

思科 ASA 系列常规操作 CLI 配置指南

软件版本 9.4
适用于 ASA 5506-X、 ASA 5506H-X、 ASA 5506W-X、 ASA 5508-X、 ASA 5512-X、 ASA 5515-X、 ASA 5516-X、 ASA 5525-X、 ASA 5545-X、 ASA 5555-X、 ASA 5585-X、 ASA 服务模块和自适应安全虚拟设备

首次发行日期：2015 年 3 月 23 日
最后更新日期：2015 年 4 月 7 日

思科系统公司
www.cisco.com

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

文本部件号：不适用，仅在线提供

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 信压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

无论在该手册中是否作出了其他担保，来自这些供应商的所有文档文件和软件都按“原样”提供且仍有可能存在缺陷。思科和上述供应商不承诺所有明示或暗示的担保，包括（但不限于）对特定用途的适销性、适用性、非侵权性以及因交易、使用或商业惯例所衍生的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请转至此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科 ASA 系列常规操作 CLI 配置指南
© 2015 思科系统公司。版权所有。



关于本指南

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

文档目标

本指南旨在帮助您使用命令行界面为思科 ASA 系列配置常规操作。本指南仅介绍最常见的一些配置场景，并未涵盖所有功能。

您也可以使用思科自适应安全设备管理器 (ASDM)（一种基于 Web 的 GUI 应用）来配置和监控 ASA。ASDM 提供配置向导指导您完成一些常见配置场景，并提供联机帮助以使您获得不常见场景的信息。

本指南中，术语 “ASA” 一般适用于所支持的型号，除非另有说明。

相关文档

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

约定

本文档使用下列约定：

约定	说明
粗体	命令和关键字及用户输入的文本以**粗体**显示。
斜体	文档标题、新出现或强调的术语，以及要为其提供数值的参数以*斜体*显示。
[ ]	方括号中的元素是可选项。
{x | y | z }	必需的备选关键字集中在大括号内，以竖线分隔。
[x | y | z]	可选的备选关键字集中在方括号内，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，否则会将引号视为字符串的一部分。
`courier` 字体	系统显示的终端会话和信息以 `courier` 字体显示。
`courier` **粗体**	命令和关键字及用户输入的文本以 **`courier`** **粗体**显示。
`courier` *斜体*	需要提供值的参数以 *`courier`* *斜体*显示。
< >	非打印字符 （如密码）括在尖括号中。
[ ]	系统提示的默认回复括在方括号中。
!， #	代码行开头的感叹号 (!) 或井字号 (#) 表示注释行。

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

获取文档和提交服务请求

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

通过 RSS 摘要的方式订阅*思科产品文档更新*，其中列出了所有最新及修订的思科技术文档，相关内容将通过阅读器应用程序直接发送至您的桌面。RSS 摘要是一种免费服务。



第 1 部分

ASA 入门



思科 ASA 简介

首次发行日期：2015 年 3 月 23 日
最后更新日期：2015 年 4 月 7 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 支持以及许多其他功能。

- 硬件和软件兼容性，第 1-1 页
- VPN 兼容性，第 1-1 页
- 新功能，第 1-1 页
- 防火墙功能概述，第 1-8 页
- VPN 功能概述，第 1-11 页
- 安全情景概述，第 1-12 页
- ASA 集群概述，第 1-12 页
- 特殊和传统服务，第 1-12 页

硬件和软件兼容性

有关受支持硬件和软件的完整列表，请参阅思科 ASA 兼容性

VPN 兼容性

请参阅支持的 VPN 平台（思科 ASA 系列）。

新功能

发布日期：2015 年 3 月 23 日

下表列出了 ASA 9.4(1) 版的新功能。

表 1-1　ASA 9.4(1) 版的新功能

功能	描述
平台功能	
ASA 5506W-X、 ASA 5506H-X、ASA 5508-X 和 ASA 5516-X	引入了以下型号：带有无线接入点的 ASA 5506W-X、强化型 ASA 5506H-X、 ASA 5508-X 和 ASA 5516-X。 引入了以下命令：**hw-module module wlan recover image** 和 **hw-module module wlan recover image**。
认证功能	
美国国防部统一功能要求 (UCR) 2013 认证	更新了 ASA，以满足 DoD UCR 2013 要求。请参阅下表中的各行，了解下列为 UCR 2013 认证添加的功能： • 定期证书身份验证 • 证书到期警报 • 执行基本约束 CA 标记 • 从证书配置 ASDM 用户名 • IKEv2 无效选择器通知配置 • IKEv2 十六进制预共享密钥
FIPS 140-2 认证合规更新	当在 ASA 上启用 FIPS 模式时，将会对 ASA 实施其他限制，以使其符合 FIPS 140-2。限制包括： • RSA 和 DH 密钥大小限制 - 仅允许使用大小为 2K（2048 位）或以上的 RSA 和 DH 密钥。对于 DH，这意味着不允许使用第 1 组 （768 位）、第 2 组 （1024 位）和第 5 组 （1536 位）密钥。 **注意：**密钥大小限制禁止 IKEv1 与 FIPS 结合使用。 • 数字签名的散列算法限制 - 仅允许使用 SHA256 或更安全的算法。 • SSH 密码限制 - 允许的密码为：aes128-cbc 或 aes256-cbc。MAC：SHA1 要查看 ASA 的 FIPS 认证状态，请参阅： http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf 此 PDF 每周更新一次。 有关详细信息，请访问计算机安全部门的计算机安全资源中心网站： http://csrc.nist.gov/groups/STM/cmvp/inprocess.html 修改了以下命令：**fips enable**
防火墙功能	
改进了多核心 ASA 的 SIP 检测性能。	如果有多条 SIP 信令流通过具有多核心的 ASA，则表明 SIP 检测性能已经过改进。但是，如果您使用的是 TLS、电话或 IME 代理，则不会看到性能改进。 未修改任何命令。

