver

Keypair generation process begin.Please wait...
```

以下是显示本地 CA 服务器配置和状态的示例输出：

```
Certificate Server LOCAL-CA-SERVER:
    Status: enabled
    State: enabled
    Server's configuration is locked (enter "shutdown" to unlock it)
    Issuer name: CN=wz5520-1-16
    CA certificate fingerprint/thumbprint: (MD5)
        76dd1439 ac94fdbc 74a0a89f cb815acc
    CA certificate fingerprint/thumbprint: (SHA1)
        58754ffd 9f19f9fd b13b4b02 15b3e4be b70b5a83
    Last certificate issued serial number: 0x6
    CA certificate expiration timer: 14:25:11 UTC Jan 16 2008
    CRL NextUpdate timer: 16:09:55 UTC Jan 24 2007
    Current primary storage dir: flash:
```

配置本地 CA 服务器

如要配置本地 CA 服务器，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。生成本地 CA。
步骤 2	**smtp from-address** *e-mail_address* **示例：** `ciscoasa (config-ca-server) # smtp from-address SecurityAdmin@example.com`	指定 SMTP 发件人地址，即本地 CA 在向用户发送提供 OTP 的注册邀请邮件时用作发件人地址的有效邮件地址。
步骤 3	**subject-name-default** *dn* **示例：** `hostname (config-ca-server)# subject-name-default cn=engineer, o=asc systems, c="US"`	（可选）指定附加到已颁发证书上的每个用户名的使用者名称 DN。 使用者名称 DN 和用户名结合组成由本地 CA 服务器颁发的所有用户证书中的 DN。如果未指定使用者名称 DN，则必须在每次将用户添加到用户数据库时指定要包含在用户证书中的准确使用者名称 DN。 **注**　确保在启用配置的本地 CA 之前仔细检查所有可选参数，因为在第一次启用本地 CA 后就不能更改颁发者名称和密钥长度服务器值。

	命令	用途
步骤 4	**no shutdown** **示例：** `hostname (config-ca-server)# no shutdown`	在 ASA 上创建自签名证书并将其与本地 CA 关联。自签名证书密钥用途扩展具有密钥加密、密钥签名、 CRL 签名和证书签名功能。 **注**　在生成自签名的本地 CA 证书后，若要更改任意特征，您必须删除现有的本地 CA 服务器并完全重新创建。 本地 CA 服务器将跟踪用户证书，因此，管理员可以根据需要撤销或恢复权限。

示例

以下示例显示了如何使用所有所需参数的预定义默认值配置和启用本地 CA 服务器：

```
hostname (config)# crypto ca server
hostname (config-ca-server) # smtp from-address SecurityAdmin@example.com
hostname (config-ca-server)# subject-name-default cn=engineer, o=asc Systems, c=US
hostname (config-ca-server)# no shutdown
```

自定义本地 CA 服务器

如要自定义本地 CA 服务器，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**issuer-name** *DN-string* **示例：** `hostname (config-ca-server)# issuer-name cn=xx5520,cn=30.132.0.25,ou=DevTest,ou=QA,o=ASC Systems`	指定没有默认值的参数。
步骤 3	**smtp subject** *subject-line* **示例：** `hostname (config-ca-server) # smtp subject Priority E-Mail: Enclosed Confidential Information is Required for Enrollment`	自定义显示在从本地 CA 服务器发送的所有邮件的主题字段中的文本
步骤 4	**smtp from-address** *e-mail_address* **示例：** `hostname (config-ca-server) # smtp from-address SecurityAdmin@example.com`	**指定**要用作由本地 CA 服务器生成的所有邮件的发件人字段的邮件地址。

	命令	用途
步骤 5	**subject-name-default** *dn* **示例：** `hostname (config-ca-server) # subject-name default cn=engineer, o=ASC Systems, c=US`	指定要附加到已颁发证书上的某个用户名的可选使用者名称 DN。默认使用者名称 DN 变成了由本地 CA 服务器颁发的所有用户证书中的用户名的一部分。 允许 DN 属性关键字如下所示： • C = 国家/地区 • CN= 公用名称 • EA = 邮件地址 • L = 地区 • O = 组织名称 • OU = 组织单位 • ST = 州/省 • SN = 姓氏 • ST = 州/省 **注**　如果未指定 subject-name-default 作为标准使用者名称默认值，则必须在每次添加用户时指定 DN。

调试本地 CA 服务器

如要调试新配置的本地 CA 服务器，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**debug crypto ca server** **示例：** `ciscoasa (config-ca-server)# debug crypto ca server`	配置和启用本地 CA 服务器时，显示调试消息。执行 1 级调试功能；有 1-255 个级别可用。 **注**　调试命令可能会减缓繁忙网络上的流量。5 级或更高级别的调试应为原始数据转储而预留，但由于过多输出，应在正常调试过程中避免这些级别的调试。

禁用本地 CA 服务器

如要禁用本地 CA 服务器，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**shutdown** **示例：** `ciscoasa (config-ca-server)# shutdown` `INFO: Local CA Server has been shutdown.`	禁用本地 CA 服务器。禁用网站注册并允许您修改本地 CA 服务器配置。存储当前配置及关联文件。初始启动后，可以重新启用本地 CA，无需提示输入密码。

删除本地 CA 服务器

如要删除现有的本地 CA 服务器 （已启用或禁用），请输入以下其中一个命令：

命令	用途
执行以下操作之一：	
no crypto ca server **示例：** `ciscoasa (config)# no crypto ca server`	移除现有的本地 CA 服务器 （已启用或禁用）。 **注**　删除本地 CA 服务器将会从 ASA 中移除配置。配置删除后，将无法恢复。
clear configure crypto ca server **示例：** `ciscoasa (config)# clear config crypto ca server`	确保同时删除了关联的本地 CA 服务器数据库和配置文件（即，带通配符名称 LOCAL-CA-SERVER* 的所有文件）。

配置本地 CA 证书特征

您可以配置本地 CA 证书的以下特征：

- 显示在所有用户证书上的证书颁发者的名称。
- 本地 CA 证书 （服务器与用户）和 CRL 的有效期。
- 与本地 CA 和用户证书关联的公钥和私钥密钥对的长度。

- 第 34-25 页的配置颁发者名称
- 第 34-25 页的配置 CA 证书有效期
- 第 34-26 页的配置用户证书有效期
- 第 34-26 页的配置 CRL 有效期
- 第 34-27 页的配置服务器密钥长度
- 第 34-28 页的设置外部本地 CA 文件存储

- 第 34-29 页的下载 CRL
- 第 34-29 页的存储 CRL
- 第 34-30 页的设置注册参数
- 第 34-31 页的添加和注册用户
- 第 34-32 页的续订用户
- 第 34-32 页的恢复用户
- 第 34-33 页的移除用户
- 第 34-33 页的撤销证书
- 第 34-33 页的维护本地 CA 证书数据库
- 第 34-34 页的滚动更新本地 CA 证书
- 第 34-34 页的存档本地 CA 服务器证书和密钥对

配置颁发者名称

如要配置证书颁发者名称，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**issuer-name** *DN-string* **示例：** `hostname (config-ca-server)# issuer-name CN=xx5520,CN=30.132.0.25,ou=DevTest,ou=QA,O=ABC Systems`	指定本地 CA 证书使用者名称。配置的证书颁发者名称既是自签名本地 CA 证书的使用者名称和颁发者名称，也是所有颁发的客户端证书和颁发的 CRL 中的颁发者名称。本地 CA 中的默认颁发者名称的格式为 *hostname.domainname*。 **注**　您无法在先启用本地 CA 后更改颁发者名称值。

配置 CA 证书有效期

如要配置本地 CA 服务器证书有效期，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**lifetime ca-certificate** *time* **示例：** `hostname (config-ca-server)# lifetime ca-certificate 365`	确定包含在证书中的到期日期。本地 CA 证书的默认有效期是三年。 确保将证书的有效期限制为不超过建议的结束日期，2038 年 1 月 19 日凌晨 3:14:08 (UTC)。

	命令	用途
步骤 3	**no lifetime ca-certificate** **示例：** `hostname (config-ca-server)# no lifetime ca-certificate`	（可选）将本地 CA 证书的有效期重置为默认值三年。 本地 CA 服务器会在证书到期前 30 天自动生成一个替代 CA 证书，这可让替代证书导出和导入到任何其他设备，以在当前的本地 CA 证书过期后对由本地 CA 证书颁发的用户证书进行验证。系统将生成以下到期前系统日志消息： `%ASA-1-717049: Local CA Server certificate is due to expire in days and a replacement certificate is available for export.` **注**　在收到此自动滚动更新通知后，管理员必须确保新的本地 CA 证书在到期前已导入到所有所需的设备上。

配置用户证书有效期

如要配置用户证书有效期，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**lifetime certificate** *time* **示例：** `hostname (config-ca-server)# lifetime certificate 60`	设置要让用户证书保持有效的时间长度。 **注**　用户证书到期之前，本地 CA 服务器将自动启动证书续订处理，在证书到期日期前几天向用户授予注册权限，设置续订提醒，并发送包含用于证书续订的注册用户名和 OTP 的邮件。确保将证书的有效期限制为不超过建议的结束日期，2038 年 1 月 19 日凌晨 3:14:08 (UTC)。

配置 CRL 有效期

如要配置 CRL 有效期，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**lifetime crl** *time* **示例：** `hostname (config-ca-server)# lifetime crl 10`	设置要让 CRL 保持有效的时间长度。 本地 CA 将在每次撤销或取消撤销用户证书时更新和重新颁发 CRL，但如果未发生撤销变更，则会在每个 CRL 有效期后自动重新颁发一次 CRL。如果未指定 CRL 有效期，默认有效期为六小时。

	命令	用途
步骤 3	**crypto ca server crl issue** **示例：** ciscoasa(config)# crypto ca server crl issue 新的 CRL 已颁发。	可随时强制颁发 CRL，这会立即更新和重新生成当前的 CRL，用以覆盖现有的 CRL。 **注**　除非 CRL 文件被错误地移除或已损坏，必须重新生成，否则请不要使用此命令。

配置服务器密钥长度

如要配置服务器密钥长度，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server** **示例：** ciscoasa (config)# crypto ca server	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**keysize server** **示例：** hostname (config-ca-server)# keysize server 2048	指定在进行用户证书注册时生成的公钥和私钥的长度。密钥对长度选项包括 512、768、1024、2048 位，默认值是 1024 位。 **注**　在启用本地 CA 后，无法更改本地 CA 密钥长度，否则所有已颁发的证书将无效。要更改本地 CA 密钥长度，必须删除当前的本地 CA 并重新配置新的本地 CA。

示例

以下是显示数据库中的两个用户证书的示例输出。

```
Username: user1
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 12:45:52 UTC Fri Jan 4 2017
Certificates Issued:
serial:   0x71
issued:   12:45:52 UTC Thu Jan 3 2008
expired:  12:17:37 UTC Sun Dec 31 2017
status:   Not Revoked
Username: user2
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 12:27:59 UTC Fri Jan 4 2008
Certificates Issued:
serial:   0x2
issued:   12:27:59 UTC Thu Jan 3 2008
expired:  12:17:37 UTC Sun Dec 31 2017
status:   Not Revoked
<--- More --->
```

设置外部本地 CA 文件存储

您可以将本地 CA 服务器配置、用户、已颁发的证书和 CRL 存储在闪存或外部本地 CA 文件系统中的本地 CA 服务器数据库中。如要配置外部本地 CA 文件存储，请执行以下步骤：

	命令	用途
步骤 1	**mount** *name* **type** **示例：** `hostname (config)# mount mydata type cifs`	访问特定文件系统类型的配置模式。
步骤 2	**mount** *name* **type cifs** **示例：** `hostname (config-mount-cifs)# mount mydata type cifs` `server 10.1.1.10 share myshare` `domain example.com` `username user6` `password ********` `status enable`	安装 CIFS 文件系统。 **注**　只有安装文件系统的用户才能使用 **no mount** 命令卸载该文件系统。
步骤 3	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 4	**database path** *mount-name directory-path* **示例：** `hostname (config-ca-server)# database path mydata:newuser`	指定 *mydata*（用于本地 CA 服务器数据库的预安装 CIFS 文件系统）的位置。建立服务器路径，然后指定用于存储和检索的本地 CA 文件或文件夹名称。如要将本地 CA 文件存储返回到 ASA 闪存，请使用 **no database path** 命令。 **注**　如要保护存储在外部服务器上的本地 CA 文件，需要受到用户名和密码保护的 CIFS 或 FTP 文件类型的预安装文件系统。
步骤 5	**write memory** **示例：** `ciscoasa (config)# write memory`	保存运行配置。 对于外部本地 CA 文件存储，每次保存 ASA 配置时，用户信息都将从 ASA 保存到预安装的文件系统和文件位置 *mydata:newuser*。 对于闪存存储，用户信息将自动保存到启动配置的默认位置。

示例

以下示例显示了在闪存或外部存储器中显示的本地 CA 文件列表：

```
ciscoasa (config-ca-server)# dir LOCAL* //
Directory of disk0:/LOCAL*

75      -rwx  32          13:07:49 Jan 20 2007  LOCAL-CA-SERVER.ser
77      -rwx  229         13:07:49 Jan 20 2007  LOCAL-CA-SERVER.cdb
69      -rwx  0           01:09:28 Jan 20 2007  LOCAL-CA-SERVER.udb
81      -rwx  232         19:09:10 Jan 20 2007  LOCAL-CA-SERVER.crl
72      -rwx  1603        01:09:28 Jan 20 2007  LOCAL-CA-SERVER.p12

127119360 bytes total (79693824 bytes free)
```

下载 CRL

如要让 CRL 可用于在给定接口或端口上进行 HTTP 下载，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**publish-crl interface** *interface* **port** *portnumber* **示例：** `hostname (config-ca-server)# publish-crl outside 70`	打开接口上的端口，以便可从该接口访问 CRL。指定的接口和端口用于侦听 CRL 的传入请求。接口和可选端口选择如下所示： • 内部 - 接口名称/GigabitEthernet0/1 • 管理 - 接口名称/Management0/0 • 外部 - 接口名称/GigabitEthernet0/0 • 端口号范围是 1-65535。TCP 端口 80 是 HTTP 默认端口号。 **注**　如果未指定此命令，则不可从 CDP 位置访问 CRL，因为需要此命令才能打开接口下载 CRL 文件。 可以配置 CDP URL 使用接口的 IP 地址，并且还可以配置 CDP URL 的路径和文件名 （例如，http://10.10.10.100/user8/my_crl_file）。 在这种情况下，只有配置了该 IP 地址的接口才会侦听 CRL 请求，请求传入时，ASA 会将路径 /user8/my_crl_file 与配置的 CDP URL 进行匹配。如果路径匹配，ASA 将返回存储的 CRL 文件。 **注**　协议必须是 HTTP，因此，显示的前缀是 http://。

存储 CRL

如要为本地 CA 的自动生成 CRL 建立特定位置，请以单情景或多情景模式执行以下站点到站点的任务:

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。

	命令	用途
步骤 2	**cdp-url** *url* **示例：** `ciscoasa(config-ca-server)# cdp-url http://172.16.1.1/pathname/myca.crl`	指定要包含在所有已颁发证书中的 CDP。如果未配置 CDP 的特定位置，则默认 URL 位置是 http://*hostname.domain*/+CSCOCA+/asa_ca.crl。 本地 CA 将在每次撤销或取消撤销用户证书时更新和重新颁发 CRL。如果未发生撤销变更，则会在每个 CRL 有效期后重新颁发一次 CRL。 如果此命令设置为直接从本地 CA ASA 对 CRL 起作用，请参阅第 34-29 页的下载 CRL以了解有关**打**开接口上的端口以便可从该接口访问 CRL 的说明。 其他设备也存在 CRL，用以验证由本地 CA 颁发的证书的撤销情况。此外，本地 CA 会跟踪它自己的证书数据库中的所有已颁发证书和状态。验证方需要通过从外部服务器（可能是颁发证书的 CA 或 CA 指定的服务器）检索撤销状态来验证用户证书时，将执行撤销检查。

设置注册参数

如要设置注册参数，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**otp expiration** *timeout* **示例：** `ciscoasa(config-ca-server)# otp expiration 24`	指定已签发用于本地 CA 注册页面的 OTP 保持有效的小时数。默认到期时间为 72 小时。 **注**　用于在注册网站上注册证书的用户 OTP 还用作用于解锁包含指定用户的已颁发证书和密钥对的 PKCS12 文件的密码。
步骤 3	**enrollment-retrieval** *timeout* **示例：** `ciscoasa(config-ca-server)# enrollment-retrieval 120`	指定已注册的用户可以检索 PKCS12 注册文件的小时数。此时间从用户注册成功时开始计算。默认检索期为 24 小时。检索期的有效值范围为 1 至 720 小时。注册检索期与 OTP 有效期无关。 注册检索时间到期后，用户证书和密钥对不再可用。用户可收到证书的唯一方法是，让管理员重新初始化证书注册并允许用户重新登录。

添加和注册用户

如要添加有资格在本地 CA 数据库注册的用户，请执行以下命令：

	命令	用途
步骤 1	**crypto ca server user-db add** *username* [**dn** *dn*] [**email** *emailaddress*] **示例：** `hostname (config-ca-server)# crypto ca server user-db add user1 dn user1@example.com, Engineer, Example Company, US, email user1@example.com`	将新用户添加到本地 CA 数据库。选项如下所示： • *username* - 一个包含 4-64 个字符的字符串，是正在添加的用户的简单用户名。用户名可以是邮件地址，之后可根据需要将其用于联系用户进行注册邀请。 • *dn* - 可分辨名称，OSI 目录 (X.500) 中某个条目的全局权威名称（例如，cn=user1@example.com、cn=Engineer、o=Example Company、c=US）。 • *e-mail-address* - 要向其发送 OTP 和通知的新用户的邮件地址。
步骤 2	**crypto ca server user-db allow** *user* **示例：** `hostname (config-ca-server)# crypto ca server user-db allow user6`	向新添加的用户提供用户权限。
步骤 3	**crypto ca server user-db email-otp** *username* **示例：** `hostname (config-ca-server)# crypto ca server user-db email-otp exampleuser1`	通知本地 CA 数据库中的用户注册和下载用户证书，自动将 OTP 电邮给用户。 **注**　管理员希望通过邮件通知用户时，必须在添加该用户时在用户名字段或邮件地址字段指定邮件地址。
步骤 4	**crypto ca server user-db show-otp** **示例：** `hostname (config-ca-server)# crypto ca server user-db show-otp`	显示已签发的 OTP。
步骤 5	**otp expiration** *timeout* **示例：** `hostname (config-ca-server)# otp expiration 24`	设置注册时间限制 （以小时为单位）。默认到期时间为 72 小时。 **otp expiration** 命令定义了 OTP 对用户注册有效的时间。此时间从允许用户注册时开始计算。 用户在该时间限制内使用正确的 OTP 注册成功后，本地 CA 服务器将创建一个 PKCS12 文件，其中包含用户的密钥对和用户证书，该证书是基于生成的密钥对中的公钥和添加用户时指定的使用者名称 DN。PKCS12 文件内容受密码（即，OTP）保护。OTP 可以手动处理，本地 CA 也可以通过邮件将此文件发送给用户以在管理员允许注册后进行下载。 PKCS12 文件以名称 *username.p12* 保存到临时存储器中。存储 PKCS12 文件后，用户可以在注册检索时间内返回以根据需要多次下载 PKCS12 文件。此时间到期后，PKCS12 文件将自动从存储器中移除且不再可供下载。 **注**　如果注册期在用户检索包含用户证书的 PKCS12 文件前到期，则不允许注册。

续订用户

如要指定续订通知的时间，请执行以下步骤：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**renewal-reminder** *time* **示例：** `ciscoasa (config-ca-server)# renewal-reminder 7`	指定初次向证书所有者发送重新注册提醒时距本地 CA 证书到期的天数 (1-90)。如果证书到期，它将无效。 续订通知及将通知电邮给用户的时间是可变的，并且可以由管理员在本地 CA 服务器配置过程中进行配置。 系统将发送三封提醒邮件。如果在用户数据库中指定了邮件地址，将针对每个提醒向证书所有者自动发送一封邮件。如果用户不存在邮件地址，系统日志消息将向您通报续订要求。 ASA 将自动向任何持有即将到期的有效证书的用户授予证书续订权限，只要这些用户仍存在于用户数据库中。因此，如果管理员不想让某用户自动续订，必须在续订时间之前从数据库中移除该用户。

恢复用户

如要恢复用户和由本地 CA 服务器颁发的、之前已撤销的证书，请执行以下步骤：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**crypto ca server unrevoke** *cert-serial-no* **示例：** `ciscoasa (config)# crypto ca server unrevoke 782ea09f`	恢复用户和取消撤销由本地 CA 服务器颁发的之前已撤销的证书。 本地 CA 保留当前的 CRL 和所有已撤销的用户证书的序列号。此列表可供外部设备使用并可直接从本地 CA 检索，只要使用 **cdp-url** 命令和 **publish-crl** 命令进行此类配置即可。按证书序列号撤销（或取消撤销）任意当前证书时，CRL 将自动反映这些更改。

移除用户

如要按用户名从用户数据库删除用户，请执行以下步骤：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**crypto ca server user-db remove** *username* **示例：** `ciscoasa (config)# crypto ca server user-db remove user1`	从用户数据库移除用户并允许撤销已颁发给用户的任意有效证书。

撤销证书

如要撤销用户证书，请执行以下步骤：

	命令	用途
步骤 1	**crypto ca server** **示例：** `ciscoasa (config)# crypto ca server`	进入 local ca server 配置模式。允许您配置和管理本地 CA。
步骤 2	**crypto ca server revoke** *cert-serial-no* **示例：** `ciscoasa (config-ca-server)# crypto ca server revoke 782ea09f`	输入十六进制格式的证书序列号。在本地 CA 服务器上的证书数据库中和 CRL（将自动重新颁发）中将证书标记为“已撤销”。 **注**　如果 ASA 的证书需要撤销，则还需要密码，因此，确保您记录密码并将它存储在安全的位置。

维护本地 CA 证书数据库

如要维护本地 CA 证书数据库，请确保在每次更改数据库时使用 **write memory** 命令保存证书数据库文件 LOCAL-CA-SERVER.cdb。本地 CA 证书数据库包含以下文件：

- LOCAL-CA-SERVER.p12 文件是在最初启用本地 CA 服务器时生成的本地 CA 证书和密钥对的档案。
- LOCAL-CA-SERVER.crl 文件是实际的 CRL。
- LOCAL-CA-SERVER.ser 文件记录了已颁发证书的序列号。

滚动更新本地 CA 证书

本地 CA 证书到期前三十天，系统会生成一个滚动更新替代证书，并且系统日志消息将通知管理员该进行本地 CA 滚动更新了。新的本地 CA 证书必须在当前证书到期前导入到所有所需的设备上。如果管理员未通过将滚动更新证书安装为新的本地 CA 证书做出回应，验证可能会失败。

本地 CA 证书将在到期后使用相同的密钥对自动滚动更新。滚动更新证书可使用 base 64 格式导出。

示例

以下示例显示了 base 64 编码的本地 CA 证书：

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHAYJKo
ZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3SDOiDwZG9
n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZTS1E4L0fSaC3
uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZPrzoG1J8BFqdPa1j
BGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYYbP86tvbZ2yOVZR6aKFVI
0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmuBeGDKOncTknfgy0XM+fG5rb3
qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

存档本地 CA 服务器证书和密钥对

如要存档本地 CA 服务器证书和密钥对，请输入以下命令：

命令	用途
copy **示例：** `hostname# copy LOCAL-CA-SERVER_0001.pl2 tftp://10.1.1.22/user6/`	使用 FTP 或 TFTP 从 ASA 复制本地 CA 服务器证书和密钥对，以及所有文件。 **注**　确保尽可能经常地备份所有本地 CA 文件。

监控数字证书

如要显示证书配置和数据库信息，请输入以下其中一个或多个命令：

命令	用途
show crypto ca server	显示本地 CA 配置和状态。
show crypto ca server cert-db	显示本地 CA 颁发的用户证书。
show crypto ca server certificate	显示控制台上的 base 64 格式的本地 CA 证书和滚动更新证书 （如可用），包括滚动更新证书指纹以在导入到其他设备时验证新证书。
show crypto ca server crl	显示 CRL。

命令	用途
show crypto ca server user-db	显示用户及其状态，可与以下限定符配合使用来减少显示的记录数： • allowed.仅显示当前允许注册的用户。 • enrolled.仅显示已注册并具有有效证书的用户。 • expired.仅显示持有过期证书的用户。 • on-hold.仅列出无证书且当前不允许注册的用户。
show crypto ca server user-db allowed	显示有资格注册的用户。
show crypto ca server user-db enrolled	显示具有有效证书的已注册用户。
show crypto ca server user-db expired	显示具有过期证书的用户。
show crypto ca server user-db on-hold	显示无证书且不允许注册的用户。
show crypto key *name of key*	显示已生成的密钥对。
show running-config	显示本地 CA 证书映射规则。

示例

以下示例显示了 RSA 通用密钥：

```
ciscoasa/contexta(config)# show crypto key mypubkey
Key pair was generated at: 16:39:47 central Feb 10 2010
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 1024
 Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ea51b7
  0781848f 78bccac2 4a1b5b8d 2f3e30b4 4cae9f86 f4485207 159108c9 f5e49103
  9eeb0f5d 45fd1811 3b4aafce 292b3b64 b4124a6f 7a777b08 75b88df1 8092a9f8
  5508e9e5 2c271245 7fd1c0c3 3aaf1e04 c7c4efa4 600f4c4a 6afe56ad c1d2c01c
  e08407dd 45d9e36e 8cc0bfef 14f9e6ac eca141e4 276d7358 f7f50d13 79020301 0001
Key pair was generated at: 16:34:54 central Feb 10 2010
```

以下示例显示了本地 CA CRL：

```
hostname (config)# show crypto ca server crl
Certificate Revocation List:
    Issuer: cn=xx5520-1-3-2007-1
    This Update: 13:32:53 UTC Jan 4 2010
    Next Update: 13:32:53 UTC Feb 3 2010
    Number of CRL entries: 2
    CRL size: 270 bytes
Revoked Certificates:
    Serial Number: 0x6f
    Revocation Date: 12:30:01 UTC Jan 4 2010
    Serial Number: 0x47
    Revocation Date: 13:32:48 UTC Jan 4 2010
```

以下示例显示了一个暂停用户：

```
hostname (config)# show crypto ca server user-db on-hold
username: wilma101
email:    <None>
dn:       <None>
allowed:  <not allowed>
notified: 0
hostname (config)#
```

以下示例显示了 **show running-config** 命令的输出，其中将显示本地 CA 证书映射规则：

```
crypto ca certificate map 1
 issuer-name co asc
 subject-name attr ou eq Engineering
```

证书管理的功能历史

表 34-1　　证书管理的功能历史

功能名称	平台版本	功能信息
证书管理	7.0(1)	数字证书（包括 CA 证书、身份证书和代码签名证书）是一种用于身份验证的数字识别方式。数字证书包括识别设备或用户的信息，如名称、序列号、公司、部门或 IP 地址。CA 是“签署”证书以验证其真实性，从而确保设备或用户的身份的可信颁发机构。CA 在 PKI（使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。
证书管理	7.2(1)	我们引入了以下命令： **issuer-name** *DN-string*、 **revocation-check crl none**、**revocation-check crl**、 **revocation-check none**。 我们废弃了以下命令：**crl** {**required** | **optional** | **nocheck**}。

表 34-1　　证书管理的功能历史（续）

功能名称	平台版本	功能信息
证书管理	8.0(2)	我们引入了以下命令： **cdp-url**、 **crypto ca server**、 **crypto ca server crl issue**、 **crypto ca server revoke** *cert-serial-no*、**crypto ca server unrevoke** *cert-serial-no*、 **crypto ca server user-db add** *user* [**dn** *dn*] [**email** *e-mail-address*]、 **crypto ca server user-db allow** {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**]、 **crypto ca server user-db email-otp** {*username* | **all-unenrolled** | **all-certholders**}、 **crypto ca server user-db remove** *username*、 **crypto ca server user-db show-otp** {*username* | **all-certholders** | **all-unenrolled**}、 **crypto ca server user-db write**、 **[no] database path** *mount-name directory-path*、 **debug crypto ca server** [*level*]、 **lifetime {ca-certificate | certificate | crl}** *time*、 no shutdown、 **otp expiration** *timeout*、 **renewal-reminder** *time*、 **show crypto ca server**、 **show crypto ca server cert-db [user** *username* **| allowed | enrolled | expired | on-hold] [serial** *certificate-serial-number*]、 **show crypto ca server certificate**、**show crypto ca server crl**、**show crypto ca server user-db** [**expired | allowed | on-hold | enrolled**]、 **show crypto key** *name of key*、 **show running-config**、 **shutdown**。
SCEP 代理	8.4(1)	我们引入此此功能，可从第三方 CA 对设备证书进行安全部署。 我们引入了以下命令： **crypto ikev2 enable outside client-services port** *portnumber*、 **scep-enrollment enable**、 **scep-forwarding-url value** *URL*、 **secondary-pre-fill-username clientless hide use-common-password** *password*、 **secondary-pre-fill-username ssl-client hide use-common-password** *password*、 **secondary-username-from-certificate** {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]。

第 8 部分

系统管理

管理访问

本章介绍如何通过 Telnet、SSH 和 HTTPS（使用 ASDM）访问思科 ASA 进行系统管理、如何对用户进行身份验证和授权以及如何创建登录横幅。

- 第 35-1 页的配置 ASDM、 Telnet 或 SSH 的 ASA 访问
- 第 35-6 页的配置 CLI 参数
- 第 35-9 页的配置 VPN 隧道上的管理访问
- 第 35-10 页的配置系统管理员 AAA
- 第 35-30 页的管理访问的功能历史记录

注 如要访问 ASA 接口进行管理访问，您也不需要允许主机 IP 地址的访问规则，只需根据本章内各节配置管理访问。

配置 ASDM、 Telnet 或 SSH 的 ASA 访问

本节介绍如何使客户端使用 ASDM、 Telnet 或 SSH 访问 ASA。

- 第 35-2 页的 ASDM、 Telnet 或 SSH 的 ASA 访问许可要求
- 第 35-2 页的准则和限制
- 第 35-3 页的配置 Telnet 访问
- 第 35-3 页的使用 Telnet 客户端
- 第 35-4 页的配置 SSH 访问
- 第 35-5 页的使用 SSH 客户端
- 第 35-5 页的配置 ASDM 的 HTTPS 访问

ASDM、 Telnet 或 SSH 的 ASA 访问许可要求

下表显示此功能的许可要求：

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

IPv6 准则

支持 IPv6。

型号准则

对于 ASASM，从交换机到 ASASM 的会话是 Telnet 会话，但是，不要求根据本节进行 Telnet 访问配置。

其他指导原则

- 除非使用 VPN 隧道中的 Telnet，否则，无法使用 Telnet 登录到最低安全接口。
- 不支持对进入 ASA 时所经由的接口以外的接口进行管理访问。例如，如果管理主机位于外部接口上，则只能发起直接到外部接口的管理连接。此规则的唯一例外是通过 VPN 连接。请参阅第 35-9 页的配置 VPN 隧道上的管理访问。
- ASA 允许：
  - 每个情景最多 5 个并发 Telnet 连接，在所有情景中最多分为 100 个连接 （如果有）。
  - 每个情景最多 5 个并发 SSH 连接，在所有情景中最多分为 100 个连接 （如果有）。
  - 每个情景最多 5 个并发 ASDM 连接，在所有情景中最多分为 32 个 ASDM 实例（如果有）。
- ASA 支持 SSH 第 1 版和第 2 版中提供的 SSH 远程外壳程序功能，并支持 DES 和 3DES 加密。
- 不支持通过 SSL 和 SSH 进行 XML 管理。
- （8.4 及更高版本）不再支持 SSH 默认用户名。使用 SSH 以及 **pix** 或 **asa** 用户名和登录密码 无法再连接至 ASA。要使用 SSH，必须使用 **aaa authentication ssh console LOCAL** 命令配置 AAA 身份验证；然后，通过输入 **username** 命令。如果要使用 AAA 服务器而不是本地数据库进行身份验证，我们建议也将本地身份验证配置为备用方法。
- （9.1(2) 及更高版本）已移除默认 Telnet 登录密码；使用 Telnet 前必须手动设置密码。请参阅第 13-1 页的设置主机名、域名及启用和 Telnet 密码。

- 如果无法建立到 ASA 接口的 Telnet 或 SSH 连接，请确保已根据第 35-1 页的配置 ASDM、Telnet 或 SSH 的 ASA 访问中的说明启用到 ASA 的 Telnet 或 SSH。

配置 Telnet 访问

如要识别允许使用 Telnet 连接 ASA 的客户端 IP 地址，请执行以下步骤。

详细步骤

	命令	用途
步骤 1	**telnet** *source_IP_address mask source_interface* **示例：** `ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside`	对于每个地址或子网，识别 ASA 从其接受连接的 IP 地址。 如果只有一个接口，只要接口的安全级别为 100，您就可以配置 Telnet 以访问该接口。
步骤 2	**telnet timeout** *minutes* **示例：** `ciscoasa(config)# telnet timeout 30`	设置在 ASA 断开 Telnet 会话之前，会话可空闲的持续时间。 设置超时时间，范围为 1 到 1440 分钟。默认值为 5 分钟。在大多数情况下，默认持续时间都太短，应增加为直到完成所有前期测试和故障排除所需的时间。

示例

以下示例显示如何使内部接口上且地址为 192.168.1.2 的主机访问 ASA：

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

以下示例显示如何使 192.168.3.0 网络上的所有用户可以访问内部接口上的 ASA：

```
ciscoasa(config)# telnet 192.168.3.0 255.255.255.0 inside
```

使用 Telnet 客户端

如要使用 Telnet 访问 ASA CLI，请输入通过 **password** 命令设置的登录密码。使用 Telnet 前必须手动设置该密码。请参阅第 13-1 页的设置主机名、域名及启用和 Telnet 密码。

如果配置 Telnet 身份验证 （请参阅第 35-15 页的配置 CLIASDM 和 命令访问的身份验证），则请输入通过 AAA 服务器或本地数据库定义的用户名和密码。

配置 SSH 访问

如要识别客户端 IP 地址并定义允许使用 SSH 连接 ASA 的用户，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**crypto key generate rsa modulus** *modulus_size* **示例：** `ciscoasa(config)# crypto key generate rsa modulus 1024`	生成 SSH 必需的 RSA 密钥对 （仅适用于物理 ASA）。 **注**　对于 ASAv，会在部署后自动创建 RSA 密钥对。 模块值 （单位：位）是 512、 768、 1024 或 2048。指定的密钥模块大小越大，生成 RSA 密钥对所需的时间就越长。建议值为 1024。
步骤 2	**write memory** **示例：** `ciscoasa(config)# write memory`	将 RSA 密钥保存到永久性闪存中。
步骤 3	**aaa authentication ssh console LOCAL**	启用本地身份验证进行 SSH 访问。或者，可以使用 AAA 服务器配置身份验证。有关详细信息，请参阅第 35-15 页的配置 CLIASDM 和 命令访问的身份验证。
步骤 4	**username** *username* **password** *password*	在可用于 SSH 访问的本地数据库中创建用户。
步骤 5	**ssh** *source_IP_address mask source_interface* **示例：** `ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside`	对于每个地址或子网，识别 ASA 从其接受连接的 IP 地址和在其上可以使用 SSH 的接口。与 Telnet 不同，您可以在最低安全级别的接口上使用 SSH。
步骤 6	**ssh timeout** *minutes* **示例：** `ciscoasa(config)# ssh timeout 30`	（可选）设置在 ASA 断开 SSH 会话之前，该会话可空闲的持续时间。 设置超时时间，范围为 1 到 60 分钟。默认值为 5 分钟。在大多数情况下，默认持续时间都太短，应增加为直到完成所有前期测试和故障排除所需的时间。
步骤 7	**ssh version** *version_number* **示例：** `ciscoasa(config)# ssh version 2`	（可选）限制对 SSH 第 1 版或第 2 版的访问。默认情况下，SSH 支持第 1 版和第 2 版。

示例

以下示例显示如何生成 RAS 密钥并使在内部接口上且地址为 192.168.1.2 的主机访问 ASA：

```
ciscoasa(config)# crypto key generate rsa modulus 1024
ciscoasa(config)# write memory
ciscoasa(config)# aaa authentication ssh console LOCAL
WARNING: local database is empty! Use 'username' command to define local users.
ciscoasa(config)# username exampleuser1 password examplepassword1
ciscoasa(config)# ssh 192.168.1.2 255.255.255.255 inside
ciscoasa(config)# ssh timeout 30
```

以下示例显示如何使 192.168.3.0/24 网络上的所有用户可以访问内部接口上的 ASA：

```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

使用 SSH 客户端

在管理主机上的 SSH 客户端中输入已在第 35-4 页的配置 SSH 访问中配置的用户名和密码。当启动 SSH 会话时，系统将在 ASA 控制台上显示圆点 (.)，然后显示以下 SSH 用户身份验证提示符：

```
ciscoasa(config)#.
```

显示这个圆点不会影响 SSH 的功能。在用户身份验证发生之前的 SSH 密钥交换过程中，正在生成服务器密钥或正在使用私有密钥解密消息时，系统在控制台上显示这个圆点。完成这些任务可能需要两分钟或更长的时间。圆点是验证 ASA 繁忙和未暂停的进度指示器。

或者，可以配置公用密钥而不是使用密码。请参阅第 27-3 页的向本地数据库添加用户帐户。

配置 ASDM 的 HTTPS 访问

如要使用 ASDM，则需要启用 HTTPS 服务器，并允许至 ASA 的 HTTPS 连接。HTTPS 访问已作为出厂默认配置的一部分而启用，或者在使用 **setup** 命令时启用。本节介绍如何手动配置 ASDM 访问。

详细步骤

	命令	用途
步骤 1	**http** *source_IP_address mask source_interface* **示例：** `ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside`	对于每个地址或子网，识别 ASA 从其接受 HTTPS 连接的 IP 地址。
步骤 2	**http server enable** [*port*] **示例：** `ciscoasa(config)# http server enable 443`	启用 HTTPS 服务器。 默认情况下，*port* 为 443。如果更改端口号，请务必将其包括在 ASDM 访问 URL 中。例如，如果将端口号更改为 444，请输入以下信息： **https://10.1.1.1:444**
步骤 3	**http redirect** *interface* [*port*] **示例：** `ciscoasa(config)# http redirect inside`	（可选）将 HTTP 请求重定向至 HTTPS 请求。这就使得用户可以在 ASDM URL 中输入“http://”进入 https URL，而不会出现错误。

示例

以下示例显示如何启用 HTTPS 服务器并使在内部接口上且地址为 192.168.1.2 的主机访问 ASDM：

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

以下示例显示如何使 192.168.3.0/24 网络上的所有用户可以访问内部接口上的 ASDM：

```
ciscoasa(config)# http 192.168.3.0 255.255.255.0 inside
```

配置 CLI 参数

- 第 35-6 页的CLI 参数许可要求
- 第 35-6 页的准则和限制
- 第 35-6 页的配置登录横幅
- 第 35-7 页的自定义 CLI 提示符
- 第 35-8 页的更改控制台超时

CLI 参数许可要求

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

配置登录横幅

您可以配置在用户连接至 ASA 时、在用户登录之前或在用户进入特权 EXEC 模式之前将显示的消息。

限制

在添加横幅后，如果有以下情况，可能关闭至 ASA 的Telnet 或 SSH 会话：

- 没有足够的系统内存可用来处理横幅消息。
- 在尝试显示横幅消息时发生 TCP 写入错误。

准则

- 从安全角度来看，重要的是横幅阻止未经授权的访问。请勿使用“欢迎”或“请”，因为它们看起来似乎是在邀请入侵者进入。以下横幅设置对未经授权访问的正确语调：

  您已登录到安全设备。如果您无权访问此设备，请立即注销，否则可能有犯罪的风险。

- 有关横幅消息的准则，请参阅 RFC 2196。

如要配置登录横幅，请执行以下步骤：

详细步骤

命令	用途
banner {**exec** | **login** | **motd**} *text* **示例：** `ciscoasa(config)# banner motd Welcome to $(hostname).`	添加在以下三个时间之一要显示的横幅：在用户首次连接时 (message-of-the-day (**motd**))，在用户登录时 (**login**)，以及在用户访问特权 EXEC 模式时 (**exec**)。当用户连接 ASA 时，系统首先显示 message-of-the-day 横幅，然后显示 login 横幅和提示符。在用户成功登录 ASA 后，系统将显示 exec 横幅。 要添加一行以上，请将 **banner** 命令放在每行之前。 对于横幅文本： • 允许空格，但使用 CLI 时无法输入制表符。 • 除了 RAM 和闪存对横幅长度的限制外，无其他长度限制。 • 通过包含字符串 **$(hostname)** 和 **$(domain)**，可以动态添加 ASA 的主机名或域名。 • 如果在系统配置中配置横幅，可以通过在情景配置中使用 **$(system)** 字符串来在情景中使用该横幅文本。

示例

以下示例显示如何添加 message-of-the-day 横幅：

```
ciscoasa(config)# banner motd Welcome to $(hostname).
ciscoasa(config)# banner motd Contact me at admin@example.com for any
ciscoasa(config)# banner motd issues.
```

自定义 CLI 提示符

CLI Prompt 窗格可用于自定义在 CLI 会话期间使用的提示符。默认情况下，提示符显示 ASA 的主机名。在多情景模式中，提示符还显示情景名称。在 CLI 提示符中可以显示以下项目：

cluster-unit	（单模式和多模式）显示集群设备名称。集群中的每个设备都有一个唯一的名称。
context	（仅多模式）显示当前情景的名称。
domain	显示域名。
hostname	显示主机名。

priority	显示故障转移优先级为 pri（主要）或 sec（辅助）。
state	显示设备的流量传输状态。系统显示以下状态值： • act - 故障转移已启用，并且设备正在主动传输流量。 • stby - 故障转移已启用，并且设备当前没有传输流量，正处于备用、故障或其他非活动状态。 • actNoFailover - 故障转移未启用，并且设备正在主动传输流量。 • stbyNoFailover - 故障转移未启用，并且设备当前没有传输流量。在备用设备上存在高于阈值的接口故障时，可能出现这种情况。 显示集群内设备的角色 （主或从）。例如，在提示符 ciscoasa/cl2/slave 中，主机名为 ciscoasa，设备名称为 cl2，状态名称为 slave。

详细步骤

如要自定义 CLI 提示符，请输入以下命令：

命令	用途
prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]} **示例：** `ciscoasa(config)# firewall transparent`	自定义 CLI 提示符。

更改控制台超时

控制台超时设置在特权 EXEC 模式或配置模式中连接可以保持的时间；达到超时的情况下，会话进入到用户 EXEC 模式。默认情况下，会话不会超时。此设置不会影响可保持控制台端口连接的时间，该连接永不超时。

如要更改控制台超时，请执行以下步骤：

详细步骤

命令	用途
console timeout *number* **示例：** `ciscoasa(config)# console timeout 0`	指定超级会话结束后的空闲时间 （以分钟为单位，范围为 0 到 60 分钟）。默认超时时间为 0，这意味着会话不会超时。

配置 VPN 隧道上的管理访问

如果 VPN 隧道在一个接口上终止，但是需要通过访问不同的接口管理 ASA，则可以将该接口识别为管理访问接口。例如，如果从外部接口进入 ASA，通过此功能可以使用 ASDM、 SSH、 Telnet 或 SNMP 连接内部接口；或者，当从外部接口进入时，可以 ping 内部接口。通过以下 VPN 隧道类型可以实现管理访问：IPsec 客户端、 IPsec 站到站和 AnyConnect SSL VPN 客户端。

- 第 35-9 页的管理接口的许可要求
- 第 35-2 页的准则和限制
- 第 35-10 页的配置管理接口

管理接口的许可要求

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单模式中受支持。

防火墙模式准则

在路由模式中受支持。

IPv6 准则

支持 IPv6。

附加准则

仅可以定义一个管理访问接口。

注　对于下面的配置，192.168.10.0/24 是 AnyConnect 或 IPsec VPN 客户端的 VPN 池。每个配置允许 VPN 客户端用户使用管理接口 IP 地址将 ASDM 或 SSH 连接至 ASA。

如要仅允许 VPN 客户端用户访问 ASDM 或 HTTP（以及拒绝访问所有其他用户），请输入以下命令：

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.10.0 255.255.255.0 management_interface
```

如要仅允许 VPN 客户端用户使用 SSH 访问 ASA（以及拒绝访问所有其他用户），请输入以下命令：