表 1-1　　ASA 9.4(1) 版的新功能 （续）

功能	描述
取消了对电话代理和 UC-IME 代理的 SIP 检测支持。	当配置 SIP 检测后，您将无法再使用电话代理或 UC-IME 代理。使用 TLS 代理检测加密流量。 删除了以下命令：**phone-proxy** 和 **uc-ime**。从 **inspect sip** 命令中删除了 **phone-proxy** 和 **uc-ime** 关键字。
DCERPC 检测支持 ISystemMapper UUID 消息 RemoteGetClassObject opnum3。	ASA 从版本 8.3 开始支持非 EPM DCERPC 消息，支持 ISystemMapper UUID 消息 RemoteCreateInstance opnum4。此更改扩展了对 RemoteGetClassObject opnum3 消息的支持。 未修改任何命令。
每个情景的 SNMP 服务器陷阱主机数没有限制	ASA 支持每个情景的 SNMP 服务器陷阱主机数不受限制。**show snmp-server host** 命令输出仅显示正在轮询 ASA 的活动主机，以及静态配置的主机。 修改了以下命令：**show snmp-server host**。
VXLAN 数据包检测	ASA 可检测 VXLAN 报头以强制遵守标准格式。 引入了以下命令：**inspect vxlan**。
IPv6 的 DHCP 监控	您现在可以监控 IPv6 的 DHCP 统计信息和 DHCP 绑定。
高可用性功能	
阻止在备用 ASA 上生成系统日志	您现在可以阻止在备用设备上生成特定系统日志。 引入了以下命令：**no logging message** *syslog-id* **standby**。
按接口启用和禁用 ASA 集群运行状况监控	您现在可以按接口启用或禁用运行状况监控。默认情况下，运行状况监控在所有端口通道冗余接口和单一物理接口上处于启用状态。运行状况监控不在 VLAN 子接口或虚拟接口 （例如， VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。您可能想禁用不重要的接口 （例如管理接口）的运行状况检查。 引入了以下命令：**health-check monitor-interface**。
DHCP 中继的 ASA 集群支持	现在可以在 ASA 集群上配置 DHCP 中继。通过使用客户端 MAC 地址散列，使客户端 DHCP 请求在集群成员中实现了负载均衡。仍然不支持 DHCP 客户端和服务器功能。 引入了以下命令：**debug cluster dhcp-relay**
ASA 集群中的 SIP 检测支持	您现在可以在 ASA 集群上配置 SIP 检测。控制流可以在任何设备上创建 （由于负载均衡），但其子数据流必须驻留在同一设备上。不支持 TLS 代理配置。 引入了以下命令：**show cluster service-policy**

表 1-1　　ASA 9.4(1) 版的新功能 （续）

功能	描述
路由功能	
基于策略的路由	基于策略的路由 (PBR) 是一种机制，基于该机制，流量可以使用 ACL，通过带有指定 QoS 的特定路径进行路由。基于数据包的第 3 层和第 4 层报头的内容， ACL 可以对流量进行分类。管理员通过此解决方案可向不同的流量提供 QoS，在低带宽、低成本永久路径与高带宽、高成本交换式路径之间分发交互式和批处理流量，并允许互联网运营商和其他组织通过明确定义的互联网连接来路由源自各类用户的流量。 引入了以下命令：**set ip next-hop verify-availability**、 **set ip next-hop**、 **set ip next-hop recursive**、 **set interface**、 **set ip default next-hop**、 **set default interface**、 **set ip df**、 **set ip dscp**、 **policy-route route-map**、 **show policy-route** 和 **debug policy-route**
接口功能	
VXLAN 支持	增加了 VXLAN 支持，包括 VXLAN 隧道终端 (VTEP) 支持。每个 ASA 或安全情景可以定义一个 VTEP 源接口。 引入了以下命令：**debug vxlan**、 **default-mcast-group**、 **encapsulation vxlan**、 **inspect vxlan**、 **interface vni**、 **mcast-group**、 **nve**、 **nve-only**、 **peer ip**、 **segment-id**、 **show arp vtep-mapping**、 **show interface vni**、 **show mac-address-table vtep-mapping**、 **show nve**、 **show vni vlan-mapping**、 **source-interface**、 **vtep-nve** 和 **vxlan port**
监控功能	
EEM 的内存跟踪	添加了一项新的调试功能来记录内存分配和内存使用情况，以响应内存日志记录封装事件。 引入或修改了以下命令：**memory logging**、 **show memory logging**、 **show memory logging include** 和 **event memory-logging-wrap**。
对崩溃进行故障排除	**show tech-support** 命令输出和 **show crashinfo** 命令输出包含最新生成的 50 行系统日志。请注意，必须启用 **logging buffer** 命令才能出现这些结果。
远程访问功能	

表 1-1　　ASA 9.4(1) 版的新功能 （续）

功能	描述
支持 ECDHE-ECDSA 密码	TLSv1.2 增加了对以下密码的支持： • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 **注意：**ECDSA 和 DHE 密码具有最高优先级。 引入了以下命令：**ssl ecdh-group**。
无客户端 SSL VPN 会话 Cookie 访问限制	您现在可以防止第三方通过 JavaScript 等客户端侧脚本访问无客户端 SSL VPN 会话 Cookie。 **注意：**请仅遵照思科 TAC 的建议使用此功能。启用此功能会引发安全风险，因为系统在以下无客户端 SSL VPN 功能不运行时不提供任何警告。 • Java 插件 • Java 重写工具 • 端口转发 • 文件浏览器 • 需要桌面应用的 Sharepoint 功能 （例如 MS Office 应用） • AnyConnect Web 启动 • Citrix Receiver、 XenDesktop 和 Xenon • 其他不基于浏览器和浏览器插件的应用 引入了以下命令：**http-only-cookie**。 *9.2(3) 中也包含此功能。*

表 1-1　　ASA 9.4(1) 版的新功能 （续）

功能	描述
使用安全组标记的虚拟桌面访问控制	ASA 现在支持基于安全组标记的策略控制，从而可对内部应用和网站进行无客户端 SSL 远程访问。此功能将 Citrix 的虚拟桌面基础架构 (VDI) 与 XenDesktop 配合使用，将其用作交付控制器和 ASA 的内容转换引擎。 有关详细信息，请参阅以下 Citrix 产品文档： • 用于 XenDesktop 和 XenApp 的策略：http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html • 管理 XenDesktop 7 中的策略：http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-wrapper-rho.html • 将组策略编辑器用于 XenDesktop 7 策略：http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-use-gpmc.html
为无客户端 SSL VPN 添加了 OWA 2013 功能支持	无客户端 SSL VPN 支持 OWA 2013 中除以下功能外的新功能： • 支持平板电脑和智能手机 • 离线模式 • Active Directory 联合身份验证服务 (AD FS) 2.0。ASA 和 AD FS 2.0 无法协商加密协议。 未修改任何命令。

表 1-1　　ASA 9.4(1) 版的新功能 （续）

功能	描述
为无客户端 SSL VPN 添加了 Citrix XenDesktop 7.5 和 StoreFront 2.5 支持	无客户端 SSL VPN 支持访问 XenDesktop 7.5 和 StoreFront 2.5。 有关 XenDesktop 7.5 功能的完整列表以及详细信息，请参阅 http://support.citrix.com/proddocs/topic/xenapp-xendesktop-75/cds-75-about-whats-new.html。 有关 StoreFront 2.5 功能的完整列表以及详细信息，请参阅 http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-about.html。 未修改任何命令。
定期证书身份验证	启用定期证书身份验证时， ASA 存储从 VPN 客户端接收的证书链，并且定期重新进行身份验证。 引入或修改了以下命令：**periodic-authentication certificate**、 **revocation-check** 和 **show vpn-sessiondb**
证书到期警报	ASA 每 24 小时检查一次信任点中的所有 CA 和 ID 证书是否到期。如果证书即将到期，则会将一条系统日志作为警报发出。可以配置提醒和重现间隔。默认情况下，提醒将在到期之前 60 天启动，每 7 天重现一次。 引入或修改了以下命令：**crypto ca alerts expiration**
执行基本约束 CA 标记	默认情况下，现在不带 CA 标记的证书无法作为 CA 证书安装在 ASA 上。基本约束扩展标可确定证书的主题是否为 CA，及包含此证书的有效证书路径的最大深度。如果需要，可将 ASA 配置为允许安装这些证书。 引入了以下命令：**ca-check**
IKEv2 无效选择器通知配置	目前，如果 ASA 在 SA 上接收到入站数据包，并且数据包的报头字段与 SA 的选择器不一致，则 ASA 会丢弃该数据包。您现在可以启用或禁用向对等方发送 IKEv2 通知。默认情况下禁用发送此通知。 **注意：**在 AnyConnect 3.1.06060 和更高版本中支持此功能。 引入了以下命令：**crypto ikev2 notify invalid-selectors**
IKEv2 十六进制预共享密钥	您现在可以配置十六进制形式的 IKEv2 预共享密钥。 引入了以下命令：**ikev2 local-authentication pre-shared-key hex** 和 **ikev2 remote-authentication pre-shared-key hex**
管理功能	
从证书配置 ASDM 用户名	利用此功能，能够通过从证书提取用户名以及使用由用户提供的用户名对 ASDM 用户进行授权。 引入了以下命令：**aaa authorization http console** 和 **http username-from-certificate**

表 1-1　　ASA 9.4(1) 版的新功能 （续）

功能	描述
terminal interactive 命令用于在 CLI 处输入 **?** 时启用或禁用帮助	通常，当在 ASA CLI 输入 **?** 时，会显示命令帮助。要支持输入 **?** 作为命令中的文本（例如，将 **?** 加入 URL 中），可以使用 **no terminal interactive** 命令禁用交互式帮助。 引入了以下命令：**terminal interactive**
REST API 版本 1.1	添加了对 REST API 1.1 版的支持。

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。防火墙同时可以为不同的内部网络提供保护，例如将人力资源网络与用户网络分开。如果需要向外部用户提供某些网络资源（例如 Web 服务器或 FTP 服务器），可以将这些资源放置在防火墙后面单独的网络上 （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，因此发生在这个位置的攻击只会影响到服务器，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*网络受到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 [如果需要]），这些术语仅具有一般意义。