```
ciscoasa(config)# ssh 192.168.10.0 255.255.255.0 management_interface
```

配置管理接口

如要配置管理接口，请执行以下操作：

详细步骤

命令	用途
management-access *management_interface* **示例：** `ciscoasa(config)# management-access inside`	*management_interface* 指定当从另一个接口进入 ASA 时要访问的管理接口的名称。

配置系统管理员 AAA

本节介绍如何启用系统管理员的身份验证和命令授权。

- 第 35-10 页的有关系统管理员 AAA 的信息
- 第 35-13 页的系统管理员的 AAA 许可要求
- 第 35-13 页的先决条件
- 第 35-14 页的准则和限制
- 第 35-14 页的默认设置
- 第 35-15 页的配置 CLIASDM 和 命令访问的身份验证
- 第 35-16 页的配置访问特权 EXEC 模式 （enable 命令）的身份验证
- 第 35-18 页的使用管理授权限制用户的 CLI 和 ASDM 访问
- 第 35-20 页的为本地数据库用户配置密码策略
- 第 35-22 页的配置命令授权
- 第 35-26 页的配置管理访问记帐
- 第 35-27 页的查看当前登录用户
- 第 35-28 页的设置管理会话配额
- 第 35-28 页的在 SSH 会话中交换密钥
- 第 35-29 页的从锁定中恢复

有关系统管理员 AAA 的信息

本节介绍系统管理员 AAA。

- 第 35-11 页的有关管理身份验证的信息
- 第 35-11 页的有关命令授权的信息

有关管理身份验证的信息

本节介绍管理访问的身份验证。

- 第 35-11 页的比较有无身份验证的 CLI 访问
- 第 35-11 页的比较有无身份验证的 ASDM 访问
- 第 35-11 页的对从交换机到 ASA 服务模块的会话进行身份验证

比较有无身份验证的 CLI 访问

如何登录 ASA 取决于是否启用身份验证：

- No Authentication - 如果不启用 Telnet 的任何身份验证，则不输入用户名；请输入登录密码（使用 **password** 命令设置）。（无身份验证时，SSH 不可用）。将访问用户 EXEC 模式。
- Authentication - 如果根据此节启用 Telnet 或 SSH 身份验证，请输入如 AAA 服务器或本地用户数据库所定义的用户名和密码。将访问用户 EXEC 模式。

如要在登录后进入特权 EXEC 模式，请输入 **enable** 命令。 **enable** 如何使用取决于是否启用身份验证：

- No Authentication - 如果不配置启用身份验证，请在输入 **enable** 命令时进入系统启用密码（通过 **enable password** 命令设置）。但是，如果不使用启用身份验证，在输入 **enable** 命令后，则不再以特定用户身份登录。为了保留用户名，请使用启用身份验证。
- Authentication - 如果配置启用身份验证（请参阅第 35-16 页的配置访问特权 EXEC 模式（enable 命令）的身份验证），ASA 将再次提示您输入用户名和密码。当执行命令授权时此功能特别有用，因为用户名在确定用户可以输入的命令时非常重要。

对于使用本地数据库的启用身份验证，可以使用 **login** 命令，而不是 **enable** 命令。**login** 保留用户名，但不需要配置开启身份验证。有关详细信息，请参阅第 35-17 页的使用 login 命令对用户进行身份验证。

比较有无身份验证的 ASDM 访问

默认情况下，可以使用空的用户名和通过 **enable password** 命令设置的启用密码登录到 ASDM。请注意，如果在登录屏幕输入用户名和密码 （而不是将用户名留空），则 ASDM 将检查本地数据库是否有匹配项。

如果配置 HTTP 身份验证，则无法再使用空的用户名和启用密码来使用 ASDM。

对从交换机到 ASA 服务模块的会话进行身份验证

对于从交换机到 ASASM 的会话 （使用 **session** 命令），您可以配置 Telnet 身份验证。对于从交换机到 ASASM 的虚拟控制台连接 （使用 **service-module session** 命令），您可以配置串行端口身份验证。

在多情景模式中，您无法在系统配置中配置任何 AAA 命令。但是，如果在管理员情景中配置 Telnet 或串行身份验证，则身份验证也适用于从交换机到 ASASM 的会话。在此实例中使用管理员情景 AAA 服务器或本地用户数据库。

有关命令授权的信息

本节介绍命令授权。

- 第 35-12 页的支持的命令授权方法
- 第 35-12 页的关于用户凭证保留
- 第 35-12 页的安全情境和命令授权

支持的命令授权方法

您可以使用以下两种命令授权方法之一：

- 本地权限级别 - 在 ASA 上配置命令权限级别。当本地、RADIUS 或 LDAP（如果将 LDAP 属性映射到 RADIUS 属性）用户对 CLI 访问进行身份验证时，ASA 将该用户置于由本地数据库、RADIUS 或 LDAP 服务器定义的权限级别中。用户可以访问分配的权限级别及此级别以下的命令。请注意，当所有用户首次登录时，他们都访问用户 EXEC 模式（0 级或 1 级命令）。用户需要使用 **enable** 命令重新进行身份验证以进入特权 EXEC模式（2 级或更高级别命令），或者可以使用 **login** 命令登录（仅适用于本地数据库）。

注　您可以使用本地命令授权，无需作为本地数据库的任何用户，也无需 CLI 或 **enable** 身份验证。在输入 **enable** 命令时，您却输入系统启用密码，从而 ASA 将您置于 15 级。然后您可以创建每个级别的启用密码，从而当输入 **enable** *n*（范围为 2 到 15）时，ASA 将您置于 *n* 级。除非启用本地命令授权（请参阅第 35-22 页的配置本地命令授权），否则，不使用这些级别。（有关 **enable** 命令的详细信息，请参阅命令参考。）

- TACACS+ 服务器权限级别 - 在 TACACS+ 服务器上，配置用户或组在对 CLI 访问进行身份验证后可以使用的命令。用户在 CLI 输入的每个命令都使用 TACACS+ 服务器进行验证。

关于用户凭证保留

当用户登录到 ASA 时，该用户需要提供进行身份验证的用户名和密码。 ASA 保留这些会话凭证，以防以后在会话中需要进一步身份验证。

在以下配置就绪后，用户只需使用本地服务器进行登录的身份验证。随后的串行授权使用保存的凭证。系统还会提示用户输入 15 级权限的密码。当退出特权模式时，用户再次进行身份验证。在特权模式中不会保留用户凭据。

- 本地服务器配置为对用户访问进行身份验证。
- 15 级权限命令访问配置为需要密码才能实现。
- 用户帐户配置为仅串行授权 （无法访问控制台或 ASDM）。
- 用户帐户配置为 15 级权限命令访问。

下表显示在此情况下 ASA 如何使用凭证。

所需凭证	用户名和密码身份验证	串行 授权	特权模式命令授权	特权 模式退出授权
Username	是	否	否	是
密码	是	否	否	是
特权模式密码	否	否	是	否

安全情境和命令授权

以下是在多个安全情境中实施命令授权时要考虑的重点：

- AAA 设置按每个情景分立，在情景中没有共享。

  在配置命令授权时，必须单独配置每个安全情境。此配置能够实现对不同安全情境执行不同的命令授权。

在安全情境之间切换时，管理员应该清楚，在他们登录时指定的用户名所允许的命令在新的情景会话中可能不同，或者可能根本没有在新的情景中配置该命令授权。如果不知道安全情境之间的命令授权可能不同，这可能会使管理员感到困惑。该行为在下一点更为复杂。

- 无论在以前的情景会话中使用了哪个用户名，以 **changeto** 命令开始的新情景会话始终将默认 enable_15 用户名用作管理员身份。如果没有为 enable_15 用户配置命令授权，或者如果对 enable_15 用户的授权不同于对以前情景会话中的用户的授权，则此行为可能导致混淆。

  此行为也影响命令记帐，这只有在可以将发出的每个命令与特定管理员准确关联时才有用。由于有权限使用 **changeto** 命令的所有管理员都可以在其他情景中使用 enable_15 用户名，因此命令记帐记录可能不容易识别谁曾经以 enable_15 用户名登录系统。如果对每个情景都使用不同的记帐服务器，则跟踪谁曾经使用 enable_15 用户名需要从多个服务器关联数据。

  在配置命令授权时，请考虑以下事项：

  - 有权限使用 **changeto** 命令的管理员实际上有权限在每一个其他情景中使用 enable_15 用户可以使用的所有命令。
  - 如果要对每个情景授权不同命令，请确保在每个情景中拒绝 enable_15 用户名使用对有权使用 **changeto** 命令的管理员也拒绝的命令。

  在安全情境之间切换时，管理员可以退出特权 EXEC 模式并再次输入 **enable** 命令以使用所需的用户名。

注　系统执行空间不支持 AAA 命令；因此，命令授权在系统执行空间不可用。

系统管理员的 AAA 许可要求

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	基础许可证。

先决条件

AAA 服务器或本地数据库的先决条件

您必须在 AAA 服务器或本地数据库中配置用户。对于 AAA 服务器，则需要配置 ASA 与其通信。请参阅以下各章：

- AAA 服务器 - 请参阅适用的 AAA 服务器类型一章。
- 本地数据库 - 请参阅第 27-3 页的向本地数据库添加用户帐户。

管理身份验证的先决条件

在 ASA 可以对 Telnet、SSH 或 HTTP 用户进行身份验证之前，必须识别允许与 ASA 通信的 IP 地址。对于 ASASM，在多情景模式中对系统进行访问是一个例外情况；从交换机到 ASASM 的会话是 Telnet 会话，但是无需进行 Telnet 访问配置。有关详细信息，请参阅第 35-1 页的配置 ASDM、 Telnet 或 SSH 的 ASA 访问。

本地命令授权的先决条件

- 配置 **enable** 身份验证。（请参阅第 35-15 页的配置 CLIASDM 和 命令访问的身份验证。）

  enable 身份验证对于在用户访问 **enable** 命令后保持用户名是很有必要的。

  或者，您可以使用 **login** 命令 （身份验证时与 **enable** 命令相同；仅适用于本地数据库），无需配置。因为它不如 **enable** 身份验证安全，所以不建议您使用此选项。

  您也可以使用 CLI 身份验证，但不是必需的。

- 请参阅每个用户类型的以下先决条件：
  - 本地数据库用户 - 在本地数据库中为每个用户配置 0 到 15 级权限。
  - RADIUS 用户 - 为用户配置思科 VSA CVPN3000 权限级别 0 到 15 之间的值。
  - LDAP 用户 - 为用户配置值在 0 到 15 之间的权限级别，然后根据第 30-4 页的配置 LDAP 属性映射将 LDAP 属性映射到思科 VSA CVPN3000 权限级别。

TACACS+ 命令授权的先决条件

- 配置 CLI 身份验证 （请参阅第 35-15 页的配置 CLIASDM 和 命令访问的身份验证）。
- 配置 **enable** 身份验证 （请参阅第 35-16 页的配置访问特权 EXEC 模式 （enable 命令）的身份验证）。

管理记帐的先决条件

- 配置 CLI 身份验证 （请参阅第 35-15 页的配置 CLIASDM 和 命令访问的身份验证）。
- 配置 **enable** 身份验证 （请参阅第 35-16 页的配置访问特权 EXEC 模式 （enable 命令）的身份验证）。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

IPv6 准则

支持 IPv6。

默认设置

默认命令权限级别

默认情况下，以下命令会分配到 0 级权限。所有其他命令会分配到 15 级权限。

- **show checksum**
- **show curpriv**
- **enable**
- **help**

- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

如果将任何配置模式命令移到低于 15 的级别，请确保也将 **configure** 命令移到该级别，否则，用户将无法进入配置模式。

如要查看所有权限级别，请参阅第 35-24 页的查看本地命令的权限级别。

配置 CLIASDM 和 命令访问的身份验证

您可以要求进行 CLI、 ASDM 和 enable 命令访问的身份验证。

先决条件

- 根据第 35-1 页的配置 ASDM、 Telnet 或 SSH 的 ASA 访问配置 Telnet、 SSH 或 HTTP 访问。
- 对于 SSH 访问，必须配置 SSH 身份验证；无默认用户名。

详细步骤

	命令	用途
步骤 1	**aaa authentication** {**telnet** | **ssh** | **http** | **serial**} **console** {**LOCAL** | *server_group* [**LOCAL**]} **示例：** `ciscoasa(config)# aaa authentication ssh console radius_1 LOCAL` `ciscoasa(config)# aaa authentication http console radius_1 LOCAL` `ciscoasa(config)# aaa authentication serial console LOCAL`	进行用户身份验证实现管理访问。 **telnet** 关键字控制 Telnet 访问。对于 ASASM，此关键字还可使用 **session** 命令影响来自交换机的会话。对于多模式访问，请参阅第 35-11 页的对从交换机到 ASA 服务模块的会话进行身份验证。 **ssh** 关键字控制 SSH 访问。 **http** 关键字控制 ASDM 访问。 **serial** 关键字控制控制台端口访问。对于 ASASM，此关键字使用 **service-module session** 命令影响从交换机访问的虚拟控制台。对于多模式访问，请参阅第 35-11 页的对从交换机到 ASA 服务模块的会话进行身份验证。 HTTP 管理身份验证不支持 AAA 服务器组的 SDI 协议。 如果使用 AAA 服务器组进行身份验证，您可以配置 ASA 以在 AAA 服务器不可用时使用本地数据库作为回退方法。指定 **LOCAL** 前面的服务器组名称 （**LOCAL** 区分大小写）。我们建议您在本地数据库中使用与 AAA 服务器相同的用户名和密码，因为 ASA 提示符不会给出使用何种方法的任何指示。 或者，可以通过单独输入 **LOCAL**，使用本地数据库作为身份验证的主要方法 （无回退）。
步骤 2	**http authentication-certificate** *interface* **示例：** `http authentication-certificate inside`	要求在指定接口上通过 HTTP 连接来自 ASDM 客户端的证书。除 **aaa authentication** 命令可用于 ASDM 之外，还可使用此命令。 此命令仅用于ASDM 访问，请使用 **ssl certificate-authentication** 命令要求提供所有其他 SSL 流量的证书，例如直接转发代理。

配置访问特权 EXEC 模式 （enable 命令）的身份验证

您可以将 ASA 配置为在用户输入 **enable** 命令通过 AAA 服务器或本地数据库对用户进行身份验证。或者，用户在输入 **login** 命令时使用本地数据库自动进行身份验证，这也会根据本地数据库中的用户级别来访问特权 EXEC 模式。

- 第 35-17 页的配置 enable 命令的身份验证
- 第 35-17 页的使用 login 命令对用户进行身份验证

配置 enable 命令的身份验证

您可以将 ASA 配置为在用户输入 **enable** 命令时对其进行身份验证。有关详细信息，请参阅第 35-11 页的比较有无身份验证的 CLI 访问。

如要对输入 **enable** 命令的用户进行身份验证，请输入以下命令。

命令	用途
aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]} **示例：** `ciscoasa(config)# aaa authentication enable console LOCAL`	对输入 **enable** 命令的用户进行身份验证。系统提示用户输入用户名和密码。 如果使用 AAA 服务器组进行身份验证，您可以配置 ASA 以在 AAA 服务器不可用时使用本地数据库作为回退方法。指定 **LOCAL** 前面的服务器组名称 （**LOCAL** 区分大小写）。我们建议您在本地数据库中使用与 AAA 服务器相同的用户名和密码，因为 ASA 提示符不会给出使用何种方法的任何指示。 或者，可以通过单独输入 **LOCAL**，使用本地数据库作为身份验证的主要方法 （无回退）。

使用 login 命令对用户进行身份验证

从用户 EXEC 模式，可以使用 **login** 命令以本地数据库中的任何用户名登录。

此功能使用户可以使用自己的用户名和密码登录来访问特权 EXEC 模式，因此，无须为每个人提供系统启用密码。要允许用户在登录后访问特权 EXEC 模式（以及所有命令），请将用户权限级别设置为 2（默认）到 15。如果配置本地命令授权，则用户只能输入分配给该权限级别或更低级别的命令。有关详细信息，请参阅第 35-22 页的配置本地命令授权。

注意事项　如果您将用户添加到能够访问 CLI 以及不希望其进入特权 EXEC 模式的本地数据库中，则应该配置命令授权。在无命令授权的情况下，如果用户的权限级别为 2 或更高 （2 是默认值），则用户可以在 CLI 使用自己的密码访问特权 EXEC 模式 （以及所有命令）。或者，您可以使用 AAA 服务器进行身份验证，或者可以将所有本地用户设为 1 级，以便可以控制谁可以使用系统启用密码访问特权 EXEC 模式。

如要以本地数据库中一位用户的身份登录，请输入以下命令：

命令	用途
login **示例：** `ciscoasa# login`	以本地数据库中一位用户的身份登录。ASA 提示输入用户名和密码。在输入密码后，ASA 将该用户置于本地数据库指定的权限级别中。

使用管理授权限制用户的 CLI 和 ASDM 访问

ASA 使您能够在管理用户和远程访问用户使用 RADIUS、 LDAP、 TACACS+ 或本地用户数据库进行身份验证时对他们加以区分。用户角色差异化可防止远程访问 VPN 和网络访问用户建立到 ASA 的管理连接。

注　串行访问未包含在管理授权内，因此，如果您配置 **aaa authentication serial console**命令 ，那么进行身份验证的任何用户都可以访问控制台端口。

详细步骤

步骤 1　如要启用本地、RADIUS、LDAP（已映射）和 TACACS+ 用户的管理授权，请输入以下命令：

```
ciscoasa(config)# aaa authorization exec {authentication-server | LOCAL} [auto-enable]
```

当配置 **LOCAL** 选项时，本地用户数据库是输入的用户名和已分配的 Service-Type 和 Privilege-Level 属性的源。

此选项也启用通过 RADIUS 对管理用户权限级别提供的支持，这些权限级别可与本地命令权限级别配合使用进行命令授权。有关详细信息，请参阅第 35-22 页的配置本地命令授权。

当配置 **authentication-server** 选项时，可使用同一服务器进行身份验证和授权。

auto-enable 选项使来自登录身份验证服务器的拥有足够权限的用户能够直接进入特权 EXEC 模式。否则，用户将处于用户 EXEC 模式。这些权限由进入每个 EXEC 模式必须的 Service-Type 和 Privilege-Level 属性决定。要进入特权 EXEC 模式，用户必须具有 Administrative 的 Service-Type 属性和分配给这些用户的大于 1 的 Privilege Level 属性。

在系统情景中不支持此选项。但是，如果在管理员情景中配置 Telnet 或串行身份验证，则身份验证也适用于从交换机到 ASASM 的会话。

如果单独输入 **aaa authorization exec** 命令，则没有影响。

在管理授权中使用串行身份验证时，不包括 **auto-enable** 选项。

auto-enable 选项不会影响 **aaa authentication http** 命令。

在配置 **auto-enable** 选项之前，我们建议您同时配置协议登录和启用身份验证，使所有身份验证请求都转至相同的 AAA 服务器组，如以下示例所示：

```
ciscoasa (config)# aaa authentication ssh console RADIUS
ciscoasa (config)# aaa authentication enable console RADIUS
ciscoasa (config)# aaa authorization exec authentication-server auto-enable
```

我们*不*建议您使用其他类型的配置。

步骤 2　如要配置用户进行管理授权，请参阅每个 AAA 服务器类型或本地用户的以下要求：

RADIUS 或 LDAP（已映射）用户

当用户通过 LDAP 进行身份验证时，本地 LDAP 属性及其值可以映射到思科 ASA 属性以提供特定授权功能。为思科 VSA CVPN3000 权限级别配置 0 到 15 之间的值。然后，使用 **ldap map-attributes** 命令将 LDAP 属性映射到思科 VAS CVPN3000 权限级别。有关详细信息，请参阅第 30-4 页的配置 LDAP 属性映射。

当 RADIUS IETF **service-type** 属性作为 RADIUS 身份验证和授权请求的结果在访问接受消息中进行发送时，其用于表示授予通过身份验证的用户的服务类型：

- Service-Type 6 (Administrative) - 允许对通过 **aaa authentication console** 命令 指定的任何服务进行完全访问。

- Service-Type 7 (NAS prompt) - 允许在配置 **aaa authentication {telnet | ssh} console** 命令 时对 CLI 进行访问，但是，如果配置 **aaa authentication http console** 命令 ，则拒绝 ASDM 配置访问。允许进行 ASDM 监控访问。如果使用 **aaa authentication enable console** 命令 配置 **enable** 身份验证，则用户无法使用 **enable** 命令访问特权 EXEC 模式。Framed (2) 和 Login (1) 服务类型按同一方式处理。
- Service-Type 5 (Outbound) - 拒绝管理访问。用户无法使用由 **aaa authentication console** 命令指定的任何服务 （不包括 **serial** 关键字 ； 允许串行访问）。远程访问 （IPsec 和 SSL）用户仍然可以进行身份验证并终止其远程访问会话。所有其他类型 （Voice、 FAX 等）按同一方式处理。

在访问接受消息中发送 RADIUS Cisco VSA **privilege-level** 属性 (Vendor ID 3076, sub-ID 220) 时，该属性用于表示用户的权限级别。

当通过身份验证的用户尝试通过 ASDM、 SSH 或 Telnet 对 ASA 进行管理访问，但没有相应的权限级别实现此操作时，则 ASA 将生成系统日志消息 113021。此消息会通知用户，由于不适当的管理权限，尝试登录失败。

以下示例显示如何定义 LDAP 属性映射：在本示例中，安全策略指定正在通过 LDAP 进行身份验证的用户将用户记录字段或参数标题和公司分别到映射 IETF-RADIUS 服务类型和权限级别。

```
ciscoasa(config)# ldap attribute-map admin-control
ciscoasa(config-ldap-attribute-map)# map-name title IETF-RADIUS-Service-Type
ciscoasa(config-ldap-attribute-map)# map-name company Privilege-Level
```

以下示例向 LDAP AAA 服务器应用 LDAP 属性映射：

```
ciscoasa(config)# aaa-server ldap-server (dmz1) host 10.20.30.1
ciscoasa(config-aaa-server-host)# ldap-attribute-map admin-control
```

TACACS+ 用户

使用“service=shell”请求授权，服务器以 PASS 或 FAIL 作为响应。

- PASS, privilege level 1 - 仅允许对 ASDM 进行访问 （对配置和监控部分进行有限只读访问）和权限级别为 1 的 **show** 命令访问。
- PASS, privilege level 2 and higher - 允许在配置 **aaa authentication {telnet | ssh} console** 命令 时对 CLI 进行访问，但是，如果配置 **aaa authentication http console** 命令 ，则拒绝 ASDM 配置访问。允许进行 ASDM 监控访问。如果使用 **aaa authentication enable console** 命令 配置 **enable** 身份验证，则用户无法使用 **enable** 命令访问特权 EXEC 模式。如果 enable 权限级别设为 14 或以下，则不允许使用 **enable** 命令访问特权 EXEC 模式。
- FAIL - 拒绝管理访问。您无法使用由 **aaa authentication console** 命令 指定的任何服务 （不包括 **serial** 关键字 ； 允许进行串行访问）。

本地用户

为给定用户名设置 **service-type** 命令。默认情况下，**service-type** 是 **admin**，允许对 **aaa authentication console** 命令指定的任何服务进行完全访问。有关详细信息，请参阅第 27-3 页的向本地数据库添加用户帐户。

为本地数据库用户配置密码策略

您使用本地数据库配置身份验证进行 CLI 或 ASDM 访问时，可以配置密码策略，该策略要求用户在指定的时间后更改其密码，还规定密码标准，例如最短长度和更改后的最小字符数。

密码策略仅适用于使用本地数据库的管理用户，而不适用于可以使用本地数据库的其他流量类型，例如网络访问的 VPN 或 AAA，也不适用于通过 AAA 服务器进行身份验证的用户。

- 第 35-20 页的配置密码策略
- 第 35-22 页的更改密码

配置密码策略

配置密码策略后，当您更改密码 （自己本人的或其他用户的）时，密码策略将应用于新密码。任何现有密码都受新策略约束。使用 **username** 命令 更改密码时，以及使用 **change-password** 命令更改密码时，将应用新策略。

先决条件

- 根据第 35-15 页的配置 CLIASDM 和 命令访问的身份验证配置 CLI/ASDM 。请确保指定本地数据库。
- 根据第 35-16 页的配置访问特权 EXEC 模式 （enable 命令）的身份验证配置 enable 身份验证。请确保指定本地数据库。

详细步骤

	命令	用途
步骤 1	**password-policy lifetime** *days* **示例：** `ciscoasa(config)# password-policy lifetime 180`	（可选）设置远程用户 （SSH、 Telnet、 HTTP）密码到期前的天数间隔；控制台端口的用户不会由于密码到期而锁定。有效值为 0 和 65536 天之间。默认值为 0 天，表示密码不会到期。 在密码到期前 7 天，系统会显示警告消息。在密码到期后，拒绝远程用户访问系统。如要在到期后访问，请执行以下步骤： • 让另一个管理员使用 **username** 命令更改密码。 • 登录到物理控制台端口更改密码。
步骤 2	**password-policy minimum-changes** *value* **示例：** `ciscoasa(config)# password-policy minimum-changes 2`	（可选）设置与旧密码相比，新密码中必须更改的最小字符数。有效值为 0 和 64 个字符之间。默认值为 0。 字符匹配与位置无关，意味着只有新密码字符不在当前密码的任何地方出现时才视为被更改。
步骤 3	**password-policy minimum-length** *value* **示例：** `ciscoasa(config)# password-policy minimum-length 8`	（可选）设置密码最小长度。有效值为 3 和 64 个字符之间。建议最小密码长度为 8 个字符。

	命令	用途
步骤 4	**password-policy minimum-uppercase** *value* **示例：** `ciscoasa(config)# password-policy minimum-uppercase 3`	（可选）设置密码必须具有的最小大写字符数。有效值为 0 和 64 个字符之间。默认值为 0，表示无最小数。
步骤 5	**password-policy minimum-lowercase** *value* **示例：** `ciscoasa(config)# password-policy minimum-lowercase 6`	（可选）设置密码必须具有的最小小写字符数。有效值为 0 和 64 个字符之间。默认值为 0，表示无最小数。
步骤 6	**password-policy minimum-numeric** *value* **示例：** `ciscoasa(config)# password-policy minimum-numeric 1`	（可选）设置密码必须具有的最小数字字符数。有效值为 0 和 64 个字符之间。默认值为 0，表示无最小数。
步骤 7	**password-policy minimum-special** *value* **示例：** `ciscoasa(config)# password-policy minimum-special 2`	（可选）设置密码必须具有的最小特殊字符数。有效值为 0 和 64 个字符之间。特殊字符包括：！、@、#、$、%、^、&、*、'(‘ 和 ‘)’。默认值为 0，表示无最小数。
步骤 8	**password-policy authenticate enable** **示例：** `ciscoasa(config)# password-policy authenticate enable`	（可选）设置用户是否必须使用 **change-password** 命令更改密码，而不是让用户使用 **username** 命令更改密码。默认设置被禁用：用户可以使用任何一种方法更改密码。 如果启用此功能，在尝试使用 **username** 命令更改密码时，系统会显示以下错误消息： `ERROR: Changing your own password is prohibited` 您也无法使用 **clear configure username** 命令删除自己的帐户。如果尝试删除，系统会显示以下错误消息： `ERROR: You cannot delete all usernames because you are not allowed to delete yourself`

更改密码

如果在密码策略中配置密码生存期，则需要在旧密码到期时将 **username** 密码更改为新密码。如果启用密码策略身份验证 （**password-policy authenticate enable** 命令），此密码更改方法是必需的。如果未启用密码策略身份验证，则可以使用此方法，或者直接使用 **username** 命令 窗格更改用户帐户。

详细步骤

命令	用途
change-password [**old-password** *old_password* [**new-password** *new_password*]] **示例：** `hostname# change-password old-password j0hncr1chton new-password a3rynsun`	更改 **username** 密码。如果不在命令中输入旧密码和新密码，则 ASA 会提示您输入。

配置命令授权

如果要控制对命令的访问，可以通过 ASA 配置命令授权，在其中可以确定对用户可用的命令。默认情况下，当登录时，可以访问用户 EXEC 模式，此模式仅提供最小数量的命令。当输入 **enable** 命令 （或在使用本地数据库时输入 **login** 命令），则可以访问特权 EXEC 模式和高级命令（包括配置命令）。

您可以使用以下两种命令授权方法之一：

- 本地权限级别
- TACACS+ 服务器权限级别

有关命令授权的详细信息，请参阅第 35-11 页的有关命令授权的信息。

- 第 35-22 页的配置本地命令授权
- 第 35-24 页的查看本地命令的权限级别
- 第 35-25 页的在 Commands TACACS+ 服务器上配置命令
- 第 35-26 页的配置 TACACS+ 命令授权

配置本地命令授权

通过本地命令授权可以为 16 个权限级别 （0 到 15）之一分配命令。默认情况下，会向每个命令分配 0 级或 15 级权限。您可以将每个用户定义在特定权限级别，并且，每个用户可以输入在分配权限级别或以下的任何命令。 ASA 支持在本地数据库、 RADIUS 服务器或 LDAP 服务器 （如果将 LDAP 属性映射到 RADIUS 属性）中定义的用户权限级别。有关详细信息，请参阅以下各节：

- 第 27-3 页的向本地数据库添加用户帐户
- 第 28-1 页的支持的身份验证方法
- 第 30-4 页的配置 LDAP 属性映射

如要配置本地命令授权，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**privilege** [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** *command* **示例：** `ciscoasa(config)# privilege show level 5 command filter`	将命令分配到权限级别。 对要重新分配的每个命令重复此命令。 此命令中的选项如下： • **show** | **clear** | **cmd** - 这些可选关键字可用于仅为命令的显示、清除或配置形式设置权限。命令的配置形式通常是导致配置更改的形式，或者是以未修改的命令形式（无 **show** 或 **clear** 前缀），或者是以 **no** 形式。如果不使用这些关键字的其中一个，则会影响命令的所有形式。 • **level** *level* - 介于 0 和 15 之间的级别。 • **mode** {**enable** | **configure**} - 如果可以在用户 EXEC 模式或特权 EXEC 模式中以及配置模式中输入命令，并且命令在各个模式中执行不同的操作，则您可以分别设置这些模式的权限级别： – **enable** - 指定用户 EXEC 模式和特权 EXEC 模式。 – **configure** - 指定配置模式，可以使用 **configure terminal** 命令进行访问。 • **command** *command* - 将配置的命令。您只能配置*主*命令的权限级别。例如，可以配置**所有** aaa 命令的级别，但是不可以单独配置 **aaa authentication** 命令和 **aaa authorization** 命令的级别。
步骤 2	**aaa authorization exec authentication-server** **示例：** `ciscoasa(config)# aaa authorization exec authentication-server`	通过 RADIUS 支持管理用户权限级别。 对进行身份验证实现管理访问的用户实施用户特定访问级别 （请参阅 **aaa authentication console LOCAL** 命令）。 如果没有此命令，则 ASA 仅支持本地数据库用户的权限级别，并将所有其他类型的用户默认设置为 15 级。 此命令还启用本地、RADIUS、LDAP（已映射）和 TACACS+ 用户的管理授权。 使用 **aaa authorization exec LOCAL** 命令启用将从本地数据库中采用的属性。有关在 AAA 服务器上配置用户来满足管理授权的信息，请参阅第 35-18 页的使用管理授权限制用户的 CLI 和 ASDM 访问。
步骤 3	**aaa authorization command LOCAL** **示例：** `ciscoasa(config)# aaa authorization command LOCAL`	支持使用本地命令权限级别，通过本地数据库、 RADIUS 服务器或 LDAP 服务器 （具有映射的属性）中的用户权限等级可以选中这些级别。 在设置命令权限级别时，除非使用此命令来配置命令授权，否则不会进行命令授权。

示例

filter 命令具有以下形式：

- **filter**（由 **configure** 选项表示）
- **show running-config filter**

- **clear configure filter**

您可以为每种形式分别设置权限级别，或通过忽略此选项为所有形式设置同一权限级别。以下示例显示如何分别设置每种形式：

```
ciscoasa(config)# privilege show level 5 command filter
ciscoasa(config)# privilege clear level 10 command filter
ciscoasa(config)# privilege cmd level 10 command filter
```

或者，以下示例显示如何将所有过滤命令设置为同一级别：

```
ciscoasa(config)# privilege level 5 command filter
```

show privilege 命令分隔显示的形式。

以下示例显示 **mode** 关键字的使用。必须从用户 EXEC 模式输入**enable** 命令，而可在配置模式中访问的 **enable password** 命令则要求最高的权限级别：

```
ciscoasa(config)# privilege cmd level 0 mode enable command enable
ciscoasa(config)# privilege cmd level 15 mode cmd command enable
ciscoasa(config)# privilege show level 15 mode cmd command enable
```

以下示例显示使用 **mode** 关键字的附加命令：**configure** 命令：

```
ciscoasa(config)# privilege show level 5 mode cmd command configure
ciscoasa(config)# privilege clear level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode enable command configure
```

注　最后一行用于 **configure terminal** 命令。

查看本地命令的权限级别

以下命令后，可以查看命令的权限级别。

命令	用途
show running-config all privilege all	显示所有命令。
show running-config privilege level *level*	显示特定级别的命令。 *level* 是 0 和 15 之间的整数。
show running-config privilege command *command*	显示特定命令的级别。

示例

对于 **show running-config all privilege all** 命令，ASA 显示当前分配到权限级别的每个 CLI 命令。以下是此命令的输出示例：

```
ciscoasa(config)# show running-config all privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

```
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
....
```

以下示例显示 10 级权限的命令分配：

```
ciscoasa(config)# show running-config privilege level 10
privilege show level 10 command aaa
```

以下示例显示 **access - list** 命令的命令分配：

```
ciscoasa(config)# show running-config privilege command access-list
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

在 Commands TACACS+ 服务器上配置命令

您可以在思科安全访问控制服务器 (ACS) TACACS+ 服务器上，为组或为单个用户将命令配置为共享配置文件组件。对于第三方 TACACS+ 服务器，有关命令授权支持的详细信息，请参阅服务器文档。

请参阅以下在思科安全 ACS 3.1 版本中配置命令的准则；许多这些准则也适用于第三方服务器。

- ASA 将待授权的命令作为外壳命令发送，因此请在 TACACS+ 服务器上将命令配置为外壳命令。

注　思科安全 ACS 可能包括称为“pix-shell”的命令类型。请勿将此类型用于 ASA 命令授权。

- 命令的第一个词被视为主命令。所有附加的单词都被视为参数，需要在其前面放置 **permit** 或 **deny**。

  例如，要允许 **show running-configuration aaa-server** 命令，请向命令字段添加 **show running-configuration**，然后在参数字段键入 **permit aaa-server**。

- 您可以通过选中 **Permit Unmatched Args** 复选框，允许不会明确拒绝的命令的所有参数。

  例如，您可以仅配置 **show** 命令，那么将允许所有 **show** 命令。我们建议使用此方法，这样您就无需预测命令的每个变量 （包括缩写和问号），其显示 CLI 的使用情况。

- 对于单个单词的命令，即使命令没有参数，也*必须*允许不匹配的参数，例如 **enable** 或 **help**。

- 如要禁止某些参数，请输入参数并在前面放置 **deny**。

  例如，要允许 **enable**，但不允许 **enable password**，请在命令字段中输入 **enable**，在参数字段内输入 **deny password**。确保选中 **Permit Unmatched Args** 复选框，这样仍能单独允许 **enable**。

- 当缩写命令行中的命令时，ASA 将前缀和主 命令扩展为全文本，但是您输入过程中，它将附加参数发送到 TACACS+ 服务器。

  例如，如果您输入 **sh log**，那么 ASA 将整个 **show logging** 命令发送到 TACACS+ 服务器。但是，如果您输入 **sh log mess**，那么 ASA 将 **show logging mess** 命令发送到 TACACS+ 服务器，而不是发送扩展的 **show logging message** 命令。您可以将同一参数的多种拼写配置为预期缩写。

- 我们建议您允许所有用户使用以下基本命令：
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**

- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

配置 TACACS+ 命令授权

如果启用 TACACS+ 命令授权，且用户在 CLI 输入命令，则 ASA 将向 TACACS+ 服务器发送命令和用户名以确定命令是否经过授权。

在启用 TACACS+ 命令授权之前，请确保您已经以在 TACACS+ 服务器上定义的用户身份登录 ASA，并且具有必要的命令授权来继续配置 ASA。例如，您应该以授权所有命令的管理员用户身份登录。否则，可能会意外锁定。

请勿保存配置，直到您确定配置会以所需的方式发挥作用。如果由于错误发生锁定，通常您可以通过重新启动 ASA 恢复访问。如果仍然锁定，请参阅第 35-29 页的从锁定中恢复。

请确保 TACACS+ 系统完全稳定且可靠。必要的可靠性级别通常需要完全冗余的 TACACS+ 服务器系统和完全冗余的 ASA 连接性。例如，在 TACACS+ 服务器池中，包括一个连接至接口 1 的服务器 和另一个连接至接口 2 的服务器。如果 TACACS+ 服务器不可用，您也可以将本地命令授权配置为回退方法。在这种情况下，您需要根据第 35-22 页的配置命令授权中列出的操作步骤配置本地用户和命令权限级别。

如要配置 TACACS+ 命令授权，请输入以下命令：

详细步骤

命令	用途
aaa authorization command *tacacs+_server_group* [**LOCAL**] **示例：** `ciscoasa(config)# aaa authorization command group_1 LOCAL`	使用 TACACS+ 服务器执行命令授权。 如果 TACACS+ 服务器不可用，则您可以配置 ASA 使用本地数据库作为回退方法。要启用回退，请指定 **LOCAL** 前面的服务器组名（**LOCAL** 区分大小写）。我们建议您在本地数据库中使用与 TACACS+ 服务器相同的用户名和密码，因为 ASA 提示符不会给出使用何种方法的任何指示。请确保在本地数据库（请参阅第 27-3 页的“向本地数据库添加用户帐户”章节）和命令权限级别（请参阅第 35-22 页的配置本地命令授权）中配置用户。

配置管理访问记帐

在 CLI 中输入 **show** 命令之外的任何命令时，您可以将记帐消息发送到 TACACS+ 记帐服务器。您可以在用户登录时、输入 **enable** 命令时或者发出命令时配置记帐。

对于命令记帐，您只可以使用 TACACS+ 服务器。

如要配置管理访问和 enable 命令记帐，请执行以下步骤：

详细步骤

	命令	用途
步骤 1	**aaa accounting** {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag* **示例：** `ciscoasa(config)# aaa accounting telnet console group_1`	允许支持管理访问的 AAA 记帐。 有效的服务器组协议是 RADIUS 和 TACACS+。
步骤 2	**aaa accounting command** [**privilege** *level*] *server-tag* **示例：** `ciscoasa(config)# aaa accounting command privilege 15 group_1`	启用命令记帐。只有 TACACS+ 服务器支持命令记帐。 其中，**privilege** *level* 是最小的权限级别，*server-tag* 是ASA 应该向其发送命令记帐消息的 TACACS+ 服务器组的名称。

查看当前登录用户

如要查看当前登录用户，请在 中输入以下命令：

```
ciscoasa# show curpriv
```

示例

以下是 **show curpriv** 命令的输出示例：

```
ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

表 35-1介绍 **show curpriv** 命令输出。

表 35-1　　show curpriv 命令输出说明

字段	说明
Username	用户名。如果您以默认用户身份登录，则名称是 enable_1（用户 EXEC）或 enable_15（特权 EXEC）。
Current privilege level	级别范围为 0 到 15。除非您配置本地命令授权并为中间权限级别分配命令，否则只能使用 0 级和 15 级。
Current Modes	可用的访问模式如下： • P_UNPR - 用户 EXEC 模式（0 级和 1 级） • P_PRIV - 特权 EXEC 模式（2 级到 15 级） • P_CONF - 配置模式

设置管理会话配额

您可以建立同步管理会话的最大数量。如果达到最大值，则不允许其他会话，并生成系统日志消息。要防止系统锁定，则管理会话配额机制无法阻止控制台会话。

如要设置管理会话配额，请输入以下命令：

命令	用途
quota management-session *number* **示例：** `hostname(config)# quota management-session 1000`	设置在 ASA 上允许的同步 ASDM、SSH 和 Telnet 会话的最大数量。此命令的 **no** 形式将配额值设置为 0，这意味着没有会话限制。

在 SSH 会话中交换密钥

(DH) Diffie - Hellman 密钥交换提供无法单独由任何一方确定的共享密钥。密钥交换与签名和主机密钥进行组合以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。

用于密钥交换的 DH 组 1 和组 14 密钥交换方法在 ASA 上均受支持。如果未指定 DH 组密钥交换方法，则将使用 DH 组 1 密钥交换方法。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。

如要在 SSH 会话中交换密钥，请输入以下命令：

命令	用途
ssh key-exchange group {**dh-group1** | **dh-group14**} **sha-1** **示例：** `ciscoasa(config)# ssh key-exchange group dh-group14 sha-1` `ciscoasa# show running-config key-exchange` `ssh key-exchange dh-group14-sha1`	使用 DH 组 1 或 DH 组 14 的密钥交换方法来交换密钥。 **key-exchange** 关键字指定在交换密钥时将遵循并且应使用 DH 组 1 或 DH 组 14 密钥交换方法。 **group** 关键字表明在交换密钥时将遵循并且应使用 DH 组 1 密钥交换方法或 DH 组 14 密钥交换方法。 **dh-group1** 关键字表明在交换密钥时将遵循并应使用 DH 组 1 密钥交换方法。由于旧版原因， DH 组 2 称为 DH 组 1。 **dh-group14** 关键字表明在交换密钥时将遵循并应使用 DH 组 14 密钥交换方法。 **sha-1** 关键字表明应使用 SHA - 1 加密算法。 使用 **show running-config ssh key-exchange** 命令显示当前使用的 DH 组密钥交换方法。

从锁定中恢复

在某些情况下，当开启命令授权或 CLI 身份验证时，您可能被锁定在ASA CLI 之外。通常，您可以通过重新启动 ASA 恢复访问。但是，如果您已经保存配置，则可能会被锁定。表 35-2列出常见锁定条件以及如何从中恢复：

表 35-2　CLI 身份验证和命令授权锁定场景

功能	锁定条件	说明	解决方法：单模	解决方法：多模
本地 CLI 身份验证	未在本地数据库中配置用户。	如果本地数据库中没有用户，则您无法登录，并且无法添加任何用户。	登录并重置密码和 **aaa** 命令。	从交换机会话到 ASA。从系统执行空间，您可以变更到情景并添加用户。
TACACS+ 命令授权 TACACS+ CLI 身份验证 RADIUS CLI 身份验证	服务器关闭或无法访问，且没有配置回退方法。	如果服务器无法访问，则您无法登录或无法输入任何命令。	1. 登录并重置密码和 AAA 命令。 2. 将本地数据库配置为回退方法，这样服务器关闭时不会锁定。	1. 如果服务器由于 ASA 上的网络配置不正确而无法访问，则请从交换机会话到 ASA。从系统执行空间，您可以变更到情景并重新配置网络设置。 2. 将本地数据库配置为回退方法，这样服务器关闭时不会锁定。
TACACS+ 命令授权	您以没有足够权限的用户或不存在的用户身份登录。	启用命令授权，但是然后发现用户无法再输入任何命令。	修复 TACACS+ 服务器用户帐户。 如果无法访问 TACACS+ 服务器，并且需要立即配置 ASA，则请登录维护分区并重置密码和 **aaa** 命令。	从交换机会话到 ASA。从系统执行空间，您可以变更到情景并完成配置更改。您也可以禁用命令授权，直到修复 TACACS+ 配置。
本地命令授权	您以没有足够权限的用户登录。	启用命令授权，但是然后发现用户无法再输入任何命令。	登录并重置密码和 **aaa** 命令。	从交换机会话到 ASA。从系统执行空间，您可以变更到情景并更改用户级别。

管理访问的功能历史记录

表 35-3 列出了各种功能变更以及实施该等功能变更的平台版本。

表 35-3　　管理访问的功能历史记录

功能名称	平台版本	功能信息
管理访问	7.0(1)	我们引入了此功能。 我们引入了以下命令： **show running-config all privilege all, show running-config privilege level, show running-config privilege command, telnet, telnet timeout, ssh, ssh timeout, http, http server enable, asdm image disk, banner, console timeout, icmp, ipv6 icmp, management access, aaa authentication console, aaa authentication enable console, aaa authentication telnet | ssh console, service-type, login, privilege, aaa authentication exec authentication-server, aaa authentication command LOCAL, aaa accounting serial | telnet | ssh | enable console, show curpriv, aaa accounting command privilege**.
提高了 SSH 安全性；不再支持 SSH 默认用户名。	8.4(2)	从 8.4(2) 开始，您无法再使用 pix 或 asa 用户名和登录密码通过 SSH 连接至 ASA。要使用 SSH，您必须使用 **aaa authentication ssh console LOCAL** 命令 (CLI) 或 Configuration > Device Management > Users/AAA > AAA Access > Authentication 配置 AAA 身份验证；然后通过输入 **username** 命令 (CLI) 或选择 Configuration > Device Management > Users/AAA > User Accounts (ASDM) 定义本地用户。如果要使用 AAA 服务器而不是本地数据库进行身份验证，我们建议也将本地身份验证配置为备用方法。
使用本地数据库时，支持管理员密码策略。	8.4(4.1)、9.1(2)	您使用本地数据库配置身份验证进行 CLI 或 ASDM 访问时，可以配置密码策略，该策略要求用户在指定的时间后更改其密码，还规定密码标准，例如最短长度和更改后的最小字符数。 我们引入了以下命令：**change-password, password-policy lifetime**、**password-policy minimum changes**、**password-policy minimum-length**、**password-policy minimum-lowercase**、**password-policy minimum-uppercase**、**password-policy minimum-numeric**、**password-policy minimum-special**、**password-policy authenticate enable**、**clear configure password-policy**、**show running-config password-policy**。
对 SSH 公钥身份验证的支持	8.4(4.1)、9.1(2)	您可以基于每个用户启用到 ASA 的 SSH 连接的公钥身份验证。您可以指定公钥文件 (PKF) 格式的密钥或 Base64 密钥。PKF 密钥的长度可达 4096 位。对于由于过长而导致 ASA 不支持使用 Base64 格式 （限长 2048 位）的密钥，请使用 PKF 格式。 我们引入了以下命令：**ssh authentication**。 *仅在 9.1(2) 及更高版本中支持 PKF 密钥格式。*
支持 SSH 密钥交换的 Diffie-Hellman 群 14	8.4(4.1)、9.1(2)	已添加支持 Diffie-Hellman 群 14 进行 SSH 密钥交换 以前，只支持组 1。 我们引入了以下命令：**ssh key-exchange**。

表 35-3　　管理访问的功能历史记录（续）

功能名称	平台版本	功能信息
支持最大数量的管理会话	8.4(4.1)、9.1(2)	您可以设置同步 ASDM、 SSH 和 Telnet 会话的最大数量。 我们引入了以下命令：**quota management-session**、**show running-config quota management-session**、 **show quota management-session**。
对于在多情景模式中的 ASASM，支持从交换机进行 Telnet 和虚拟控制台身份验证。	8.5(1)	虽然从多情景模式中的交换机连接至 ASASM 也连接至系统执行空间，但是您可以在管理员情景中配置身份验证以监管这些连接。
SSH 的 AES-CTR 加密	9.1(2)	ASA 中的 SSH 服务器实施现在支持 AES - CTR 模式加密。
改进的 SSH 重新生成密钥间隔		在连接时间达到 60 分钟后或数据流量达到 1 GB 后， SSH 连接重新生成密钥。 我们引入了以下命令：**show ssh sessions detail**。
改进的一次性密码身份验证	9.2(1)	有足够授权权限的管理员可以通过输入自己的身份验证凭证一次进入特权 EXEC 模式。 **auto-enable** 选项已添加到 **aaa authorization exec** 命令中。 我们修改了以下命令：**aaa authorization exec**。