- 安全策略概述，第 1-8 页
- 防火墙模式概述，第 1-10 页
- 状态检测概述，第 1-10 页

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）。可以将操作应用于流量，以自定义安全策略。

- 通过访问列表允许或拒绝，第 1-9 页
- 应用 NAT，第 1-9 页
- 保护 IP 分片，第 1-9 页
- 应用 HTTP、 HTTPS 或 FTP 过滤，第 1-9 页
- 应用应用检测，第 1-9 页
- 向受支持的硬件或软件模块发送流量，第 1-9 页
- 应用 QoS 策略，第 1-9 页
- 应用连接限制和 TCP 规范化，第 1-9 页
- 启用威胁检测，第 1-10 页

通过访问列表允许或拒绝

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 EtherType 访问列表来允许非 IP 流量。

应用 NAT

NAT 的一些优势如下：

- 可以在内部网络上使用专用地址。专用地址不能在互联网上进行路由。
- NAT 可隐藏其他网络的本地地址，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。系统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。

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合实际。

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）。您还可以将 ASA 与思科网络安全设备 (WSA) 等外部产品结合使用。

应用应用检测

针对在用户数据包内嵌入 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来阻止流量。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 （例如声音和流传输视频）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遭受 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）。半开连接是源与目标之间尚未完成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信息来分析威胁。

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。

典型的扫描攻击包含测试子网中每个 IP 地址可达性 （通过扫描子网中的多台主机或扫描主机或子网中的多个端口）的主机。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包含可分析扫描活动的主机统计信息的广泛数据库。

主机数据库跟踪可疑的活动 （例如没有返回活动的连接、访问关闭的服务端口、如非随机 IPID 等易受攻击的 TCP 行为以及更多行为）。

可以将 ASA 配置为发送关于攻击者的系统日志消息，也可以自动回避该主机。

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 “隐藏防火墙”，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。还可以针对在路由模式中会以其他方式被阻止的流量使用透明防火墙。例如，透明防火墙可通过 EtherType 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，检测后的流量或者允许通过，或者被丢弃。简单的数据包过滤器可以检查源地址、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。

备注　TCP 状态绕行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。要执行这项检查，会话的第一个数据包需要通过 “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。

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

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 （一个使用已知端口号的数据信道，一个对每个会话使用不同端口号的控制信道，）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？

  如果连接已经建立， 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 是一个跨 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入站和出站数据传输

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 分区成多台虚拟设备，这些虚拟设备称为安全情景。每个情景都是一台独立设备，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，某些功能不受支持。有关详细信息，请参阅介绍功能的章节。

在多情景模式下， ASA 包括每个情景的配置，此类配置用于标识安全策略、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，是启动配置。系统配置可标识 ASA 的基本设置。系统配置本身并不包含任何网络接口或网络设置；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某个情景。

管理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，您可以将多台 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 （引导程序配置除外）；然后配置将被复制到成员设备中。

特殊和传统服务

对于某些服务，可以在主配置指南和在线帮助以外找到相关文档。有关指南的完整列表，请参阅导航思科 ASA 系列文档。

- 特殊服务指南，第 1-12 页
- 传统服务指南，第 1-12 页

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。

- 访问命令行界面的控制台，第 2-1 页
- 配置 ASDM 访问，第 2-7 页
- 启动 ASDM，第 2-12 页
- 出厂默认配置，第 2-13 页
- 处理配置，第 2-18 页
- 将配置更改应用于连接，第 2-22 页
- 重新加载 ASA，第 2-22 页

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。之后可根据第 32 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。

备注 有关 ASAv 控制台访问，请参阅 《ASAv 快速入门指南》。

- 访问设备控制台，第 2-1 页
- 访问 ASA 服务模块控制台，第 2-2 页
- 访问软件模块控制台，第 2-6 页
- 访问 ASA 5506W-X 无线接入点控制台，第 2-7 页

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计算机连接到控制台端口，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** 键将看到以下提示符：

```
ciscoasa>
```

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

步骤 3　要访问特权 EXEC 模式，请输入以下命令：

```
ciscoasa> enable
```

系统将显示以下提示：

```
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** 键继续操作。要更改启用密码，请参阅设置主机名、域名及启用密码和 Telnet 密码，第 16-1 页。

提示符更改为：

```
ciscoasa#
```

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

步骤 5　要访问全局配置模式，请输入以下命令：

```
ciscoasa# configure terminal
```

提示将更改为以下形式：

```
ciscoasa(config)#
```

可从全局配置模式开始配置 ASA。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，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。

- 关于连接方法，第 2-2 页
- 登录 ASA 服务模块，第 2-3 页
- 注销控制台会话，第 2-5 页
- 断开活动控制台连接，第 2-5 页
- 注销 Telnet 会话，第 2-6 页

关于连接方法

可以使用两种方法从交换机 CLI 连接到 ASASM：

- 虚拟控制台连接 - 通过使用 **service-module session** 命令，可创建到 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。

  您可以获得以下优势：

  - 在重新加载时连接会保持，不会超时。
  - 可以通过 ASASM 重新加载保持连接并查看启动消息。

- 如果 ASASM 无法加载镜像，可以访问 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；无法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到交换机提示符。在这种情况下，请更改终端服务器或思科 IOS 软件中的交换机转义字符，或改用 Telnet **session** 命令。

注意　由于控制台连接具有持久性，因此如果未能正确注销 ASASM，则该连接存在的时间可能超过预期。如果其他人希望登录，他们需要先中断现有连接。

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

注意　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。

您可以获得以下优势：

- 可以同时拥有多个到 ASASM 的会话。
- Telnet 会话是快速连接。

限制包括：

- Telnet 会话在 ASASM 重新加载时终止，并且可能会超时。
- 在 ASASM 完全加载之前无法访问它；不能访问 ROMMON。
- 必须首先设置 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，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。

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

将进入用户 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。

  其他服务模块支持的 **session** *slot* **processor 0** 命令在 ASASM 上不受支持；ASASM 没有处理器 0。

  要查看模块插槽编号，请在交换机提示符下输入 **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。

  将进入用户 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。

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

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

相关主题

- 管理访问规定，第 32-1 页
- 设置主机名、域名及启用密码和 Telnet 密码，第 16-1 页

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。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，请参阅断开活动控制台连接，第 2-5 页。

操作步骤

步骤 1　要返回交换机 CLI，请键入以下信息：

Ctrl-Shift-6, **x**

将返回交换机提示符：

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

注意　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。如果其他人希望登录，他们需要先中断现有连接。

操作步骤

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

```
Router# show users
```

例如，以下命令输出显示位于模块插槽 2 中 0 行的用户 “con”：

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

步骤 2　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

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　要返回交换机 CLI，请从 ASASM 特权模式或用户 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。

将返回交换机提示符：

```
asasm# exit
Router#
```

注意　或者，也可使用转义序列 **Ctrl-Shift-6**, **x** 转义 Telnet 会话；该转义序列使您可以通过在交换机提示符处按 **Enter** 键来恢复 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，会话最终会根据 ASASM 配置超时。

访问软件模块控制台

如果已安装软件模块，例如，在 ASA 5506-X 上已安装 ASA FirePOWER 模块，则可以发起到模块控制台的会话。

备注　无法使用 **session** 命令访问 ASA 背板上的*硬件*模块 CLI。

操作步骤

步骤 1　从 ASA CLI 发起到模块的会话：

session {**sfr** | **cxsc** | **ips**} **console**

示例：

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

访问 ASA 5506W-X 无线接入点控制台

要访问无线接入点控制台，请执行以下步骤。

操作步骤

步骤 1　从 ASA CLI 发起到接入点的会话：

```
session wlan console
```

示例：

```
ciscoasa# session wlan console
opening console session with module wlan
connected to module wlan. Escape character sequence is  'CTRL-^X'

ap>
```

步骤 2　有关接入点 CLI 的详细信息，请参阅 《自主 Aironet 接入点思科 IOS 配置指南》。

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。

- 使用出厂默认配置进行 ASDM 访问 （设备、 ASAv），第 2-7 页
- 为设备和 ASAv 自定义 ASDM 访问，第 2-8 页
- 为 ASA 服务模块配置 ASDM 访问，第 2-10 页

使用出厂默认配置进行 ASDM 访问 （设备、 ASAv）

通过出厂默认配置，已采用默认网络设置对 ASDM 连接进行了预配置。

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 5506-X、 ASA 5508-X 和 ASA 5516-X - 要连接到 ASDM 的接口是 GigabitEthernet 1/2。
  - 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 - 在部署过程中设置管理接口 IP 地址。

- 允许访问 ASDM 的客户端：
  - ASA 设备 - 客户端必须位于 192.168.1.0/24 网络中。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 - 在部署过程中设置管理客户端 IP 地址。ASAv 不充当已连接客户端的 DHCP 服务器。

备注　如果更改为多情景模式，则可使用上述网络设置从管理情景访问 ASDM。

相关主题

- 出厂默认配置，第 2-13 页
- 启用或禁用多情景模式，第 6-14 页
- 启动 ASDM，第 2-12 页

为设备和 ASAv 自定义 ASDM 访问

如果满足*一个或多个*以下条件，可使用该程序：

- 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，才应使用本节所述程序。

备注　对于 ASAv，可以在部署过程中配置透明模式，所以此程序主要用在类似于部署之后需要清除配置等情况。

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：

该命令清除您的配置。

```
firewall transparent
```

步骤 3　配置管理接口：

```
interface interface_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接口地址。

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

出现提示时，请确认要将现有配置转换为管理情景。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

- 恢复出厂默认配置，第 2-14 页
- 设置防火墙模式，第 5-7 页
- 访问设备控制台，第 2-1 页
- 启动 ASDM，第 2-12 页
- 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，因此不会进行预配置以用于 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》将一个 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
```

该命令清除您的配置。

步骤 3　根据您使用的模式，执行以下操作之一，以配置管理接口：

- 路由模式 - 在路由模式下配置接口：