软件和配置

本章介绍如何管理思科 ASA 软件和配置。

- 第 36-1 页的升级软件
- 第 36-10 页的管理文件
- 第 36-19 页的配置要使用的映像和启动配置
- 第 36-20 页的使用 ROM 监控模式加载映像
- 第 36-23 页的备份和还原 配置或其他文件
- 第 36-31 页的将您的软件降级
- 第 36-33 页的配置自动更新
- 第 36-39 页的软件和配置的功能历史记录

升级软件

- 第 36-1 页的升级路径和迁移
- 第 36-3 页的查看当前版本
- 第 36-3 页的从 Cisco.com 下载软件
- 第 36-3 页的升级独立设备
- 第 36-4 页的升级故障转移对或 ASA 集群

升级路径和迁移

- 如果您从 9.0 之前的版本升级，由于 ACL 迁移，您以后可能无法执行降级；如果您想要降级，请务必备份您的配置文件。有关详细信息，请参阅 9.0 升级指南中的 ACL 迁移章节。
- 如要将 9.1(2.8) 之前的版本升级至 9.1(2.8) 或更高版本，您必须正在运行以下任一版本：
  - 8.4(5) 或更高版本
  - 9.0(2) 或更高版本
  - 9.1(2)

如果您运行任意 *早期*版本，则必须 *先*升级至以上任一版本，否则无法直接升级至 9.1(2.8) 或更高版本。例如：

9.1(2.8) 之前的 ASA 版本	首先升级到：	然后升级到：
8.2(1)	8.4(7)	9.3(1) 或更高版本
8.4(4)	8.4(7)	9.3(1) 或更高版本
9.0(1)	9.0(4)	9.3(1) 或更高版本
9.1(1)	9.1(2)	9.3(1) 或更高版本

- 如果您将从 8.3 之前的版本升级：
  - 有关迁移配置的重要信息，请参阅 *《至 8.3 版本的思科 ASA 5500 迁移指南》*。
  - 您无法直接升级到 9.0 或更高版本。如要成功迁移，您必须先升级至 8.4 版本。
- 零停机时间升级的软件版本要求：

  故障转移配置或 ASA 集群中的设备应具有相同的主要 （第一个编号数字）和次要 （第二个编号）软件版本。然而，在升级过程中，您不需要使设备保持版本相同；您可在每台设备上运行不同版本的软件，并且仍然保持故障转移支持。为确保长期的兼容性和稳定性，我们建议尽可能地将所有设备升级至相同版本。

  表 36-1展示了执行零停机时间升级的受支持方案。

表 36-1　　零停机时间升级支持

升级类型	支持
维护版本	您可以在次要版本中从任何维护版本升级到任何其他维护版本。 例如，您可以从 9.1(1) 升级至 9.1(5)，而无需先安装两者之间的维护版本。
次要版本	您可以从一个次要版本升级至下一个次要版本。您无法跳过某个次要版本。 例如，您可以从 9.0 升级到 9.1。从 9.0 直接升级到 9.2 不支持零停机升级；您必须首先升级到 9.1。 **注**　即使功能配置已迁移，但仍有可能实现零停机升级。
主要版本	您可以从上一个版本的最后一个次要版本，升级至下一个主要版本。 例如，假设 8.6 是您的型号的 8.x 版本系列的最后一个次要版本，则您可以从 8.6 升级至 9.0。从 8.6 直接升级到 9.1 不支持零停机升级；您必须首先升级到 9.0。对于次要版本不支持的型号，您可以跳过次要版本；例如，对于 ASA 5585-X，您可以从 8.4 升级到 9.0（8.5 或 8.6 不支持该型号）。 **注**　即使功能配置已迁移，但仍有可能实现零停机升级。

查看当前版本

使用 **show version** 命令验证 ASA 的软件版本。

从 Cisco.com 下载软件

如果您拥有 Cisco.com 登录帐户，您可以从以下网站获取操作系统和 ASDM 映像：
http://www.cisco.com/go/asa-software

此操作步骤假设您将映像存放在 TFTP 服务器上，尽管其他服务器类型也受支持。

升级独立设备

本节介绍如何安装 ASDM 和操作系统 (OS) 映像。

操作步骤

此操作步骤使用 TFTP。对于 FTP 或 HTTP，请参阅 **copy** 命令。

步骤 1　（如果有配置迁移）在终端显示配置，以便您能够备份配置：

```
more system:running-config
```

复制此命令的输出，然后将配置粘贴到文本文件中。有关其他备份方法的信息，请参阅配置指南。

步骤 2　将 ASA 软件复制至主用设备闪存：

copy tftp://*server*[*/path*]*/asa_image_name* {**disk0:/** | **disk1:/**}[*path/*]*asa_image_name*

示例：

```
ciscoasa# copy tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

对于 TFTP 以外的其他方法，请见 **copy** 命令。

步骤 3　将 ASDM 映像复制至主用设备闪存：

copy tftp://*server*[*/path*]*/asdm_image_name* {**disk0:/** | **disk1:/**}[*path/*]*asdm_image_name*

示例：

```
ciscoasa# copy tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

步骤 4　如果您当前未处于全局配置模式中，请访问全局配置模式：

```
configure terminal
```

步骤 5　显示当前配置的启动映像 （最多 4 个）：

```
show running-config boot system
```

示例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa914-smp-k8.bin
```

ASA 将按列出的顺序使用映像；如果第一个映像不可用，则使用第二个映像，以此类推。您无法在列表顶端插入新映射 URL；要将新映像指定为第一个映像，您必须根据步骤 6 和步骤 7 移除任何现有条目，并按所需的顺序输入映像 URL。

步骤 6　请删除所有的现有启动映像配置，以便您能够输入作为首选的新启动映像：

no boot system {**disk0:/** | **disk1:/**}[*path***/**]*asa_image_name*

示例：

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa914-smp-k8.bin
```

步骤 7　设置要启动的 ASA 映像 （您刚上传的映像）：

boot system {**disk0:/** | **disk1:/**}[*path***/**]*asa_image_name*

示例：

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

如果此映像不可用，请对要使用的任何备份映像重复运行此命令。例如，您可以重新输入之前在步骤 6 中移除的映像。

步骤 8　设置要使用的 ASDM 映像 （您刚上传的映像）：

asdm image {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

示例：

```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

您只能配置一个要使用的 ASDM 映像，因此，您不需要先删除现有配置。

步骤 9　将新设置保存至启动配置：

write memory

步骤 10　重新加载 ASA：

reload

升级故障转移对或 ASA 集群

- 第 36-4 页的升级主用/备用故障转移对
- 第 36-6 页的升级主用/主用故障转移对
- 第 36-8 页的升级 ASA 集群

升级主用/备用故障转移对

如要升级主用/备用故障转移对，请执行以下步骤。

准备工作

在主用设备上执行这些步骤。

操作步骤

步骤 1　（如果有配置迁移）在终端显示配置，以便您能够备份配置：

more system:running-config

示例：

```
active# more system:running-config
```

复制此命令的输出，然后将配置粘贴到文本文件中。有关其他备份方法的信息，请参阅配置指南。

步骤 2　将 ASA 软件复制至主用设备闪存：

copy tftp://*server*[*/path*]*/asa_image_name* {**disk0:/** | **disk1:/**}[*path/*]*asa_image_name*

示例：

```
active# copy tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

对于 TFTP 以外的其他方法，请见 **copy** 命令。

步骤 3　将软件复制到备用设备；请确保指定与主用设备相同的路径：

failover exec mate copy /noconfirm tftp://*server*[*/path*]*/filename* {**disk0:/** | **disk1:/**}[*path/*]*filename*

示例：

```
active# failover exec mate copy /noconfirm tftp://10.1.1.1/asa931-smp-k8.bin
disk0:/asa931-smp-k8.bin
```

步骤 4　将 ASDM 映像复制至主用设备闪存：

copy tftp://*server*[*/path*]*/asdm_image_name* {**disk0:/** | **disk1:/**}[*path/*]*asdm_image_name*

示例：

```
active# copy tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

步骤 5　将 ASDM 映像复制至备用设备；请确保指定与主用设备相同的路径：

failover exec mate copy /noconfirm tftp://*server*[*/path*]*/asdm_image_name* {**disk0:/** | **disk1:/**}[*path/*]*asdm_image_name*

示例：

```
active# failover exec mate copy /noconfirm tftp://10.1.1.1/asdm-731.bin
disk0:/asdm-731.bin
```

步骤 6　如果您当前未处于全局配置模式中，请访问全局配置模式：

configure terminal

步骤 7　显示当前配置的启动映像 （最多 4 个）：

show running-config boot system

示例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa921-smp-k8.bin
```

ASA 将按列出的顺序使用映像；如果第一个映像不可用，则使用第二个映像，以此类推。您无法在列表顶端插入新映射 URL；要将新映像指定为第一个映像，您必须根据步骤 8 和步骤 9 移除任何现有条目，并按所需的顺序输入映像 URL。

步骤 8　请删除所有的现有启动映像配置，以便您能够输入作为首选的新启动映像：

no boot system {**disk0:/** | **disk1:/**}[*path/*]*asa_image_name*

示例：

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa921-smp-k8.bin
```

步骤 9　设置要启动的 ASA 映像 （您刚上传的映像）：

boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

示例：

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

如果此映像不可用，请对要使用的任何备份映像重复运行此命令。例如，您可以重新输入之前在步骤 8中移除的映像。

步骤 10　设置要使用的 ASDM 映像 （您刚上传的映像）：

asdm image {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

示例：

```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

您只能配置一个要使用的 ASDM 映像，因此，您不需要先删除现有配置。

步骤 11　将新设置保存至启动配置：

write memory

步骤 12　重新加载备用设备，以便启动新映像：

failover reload-standby

等待备用设备完成加载。使用 **show failover** 命令，以便验证备用设备是否处于 Standby Ready 状态。

步骤 13　强行要求主用设备故障转移至备用设备：

no failover active

步骤 14　重新加载以前的主用设备 （当前的新备用设备）：

reload

如果您想要此设备在重新加载后，还原为主用状态，请输入 **failover active** 命令。

升级主用/主用故障转移对

如要升级处于主用/主用故障转移配置的两台设备，请执行以下步骤。

准备工作

在系统执行空间中执行以下步骤。另外请在主设备上执行这些步骤。

操作步骤

步骤 1　（如果有配置迁移）在终端显示配置，以便您能够备份配置：

more system:running-config

复制此命令的输出，然后将配置粘贴到文本文件中。有关其他备份方法的信息，请参阅配置指南。

步骤 2　将 ASA 软件复制至主设备闪存：

copy tftp://*server*[**/***path*]**/***asa_image_name* {**disk0:/** | **disk1:/**}[*path***/**]*asa_image_name*

示例：

```
primary# copy tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

对于 TFTP 以外的其他方法，请见 **copy** 命令。

步骤 3　将软件复制至辅助设备；请确保指定与主设备相同的路径：

failover exec mate copy /noconfirm tftp://*server*[**/***path*]**/***filename* {**disk0:/** | **disk1:/**}[*path***/**]*filename*

示例：

```
primary# failover exec mate copy /noconfirm tftp://10.1.1.1/asa931-smp-k8.bin
disk0:/asa931-smp-k8.bin
```

步骤 4　将 ASDM 映像复制至主设备闪存：

copy tftp://*server*[**/***path*]**/***asdm_image_name* {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

示例：

```
primary# copy tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

步骤 5　将 ASDM 映像复制至辅助设备；请确保指定与主用设备相同的路径：

failover exec mate copy /noconfirm tftp://*server*[**/***path*]**/***asdm_image_name* {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

示例：

```
primary# failover exec mate copy /noconfirm tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

步骤 6　使两个故障转移组在主设备上均处于活动状态：

```
failover active group 1
failover active group 2
```

步骤 7　如果您当前未处于全局配置模式中，请访问全局配置模式：

configure terminal

示例：

```
primary(config)# configure terminal
```

步骤 8　显示当前配置的启动映像 （最多 4 个）：

show running-config boot system

示例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa921-smp-k8.bin
```

ASA 将按列出的顺序使用映像；如果第一个映像不可用，则使用第二个映像，以此类推。您无法在列表顶端插入新映射 URL；要将新映像指定为第一个映像，您必须根据步骤 9 和步骤 10 移除任何现有条目，并按所需的顺序输入映像 URL。

步骤 9　请删除所有的现有启动映像配置，以便您能够输入作为首选的新启动映像：

no boot system {**disk0:/** | **disk1:/**}[*path***/**]*asa_image_name*

示例：

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa921-smp-k8.bin
```

步骤 10　设置要启动的 ASA 映像 （您刚上传的映像）：

boot system {**disk0:/** | **disk1:/**}[*path***/**]*asa_image_name*

示例：

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

如果此映像不可用，请对要使用的任何备份映像重复运行此命令。例如，您可以重新输入之前在步骤 9 中移除的映像。

步骤 11　设置要使用的 ASDM 映像 （您刚上传的映像）：

asdm image {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

示例：

```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

您只能配置一个要使用的 ASDM 映像，因此，您不需要先删除现有配置。

步骤 12　将新设置保存至启动配置：

write memory

步骤 13　重新加载辅助设备，以便启动新映像：

failover reload-standby

等待辅助设备完成加载。使用 **show failover** 命令验证两个故障转移组，是否均处于 Standby Ready 状态。

步骤 14　强行要求两个故障转移组在辅助设备上变为活动状态：

```
no failover active group 1
no failover active group 2
```

步骤 15　重新加载主设备：

reload

如果使用 **preempt** 命令配置故障转移组，在抢占延迟过后，它们会在其指定设备上自动变为活动状态。如果未使用 **preempt** 命令配置故障转移组，您可以使用 **failover active group** 命令，使它们在其指定设备上返回活动状态。

升级 ASA 集群

如要升级 ASA 集群中的所有设备，请在主设备上执行以下步骤。对于多情景模式，请在系统执行空间中执行以下步骤。

操作步骤

步骤 1　（如果要进行配置迁移）备份您的配置文件：

more system:running-config

复制此命令的输出，然后将配置粘贴到文本文件中。有关其他备份方法的信息，请参阅常规操作配置指南。

步骤 2　将 ASA 软件复制至集群中的所有设备：

cluster exec copy /noconfirm tftp://*server*[*/path*]*/asa_image_name* {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

示例：

```
master# cluster exec copy /noconfirm tftp://10.1.1.1/asa931-smp-k8.bin
disk0:/asa931-smp-k8.bin
```

对于 TFTP 以外的其他方法，请见 **copy** 命令。

步骤 3　将 ASDM 映像复制至集群中的所有设备：

cluster exec copy /noconfirm tftp://*server*[*/path*]*/asdm_image_name* {**disk0:/** | **disk1:/**}[*path*/]*asdm_image_name*

示例：

```
master# cluster exec copy /noconfirm tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

步骤 4　如果您当前未处于全局配置模式中，请访问全局配置模式：

configure terminal

步骤 5　显示当前配置的启动映像 （最多 4 个）：

show running-config boot system

示例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa921-smp-k8.bin
```

ASA 将按列出的顺序使用映像；如果第一个映像不可用，则使用第二个映像，以此类推。您无法在列表顶端插入新映射 URL；要将新映像指定为第一个映像，您必须根据步骤 6 和步骤 7 移除任何现有条目，并按所需的顺序输入映像 URL。

步骤 6　请删除所有的现有启动映像配置，以便您能够输入作为首选的新启动映像：

no boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

示例：

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa921-smp-k8.bin
```

步骤 7　设置要启动的 ASA 映像 （您刚上传的映像）：

boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

示例：

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

如果此映像不可用，请对要使用的任何备份映像重复运行此命令。例如，您可以重新输入之前在步骤 6 中移除的映像。

步骤 8　设置要使用的 ASDM 映像 （您刚上传的映像）：

asdm image {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

示例：

```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

您只能配置一个要使用的 ASDM 映像，因此，您不需要先删除现有配置。

步骤 9　将新设置保存至启动配置：

```
write memory
```

步骤 10　当您对每个设备名称重复此命令时，会重新加载每台从属设备：

```
cluster exec unit slave-unit reload noconfirm
```

示例：

```
master# cluster exec unit unit2 reload noconfirm
```

如要避免连接中断并保持流量稳定，请在重新加载下一台设备之前，等待每台设备恢复运行（约 5 分钟）。要查看成员名称，请输入 **cluster exec unit ?**，或者输入 **show cluster info** 命令。

步骤 11　在主设备上禁用集群：

```
no enable
```

等待 5 分钟，以便系统选出新的主设备，并且流量变得稳定。请勿输入 **write memory**；当主设备重新加载时，您可能会想要在其上启用集群。

步骤 12　重新加载主设备：

```
reload noconfirm
```

发生新一轮的新主设备选择。当以前的主设备重新加入集群时，它将成为从属设备。

管理文件

- 第 36-10 页的查看闪存中的文件
- 第 36-11 页的从闪存中删除文件
- 第 36-11 页的擦除闪存文件系统
- 第 36-11 页的配置文件访问
- 第 36-15 页的将文件复制到 ASA
- 第 36-17 页的将文件复制至启动或运行配置

查看闪存中的文件

您可以查看闪存中的文件，并查看有关文件的信息，如下所示：

- 如要查看闪存中的文件，请输入以下命令：

  ```
  ciscoasa# dir [disk0: | disk1:]
  ```

  对于内部闪存，请输入 **disk0**。 **disk1** 关键字表示外部闪存。内部闪存是默认值。

  例如：

  ```
  hostname# dir

  Directory of disk0:/
  500    -rw-  4958208     22:56:20 Nov 29 2004  cdisk.bin
  2513   -rw-  4634        19:32:48 Sep 17 2004  first-backup
  2788   -rw-  21601       20:51:46 Nov 23 2004  backup.cfg
  2927   -rw-  8670632     20:42:48 Dec 08 2004  asdmfile.bin
  ```

- 如要查看有关特定文件的扩展信息，请输入以下命令：

  ```
  hostname# show file information [path:/]filename
  ```

  默认路径是内部闪存的根目录 (disk0:/)。

  例如：

  ```
  hostname# show file information cdisk.bin

  disk0:/cdisk.bin:
  type is image (XXX) []
    file size is 4976640 bytes version 7.0(1)
  ```

  列出的文件大小仅用作示例。

从闪存中删除文件

您可以从闪存中删除不再需要的文件。要从闪存中删除文件，请输入以下命令：

```
hostname# delete disk0: filename
```

默认情况下，如果您未指定路径，将从当前工作目录中删除文件。删除文件时，您可以使用通配符。系统会提示您，要删除的文件的文件名，然后您必须确认删除。

擦除闪存文件系统

如要擦除闪存文件系统，请执行以下步骤：

步骤 1　按照第 2-2 页的访问 ASA 服务模块控制台或第 2-1 页的访问设备控制台中的说明，连接至 ASA 控制台端口。

步骤 2　关闭 ASA，然后再启动。

步骤 3　在启动过程中，系统提示您进入 ROMMON 模式时，请按 **Escape** 键。

步骤 4　输入 **erase** 命令，这会覆盖所有文件并擦除文件系统，包括隐藏的系统文件。

```
rommon #1> erase [disk0: | disk1: | flash:]
```

配置文件访问

- 第 36-12 页的配置 FTP 客户端模式
- 第 36-12 页的将 ASA 配置为安全复制服务器
- 第 36-13 页的自定义 ASA 安全复制客户端
- 第 36-14 页的配置 ASA TFTP 客户端路径

配置 FTP 客户端模式

ASA 可使用 FTP，向 FTP 服务器上传映像文件或配置文件，或者从中下载这些文件。在被动 FTP 模式中，客户端发起控制连接和数据连接。服务器是被动模式中的数据连接的接收方，会响应其针对特定连接而侦听的端口号。

详细步骤

命令	用途
ftp mode passive **示例：** `ciscoasa(config)# ftp mode passive`	将 FTP 模式设置为被动。

将 ASA 配置为安全复制服务器

您可以在 ASA 上，启用安全复制 (SCP) 服务器。只有被允许使用 SSH 访问 ASA 的客户端，可以建立安全复制连接。

限制

- 该服务器没有目录支持。目录支持的缺乏，会限制远程客户端访问 ASA 的内部文件。
- 该服务器不支持欢迎信息。
- 该服务器不支持通配符。

先决条件

- 根据 第 35-4 页的配置 SSH 访问，在 ASA 上启用 SSH。
- ASA 许可证必须具有强加密 (3DES/AES) 许可证，才能支持 SSH V2 连接。

详细步骤

命令	用途
ssh scopy enable **示例：** `ciscoasa(config)# ssh scopy enable`	启用 SCP 服务器。

示例

在外部主机上的客户端中，执行 SCP 文件传输。例如，在 Linux 中输入以下命令：

scp -v -pw *password source_filename username@asa_address*:{**disk0**|**disk1**}:/*dest_filename*

-v 表示详细，如果您未指定 **-pw**，会收到输入密码的提示。

自定义 ASA 安全复制客户端

您可以使用板载 SCP 客户端，将文件复制至 ASA，或者从中复制文件 （请参阅 第 36-15 页的将文件复制到 ASA）。此部分允许您自定义 SCP 客户端操作。

先决条件

对于多情景模式，请在系统执行空间中完成本操作步骤。要从该情景切换至系统执行空间，请输入 **changeto system** 命令。

详细步骤

	命令	用途
步骤 1	**[no] ssh stricthostkeycheck** **示例：** ciscoasa# ssh stricthostkeycheck ciscoasa# copy x scp://cisco@10.86.95.9/x The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established. RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a. Are you sure you want to continue connecting (yes/no)? **yes** Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts. Source filename [x]? Address or name of remote host [10.86.95.9]? Destination username [cisco]? Destination password []?cisco123 Destination filename [x]?	启用或禁用 SSH 主机密钥检查。默认情况下，系统会启用此选项。启用此选项时，如果主机密钥尚未存储在 ASA 上，系统会提示您选择接受或拒绝主机密钥。禁用此选项时，如果以前没有存储主机密钥，ASA 会自动接受主机密钥。
步骤 2	**ssh pubkey-chain** **[no] server** *ip_address* **{key-string** *key_string* **exit**| **key-hash** {**md5** | **sha256**} *fingerprint*} **示例：** ciscoasa(config)# ssh pubkey-chain ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9 ciscoasa(config-ssh-pubkey-server)# key-string Enter the base 64 encoded RSA public key. End with the word "exit" on a line by itself ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87 ciscoasa(config-ssh-pubkey-server-string)# exit ciscoasa(config-ssh-pubkey-server)# show running-config ssh pubkey-chain ssh pubkey-chain server 10.7.8.9 key-hash sha256 f1:22:49:47:b6:76:74:b2:db:26:fb:13:65:d8:99:19:e7:9e:24:46:59:be:13:7f:25:27:70:9b:0e:d2:86:12	ASA 会存储其所连接至的每个 SCP 服务器的 SSH 主机密钥。您可以在 ASA 数据库中，视需要手动添加或删除服务器及其密钥。 对于每个服务器，您可以指定 SSH 主机的 **key-string**（公钥）或 **key-hash**（哈希值）。 *key_string* 是远端对等体的采用 Base64 编码的 RSA 公钥。您可以从打开的 SSH 客户端 （即 .ssh/id_rsa.pub 文件）获得公钥值。在您提交采用 Base64 编码的公钥之后，系统会通过 SHA-256 对其进行哈希处理。 **key-hash**{**md5** | **sha256**}*fingerprint* 可用于输入已经过哈希处理的密钥 （使用 MD5 或 SHA-256 密钥）；例如，您从 **show** 命令输出复制的密钥。

示例

以下示例会为处于 10.86.94.170 的服务器，添加已经过哈希处理的主机密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:
2e:19
```

以下示例会为处于 10.7.8.9 的服务器，添加主机字符串密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

配置 ASA TFTP 客户端路径

TFTP 是一种简单的客户端/服务器文件传输协议，RFC 783 和 RFC 1350 修订版对其进行了描述。2.您可以将 ASA 配置为 TFTP *客户端*，以便其可以将文件复制至 TFTP *服务器*，或者从中复制文件（请参阅 第 36-15 页的将文件复制到 ASA和第 36-23 页的备份和还原 配置或其他文件。这样，您可以备份配置文件，并将其传播至多台 ASA。

此部分允许您预定义到 TFTP 服务器的路径，这样您就无需在诸如 **copy** 和 **configure net** 的命令中，输入该路径。

详细步骤

命令	用途
tftp-server *interface_name server_ip filename* **示例：** `ciscoasa(config)# tftp-server inside 10.1.4.7 files/config1.cfg` `ciscoasa(config)# copy tftp: test.cfg` `Address or name of remote host [10.1.4.7]?` `Source filename [files/config1.cfg]?`**`config2.cfg`** `Destination filename [test.cfg]?` `Accessing tftp://10.1.4.7/files/config2.cfg;int=outside...`	预定义用于 **configure net** 和 **copy** 命令的 TFTP 服务器地址和文件名。输入命令时，您可以覆盖文件名；例如，当您使用 **copy** 命令时，您可以利用预定义的 TFTP 服务器地址，但仍然在交互式提示符处输入任意文件名。 对于 copy 命令，请输入 **tftp:** 来使用 tftp-server 值，而不是输入 **tftp://***url*。

将文件复制到 ASA

本部分介绍如何复制应用映像、 ASDM 软件、配置文件，或者任何其他需要从 TFTP、 FTP、 SMB、 HTTP、 HTTPS 或 SCP 服务器下载至内部或外部闪存的文件。

准则

- 对于 IPS SSP 软件模块，在您将 IPS 软件下载至 disk0 之前，请确保至少 50% 的闪存可用。当您安装 IPS 时，IPS 会为其文件系统保留 50% 的内部闪存。
- 您不能在闪存中的相同目录下，拥有两个名称相同，但字母大小写不同的文件。例如，如果您尝试将文件 Config.cfg 下载至包含 config.cfg 文件的位置，您会收到以下错误消息：

  ```
  %Error opening disk0:/Config.cfg (File exists).
  ```

- 有关安装 Cisco SSL VPN 客户端的信息，请参阅 *《思科 AnyConnect VPN 客户端管理员指南》*。有关在 ASA 上安装思科安全桌面的信息，请参阅 *《面向思科 ASA 5500 系列管理员的思科安全桌面配置指南》*。
- 如要配置 ASA，以便使用特定应用映像或 ASDM 映像 （如果您安装了多个映像，或者将它们安装在外部闪存中），请参阅第 36-19 页的配置要使用的映像和启动配置。
- 对于多情景模式，您必须处于系统执行空间。

详细步骤

命令	用途
copy [/noconfirm] tftp://*server[/path]/src_filename* **{disk0|disk1}:/[***path/***]***dest_filename* **示例：** `ciscoasa# copy tftp://10.1.1.67/files/context1.cfg disk0:/context1.cfg` `Address or name of remote host [10.1.1.67]?` `Source filename [files/context1.cfg]?` `Destination filename [context1.cfg]?` `Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b` `!!!!!!!!!!!` `11143 bytes copied in 5.710 secs (2228 bytes/sec)`	从 TFTP 服务器复制文件。

命令	用途
copy [**/noconfirm**] **ftp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***src_filename* {**disk0**|**disk1**}**:/**[*path***/**]*dest_filename* **示例：** ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/context1.cfg disk0:/contexts/context1.cfg Address or name of remote host [10.1.1.67]? Source username [jcrichton]? Source password [aeryn]? Source filename [files/context1.cfg]? Destination filename [contexts/context1.cfg]? Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b !!!!!!!!!!! 11143 bytes copied in 5.710 secs (2228 bytes/sec)	从 FTP 服务器复制文件。
copy [**/noconfirm**] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][**/***path*]**/***src_filename* {**disk0**|**disk1**}**:/**[*path***/**]*dest_filename* **示例：** ciscoasa# copy https://asun:john@10.1.1.67/files/moya.cfg disk0:/contexts/moya.cfg Address or name of remote host [10.1.1.67]? Source username [asun]? Source password [john]? Source filename [files/moya.cfg]? Destination filename [contexts/moya.cfg]? Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b !!!!!!!!!!! 11143 bytes copied in 5.710 secs (2228 bytes/sec)	从 HTTP 服务器复制文件。
copy [**/noconfirm**] **smb://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***src_filename* {**disk0**|**disk1**}**:/**[*path***/**]*dest_filename* **示例：** ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/test.xml disk0:/test.xml Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b !!!!!!!!!!! 11143 bytes copied in 5.710 secs (2228 bytes/sec)	从 SMB 服务器复制文件。

命令	用途
copy [**/noconfirm**] **scp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***src_filename*[**;int=***interface_name*] {**disk0**|**disk1**}**:/**[*path/*]*dest_filename* **示例：** ciscoasa# copy scp://pilot@10.86.94.170/test.cfg disk0:/test.cfg Address or name of remote host [10.86.94.170]? Source username [pilot]? Destination filename [test.cfg]? The authenticity of host '10.86.94.170 (10.86.94.170)' can't be established. RSA key fingerprint is <65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d: 2d:bf:a9:2b:85:2e:19>(SHA256). Are you sure you want to continue connecting (yes/no)?yes Please use the following commands to add the hash key to the configuration: ssh pubkey-chain server 10.86.94.170 key-hash sha256 65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2 d:bf:a9:2b:85:2e:19 Password: <type in password> !!!!!! 6006 bytes copied in 8.160 secs (750 bytes/sec)	从 SCP 服务器复制文件。**;int=***interface* 选项会绕过路由查找，并始终使用指定接口来访问 SCP 服务器。

将文件复制至启动或运行配置

您可以将文本文件从 TFTP、 FTP、 SMB、 HTTP 或 SCP 服务器，或者从闪存，下载至运行或启动配置。

如要配置 ASA，以便将特定配置用作启动配置，请参阅第 36-19 页的配置要使用的映像和启动配置。

准则

当您将配置复制至运行配置时，会合并这两个配置。合并会将新配置中的所有新命令添加至运行配置。如果配置相同，则不会发生更改。如果命令有冲突，或者如果命令影响情景运行，则合并的效果取决于命令。可能出现错误，或者出现意外结果。

详细步骤

如要将文件复制至启动配置或运行配置，请针对适当的下载服务器，输入以下任一命令：

命令	用途
copy [/noconfirm] tftp://*server[/path]/src_f***ilename {startup-config | running-config}** **示例：** ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config	从 TFTP 服务器复制文件。
copy [**/noconfirm**] **ftp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***src_filename* {**startup-config** | **running-config**} **示例：** ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/old-startup.cfg startup-config	从 FTP 服务器复制文件。
copy [**/noconfirm**] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][**/***path*]**/***src_filename* {**startup-config** | **running-config**} **示例：** ciscoasa# copy https://asun:john@10.1.1.67/files/new-running.cfg running-config	从 HTTP 服务器复制文件。
copy [**/noconfirm**] **smb://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***src_filename* {**startup-config** | **running-config**} **示例：** ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/new-running.cfg running-config	从 SMB 服务器复制文件。
copy [**/noconfirm**] **scp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***src_filename*[**;int=***interface_name*] {**startup-config** | **running-config**} **示例：** ciscoasa# copy scp://pilot:moya@10.86.94.170/new-startup.cfg startup-config	从 SCP 服务器复制文件。**;int=***interface* 选项会绕过路由查找，并始终使用指定接口来访问 SCP 服务器。

示例

例如，如要从 TFTP 服务器复制配置，请输入以下命令：

```
ciscoasa# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

如要从 FTP 服务器复制配置，请输入以下命令：

```
ciscoasa# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

如要从 HTTP 服务器复制配置，请输入以下命令：

```
ciscoasa# copy http://209.165.200.228/configs/startup.cfg startup-config
```

配置要使用的映像和启动配置

如果您有多台 ASA 或多个 ASDM 映像，应指定想要启动的映像。如果您不设置映像，则会使用默认启动映像，并且该映像可能不是想要使用的映像。对于启动配置，您或者可以指定配置文件。

默认设置

ASA Image

- Physical ASA - 启动其在内部闪存中找到的第一个应用映像。
- ASAv - 启动您在首次部署时创建的只读 boot:/ 分区中的映像。您可以升级闪存中的映像，并配置 ASAv，以便从该映像启动。请注意，如果您随后清除您的配置 (**clear configure all**)，则 ASAv 将还原为加载原始部署映像。

ASDM Image

All ASA - 启动其在内部闪存中 （或者，如果此位置不存在映像，则在外部闪存中）找到的第一个 ASDM 映像。

Startup Configuration

默认情况下，ASA 会从是隐藏文件的启动配置启动。

详细步骤

	命令	用途
步骤 1	**boot system** *url* **示例：** `ciscoasa(config)# boot system disk:/images/asa921.bin`	设置 ASA 启动映像的位置。 URL 可以是： • {**disk0:/** | **disk1:/**}[*path*/]*filename* • **tftp://**[*user*[**:*password***]**@**]*server*[:*port*]/[*path*/]*filename* 并非所有型号都支持 TFTP 选项。 您可以输入最多四个 **boot system** 命令条目，以便指定按顺序启动的不同映像；ASA 将启动其成功找到的第一个映像。当您输入 **boot system** 命令时，该命令会在列表的底部添加一个条目。如要对启动条目重新排序，您必须使用 **clear configure boot system** 命令移除所有条目，然后按所需顺序，重新输入这些条目。仅可配置一条 **boot system tftp** 命令，而且该命令必须是第一条配置的命令。 **注**　如果 ASA 陷入不断启动的循环中，您可以重新启动 ASA 至 ROMMON 模式。有关 ROMMON 模式的详细信息，请参阅第 38-1 页的查看调试消息。
步骤 2	**asdm image** {**disk0:/** | **disk1:/**}[*path*/]*filename* **示例：** `ciscoasa(config)# asdm image disk0:/images/asdm721.bin`	设置要启动的 ASDM 映像。如果您没有指定要启动的映像，即使仅安装了一个映像，ASA 也会在运行配置中插入 **asdm image** 命令。为了避免与自动更新 （如已配置）相关的问题，以及避免在每次启动时都搜索映像，您应在启动配置中指定想要启动的 ASDM 映像。

	命令	用途
步骤 3	（可选） **boot config** {**disk0:/** | **disk1:/**}[*path*/]*filename* **示例：** ciscoasa(config)# boot config disk0:/configs/startup1.cfg	将启动配置设置为一个已知文件，而不是默认的隐藏文件。

使用 ROM 监控模式加载映像

- 第 36-20 页的使用 ASA 5500-X 系列的 ROM 监控模式
- 第 36-21 页的使用 ASASM 的 ROM 监控模式

使用 ASA 5500-X 系列的 ROM 监控模式

如要在 ROM 监控模式中使用 TFTP 将软件映像加载到 ASA，请执行以下步骤：

步骤 1　按照第 2-1 页的访问设备控制台中的说明，连接至 ASA。

步骤 2　关闭 ASA，然后再启动。

步骤 3　在启动过程中，系统提示您进入 ROMMON 模式时，请按 **Escape** 键。

步骤 4　在 ROMMOM 模式中，定义 ASA 的接口设置，包括 IP 地址、 TFTP 服务器地址、网关地址、软件映像文件和端口，如下所示：

注　对于 ASA 5506、ASA 5506-W 和 ASA 5508，您不需要包括 PORT=Ethernet0/0 条目。仅管理端口可用。

```
rommon #1> ADDRESS=10.132.44.177
rommon #2> SERVER=10.129.0.30
rommon #3> GATEWAY=10.132.44.1
rommon #4> IMAGE=f1/asa800-232-k8.bin
rommon #5> PORT=Ethernet0/0
Ethernet0/0
Link is UP
MAC Address: 0012.d949.15b8
```

注　请确保已存在网络连接。

步骤 5　如要验证您的设置，请输入 **set** 命令。

```
rommon #6> set
ROMMON Variable Settings:
ADDRESS=10.132.44.177
  SERVER=10.129.0.30
  GATEWAY=10.132.44.1
  PORT=Ethernet0/0
  VLAN=untagged
  IMAGE=f1/asa840-232-k8.bin
```

```
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

步骤 6　输入 **ping server** 命令，从而 Ping TFTP 服务器。

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.129.0.30, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

步骤 7　输入 **tftp** 命令，从而加载软件映像。

```
rommon #8> tftp
ROMMON Variable Settings:
ADDRESS=10.132.44.177
  SERVER=10.129.0.30
  GATEWAY=10.132.44.1
  PORT=Ethernet0/0
  VLAN=untagged
  IMAGE=f1/asa840-232-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp f1/asa840-232-k8.bin@10.129.0.30 via 10.132.44.1

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2011

Loading...N
```

成功加载软件映像后， ASA 会自动退出 ROMMON 模式。

步骤 8　如要验证正确的软件映像是否已加载至 ASA，请输入以下命令检查 ASA 中的版本：

```
ciscoasa# show version
```

使用 ASASM 的 ROM 监控模式

如要在 ROM 监控模式中使用 TFTP 将软件映像加载到 ASASM，请执行以下步骤：

步骤 1　按照第 2-2 页的访问 ASA 服务模块控制台中的说明，连接至 ASA。

步骤 2　确保您重新加载了 ASASM 映像。

步骤 3　在启动过程中，系统提示您进入 ROMMON 模式时，请按 **Escape** 键。

步骤 4　在 ROMMOM 模式中，定义 ASASM 的接口设置，包括 IP 地址、 TFTP 服务器地址、网关地址、软件映像文件、端口和 VLAN，如下所示：

```
rommon #1> ADDRESS=172.16.145.149
rommon #2> SERVER=172.16.171.125
rommon #3> GATEWAY=172.16.145.129
rommon #4> IMAGE=f1/asa851-smp-k8.bin
rommon #5> PORT=Data0
rommon #6> VLAN=1
```

```
Data0
Link is UP
MAC Address: 0012.d949.15b8
```

注　请确保已存在网络连接。

步骤 5　如要验证您的设置，请输入 **set** 命令。

```
rommon #7> set
ROMMON Variable Settings:
ADDRESS=172.16.145.149
  SERVER=172.16.171.125
  GATEWAY=172.16.145.129
  PORT=Data0
  VLAN=1
  IMAGE=f1/asa851-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20
```

步骤 6　输入 **ping server** 命令，从而 Ping TFTP 服务器。

```
rommon #8> ping server
Sending 20, 100-byte ICMP Echoes to server 172.16.171.125, timeout is 2 seconds:

Success rate is 100 percent (20/20)
```

步骤 7　输入 **tftp** 命令，从而加载软件映像。

```
rommon #9> tftp
Clearing EOBC receive queue ...
cmostime_set = 1
ROMMON Variable Settings:
ADDRESS=172.16.145.149
  SERVER=172.16.171.125
  GATEWAY=172.16.145.129
  PORT=Data0
  VLAN=1
  IMAGE=f1/asa851-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20

tftp f1/asa851-smp-k8.bin@172.16.171.125 via 172.16.145.129
Starting download.Press ESC to abort.
```

成功加载软件映像后，ASASM 会自动退出 ROMMON 模式。

注　ROMMON 启动完成后，您必须单独将映像下载至系统闪存；将模块启动至 ROMMON 模式在重新加载后，不会保留系统映像。

步骤 8　如要验证正确的软件映像是否已加载至 ASASM，请输入以下命令检查版本：

```
hostname# show version
```

备份和还原 配置或其他文件

- 第 36-23 页的备份单模式配置或多模式系统配置
- 第 36-24 页的备份闪存中的情景配置或其他文件
- 第 36-24 页的备份情景中的情景配置
- 第 36-25 页的从终端显示复制配置
- 第 36-25 页的使用导出和导入命令备份其他文件
- 第 36-25 页的使用脚本来备份和还原文件

备份单模式配置或多模式系统配置

在单情景模式中，或者从多模式中的系统配置中，您可以将启动配置或运行配置复制至外部服务器或本地闪存。

详细步骤

命令	用途
copy [/noconfirm] {startup-config | running-config} tftp://*server[/path]/dst_f***ilename** **示例：** ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg	将文件复制至 TFTP 服务器。
copy [**/noconfirm**] {**startup-config** | **running-config**} **ftp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***dst_filename* **示例：** ciscoasa# copy startup-config ftp://jcrichton:aeryn@10.1.1.67/files/new-startup.cfg	将文件复制至 FTP 服务器。
copy [**/noconfirm**] {**startup-config** | **running-config**} **smb://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***dst_filename* **示例：** ciscoasa# copy /noconfirm running-config smb://chiana:dargo@10.1.1.67/new-running.cfg	将文件复制至 SMB 服务器。
copy [**/noconfirm**] {**startup-config** | **running-config**} **scp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***dst_filename*[**;int=***interface_name*] **示例：** ciscoasa# copy startup-config scp://pilot:moya@10.86.94.170/new-startup.cfg	将文件复制至 SCP 服务器。**;int=***interface* 选项会绕过路由查找，并始终使用指定接口来访问 SCP 服务器。
copy [**/noconfirm**] {**startup-config** | **running-config**} {**disk0**|**disk1**}**:/**[*path/*]*dst_filename* **示例：** ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg	将文件复制至本地闪存。请确保目标目录存在。如果该目标不存在，请先使用 **mkdir** 命令创建目录。

备份闪存中的情景配置或其他文件

通过在系统执行空间中输入以下任一命令，可以复制本地闪存中的情景配置或其他文件。

详细步骤

命令	用途
copy [/noconfirm] {disk0|disk1}:/[*path/*]*src_filename* tftp://*server*[/*path*]/*dst_filename* **示例：** ciscoasa# copy disk0:/asa-os.bin tftp://10.1.1.67/files/asa-os.bin	从闪存复制至 TFTP 服务器。
copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **ftp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***dst_filename* **示例：** ciscoasa# copy disk0:/asa-os.bin ftp://jcrichton:aeryn@10.1.1.67/files/asa-os.bin	从闪存复制至 FTP 服务器。
copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **smb://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***dst_filename* **示例：** ciscoasa# copy /noconfirm copy disk0:/asdm.bin smb://chiana:dargo@10.1.1.67/asdm.bin	从闪存复制至 SMB 服务器。
copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **scp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***dst_filename*[**;int=***interface_name*] **示例：** ciscoasa# copy disk0:/context1.cfg scp://pilot:moya@10.86.94.170/context1.cfg	从闪存复制至 SCP 服务器。**;int=***interface* 选项会绕过路由查找，并始终使用指定接口来访问 SCP 服务器。
copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dst_filename* **示例：** ciscoasa# copy /noconfirm disk1:/file1.cfg disk0:/file1.cfgnew-running.cfg	从闪存复制到本地闪存。请确保目标目录存在。如果该目标不存在，请先使用 **mkdir** 命令创建目录。

备份情景中的情景配置

在多情景模式中，您可以从情景中执行以下备份操作：

- 如要将运行配置复制至启动配置服务器 （连接至管理情景），请输入以下命令：

  ciscoasa/contexta# **copy running-config startup-config**

- 如要将运行配置复制至已连接至情景网络的 TFTP 服务器，请输入以下命令：

  ciscoasa/contexta# **copy running-config tftp:/***server*[/*path*]/*filename*

从终端显示复制配置

如要将配置显示至终端，请输入以下命令：

```
ciscoasa# show running-config
```

请复制此命令的输出，然后将配置粘贴至文本文件。

使用导出和导入命令备份其他文件

对您的配置至关重要的其他文件可能包括以下文件：

- 您使用 **import webvpn** 命令导入的文件。目前，这些文件包括自定义、 URL 列表、网络内容、插件和语言转换文件。
- DAP 策略 (dap.xml)。
- CSD 配置 (data.xml)。
- 数字密钥和证书。
- 本地 CA 用户数据库和证书状态文件。

CLI 允许您使用 **export** 和 **import** 命令备份和还原配置的各个元素。

如要备份这些文件，例如，您使用 **import webvpn** 命令导入的那些文件或证书，请执行以下步骤：

步骤 1　运行适用的 **show** 命令，如下所示：

```
ciscoasa # show import webvpn plug-in
ica
rdp
ssh, telnet
vnc
```

步骤 2　对于您想要备份的文件，请运行 **export** 命令 （在本示例中，即 rdp 文件）：

```
ciscoasa # export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

使用脚本来备份和还原文件

您可以使用脚本来备份和还原 ASA 上的配置文件，包括通过 **import webvpn** CLI 命令导入的所有扩展文件、CSD 配置 XML 文件和 DAP 配置 XML 文件。出于安全原因，我们不建议您执行数字密钥和证书或者本地 CA 密钥的自动备份。

本部分对此操作提供说明，并包含您可以原样使用，或根据环境要求修改后使用的示例脚本。此示例脚本特定于 Linux 系统。要将其用于 Microsoft Windows 系统，您需要运用此示例的逻辑对其进行修改。

注　现有 CLI 允许您使用 **copy**、 **export** 和 **import** 命令备份和还原个别文件。但是，它没有允许您在一次操作中备份所有 ASA 配置文件的工具。运行脚本便于使用多个 CLI。

- 第 36-26 页的先决条件
- 第 36-26 页的运行脚本
- 第 36-26 页的示例脚本

先决条件

如要使用脚本备份和还原 ASA 配置，请先执行以下任务：

- 使用 Expect 模块安装 Perl。
- 安装可以访问 ASA 的 SSH 客户端。
- 安装 TFTP 服务器，以便将文件从 ASA 发送至备份站点。

还有一个选项是使用商用工具。您可以将此脚本的逻辑运用于此类工具。

运行脚本

如要运行备份和还原脚本，请执行以下步骤：

步骤 1　将脚本文件下载或剪切并粘贴至您系统上的任意位置。

步骤 2　在命令行中，输入 **Perl** *scriptname*，其中 *scriptname* 是脚本文件的名称。

步骤 3　按 **Enter** 键。

步骤 4　系统会提示您输入每个选项的值。或者，您可以在输入 **Perl** *scriptname* 命令时，在按 **Enter** 之前输入选项的值。无论采用哪种方式，脚本都会要求您输入每个选项的值。

步骤 5　脚本会开始运行，显示其发出的命令，这可以为您提供 CLI 内容的记录。您可以将这些 CLI 内容用于将来的还原，当您想要仅还原一个或两个文件时，它们特别有用。

示例脚本