```
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，并将一个管理 VLAN 分配至网桥组：

```
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　（对于直连管理主机）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

出现提示时，请确认要将现有配置转换为管理情景。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 接口并将其分配至 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

- 访问 ASA 服务模块控制台，第 2-2 页
- 第 6 章 “多情景模式”
- 设置防火墙模式，第 5-7 页

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。如果要连接到其他 ASA，无需重现下载该启动程序。通过该启动程序，也可使用本地下载的文件以演示模式运行虚拟 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计算机；但每个 ASA IP 地址均需单独的快捷方式。

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。

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 客户端的计算机上，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　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，可以在没有用户名和 **enable** 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. 将安装程序保存到计算机，然后启动安装程序。安装完成后，将自动打开 ASDM-IDM 启动程序。

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　要使用 Java Web Start，请执行以下操作：

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

b. 出现提示时，将快捷方式保存到计算机上。或者，也可以选择打开快捷方式，而不是保存快捷方式。

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对新的 ASA 应用的配置。

- 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 - 取决于虚拟机监控程序，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。还可以配置故障切换 IP 地址。还可应用 “出厂默认”配置 （如果需要）。
- ASASM - 无默认配置。要开始配置，请参阅访问 ASA 服务模块控制台，第 2-2 页。

对于设备，出厂默认配置仅可用于路由防火墙模式和单一情景模式。对于 ASAv，可以在部署时选择透明模式或路由模式。

备注　除映像文件和 （隐藏的）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与闪存中映像文件的日期不匹配。这些文件有助于潜在的故障排除；它们不表示已发生故障。

- 恢复出厂默认配置，第 2-14 页
- 恢复 ASAv 部署配置，第 2-14 页
- ASA 5506-X、 5508-X 和 5516-X 默认配置，第 2-15 页
- ASA 5512-X、 5515-X、 5525-X 及更高型号默认配置，第 2-16 页
- ASAv 部署配置，第 2-16 页

恢复出厂默认配置

本节介绍如何恢复出厂默认配置。对于 ASAv，该程序可擦除部署配置并对各 ASA 设备应用相同的出厂默认配置。

备注　在 ASASM 上，恢复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　恢复出厂默认配置：

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。同样， **dhcpd address** 命令范围包含指定子网内的地址。

此命令还将清除 **boot system** 命令 （如果存在）和其他配置。**boot system** 命令使您可以从特定映像上启动，包括外部闪存卡上的映像。下次在恢复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也是如此；配置清除后，该路径也将清除。

恢复 ASAv 部署配置

本节介绍如何恢复 ASAv 部署 （第 0 天）配置。

操作步骤

步骤 1　为了执行故障切换，请关闭备用设备。

为防止备用设备变成主用设备，必须将其关闭。如果让其处于打开状态，则当清除主用设备配置后，备用设备将变为主用设备。当原来的主用设备重新加载并且通过故障切换链路重新连接后，旧配置将从新主用设备同步，并且擦除所需要的部署配置。

步骤 2　重新加载后，恢复部署配置。为了执行故障切换，请在主用设备上输入以下命令：

write erase

备注　ASAv 会启动当前运行的映像，因此，不会恢复到原始启动映像。要使用原始启动映像，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　为了执行故障切换，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 5506-X、 5508-X 和 5516-X 默认配置

ASA 5506-X 系列、 5508-X 和 5516-X 的默认出厂配置如下：

- 内部 --> 外部流量 - GigabitEthernet 1/1 （外部）、 GigabitEthernet 1/2 （内部）
- 从 DHCP 的外部 IP 地址，内部 IP 地址 - 192.168.1.1
- (ASA 5506W-X) WiFi <--> 内部， WiFi --> 外部流量 - GigabitEthernet 1/9 (WiFi)
- (ASA 5506W-X) WiFi IP 地址 - 192.168.10.1
- 内部和 WiFi 中客户端的 DHCP。接入点本身及其所有客户端均将 ASA 用作 DHCP 服务器。
- Management 1/1 接口启用，但未进行其他配置。然后，ASA FirePOWER 模块可以使用此接口访问 ASA 内部网络并将此内部接口用作互联网网关。
- ASDM 访问 - 允许内部和 WiFi 主机。
- NAT - 适用于从内部、 WiFi 和管理到外部的所有流量的接口 PAT

配置由以下命令组成：

```
interface Management1/1
    management-only
    no nameif
    no security-level
    no ip address
    no shutdown
interface GigabitEthernet1/1
    nameif outside
    security-level 0
    ip address dhcp setroute
    no shutdown
interface GigabitEthernet1/2
    nameif inside
    security-level 100
    ip address 192.168.1.1 255.255.255.0
    no shutdown
object network obj_any
    subnet 0.0.0.0 0.0.0.0
    nat (any,outside) dynamic interface
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
```

```
dhcpd enable inside
logging asdm informational
```

对于 ASA 5506W-X，还包括以下命令：

```
same-security-traffic permit inter-interface
    interface GigabitEthernet 1/9
    security-level 100
    nameif wifi
    ip address 192.168.10.1 255.255.255.0
    no shutdown
http 192.168.10.0 255.255.255.0 wifi
dhcpd address 192.168.10.2-192.168.10.254 wifi
dhcpd enable wifi
```

ASA 5512-X、 5515-X、 5525-X 及更高型号默认配置

ASA 5512-X、 5515-X、 5525-X 及更高型号的默认出厂配置如下：

- 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计算机可接收介于 192.168.1.2 和 192.168.1.254 之间的地址。
- ASDM 访问 - 允许管理主机。

配置由以下命令组成：

```
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：

- 路由或透明防火墙模式
- Management 0/0 接口：
  - 命名为“management”
  - IP 地址或 DHCP
  - 安全级别为 0
  - 管理专用
- 管理主机 IP 地址的静态路由 （如果其没有位于管理子网中）

- 启用或禁用 HTTP 服务器
- 管理主机 IP 地址的 HTTP 访问
- （可选） GigabitEthernet 0/8 的故障切换链路 IP 地址和 Management0/0 备用 IP 地址
- DNS 服务器
- 智能许可 ID 令牌
- 智能许可吞吐量水平和标准功能层
- （可选） Smart Call Home HTTP 代理 URL 和端口
- （可选） SSH 管理设置：
  - 客户端 IP 地址
  - 本地用户名和密码
  - 使用本地数据库进行 SSH 所需的身份验证
- （可选）启用或禁用 REST API



备注　要向思科许可颁发机构成功注册 ASAv，ASAv 需要访问互联网。部署之后，可能需要执行其他配置，以实现互联网访问和成功注册许可证。

有关独立设备，请参阅以下配置示例：

```
interface Management0/0
    nameif management
    security-level 0
    ip address ip_address
    management-only
    no shutdown
http server enable
http managemment_host_IP mask management
route management management_host_IP mask gateway_ip 1
dns server-group DefaultDNS
    name-server ip_address
call-home
    http-proxy ip_address port port
license smart
    feature tier standard
    throughput level {100M | 1G | 2G}
license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
```

有关故障切换对中的主要设备，请参阅以下配置示例：

```
interface Management0/0
    nameif management
    security-level 0
    ip address ip_address standby standby_ip
    management-only
    no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
dns server-group DefaultDNS
    name-server ip_address
call-home
    http-proxy ip_address port port
```

```
license smart
    feature tier standard
    throughput level {100M | 1G | 2G}
license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
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，仅对内存中的运行配置进行更改。必须将运行配置手动保存到启动配置，以便重新启动后更改仍旧有效。

除非另有说明，否则本节中的信息适用于单一安全情景和多安全情景。

- 保存配置更改，第 2-18 页
- 将启动配置复制到运行配置，第 2-20 页
- 查看配置，第 2-20 页
- 清除和删除配置设置，第 2-21 页
- 离线创建文本配置文件，第 2-21 页

保存配置更改

本节介绍如何保存配置。

- 在单一情景模式下保存配置更改，第 2-18 页
- 在多情景模式下保存配置更改，第 2-19 页

在单一情景模式下保存配置更改

要将运行配置保存到启动配置，请执行以下程序。

操作步骤

步骤 1　将运行配置保存到启动配置中。

```
write memory
```

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

在多情景模式下保存配置更改

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。

- 分别保存每个情景和系统，第 2-19 页
- 同时保存所有情景配置，第 2-19 页

分别保存每个情景和系统

使用以下程序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，情景启动配置可以驻留在外部服务器。在这种情况下，ASA 将配置保存回在情景 URL 中确定的服务器，但是 HTTP 或 HTTPS URL（不允许将配置保存到服务器）除外。

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

同时保存所有情景配置

使用以下程序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：

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

输入 **Y** 后，ASA 将保存系统配置和每个情景。情景启动配置可驻留在外部服务器上。在这种情况下，ASA 将配置保存回在情景 URL 中确定的服务器，但是 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，情景因错误而无法保存。请参阅以下错误的相关信息：

- 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
  ```

- 对于因无法到达远程目标而未保存的情景，系统将显示以下消息：

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

- 对于因情景被锁定而无法保存的情景，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’ .
```

仅当另一位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，在 HTTP 服务器上），在所有其他消息的末尾将显示以下消息报告：

```
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**

  将启动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到运行配置中。如果配置相同，则不会发生任何更改。如果命令冲突或命令影响情景的运行，则合并的影响取决于命令。可能会发生错误，也可能出现意外结果。

- **reload**

  重新加载 ASA，其加载启动配置并丢弃运行配置。

- **clear configure all**，然后 **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。

清除和删除配置设置

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。在这种情况下，可使用 **no** 命令删除 *qualifier* 识别的特定配置。

  例如，要删除特定 **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**

  清除启动配置。

注意　对于 ASAv，此命令将在重新加载后恢复部署配置。要完全擦除配置，请使用 **clear configure all** 命令。

- **clear configure all**

  擦除运行配置。

注意　在多情景模式下，如果从系统配置输入 **clear configure all**，还将删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。

此命令还将清除 **boot system** 命令（如果存在）和其他配置。**boot system** 命令使您可以从特定映像上启动，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，则可以直接在计算机上编辑文本文件，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 33 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
```

有关格式化文件的其他信息，请参阅附录 39 “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在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，如果要从接口删除 QoS **service-policy**，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。

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。

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，例如连接限制和初始化限制。因此，该命令可删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-host 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 **all** 关键字。要清除特定 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 **all** 关键字。要根据源 IP 地址、目标 IP 地址、端口和/或协议清除特定连接，可以指定所需选项。

重新加载 ASA

要重新加载 ASA，请完成以下程序。

操作步骤

步骤 1　重新加载 ASA：