```
#!/usr/bin/perl
#Function: Backup/restore configuration/extensions to/from a TFTP server.
#Description: The objective of this script is to show how to back up
configurations/extensions before the backup/restore command is developed.
# It currently backs up the running configuration, all extensions imported via "import
webvpn" command, the CSD configuration XML file, and the DAP configuration XML file.
#Requirements: Perl with Expect, SSH to the ASA, and a TFTP server.
#Usage: backupasa -option option_value
#       -h: ASA hostname or IP address
#       -u: User name to log in via SSH
#       -w: Password to log in via SSH
#       -e: The Enable password on the security appliance
#       -p: Global configuration mode prompt
#       -s: Host name or IP address of the TFTP server to store the configurations
#       -r: Restore with an argument that specifies the file name.This file is produced
during backup.
#If you don't enter an option, the script will prompt for it prior to backup.
#
#Make sure that you can SSH to the ASA.

use Expect;
use Getopt::Std;

#global variables
%options=();
$restore = 0; #does backup by default
$restore_file = '';
$asa = '';
$storage = '';
```

```
$user = '';
$password = '';
$enable = '';
$prompt = '';
$date = `date +%F';
chop($date);
my $exp = new Expect();

getopts("h:u:p:w:e:s:r:",\%options);
do process_options();

do login($exp);
do enable($exp);
if ($restore) {
   do restore($exp,$restore_file);
}
else {
   $restore_file = "$prompt-restore-$date.cli";
   open(OUT,">$restore_file") or die "Can't open $restore_file\n";
   do running_config($exp);
   do lang_trans($exp);
   do customization($exp);
   do plugin($exp);
   do url_list($exp);
   do webcontent($exp);
   do dap($exp);
   do csd($exp);
   close(OUT);
}
do finish($exp);

sub enable {
   $obj = shift;
   $obj->send("enable\n");
   unless ($obj->expect(15, 'Password:')) {
      print "timed out waiting for Password:\n";
   }
   $obj->send("$enable\n");
   unless ($obj->expect(15, "$prompt#")) {
      print "timed out waiting for $prompt#\n";
   }
}

sub lang_trans {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn translation-table\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /Translation Tables/;
     next unless (/^.+\s+.+$/);
     ($lang, $transtable) = split(/\s+/,$_);
     $cli = "export webvpn translation-table $transtable language $lang
$storage/$prompt-$date-$transtable-$lang.po";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
```

```
      $obj->expect(15, "$prompt#" );
    }
}

sub running_config {
  $obj = shift;
  $obj->clear_accum();
  $cli ="copy /noconfirm running-config $storage/$prompt-$date.cfg";
  print "$cli\n";
  $obj->send("$cli\n");
  $obj->expect(15, "$prompt#" );
}


sub customization {
  $obj = shift;
  $obj->clear_accum();
  $obj->send("show import webvpn customization\n");
  $obj->expect(15, "$prompt#" );
  $output = $obj->before();
  @items = split(/\n+/, $output);

  for (@items) {
    chop;
    next if /^Template/ or /show import/ or /^\s*$/;
    $cli = "export webvpn customization $_ $storage/$prompt-$date-cust-$_.xml";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
  }
}

sub plugin {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn plug-in\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/;
     $cli = "export webvpn plug-in protocol $_ $storage/$prompt-$date-plugin-$_.jar";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub url_list {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn url-list\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);
```

```
   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/ or /No bookmarks/;
     $cli="export webvpn url-list $_ $storage/$prompt-$date-urllist-$_.xml";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub dap {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir dap.xml\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm dap.xml $storage/$prompt-$date-dap.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-dap.xml disk0:/dap.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub csd {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir sdesktop\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm sdesktop/data.xml $storage/$prompt-$date-data.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-data.xml disk0:/sdesktop/data.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub webcontent {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn webcontent\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /No custom/;
     next unless (/^.+\s+.+$/);
     ($url, $type) = split(/\s+/,$_);
     $turl = $url;
     $turl =~ s/\/\+//;
     $turl =~ s/\+\//-/;
```

```
      $cli = "export webvpn webcontent $url $storage/$prompt-$date-$turl";
      $ocli = $cli;
      $ocli =~ s/^export/import/;
      print "$cli\n";
      print OUT "$ocli\n";
      $obj->send("$cli\n");
      $obj->expect(15, "$prompt#" );
   }
}

sub login {
    $obj = shift;
    $obj->raw_pty(1);
    $obj->log_stdout(0); #turn off console logging.
    $obj->spawn("/usr/bin/ssh $user\@$asa") or die "can't spawn ssh\n";
    unless ($obj->expect(15, "password:" )) {
        die "timeout waiting for password:\n";
    }

    $obj->send("$password\n");

    unless ($obj->expect(15, "$prompt>" )) {
        die "timeout waiting for $prompt>\n";
    }
}

sub finish {
    $obj = shift;
    $obj->hard_close();
    print "\n\n";

}

sub restore {
   $obj = shift;
   my $file = shift;
   my $output;
   open(IN,"$file") or die "can't open $file\n";
   while (<IN>) {
      $obj->send("$_");
      $obj->expect(15, "$prompt#" );
      $output = $obj->before();
      print "$output\n";
   }
   close(IN);
}

sub process_options {
  if (defined($options{s})) {
      $tstr= $options{s};
      $storage = "tftp://$tstr";
  }
  else {
      print "Enter TFTP host name or IP address:";
      chop($tstr=<>);
      $storage = "tftp://$tstr";
  }
  if (defined($options{h})) {
      $asa = $options{h};
  }
  else {
      print "Enter ASA host name or IP address:";
      chop($asa=<>);
  }
```

```
  if (defined ($options{u})) {
      $user= $options{u};
  }
  else {
      print "Enter user name:";
      chop($user=<>);
  }

  if (defined ($options{w})) {
      $password= $options{w};
  }
  else {
      print "Enter password:";
      chop($password=<>);
  }
  if (defined ($options{p})) {
      $prompt= $options{p};
  }
  else {
      print "Enter ASA prompt:";
      chop($prompt=<>);
  }
  if (defined ($options{e})) {
      $enable = $options{e};
  }
  else {
      print "Enter enable password:";
      chop($enable=<>);
  }

  if (defined ($options{r})) {
     $restore = 1;
     $restore_file = $options{r};
  }
}
```

将您的软件降级

当您升级至 8.3 版本时，您的配置会被迁移。旧的配置会自动存储在闪存中。例如，当您从 8.2(1) 版本升级至 8.3(1) 版本时，旧的 8.2(1) 配置会被将存储在闪存中名为 8_2_1_0_startup_cfg.sav 的文件中。

注　在降级前，您必须手动还原旧的配置。

本部分介绍如何执行降级。

- 第 36-32 页的激活密钥兼容性的相关信息
- 第 36-32 页的执行降级

激活密钥兼容性的相关信息

如果您从任何之前的版本升级至最新版本，您的激活密钥会保持兼容。但是，如果您想要保持降级能力，则可能会遇到问题。

- 降级到 8.1 版本或更早的版本 - 在升级之后，如果您激活了在 *8.2 之前*引入的附加功能许可证，激活密钥在您降级时，会继续与更早的版本兼容。但是，如果您激活在 8.2 版本或更高的版本中引入的功能许可证，激活密钥不会向后兼容。如果您有不兼容的许可证密钥，请参阅以下准则：
  - 如果您之前在早期版本中输入了激活密钥，ASA 会使用该密钥（不包括在 8.2 版本或更高的版本中激活的任意新许可证）。
  - 如果您有新的系统，并且没有早期的激活密钥，您需要请求与早期版本兼容的新激活密钥。
- 降级至 8.2 版本或更早的版本 - 8.3 版本引入了更可靠的基于时间的密钥用法以及故障转移许可证更改：
  - 如果您有多个基于时间的激活密钥处于活动状态，当您降级时，只有最新的基于时间的密钥可以处于活动状态。所有其他密钥将进入非活动状态。
  - 如果您在故障转移对上具有不匹配的许可证，降级将会禁用故障转移。即使密钥匹配，使用的许可证也不再是组合许可证。

执行降级

如要从 8.3 版本降级，请执行以下步骤：

详细步骤

步骤 1　输入以下命令：

```
ciscoasa(config)# downgrade [/noconfirm] old_image_url old_config_url [activation-key old_key]
```

其中的 **/noconfirm** 选项表示，会在不进行提示的情况下执行降级。 *image_url* 是旧映像在 disk0、disk1、 tftp、 ftp 或 smb 上的路径。 *old_config_url* 保存的预迁移配置的路径 （默认情况下，此配置保存在 disk0 上）。如果您需要还原至 8.3 之前的激活密钥，您可以输入旧的激活密钥。

此命令是完成以下功能的快捷方式：

1. 清除启动映像配置 (**clear configure boot**)。
2. 将启动映像设置为旧映像 (**boot system**)。
3. （可选）输入新的激活密钥 (**activation-key**)。
4. 将运行配置保存至启动 (**write memory**)。此操作会将 BOOT 环境变量设置为旧映像，因此，当您重新加载时，将会加载旧映像。
5. 将旧配置复制至启动配置 (**copy** *old_config_url* **startup-config**)。
6. 重新加载 (**reload**)。

例如：

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

配置自动更新

- 第 36-33 页的有关自动更新的信息
- 第 36-36 页的准则和限制
- 第 36-36 页的配置与自动更新服务器的通信
- 第 36-37 页的将客户端更新配置为自动更新服务器
- 第 36-38 页的查看自动更新状态

有关自动更新的信息

自动更新是一种协议规范，它允许自动更新服务器将配置和软件映像下载至许多 ASA，并可提供从中央位置对 ASA 的基本监控。

- 第 36-33 页的自动更新客户端或服务器
- 第 36-33 页的自动更新的优势
- 第 36-33 页的故障转移配置中的自动更新服务器支持

自动更新客户端或服务器

ASA 可以被配置为客户端或服务器。作为自动更新客户端，它会定期轮询自动更新服务器，以便获取软件映像和配置文件的更新。作为自动更新服务器，它会向配置为自动更新客户端的 ASA 发送更新。

自动更新的优势

在解决管理 ASA 的管理员所面临的许多问题方面，自动更新十分有用，例如：

- 解决动态寻址和 NAT 挑战。
- 执行一次操作即可提交配置更改。
- 提供更新软件的可靠方法。
- 利用易于理解的方法来实现高可用性 （故障转移）。
- 通过开放接口提供灵活性。
- 简化了用于服务提供商环境的安全解决方案。

自动更新规范提供了远程管理应用所需的基础设施，以便下载 ASA 配置、软件映像和从一个中心位置或多个位置执行基本监控。

自动更新规范允许自动更新服务器向 ASA 推送配置信息或向其发送信息请求，或者通过让 ASA 定期轮询自动更新服务器来拉取配置信息。自动更新服务器也可以向 ASA 发送命令，以便随时发出即时的轮询请求。自动更新服务器与 ASA 之间的通信需要每个 ASA 上的通信路径和本地 CLI 配置。

故障转移配置中的自动更新服务器支持

您可以使用自动更新服务器，将软件映像和配置文件部署至主用/备用故障转移配置下的 ASA。要在主用/备用故障转移配置上启用自动更新，请在故障转移对中的主设备上输入自动更新服务器配置。

以下限制和行为适用于故障转移配置下的自动更新服务器支持：

- 仅支持单模式、主用/备用配置。
- 加载新的平台软件映像时，故障转移对会停止传输流量。
- 使用基于局域网的故障转移时，新的配置不得更改故障转移链路配置。如果新的配置更改了故障转移链路配置，设备之间的通信将会失败。
- 仅主设备将会自动通报自动更新服务器。主设备必须处于主用状态才能进行自动通报。如果主设备不处于主用状态，ASA 会自动故障转移至主设备。
- 仅主设备会下载软件映像或配置文件。软件映像或配置随后会被复制至辅助设备。
- 接口 MAC 地址和硬件串行 ID 均来自主设备。
- 存储在自动更新服务器或 HTTP 服务器上的配置文件仅用于主设备。

自动更新过程概述

以下是故障转移配置下的自动更新过程的概述。此过程假设故障转移已启用且正常运行。如果设备正在同步配置，备用设备由于 SSM 卡故障以外的原因处于故障状态，或者故障转移链路发生故障，则无法进行自动更新。

1. 两台设备会交换平台和 ASDM 软件校验和以及版本信息。
2. 主设备会联系自动更新服务器。如果主设备不处于主用状态，ASA 会先故障转移至主设备，然后与自动更新服务器联系。
3. 自动更新服务器会使用软件校验和与 URL 信息进行回复。
4. 如果主设备确定主用设备或备用设备的平台映像文件需要更新，将会进行以下操作：
   a. 主设备使用来自自动更新服务器的 URL，从 HTTP 服务器检索适当的文件。
   b. 主设备将映像复制至备用设备，然后更新自身的映像。
   c. 如果两台设备都有新映像，则辅助 （备用）设备会先重新加载。
   – 如果在辅助设备启动时可以执行无中断升级，则辅助设备成为主用设备，并且主设备将重新加载。主设备在完成加载后将成为主用单元。
   – 如果在备用设备启动时无法执行无中断升级，则两台设备会同时重新加载。
   d. 如果仅辅助 （备用）设备有新映像，则只有辅助设备会重新加载。主设备会进行等待，直到辅助设备完成重新加载。
   e. 如果仅主 （主用）设备有新映像，则辅助设备会成为主用设备，并且主设备将重新加载。
   f. 更新过程会再次从步骤 1 开始。
5. 如果 ASA 确定主设备或辅助设备的 ASDM 文件需要更新，将会进行以下操作：
   a. 主设备使用自动更新服务器提供的 URL，从 HTTP 服务器检索 ASDM 映像文件。
   b. 主设备将会视需要，将 ASDM 映像复制至备用设备。
   c. 主设备会更新自身的 ASDM 映像。
   d. 更新过程会再次从步骤 1 开始。
6. 如果主设备确定需要更新配置，将会进行以下操作：
   a. 主设备会从指定 URL 检索配置文件。
   b. 新配置会同时替换两台设备上的旧配置。
   c. 更新过程会再次从步骤 1 开始。
7. 如果所有映像和配置文件的校验和匹配，则无需更新。更新过程结束，直到下一次轮询时间。

监控自动更新过程

您可以使用 **debug auto-update client** 或 **debug fover cmd-exe** 命令，以便显示在自动更新过程中执行的操作。以下内容是 **debug auto-update client** 命令的示例输出。

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
   Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum:
0x94bced0261cc992ae710faf8d244cf32
   Component: config, URL: http://192.168.0.21/config-rms.xml, checksum:
0x67358553572688a805a155af312f6898
   Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum:
0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name
ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msecs
Auto-update client: update img on active unit...
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
auto-update: HA safe reload: reload active waiting with mate state: 50

auto-update: HA safe reload: reload active waiting with mate state: 80
        Sauto-update: HA safe reload: reload active unit at clock tick: 6266860
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419
```

如果自动更新过程失败，将会生成以下系统日志消息：

```
%ASA4-612002: Auto Update failed: file version: version reason: reason
```

file 是“image”、“asdm”或“configuration”，具体取决于哪一更新失败。 *version* 是更新的版本号。 *reason* 是更新失败的原因。

准则和限制

- 如果 HTTPS 被选为用于与自动更新服务器进行通信的协议，ASA 将会使用 SSL，这要求 ASA 具有 DES 或 3DES 许可证。
- 自动更新仅在单情景模式中受支持。

配置与自动更新服务器的通信

详细步骤

如要将 ASA 配置为自动更新客户端，请执行以下步骤：

步骤 1　如要指定自动更新服务器的 URL，请输入以下命令：

```
ciscoasa(config)# auto-update server url [source interface] [verify-certificate |
no-verification]
```

其中的 *url* 有以下语法：

```
http[s]://[user:password@]server_ip[:port]/pathname
```

source *interface* 关键字和参数用于指定，向自动更新服务器发送请求时使用的接口。如果您指定了通过 **management-access** 命令指定的相同接口，则自动更新请求会通过用于管理访问的相同 IPsec VPN 隧道。

对于 HTTPS，**verify-certificate** 关键字（默认）会验证自动更新服务器返回的证书。要禁用验证（不推荐），请指定 **no-verification** 关键字。

步骤 2　（可选）如要确定与自动更新服务器通信时发送的设备 ID，请输入以下命令：

```
ciscoasa(config)# auto-update device-id {hardware-serial | hostname | ipaddress [if-name]
| mac-address [if-name] | string text}
```

使用的标识符通过指定以下任一参数确定：

- *hardware-serial* 参数指定 ASA 序列号。
- *hostname* 参数用于指定 ASA 主机名。
- **ipaddress** 关键字用于指定，指定接口的 IP 地址。如果未指定接口名称，它将使用用于与自动更新服务器通信的接口的 IP 地址。
- **mac-address** 关键字用于指定，指定接口的 MAC 地址。如果未指定接口名称，它将使用用于与自动更新服务器通信的接口的 MAC 地址。
- **string** 关键字用于指定，不能含有空格或字符‘、“、>、 & 和 ? 的指定文本标识符。

步骤 3　（可选）要指定轮询自动更新服务器，以获取配置或映像更新的频率，请输入以下命令：

```
ciscoasa(config)# auto-update poll-period poll-period [retry-count [retry-period]]
```

poll-period 参数用于指定检查更新的频率 （以分钟为单位）。默认值为 720 分钟 （12 小时）。

retry-count 参数用于指定尝试重新连接至服务器的次数 （如果第一次尝试失败）。默认值为零。

retry-period 参数用于指定重试之间的等待时间 （以分钟为单位）。默认值为五分钟。

步骤 4　（可选）要计划 ASA 在特定时间轮询自动更新服务器，请输入以下命令：

```
ciscoasa(config)# auto-update poll-at days-of-the-week time [randomize minutes]
[retry_count [retry_period]]
```

days-of-the-week 参数是一个星期中的任一天或几天的组合：星期一、星期二、星期三、星期四、星期五、星期六和星期天。其他可能的值为每天 （星期一到星期天）、工作日 （星期一到星期五）和周末 （星期六和星期天）。

time 参数用于以 HH:MM 格式指定开始轮询的时间。例如，8.00 是上午 8:00，而 20:00 是下午 8:00

randomize *minutes* 关键字和参数用于指定，在指定开始时间之后随机选择轮询时间的时间段。时间范围为 1 至 1439 分钟。

retry_count 参数用于，指定尝试重新连接至自动更新服务器的次数 （如果第一次尝试失败）。默认值为零。

retry_period 参数用于指定连接尝试之间的等待时长。默认值为五分钟。时间范围为 1 至 35791 分钟。

步骤 5　（可选）如果自动更新服务器已有一段时间未联系，请输入以下命令使其停止传输流量：

```
ciscoasa(config)# auto-update timeout period
```

period 参数用于指定，以分钟为单位的介于 1 至 35791 的超时时间段。默认值为永不超时 （0 分钟）。要还原默认设置，请输入此命令的 **no** 形式。

使用 **auto-update timeout** 命令确保 ASA 拥有最新的映像和配置。此情况由系统日志消息 201008 报告。

在以下示例中，ASA 被配置为，于端口号 1742，使用证书验证，通过外部接口轮询 IP 地址为 209.165.200.224 的自动更新服务器。

ASA 还被配置为使用主机名作为设备 ID，并在每个星期五和星期六晚上 10:00 至 11:00 之间的一个随机时间 轮询自动更新服务器。在轮询尝试失败后，ASA 会尝试重新连接至自动更新服务器十次，并将在每次重新连接尝试之间等待三分钟，如以下示例中所示：

```
ciscoasa(config)# auto-update server
https://jcrichton:farscape@209.165.200.224:1742/management source outside verify-certificate
ciscoasa (config)# auto-update device-id hostname
hostname (config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
```

将客户端更新配置为自动更新服务器

输入 **client-update** 命令可以启用配置为自动更新客户端的 ASA 的更新，并且允许您指定软件组件的类型（ASDM 或启动映像）、ASA 的类型或系列、更新应用至的修订版本号以及从中获得更新的 URL 或 IP 地址。

如要将 ASA 配置为自动更新服务器，请执行以下步骤：

步骤 1　如要启用客户端更新，请输入以下命令：

```
ciscoasa(config)# client-update enable
```

步骤 2　为您想要应用于 ASA 的 **client-update** 命令，配置以下参数：

client-update {**component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

component {**asdm** | **image**} 参数用于指定软件组件，即 ASA 的 ASDM 或启动映像。

device-id *dev_string* 参数用于指定，自动更新客户端用来标识自身的唯一字符串。最大长度为 63 个字符。

family *family_name* 参数用于指定，自动更新客户端用来标识自身的系列名称。它可以是 asa、pix 或最大长度为七个字符的文本字符串。

rev-nums *rev-nums* 参数用于指定，此客户端的软件或固件映像。可以按任意顺序输入最多四个用逗号分隔的软件或固件映像。

type *type* 参数用于指定，要向其通知客户端更新的客户端的类型。由于此命令也可用于更新 Windows 客户端，客户端列表可以包括多个 Windows 操作系统。

url *url-string* 参数用于指定软件/固件映像的 URL。此 URL 必须指向适合此客户端的文件。对于所有自动更新客户端，您必须使用协议“http://”或“https://”作为 URL 前缀。

为您想要应用于所有特定类型的 ASA 的客户端更新配置参数。即指定 ASA 的类型，以及从中获取经过更新的映像的 URL 或 IP 地址。此外，您必须指定修订版本号。如果远程 ASA 的修订版本号与某个指定的修订版本号匹配，则不需要更新客户端，并且更新将会被忽略。

如要配置思科 5525-X ASA 的客户端更新，请输入以下命令：

```
ciscoasa(config)# client-update type asa5525 component asdm url
http://192.168.1.114/aus/asdm601.bin rev-nums 8.0(1)
```

查看自动更新状态

如要查看自动更新状态，请输入以下命令：

```
ciscoasa(config)# show auto-update
```

以下内容是 **show auto-update** 命令的示例输出：

```
ciscoasa(config)# show auto-update

Server: https://********@209.165.200.224:1742/management.cgi?1276
Certificate will be verified
Poll period: 720 minutes, retry count: 2, retry period: 5 minutes
Timeout: none
Device ID: host name [corporate]
Next poll in 4.93 minutes
Last poll: 11:36:46 PST Tue Nov 13 2004
Last PDM update: 23:36:46 PST Tue Nov 12 2004
```

软件和配置的功能历史记录

表 36-2 列出了各种功能变更以及实施该等功能变更的平台版本。。

表 36-2　　软件和配置的功能历史记录

功能名称	平台版本	功能信息
安全复制客户端	9.1(5)/9.2(1)	ASA 现在支持安全复制 (SCP) 客户端，以便将文件传输至 SCP 服务器，或从中传出文件。 我们引入了以下命令：**ssh pubkey-chain**、 **server (ssh pubkey-chain)**、 **key-string**、 **key-hash** 和 **ssh stricthostkeycheck**。 我们修改了以下命令：**copy scp**。
默认启用的自动更新服务器证书验证	9.2(1)	现在，自动更新服务器证书验证会默认启用；对于新的配置，您必须显式禁用证书验证。如果您从早期版本升级，而且您没有启用证书验证，则证书验证不会被启用，并且，您会看到以下警告： `WARNING: The certificate provided by the auto-update servers will not be verified.In order to verify this certificate please use the verify-certificate option.` 配置将会被迁移为显式配置的无验证： **auto-update server no-verification** 我们修改了以下命令：**auto-update server** {**verify-certificate** | **no-verification**}。

第 37 章

系统事件的响应自动化

本章介绍如何配置嵌入式事件管理器 (EEM)。

- 第 37-1 页的关于 EEM
- 第 37-2 页的 EEM 准则
- 第 37-3 页的配置 EEM
- 第 37-6 页的 EEM 示例
- 第 37-7 页的监控 EEM
- 第 37-7 页的 EEM 的历史记录

关于 EEM

EEM 服务使您可以调试问题并提供用于故障排除的通用日志记录。这项服务由两个部分组成：EEM 响应或侦听的事件，以及定义操作和 EEM 所响应事件的事件管理器小程序。可以配置多个事件管理器小程序来响应不同的事件和执行不同的操作。

受支持的事件

EEM 支持以下事件：

- 系统日志 - ASA 使用系统日志消息 ID 来识别触发事件管理器小程序的系统日志消息。您可以配置多个系统日志事件，但系统日志消息 ID 可能不会在一个事件管理器小程序内重叠。
- 计时器 - 可以使用计时器触发事件。对于每个事件管理器小程序，每个计时器只能配置一次。每个事件管理器小程序最多可以有三个计时器。计时器的三种类型如下：
  - 看门狗 （定期）计时器在小程序操作完成后的指定时间段后触发事件管理器小程序，并会自动重新启动。
  - 倒数 （一次性）计时器在指定时间段后立即触发事件管理器小程序，且通常不会重新启动，除非移除并重新添加它们。
  - 绝对 （一天一次）计时器促使事件在每天的指定时间发生一次，并会自动重新启动。时间格式为 hh:mm:ss。

  对于上述类型的每个事件管理器小程序，只能配置一个计时器事件。
- 无 - 当您使用 CLI 或 ASDM 手动运行事件管理器小程序时，会触发 None 事件。
- 崩溃 - 如果 ASA 崩溃，会触发崩溃事件。无论 **output** 命令的值是什么，**action** 命令都会指向 crashinfo 文件。输出在 **show tech** 命令之前生成。

事件管理器小程序上的操作

当事件管理器小程序被触发时，会执行事件管理器小程序上的操作。每个操作都具有用于指定操作序列的编号。该序列号在事件管理器小程序中必须是唯一的。可以为一个事件管理器小程序配置多个操作。命令是典型的 CLI 命令，例如 **show blocks**。

输出目标

可以使用 **output** 命令将操作输出发送到指定的位置。一次只能启用一个输出值。默认值为 **output none**。此值丢弃 **action** 命令的任何输出。此命令在全局配置模式中作为权限级别为 15（最高）的用户运行。此命令可能不接受任何输入，因为它处于禁用状态。您可以将 **action** CLI 命令的输出发送到以下三个位置之一：

- **None** - 这是默认位置，会丢弃输出
- **Console** - 此位置将输出发送到 ASA 控制台
- **File** - 此位置将输出发送到文件。以下四个文件选项可用：
  - **Create a unique file** - 每次调用事件管理器小程序时，此选项会创建具有唯一名称的新文件
  - **Create/overwrite a file** - 每次调用事件管理器小程序时，此选项会覆盖指定的文件。
  - **Create/append to a file** - 每次调用事件管理器小程序时，此选项会附加到指定的文件。如果指定的文件不存在，则会创建文件。
  - **Create a set of files** - 此选项会创建一组具有唯一名称的文件，每次调用事件管理器小程序时，都会轮换这些文件。

EEM 准则

情景模式准则

多情景模式不支持 EEM。

其他指导原则

- 在发生崩溃期间，ASA 的状态一般是未知的。在这种情况下运行某些命令可能不安全。
- 事件管理器小程序的名称不能包含空格。
- 不能修改 None 事件和 Crashinfo 事件参数。
- 因为系统日志消息会发送到 EEM 中进行处理，因此可能会影响性能。
- 每个事件管理器小程序的默认输出均为 **output none**。如要更改此设置，必须输入其他输出值。
- 只能为每个事件管理器小程序定义一个输出选项。

配置 EEM

EEM 的配置由以下任务组成：

步骤 1　创建事件管理器小程序，然后配置各种事件。请参阅第 37-3 页的创建事件管理器小程序并配置事件。

步骤 2　在事件管理器小程序上配置操作，然后配置操作输出的目标。请参阅第 37-4 页的配置操作和操作输出的目标。

步骤 3　运行事件管理器小程序。请参阅第 37-6 页的运行事件管理器小程序。

创建事件管理器小程序并配置事件

如要创建事件管理器小程序并配置事件，请执行以下步骤：

操作步骤

步骤 1　创建事件管理器小程序并进入事件管理器小程序配置模式。

event manager applet *name*

示例：

```
ciscoasa(config)# event manager applet exampleapplet1
```

name 参数最多可包含 32 个字母数字字符。不允许使用空格。

如要移除事件管理器小程序，请输入此命令的 **no** 形式。

步骤 2　描述事件管理器小程序。

description *text*

示例：

```
ciscoasa(config-applet)# description applet1example
```

text 参数最多可包含 256 个字符。如果用引号将描述文本引起来，描述文本可包含空格。

步骤 3　如要配置指定的事件，请输入以下命令之一。要移除已配置的事件，请输入相应命令的 **no** 形式。

- 要配置系统日志事件，请识别一条或一系列触发事件管理器小程序的系统日志消息。

  event syslog id *nnnnnn*[*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

  示例：

  ```
  ciscoasa(config-applet)# event syslog id 106201
  ```

  nnnnnn 参数识别系统日志消息 ID。 **occurs** *n* 关键字-参数对指明系统日志消息必须出现多少次才会调用事件管理器小程序。默认情况为每 0 秒出现 1 次。有效值为 1 到 4294967295。 **period** *seconds* 关键字-参数对指明必须发生事件的时间段 （以秒为单位），并将事件管理器小程序在配置的时间段内出现的最高频率限制为一次。有效值为 0 到 604800。 0 表示未定义时间段。

- 如要将事件配置为在每个配置的时间段内发生一次并自动重新启动，请输入以下命令。

  event timer watchdog time *seconds*

示例：

```
ciscoasa(config-applet)# event timer watchdog time 30
```

时间范围可以是 1 到 604800 秒。

- 如要将事件配置为发生一次且不会重新启动 （除非移除然后重新添加事件），请输入以下命令。

  event timer countdown time *seconds*

  示例：

  ```
  ciscoasa(config-applet)# event timer countdown time 60
  ```

  时间范围可以是 1 到 604800 秒。使用此命令的 **no** 形式可移除倒数计时器事件。

注　如果这是启动配置，当您重新启动时此计时器将会重新运行。

- 如要将事件配置为在指定时间一天发生一次并自动重新启动，请输入以下命令。

  event timer absolute time *hh:mm:ss*

  示例：

  ```
  ciscoasa(config-applet)# event timer absolute time 10:30:20
  ```

  时间格式为 hh:mm:ss。时间范围为 00:00:00（午夜）到 23:59:59。

- 在 ASA 崩溃时触发崩溃事件。

  event crashinfo

  示例：

  ```
  ciscoasa(config-applet)# event crashinfo
  ```

  无论 **output** 命令的值是什么，**action** 命令都会指向 crashinfo 文件。输出在 **show tech** 命令之前生成。

配置操作和操作输出的目标

如要配置操作和操作输出的特定发送目标，请执行以下步骤：

操作步骤

步骤 1　在事件管理器小程序上配置操作。

action *n* **cli command** "*command*"

示例：

```
ciscoasa(config-applet)# action 1 cli command "show version"
```

n 选项是操作 ID。有效 ID 范围是 0 到 4294967295。 *command* 选项的值必须用引号引起来；否则，如果命令包含多于一个词，将会发生错误。此命令在全局配置模式中作为权限级别为 15 （最高）的用户运行。此命令可能不接受任何输入，因为它处于禁用状态。可使用此命令的 **noconfirm** 选项（如果可用）。

步骤 2　选择一个可用的输出目标选项。使用相应命令的 **no** 形式可移除输出目标。

- **None** 选项丢弃 **action** 命令的任何输出 （这是默认设置）：

  output none

  示例：

  ```
  ciscoasa(config-applet)# output none
  ```

- **Console** 选项将 **action** 命令的输出发送到控制台。

  output console

  示例：

  ```
  ciscoasa(config-applet)# output console
  ```

  注　运行此命令会影响性能。

- **New File** 选项为调用的每个事件管理器小程序将 **action** 命令的输出发送到新文件。

  output file new

  示例：

  ```
  ciscoasa(config-applet)# output file new
  ```

  文件名的格式为 eem-*applet-timestamp*.log，其中，*applet* 是事件管理器小程序的名称，*timestamp* 是注有日期的时间戳，其格式为 YYYYMMDD-hhmmss。

- **New Set of Rotated Files** 选项创建一组会轮换的文件。当要写入新文件时，最 旧的文件会被删除，且所有的后续文件都会在写入第一个文件之前进行重新编号。

  output file rotate *n*

  示例：

  ```
  ciscoasa(config-applet)# output file rotate 50
  ```

  最新的文件以 0 表示，最 旧的文件以最高编号 (*n*-1) 表示。*n* 选项是轮换值。有效值范围为 2 到 100。文件名格式为 eem-*applet-x*.log，其中，*applet* 是小程序的名称，*x* 是文件编号。

- **Single Overwritten File** 选项将 **action** 命令输出写入到一个文件中，每次写入都会覆盖原有文件。

  output file overwrite *filename*

  示例：

  ```
  ciscoasa(config-applet)# output file overwrite examplefile1
  ```

  filename 参数是本地 （至 ASA）文件名。此命令也可以使用 FTP、 TFTP 和 SMB 目标文件。

- **Single Appended File** 选项将 **action** 命令输出写入到一个文件中，每次写入时都会附加到原有文件。

  output file append *filename*

  示例：

  ```
  ciscoasa(config-applet)# output file append examplefile1
  ```

  filename 参数是本地 （至 ASA）文件名。

运行事件管理器小程序

如要运行事件管理器小程序，请执行以下步骤：

操作步骤

步骤 1　运行事件管理器小程序。

event manager run *applet*

示例：

```
ciscoasa# event manager run exampleapplet1
```

如果运行尚未配置 **event none** 命令的事件管理器小程序，将会发生错误。 *applet* 参数是事件管理器小程序的名称。

EEM 示例

以下示例显示这样的事件管理器小程序：每小时记录一次有关阻止泄露情况信息，并将输出写入到一组会轮换的日志文件中，从而保存一天的日志：

```
ciscoasa(config)# event manager applet blockcheck
ciscoasa(config-applet)# description "Log block usage"
ciscoasa(config-applet)# event timer watchdog time 3600
ciscoasa(config-applet)# output rotate 24
ciscoasa(config-applet)# action 1 cli command "show blocks old"
```

以下示例显示这样的事件管理器小程序：在每天凌晨 1 点重新启动 ASA，并根据需要保存配置：

```
ciscoasa(config)# event manager applet dailyreboot
ciscoasa(config-applet)# description "Reboot every night"
ciscoasa(config-applet)# event timer absolute time 1:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "reload save-config noconfirm"
```

以下示例显示在午夜与凌晨 3 点之间禁用给定接口的事件管理器小程序。

```
ciscoasa(config)# event manager applet disableintf
ciscoasa(config-applet)# description "Disable the interface at midnight"
ciscoasa(config-applet)# event timer absolute time 0:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"

ciscoasa(config)# event manager applet enableintf
ciscoasa(config-applet)# description "Enable the interface at 3am"
ciscoasa(config-applet)# event timer absolute time 3:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "no shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"
```

监控 EEM

可使用以下命令监控 EEM。

- **clear configure event manager**

  此命令移除事件管理器的运行配置。

- **clear configure event manager applet** *appletname*

  此命令从配置中移除已命名的事件管理器小程序。

- **show counters protocol eem**

  此命令显示事件管理器的计数器。

- **show event manager**

  此命令显示有关已配置的事件管理器小程序的信息，包括命中次数和上一次调用事件管理器小程序的时间。

- **show running-config event manager**

  此命令显示事件管理器的运行配置。

EEM 的历史记录

表 37-1　　EEM 的历史记录

功能名称	平台版本	说明
嵌入式事件管理器 (EEM)	9.2(1)	EEM 服务使您可以调试问题并提供用于故障排除的通用日志记录。这项服务由两个部分组成：EEM 响应或侦听的事件，以及定义操作和 EEM 所响应事件的事件管理器小程序。可以配置多个事件管理器小程序来响应不同的事件和执行不同的操作。 引入或修改了以下命令：**event manager applet**、**description**、**event syslog id**、**event none**、**event timer** {**watchdog time** *seconds* | **countdown time** *seconds* | **absolute time** *hh:mm:ss*}、**event crashinfo**、**action cli command**、**output** {**none** | **console** | **file** {**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*}}、**show running-config event manager**、**event manager run**、**show event manager**、**show counters protocol eem**、**clear configure event manager**、**debug event manager**、**debug menu eem**。

故障排除

本章介绍了如何对思科 ASA 进行故障排除。

- 第 38-1 页的查看调试消息
- 第 38-1 页的捕获数据包
- 第 38-4 页的查看崩溃转储
- 第 38-4 页的查看核心转储
- 第 38-5 页的 ASAv 中的 vCPU 使用率

查看调试消息

调试输出在 CPU 处理中享有高优先级，因此可导致系统不可用。为此，只能在出现特定问题或在思科 TAC 的故障排除会话过程中使用 **debug** 命令进行故障排除。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。要启用调试消息，请参阅命令参考中的 **debug** 命令。

捕获数据包

捕获数据包可能在对连接问题进行故障排除或监控可疑活动时非常有用。如果要使用数据包捕获服务，我们建议您联系思科 TAC。

如要捕获数据包，请执行以下步骤：

操作步骤

步骤 1 启用数据包捕获功能以进行数据包探查和网络故障隔离。

[cluster exec] **capture** *capture_name* [**type** {**asp-drop all** [*drop-code*] | **tls-proxy** | **raw-data** | **lacp** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] [**interface asa_dataplane**] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**reinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** *trace_count*] [**real-time**] [**trace**] [**match prot** {**host** *source-ip* | *source-ip mask* |**any**}{**host** *destination-ip* |*destination-ip mask* | **any**} [*operator* **port**]

示例：

```
ciscoasa# capture captest interface inside
```

有关完整的语法说明，请参阅命令参考或 CLI 帮助 (**help capture**)。并非所有选项均可通过一个命令指定。请参阅 CLI 帮助以了解允许的组合。

在多个 **capture** 语句中使用同一个 *capture_name* 以捕获多种类型的流量。

type asp-drop 关键字可捕获加速安全路径丢弃的数据包。在集群中，还将捕获从一台设备转发到另一台设备时丢失的转发数据包。在多情景模式中，在系统情景中发出此命令时，将捕获所有丢弃的数据包；在用户情景中发出此命令时，将只捕获从属于用户情景的接口中输入的丢弃数据包。

inline-tag *tag* 关键字参数对为特定 SGT 值指定标记，或保留不指定以捕获带任何 SGT 值的标记数据包。

buffer 关键字定义了用于存储数据包的缓冲区大小。字节缓冲区已满时，数据包捕获停止。用于集群中时，这是指每台设备的大小，而不是所有设备的总和。 **circular-buffer** 关键字**可**在缓冲区已满时从头开始覆盖缓冲区。

interface 关键字**可**设置要在其上使用数据包捕获的接口的名称。您必须为任何要捕获的数据包配置接口。

如要在数据层面捕获数据包，请使用 **asa_dataplane** 关键字。要过滤在 ASA CX 背板上捕获的数据包，请使用 **asa_dataplane** 选项并遵守以下准则。在单模式中，背板控制数据包会绕过访问列表，然后被捕获。在多情景模式中，系统情景中仅可捕获控制数据包。用户情景中可捕获数据包。 **access-list** 和 **match** 选项仅在用户情景中可用。

如要在集群控制链路上捕获流量，请使用 **cluster** 关键字。如果配置 **type lacp**，请指定物理接口 ID，而非 nameif 名称。

match 关键字通过匹配协议、源和目标 IP 地址与可选端口进行捕获。此关键字最多可在一个命令中使用三次。*操作符*可以是以下任意一项：

- **lt -** 小于
- **gt -** 大于
- **eq -** 等于

type raw-data 关键字**可**捕获入站和出站数据包。该设置为默认设置。

real-time 关键字可显示连续、实时捕获的数据包。要终止实时数据包捕获，请输入 **Ctrl + c**。要永久移除捕获，请使用此命令的 **no** 形式。此选项仅适用于 **raw-data** 和 **asp-drop** 捕获。使用 **cluster exec capture** 命令时不支持此选项。

reinject-hide 关键字可指定不捕获任何重新注入的数据包，此关键字仅适用于集群分析环境。

注　如果已配置 ACL 优化，则您无法在捕获中使用 **access-list** 命令。您仅可以使用 **access-group** 命令。如果您在此情况下尝试使用 **access-list** 命令，系统将显示错误。

在集群环境中捕获数据包

如要支持集群范围的故障排除，可以使用 **cluster exec capture** 命令在主设备上启用捕获集群特定流量的功能，随后集群中的所有从设备上将自动启用此功能。 **cluster exec** 关键字是放在 **capture** 命令前面的新关键字，可启用集群范围的捕获。

“cluster”接口名称是集群控制链路的默认名称，是不可配置的。您可将“cluster”指定为接口名称以捕获集群控制链路接口上的流量。集群控制链路上有两种类型的数据包：控制层面数据包和数据层面数据包，它们都包含转发的数据流量和集群 LU 消息。IP 地址报头中的 TTL 字段经过编码以区分这两种类型的数据包。捕获转发的数据包时，其集群尾部包含在捕获文件中以用于调试。

在多情景模式中，虽然集群接口属于系统情景，但您可以看到接口，因此您可以在用户情景中于集群链路上配置捕获。在系统情景中，控制层面和数据层面数据包均可用。数据层面可捕获 LU 数据包和仅属于系统情景的转发数据包。在用户情景中，控制层面数据包不可见。此情景中只可捕获属于指定用户情景的转发数据包和 LU 数据包。出于安全考虑，每个情景只能看到所属的数据包。

捕获数据包准则

- 如果 ASA 接收到未正确格式化 TCP 报头的数据包并由于 *invalid-tcp-hdr-length* ASP 丢弃而将其丢弃，则接收到这些数据包的接口上的 **show capture** 命令输出不显示这些数据包。
- 您只能捕获 IP 流量；您无法捕获 ARP 等非 IP 数据包。
- 对于多情景模式中的集群控制链路捕获，将只捕获与集群控制链路中发送的情景相关联的数据包。
- 对于内联 SGT 标记数据包，捕获的数据包包含您的 PCAP 查看器可能无法识别的其他 CMD 报头。
- 在多情景模式中，**copy capture** 命令仅在系统空间中可用。语法如下所示：

  copy /pcap capture:*Context-name*/*in-cap* **tftp**:

  其中 *in-cap* 是在 *context-name* 情景中配置的捕获
- 不支持 **cluster exec capture realtime** 命令。系统将显示以下错误消息：

  ```
  Error: Real-time capture can not be run in cluster exec mode.
  ```

- 对于共享 VLAN，适用以下准则：
  - 您只能为 VLAN 配置一个捕获；如果您在共享 VLAN 上于多情景中配置一个捕获，则将只使用配置的最后一个捕获。
  - 如果移除最后配置的 （活动）捕获，则没有捕获会变成活动状态，即使您之前已在其他情景中配置捕获；您必须移除捕获并重新添加才能让它变成活动状态。
  - 流入该捕获所关联的接口的所有流量都将被捕获，包括流向共享 VLAN 上的其他情景的流量。
  - 因此，如果您在情景 A 中为同时被情景 B 使用的 VLAN 启用捕获，则将同时捕获情景 A 和情景 B 的入口流量。
- 对于出口流量，将只捕获带活动捕获的情景的流量。唯一的异常情况是您不启用 ICMP 检查（因此 ICMP 流量在加速路径中没有会话）。在这种情况下，将捕获共享 VLAN 上所有情景的入口和出口 ICMP 流量。
- 配置捕获通常包括配置匹配需要捕获的流量的 ACL。在配置匹配流量模式的 ACL 之后，您需要定义捕获并将此 ACL 与该捕获以及需要在其上配置捕获的接口相关联。
- 在执行一个集群范围的捕获之后，如要将此集群范围的捕获文件复制到 TFTP 服务器，请在主设备上输入以下命令：

  ```
  ciscoasa (cfg-cluster)# cluster exec copy /pcap capture: cap_name
  tftp://location/path/filename.pcap
  ```

- 分别来自每台设备（各一个）的多个 PCAP 文件被复制到 TFTP 服务器。目标捕获文件名将自动附加设备名称，如 filename_A.pcap、filename_B.pcap 等。在本示例中，A 和 B 为集群设备名称。如果在文件名末尾添加设备名称，将生成不同的目标名称。
- 如要在指定接口上启用集群范围的捕获，您可以在示例中所示的每个命令的前面添加 **cluster exec** 关键字。这些 **capture** 命令仅可从主设备复制到从设备。但是，您仍可以在指定接口上使用任意这些 **capture** 命令为本地设备配置捕获。

示例

以下示例显示了如何创建集群范围的 LACP 捕获：

```
ciscoasa (config)# cluster exec capture lacp type lacp interface gigabitEthernet0/0
```

以下示例显示了如何在集群链路上为控制路径数据包创建捕获：

```
ciscoasa (config)# capture cp interface cluster match udp any eq 49495 any
ciscoasa (config)# capture cp interface cluster match udp any any eq 49495
```

以下示例显示了如何在集群链路上为数据路径数据包创建捕获：

```
ciscoasa (config)# access-list cc1 extended permit udp any any eq 4193
ciscoasa (config)# access-list cc1 extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list cc1
```

以下示例显示了如何通过集群捕获数据路径流量：

```
ciscoasa (config)# capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
ciscoasa (config)# capture abc interface inside match udp host 1.1.1.1 any
ciscoasa (config)# capture abc interface inside access-list xxx
```

以下示例显示了如何为实际源与实际目标相匹配的流量捕获逻辑更新消息，以及如何捕获通过 CCL 转发、实际源与实际目标相匹配的数据包。

```
ciscoasa (config)# access-list dp permit ip real_src real_dst
```

以下示例显示了如何捕获某种类型的数据层面消息，如 ICMP 回应请求/回复，它是使用 **match** 关键字或该消息类型的 ACL 从一个 ASA 转发到另一个 ASA：

```
ciscoasa (config)# capture capture_name interface cluster access-list match icmp any any
```

以下示例显示了如何通过使用 ACL 103 在集群控制链路上创建捕获：

```
ciscoasa (config)# access-list 103 permit ip A B
ciscoasa (config)# capture example1 interface cluster access-list 103
```

在上一个示例中，如果 A 和 B 是 CCL 接口的 IP 地址，则将只捕获在这两台设备之间发送的数据包。

如果 A 和 B 是直通设备流量的 IP 地址，则会发生以下情况：

- 像往常一样捕获转发的数据包，但前提是源和目标 IP 地址与 ACL 相匹配。
- 捕获数据路径逻辑更新消息，但前提是它是 A 与 B 之间的流量或 ACL（例如，访问列表 103）的逻辑更新消息。捕获匹配嵌入式流量的五元组。