```
reload
```

注意　在多情景模式下，仅可从系统执行空间重新加载。



产品授权密钥许可证

许可证指定在给定思科 ASA 上启用的选项。本文档介绍所有物理 ASA 的产品授权密钥 (PAK) 许可证。有关 ASAv 的信息，请参阅第 4 章 “适用于 ASAv 的智能软件许可”。

- 每个型号支持的功能许可证，第 3-1 页
- 关于 PAK 许可证，第 3-17 页
- PAK 许可证准则，第 3-24 页
- 配置 PAK 许可证，第 3-25 页
- 配置共享许可证 （AnyConnect 3 或更早版本），第 3-27 页
- 监控 PAK 许可证，第 3-33 页
- PAK 许可证历史记录，第 3-45 页

每个型号支持的功能许可证

本节介绍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。

- 每个型号的许可证，第 3-1 页
- 许可证说明，第 3-13 页

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：

- ASA 5506-X、 ASA 5506W-X 和 ASA 5506H-X，第 3-2 页
- ASA 5508-X，第 3-3 页
- ASA 5512-X，第 3-3 页
- ASA 5515-X，第 3-4 页
- ASA 5516-X，第 3-5 页
- ASA 5525-X，第 3-6 页
- ASA 5545-X，第 3-7 页
- ASA 5555-X，第 3-8 页
- 带 SSP-10 的 ASA 5585-X，第 3-9 页
- 带 SSP-20 的 ASA 5585-X，第 3-10 页

- 带 SSP-40 和 SSP-60 的 ASA 5585-X，第 3-11 页
- ASA 服务模块，第 3-12 页

显示为*斜体*的项是可以替代基础 （或增强型安全等）许可证版本的独立可选许可证。您可以混合使用以下许可证；例如， 24 统一通信许可证和强加密许可证；或 500 AnyConnect 高级版许可证和 GTP/GPRS 许可证；或全部四个许可证。

备注　某些功能互不兼容。有关兼容性信息，请参阅单独的功能章节。

如果您拥有一个无负载加密型号，则无法支持下面的部分功能。有关不支持功能的列表，请参阅无负载加密型号，第 3-23 页。

有关许可证的详细信息，请参阅许可证说明，第 3-13 页。

ASA 5506-X、 ASA 5506W-X 和 ASA 5506H-X

表 3-1　ASA 5506-X， ASA 5506W-X 和 ASA 5506H-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	不支持	启用
并发防火墙连接数	20,000	50,000
GTP/GPRS	不支持	不支持
UC 代理总会话数	160	160
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。		
AnyConnect 高级版对等体数 （最大数量）	50	50
	共享许可证：不支持	*共享许可证：不支持*
高级 终端评估	启用	启用
适用于思科 VPN 电话的 AnyConnect	启用	启用
AnyConnect Essentials	不支持	不支持
适用于移动设备的 AnyConnect	启用	启用
其他 VPN 许可证		
VPN 对等体总数 （包括所有类型）	50	50
其他 VPN 对等体数	10	50
VPN 负载均衡	不支持	不支持
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)*
故障切换	不支持	现用/备用
所有类型的最大接口数	536	636
安全情景	不支持	不支持
群集	不支持	不支持
最大 VLAN 数量	5	30

ASA 5508-X

表 3-2　　ASA 5508-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	启用	
并发防火墙连接数	100,000	
GTP/GPRS	不支持	
UC 代理总会话数	320	
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。		
AnyConnect 高级版对等体数（最大数量）	100	
	共享许可证：不支持	
高级 终端评估	启用	
适用于思科 VPN 电话的 AnyConnect	启用	
AnyConnect Essentials	不支持	
适用于移动设备的 AnyConnect	启用	
其他 VPN 许可证		
VPN 对等体总数 （包括所有类型）	100	
其他 VPN 对等体数	100	
VPN 负载均衡	启用	
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	
所有类型的最大接口数	716	
安全情景	2	*可选许可证：* *5*
群集	不支持	
最大 VLAN 数量	50	

ASA 5512-X

表 3-3　　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*				
并发防火墙连接数	100,000						250,000					
GTP/GPRS	不支持						禁用	*可选许可证：可用*				
UC 代理总会话数	2	*可选许可证：*					2	*可选许可证：*				
		24	*50*	*100*	*250*	*500*		*24*	*50*	*100*	*250*	*500*

表 3-3　　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
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。		
AnyConnect 高级版对等体数 （最大数量）	250	250
	可选共享许可证：我们建议升级到 AnyConnect Plus 或 Apex 许可，从而替换共享服务器功能。	*可选共享许可证：我们建议升级到 AnyConnect Plus 或 Apex 许可，从而替换共享服务器功能。*
高级 终端评估	启用	启用
适用于思科 VPN 电话的 AnyConnect	启用	启用
AnyConnect Essentials	禁用	禁用
适用于移动设备的 AnyConnect	启用	启用
其他 VPN 许可证		
VPN 对等体总数 （包括所有类型）	250	250
其他 VPN 对等体数	250	250
VPN 负载均衡	不支持	启用
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
所有类型的最大接口数	716	916
安全情景	不支持	2　*可选许可证：*　*5*
群集	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*
最大 VLAN 数量	50	100

ASA 5515-X

表 3-4　　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*
并发防火墙连接数	250,000
GTP/GPRS	禁用　*可选许可证：可用*
UC 代理总会话数	2　*可选许可证：*　*24*　*50*　*100*　*250*　*500*
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。	
AnyConnect 高级版对等体数 （最大数量）	250
	可选共享许可证：我们建议升级到 AnyConnect Plus 或 Apex 许可，从而替换共享服务器功能。
高级 终端评估	启用

表 3-4　　ASA 5515-X 许可证功能 （续）

许可证	基础许可证	
适用于思科 VPN 电话的 AnyConnect	启用	
AnyConnect Essentials	禁用	
适用于移动设备的 AnyConnect	启用	
其他 VPN 许可证		
VPN 对等体总数 （包括所有类型）	250	
其他 VPN 对等体数	250	
VPN 负载均衡	启用	
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	
所有类型的最大接口数	916	
安全情景	2	*可选许可证：* *5*
群集	2	
IPS 模块	禁用	*可选许可证：可用*
最大 VLAN 数量	100	

ASA 5516-X

表 3-5　　ASA 5516-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	启用	
并发防火墙连接数	250,000	
GTP/GPRS	