虽然 UDP 数据包中的源地址和目标地址是 CCL 地址，但如果该数据包要更新与地址 A 和 B 相关联的流量，则还将捕获该数据包。例如，只要匹配嵌入数据包的地址 A 和 B，就还会捕获该数据包。

查看崩溃转储

如果 ASA 或 ASAv 崩溃，则您可以查看崩溃转储信息。如果要解释崩溃转储，我们建议您联系 Cisco TAC。请参阅命令参考中的 **show crashdump** 命令。

查看核心转储

核心转储是程序异常终止或崩溃时的运行程序快照。核心转储用于诊断或调试错误并保存崩溃以备将来进行非现场分析。Cisco TAC 可能会要求您启用核心转储功能以对 ASA 或 ASAv 上的应用或系统崩溃进行故障排除。请参阅命令参考中的 **coredump** 命令。

ASAv 中的 vCPU 使用率

ASAv vCPU 使用率显示了用于数据路径、控制点和外部进程的 vCPU 用量。

vSphere 报告的 vCPU 使用率包括上述 ASAv 使用率，及：

- ASAv 空闲时间
- 用于 ASAv VM 的 %SYS 开销
- 在 vSwitch、 vNIC 和 pNIC 之间移动数据包的开销。此开销可能会非常大。

CPU 使用率示例

在以下示例中，报告的 vCPU 使用率截然不同：

- ASAv 报告：40%
- DP：35%
- 外部进程：5%
- vSphere 报告：95%
- ASA（作为 ASAv 报告）：40%
- ASA 空闲轮询：10%
- 开销：45%

开销用于执行虚拟机监控程序功能，以及使用 vSwitch 在 NIC 与 vNIC 之间移动数据包。

由于 ESXi 服务器能够代表 ASAv 将其他计算资源用于开销，因此使用率可能会超过 100%。

VMware CPU 使用率报告

在 vSphere 中，点击 **VM Performance** 选项卡，然后点击 **Advanced** 以显示 **Chart Options** 下拉列表，该列表将显示 VM 的每种状态的 vCPU 使用率（%USER、%IDLE、%SYS 等）。此信息有助于从 VMware 的角度了解使用 CPU 资源的位置。

在 ESXi 服务器外壳上（使用 SSH 访问外壳以连接主机），esxtop 是可用的。Esxtop 具有一个与 Linux **top** 命令类似的外观，为 vSphere 性能提供了 VM 状态信息，包括以下信息：

- vCPU、内存和网络使用率的详细信息
- 每个 VM 的每种状态的 vCPU 使用率
- 内存 （运行时键入 M）和网络 （运行时键入 N），以及统计信息和 RX 丢弃的数量

ASAv 和 vCenter 图表

ASAv 与 vCenter 之间的 CPU 使用率 (%) 存在差异：

- vCenter 图表值始终大于 ASAv 值。
- vCenter 称之为 %CPU 使用率；ASAv 称之为 %CPU 利用率。

术语“%CPU 使用率”和“%CPU 利用率”表示不同的东西：

- CPU 利用率提供了物理 CPU 的统计信息。

- CPU 使用率提供了基于 CPU 超线程的逻辑 CPU 统计信息。但是，由于只使用一个 vCPU，因此超线程未打开。

vCenter 按如下方式计算 CPU 使用率 (%)：

当前使用的虚拟 CPU 的用量，以总可用 CPU 的百分比表示

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式如下：

以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率

当比较以 MHz 为单位的使用率时，vCenter 和 ASAv 值是一致的。根据 vCenter 图表，MHz % CPU 使用率计算方式如下：

60/(2499 x 1 vCPU) = 2.4

第 9 部分

记录、SNMP 和 Smart Call Home

日志记录

本章描述如何记录系统消息并将其用于故障排除。

- 第 39-1 页的关于日志记录
- 第 39-4 页的日志记录准则
- 第 39-5 页的配置日志记录
- 第 39-17 页的监控日志
- 第 39-18 页的日志记录示例
- 第 39-18 页的日志记录的历史记录

关于日志记录

系统日志记录是将来自设备的消息收集到运行系统日志守护程序的服务器的方法。记录到中央系统日志服务器有助于汇聚日志和警报。思科设备可以将其日志消息发送到 UNIX 样式系统日志服务。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件将其打印。此形式的日志记录为日志提供受保护的长期存储。日志在例程故障排除和事件处理方面均有帮助。

思科 ASA 系统日志提供有关对 ASA 进行监控和故障排除的信息。通过日志记录功能，可以执行以下操作：

- 指定应记录哪些系统日志消息。
- 禁用或更改系统日志消息的严重性级别。
- 指定一个或多个应发送系统日志消息的位置，包括内部缓冲区、一个或多个系统日志服务器、 ASDM、 SNMP 管理站、指定的邮件地址或 Telnet 和 SSH 会话。
- 以组形式 （例如，按严重性级别或消息类）配置和管理系统日志消息。
- 指定是否对系统日志生成应用速率限制。
- 指出在内部日志缓冲区已满时如何处理其内容，将缓冲区内容发送到 FTP 服务器，或者将内容保存到内部闪存。
- 按位置、严重性级别、类或自定义消息列表过滤系统日志消息。

多情景模式中的日志记录

每个安全情景包含其自己的日志记录配置并生成其自己的消息。如果登录到系统或管理情景，然后更改为其他情景，则在会话中查看的消息只是与当前情景相关的消息。

在系统执行空间中生成的系统日志消息（包括故障转移消息）连同在管理情景中生成的消息在管理情景中进行查看。无法在系统执行空间中配置日志记录或查看任何日志记录信息。

可以配置 ASA 和 ASASM 来将情景名称随附于各消息，从而帮助区分发送到单个系统日志服务器的情景消息。此功能还帮助确定哪些消息来自管理情景，哪些消息来自系统；源于系统执行空间的消息使用设备 ID **system**，源于管理情景的消息使用管理情景的名称作为设备 ID。

系统日志消息分析

以下是可以从各种系统日志消息审阅中获取的信息类型的一些示例：

- ASA 和 ASASM 安全策略允许的连接。这些消息帮助确定安全策略中仍然存在的漏洞。
- ASA 和 ASASM 安全策略拒绝的连接。这些消息显示将哪些类型的活动定向到受保护内部网络。
- 使用 ACE 拒绝速率日志记录功能将显示在 ASA 或 ASA 服务模块 上发生的攻击。
- IDS 活动消息可以显示已发生的攻击。
- 用户身份验证和命令使用情况提供安全策略更改的审计线索。
- 带宽使用情况消息显示已构建和中断的各连接以及使用的持续时间和流量。
- 协议使用情况消息显示用于各连接的协议和端口号。
- 地址转换审计线索消息记录构建或中断的 NAT 或 PAT 连接，在接收到从网络内部到外部环境的恶意活动报告的情况下，这些消息可有所帮助。

系统日志消息格式

系统日志消息以百分比符号 (%) 开头并构造如下：

```
%ASA Level Message_number: Message_text
```

字段描述如下：

ASA	由 ASA 和 ASASM 生成的消息的系统日志消息设备代码。该值始终为 ASA。
Level	1 至 7。级别反映系统日志消息描述的情况的严重性 - 数字越低，情况越严重。
Message_number	用于标识系统日志消息的六位数编号。
Message_text	用于描述情况的文本字符串。系统日志消息的此部分有时包含 IP 地址、端口号或用户名。

严重性级别

表 39-1 列出系统日志消息严重性级别。可以将自定义颜色分配给各严重性级别，从而更轻松地在 ASDM 日志查看器中对其进行区分。如要配置系统日志消息颜色设置，请选择 **Tools > Preferences > Syslog** 选项卡，或者在日志查看器本身中，点击工具栏上的 **Color Settings**。

表 39-1　　系统日志消息严重性级别

级别号	严重性级别	说明
0	**emergencies**	系统不可用。
1	**alert**	需要立即采取措施。
2	**critical**	严重情况。
3	**error**	错误情况。
4	**warning**	警告情况。
5	**notification**	正常但重大的情况。
6	**informational**	消息仅供参考。
7	**debugging**	消息仅供调试。

注　ASA 和 ASASM 不会生成严重性级别为零 (emergencies) 的系统日志消息。此级别在 **logging** 命令中提供用于与 UNIX 系统日志功能兼容，但是不由 ASA 使用。

消息类和系统日志 ID 范围

有关系统日志消息类以及与每个类关联的系统日志消息 ID 范围的列表，请参阅系统日志消息指南。

系统日志消息过滤

您可以过滤生成的系统日志消息，以便仅将某些系统日志消息发送到特定输出目标。例如，可以将 ASA 和 ASASM 配置为将所有系统日志消息发送到一个输出目标，并将这些系统日志消息的子集发送到其他输出目标。

具体而言，可以配置 ASA 和 ASASM，以便根据以下条件将系统日志消息定向到输出目标：

- 系统日志消息 ID 号
- 系统日志消息严重性级别
- 系统日志消息类 （相当于 ASA 和 ASASM 的功能区域）

通过创建在设置输出目标时可以指定的消息列表来定制这些条件。或者，可以将 ASA 或 ASASM 配置为独立于消息列表将特定消息类发送到各类型的输出目标。

可以通过两种方法使用系统日志消息类：

- 使用 **logging class** 命令指定整个类别的系统日志消息的输出位置。
- 使用 **logging list** 命令创建指定消息类的消息列表。

系统日志消息类提供按类型将系统日志消息分类的方法，相当于 ASA 和 ASASM 的特性或功能。例如，vpnc 类表示 VPN 客户端。

特定类中的所有系统日志消息都共享其系统日志消息 ID 号中相同的前三位数字。例如，所有以数字 611 开头的系统日志消息 ID 都与 vpnc（VPN 客户端）类相关联。系统日志消息与从 611101 至 611323 的 VPN 客户端功能范围相关联。

此外，大多数 ISAKMP 系统日志消息都具有公用预置对象集来帮助识别隧道。这些对象在适用时前置于系统日志消息的描述性文本。如果在生成了系统日志消息时对象未知，则不显示特定的*标题 = 值*组合。

对象的前缀如下：

Group = *groupname*, Username = *user*, IP = *IP_address*

其中组是隧道组，用户名是来自本地数据库或 AAA 服务器的用户名，IP 地址是远程访问客户端或第 2 层对等体的公用 IP 地址。

自定义消息列表

创建自定义消息列表是对将哪些系统日志消息发送到哪个输出目标实行控制的一种灵活方法。在自定义系统日志消息列表中，使用以下任何或所有条件指定系统日志消息组：严重性级别、消息 ID、范围日志消息 ID 范围或消息类。

例如，可以使用消息列表执行以下操作：

- 选择严重性级别为 1 和 2 的系统日志消息，然后将其发送到一个或多个邮件地址。
- 选择与消息类 （例如 ha）关联的所有系统日志消息，然后将其保存到内部缓冲区。

消息列表可以包含多个消息选择条件。但是，必须与新命令条目一起添加各消息选择条件。可以创建包含重叠消息选择条件的消息列表。如果消息列表中的两个条件选择同一消息，则仅记录一次消息。

集群

系统日志消息是用于在集群环境中记帐、监控和故障排除的一种实用工具。集群中的每个 ASA 设备 （最多允许八台设备）独立生成系统日志消息；然后，通过某些 **logging** 命令可以控制报头字段，包括时间戳和设备 ID。系统日志服务器使用设备 ID 标识系统日志生成器。您可以使用 **logging device-id** 命令生成具有相同或不同设备 ID 的系统日志消息，使消息看似来自集群中的相同或不同设备。

日志记录准则

IPv6 准则

不支持 IPv6。

其他指导原则

- 系统日志服务器必须运行一个名为 syslogd 的服务器程序。Windows（Windows 95 和 Windows 98 除外）提供系统日志服务器作为其操作系统的一部分。对于 Windows 95 和 Windows 98，必须从其他供应商获取 syslogd 服务器。
- 如要查看 ASA 或 ASASM 生成的日志，必须指定日志记录输出目标。如果启用日志记录而不指定日志记录输出目标，则 ASA 和 ASASM 会生成消息，但不会将其保存到可对其进行查看的位置。必须单独指定每个不同的日志记录输出目标。例如，要将多个系统日志服务器指定为输出目标，请输入新命令为每个系统日志服务器指定单独的条目。

- 在备用 ASA 上不支持通过 TCP 发送系统日志。
- ASA 支持在单情景模式中使用 **logging host** 命令配置 16 个系统日志服务器。在多情景模式中，限制为每个情景 4 个服务器。
- 应该可以通过 ASA 和 ASASM 到达系统日志服务器。应该将 ASASM 配置为拒绝可以从其到达系统日志服务器的接口上的 ICMP 不可达消息，并将系统日志发送到同一服务器。请确保已对所有严重性级别启用日志记录。要防止系统日志服务器崩溃，请抑制生成系统日志 313001、 313004 和 313005。
- 使用自定义消息列表仅与访问列表命中相匹配时，对于已将其日志记录严重性级别提高至调试 （级别 7）的访问列表不会生成访问列表日志。对于 **logging list** 命令，默认日志记录严重性级别设置为 6。此默认行为是故意的。将访问列表配置的日志记录严重性级别显式更改为调试时，还必须更改日志记录配置本身。

  以下是来自 **show running-config logging** 命令的不含访问列表命中的样本输出，因为其日志记录严重性级别已更改为调试：

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test
```

  以下是来自 **show running-config logging** 命令的包含访问列表命中的样本输出：

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging buffered debugging
```

  在此情况下，访问列表配置不更改并会显示访问列表命中数，如下例所示：

```
ciscoasa(config)# access-list global line 1 extended permit icmp any host 4.2.2.2 log
debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended permit tcp host 10.1.1.2 any eq
www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
ciscoasa(config)# access-list global line 3 extended permit ip any any (hitcnt=543)
0x25f9e609
```

配置日志记录

本节描述如何配置日志记录。

步骤 1　启用日志记录 请参阅第 39-6 页的启用日志记录。

步骤 2　配置系统日志消息的输出目标。请参阅第 39-6 页的配置输出目标。

注　最低配置取决于要执行的操作，以及在 ASA 和 ASASM 中处理系统日志消息的要求。

启用日志记录

如要启用日志记录，请执行以下步骤：

操作步骤

步骤 1　启用日志记录

logging enable

示例：

```
ciscoasa(config)# logging enable
```

配置输出目标

如要优化系统日志消息使用情况以进行故障排除和性能监控，建议指定一个或多个应该发送系统日志消息的位置，包括内部日志缓冲区、一个或多个外部系统日志服务器、 ASDM、 SNMP 管理站、控制台端口、指定的邮件地址或 Telnet 和 SSH 会话。

将系统日志消息发送到外部系统日志服务器

可以根据外部系统日志服务器上的可用磁盘空间将消息存档，并在保存日志记录数据后对其进行处理。例如，可以指定在记录特定类型的系统日志消息后要执行的操作，从日志提取数据并将记录保存到其他文件以进行报告，或者使用特定于站点的脚本跟踪统计信息。

如要将系统日志消息发送到外部系统日志服务器，请执行以下步骤：

操作步骤

步骤 1　将 ASA 和 ASASM 配置为向系统日志服务器发送消息。

logging host *interface_name syslog_ip* [**tcp**[*/port*] | **udp**[*/port*] [**format emblem**]]

示例：

```
ciscoasa(config)# logging host dmz1 192.168.1.5 udp 1026 format emblem
```

format emblem 关键字仅对具有 UDP 的系统日志服务器启用 EMBLEM 格式日志记录。*interface_name* 参数指定访问系统日志服务器所通过的接口。 *syslog_ip* 参数指定系统日志服务器的 IP 地址。**tcp**[*/port*] 或 **udp**[*/port*] 关键字/参数对指定 ASA 和 ASASM 应该使用 TCP 或 UDP 将系统日志消息发送到系统日志服务器。

可以将 ASA 配置为使用 UDP 或 TCP（但不同时使用两者）将数据发送到系统日志服务器。如果未指定协议，则默认协议为 UDP。

如果指定 TCP，则在系统日志服务器发生故障时 ASA 和 ASASM 会发现此情况，作为安全防御措施，将会阻止通过 ASA 和 ASA 服务模块 的新连接。如要允许新连接而不考虑与 TCP 系统日志服务器的连接，请参阅第 3 步。如果指定 UDP，则无论系统日志服务器是否可运行， ASA 和 ASASM 都会继续允许新连接。任一协议的有效端口值为 1025 至 65535。默认 UDP 端口为 514。默认 TCP 端口为 1470。

步骤 2　指定应将哪些系统日志消息发送到系统日志服务器。

logging trap {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging trap errors
```

可以指定严重性级别号 （1 至 7）或名称。例如，如果将严重性级别设置为 3，则 ASA 和 ASASM 会发送严重性级别为 3、2 和 1 的系统日志消息。可以指定标识要发送到系统日志服务器的系统日志消息的自定义消息列表。

步骤 3　（可选）禁用在 TCP 连接的系统日志服务器关闭时阻止新连接的功能。

logging permit-hostdown

示例：

```
ciscoasa(config)# logging permit-hostdown
```

如果 ASA 或 ASASM 配置为将系统日志消息发送到基于 TCP 的系统日志服务器，并且如果系统日志服务器关闭或日志队列已满，则会阻止新连接。备份系统日志服务器并且日志队列不再已满后，将再次允许新连接。

步骤 4　（可选）将日志记录设备设置为大多数 UNIX 系统期望的除 20 以外的值。

logging facility *number*

示例：

```
ciscoasa(config)# logging facility 21
```

将系统日志消息发送到内部日志缓冲区

您需要指定应将哪些系统日志记录消息发送到充当临时存储位置的内部日志缓冲区。新消息附加到列表的末尾。当缓冲区已满时 （也就是说，当缓冲区换行时），除非 ASA 和 ASASM 配置为将完整缓冲区保存到其他位置，否则在生成新消息时会覆盖旧消息。

如要将系统日志消息发送到内部日志缓冲区，请执行以下步骤：

操作步骤

步骤 1　指定应将哪些系统日志记录消息发送到充当临时存储位置的内部日志缓冲区。

logging buffered {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging buffered critical

ciscoasa(config)# logging buffered level 2

ciscoasa(config)# logging buffered notif-list
```

新消息附加到列表的末尾。当缓冲区已满时 （也就是说，当缓冲区换行时），除非 ASA 和 ASASM 配置为将完整缓冲区保存到其他位置，否则在生成新消息时会覆盖旧消息。要清空内部日志缓冲区，请输入 **clear logging buffer** 命令。

步骤 2　更改内部日志缓冲区的大小。默认缓冲区大小为 4 KB。

logging buffer-size *bytes*

示例：

```
ciscoasa(config)# logging buffer-size 16384
```

步骤 3　选择以下选项之一：

- 将新消息保存到内部日志缓冲区并将完整日志缓冲区内容保存到内部闪存。

  logging flash-bufferwrap

  示例：

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

- 将新消息保存到内部日志缓冲区并将完整日志缓冲区内容保存到 FTP 服务器。

  logging ftp-bufferwrap

  示例：

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

  将缓冲区内容保存到其他位置时，ASA 和 ASASM 会创建具有使用以下时间戳格式的名称的日志文件：

  LOG-YYYY-MM-DD-HHMMSS.TXT

  其中 *YYYY* 是年，*MM* 是月，*DD* 是月日期，*HHMMSS* 是时间（以小时、分钟和秒为单位）。

- 标识要存储日志缓冲区内容的 FTP 服务器。

  logging ftp-server *server path username password*

  示例：

  ```
  ciscoasa(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
  ```

  server 参数指定外部 FTP 服务器的 IP 地址。*path* 参数指定 FTP 服务器上将保存日志缓冲区数据的目录路径。此路径相对于 FTP 根目录。*username* 参数指定对于登录到 FTP 服务器有效的用户名。 *password* 参数指示所指定用户名的密码。

- 将当前日志缓冲区内容到内部闪存。

  logging savelog [*savefile*]

  示例：

  ```
  ciscoasa(config)# logging savelog latest-logfile.txt
  ```

将系统日志消息发送到邮件地址

如要将系统日志消息发送到邮件地址，请执行以下步骤：

操作步骤

步骤 1　指定应将哪些系统日志消息发送到邮件地址。

logging mail {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging mail high-priority
```

通过邮件发送时，系统日志消息显示在邮件消息的主题行中。因此，建议将此选项配置为通知管理员具有高严重性级别 （例如 critical、 alert 和 emergency）的系统日志消息。

步骤 2　指定在将系统日志消息发送到邮件地址时要使用的源邮件地址。

logging from-address *email_address*

示例：

```
ciscoasa(config)# logging from-address xxx-001@example.com
```

步骤 3　指定在将系统日志消息发送到邮件地址时要使用的收件人邮件地址。

logging recipient-address *e-mail_address* [*severity_level*]

示例：

```
ciscoasa(config)# logging recipient-address admin@example.com
```

步骤 4　指定在将系统日志消息发送到邮件地址时要使用的 SMTP 服务器。

smtp-server *ip_address*

示例：

```
ciscoasa(config)# smtp-server 10.1.1.1
```

将系统日志消息发送 ASDM

如要将系统日志消息发送到 ASDM，请执行以下步骤：

操作步骤

步骤 1　指定应将哪些系统日志消息发送到 ASDM。

logging asdm {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging asdm 2
```

ASA 或 ASASM 为等待发送到 ASDM 的系统日志消息预留一个缓冲区，并在消息出现时将其保存在缓冲区中。ASDM 日志缓冲区是不同于内部日志缓冲区的缓冲区。当 ASDM 日志缓冲区已满时，ASA 或 ASASM 将删除最早的系统日志消息以在缓冲区中为新系统日志消息腾出空间。删除最早的系统日志消息来为新系统日志消息腾出空间是 ASDM 中的默认设置。要控制 ASDM 日志缓冲区中保留的系统日志消息数，可以更改缓冲区的大小。

步骤 2　指定要在 ASDM 日志缓冲区中保留的系统日志消息数。

logging asdm-buffer-size *num_of_msgs*

示例：

```
ciscoasa(config)# logging asdm-buffer-size 200
```

输入 **clear logging asdm** 命令以清空 ASDM 日志缓冲区的当前内容。

将系统日志消息发送到控制台端口

如要将系统日志消息发送到控制台端口，请执行以下步骤：

操作步骤

步骤 1　指定应将哪些系统日志消息发送到控制台端口。

logging console {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging console errors
```

将系统日志消息发送到 SNMP 服务器

如要启用到 SNMP 服务器的日志记录，请执行以下步骤：

步骤 1　启用 SNMP 日志记录并指定要将哪些消息发送到 SNMP 服务器。

logging history [*logging_list* | *level*]

示例：

ciscoasa(config)# logging history errors

输入 **no logging history** 命令以禁用 SNMP 日志记录。

将系统日志消息发送到 Telnet 或 SSH 会话

如要将系统日志消息发送到 Telnet 或 SSH 会话，请执行以下步骤：

操作步骤

步骤 1　指定应将哪些系统日志消息发送到 Telnet 或 SSH 会话。

logging monitor {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging monitor 6
```

步骤 2　启用仅到当前会话的日志记录。

terminal monitor

示例：

```
ciscoasa(config)# terminal monitor
```

如果注销然后再次登录，则需要重新输入此命令。输入 **terminal no monitor** 命令以禁用到当前会话的日志记录。

创建自定义事件列表

可以使用以下三个条件定义事件列表：

- 事件类
- 严重性
- 消息 ID

如要创建将发送到特定日志记录目标（例如，SNMP 服务器）的自定义事件列表，请执行以下步骤：

操作步骤

步骤 1　指定用于选择要保存在内部日志缓冲区中的消息的条件。例如，如果将严重性级别设置为 3，则 ASA 会发送严重性级别为 3、 2 和 1 的系统日志消息。

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

示例：

```
ciscoasa(config)# logging list notif-list level 3
```

name 参数指定列表的名称。 **level** *level* 关键字/参数对指定严重性级别。 **class** *message_class* 关键字/参数对指定特定信息类。 **message** *start_id*[**-***end_id*] 关键字/参数对指定单个系统日志消息号或编号范围。

注　请勿使用严重性级别的名称作为系统日志消息列表的名称。禁止的名称包括 emergencies、alert、 critical、 error、 warning、 notification、 informational 和 debugging。同样，请勿在事件列表名称的开头使用这些单词的前三个字符。例如，请勿使用以字符“err”开头的事件列表名称。

步骤 2　（可选）向列表中添加更多消息选择条件。

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

示例：

```
ciscoasa(config)# logging list notif-list message 104024-105999

ciscoasa(config)# logging list notif-list level critical

ciscoasa(config)# logging list notif-list level warning class ha
```

输入与上一步中相同的命令，指定现有消息列表的名称和其他条件。为要添加到列表的每个条件输入新命令。例如，可以将在列表中包含系统日志消息的条件指定如下：

- 日志消息 ID 属于范围为 104024 至 105999。
- 所有系统日志消息都具有 critical 或更高的严重性级别 （emergency、 alert 或 critical）。
- 所有 ha 类系统日志消息都具有 warning 或更高的严重性级别 （emergency、 alert、 critical、 error 或 warning）。

注　如果系统日志消息满足以下任何条件，则会将其记录。如果系统日志消息满足其中多个条件，则仅记录一次该消息。

将 EMBLEM 格式的系统日志消息生成到系统日志服务器

如要将 EMBLEM 格式的系统日志消息生成到系统日志服务器，请执行以下步骤：

操作步骤

步骤 1　使用端口 514 通过 UDP 将 EMBLEM 格式的系统日志消息发送到系统日志服务器。

logging host *interface_name ip_address* {**tcp**[*/port*] | **udp**[*/port*]} [**format emblem**]

示例：

```
ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
```

format emblem 关键字为系统日志服务器启用 EMBLEM 格式日志记录 （仅限 UDP）。*interface_name* 参数指定访问系统日志服务器所通过的接口。*ip_address* 参数指定系统日志服务器的 IP 地址。**tcp[***/port***]** 或 **udp[***/port***]** 关键字/参数对指定 ASA 和 ASASM 应该使用 TCP 或 UDP 将系统日志消息发送到系统日志服务器。

可以将 ASA 和 ASASM 配置为使用 UDP 或 TCP（但不同时使用两者）将数据发送到系统日志服务器。如果未指定协议，则默认协议为 UDP。

可以使用多个 **logging host** 命令指定将全部接收系统日志消息的其他服务器。如果配置两个或多个系统日志服务器，请确保对于所有日志记录服务器将日志记录严重性级别限于警告。

如果指定 TCP，则在系统日志服务器发生故障时 ASA 或 ASASM 会发现此情况，作为安全防御措施，将会阻止通过 ASA 的新连接。如果指定 UDP，则无论系统日志服务器是否可运行， ASA 或 ASASM 都会继续允许新连接。任一协议的有效端口值为 1025 至 65535。默认 UDP 端口为 514。默认 TCP 端口为 1470。

注　在备用 ASA 上不支持通过 TCP 发送系统日志。

将 EMBLEM 格式的系统日志消息生成到其他输出目标

如要将 EMBLEM 格式的系统日志消息生成到其他输出目标，请执行以下步骤：

操作步骤

步骤 1　将 EMBLEM 格式的系统日志消息发送到除系统日志服务器以外的输出目标，例如 Telnet 或 SSH 会话。

logging emblem

示例：

```
ciscoasa(config)# logging emblem
```

更改可用于日志的内部闪存量

如要更改可用于日志的内部闪存量，请执行以下步骤：

操作步骤

步骤 1　指定可用于保存日志文件的最大内部闪存量。

logging flash-maximum-allocation *kbytes*

示例：

```
ciscoasa(config)# logging flash-maximum-allocation 1200
```

默认情况下，ASA 可以为日志数据使用最多 1 MB 的内部闪存。可供 ASA 和 ASASM 用于保存日志数据的最小内部闪存量为 3 MB。

如果保存到内部闪存的日志文件会导致可用内部闪存量低于配置的最小限制，则 ASA 或 ASASM 会删除最早的日志文件，以确保保存新日志文件后最小内存量保持可用。如果没有要删除的文件，或者如果在删除所有旧文件后可用内存仍然低于限制，则 ASA 或 ASASM 将无法保存新日志文件。

步骤 2　指定必须可供 ASA 或 ASASM 用于保存日志文件的最小内部闪存量。

logging flash-minimum-free *kbytes*

示例：

```
ciscoasa(config)# logging flash-minimum-free 4000
```

配置日志记录队列

如要配置日志记录队列，请执行下列操作：

操作步骤

步骤 1　指定在 ASA 和 ASASM 将系统日志消息发送到已配置的输出目标之前可以在其队列中保留的系统日志消息数。

logging queue *message_count*

示例：

```
ciscoasa(config)# logging queue 300
```

ASA 和 ASASM 在内存中具有固定的块数，这些块可以分配用于在系统日志消息等待发送到已配置的输出目标时将其缓冲存储。所需的块数取决于系统日志消息队列的长度和所指定系统日志服务器的数量。默认队列大小为 512 条系统日志消息。队列大小仅受块内存可用性的限制。有效值为 0 至 8192 条消息，具体视平台而定。如果日志记录队列设置为零，则队列的最大可配置大小为 8192 条消息。

将类中的所有系统日志消息发送到指定输出目标

如要将类中的所有系统日志消息发送到指定输出目标，请执行以下步骤：

操作步骤

步骤 1　覆盖指定的输出目标命令中的配置。例如，如果指定严重性级别为 7 的消息应该转至内部日志缓冲区，并且严重性级别为 3 的 ha 类消息应该转至内部日志缓冲区，则后者配置优先。

logging class *message_class* {**buffered** | **console** | **history** | **mail** | **monitor** | **trap**} [*severity_level*]

示例：

```
ciscoasa(config)# logging class ha buffered alerts
```

buffered、**history**、**mail**、**monitor** 和 **trap** 关键字指定应将此类中的系统日志消息发送到的输出目标。**history** 关键字启用 SNMP 记录。**monitor** 关键字启用 Telnet 和 SSH 日志记录。**trap** 关键字启用系统日志服务器日志记录。每个命令行条目选择一个目标。要指定类应转至多个目标，请为每个输出目标输入一个新命令。

启用安全日志记录

如要启用安全日志记录，请执行以下步骤：

操作步骤

步骤 1　启用安全日志记录

logging host *interface_name syslog_ip* [**tcp**/port | **udp**/*port*] [**format emblem**] [**secure**]

示例：

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure
```

interface_name 参数指定系统日志服务器驻留所在的接口。*syslog_ip* 参数指定系统日志服务器的 IP 地址。*port* 参数指定系统日志服务器侦听以获取系统日志消息的端口（TCP 或 UDP）。**tcp** 关键字指定 ASA 或 ASASM 应使用 TCP 将系统日志消息发送到系统日志服务器。**udp** 关键字指定 ASA 或 ASASM 应使用 UDP 将系统日志消息发送到系统日志服务器。**format emblem** 关键字为系统日志服务器启用 EMBLEM 格式日志记录。 **secure** 关键字指定与远程日志记录主机的连接应仅对 TCP 使用 SSL/TLS。

注　安全日志记录不支持 UDP；如果尝试使用此协议，则会发生错误。

在非 EMBLEM 格式系统日志消息中包含设备 ID

如要在非 EMBLEM 格式系统日志消息中包含设备 ID，请执行以下步骤：

操作步骤

步骤 1　将 ASA 或 ASASM 配置为在非 EMBLEM 格式系统日志消息中包含设备 ID。只能为系统日志消息指定一种类型的设备 ID。

logging device-id {**cluster-id** |**context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

示例：

```
ciscoasa(config)# logging device-id hostname

ciscoasa(config)# logging device-id context-name
```

context-name 关键字指示应用作设备 ID 的当前情景的名称 （仅适用于多情景模式）。如果在多情景模式中为管理情景启用日志记录设备 ID，则源于系统执行空间中的消息使用设备 ID **system**，源于管理情景中的消息使用管理情景的名称作为设备 ID。

注　在 ASA 集群中，始终使用所选接口的主设备 IP 地址。

cluster-id 关键字指定集群中单个 ASA 设备的启动配置中的唯一名称作为设备 ID。**hostname** 关键字指定应用作设备 ID 的 ASA 的主机名。**ipaddress** *interface_name* 关键字/参数对指定应将指定为 *interface_name* 的接口 IP 地址用作设备 ID。如果使用 **ipaddress** 关键字，则无论从哪个接口发送系统日志消息，设备 ID 都会成为指定的 ASA 接口 IP 地址。在群集环境中，**system** 关键字指示设备 ID 成为接口上的系统 IP 地址。此关键字为从设备发送的所有系统日志消息提供单个一致的设备 ID。**string** *text* 关键字/参数对指定应将文本字符串用作设备 ID。字符串可以包含多达 16 个字符。

不能使用空格或以下任何字符：

- & （与号）
- ‘（单引号）
- “（双引号）
- <（小于）
- >（大于）
- ?（问号）

注　如果启用，则在 EMBLEM 格式化系统日志消息和 SNMP 陷阱中不会显示设备 ID。

在系统日志消息中包含日期和时间

如要在系统日志消息中包含日期和时间，请执行以下步骤：

操作步骤

步骤 1　指定系统日志消息应包含其生成日期和时间。

logging timestamp

示例：

```
ciscoasa(config)# logging timestamp
LOG-2008-10-24-081856.TXT
```

如要从系统日志消息中移除日期和时间，请输入 **no logging timestamp** 命令。

禁用系统日志消息

如要禁用指定的系统日志消息，请执行以下步骤：

操作步骤

步骤 1　阻止 ASA 或 ASASM 生成特定系统日志消息。

no logging message *syslog_id*

示例：

```
ciscoasa(config)# no logging message 113019
```

如要重新启用已禁用的系统日志消息，请输入 **logging message** *syslog_id* 命令（例如 **logging message 113019**）。要重新启用所有已禁用的系统日志消息的日志记录，请输入 **clear configure logging disabled** 命令。

更改系统日志消息的严重性级别

如要更改系统日志消息的严重性级别，请执行以下步骤：

操作步骤

步骤 1　指定系统日志消息的严重性级别。

logging message *syslog_id* **level** *severity_level*

示例：

```
ciscoasa(config)# logging message 113019 level 5
```

如要将系统日志消息的严重性级别重置为其设置，请输入 **no logging message** *syslog_id* **level** *severity_level* 命令（例如 **no logging message 113019 level 5**）。要将所有已修改的系统日志消息的严重性级别重置为其设置，请输入 **clear configure logging level** 命令。

限制系统日志消息生成速率

如要限制系统日志消息生成速率，请执行以下步骤：

操作步骤

步骤 1　在指定时间段内将指定的严重性级别 （1 至 7）应用于消息集或单条消息 （不是目标）。

logging rate-limit {unlimited | {*num* [*interval*]}} message *syslog_id* | level *severity_level*

示例：

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

速率限制会影响发送到所有已配置的目标的消息量。要将日志记录速率限制重置为默认值，请输入 **clear running-config logging rate-limit** 命令。要重置日志记录速率限制，请输入 **clear configure logging rate-limit** 命令。

监控日志

有关监控日志记录状态的信息，请参阅以下命令。

- **show logging**

  此命令显示系统日志消息，包括严重性级别。

  注　可供查看的最大系统日志消息数为 1000，这是默认设置。可供查看的最大系统日志消息数为 2000。

- **show logging message**

  此命令显示严重性级别已修改的系统日志消息和已禁用的系统日志消息的列表。

- **show logging message** *message_ID*

  此命令显示特定系统日志消息的严重性级别。

- **show logging queue**

  此命令显示日志记录队列和队列统计信息。

- **show logging rate-limit**

  此命令显示不允许的系统日志消息。

- **show running-config logging rate-limit**

  此命令显示当前日志记录速率限制设置。

日志记录示例

以下示例显示所显示的有关 **show logging** 命令的日志记录信息。

```
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address “10.1.1.1”
    Mail logging: disabled
    ASDM logging: disabled
```

以下示例显示如何同时控制是否启用了系统日志消息以及指定的系统日志消息的严重性级别：

```
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)

ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (disabled)

ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)
```

日志记录的历史记录

表 39-2　　日志记录的历史记录

功能名称	平台版本	说明
日志记录	7.0(1)	通过各种输出目标提供 ASA 网络日志记录信息，并且包含用于查看和保存日志文件的选项。
速率限制	7.0(4)	限制生成系统日志消息的速率。 引入了以下命令：**logging rate-limit**。

表 39-2　　日志记录的历史记录（续）

功能名称	平台版本	说明
日志记录列表	7.2(1)	创建要在其他命令中用于按各种条件 （日志记录级别、事件类和消息 ID）指定消息的日志记录列表。 引入了以下命令：**logging** list。
安全日志记录	8.0(2)	指定与远程日志记录主机的连接应使用 SSL/TLS。仅在所选的协议为 TCP 的情况下此选项才有效。 修改了以下命令：**logging host**。
日志记录类	8.0(4) 和 8.1(1)	添加了对日志记录消息的 ipaa 事件类的支持。 修改了以下命令：**logging class**。
日志记录类和已保存的日志记录缓冲区	8.2(1)	添加了对日志记录消息的 dap 事件类的支持。 修改了以下命令：**logging class**。 添加了对清除已保存的日志记录缓冲区 （ASDM、内部、 FTP 和闪存）的支持。 引入了以下命令：**clear logging queue bufferwrap**。
密码加密	8.3(1)	添加了对密码加密的支持。 修改了以下命令：**logging ftp server**。
增强型日志记录和连接阻止	8.3(2)	将系统日志服务器配置为使用 TCP 并且系统日志服务器不可用时，ASA 会阻止可生成系统日志消息的新连接，直到服务器再次变为可用为止 （例如，VPN、防火墙和直通代理连接）。此功能已增强为在 ASA 上的日志记录队列已满时也阻止新连接，清除日志记录队列后，连接会恢复。 为符合通用标准 EAL4+ 而添加了此功能。除非要求，否则建议在无法发送或接收系统日志消息时允许连接。要允许连接，请继续使用 **logging permit-hostdown** 命令。 修改了以下命令：**show logging**。 引入了以下系统日志消息：414005、 414006、 414007 和 414008。
集群	9.0(1)	添加了对于在 ASA 5580 和 5585-X 上的集群环境中生成系统日志消息的支持。 修改了以下命令：**logging device-id**。

SNMP

本章描述如何配置简单网络管理协议 (SNMP) 以监控思科 ASA。

- 第 40-1 页的关于 SNMP
- 第 40-16 页的 SNMP 准则
- 第 40-18 页的配置 SNMP
- 第 40-26 页的 SNMP 第 1 和 2c 版示例
- 第 40-26 页的 SNMP 第 3 版示例
- 第 40-25 页的监控 SNMP
- 第 40-27 页的 SNMP 历史记录

关于 SNMP

SNMP 是促进网络设备之间的管理信息交换的应用层协议，并且是 TCP/IP 协议套件的一部分。ASA、 ASAv 和 ASASM 使用 SNMP 第 1、 2c 和 3 版为网络监控提供支持，并且支持同时使用全部三个版本。利用在 ASA 接口上运行的 SNMP 代理，可以通过诸如 HP OpenView 之类的网络管理系统 (NMS) 监控 ASA 和 ASASM。 ASA、 ASAv 和 ASASM 通过发出 GET 请求来支持 SNMP 只读访问。不允许 SNMP 写访问，因此，无法对 SNMP 进行更改。此外，不支持 SNMP SET 请求。

可以将 ASA、 ASAv 和 ASASM 配置为发送陷阱，它们是指向 NMS 的特定事件 （事件通知）的从受管设备到管理站的未经请求的消息，也可以使用 NMS 在 ASA 上浏览管理信息库 (MIB)。MIB 是定义的集合，ASA、ASAv 和 ASASM 维护由每个定义的值组成的数据库。浏览 MIB 意味着从 NMS 发出 MIB 树的一系列 GET-NEXT 或 GET-BULKGET 请求以确定值。

ASA、 ASAv 和 ASASM 具有 SNMP 代理，用于在发生预定义为需要通知 （例如，当网络中的链路开启或关闭时）的事件的情况下通知指定的管理站。它发送的通知包括用于向管理站表明其自身身份 SNMP OID。 ASA、 ASAv 或 ASASM SNMP 代理还会在管理站请求信息时进行应答。

SNMP 术语

表 40-1 列出在使用 SNMP 时常用的术语。

表 40-1 SNMP 术语

术语	说明
代理	在 ASA 上运行的 SNMP 服务器。 SNMP 代理具有以下功能： • 对来自网络管理站的信息和操作请求作出响应。 • 控制对其管理信息库（即 SNMP 可以查看或更改的对象的集合）的访问。 • 不允许 SET 操作。
浏览	通过从设备上的 SNMP 代理轮询所需信息来从网络管理站监控该设备的运行状况。此活动可能包括从网络管理站发出 MIB 树的一系列 GET-NEXT 或 GET-BULK 请求以确定值。
管理信息库 (MIB)	用于收集有关数据包、连接、缓冲区、故障转移等的信息的标准化数据结构。 MIB 由大多数网络设备使用的产品、协议和硬件标准来定义。 SNMP 网络管理站可以浏览 MIB，并请求在出现特定数据或事件时将其发送。
网络管理站 (NMS)	PC 或工作站设置为监控 SNMP 事件和管理设备，例如 ASA、 ASAv 和 ASASM。
对象标识符 (OID)	用于向设备的 NMS 表明该设备的身份并向用户指示监控和显示的信息源的系统。
陷阱	用于生成从 SNMP 代理到 NMS 的消息的预定义事件。事件包括警报条件，例如链路开启、链路关闭、冷启动、热启动、身份验证或系统日志消息。

MIB 和陷阱

MIB 特定于标准或特定于企业。标准 MIB 由 IETF 创建并记录在各种 RFC 中。陷阱报告发生在网络设备上的重大事件，大多数情况下是错误或故障。 SNMP 陷阱在特定于标准或特定于企业的 MIB 中进行定义。标准陷阱由 IETF 创建并记录在各种 RFC 中。 SNMP 陷阱会编译成 ASA、ASAv 或 ASASM 软件。

如果需要，还可以从以下位置下载 RFC、标准 MIB 和标准陷阱：

http://www.ietf.org/

ftp://ftp-sj.cisco.com/pub/mibs

从以下位置下载 Cisco MIB、陷阱和 OID 的完整列表：

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

此外，从以下位置通过 FTP 下载思科 OID：

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

注 在软件 7.2(1) 版、 8.0(2) 版及更高版本中，通过 SNMP 访问的接口信息大约每 5 秒进行刷新。因此，建议在连续的轮询之间等待至少 5 秒。

MIB 中的所有 OID 并非都受支持。要获取特定 ASA 或 ASASM 的受支持 SNMP MIB 和 OID 的列表，请输入以下命令：

```
ciscoasa(config)# show snmp-server oidlist
```

注　尽管 **oidlist** 关键字没有显示在 **show snmp-server** 命令的选项列表中，但是它可用。不过，此命令仅供思科 TAC 使用。使用此命令之前，请联系思科 TAC。

以下是来自 **show snmp-server oidlist** 命令的样本输出：

```
ciscoasa(config)# show snmp-server oidlist
[0]     1.3.6.1.2.1.1.1.          sysDescr
[1]     1.3.6.1.2.1.1.2.          sysObjectID
[2]     1.3.6.1.2.1.1.3.          sysUpTime
[3]     1.3.6.1.2.1.1.4.          sysContact
[4]     1.3.6.1.2.1.1.5.          sysName
[5]     1.3.6.1.2.1.1.6.          sysLocation
[6]     1.3.6.1.2.1.1.7.          sysServices
[7]     1.3.6.1.2.1.2.1.          ifNumber
[8]     1.3.6.1.2.1.2.2.1.1.      ifIndex
[9]     1.3.6.1.2.1.2.2.1.2.      ifDescr
[10]    1.3.6.1.2.1.2.2.1.3.      ifType
[11]    1.3.6.1.2.1.2.2.1.4.      ifMtu
[12]    1.3.6.1.2.1.2.2.1.5.      ifSpeed
[13]    1.3.6.1.2.1.2.2.1.6.      ifPhysAddress
[14]    1.3.6.1.2.1.2.2.1.7.      ifAdminStatus
[15]    1.3.6.1.2.1.2.2.1.8.      ifOperStatus
[16]    1.3.6.1.2.1.2.2.1.9.      ifLastChange
[17]    1.3.6.1.2.1.2.2.1.10.     ifInOctets
[18]    1.3.6.1.2.1.2.2.1.11.     ifInUcastPkts
[19]    1.3.6.1.2.1.2.2.1.12.     ifInNUcastPkts
[20]    1.3.6.1.2.1.2.2.1.13.     ifInDiscards
[21]    1.3.6.1.2.1.2.2.1.14.     ifInErrors
[22]    1.3.6.1.2.1.2.2.1.16.     ifOutOctets
[23]    1.3.6.1.2.1.2.2.1.17.     ifOutUcastPkts
[24]    1.3.6.1.2.1.2.2.1.18.     ifOutNUcastPkts
[25]    1.3.6.1.2.1.2.2.1.19.     ifOutDiscards
[26]    1.3.6.1.2.1.2.2.1.20.     ifOutErrors
[27]    1.3.6.1.2.1.2.2.1.21.     ifOutQLen
[28]    1.3.6.1.2.1.2.2.1.22.     ifSpecific
[29]    1.3.6.1.2.1.4.1.          ipForwarding
[30]    1.3.6.1.2.1.4.20.1.1.     ipAdEntAddr
[31]    1.3.6.1.2.1.4.20.1.2.     ipAdEntIfIndex
[32]    1.3.6.1.2.1.4.20.1.3.     ipAdEntNetMask
[33]    1.3.6.1.2.1.4.20.1.4.     ipAdEntBcastAddr
[34]    1.3.6.1.2.1.4.20.1.5.     ipAdEntReasmMaxSize
[35]    1.3.6.1.2.1.11.1.         snmpInPkts
[36]    1.3.6.1.2.1.11.2.         snmpOutPkts
[37]    1.3.6.1.2.1.11.3.         snmpInBadVersions
[38]    1.3.6.1.2.1.11.4.         snmpInBadCommunityNames
[39]    1.3.6.1.2.1.11.5.         snmpInBadCommunityUses
[40]    1.3.6.1.2.1.11.6.         snmpInASNParseErrs
[41]    1.3.6.1.2.1.11.8.         snmpInTooBigs
[42]    1.3.6.1.2.1.11.9.         snmpInNoSuchNames
[43]    1.3.6.1.2.1.11.10.        snmpInBadValues
[44]    1.3.6.1.2.1.11.11.        snmpInReadOnlys
[45]    1.3.6.1.2.1.11.12.        snmpInGenErrs
[46]    1.3.6.1.2.1.11.13.        snmpInTotalReqVars
[47]    1.3.6.1.2.1.11.14.        snmpInTotalSetVars
[48]    1.3.6.1.2.1.11.15.        snmpInGetRequests
[49]    1.3.6.1.2.1.11.16.        snmpInGetNexts
[50]    1.3.6.1.2.1.11.17.        snmpInSetRequests
[51]    1.3.6.1.2.1.11.18.        snmpInGetResponses
[52]    1.3.6.1.2.1.11.19.        snmpInTraps
[53]    1.3.6.1.2.1.11.20.        snmpOutTooBigs
[54]    1.3.6.1.2.1.11.21.        snmpOutNoSuchNames
```

```
[55]    1.3.6.1.2.1.11.22.      snmpOutBadValues
[56]    1.3.6.1.2.1.11.24.      snmpOutGenErrs
[57]    1.3.6.1.2.1.11.25.      snmpOutGetRequests
[58]    1.3.6.1.2.1.11.26.      snmpOutGetNexts
[59]    1.3.6.1.2.1.11.27.      snmpOutSetRequests
[60]    1.3.6.1.2.1.11.28.      snmpOutGetResponses
[61]    1.3.6.1.2.1.11.29.      snmpOutTraps
[62]    1.3.6.1.2.1.11.30.      snmpEnableAuthenTraps
[63]    1.3.6.1.2.1.11.31.      snmpSilentDrops
[64]    1.3.6.1.2.1.11.32.      snmpProxyDrops
[65]    1.3.6.1.2.1.31.1.1.1.1. ifName
[66]    1.3.6.1.2.1.31.1.1.1.2. ifInMulticastPkts
[67]    1.3.6.1.2.1.31.1.1.1.3. ifInBroadcastPkts
[68]    1.3.6.1.2.1.31.1.1.1.4. ifOutMulticastPkts
[69]    1.3.6.1.2.1.31.1.1.1.5. ifOutBroadcastPkts
[70]    1.3.6.1.2.1.31.1.1.1.6. ifHCInOctets
--More--
```

SNMP 对象标识符

每个思科系统级产品都具有供用作 MIB-II sysObjectID 的 SNMP 对象标识符 (OID)。CISCO-PRODUCTS-MIB 包含可以在 SNMPv2-MIB 中的 sysObjectID 对象内报告的 OID。可以使用该值标识型号。表 40-2 列出 ASA 型号的 sysObjectID OID。

表 40-2 SNMP 对象标识符

产品标识符	sysObjectID	型号编号
ASA5585-SSP10	ciscoASA5585Ssp10 (ciscoProducts 1194)	ASA 5585-X SSP-10
ASA5585-SSP20	ciscoASA5585Ssp20 (ciscoProducts 1195)	ASA 5585-X SSP-20
ASA5585-SSP40	ciscoASA5585Ssp40 (ciscoProducts 1196)	ASA 5585-X SSP-40
ASA5585-SSP60	ciscoASA5585Ssp60 (ciscoProducts 1197)	ASA 5585-X SSP-60
ASA5585-SSP10	ciscoASA5585Ssp10sc (ciscoProducts 1198)	ASA 5585-X SSP-10 安全情景
ASA5585-SSP20	ciscoASA5585Ssp20sc (ciscoProducts 1199)	ASA 5585-X SSP-20 安全情景
ASA5585-SSP40	ciscoASA5585Ssp40sc (ciscoProducts 1200)	ASA 5585-X SSP-40 安全情景
ASA5585-SSP60	ciscoASA5585Ssp60sc (ciscoProducts 1201)	ASA 5585-X SSP-60 安全情景
ASA5585-SSP10	ciscoASA5585Ssp10sy (ciscoProducts 1202)	ASA 5585-X SSP-10 系统情景
ASA5585-SSP20	ciscoASA5585Ssp20sy (ciscoProducts 1203)	ASA 5585-X SSP-20 系统情景
ASA5585-SSP40	ciscoASA5585Ssp40sy (ciscoProducts 1204)	ASA 5585-X SSP-40 系统情景
ASA5585-SSP60	ciscoASA5585Ssp60sy (ciscoProducts 1205)	ASA 5585-X SSP-60 系统情景
适用于 Catalyst 交换机/7600 路由器的ASA 服务模块	ciscoAsaSm1 (ciscoProducts 1277)	适用于 Catalyst 交换机/7600 路由器的自适应安全设备 (ASA) 服务模块
适用于 Catalyst 交换机/7600 路由器的ASA 服务模块安全情景	ciscoAsaSm1sc (ciscoProducts 1275)	适用于 Catalyst 交换机/7600 路由器的自适应安全设备 (ASA) 服务模块安全情景
无负载加密的适用于 Catalyst 交换机/7600 路由器的ASA 服务模块安全情景	ciscoAsaSm1K7sc (ciscoProducts 1334)	无负载加密的适用于Catalyst交换机/7600 路由器的自适应安全设备 (ASA) 服务模块安全情景
适用于 Catalyst 交换机/7600 路由器的ASA 服务模块系统情景	ciscoAsaSm1sy (ciscoProducts 1276)	适用于 Catalyst 交换机/7600 路由器的自适应安全设备 (ASA) 服务模块系统情景

表 40-2　SNMP 对象标识符（续）

无负载加密的适用于 Catalyst 交换机/7600 路由器的ASA 服务模块系统情景	ciscoAsaSm1K7sy (ciscoProducts 1335)	无负载加密的适用于 Catalyst 交换机/7600 路由器的自适应安全设备 (ASA) 服务模块系统情景
无负载加密的适用于 Catalyst 交换机/7600 路由器的ASA 服务模块系统情景	ciscoAsaSm1K7 (ciscoProducts 1336)	无负载加密的适用于 Catalyst 交换机/7600 路由器的自适应安全设备 (ASA) 服务模块
ASA 5512	ciscoASA5512 (ciscoProducts 1407)	ASA 5512 自适应安全设备
ASA 5525	ciscoASA5525 (ciscoProducts 1408)	ASA 5525 自适应安全设备
ASA 5545	ciscoASA5545 (ciscoProducts 1409)	ASA 5545 自适应安全设备
ASA 5555	ciscoASA5555 (ciscoProducts 1410)	ASA 5555 自适应安全设备
ASA 5512 安全情景	ciscoASA5512sc (ciscoProducts 1411)	ASA 5512 自适应安全设备安全情景
ASA 5525 安全情景	ciscoASA5525sc (ciscoProducts 1412)	ASA 5525 自适应安全设备安全情景
ASA 5545 安全情景	ciscoASA5545sc (ciscoProducts 1413)	ASA 5545 自适应安全设备安全情景
ASA 5555 安全情景	ciscoASA5555sc (ciscoProducts 1414)	ASA 5555 自适应安全设备安全情景
ASA 5512 系统情景	ciscoASA5512sy (ciscoProducts 1415)	ASA 5512 自适应安全设备系统情景
ASA 5515 系统情景	ciscoASA5515sy (ciscoProducts 1416)	ASA 5515 自适应安全设备系统情景
ASA 5525 系统情景	ciscoASA5525sy (ciscoProducts1417)	ASA 5525 自适应安全设备系统情景
ASA 5545 系统情景	ciscoASA5545sy (ciscoProducts 1418)	ASA 5545 自适应安全设备系统情景
ASA 5555 系统情景	ciscoASA5555sy (ciscoProducts 1419)	ASA 5555 自适应安全设备系统情景
ASA 5515 安全情景	ciscoASA5515sc (ciscoProducts 1420)	ASA 5515 自适应安全设备系统情景
ASA 5515	ciscoASA5515 (ciscoProducts 1421)	ASA 5515 自适应安全设备
ASAv	ciscoASAv (ciscoProducts 1902)	思科自适应安全虚拟设备 (ASAv)
ASAv 系统情景	ciscoASAvsy (ciscoProducts 1903)	思科自适应安全虚拟设备 (ASAv) 系统情景
ASAv 安全情景	ciscoASAvsc (ciscoProducts 1904)	思科自适应安全虚拟设备 (ASAv) 安全情景

物理供应商类型值

每个 Cisco 机箱或独立系统都具有供 SNMP 使用的唯一类型编号。entPhysicalVendorType OID 在 CISCO-ENTITY-VENDORTYPE-OID-MIB 中进行定义。可以从 ASA、ASAv 或 ASASM SNMP 代理在 entPhysicalVendorType 对象中返回该值。可以使用该值标识组件的类型 （模块、电源、风扇、传感器、 CPU 等）。表 40-3 列出 ASA 和 ASASM 型号的物理供应商类型值。

表 40-3　物理供应商类型值

项目	entPhysicalVendorType OID 说明
适用于 Catalyst 交换机/7600 路由器的ASA 服务模块	cevCat6kWsSvcAsaSm1 (cevModuleCat6000Type 169)
无负载加密的适用于 Catalyst 交换机/7600 路由器的ASA 服务模块	cevCat6kWsSvcAsaSm1K7 (cevModuleCat6000Type 186)
思科自适应安全设备 (ASA) 5512 自适应安全设备	cevChassisASA5512 (cevChassis 1113)

表 40-3 物理供应商类型值（续）

无负载加密的思科自适应安全设备 (ASA) 5512 自适应安全设备	cevChassisASA5512K7 (cevChassis 1108)
思科自适应安全设备 (ASA) 5515 自适应安全设备	cevChassisASA5515 (cevChassis 1114)
无负载加密的思科自适应安全设备 (ASA) 5515 自适应安全设备	cevChassisASA5515K7 (cevChassis 1109)
思科自适应安全设备 (ASA) 5525 自适应安全设备	cevChassisASA5525 (cevChassis 1115)
无负载加密的思科自适应安全设备 (ASA) 5525 自适应安全设备	cevChassisASA5525K7 (cevChassis 1110)
思科自适应安全设备 (ASA) 5545 自适应安全设备	cevChassisASA5545 (cevChassis 1116)
无负载加密的思科自适应安全设备 (ASA) 5545 自适应安全设备	cevChassisASA5545K7 (cevChassis 1111)
思科自适应安全设备 (ASA) 5555 自适应安全设备	cevChassisASA5555 (cevChassis 1117)
无负载加密的思科自适应安全设备 (ASA) 5555 自适应安全设备	cevChassisASA5555K7 (cevChassis 1112)
思科自适应安全设备 5512 的中央处理器	cevCpuAsa5512 (cevModuleCpuType 229)
无负载加密的思科自适应安全设备 5512 的中央处理器	cevCpuAsa5512K7 (cevModuleCpuType 224)
思科自适应安全设备 5515 的中央处理器	cevCpuAsa5515 (cevModuleCpuType 230)
无负载加密的思科自适应安全设备 5515 的中央处理器	cevCpuAsa5515K7 (cevModuleCpuType 225)
思科自适应安全设备 5525 的中央处理器	cevCpuAsa5525 (cevModuleCpuType 231)
无负载加密的思科自适应安全设备 5525 的中央处理器	cevCpuAsa5525K7 (cevModuleCpuType 226)
思科自适应安全设备 5545 的中央处理器	cevCpuAsa5545 (cevModuleCpuType 232)
无负载加密的思科自适应安全设备 5545 的中央处理器	cevCpuAsa5545K7 (cevModuleCpuType 227)
思科自适应安全设备 5555 的中央处理器	cevCpuAsa5555 (cevModuleCpuType 233)
无负载加密的思科自适应安全设备 5555 的中央处理器	cevCpuAsa5555K7 (cevModuleCpuType 228)
ASA 5585 SSP-10 的 CPU	cevCpuAsa5585Ssp10 (cevModuleCpuType 204)
无负载加密的 ASA 5585 SSP-10 的 CPU	cevCpuAsa5585Ssp10K7 (cevModuleCpuType 205)
ASA 5585 SSP-20 的 CPU	cevCpuAsa5585Ssp20 (cevModuleCpuType 206)
无负载加密的 ASA 5585 SSP-20 的 CPU	cevCpuAsa5585Ssp20K7 (cevModuleCpuType 207)
ASA 5585 SSP-40 的 CPU	cevCpuAsa5585Ssp40 (cevModuleCpuType 208)
无负载加密的 ASA 5585 SSP-40 的 CPU	cevCpuAsa5585Ssp40K7 (cevModuleCpuType 209)
ASA 5585 SSP-60 的 CPU	cevCpuAsa5585Ssp60 (cevModuleCpuType 210)
无负载加密的 ASA 5585 SSP-60 的 CPU	cevCpuAsa5585Ssp60K (cevModuleCpuType 211)
适用于 Catalyst 交换机/7600 路由器的思科ASA 服务模块的 CPU	cevCpuAsaSm1 (cevModuleCpuType 222)
无负载加密的适用于 Catalyst 交换机/7600 路由器的思科 ASA 服务模块的 CPU	cevCpuAsaSm1K7 (cevModuleCpuType 223)
自适应安全设备 5512 中的机箱冷却风扇	cevFanASA5512ChassisFan (cevFan 163)
无负载加密的自适应安全设备 5512 中的机箱冷却风扇	cevFanASA5512K7ChassisFan (cevFan 172)
自适应安全设备 5515 中的机箱冷却风扇	cevFanASA5515ChassisFan (cevFan 164)

表 40-3　　物理供应商类型值（续）

无负载加密的自适应安全设备 5515 中的机箱冷却风扇	cevFanASA5515K7ChassisFan (cevFan 171)
自适应安全设备 5525 中的机箱冷却风扇	cevFanASA5525ChassisFan (cevFan 165)
无负载加密的自适应安全设备 5525 中的机箱冷却风扇	cevFanASA5525K7ChassisFan (cevFan 170)
自适应安全设备 5545 中的机箱冷却风扇	cevFanASA5545ChassisFan (cevFan 166)
无负载加密的自适应安全设备 5545 中的机箱冷却风扇	cevFanASA5545K7ChassisFan (cevFan 169)
无负载加密的自适应安全设备 5545 中的电源风扇	cevFanASA5545K7PSFan (cevFan 161)
自适应安全设备 5545 中的电源风扇	cevFanASA5545PSFan (cevFan 159)
自适应安全设备 5555 中的机箱冷却风扇	cevFanASA5555ChassisFan (cevFan 167)
无负载加密的自适应安全设备 5555 中的机箱冷却风扇	cevFanASA5555K7ChassisFan (cevFan 168)
自适应安全设备 5555 中的电源风扇	cevFanASA5555PSFan (cevFan 160)
无负载加密的自适应安全设备 5555 中的电源风扇	cevFanASA5555PSFanK7 (cevFan 162)
ASA 5585-X 的电源风扇	cevFanASA5585PSFan (cevFan 146)
10 千兆以太网接口	cevPort10GigEthernet (cevPort 315)
千兆以太网端口	cevPortGe (cevPort 109)
自适应安全设备 5545 中的电源装置	cevPowerSupplyASA5545PSInput (cevPowerSupply 323)
自适应安全设备 5545 中的电源输入状态传感器	cevPowerSupplyASA5545PSPresence (cevPowerSupply 321)
自适应安全设备 5555 中的电源装置	cevPowerSupplyASA5555PSInput (cevPowerSupply 324)
自适应安全设备 5555 中的电源输入状态传感器	cevPowerSupplyASA5555PSPresence (cevPowerSupply 322)
ASA 5585 的电源输入	cevPowerSupplyASA5585PSInput (cevPowerSupply 304)
思科自适应安全设备 (ASA) 5512 机箱风扇传感器	cevSensorASA5512ChassisFanSensor (cevSensor 120)
思科自适应安全设备 5512 的机箱环境温度传感器	cevSensorASA5512ChassisTemp (cevSensor 107)
思科自适应安全设备 5512 的中央处理器温度传感器	cevSensorASA5512CPUTemp (cevSensor 96)
无负载加密的思科自适应安全设备 (ASA) 5512 机箱风扇传感器	cevSensorASA5512K7ChassisFanSensor (cevSensor 125)
无负载加密的思科自适应安全设备 5512 的中央处理器温度传感器	cevSensorASA5512K7CPUTemp (cevSensor 102)
无负载加密的自适应安全设备 5512 中的机箱冷却风扇传感器	cevSensorASA5512K7PSFanSensor (cevSensor 116)
自适应安全设备 5512 中的机箱冷却风扇传感器	cevSensorASA5512PSFanSensor (cevSensor 119)
思科自适应安全设备 (ASA) 5515 机箱风扇传感器	cevSensorASA5515ChassisFanSensor (cevSensor 121)
思科自适应安全设备 5515 的机箱环境温度传感器	cevSensorASA5515ChassisTemp (cevSensor 98)
思科自适应安全设备 5515 的中央处理器温度传感器	cevSensorASA5515CPUTemp (cevSensor 97)
无负载加密的思科自适应安全设备 (ASA) 5515 机箱风扇传感器	cevSensorASA5515K7ChassisFanSensor (cevSensor 126)
无负载加密的思科自适应安全设备 5515 的中央处理器温度传感器	cevSensorASA5515K7CPUTemp (cevSensor 103)

表 40-3 物理供应商类型值（续）

无负载加密的自适应安全设备 5515 中的机箱冷却风扇传感器	cevSensorASA5515K7PSFanSensor (cevSensor 115)
自适应安全设备 5515 中的机箱冷却风扇传感器	cevSensorASA5515PSFanSensor (cevSensor 118)
思科自适应安全设备 (ASA) 5525 机箱风扇传感器	cevSensorASA5525ChassisFanSensor (cevSensor 122)
思科自适应安全设备 5525 的机箱环境温度传感器	cevSensorASA5525ChassisTemp (cevSensor 108)
思科自适应安全设备 5525 的中央处理器温度传感器	cevSensorASA5525CPUTemp (cevSensor 99)
无负载加密的思科自适应安全设备 (ASA) 5525 机箱风扇传感器	cevSensorASA5525K7ChassisFanSensor (cevSensor 127)
无负载加密的思科自适应安全设备 5525 的中央处理器温度传感器	cevSensorASA5525K7CPUTemp (cevSensor 104)
无负载加密的自适应安全设备 5525 中的机箱冷却风扇传感器	cevSensorASA5525K7PSFanSensor (cevSensor 114)
自适应安全设备 5525 中的机箱冷却风扇传感器	cevSensorASA5525PSFanSensor (cevSensor 117)
思科自适应安全设备 (ASA) 5545 机箱风扇传感器	cevSensorASA5545ChassisFanSensor (cevSensor 123)
思科自适应安全设备 5545 的机箱环境温度传感器	cevSensorASA5545ChassisTemp (cevSensor 109)
思科自适应安全设备 5545 的中央处理器温度传感器	cevSensorASA5545CPUTemp (cevSensor 100)
无负载加密的思科自适应安全设备 (ASA) 5545 机箱风扇传感器	cevSensorASA5545K7ChassisFanSensor (cevSensor 128)
无负载加密的思科自适应安全设备 5545 的机箱环境温度传感器	cevSensorASA5545K7ChassisTemp (cevSensor 90)
无负载加密的思科自适应安全设备 5545 的中央处理器温度传感器	cevSensorASA5545K7CPUTemp (cevSensor 105)
无负载加密的自适应安全设备 5545 中的机箱冷却风扇传感器	cevSensorASA5545K7PSFanSensor (cevSensor 113)
无负载加密的自适应安全设备 5545 中的电源输入状态传感器	cevSensorASA5545K7PSPresence (cevSensor 87)
无负载加密的自适应安全设备 5545 中的电源风扇温度传感器	cevSensorASA5545K7PSTempSensor (cevSensor 94)
无负载加密的自适应安全设备 5545 中的电源风扇传感器	cevSensorASA5545PSFanSensor (cevSensor 89)
自适应安全设备 5545 中的电源输入状态传感器	cevSensorASA5545PSPresence (cevSensor 130)
自适应安全设备 5555 中的电源输入状态传感器	cevSensorASA5545PSPresence (cevSensor 131)
自适应安全设备 5545 中的电源风扇温度传感器	cevSensorASA5545PSTempSensor (cevSensor 92)
思科自适应安全设备 (ASA) 5555 机箱风扇传感器	cevSensorASA5555ChassisFanSensor (cevSensor 124)
思科自适应安全设备 5555 的机箱环境温度传感器	cevSensorASA5555ChassisTemp (cevSensor 110)
思科自适应安全设备 5555 的中央处理器温度传感器	cevSensorASA5555CPUTemp (cevSensor 101)
无负载加密的思科自适应安全设备 (ASA) 5555 机箱风扇传感器	cevSensorASA5555K7ChassisFanSensor (cevSensor 129)
无负载加密的思科自适应安全设备 5555 的机箱环境温度传感器	cevSensorASA5555K7ChassisTemp (cevSensor 111)
无负载加密的思科自适应安全设备 5555 的中央处理器温度传感器	cevSensorASA5555K7CPUTemp (cevSensor 106)

表 40-3　物理供应商类型值（续）

无负载加密的自适应安全设备 5555 中的机箱冷却风扇传感器	cevSensorASA5555K7PSFanSensor (cevSensor 112)
无负载加密的自适应安全设备 5555 中的电源输入状态传感器	cevSensorASA5555K7PSPresence (cevSensor 88)
无负载加密的自适应安全设备 5555 中的电源风扇温度传感器	cevSensorASA5555K7PSTempSensor (cevSensor 95)
自适应安全设备 5555 中的电源风扇传感器	cevSensorASA5555PSFanSensor (cevSensor 91)
自适应安全设备 5555 中的电源风扇温度传感器	cevSensorASA5555PSTempSensor (cevSensor 93)
ASA 5585-X 的电源风扇传感器	cevSensorASA5585PSFanSensor (cevSensor 86)
ASA 5585-X 的电源输入传感器	cevSensorASA5585PSInput (cevSensor 85)
ASA 5585 SSP-10 的 CPU 温度传感器	cevSensorASA5585SSp10CPUTemp (cevSensor 77)
无负载加密的 ASA 5585 SSP-10 的 CPU 温度传感器	cevSensorASA5585SSp10K7CPUTemp (cevSensor 78)
ASA 5585 SSP-20 的 CPU 温度传感器	cevSensorASA5585SSp20CPUTemp (cevSensor 79)
无负载加密的 ASA 5585 SSP-20 的 CPU 温度传感器	cevSensorASA5585SSp20K7CPUTemp (cevSensor 80)
ASA 5585 SSP-40 的 CPU 温度传感器	cevSensorASA5585SSp40CPUTemp (cevSensor 81)
无负载加密的 ASA 5585 SSP-40 的 CPU 温度传感器	cevSensorASA5585SSp40K7CPUTemp (cevSensor 82)
ASA 5585 SSP-60 的 CPU 温度传感器	cevSensorASA5585SSp60CPUTemp (cevSensor 83)
无负载加密的 ASA 5585 SSP-60 的 CPU 温度传感器	cevSensorASA5585SSp60K7CPUTemp (cevSensor 84)
自适应安全设备 5555-X 现场可更换固态驱动器	cevModuleASA5555XFRSSD (cevModuleCommonCards 396)
自适应安全设备 5545-X 现场可更换固态驱动器	cevModuleASA5545XFRSSD (cevModuleCommonCards 397)
自适应安全设备 5525-X 现场可更换固态驱动器	cevModuleASA5525XFRSSD (cevModuleCommonCards 398)
自适应安全设备 5515-X 现场可更换固态驱动器	cevModuleASA5515XFRSSD (cevModuleCommonCards 399)
自适应安全设备 5512-X 现场可更换固态驱动器	cevModuleASA5512XFRSSD (cevModuleCommonCards 400)
思科自适应安全虚拟设备	cevChassisASAv (cevChassis 1451)

MIB 中受支持的表和对象

表 40-4 列出指定 MIB 的受支持的表和对象。

表 40-4　MIB 中受支持的表和对象

MIB 名称	受支持的表和对象
CISCO-ENHANCED-MEMPOOL-MIB	cempMemPoolTable、 cempMemPoolIndex、 cempMemPoolType、 cempMemPoolName、 cempMemPoolAlternate、 cempMemPoolValid、 cempMemPoolUsed、 cempMemPoolFree、 cempMemPoolUsedOvrflw、 cempMemPoolHCUsed、 cempMemPoolFreeOvrflw、 cempMemPoolHCFree

表 40-4 MIB 中受支持的表和对象（续）

CISCO-ENTITY-SENSOR-EXT-MIB **注** 在适用于 Catalyst 6500 交换机/7600 路由器的ASA 服务模块上不受支持。	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB **注** 在思科自适应安全虚拟设备 (ASAv) 上不受支持。	ctsxSxpGlobalObjects、 ctsxSxpConnectionObjects、 ctsxSxpSgtObjects
DISMAN-EVENT-MIB	mteTriggerTable、 mteTriggerThresholdTable、 mteObjectsTable、 mteEventTable、 mteEventNotificationTable
DISMAN-EXPRESSION-MIB **注** 在适用于 Catalyst 6500 交换机/7600 路由器的ASA 服务模块上不受支持。	expExpressionTable、 expObjectTable、 expValueTable
ENTITY-SENSOR-MIB **注** 在适用于 Catalyst 6500 交换机/7600 路由器的ASA 服务模块上不受支持。	entPhySensorTable
NAT-MIB	natAddrMapTable、 natAddrMapIndex、 natAddrMapName、 natAddrMapGlobalAddrType、 natAddrMapGlobalAddrFrom、 natAddrMapGlobalAddrTo、 natAddrMapGlobalPortFrom、 natAddrMapGlobalPortTo、 natAddrMapProtocol、 natAddrMapAddrUsed、 natAddrMapRowStatus

受支持的陷阱 （通知）

表 40-5 列出受支持的陷阱 （通知）及其关联 MIB。

表 40-5 受支持的陷阱（通知）

陷阱和 MIB 名称	Varbind 列表	说明
authenticationFailure (SNMPv2-MIB)	-	对于 SNMP 第 1 版或第 2 版， SNMP 请求中提供的社区字符串不正确。对于 SNMP 第 3 版，如果 auth 或 priv 关键字或用户名不正确，则会生成报告 PDU 而不是陷阱。 **snmp-server enable traps snmp authentication** 命令用于启用和禁用这些陷阱的传输。
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)	-	**snmp-server enable traps entity fru-insert** 命令用于启用此通知。
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)	-	**snmp-server enable traps entity fru-remove** 命令用于启用此通知。

表 40-5　　受支持的陷阱（通知）（续）

ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB) **注**　在适用于 Catalyst 6500 交换机/7600 路由器的ASA 服务模块上不受支持。	ceSensorExtThresholdValue、entPhySensorValue、entPhySensorType、entPhysicalName	**snmp-server enable traps entity [power-supply-failure | fan-failure | cpu-temperature]** 命令用于启用实体阈值通知的传输。对于电源故障会发送此通知。所发送的对象会标识风扇和 CPU 温度。 **snmp-server enable traps entity fan-failure** 命令用于启用风扇故障陷阱的传输。 **snmp-server enable traps entity power-supply-failure** 命令用于启用电源故障陷阱的传输。 **snmp-server enable traps entity chassis-fan-failure** 命令用于启用机箱风扇故障陷阱的传输。 **snmp-server enable traps entity cpu-temperature** 命令用于启用高 CPU 温度陷阱的传输。 **snmp-server enable traps entity power-supply-presence** 命令用于启用电源状态故障陷阱的传输。 **snmp-server enable traps entity power-supply-temperature** 命令用于启用电源温度阈值陷阱的传输。 **snmp-server enable traps entity chassis-temperature** 命令用于启用机箱环境温度陷阱的传输。
cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunLifeTime、cipSecTunLifeSize	**snmp-server enable traps ipsec start** 命令用于启用此陷阱的传输。
cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunActiveTime	**snmp-server enable traps ipsec stop** 命令用于启用此陷阱的传输。
ciscoRasTooManySessions (CISCO-REMOTE-ACCESS-MONITOR-MIB)	crasNumSessions、crasNumUsers、crasMaxSessionsSupportable、crasMaxUsersSupportable、crasThrMaxSessions	**snmp-server enable traps remote-access session-threshold-exceeded** 命令用于启用这些陷阱的传输。
clogMessageGenerated (CISCO-SYSLOG-MIB)	clogHistFacility、clogHistSeverity、clogHistMsgName、clogHistMsgText、clogHistTimestamp	系统将生成系统日志消息。 clogMaxSeverity 对象的值用于决定哪些系统日志消息作为陷阱发送。 **snmp-server enable traps syslog** 命令用于启用和禁用这些陷阱的传输。

表 40-5 受支持的陷阱（通知）（续）

clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB)	crlResourceLimitValueType、crlResourceLimitMax、clogOriginIDType、 clogOriginID	**snmp-server enable traps connection-limit-reached** 命令用于启用 connection-limit-reached 通知的传输。clogOriginID 对象包括陷阱源于的情景名称。
coldStart (SNMPv2-MIB)	-	SNMP 代理已启动。 **snmp-server enable traps snmp coldstart** 命令用于启用和禁用这些陷阱的传输。
cpmCPURisingThreshold (CISCO-PROCESS-MIB)	cpmCPURisingThresholdValue、cpmCPUTotalMonIntervalValue、cpmCPUInterruptMonIntervalValue、cpmCPURisingThresholdPeriod、cpmProcessTimeCreated、cpmProcExtUtil5SecRev	**snmp-server enable traps cpu threshold rising** 命令用于启用 cpu threshold rising 通知的传输。 cpmCPURisingThresholdPeriod 对象与其他对象一起发送。
entConfigChange (ENTITY-MIB)	-	**snmp-server enable traps entity config-change fru-insert fru-remove** 命令用于启用此通知。 **注** 仅当创建或移除了安全情景时，才会以多模方式发送此通知。
linkDown (IF-MIB)	ifIndex、 ifAdminStatus、ifOperStatus	接口的链路关闭陷阱。 **snmp-server enable traps snmp linkdown** 命令用于启用和禁用这些陷阱的传输。
linkUp (IF-MIB)	ifIndex、 ifAdminStatus、ifOperStatus	接口的链路开启陷阱。 **snmp-server enable traps snmp linkup** 命令用于启用和禁用这些陷阱的传输。
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger、mteHotTargetName、mteHotContextName、mteHotOID、 mteHotValue、cempMemPoolName、cempMemPoolHCUsed	**snmp-server enable traps memory-threshold** 命令用于启用内存阈值通知。 mteHotOID 设置为 cempMemPoolHCUsed。cempMemPoolName 和 cempMemPoolHCUsed 对象与其他对象一起发送。
mteTriggerFired (DISMAN-EVENT-MIB) **注** 在适用于 Catalyst 6500 交换机/7600 路由器的ASA 服务模块上不受支持。	mteHotTrigger、mteHotTargetName、mteHotContextName、mteHotOID、 mteHotValue、ifHCInOctets、 ifHCOutOctets、ifHighSpeed、 entPhysicalName	**snmp-server enable traps interface-threshold** 命令用于启用接口阈值通知。 entPhysicalName 对象将与其他对象一起发送。

表 40-5 受支持的陷阱（通知）（续）

natPacketDiscard (NAT-MIB)	ifIndex	**snmp-server enable traps nat packet-discard** 命令用于启用 NAT 数据包丢弃通知。此通知会受到时长为 5 分钟的速率限制，并且是在 IP 数据包因映射空间不可用而被 NAT 丢弃的情况下生成。ifIndex 提供映射接口的 ID。
warmStart (SNMPv2-MIB)	-	**snmp-server enable traps snmp warmstart** 命令用于启用和禁用这些陷阱的传输。

接口类型和示例

产生 SNMP 流量统计信息的接口类型包括：

- Logical - 由软件驱动程序收集的统计信息，它是物理统计信息的子集。
- Physical - 由硬件驱动程序收集的统计信息。每个物理指定接口具有一组与其关联的逻辑和物理统计信息。每个物理接口可能具有多个与其关联的 VLAN 接口。 VLAN 接口仅具有逻辑统计信息。

注 对于具有多个与其关联的 VLAN 接口的物理接口，请注意，ifInOctets OID 和 ifOutoctets OID 的 SNMP 计数器与该物理接口的汇聚流量计数器相匹配。

- VLAN 专用- SNMP 使用 ifInOctets 和 ifOutOctets 的逻辑统计信息。

表 40-6 中的示例显示 SNMP 流量统计信息中的差异。示例 1 显示对于 **show interface** 命令和 **show traffic** 命令而言物理与逻辑输出统计信息中的差异。示例 2 显示对于 **show interface** 命令和 **show traffic** 命令而言 VLAN 专用接口的输出统计信息。该示例表明统计信息接近于为 **show traffic** 命令显示的输出。

表 40-6 物理和 VLAN 接口的 SNMP 流量统计信息

示例 1

```
ciscoasa# show interface GigabitEthernet3/2
interface GigabitEthernet3/2
    description fullt-mgmt
    nameif mgmt
    security-level 10
    ip address 10.7.14.201 255.255.255.0
    management-only

ciscoasa# show traffic
(Condensed output)

Physical Statistics
GigabitEthernet3/2:
    received (in 121.760 secs)
        36 packets       3428 bytes
        0 pkts/sec      28 bytes/sec

Logical Statistics
mgmt:
    received (in 117.780 secs)
        36 packets       2780 bytes
        0 pkts/sec      23 bytes/sec
```

以下示例显示管理接口和物理接口的 SNMP 输出统计信息。ifInOctets 值接近于 **show traffic** 命令输出中显示的物理统计信息输出，但不接近于逻辑统计信息输出。

管理接口的 ifIndex：

```
IF_MIB::ifDescr.6 = Adaptive Security Appliance 'mgmt'
interface
```

对应于物理接口统计信息的 ifInOctets：

```
IF-MIB::ifInOctets.6 = Counter32:3246
```

示例 2

```
ciscoasa# show interface GigabitEthernet0/0.100
interface GigabitEthernet0/0.100
    vlan 100
    nameif inside
    security-level 100
    ip address 10.7.1.101 255.255.255.0 standby
    10.7.1.102

ciscoasa# show traffic
inside
    received (in 9921.450 secs)
        1977 packets       126528 bytes
        0 pkts/sec      12 bytes/sec
    transmitted (in 9921.450 secs)
        1978 packets       126556 bytes
        0 pkts/sec      12 bytes/sec
```

VLAN 内部的 ifIndex：

```
IF-MIB::ifDescr.9 = Adaptive Security Appliance
'inside' interface
IF-MIB::ifInOctets.9 = Counter32: 126318
```

SNMP 第 3 版概述

SNMP 第 3 版提供第 1 或 2c 版中没有的安全增强功能。SNMP 第 1 和 2c 版以明文形式在 SNMP 服务器和 SNMP 代理之间传输数据。 SNMP 第 3 版向安全协议操作中添加了身份验证和隐私选项。此外，该版本通过基于用户的安全模型 (USM) 和基于视图的访问控制模型 (VACM) 控制对 SNMP 代理和 MIB 对象的访问。 ASA 和 ASASM 还支持创建 SNMP 组和用户，以及为安全 SNMP 通信启用传输身份验证和加密所需的主机。

安全模型

为进行配置，身份验证和隐私选项会共同组成安全模型。安全模型适用于用户和组，分为以下三种类型：

- NoAuthPriv - 无身份验证且无隐私，意味着未对消息应用安全性。
- AuthNoPriv - 有身份验证但无隐私，意味着消息会进行身份验证。
- AuthPriv - 有身份验证并有隐私，意味着消息会进行身份验证并加密。

SNMP 组

SNMP 组是可以将用户添加到的访问控制策略。每个 SNMP 组配置有安全模型，并与 SNMP 视图关联。SNMP 组内的用户必须与 SNMP 组的安全模型匹配。这些参数指定 SNMP 组内的用户使用的身份验证和隐私类型。每个 SNMP 组名称/安全模型对必须唯一。

SNMP 用户

SNMP 用户具有指定的用户名、用户所属的组、身份验证密码、加密密码，以及要使用的身份验证和加密算法。身份验证算法选项为 MD5 和 SHA。加密算法选项为 DES、3DES 和 AES（在 128、192 和 256 版中可用）。创建用户时，必须将其与 SNMP 组相关联。然后，用户将继承该组的安全模型。

SNMP 主机

SNMP 主机是 SNMP 通知和陷阱发送到的 IP 地址。如要配置 SNMP 第 3 版主机及目标 IP 地址，必须配置用户名，因为陷阱仅发送到已配置的用户。 SNMP 目标 IP 地址和目标参数名称在 ASA 和 ASA 服务模块上必须唯一。每个 SNMP 主机只能具有一个与其关联的用户名。如要接收 SNMP 陷阱，请在添加 **snmp-server host** 命令后，确保将 NMS 上的用户凭证配置为与 ASA 和 ASASM的凭证相匹配。

ASA、 ASA 服务模块和思科 IOS 软件之间的实施差异

ASA 和 ASASM 中的 SNMP 第 3 版实施在以下方面不同于思科 IOS 软件中的 SNMP 第 3 版实施：

- 本地引擎和远程引擎 ID 不可配置。本地引擎 ID 是在 ASA 或ASASM启动时或者创建了情景时生成。
- 不支持基于视图的访问控制，导致 MIB 浏览不受限制。
- 支持限于以下 MIB：USM、 VACM、 FRAMEWORK 和 TARGET。
- 必须使用正确的安全模型创建用户和组。
- 必须按正确的顺序移除用户、组和主机。
- 使用 **snmp - server host** 命令创建 ASA、 ASAv 或 ASASM 规则以允许传入 SNMP 流量。

SNMP 系统日志消息传递

SNMP 生成编号为 212*nnn* 的详细系统日志消息。系统日志消息向指定接口上的指定主机表明 SNMP 请求、 SNMP 陷阱、 SNMP 信道和来自 ASA 或 ASASM 的 SNMP 响应的状态。

有关系统日志消息的详细信息，请参阅系统日志消息指南。

注　如果 SNMP 系统日志消息超过较高的速率 （约 4000 条/秒），则 SNMP 轮询将失败。

应用服务和第三方工具

有关 SNMP 支持的信息，请参阅以下 URL：

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

有关使用第三方工具处理 SNMP 第 3 版 MIB 的信息，请参阅以下 URL：

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP 准则

故障转移准则

每个 ASA、 ASAv 或 ASASM 中的 SNMP 客户端与其对等体共享引擎数据。引擎数据包括 SNMP-FRAMEWORK-MIB 的 engineID、 engineBoots 和 engineTime 对象。引擎数据作为二进制文件写入到 flash:/snmp/*contextname*。

IPv6 准则

不支持 IPv6。

其他指导原则

- 您必须具有 Cisco Works for Windows 或其他 SNMP MIB-II 兼容浏览器才能接收 SNMP 陷阱或浏览 MIB。
- 不支持基于视图的访问控制，但是 VACM MIB 可供浏览来确定默认视图设置。
- ENTITY-MIB 在非管理情景中不可用。在非管理情景中改用 IF-MIB 执行查询。
- 对于 AIP SSM 或 AIP SSC 不支持 SNMP 第 3 版。
- 不支持 SNMP 调试。
- 不支持 ARP 信息检索。
- 不支持 SNMP SET 命令。
- 使用 NET-SNMP 第 5.4.2.1 版时，仅支持 AES128 加密算法版本。不支持 AES256 或 AES192 加密算法版本。
- 如果结果导致 SNMP 处于不一致状态，则会对现有配置进行更改。
- 对于 SNMP 第 3 版，必须按以下顺序进行配置：组、用户、主机。
- 在删除组之前，必须确保删除与该组关联的所有用户。
- 在删除用户之前，必须确保未配置与该用户名关联的主机。
- 如果已使用特定安全模型将用户配置为属于特定组，并且，如果该组的安全级别进行了更改，则必须按此顺序执行以下操作：
  - 从该组中移除用户。
  - 更改组安全级别。
  - 添加属于新组的用户。
- 不支持创建自定义视图来限制对 MIB 对象子集的用户访问。
- 所有的请求和陷阱只能在默认的 Read/Notify View 中获取。
- 在管理情景中生成 connection-limit-reached 陷阱。要生成此陷阱，必须在已达到连接限制的用户情景中配置至少一个 SNMP 服务器主机。
- 不能在 ASA 5585 SSP-40 (NPE) 上查询机箱温度。
- 最多可以添加 4000 台主机。不过，其中仅 128 台可用于陷阱。
- 支持的活动轮询目标总数为 128。
- 可以指定网络对象来表示要添加为主机组的单个主机。

- 可以将多个用户与一台主机关联。
- 可以在不同的 **host-group** 命令中指定重叠网络对象。为最后一个主机组指定的值对于不同网络对象中的公用主机集合生效。
- 如果删除主机组或与其他主机组重叠的主机，则会使用所配置的主机组中已指定的值再次设置主机。
- 主机获取的值取决于用于运行命令的指定序列。
- SNMP 发送的消息大小的限制为 1472 字节。
- 集群成员不同步其 SNMPv3 引擎 ID。因此，集群中的每个设备应具有唯一的 SNMPv3 用户配置。

故障排除提示

- 如要确保接收来自 NMS 的传入数据包的 SNMP 进程在运行，请输入以下命令：

```
ciscoasa(config)# show process | grep snmp
```

- 如要捕获来自 SNMP 的系统日志消息并将其显示在 ASA、 ASAv、或 ASASM 控制台上，请输入以下命令：

```
ciscoasa(config)# logging list snmp message 212001-212015
ciscoasa(config)# logging console snmp
```

- 如要确保 SNMP 进程正在发送和接收数据包，请输入以下命令：

```
ciscoasa(config)# clear snmp-server statistics
ciscoasa(config)# show snmp-server statistics
```

  输出基于 SNMPv2-MIB 的 SNMP 组。

- 如要确保 SNMP 数据包通过 ASA、ASAv、或 ASASM 并指向 SNMP 进程，请输入以下命令：

```
ciscoasa(config)# clear asp drop
ciscoasa(config)# show asp drop
```

- 如果 NMS 无法成功请求对象或者未在正确处理来自 ASA、 ASAv、或 ASASM 的传入陷阱，请使用数据包捕获确定问题，方法是输入以下命令：

```
ciscoasa (config)# access-list snmp permit udp any eq snmptrap any
ciscoasa (config)# access-list snmp permit udp any any eq snmp
ciscoasa (config)# capture snmp type raw-data access-list snmp interface mgmt
ciscoasa (config)# copy /pcap capture:snmp tftp://192.0.2.5/exampledir/snmp.pcap
```

- 如果 ASA、ASAv、或 ASASM 不是按预期执行，请通过执行以下操作来获取有关网络拓扑和流量的信息：
  - 对于 NMS 配置，请获取以下信息：

    超时次数

    重试计数

    引擎 ID 缓存

    使用的用户名和密码
  - 发出以下命令：

    show block

    show interface

    show process

    show cpu

show vm

- 如果发生严重错误，要帮助重现错误，请将回溯文件和 **show tech-support** 命令的输出发送到思科 TAC。
- 如果不允许 SNMP 流量通过 ASA、ASAv、或 ASASM 接口，可能还需要使用 **icmp permit** 命令允许来自远程 SNMP 服务器的 ICMP 流量。

配置 SNMP

本节描述如何配置 SNMP。

步骤 1 启用 SNMP 代理和 SNMP 服务器。请参阅第 40-18 页的启用 SNMP 代理和 SNMP 服务器。

步骤 2 配置 SNMP 陷阱。请参阅第 40-18 页的配置 SNMP 陷阱。

步骤 3 配置 SNMP 第 1 和 2c 版参数或 SNMP 第 3 版参数。请参阅第 40-20 页的配置 SNMP 第 1 或 2c 版的参数或第 40-21 页的配置 SNMP 第 3 版的参数。

启用 SNMP 代理和 SNMP 服务器

如要启用 SNMP 代理和 SNMP 服务器，请执行以下步骤：

操作步骤

步骤 1 在 ASA、ASAv 或 ASASM 上启用 SNMP 代理和 SNMP 服务器。默认情况下，已启用 SNMP 服务器。

snmp-server enable

示例：

```
ciscoasa(config)# snmp-server enable
```

配置 SNMP 陷阱

如要指定 SNMP 代理生成哪些陷阱以及如何将其收集并发送到 NMS，请执行以下步骤：

操作步骤

步骤 1 将单个陷阱、陷阱集合或所有陷阱发送到 NMS。

snmp-server enable traps [**all** | **syslog** | **snmp** [*authentication* | *linkup* | *linkdown* | *coldstart* | *warmstart*] | | **entity** [*config-change* | *fru-insert* | *fru-remove* | *fan-failure* | *cpu-temperature* | *chassis-fan- failure* | *power-supply-failure*] | *chassis-temperature* | *power-supply-presence* | *power-supply-temperature* |] | **ikev2** [*start* | *stop*] |**ipsec** [*start* | *stop*] | **remote-access** [*session-threshold-exceeded*]| **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [*packet-discard*]

示例：

```
ciscoasa(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart
warmstart
```

通过此命令可以将系统日志消息作为陷阱发送到 NMS。默认配置已启用所有 SNMP 标准陷阱，如示例所示。如要禁用这些陷阱，请使用 **no snmp-server enable traps snmp** 命令。如果输入此命令而不指定陷阱类型，则默认为**系统日志**陷阱。默认情况下，会启用**系统日志**陷阱。默认 SNMP 陷阱随**系统日志**陷阱继续启用。需要同时配置 **logging history** 命令和 **snmp-server enable traps syslog** 命令来从系统日志 MIB 生成陷阱。如要还原 SNMP 陷阱的默认启用，请使用 **clear configure snmp-server** 命令。默认情况下会禁用所有其他陷阱。

仅在管理情景中可用的陷阱：

- **connection-limit-reached**
- **entity**
- **memory-threshold**

仅通过管理情景为系统情景中物理连接的接口生成的陷阱：

- **interface-threshold**

注　在适用于 Catalyst 6500 交换机/7600 路由器的ASA 服务模块上不支持 **interface-threshold** 陷阱。

在单一模式中所有其他陷阱在管理情景和用户环境中都可用。

在多情景模式中，仅从管理情景而不从用户情景生成 **fan-failure** 陷阱、 **power-supply-failure** 陷阱和 **cpu-temperature** 陷阱 （适用于 ASA 5512-X、 5515-X、 5525-X、 5545-X 和 5555-X）。

如果 CPU 使用率大于所配置监控期的所配置阈值，则会生成 **cpu threshold rising** 陷阱。

当已用系统情景内存达到总系统内存的 80% 时，会从管理情景中生成 **memory-threshold** 陷阱。对于所有其他用户情景，当在该特定情景中已用内存达到总系统内存的 80% 时会生成此陷阱。

注　SNMP 不监控电压传感器。

配置 CPU 使用率阈值

如要配置 CPU 使用率阈值，请执行以下步骤：

操作步骤

步骤 1　为高 CPU 阈值和阈值监控期配置阈值。

snmp cpu threshold rising *threshold_value monitoring_period*

示例：

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```

如要清除 CPU 利用率的阈值和监控期，请使用 **no** 形式的此命令。如果未配置 **snmp cpu threshold rising** 命令，则高阈值级别的默认值超过 70%，临界阈值级别的默认值超过 95%。默认监控期设置为 1 分钟。

您无法配置临界 CPU 阈值级别，该值维持在恒定 95%。高 CPU 阈值的有效阈值范围为 10% 至 94%。监控期的有效值范围为 1 至 60 分钟。

配置物理接口阀值

如要配置物理接口阈值，请执行以下步骤：

操作步骤

步骤 1 配置 SNMP 物理接口的阀值。

snmp interface threshold *threshold_value*

示例：

```
ciscoasa(config)# snmp interface threshold 75%
```

如要清除 SNMP 物理接口的阈值，请使用 **no** 形式的此命令。阈值定义为接口带宽利用率的百分比。有效阈值范围为 30% 至 99%。默认值为 70%。

snmp interface threshold 命令仅在管理情景中可用。

物理接口使用情况在单模和多模下受到监控，系统情景中物理接口的陷阱通过管理情景发送。仅物理接口用于计算阈值使用情况。

注 在适用于 Catalyst 6500 交换机/7600 路由器的ASA 服务模块上不支持此命令。

配置 SNMP 第 1 或 2c 版的参数

如要配置 SNMP 第 1 或 2c 版的参数，请执行以下步骤：

操作步骤

步骤 1 指定 SNMP 通知的收件人，指示从其发送陷阱的接口以及标识可以陷阱发送的接口，并确定可以连接到 ASA 的 NMS 或 SNMP 管理器的名称和 IP 地址。

snmp-server host {*interface hostname* | *ip_address*} [**trap** | **poll**] [**community** *community-string*] [**version** {***1*** | **2c** *username*}] [**udp-port** *port*]

示例：

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 2

ciscoasa(config)# snmp-server host corp 172.18.154.159 community public
```

trap 关键字将 NMS 限制为仅接收陷阱。**poll** 关键字将 NMS 限制为仅发送请求（轮询）。默认情况下，会启用 SNMP 陷阱。默认情况下，UDP 端口为 162。社区字符串是 ASA、ASAv 或 ASASM 与 NMS 之间的共享密钥。密钥是一个区分大小写的值，长度最多为 32 个字母数字字符。不允许使用空格。默认社区字符串为 public。ASA 使用此密钥确定传入 SNMP 请求是否有效。例如，可以使用某社区字符串来指定站点，然后使用同一字符串配置 ASA 和管理站。ASA、ASAv 和 ASASM 使用

指定的字符串，并且不会对包含无效社区字符串的请求作出响应。使用加密社区字符串后，仅加密形式对于所有系统（例如，CLI、ASDM、CSM 等）可见。明文密码不可见。加密社区字符串始终由 ASA 生成；通常输入明文形式。

注　如果从 8.3(1) 版降级到 ASA 软件的更低版本并已配置加密密码，则必须先使用 **no key config-key password encryption** 命令将加密密码还原为明文，然后保存结果。

如要在添加 **snmp-server host** 命令后接收陷阱，请确保使用与 ASA、 ASAv 和 ASASM 上配置的凭证相同的凭证来配置 NMS 上的用户。

步骤 2　设置*仅*供与 SNMP 第 1 或 2c 版配合使用的社区字符串。

snmp-server community *community-string*

示例：

```
ciscoasa(config)# snmp-server community onceuponatime
```

步骤 3　设置 SNMP 服务器位置或联系人信息。

snmp-server [**contact** | **location**] *text*

示例：

```
ciscoasa(config)# snmp-server location building 42

ciscoasa(config)# snmp-server contact EmployeeA
```

text 参数指定联系人或 ASA 系统管理员的名称。名称区分大小写，并且最多可以为 127 个字符。接受空格，但是多个空格会缩短为单个空格。

步骤 4　设置 SNMP 请求的侦听端口。

snmp-server listen-port *lport*

示例：

```
ciscoasa(config)# snmp-server lport 192
```

lport 参数是接受传入请求的端口。默认侦听端口为 161。**snmp-server listen-port** 命令仅在管理情景中可用，在系统情景中不可用。如果在当前在使用中的端口上配置 **snmp-server listen-port** 命令，则将显示以下消息：

警告　**UDP 端口 *port* 在由其他功能使用。对设备的 SNMP 请求将失败，直到 snmp-server listen-port 命令配置为使用其他端口为止。**

现有 SNMP 线程继续每 60 秒进行轮询，直到端口可用为止，如果端口仍在使用中，则会发出系统日志消息 %ASA-1-212001。

配置 SNMP 第 3 版的参数

如要配置 SNMP 第 3 版的参数，请执行以下步骤：

操作步骤

步骤 1　指定*仅*供与 SNMP 第 3 版配合使用的新 SNMP 组。

snmp-server group *group-name* **v3** [**auth** | **noauth** | **priv**]

示例：

```
ciscoasa(config)# snmp-server group testgroup1 v3 auth
```

配置社区字符串后，会自动生成具有与社区字符串相匹配的名称的另外两个组：一个表示第 1 版的安全模型，一个表示第 2 版的安全模型。有关安全模型的详细信息，请参阅第 40-14 页的安全模型。 **auth** 关键字启用数据包身份验证。 **noauth** 关键字表示未在使用数据包身份验证或加密。 **priv** 关键字启用数据包加密和身份验证。对于 **auth** 或 **priv** 关键字不存在默认值。

步骤 2 为仅供与 SNMP 第 3 版配合使用的 SNMP 组配置新用户。

snmp-server user *username group-name* {**v3** [**encrypted**]] [**auth** {**md5** | **sha**]} *auth-password* [**priv**] [**des** | **3des** | **aes**] [**128** | **192** | **256**] *priv-password*

示例：

```
ciscoasa(config)# snmp-server user testuser1 testgroup1 v3 auth md5 testpassword aes 128
mypassword

ciscoasa(config)# snmp-server user testuser1 public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

username 参数是属于 SNMP 代理的主机上用户的名称。 *group-name* 参数是用户所属的组的名称。**v3** 关键字指定应该使用 SNMP 第 3 版安全模型并允许使用 **encrypted**、**priv** 和 **auth** 关键字。**encrypted** 关键字指定加密格式的密码。加密密码必须为十六进制格式。 **auth** 关键字指定应使用的身份验证级别 （**md5** 或 **sha**）。 **priv** 关键字指定加密级别。不存在 **auth** 或 **priv** 关键字或默认关键字的默认值。对于加密算法，可以指定 **des**、 **3des** 或 **aes** 关键字。您还可以指定要使用的 AES 加密算法版本：**128**、 **192** 或 **256**。 *auth-password* 参数指定身份验证用户密码。*priv-password* 参数指定加密用户密码。

注 如果忘记密码，则无法将其恢复，必须重新配置用户。可以指定纯文本密码或本地化摘要。本地化摘要必须与为用户选择的身份验证算法 （可以为 MD5 或 SHA）相匹配。当用户配置显示在控制台上或写入到文件 （例如，启动配置文件）时，始终显示本地化身份验证和隐私摘要而非纯文本密码 （请参阅第二个示例）。密码的最小长度为 1 个字母数字字符；但是，出于安全原因，建议使用至少 8 个字母数字字符。

在集群中，必须使用 SNMPv3 用户手动更新每个集群式 ASA。可以通过在主设备上输入 **snmp-server user** *username group-name* **v3** 命令来执行此操作，其中 *priv-password* 选项和 *auth-password* 选项采用其非本地化形式。

系统将显示一条错误消息，通知您在集群复制或配置期间将不会复制 SNMPv3 用户命令。然后，可以独立在从属 ASA 上配置 SNMPv3 用户和组命令。这也意味着在复制期间未清除现有 SNMPv3 用户和组命令，并且，可以在集群中的所有从属设备上输入 SNMPv3 用户和组命令。例如：

在使用随同已经本地化的密钥输入的命令的主设备上：

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a priv aes 256
cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:f6:86:cf:18:c0:f0:47:d6:94:e5:
da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

在集群复制期间的从属设备上 （仅在配置中存在 **snmp-server user** 命令的情况下才会显示）：

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

步骤 3　指定 SNMP 通知的接收方。指示从其发送陷阱的接口。标识可以连接到 ASA 的 NMS 或 SNMP 管理器的名称和 IP 地址。

snmp-server host *interface* {*hostname* | *ip_address*} [**trap** | **poll**] [**community** *community-string*] [**version** {***1*** | **2c** | ***3*** *username*}] [**udp-port** *port*]

示例：

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1

ciscoasa(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2
```

trap 关键字将 NMS 限制为仅接收陷阱。**poll** 关键字将 NMS 限制为仅发送请求（轮询）。默认情况下，会启用 SNMP 陷阱。默认情况下，UDP 端口为 162。社区字符串是 ASA 与 NMS 之间的共享密钥。密钥是一个区分大小写的值，最多为 32 个字母数字字符。不允许使用空格。默认社区字符串为 public。ASA、ASAv 和 ASASM 使用此密钥确定传入 SNMP 请求是否有效。例如，可以使用某社区字符串来指定站点，然后使用同一字符串配置 ASA、ASAv 或 ASASM 和 NMS。ASA、ASAv 和 ASASM 使用指定的字符串，并且不会对包含无效社区字符串的请求作出响应。使用加密社区字符串后，仅加密形式对于所有系统（例如，CLI、ASDM、CSM 等）可见。明文密码不可见。加密社区字符串始终由 ASA 生成；通常输入明文形式。

注　如果从 8.3(1) 版降级到 ASA 软件的更低版本并已配置加密密码，则必须先使用 **no key config-key password encryption** 命令将加密密码还原为明文，然后保存结果。

version 关键字指定 SNMP 陷阱版本。 ASA 不支持根据 SNMP 请求 （轮询）进行过滤。

在 ASA、 ASAv 和 ASASM 上配置 SNMP 第 3 版主机时，用户必须与该主机关联。

要在添加 **snmp-server host** 命令后接收陷阱，请确保使用与 ASA、 ASAv 或 ASASM 上配置的凭证相同的凭证来配置 NMS 上的用户。有关 SNMP 主机的详细信息，请参阅第 40-15 页的 SNMP 主机。

步骤 4　设置 SNMP 服务器位置或联系人信息。

snmp-server [**contact** | **location**] *text*

示例：

```
ciscoasa(config)# snmp-server location building 42

ciscoasa(config)# snmp-server contact EmployeeA
```

text 参数指定联系人或 ASA 系统管理员的名称。名称区分大小写，并且最多可以为 127 个字符。接受空格，但是多个空格会缩短为单个空格。

步骤 5　设置 SNMP 请求的侦听端口。

snmp-server listen-port *lport*

示例：

```
ciscoasa(config)# snmp-server lport 192
```

lport 参数是接受传入请求的端口。默认侦听端口为 161。**snmp-server listen-port** 命令仅在管理情景中可用，在系统情景中不可用。如果在当前在使用中的端口上配置 **snmp-server listen-port** 命令，则将显示以下消息：

警告　**UDP 端口 *port* 在由其他功能使用。对设备的 SNMP 请求将失败，直到 snmp-server listen-port 命令配置为使用其他端口为止。**

现有 SNMP 线程继续每 60 秒进行轮询，直到端口可用为止，如果端口仍在使用中，则会发出系统日志消息 %ASA-1-212001。

配置用户组

如要配置其中含有一组指定用户的 SNMP 用户列表，请执行以下步骤：

操作步骤

步骤 1 配置 SNMP 用户列表。

snmp-server user-list *list_name* **username** *user_name*

示例：

```
ciscoasa(config)# snmp-server user-list engineering username user1
```

listname 参数指定用户列表的名称，长度可以为最多 33 个字符。 **username** *user_name* 关键字/参数对指定在用户列表中可能配置的用户。使用 **snmp-server user** *username* 命令配置用户列表中的用户，仅在使用的是 SNMP 第 3 版的情况下该命令才可用。用户列表必须包含多个用户，并且可与主机名或 IP 地址范围关联。

将用户与网络对象相关联

如要将用户列表中的单个用户或用户组与网络对象相关联，请执行以下步骤：

操作步骤

步骤 1 将用户列表中的单个用户或用户组与网络对象相关联。

snmp-server host-group *net_obj_name* [**trap** | **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}] [**udp-port** *port*]

示例：

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1

ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c

ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1

ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

net_obj_name 参数指定用户或用户组与之关联的接口网络对象名称。 **trap** 关键字指定只能发送陷阱，并且不允许此主机浏览 （轮询）。 **poll** 关键字指定允许主机浏览 （轮询），但是不能发送陷阱。**community** 关键字指定对于来自 NMS 的请求或者在生成发送到 NMS 的陷阱时需要非默认字符串。只能将此关键字用于 SNMP 第 1 或 2c 版。*community-string* 参数指定随通知发送或在来自 NMS 的请求中发送的类似于密码的社区字符串。社区字符串可以有最多 32 个字符。 **version** 关键字将 SNMP 通知版本设置为要用于发送陷阱的第 1、2c 或 3 版。*username* 参数指定使用的是 SNMP 第 3

版的情况下的用户的名称。**user-list** *list_name* 关键字/参数对指定用户列表的名称。**udp-port** *port* 关键字/参数对指定必须将 SNMP 陷阱发送到非默认端口上的 NMS 主机并设置该 NMS 主机的 UDP 端口号。默认 UDP 端口为 162。默认版本为 1。默认情况下会启用 SNMP 陷阱。

监控 SNMP

有关监控 SNMP 的信息，请参阅以下命令。

- **show running-config snmp-server** [**default**]

  此命令显示所有 SNMP 服务器配置信息。

- **show running-config snmp-server group**

  此命令显示 SNMP 组配置设置。

- **show running-config snmp-server host**

  此命令显示供 SNMP 用于控制发送到远程主机的消息和通知的配置设置。

- **show running-config snmp-server host-group**

  此命令显示 SNMP 主机组配置。

- **show running-config snmp-server user**

  此命令显示 SNMP 基于用户的配置设置。

- **show running-config snmp-server user-list**

  此命令显示 SNMP 用户列表配置。

- **show snmp-server engineid**

  此命令显示所配置的 SNMP 引擎的 ID。

- **show snmp-server group**

  此命令显示已配置的 SNMP 组的名称。如果已经配置社区字符串，则默认情况下在输出中会显示两个额外的组。此行为是正常的。

- **show snmp-server statistics**

  此命令显示已配置的 SNMP 服务器特性。如要将所有 SNMP 计数器重置为零，请使用 **clear snmp-server statistics** 命令。

- **show snmp-server user**

  此命令已配置的用户特性。

示例

以下示例说明如何显示 SNMP 服务器统计信息。

```
ciscoasa(config)# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
```

```
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

以下示例说明如何显示 SNMP 服务器运行配置：

```
ciscoasa(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

SNMP 第 1 和 2c 版示例

以下示例显示 ASA 如何能够接收来自内部接口上的主机 192.0.2.5 的 SNMP 请求，但是不向任何主机发送任何 SNMP 系统日志请求：

```
ciscoasa(config)# snmp-server host 192.0.2.5
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
ciscoasa(config)# snmp-server community ohwhatakeyisthee
```

SNMP 第 3 版示例

以下示例显示 ASA 如何能够使用 SNMP 第 3 版安全模型接收 SNMP 请求，该安全模型要求配置遵循此特定顺序：组，后跟用户，后跟主机：

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

SNMP 历史记录

表 40-7　　SNMP 历史记录

功能名称	平台版本	说明
SNMP 第 1 和 2c 版	7.0(1)	通过明文社区字符串在 SNMP 服务器与 SNMP 代理之间传输数据来提供 ASA、ASAv 和 ASASM 网络监控及事件信息。
SNMP 第 3 版	8.2(1)	为最安全形式的受支持安全模型 SNMP 第 3 版提供 3DES 或 AES 加密和支持。通过使用 USM，此版本允许配置用户、组和主机以及身份验证特性。此外，该版本还允许对代理和 MIB 对象进行访问控制，并且包含其他 MIB 支持。 我们引入或修改了以下命令：**show snmp-server engineid**、 **show snmp-server group**、 **show snmp-server user**、 **snmp-server group**、 **snmp-server user**、 **snmp-server host**。
密码加密	8.3(1)	支持密码加密。 我们修改了以下命令：**snmp-server community** 和 **snmp-server host**。
SNMP 陷阱和 MIB	8.4(1)	支持以下其他关键字：**connection-limit-reached**、**cpu threshold rising**、**entity cpu-temperature**、**entity fan-failure**、**entity power-supply**、**ikev2 stop | start**、**interface-threshold**、 **memory-threshold**、 **nat packet-discard**、 **warmstart**。 entPhysicalTable 报告传感器、风扇、电源和相关组件的条目。 支持以下其他 MIB：CISCO-ENTITY-SENSOR-EXT-MIB、CISCO-ENTITY-FRU-CONTROL-MIB、 CISCO-PROCESS-MIB、CISCO-ENHANCED-MEMPOOL-MIB、CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB、 DISMAN-EVENT-MIB、DISMAN-EXPRESSION-MIB、 ENTITY-SENSOR-MIB、 NAT-MIB。 支持以下其他陷阱：ceSensorExtThresholdNotification、clrResourceLimitReached、 cpmCPURisingThreshold、 mteTriggerFired、natPacketDiscard、 warmStart。 我们引入或修改了以下命令：**snmp cpu threshold rising**、 **snmp interface threshold**、 **snmp-server enable traps**。
IF-MIB ifAlias OID 支持	8.2(5)/8.4(2)	ASA 现在支持 ifAlias OID。浏览 IF-MIB 时，ifAlias OID 将设置为已为接口描述设置的值。
ASA 服务模块 (ASASM)	8.5(1)	ASASM 支持 8.4(1) 中存在的所有 MIB 和陷阱，但以下除外： 8.5(1) 中不受支持的 MIB： • CISCO-ENTITY-SENSOR-EXT-MIB（仅支持 entPhySensorTable 组下的对象）。 • ENTITY-SENSOR-MIB（仅支持 entPhySensorTable 组中的对象）。 • DISMAN-EXPRESSION-MIB（仅支持 expExpressionTable、expObjectTable 和 expValueTable 组中的对象）。 8.5(1) 中不受支持的陷阱： • ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)。此陷阱仅用于电源故障、风扇故障和高 CPU 温度事件。 • InterfacesBandwidthUtilization.

表 40-7 SNMP 历史记录（续）

功能名称	平台版本	说明
SNMP 陷阱	8.6(1)	支持 ASA 5512-X、 5515-X, 5525-X、 5545-X 和 5555-X 的以下其他关键字：**entity power-supply-presence**、 **entity power-supply-failure**、 **entity chassis-temperature**、 **entity chassis-fan-failure**、 **entity power-supply-temperature**。 我们修改了以下命令：**snmp-server enable traps**。
VPN 相关 MIB	9.0(1)	已实施更新版本的 CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB 来支持下一代加密功能。 已为 ASASM 启用下列 MIB： • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	添加了对以下 MIB 的支持：CISCO-TRUSTSEC-SXP-MIB。
SNMP OID	9.1(1)	已添加五个新的 SNMP 物理供应商类型 OID 来支持 ASA 5512-X、 5515-X、 5525-X、 5545-X 和 5555-X。
NAT MIB	9.1(2)	添加了 cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 来支持 xlate_count 和 max_xlate_count 条目，相当于允许使用 **show xlate count** 命令进行轮询。
SNMP 主机、主机组和用户列表	9.1(5)	现在最多可以添加 4000 台主机。支持的活动轮询目标数为 128。可以指定网络对象来表示要添加为主机组的单个主机。可以将多个用户与一台主机关联。 我们引入或修改了以下命令：**snmp-server host-group**、 **snmp-server user-list**、 **show running-config snmp-server**、 **clear configure snmp-server**。
SNMP 消息大小	9.2(1)	SNMP 发送的消息大小限制已增大为 1472 字节。
SNMP OID 和 MIB		ASA 现在支持 cpmCPUTotal5minRev OID。 ASAv 已作为新产品添加到 SNMP sysObjectID OID 和 entPhysicalVendorType OID 中。 CISCO-PRODUCTS-MIB 和 CISCO-ENTITY-VENDORTYPE-OID-MIB 已更新为支持新的 ASAv 平台。 已添加用于监控 VPN 共享许可证使用情况的新 SNMP MIB。

表 40-7 SNMP 历史记录（续）

功能名称	平台版本	说明
SNMP OID 和 MIB	9.3(1)	已为 ASASM 添加 CISCO-REMOTE-ACCESS-MONITOR-MIB (OID 1.3.6.1.4.1.9.9.392) 支持。
SNMP MIB 和陷阱	9.3(2)	CISCO-PRODUCTS-MIB 和 CISCO-ENTITY-VENDORTYPE-OID-MIB 已更新为支持新的 ASA 5506-X、 ASA 5506W-X 和 ASA 5508-X。 ASA 5506-X 和 ASA 5508-X 已作为新产品添加到 SNMP sysObjectID OID 和 entPhysicalVendorType OID 表中。 现在，ASA 支持 CISCO-CONFIG-MAN-MIB，这使您可以执行以下操作： • 了解已为特定配置输入了哪些命令。 • 在运行配置发生更改后通知 NMS。 • 跟踪与上一次更改或保存运行配置相关的时间戳。 • 跟踪命令的其他更改，例如，终端详细信息和命令源。 我们修改了以下命令：**snmp-server enable traps**。

Anonymous Reporting 和 Smart Call Home

本章介绍如何配置 Anonymous Reporting 和 Smart Call Home 服务。

- 第 41-1 页的关于 Anonymous Reporting
- 第 41-2 页的关于 Smart Call Home
- 第 41-6 页的 Anonymous Reporting 和 Smart Call Home 指南
- 第 41-7 页的配置 Anonymous Reporting 和 Smart Call Home
- 第 41-16 页的监控 Anonymous Reporting 和 Smart Call Home
- 第 41-17 页的 Smart Call Home 的示例 (CLI)
- 第 41-18 页的 Anonymous Reporting 和 Smart Call Home 的历史

关于 Anonymous Reporting

您可以通过启用 Anonymous Reporting 服务来帮助改进思科 ASA 平台，此服务使思科能够安全地接收来自设备的最少量错误和运行状况信息。启用此功能后，客户身份将保持匿名，而不会发送任何识别信息。

启用 Anonymous Reporting 将会创建信任点并安装证书。 ASA 需要 CA 证书以验证 Smart Call Home 网络服务器上存在的服务器证书并构造 HTTPS 会话，以使 ASA 能够安全地发送消息。思科将导入软件中预定义的证书。如果您决定启用 Anonymous Reporting，则 ASA 上将会安装一个证书，其硬编码的信任点名称为 _SmartCallHome_ServerCA。当您启用 Anonymous Reporting 时，系统将会创建此信任点，安装相应的证书，并且您将接收到有关此操作的消息。然后，该证书将出现在您的配置中。

如果启用 Anonymous Reporting 时相应的证书已存在于配置中，则不会创建信任点，并且不会安装任何证书。

注 启用 Anonymous Reporting 即表示您同意将指定的数据传输至思科或代表思科运营的供应商 （包括美国以外的国家/地区）。
思科将保护所有客户的隐私。有关思科对个人信息的处置的详细信息，请参阅以下 URL 中提供的思科隐私声明：
http://www.cisco.com/web/siteassets/legal/privacy.html

DNS 需求

必须正确配置 DNS 服务器，ASA 才能访问思科 Smart Call Home 服务器并向思科发送消息。由于 ASA 可能位于专用网络中，而未接入公用网络，因此思科将验证 DNS 配置，并在必要时通过执行下列任务来配置 DNS：

1. 为所有已配置的 DNS 服务器执行 DNS 查找。
2. 通过在最高安全级别的接口上发送 DHCPINFORM 消息，从 DHCP 服务器获取 DNS 服务器。
3. 使用思科 DNS 服务器进行查找。
4. 将静态 IP 地址随机用于 tools.cisco.com。

执行这些任务并不会更改当前配置。（例如，从 DHCP 获取的 DNS 服务器不会添加到配置中。）

如果未配置任何 DNS 服务器，并且 ASA 无法访问 Cisco Smart Call Home 服务器，则对于发送的每条 Smart Call Home 消息，思科都将生成一条严重性级别为“警告”的系统日志消息，以提醒您正确配置 DNS。

有关系统日志消息的详细信息，请参阅系统日志消息指南。

关于 Smart Call Home

对 Smart Call Home 服务进行全面配置后，此服务可以检测到站点中的问题，并且通常在您知道这些问题存在之前，向思科报告这些问题或者通过用户定义的其他渠道进行报告 （例如通过邮件报告或者直接向您报告）。根据这些问题的严重性，思科将通过提供下列服务，对您的系统配置问题、产品寿命终止声明以及安全公告问题等等作出回应：

- 通过持续进行监控、发出实时的主动警报以及进行详细诊断，迅速确定问题。
- 通过 Smart Call Home 通知使您知晓潜在的问题，在这些通知中，已提交服务请求，并随附了所有诊断数据。
- 自动直接联系思科 TAC 专家，更迅速地解决紧急问题。
- 缩短故障排除时间，从而更高效地利用员工资源。
- 自动生成发往思科 TAC 的服务请求 （如果您签订了服务合同），这些请求将发送给适当的支持团队，该支持团队将提供可以加快解决问题的详细诊断信息。

您可以通过 Smart Call Home 门户快速访问使您能够执行下列活动的必需信息：

- 在一个位置查看所有 Smart Call Home 消息、诊断信息和建议。
- 检查服务请求状态。
- 查看所有已启用 Smart Call Home 的设备的最新清单和配置信息。

订用警报组

警报组是 ASA 上支持的 Smart Call Home 警报的预定义子集。各种类型的 Smart Call Home 警报根据其类型分组到不同的警报组中。每个警报组都报告特定 CLI 的输出。受支持的 Smart Call Home 警报组如下所示：

- 系统日志
- 诊断
- 环境

- 清单
- 配置
- 威胁
- 快照
- 遥测
- 测试

警报组的属性

警报组具有下列属性：

- 事件首先向一个警报组注册。
- 一个组可以与多个事件相关联。
- 您可以订用特定警报组。
- 您可以启用和禁用特定警报组。对所有警报组都启用了默认设置。
- 诊断和环境警报组支持订用周期性消息。
- 系统日志警报组支持基于消息 ID 的订用。
- 对于环境警报组，您可以配置 CPU 和内存使用率阈值。当某个参数超过预定义的阈值时，将发送消息。大部分阈值依赖于平台，并且不可更改。
- 您可以配置快照警报组，以便发送您指定的 CLI 的输出。

警报组向思科发送的消息

消息定期发送到思科，每当 ASA 重新加载时，也会发送这些消息。这些消息按警报组进行分类。

清单警报包含下列命令的输出：

- **show version** - 显示设备的 ASA 软件版本、硬件配置、许可证密钥和相关正常运行时间数据。
- **show inventory** - 检索并显示联网设备中安装的每款思科产品的相关清单信息。每款产品都由唯一的设备信息（称为 UDI）进行标识，UDI 是以下三个不同数据元素的组合：产品标识符 (PID)、版本标识符 (VID) 和序列号 (SN)。
- **show failover state** - 显示故障转移对中的两个装置的故障转移状态。显示的信息包括装置的主状态或辅助状态、装置的主动/备用状态以及上一次报告的故障转移原因。
- **show module** - 显示 ASA 上安装的任何模块的相关信息，例如，ASA 5585-X 上安装的 SSP 的相关信息以及 ASA 5585-X 上安装的 IPS SSP 的相关信息。
- **show environment** - 显示 ASA 系统组件的系统环境信息，例如机箱、驱动器、风扇和电源的硬件运行状态以及温度状态、电压和 CPU 利用率。

配置警报包含下列命令的输出：

- **show context** - 显示已分配的接口、配置文件 URL 以及配置的情景数目，如果在系统执行空间中启用了 Anonymous Reporting，则显示所有情景的列表。
- **show call-home registered-module status** - 显示已注册的模块状态。如果您使用系统配置模式，则此命令将根据整台设备 （而不是每个情景）显示系统模块状态。
- **show running-config** - 显示 ASA 上当前正在运行的配置。
- **show startup-config** - 显示启动配置。
- **show access-list | include elements** - 显示命中计数器和访问列表的时间戳值。

诊断警报包含下列命令的输出：

- **show failover** - 显示有关装置的故障转移状态的信息。
- **show interface** - 显示接口统计信息。
- **show cluster info** - 显示集群信息。
- **show cluster history** - 显示集群历史。
- **show crashinfo** (truncated) - 发生意外的软件重新加载之后，设备将发送修改后的崩溃信息文件 （仅包括该文件的回溯部分），以便仅向思科报告函数调用、注册表值和堆栈转储。
- **show tech-support no-config** - 显示由技术支持分析师用于诊断的信息。

环境警报包含下列命令的输出：

- **show environment** - 显示 ASA 系统组件的系统环境信息，例如机箱、驱动器、风扇和电源的硬件运行状态以及温度状态、电压和 CPU 利用率。
- **show cpu usage** - 显示 CPU 利用率信息。
- **show memory detail** - 显示有关可用系统内存和已分配系统内存的详细信息。

威胁警报包含下列命令的输出：

- **show threat-detection rate** - 显示威胁检测统计信息。
- **show threat-detection shun** - 显示当前绕过的主机。
- **show shun** - 显示绕过信息。
- **show dynamic-filter reports top** - 生成按僵尸网络流量过滤器分类的前 10 个恶意软件站点、端口和受感染主机的报告。

快速警报可能包含下列命令的输出：

- **show conn count** - 显示处于活动状态的连接的数目。
- **show asp drop** - 显示加速安全路径丢弃的数据包或连接数。

遥测警报包含下列命令的输出：

- **show perfmon detail** - 显示 ASA 性能详细信息。
- **show traffic** - 显示接口发送和接收活动。
- **show conn count** - 显示处于活动状态的连接的数目。
- **show vpn-sessiondb summary** - 显示 VPN 会话摘要信息。
- **show vpn load-balancing** - 显示 VPN 负载均衡虚拟集群配置的运行时统计信息。
- **show local-host | include interface** - 显示本地主机的网络状态。
- **show memory** - 显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要。
- **show context** - 显示已分配的接口、配置文件 URL 以及配置的情景数目，如果在系统执行空间中启用了 Anonymous Reporting，则显示所有情景的列表。
- **show access-list | include elements** - 显示命中计数器和访问列表的时间戳值。
- **show interface** - 显示接口统计信息。
- **show threat-detection statistics protocol** - 显示 IP 协议统计信息。
- **show phone-proxy media-sessions count** - 显示 Phone Proxy 所存储的相应媒体会话数。
- **show phone-proxy secure-phones count** - 显示数据库中存储的支持安全模式的电话数。
- **show route** - 显示路由表。
- **show xlate count** - 显示 NAT 会话 (xlate) 的数目。

消息严重性阈值

您使目标配置文件订用某些警报组时，可以设置阈值，以便根据消息严重性级别发送警报组消息。值小于目标配置文件的指定阈值的所有消息都不会发送到目标。

表 41-1 显示了消息严重性级别与系统日志严重性级别之间的映射。

表 41-1　消息严重性级别与系统日志级别之间的映射

Level	消息 严重性级别	系统日志 严重性级别	说明
9	灾难	不适用	网络范围的灾难性故障。
8	灾难	不适用	重大网络影响。
7	由指定的 CLI 关键字确定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	0	紧急。系统不可用。
6	由指定的 CLI 关键字确定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	1	警报。紧急情况；需要立即引起注意。
5	由指定的 CLI 关键字确定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	2	紧急。严重情况。
4	由指定的 CLI 关键字确定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	3	错误。轻微情况。
3	Warning	4	警告情况。
2	Notification	5	基本通知和参考消息。可能是独立的无关紧要情况。
1	正常	6	信息。正常事件，表示恢复正常状态。
0	Debugging	7	调试消息 （默认设置）。

订用配置文件

订用配置文件使您能够将目标收件人与感兴趣的组相关联。在配置文件中向订用的组注册的事件触发时，与该事件相关联的消息将发送到配置的收件人。订用配置文件具有下列属性：

- 您可以创建并配置多个配置文件。
- 一个配置文件可以配置多个邮件或 HTTPS 收件人。
- 一个配置文件可以使多个组订用指定的严重性级别。
- 配置文件支持三种消息格式：短文本、长文本和 XML。
- 您可以启用和禁用特定配置文件。默认情况下，配置文件处于禁用状态。
- 您可以指定最大消息大小。默认值为 3 MB。

我们提供了默认配置文件“思科 TAC”。默认配置文件包含一组要监控的预定义组 （诊断、环境、清单、配置和遥测）以及预定义的目标邮件地址和 HTTPS URL。您最初配置 Smart Call Home 时，系统将自动创建默认配置文件。目标邮件地址为 callhome@cisco.com，目标 URL 为 https://tools.cisco.com/its/service/oddce/services/DDCEService。

注　您无法更改默认配置文件的目标邮件地址或目标 URL。

您在使目标配置文件订用配置、清单、遥测或快照警报组时，可以选择以异步方式接收或者在指定时间定期接收警报组消息。

表 41-2 将默认警报组映射到其严重性级别订用和周期 （如果适用）：

表 41-2　警报组到严重性级别订用的映射

警报组	严重性级别	周期
配置	Informational	每月
诊断	参考及更高级别	不适用
环境	通知及更高级别	不适用
清单	Informational	每月
快照	Informational	不适用
系统日志	等效系统日志	不适用
遥测	Informational	每天
测试	不适用	不适用
威胁	Notification	不适用

Anonymous Reporting 和 Smart Call Home 指南

Anonymous Reporting

- 必须配置 DNS。
- 如果首次尝试无法发送 Anonymous Reporting 消息，则 ASA 将再重试两次，然后丢弃该消息。
- Anonymous Reporting 可以与其他 Smart Call Home 配置共存，而不会更改现有配置。例如，如果启用 Anonymous Reporting 之前 Smart Call Home 处于禁用状态，那么它将保持处于禁用状态，即使在 Anonymous Reporting 启用后也是如此。
- 如果 Anonymous Reporting 处于启用状态，您将无法删除信任点，并且禁用 Anonymous Reporting 时，信任点仍保留。如果 Anonymous Reporting 处于禁用状态，则您可以删除信任点，但禁用 Anonymous Reporting 不会导致删除信任点。
- 如果您使用的是多情景模式配置，则 **dns**、**interface** 和 **trustpoint** 命令处于管理员情景中，而 **call-home** 命令处于系统情景中。

Smart Call Home

- 在多情景模式中，**subscribe-to-alert-group snapshot periodic** 命令划分成两个命令：一个命令用于从系统配置中获取信息，另一个命令用于从用户情景中获取信息。
- Smart Call Home 后端服务器只能接受 XML 格式的消息。

- 如果已启用集群功能，并且已将 Smart Call Home 配置为订用安全级别为“紧急”的诊断警报组，那么将向思科发送 Smart Call Home 消息以报告重要的集群事件。仅对于下列事件，才会发送 Smart Call Home 集群消息：
  - 当装置加入集群时
  - 当装置离开集群时
  - 当集群装置变成集群主装置时
  - 当集群中的辅助装置发生故障时

  发送的每条消息都包含以下信息：
  - 处于活动状态的集群成员的计数
  - 对集群主装置运行的 **show cluster info** 命令和 **show cluster history** 命令的输出

相关主题

- 第 41-2 页的DNS 需求
- 第 13-13 页的配置 DNS 服务器

配置 Anonymous Reporting 和 Smart Call Home

虽然 Anonymous Reporting 是 Smart Call Home 服务的组成部分，并且使思科能够以匿名方式接收来自设备的最少量错误和运行状况信息，但是 Smart Call Home 服务提供了对系统运行状况的自定义支持，从而使思科 TAC 能够监控您的设备，并且在存在问题时 （通常在您知道问题已发生之前）提交个案。

可以在系统上同时配置这两个服务，尽管配置 Smart Call Home 服务将会提供与 Anonymous Reporting 相同的功能以及自定义服务。

进入配置模式时，系统将会显示提示符，要求您根据下列准则启用 Anonymous Reporting 和 Smart Call Home 服务：

- 在提示符处，您可以选择 [Y]（是）、[N]（否）或 [A]（稍后询问）。如果您选择 [A]（稍后询问），则系统将在 7 天后或者在 ASA 重新加载时再次提醒您。如果您继续选择 [A]（稍后询问），则 ASA 将以 7 天作为时间间隔再次提示 2 次，然后采用 [N]（否）响应并且不再询问。
- 如果系统未显示提示符，则您可以执行第 41-7 页的配置 Anonymous Reporting 中或第 41-8 页的配置 Smart Call Home 中的步骤来启用 Anonymous Reporting 或 Smart Call Home。

配置 Anonymous Reporting

如要配置 Anonymous Reporting，请执行下列步骤：

操作步骤

步骤 1　启用 Anonymous Reporting 功能并创建新的匿名配置文件。

```
call-home reporting anonymous
```

示例：

```
ciscoasa(config)# call-home reporting anonymous
```

输入此命令将会创建信任点，并安装用来验证思科网络服务器身份的证书。

步骤 2　（可选）确保已连接到服务器并且系统能够发送消息。

call-home test reporting anonymous

示例：

```
ciscoasa(config)# call-home test reporting anonymous

INFO: Sending test message to
https://tools.cisco.com/its/service/oddce/services/DDCEService...
INFO: Succeeded
```

系统将通过一条成功或错误消息返回测试结果。

配置 Smart Call Home

在 ASA 上配置 Smart Call Home 服务包括下列任务：

步骤 1　启用 Smart Call Home 服务。请参阅第 41-8 页的启用 Smart Call Home。

步骤 2　配置用于将 Smart Call Home 消息传递给用户的邮件服务器。请参阅第 41-12 页的配置邮件服务器。

步骤 3　为 Smart Call Home 消息设置联系人信息。请参阅第 41-11 页的配置客户联系信息。

步骤 4　定义警报处理参数，例如可以处理的最大事件速率。请参阅第 41-10 页的配置警报组订用。

步骤 5　设置警报订用配置文件。请参阅第 41-14 页的配置目标配置文件。

每个警报订用配置文件都标识了以下信息：

- Smart Call Home 消息所发送到的用户，例如思科的 Smart Call Home 服务器或一系列邮件收件人。
- 您想要针对其接收警报的信息类别，例如配置或清单信息。

启用 Smart Call Home

如要启用 Smart Call Home 并激活报障配置文件，请执行下列步骤：

操作步骤

步骤 1　启用 Smart Call Home 服务。

service call-home

示例：

```
ciscoasa(config)# service call-home
```

步骤 2　进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call home
```

声明证书颁发机构信任点并对其进行身份验证

如果 Smart Call Home 配置为通过 HTTPS 向网络服务器发送消息，则您需要将 ASA 配置为信任该网络服务器的证书或签发该证书的证书颁发机构 (CA) 的证书。Cisco Smart Call Home Production 服务器证书由 Verisign 签发。Cisco Smart Call Home Staging 服务器证书由 Digital Signature Trust Company 签发。

注　您不应该为客户端类型或验证用途设置信任点，以避免将信任点用于 VPN 验证。

如要声明思科服务器安全证书并对其进行身份验证，然后与 Smart Call Home 服务的思科 HTTPS 服务器进行通信，请执行下列步骤：

操作步骤

步骤 1　（仅限多情景模式）在管理员情景中安装证书。

changeto context *admincontext*

示例：

```
ciscoasa(config)# changeto context contextA
```

步骤 2　配置信任点并为证书登记作准备。

crypto ca trustpoint *trustpoint-name*

示例：

```
ciscoasa(config)# crypto ca trustpoint cisco
```

注　如果您使用 HTTP 作为传输方法，则必须通过信任点安装 HTTPS 所需的安全证书。请在以下 URL 处查找要安装的特定证书：

http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch6.html#wp1035380

步骤 3　指定以手动剪切并粘贴的方法进行证书登记。

enroll terminal

示例：

```
ciscoasa(ca-trustpoint)# enroll terminal
```

步骤 4　对指定的 CA 进行身份验证。CA 名称应该与 **crypto ca trustpoint** 命令中指定的信任点名称匹配。在提示符处，粘贴安全证书文本。

crypto ca authenticate *trustpoint*

示例：

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

步骤 5　指定安全证书文本结束，并确认接受所输入的安全证书。

quit

示例：

```
ciscoasa(ca-trustpoint)# quit
```

```
%Do you accept this certificate [yes/no]:

yes
```

配置环境警报组和快照警报组

如要配置环境警报组和快照警报组，请执行下列步骤：

操作步骤

步骤 1　进入警报组配置模式。

alert-group-config {**environment** | **snapshot**}

示例：

```
ciscoasa(config)# alert-group-config environment
```

配置警报组订用

如要使目标配置文件订用警报组，请执行下列步骤：

操作步骤

步骤 1　进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2　启用指定的 Smart Call Home 警报组。

alert-group {**all** | **configuration** | **diagnostic** | **environment** | **inventory** | **syslog**}

示例：

```
ciscoasa(cfg-call-home)# alert-group syslog
```

使用 **all** 关键字将启用所有警报组。默认情况下，所有警报组都处于启用状态。

步骤 3　进入指定目标配置文件的配置文件配置模式。

profile *profile-name*

示例：

```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

步骤 4　订用所有的可用警报组。

subscribe-to-alert-group all

示例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all
```

步骤 5　使此目标配置文件订用配置警报组。

subscribe-to-alert-group configuration periodic {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

示例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
```

periodic 关键字对配置警报组进行配置以定期发送通知。默认周期为每日。

daily 关键字以 *hh:mm* 格式指定每天发送信息的时间 （采用 24 小时制，例如 14:30）。

weekly 关键字以 *day hh:mm* 格式指定星期几和时间，其中星期几将拼写出来 （例如 Monday）。

monthly 关键字以 *date hh:mm* 格式指定数字日期 （1 到 31）和时间。

配置客户联系信息

如要配置客户联系信息，请执行下列步骤：

操作步骤

步骤 1　进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2　指定客户电话号码。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

phone-number *phone-number-string*

示例：

```
ciscoasa(cfg-call-home)# phone-number 8005551122
```

步骤 3　指定客户地址，地址是长度可达 255 个字符的自由格式字符串。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

street-address *street-address*

示例：

```
ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
```

步骤 4　指定客户姓名，姓名长度可达 128 个字符。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

contact-name *contact-name*

示例：

```
ciscoasa(cfg-call-home)# contact-name contactname1234
```

步骤 5　指定思科客户 ID，此 ID 的长度可达 64 个字符。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

customer-id *customer-id-string*

示例：

```
ciscoasa(cfg-call-home)# customer-id customer1234
```

步骤 6　指定客户站点 ID，此 ID 的长度可达 64 个字符。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

site-id *site-id-string*

示例：

```
ciscoasa(cfg-call-home)# site-id site1234
```

步骤 7　指定客户合同 ID，此 ID 的长度可达 128 个字符。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

contract-id *contract-id-string*

示例：

```
ciscoasa(cfg-call-home)# contract-id contract1234
```

示例

以下示例显示如何配置联系信息：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# contact-email-addr username@example.com
ciscoasa(cfg-call-home)# phone-number 8005551122
ciscoasa(cfg-call-home)# street-address “1234 Any Street, Any city, Any state, 12345”
ciscoasa(cfg-call-home)# contact-name contactname1234
ciscoasa(cfg-call-home)# customer-id customer1234
ciscoasa(cfg-call-home)# site-id site1234
ciscoasa(cfg-call-home)# contract-id contract1234
```

配置邮件服务器

我们建议您使用 HTTPS 进行消息传输，因为此协议最安全。但是，您可以为 Smart Call Home 配置邮件目标，然后将邮件服务器配置为使用邮件消息传输。

如要配置邮件服务器，请执行下列步骤：

操作步骤

步骤 1　进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2　指定 SMTP 邮件服务器。

mail-server *ip-address* **name priority** [**1-100**] [**all**]

示例：

```
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 smtp.example.com priority 1
```

您可以使用 5 个单独的命令指定多达 5 个邮件服务器。必须至少将一个邮件服务器配置为使用邮件传输方法来传输 Smart Call Home 消息。

数字越小，邮件服务器的优先级越高。

ip-address 参数可以是 IPv4 或 IPv6 邮件服务器地址。

示例

以下示例显示如何配置主邮件服务器 （名称为“smtp.example.com”）和辅助邮件服务器 （IP 地址为 10.10.1.1）：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# mail-server smtp.example.com priority 1
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 priority 2
ciscoasa(cfg-call-home)# exit
ciscoasa(config)#
```

配置流量速率限制

如要配置流量速率限制，请执行下列步骤：

操作步骤

步骤 1　进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2　指定 Smart Call Home 每分钟可以发送的消息数。默认值为 10 条消息/分钟。

rate-limit *msg-count*

ciscoasa(cfg-call-home)# rate-limit 5

发送 Smart Call Home 通信

如要手动发送 Smart Call Home 测试消息，请执行下列步骤：

操作步骤

步骤 1　使用配置文件配置来发送测试消息。

call-home test [*test-message*] **profile** *profile-name*

示例：

```
ciscoasa# call-home test [testing123] profile CiscoTAC-1
```

如要手动触发警报组消息，请执行下列步骤：

操作步骤

步骤 1　向一个目标配置文件 （如果已指定）发送警报组消息。如果未指定配置文件，则向所有订用了清单、配置、快照或遥测警报组的配置文件发送消息。

call-home send alert-group {**inventory** | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*]

示例：

```
ciscoasa# call-home send alert-group inventory
```

如要发出 CLI 命令并通过邮件将命令输出发送到思科 TAC 或指定的邮件地址，请执行下列步骤：

操作步骤

步骤 1　将命令输出发送到某个邮件地址。指定的 CLI 命令可以是任何命令，包括用于所有已注册的模块的命令。

call-home send *cli command* [**email** *email*]

示例：

```
ciscoasa# call-home send cli destination email username@example.com
```

如果指定了邮件地址，则命令输出将发送到该地址。如果未指定邮件地址，则输出将发送到思科 TAC。邮件将以日志文本格式发送，服务编号 （如果已指定）将包括在主题行中。

只有在未指定邮件地址，或者指定了思科 TAC 邮件地址时，才需要服务编号。

配置目标配置文件

如要配置目标配置文件以进行邮件或 HTTP 传输，请执行下列步骤：

操作步骤

步骤 1　进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2　进入指定目标配置文件的配置文件配置模式。如果指定的目标配置文件不存在，将会创建该文件。

profile *profile-name*

示例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

您最多可以创建 10 个处于活动状态的配置文件。默认配置文件将向思科 TAC 报告。如果您想要将报障信息发送到其他位置 （例如您自己的服务器），则可以配置一个单独的配置文件。

步骤 3　配置 Smart Call Home 消息接收方的目标、消息大小、消息格式和传输方法。默认消息格式为 XML，默认情况下启用的传输方法为邮件。

destination {**email** *address* | **http** *url*} | **message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} **transport-method** {**email** | **http**}}

示例：

```
ciscoasa(cfg-call-home-profile)# destination address email username@example.com

ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text
```

邮件地址是 Smart Call Home 消息接收方的邮件地址，此地址的长度可达 100 个字符。默认情况下，最大 URL 大小为 5 MB。

在移动设备上，使用短文本格式来发送和读取消息；在计算机上，使用长文本格式来发送和读取消息。

如果消息接收方是 Smart Call Home 后端服务器，请确保 **preferred-msg-format** 值是 XML，这是因为后端服务器只能接受 XML 格式的消息。

如要将传输方法设置为 HTTP，请参阅第 41-8 页的启用 Smart Call Home。使用此命令可以将传输方法重新更改为邮件。

复制目标配置文件

如要通过复制现有的目标配置文件来创建新的目标配置文件，请执行下列步骤：

操作步骤

步骤 1　进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2　指定要复制的配置文件。

profile *profile-name*

示例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

步骤 3　将现有配置文件的内容复制到新配置文件。

copy profile *src-profile-name dest-profile-name*

示例：

```
ciscoasa(cfg-call-home)# copy profile newprofile profile1
```

现有配置文件 (*src-profile-name*) 和新配置文件 (*dest-profile-name*) 的长度可达 23 个字符。

示例

以下示例显示如何复制现有配置文件：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile newprofile profile1
```

将目标配置文件重命名

如要更改现有配置文件的名称，请执行下列步骤：

操作步骤

步骤 1　进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2　指定要重命名的配置文件。

profile *profilename*

示例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

步骤 3　更改现有配置文件的名称。

rename profile *src-profile-name dest-profile-name*

示例：

```
ciscoasa(cfg-call-home)# rename profile newprofile profile1
```

现有配置文件 (*src-profile-name*) 和新配置文件 (*dest-profile-name*) 的长度可达 23 个字符。

示例

以下示例显示如何将现有配置文件重命名：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# rename profile newprofile profile1
```

监控 Anonymous Reporting 和 Smart Call Home

如要监控 Anonymous Reporting 和 Smart Call Home 服务，请参阅下列命令。

- **show call-home detail**

  此命令显示当前 Smart Call Home 详细配置。

- **show call-home mail-server status**

  此命令显示当前邮件服务器状态。

- **show call-home profile** {*profile name* | **all**}

  此命令显示 Smart Call Home 配置文件的配置。
- **show call-home registered-module status** [**all**]

  此命令显示已注册的模块状态。
- **show call-home statistics**

  此命令显示报障详细状态。
- **show call-home**

  此命令显示当前 Smart Call Home 配置。
- **show running-config call-home**

  此命令显示当前 Smart Call Home 运行配置。
- **show smart-call-home alert-group**

  此命令显示 Smart Call Home 警报组的当前状态。
- **show running-config all**

  此命令显示有关 Anonymous Reporting 用户配置文件的详细信息。

Smart Call Home 的示例 (CLI)

以下示例显示如何配置 Smart Call Home 服务：

```
ciscoasa (config)# service call-home
ciscoasa (config)# call-home
ciscoasa (cfg-call-home)# contact-email-addr customer@example.com
ciscoasa (cfg-call-home)# profile CiscoTAC-1
ciscoasa (cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService
ciscoasa (cfg-call-home-profile)# destination address email callhome@example.com
ciscoasa (cfg-call-home-profile)# destination transport-method http
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group environment
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group diagnostic
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group telemetry periodic weekly
Monday 23:30
```

Anonymous Reporting 和 Smart Call Home 的历史

表 41-3 Anonymous Reporting 和 Smart Call Home 的历史

功能名称	平台版本	说明
Smart Call Home	8.2(2)	Smart Call Home 服务用于在 ASA 上提供主动诊断和实时警报，并提供更高的网络可用性和运行效率。 我们引入或修改了下列命令： **active (call home)**、 **call-home**、 **call-home send alert-group**、**call-home test**、 **contact-email-addr**、 **customer-id (call home)**、**destination (call home)**、**profile**、**rename profile**、**service call-home**、**show call-home**、 **show call-home detail**、 **show smart-call-home alert-group**、 **show call-home profile**、 **show call-home statistics**、**show call-home mail-server status**、 **show running-config call-home**、**show call-home registered-module status all**、**site-id**、**street-address**、**subscribe-to-alert-group all**、 **alert-group-config**、**subscribe-to-alert-group configuration**、 **subscribe-to-alert-group diagnostic**、 **subscribe-to-alert-group environment**、**subscribe-to-alert-group inventory periodic**、**subscribe-to-alert-group snapshot periodic**、 **subscribe-to-alert-group syslog** 和 **subscribe-to-alert-group telemetry periodic**。
Anonymous Reporting	9.0(1)	您可以通过启用 Anonymous Reporting 服务来帮助改进 ASA 平台，此服务使思科能够安全地接收来自设备的最少量错误和运行状况信息。 我们引入了以下命令：**call-home reporting anonymous** 和 **call-home test reporting anonymous**。
Smart Call Home	9.1(2)	**show local-host** 命令已更改为 **show local-host	include interface** 命令，以进行遥测警报组报告。
Smart Call Home	9.1(3)	如果已启用集群功能，并且已将 Smart Call Home 配置为订用安全级别为“紧急”的诊断警报组，那么将向思科发送 Smart Call Home 消息以报告重要的集群事件。仅对于以下三个事件，才会发送 Smart Call Home 集群消息： • 当装置加入集群时 • 当装置离开集群时 • 当集群装置变成集群主装置时 发送的每条消息都包含以下信息： • 处于活动状态的集群成员的计数 • 对集群主装置运行的 **show cluster info** 命令和 **show cluster history** 命令的输出

第 10 部分

参考网站

第 42 章

使用命令行界面

本章描述如何在 Cisco ASA 上使用 CLI。

- 第 42-1 页的防火墙模式和安全情景模式
- 第 42-2 页的命令模式和提示符
- 第 42-3 页的语法格式化
- 第 42-3 页的缩写命令
- 第 42-3 页的命令行编辑
- 第 42-3 页的命令补全
- 第 42-3 页的命令帮助
- 第 42-4 页的查看运行配置
- 第 42-4 页的过滤 show 和 more 命令输出
- 第 42-5 页的命令输出分页
- 第 42-5 页的添加注释
- 第 42-5 页的文本配置文件
- 第 42-7 页的支持的字符集

注 CLI 使用类似于 Cisco IOS CLI 的语法和其他约定，但是 ASA 操作系统不是 Cisco IOS 软件版本。请勿假设 Cisco IOS CLI 命令适用于 ASA 或在其之上具有相同功能。 .

防火墙模式和安全情景模式

ASA 在以下模式的组合中运行：

- 透明防火墙或路由式防火墙模式

  防火墙模式确定 ASA 作为第 2 层还是第 3 层防火墙运行。

- 多情景或单情景模式

  安全情景模式确定 ASA 作为单一设备还是作为多个安全情景 （充当虚拟设备）运行。

一些命令仅在特定模式下可用。

命令模式和提示符

ASA CLI 包含命令模式。某些命令只能在特定模式下输入。例如，如要输入显示敏感信息的命令，需要输入密码并进入具有更高特权的模式。然后，为确保不会意外输入配置更改，必须进入配置模式。可以在较高模式下输入所有较低的命令，例如，可以在全局配置模式下输入特权 EXEC 命令。

注　各种类型的提示符全部是默认提示符，并且配置后可能会不同。

- 当处于系统配置模式或单情景模式时，提示符以主机名开头：

  ```
  ciscoasa
  ```

- 列显提示符字符串时，系统会解析提示符配置并按照设置 **prompt** 命令的顺序列显已配置的关键字值。关键字参数可以是以下任何一项并按照任何顺序：hostname、 domain、 context、 priority、 state。

  ```
  asa(config)# prompt hostname context priority state
  ```

- 当处于某个情景中时，提示符以主机名开头，后面跟以情景名称：

  ```
  ciscoasa/context
  ```

提示符根据访问模式而异：

- 用户 EXEC 模式

  通过用户 EXEC 模式可查看最低 ASA 设置。首次访问 ASA 时，用户 EXEC 模式提示符显示如下：

  ```
  ciscoasa>

  ciscoasa/context>
  ```

- 特权 EXEC 模式

  通过特权 EXEC 模式可查看特权级别内的所有当前设置。任何用户 EXEC 模式命令在特权 EXEC 模式下都将适用。在用户 EXEC 模式下输入 **enable** 命令 （需要密码）可启动特权 EXEC 模式。提示符包含数字符号 (#)：

  ```
  ciscoasa#

  ciscoasa/context#
  ```

- 全局配置模式

  通过全局配置模式可更改 ASA 配置。所有用户 EXEC、特权 EXEC 和全局配置命令在此模式下都可用。在特权 EXEC 模式下输入 **configure terminal** 命令可启动全局配置模式。提示符将更改为以下形式：

  ```
  ciscoasa(config)#

  ciscoasa/context(config)#
  ```

- 特定于命令的配置模式

  从全局配置模式下，某些命令可进入特定于命令的配置模式。所有用户 EXEC、特权 EXEC、全局配置和特定于命令的配置命令在此模式下都可用。例如， **interface** 命令会进入接口配置模式。提示符将更改为以下形式：

  ```
  ciscoasa(config-if)#

  ciscoasa/context(config-if)#
  ```

语法格式化

命令语法描述使用表 42-1 中列出的约定。

表 42-1　　语法约定

约定	描述
bold	粗体文本指示按字面显示输入的命令和关键字。
italics	斜体文本指示为其提供值的参数。
[x]	方括号用于将可选元素（关键字或参数）括起来。
|	竖线指示可选或必需的关键字或参数集中的选项。
[x | y]	将以竖线分隔的关键字或参数括起来的方括号指示可选选项。
{x | y}	将以竖线分隔的关键字或参数括起来的大括号指示必需选项。
[x {y | z}]	方括号或大括号的嵌套集合指示可选或必需元素中的可选或必需选项。方括号中的大括号和竖线指示可选元素中的必需选项。

缩写命令

可以将大多数命令缩写为命令的最少唯一字符；例如，可以输入 **wr t** 以查看配置而不是输入完整命令 **write terminal**，或者可以输入 **en** 以启动特权模式并输入 **conf t** 以启动配置模式。此外，还可以输入 **0** 以表示 **0.0.0.0**。

命令行编辑

ASA 使用与 Cisco IOS 软件相同的命令行编辑约定。可以使用 **show history** 命令查看所有以前输入的命令，或者使用向上箭头或 **^p** 命令逐个查看以前输入的命令。一旦检查以前输入的命令，即可使用向下箭头或 **^n** 命令在列表中前进。当到达希望重复使用的命令时，可以编辑该命令并按 **Enter** 键将其启动。您也可以使用 **^w** 删除光标左侧的单词，或者使用 **^u** 擦除该行。

ASA 在命令中允许最多 512 个字符，其他字符会被忽略。

命令补全

如要在输入部分字符串后补全命令或关键字，请按 **Tab** 键。仅当部分字符串仅与一个命令或关键字匹配时，ASA 才会补全命令或关键字。例如，如果输入 **s** 并按 **Tab** 键，则 ASA 不会补全命令，因为它与多个命令匹配。但是，如果输入 **dis**，则 **Tab** 键会补全 **disable** 命令。

命令帮助

通过输入以下命令，可从命令行获取帮助信息：

- **help** *command_name*

  显示特定命令的帮助。

- *command_name* **?**

  显示可用参数的列表。

- *string***?**（无空格）

  列出以字符串开头的可能命令。

- **?**和 **+?**

  列出所有可用命令。如果输入 **?**，则 ASA 仅显示可用于当前模式的命令。要显示所有可用命令，包括可用于较低模式的命令，请输入 **+?**。

注　如果要在命令字符串中包含问号 (?)，则在键入问号之前必须按 **Ctrl-V**，以便不会无意中调用 CLI 帮助。

查看运行配置

如要查看运行配置，请使用以下命令之一：

- **show running-config** [**all**] [*command*]

  如果指定 **all**，则还会显示所有默认设置。如果指定 *command*，则输出仅包含相关命令。

  注　许多关键字显示为 *****。如要以明文或以加密形式 （如果已启用主口令）查看密码，请使用 **more** 命令。

- **more system:running-config**

相关主题

第 13-10 页的配置主密码

过滤 show 和 more 命令输出

可以将竖线 (|) 用于任何 **show** 命令并包含过滤器选项和过滤表达式。与 Cisco IOS 软件类似，通过将各输出行与正则表达式匹配来执行过滤。通过选择不同过滤器选项，可以包含或排除与表达式匹配的所有输出。您还可以显示以与表达式匹配的行开头的所有输出。

将过滤选项与 **show** 命令配合使用的语法如下：

```
ciscoasa# show command | {include | exclude | begin | grep [-v]} regexp
```

或者

```
ciscoasa# more system:running-config | {include | exclude | begin | grep [-v]} regexp
```

注　通过输入 **more** 命令，可以查看任何文件而不仅是运行配置的内容，有关详细信息，请参阅命令参考。

在此命令字符串中，第一根竖线 (|) 是运算符，并且必须包含在命令中。此运算符将 **show** 命令的输出定向到过滤器。在语法图中，其他竖线 (|) 指示备用选项，并且不是命令的一部分。

include 选项包含与正则表达式匹配的所有输出行。不带 **-v** 的 **grep** 选项具有相同效果。 **exclude** 选项排除与正则表达式匹配的所有输出行。带有 **-v** 的 **grep** 选项具有相同效果。**begin** 选项显示以与正则表达式匹配的行开头的所有输出行。

将 *regexp* 替换为任何 Cisco IOS 正则表达式。正则表达式未用引号或双引号引起来，因此请注意尾随空格，它们将被视为正则表达式的一部分。

创建正则表达式时，可以使用要与之匹配的任何字母或数字。此外，某些关键字字符 （称为*元字符*）在正则表达式中使用时具有特殊含义。

使用 **Ctrl+V** 可将 CLI 中的所有特殊字符转义，例如问号 (?) 或跳格键。例如，键入 **d[Ctrl+V]?g** 将在配置中输入 **d?g**。

命令输出分页

对于诸如 **help** 或 **?**、**show**、**show xlate** 之类的命令或其他提供长列表的命令，可以确定信息显示屏幕并暂停，还是让命令运行至完成。通过 **pager** 命令，可以选择在 More 提示符出现之前要显示的行数。

启用分页后，会出现以下提示符：

```
<--- More --->
```

More 提示符使用类似于 UNIX **more** 命令的语法：

- 按**空格**以查看其他屏幕。
- 按 **Enter** 键以查看下一行。
- 按 **q** 键以返回到命令行。

添加注释

可以在某一行之前前置冒号 (:) 以创建注释。但是，该注释仅出现在命令历史记录缓冲区中，而不出现在配置中。因此，可以使用 **show history** 命令或者通过按箭头键检索以前的命令来查看注释，但是由于注释不在配置中，因此 **write terminal** 命令不会显示该注释。

文本配置文件

本节描述如何格式化可以下载到 ASA 的文本配置文件。

- 第 42-6 页的命令与文本文件中的行的对应方式
- 第 42-6 页的特定于命令的配置模式命令
- 第 42-6 页的自动文本条目
- 第 42-6 页的行顺序
- 第 42-6 页的文本配置中不包含的命令
- 第 42-6 页的密码
- 第 42-7 页的多安全情景文件

命令与文本文件中的行的对应方式

文本配置文件包含与本指南中描述的命令对应的行。

在示例中，命令之前前置有 CLI 提示符。以下示例中的提示符为“ciscoasa(config)#”：

```
ciscoasa(config)# context a
```

在系统未提示输出命令的文本配置文件中，会因此省略提示符：

```
context a
```

特定于命令的配置模式命令

特定于命令的配置模式命令在命令行中输入时缩进显示在主命令下。只要这些命令紧跟在主命令后显示，便无需缩进文本行。例如，以下未缩进文本的读取与缩进文本相同：

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

自动文本条目

将配置下载到 ASA 时，它会自动插入一些行。例如， ASA 为默认设置或为配置的修改时间插入行。创建文本文件时，无需输入这些自动条目。

行顺序

大致上，命令可以依照文件中的任何顺序。但是，某些行 （例如 ACE）按其显示顺序进行处理，并且顺序可影响访问列表的功能。其他命令也可能具有顺序要求。例如，必须首先为接口输入 **nameif** 命令，因为许多后续命令都使用该接口的名称。此外，特定于配置的模式下的命令必须紧跟在主命令之后。

文本配置中不包含的命令

某些命令在配置中不插入行。例如，诸如 **show running-config** 之类的运行时命令在文本文件中没有对应的行。

密码

登录名、启用和用户密码在存储在配置中之前会自动加密。例如，密码“cisco”的加密形式可能看似为 jMorNbK0514fadBh。您可以将配置密码以其加密形式复制到其他 ASA，但是无法自行解密密码。

如果在文本文件中输入未加密密码，则在将配置复制到 ASA 时， ASA 不会自动将其加密。仅当使用 **copy running-config startup-config** 或 **write memory** 命令从命令行保存运行配置时，ASA 才会将其加密。

多安全情景文件

对于多个安全情景，整个配置由以下多个部分组成：

- 安全情景配置
- 系统配置，用于标识 ASA 的配置，包括情景列表
- 管理情景，用于为系统配置提供网络接口

  系统配置不包含其自己的任何接口或网络设置。相反，当系统需要访问网络资源 （例如从服务器下载情景）时，它使用指定为管理情景的情景。

每个情景类似于单情景模式配置。系统配置与情景配置的不同在于，系统配置包含仅系统命令（例如所有情景的列表），而其他典型命令不存在 （例如许多接口参数）。

支持的字符集

ASA CLI 当前仅支持 UTF-8 编码。UTF-8 是 Unicode 符号的特定编码方案，并已设计为与符号的 ASCII 子集兼容。ASCII 在 UTF-8 中仅表示为单字节字符。所有其他字符在 UTF-8 中都表示为多字节符号。

完全支持 ASCII 可打印字符 (0x20 to 0x7e)。可打印 ASCII 字符与 ISO 8859-1 相同。UTF-8 是 ISO 8859-1 的超集，因此前 256 个字符（0 至 255）与 ISO 8859-1 相同。ASA CLI 支持 ISO 8859-1 的最多 255 个字符 （多字节字符）。

地址、协议和端口

本章提供 IP 地址、协议和应用的快速参考。

- 第 43-1 页的 IPv4 地址和子网掩码
- 第 43-4 页的 IPv6 地址
- 第 43-9 页的协议和应用
- 第 43-10 页的 TCP 和 UDP 端口
- 第 43-12 页的本地端口和协议
- 第 43-14 页的 ICMP 类型

IPv4 地址和子网掩码

本节介绍如何在思科 ASA 中使用 IPv4 地址。IPv4 地址是采用点分十进制记法的 32 位数字：从二进制转换为十进制数字的四个 8 位字段（八位组），字段之间用点分隔。 IP 地址的第一个部分识别主机所在的网络，第二个部分识别给定网络上的特定主机。网络号字段称为网络前缀。给定网络上的所有主机共享同一个网络前缀，但必须有唯一的主机号。对于有类 IP，地址类确定网络前缀与主机号之间的边界。

类

IP 主机地址分为三种不同的地址类：A 类、 B 类和 C 类。每一类在 32 位地址内的不同点固定网络前缀与主机号之间的边界。 D 类地址保留用于组播 IP。

- A 类地址 （1.xxx.xxx.xxx 到 126.xxx.xxx.xxx）仅将第一个八位组用作网络前缀。
- B 类地址 （128.0.xxx.xxx 到 191.255.xxx.xxx）将前两个八位组用作网络前缀。
- C 类地址 （192.0.0.xxx 到 223.255.255.xxx）将前三个八位组用作网络前缀。

由于 A 类地址具有 16,777,214 个主机地址，B 类地址具有 65,534 台主机，因此，可以使用子网掩码将这些庞大的网络分割成较小的子网。

专用网络

如果需要在网络上使用大量地址，但不需要在互联网上路由这些地址，可以使用互联网编号分配机构 (IANA) 推荐的专用 IP 地址（请参阅 RFC 1918）。以下地址范围被指定为不应通告的专用网络：

- 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

子网掩码

通过子网掩码，可以将一个 A 类、B 类或 C 类网络转换为多个网络。利用子网掩码，可以创建扩展网络前缀，从而将主机号中的位添加到网络前缀中。例如，C 类网络前缀始终包含 IP 地址的前三个八位组。但是，C 类扩展网络前缀还部分使用第四个八位组。

如果使用二进制记法而不是点分十进制记法，将会有助于理解子网掩码。子网掩码中的位与互联网地址一一对应：

- 如果 IP 地址中的对应位是扩展网络前缀的一部分，该位将被设置为 1。
- 如果该位是主机号的一部分，将被设置为 0。

示例 1：如果有 B 类地址 129.10.0.0，并想将第三个八位组全部用作扩展网络前缀而不是主机号的一部分，则必须将子网掩码指定为 11111111.11111111.11111111.00000000。该子网掩码将这个 B 类地址转换为等效的 C 类地址，其中的主机号仅包含最后一个八位组。

示例 2：如果只想将第三个八位组的一部分用于扩展网络前缀，必须将子网掩码指定为类似 11111111.11111111.11111000.00000000 的形式，这种形式的子网掩码仅将第三个八位组中的 5 位用于扩展网络前缀。

可以将子网掩码写成点分十进制掩码或 */位数*（“斜杠 *位数*”）掩码。在示例 1 中，对于点分十进制掩码，可以将每个二进制八位组转换为十进制数：255.255.255.0。对于 */位数*掩码，可以添加数字 1s: /24。在示例 2 中，十进制数为 255.255.248.0， /位数为 /21。

还可以将第三个八位组的一部分用于扩展网络前缀，从而将多个 C 类网络构建成一个较大的超网。例如，192.168.0.0/20。

确定子网掩码

请参阅表 43-1，以根据您希望拥有的主机数来确定子网掩码。

注　子网的第一个和最后一个数字已保留，但 /32 除外，该数字用于识别单个主机。

表 43-1　主机、位掩码和点分十进制掩码

主机	/位掩码	点分十进制掩码
16,777,216	/8	255.0.0.0 A 类网络
65,536	/16	255.255.0.0 B 类网络
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0

表 43-1　主机、位掩码和点分十进制掩码（续）

主机	/位掩码	点分十进制掩码
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	255.255.255.0 C 类网络
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
不使用	/31	255.255.255.254
1	/32	255.255.255.255 单个主机地址

确定要与子网掩码配合使用的地址

以下各节介绍如何确定要与 C 类和 B 类网络的子网掩码配合使用的网络地址。

C 类网络地址

对于主机数在 2 与 254 之间的网络，第四个八位组是主机地址数量的倍数，从 0 开始。例如，表 43-2 显示了 8 主机子网 (/29) 为 192.168.0.x。

注　子网的第一个和最后一个地址已保留。在第一个子网示例中，不能使用 192.168.0.0 或 192.168.0.7。

表 43-2　C 类网络地址

掩码为 /29 (255.255.255.248) 的子网	地址范围
192.168.0.0	192.168.0.0 到 192.168.0.7
192.168.0.8	192.168.0.8 到 192.168.0.15
192.168.0.16	192.168.0.16 到 192.168.0.31
-	-
192.168.0.248	192.168.0.248 到 192.168.0.255

B 类网络地址

如要确定与主机数在 254 与 65,534 之间的网络的子网掩码配合使用的网络地址，需要确定每个可能的扩展网络前缀的第三个八位组的值。例如，您可能想要为类似于 10.1.*x*.0 的地址构建子网，在该地址中，前两个八位组是固定的，因为它们用于扩展网络前缀中，第四个八位组是 0，因为所有位都用于主机号。

如要确定第三个八位组的值，请按照以下步骤操作：

步骤 1　用 65,536（使用第三个和第四个八位组的地址的总数）除以您想要的主机地址数量，以计算出可从网络构建的子网数量。

例如，65,536 除以 4096 个主机等于 16。

因此，4096 个地址有 16 个子网，每个都位于 B 类网络上。

步骤 2　用 256（第三个八字元值的数量）除以子网数量，以确定第三个八字元值的倍数：

在本示例中，256/16 = 16。

第三个八字元是 16 的倍数，从 0 开始。

表 43-3 显示了网络 10.1 的 16 个子网。

注　子网的第一个和最后一个地址已保留。在第一个子网示例中，不能使用 10.1.0.0 或 10.1.15.255。

表 43-3　网络的子网

掩码为 /20 的子网 (255.255.240.0)	地址范围
10.1.0.0	10.1.0.0 到 10.1.15.255
10.1.16.0	10.1.16.0 到 10.1.31.255
10.1.32.0	10.1.32.0 到 10.1.47.255
-	-
10.1.240.0	10.1.240.0 到 10.1.255.255

IPv6 地址

IPv6 是继 IPv4 之后的下一代互联网协议。它提供经过扩展的地址空间、简化的报头格式、经过改进的扩展和选项支持、流标签功能以及身份验证和隐私功能。有关 IPv6 的介绍，请参阅 RFC 2460。有关 IPv6 寻址架构的介绍，请参阅 RFC 3513。

本节介绍 IPv6 地址的格式和架构。

相关主题

第 11-10 页的配置 IPv6 寻址

IPv6 地址格式

IPv6 地址以一系列八个 16 位十六进制字段表示，字段之间用冒号 (:) 分隔，格式为：x:x:x:x:x:x:x:x。下面是 IPv6 地址的两个示例：

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

注　IPv6 地址中的十六进制字母不区分大小写。

不需要将前导零包含在地址的各个字段中，但每个字段必须至少包含一位数。因此，示例地址 2001:0DB8:0000:0000:0008:0800:200C:417A 可以通过移除从左侧数第三到第六个字段中的前导零来缩短为 2001:0DB8:0:0:8:800:200C:417A。包含所有零的字段 （从左侧数第三和第四个字段）被缩短为一个零。从左侧数起的第五个字段移除了三个前导零，仅留下了一个 8，从左侧数起的第六个字段移除了一个前导零，留下了 800。

对 IPv6 地址来说，包含几个连续的十六进制零字段很常见。可以使用两个冒号 (::) 压缩 IPv6 地址开始、中间或结尾位置的连续零字段（冒号表示连续的十六进制零字段）。表 43-4 显示了不同类型 IPv6 地址的几个地址压缩示例。

表 43-4　　IPv6 地址压缩示例

地址类型	标准形式	压缩形式
单播	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
组播	FF01:0:0:0:0:0:0:101	FF01::101
环回	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

注　两个冒号 (::) 在 IPv6 地址中只能用一次，用以表示连续的零字段。

在同时包含 IPv4 和 IPv6 地址的环境中，通常使用 IPv6 的替代格式。此替代格式为 x:x:x:x:x:x:y.y.y.y，其中，x 表示 IPv6 地址六个高位部分的十六进制值，y 表示该地址 32 位 IPv4 部分的十进制值（该部分代替 IPv6 地址的剩余两个 16 位部分）。例如，IPv4 地址 192.168.1.1 可表示为 IPv6 地址 0:0:0:0:0:0:FFFF:192.168.1.1 或 ::FFFF:192.168.1.1。

IPv6 地址类型

以下是 IPv6 地址的三种主要类型：

- **Unicast** - 单播地址是单个接口的标识符。发送到单播地址的数据包将会传输到通过该地址识别的接口。一个接口可能分配有多个单播地址。
- **Multicast** - 组播地址是一组接口的标识符。发送到某个组播地址的数据包将会传输到通过该地址识别的所有地址。
- **Anycast** - 任播地址是一组接口的标识符。与组播地址不同的是，发送到任播地址的数据包仅传输到“最近”的接口 （以路由协议的距离为测量标准）。

注　IPv6 中没有广播地址。组播地址提供广播功能。

单播地址

本节介绍 IPv6 单播地址。单播地址识别网络节点上的接口。

全局地址

IPv6 全局单播地址的通用格式为全局路由前缀，其后跟的是子网 ID，然后是接口 ID。全局路由前缀可以是未被其他 IPv6 地址类型保留的任何前缀。

所有的全局单播地址 （以二进制 000 开头的除外）都具有改良 EUI-64 格式的 64 位接口 ID。

以二进制 000 作为开头的全局单播地址在地址的接口 ID 部分的大小或结构上没有任何限制。具有嵌入式 IPv4 地址的 IPv6 地址就是属于此类型的地址。

相关主题

- 第 43-9 页的 IPv6 地址前缀
- 第 43-7 页的接口标识符
- 第 43-6 页的与 IPv4 兼容的 IPv6 地址

站点本地地址

站点本地地址用于在一个站点内寻址。此类地址可在不使用全局唯一前缀的情况下用于对整个站点进行寻址。站点本地地址具有前缀 FEC0::/10，后跟 54 位子网 ID，并以改良 EUI-64 格式的 64 位接口 ID 结尾。

站点本地路由器不将具有源或目标站点本地地址的任何数据包转发到站点外。因此，站点本地地址可被视为专用地址。

链路本地地址

所有接口均需要有至少一个链路本地地址。可以为每个接口配置多个 IPv6 地址，但只能配置一个链路本地地址。

链路本地地址是一个 IPv6 单播地址，通过使用链路本地前缀 FE80::/10 和改良 EUI-64 格式接口标识符，可在任意接口上自动配置此类地址。链路本地地址用于邻居发现协议和无状态自动配置过程。使用链路本地地址的节点可进行通信；它们不需要站点本地地址或全局唯一地址即可进行通信。

路由器不会转发具有源或目标链路本地地址的任何数据包。因此，链路本地地址可被视为专用地址。

与 IPv4 兼容的 IPv6 地址

有两种类型的 IPv6 地址可包含 IPv4 地址。

第一种类型是与 IPv4 兼容的 IPv6 地址。IPv6 过渡机制包括主机和路由器通过 IPv4 路由基础设施用隧道动态传输 IPv6 数据包的技术。使用此技术的 IPv6 节点分配有特殊的 IPv6 单播地址，从而可传送低位 32 位的全局 IPv4 地址。此类地址被称为与 IPv4 兼容的 IPv6 地址，其格式为 ::y.y.y.y，其中，y.y.y.y 是 IPv4 单播地址。

注　在与 IPv4 兼容的 IPv6 地址中使用的 IPv4 地址必须为全局唯一的 IPv4 单播地址。

第二种类型的 IPv6 地址具有嵌入式 IPv4 地址，被称为 IPv4 映射 IPv6 地址。此类地址用于将 IPv4 节点的地址表示为 IPv6 地址。此类地址的格式为 ::FFFF:y.y.y.y，其中，y.y.y.y 是 IPv4 单播地址。

未指定地址

未指定地址 0:0:0:0:0:0:0:0 表示没有 IPv6 地址。例如，IPv6 网络上新初始化的节点可能将未指定地址用作其数据包的源地址，直至它接收到 IPv6 地址。

注　未指定 IPv6 地址不能分配给接口。未指定 IPv6 地址不得用作 IPv6 数据包或 IPv6 路由报头中的目标地址。

环回地址

环回地址 0:0:0:0:0:0:0:1 可被节点用于向其自身发送 IPv6 数据包。 IPv6 中的环回地址与 IPv4 (127.0.0.1) 中的环回地址功能相同。

注　IPv6 环回地址不能分配给物理接口。将 IPv6 环回地址用作其源地址或目标地址的数据包必须留在创建该数据包的节点内。 IPv6 路由器不转发将 IPv6 环回地址用作其源地址或目标地址的数据包。

接口标识符

IPv6 单播地址中的接口标识符用于标识链路上的接口。接口标识符在子网前缀内需要是唯一的。很多情况下，接口标识符来源于接口链路层地址。可以将同一个接口标识符用在一个节点的多个接口上，前提是，这些接口连接到不同的子网。

对于所有单播地址，除了以二进制 000 开头的之外，接口标识符的长度需要是 64 位，且以改良 EUI-64 格式构造。改良 EUI-64 格式以 48 位 MAC 地址为基础，通过颠倒 MAC 地址中的通用/本地位并在 MAC 地址的上三个字节与下三个字节之间插入十六进制数 FFFE 创建而成。

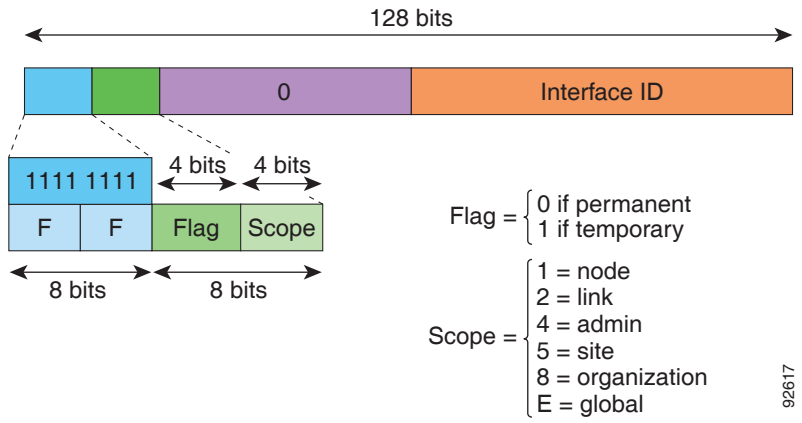
例如，具有 MAC 地址 00E0.b601.3B7A 的接口有一个 64 位接口 ID 02E0:B6FF:FE01:3B7A。

组播地址

IPv6 组播地址是一组通常位于不同节点的接口的标识符。发送到某个组播地址的数据包将会传输到通过该组播地址识别的所有接口。一个接口可属于任意数量的组播组。

IPv6 组播地址具有前缀 FF00::/8 (1111 1111)。紧跟前缀的八位组定义组播地址的类型和范围。永久分配（已知）的组播地址具有一个等于 0 的标志参数；临时（瞬时）组播地址具有一个等于 1 的标志参数。有节点范围、链路范围、站点范围、组织范围或全局范围的组播地址分别具有范围参数 1、 2、 5、 8 或 E。例如，前缀为 FF02::/16 的组播地址是具有链路范围的永久组播地址。图 43-1 显示了 IPv6 组播地址的格式。

图 43-1　　IPv6 组播地址格式



加入以下组播组需要 IPv6 节点 （主机和路由器）：

- 全节点组播地址：
  - FF01::（接口本地）
  - FF02::（链路本地）
- 节点上每个 IPv6 单播地址和任播地址的请求节点地址：FF02:0:0:0:0:1:FFXX:XXXX/104，其中， XX:XXXX 是单播地址或任播地址的低位 24 位。

注　请求节点地址用于邻居请求消息中。

加入以下组播组需要 IPv6 路由器：

- FF01::2（接口本地）
- FF02::2（链路本地）
- FF05::2（站点本地）

组播地址不得用作 IPv6 数据包中的源地址。

注　IPv6 中没有广播地址。 IPv6 组播地址取代了广播地址。

任播地址

IPv6 任播地址是分配给多个接口的单播地址 （通常属于不同的节点）。路由至一个任播地址的数据包会路由至具有该地址的最近接口，接近度由所用的路由协议确定。

任播地址从单播地址空间中进行分配。任播地址是分配给多个接口的单播地址，这些接口必须配置为将该地址识别为任播地址。

以下限制适用于任播地址：

- 任播地址不能用作 IPv6 数据包的源地址。
- 任播地址不能分配给 IPv6 主机，而只能分配给 IPv6 路由器。

注　任播地址在 ASA 上不受支持。

必需地址

IPv6 主机必须至少配置有以下地址 （自动或手动）：

- 用于每个接口的链路本地地址
- 环回地址
- 全节点组播地址
- 用于每个单播或任播地址的请求节点组播地址

IPv6 路由器必须至少配置有以下地址 （自动或手动）：

- 必需的主机地址
- 用于被配置为用作路由器的所有接口的子网路由器任播地址
- 全路由器组播地址

IPv6 地址前缀

IPv6 地址前缀（其格式为 ipv6-prefix/prefix-length）可用于表示整个地址空间的连续比特块。IPv6 前缀必须采用 RFC 2373 规定的格式，在这种格式中，地址用十六进制的 16 位值指定，各个值之间用冒号分隔。前缀长度是十进制值，表示组成前缀（地址的网络部分）的地址高位连续位有多少。例如，2001:0DB8:8086:6502::/32 是有效的 IPv6 前缀。

IPv6 前缀识别 IPv6 地址的类型。表 43-5 显示了各种 IPv6 地址类型的前缀。

表 43-5　　IPv6 地址类型前缀

地址类型	二进制前缀	IPv6 记法
未指定	000...0（128 位）	::/128
环回	000...1（128 位）	::1/128
组播	11111111	FF00::/8
链路本地（单播）	1111111010	FE80::/10
站点本地（单播）	1111111111	FEC0::/10
全局（单播）	所有其他地址。	
任播	取自单播地址空间。	

协议和应用

表 43-6 列出了协议的文字值和端口号；两者均可在 ASA 命令中输入。

表 43-6　　协议文字值

文字	值	说明
ah	51	IPv6 的身份验证报头，RFC 1826。
eigrp	88	增强型内部网关路由协议。
esp	50	IPv6 的封装安全负载，RFC 1827。
gre	47	通用路由封装。

表 43-6　协议文字值（续）

文字	值	说明
icmp	1	互联网控制消息协议，RFC 792。
icmp6	58	IPv6 的互联网控制消息协议，RFC 2463。
igmp	2	互联网组管理协议，RFC 1112。
igrp	9	内部网关路由协议。
IP	0	互联网协议。
ipinip	4	IP-in-IP 封装。
ipsec	50	IP 安全。输入 ipsec 协议文字相当于输入 esp 协议文字。
nos	94	网络操作系统（Novell 的 NetWare）。
ospf	89	开放式最短路径优先路由协议，RFC 1247。
pcp	108	负载压缩协议。
pim	103	协议无关组播。
pptp	47	点对点隧道协议。输入 pptp 协议文字相当于输入 gre 协议文字。
snp	109	Sitara 网络协议。
tcp	6	传输控制协议，RFC 793。
udp	17	用户数据报协议，RFC 768。

可以在 IANA 网站上联机查看协议号：

http://www.iana.org/assignments/protocol-numbers

TCP 和 UDP 端口

表 43-7 列出了端口的文字值和端口号；两者均可在 ASA 命令中输入。请参阅以下说明：

- ASA 将端口 1521 用于 SQL*Net。这是 Oracle for SQL*Net 所用的默认端口。但是，此值与 IANA 端口分配不一致。
- ASA 侦听端口 1645 和 1646 上的 RADIUS。如果 RADIUS 服务器使用标准端口 1812 和 1813，可以将 ASA 配置为使用 **authentication-port** 和 **accounting-port** 命令侦听这些端口。
- 如要分配 DNS 访问的端口，请使用 **domain** 文字值，而不是 **dns**。如果使用 **dns**，则 ASA 会假设您打算使用 **dnsix** 文字值。

可以在 IANA 网站上联机查看端口号：

http://www.iana.org/assignments/port-numbers

表 43-7　端口文字值

文字	TCP 还是 UDP？	值	说明
aol	TCP	5190	美国在线
bgp	TCP	179	边界网关协议，RFC 1163
biff	UDP	512	供邮件系统用于通知用户新邮件已收到

表 43-7　端口文字值（续）

文字	TCP 还是 UDP？	值	说明
bootpc	UDP	68	Bootstrap 协议客户端
bootps	UDP	67	Bootstrap 协议服务器
chargen	TCP	19	字符生成器
citrix-ica	TCP	1494	Citrix 独立计算架构 (ICA) 协议
cmd	TCP	514	与 **exec** 类似，但 **cmd** 还具有自动身份验证
ctiqbe	TCP	2748	计算机电话接口快速缓冲区编码
daytime	TCP	13	白天，RFC 867
discard	TCP、UDP	9	丢弃
domain	TCP、UDP	53	DNS
dnsix	UDP	195	DNSIX 会话管理模块审核重定向器
echo	TCP、UDP	7	回显
exec	TCP	512	远程进程执行
finger	TCP	79	Finger
ftp	TCP	21	文件传输协议（控制端口）
ftp-data	TCP	20	文件传输协议（数据端口）
gopher	TCP	70	Gopher
https	TCP	443	使用 SSL 的 HTTP
h323	TCP	1720	H.323 呼叫信令
hostname	TCP	101	NIC 主机名服务器
ident	TCP	113	身份验证服务
imap4	TCP	143	互联网消息访问协议，版本 4
irc	TCP	194	互联网中继聊天协议
isakmp	UDP	500	互联网安全关联和密钥管理协议
kerberos	TCP、UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn Shell
ldap	TCP	389	轻量级目录访问协议
ldaps	TCP	636	轻量级目录访问协议 (SSL)
lpd	TCP	515	行式打印机后台守护程序 - 打印机后台打印程序
login	TCP	513	远程登录
lotusnotes	TCP	1352	IBM Lotus Notes
mobile-ip	UDP	434	移动 IP 代理
nameserver	UDP	42	主机名服务器
NetBIOS-ns	UDP	137	NetBIOS 名称服务
netbios-dgm	UDP	138	NetBIOS 数据报服务

表 43-7　端口文字值（续）

文字	TCP 还是 UDP？	值	说明
NetBIOS-ssn	TCP	139	NetBIOS 会话服务
nntp	TCP	119	网络新闻传输协议
ntp	UDP	123	网络时间协议
pcanywhere-status	UDP	5632	pcAnywhere 状态
pcanywhere-data	TCP	5631	pcAnywhere 数据
pim-auto-rp	TCP、UDP	496	协议无关组播，反向路径泛洪，密集模式
pop2	TCP	109	邮局协议 - 版本 2
POP3	TCP	110	邮局协议 - 版本 3
pptp	TCP	1723	点对点隧道协议
radius	UDP	1645	远程身份验证拨入用户服务
radius-acct	UDP	1646	远程身份验证拨入用户服务（计帐）
rip	UDP	520	路由信息协议
secureid-udp	UDP	5510	使用 UDP 的 SecureID
smtp	TCP	25	简单邮件传输协议
snmp	UDP	161	简单网络管理协议
snmptrap	UDP	162	简单网络管理协议 - 陷阱
sqlnet	TCP	1521	结构化查询语言网络
ssh	TCP	22	安全外壳
sunrpc (rpc)	TCP、UDP	111	Sun 远程过程调用
系统日志	UDP	514	系统日志
tacacs	TCP、UDP	49	增强型终端访问控制器访问控制系统
talk	TCP、UDP	517	通话
telnet	TCP	23	RFC 854 Telnet
tftp	UDP	69	简单文件传输协议
time	UDP	37	时间
uucp	TCP	540	UNIX 对 UNIX 复制程序
who	UDP	513	谁
whois	TCP	43	是谁
www	TCP	80	万维网
xdmcp	UDP	177	X 显示管理器控制协议

本地端口和协议

表 43-8 列出了 ASA 为了处理流向 ASA 的流量而打开的协议、TCP 端口和 UDP 端口。除非启用了表 43-8 中所列的功能和服务，否则，ASA *不会*打开任何本地协议或任何 TCP 或 UDP 端口。必须为 ASA 配置功能或服务，才能打开默认的侦听协议或断开。很多情况下，启用功能或服务后，可以配置除默认端口以外的端口。

表 43-8　按功能和服务打开的协议和端口

功能或服务	协议	端口号	备注
DHCP	UDP	67,68	-
故障转移控制	105	不适用	-
HTTP	TCP	80	-
HTTPS	TCP	443	-
ICMP	1	不适用	-
IGMP	2	不适用	协议只能在目标 IP 地址 224.0.0.1 上打开
ISAKMP/IKE	UDP	500	可配置。
IPsec (ESP)	50	不适用	-
通过 UDP 的 IPsec (NAT-T)	UDP	4500	-
通过 UDP 的 IPsec（兼容思科 VPN 3000 系列）	UDP	10000	可配置。
通过 TCP 的 IPsec (CTCP)	TCP	-	未使用默认端口。配置通过 TCP 的 IPsec 时，必须指定端口号。
NTP	UDP	123	-
OSPF	89	不适用	协议只能在目标 IP 地址 224.0.0.5 和 224.0.0.6 上打开
PIM	103	不适用	协议只能在目标 IP 地址 224.0.0.13 上打开
RIP	UDP	520	-
RIPv2	UDP	520	端口只能在目标 IP 地址 224.0.0.9 上打开
SNMP	UDP	161	可配置。
SSH	TCP	22	-
状态更新	8（非安全）9（安全）	不适用	-
Telnet	TCP	23	-
VPN 负载均衡	UDP	9023	可配置。
VPN 个人用户身份验证代理	UDP	1645、1646	端口只能通过 VPN 隧道访问。

ICMP 类型

表 43-9 列出了可以在 ASA 命令中输入的 ICMP 类型编号和名称。

表 43-9　　ICMP 类型

ICMP 编号	ICMP 名称
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect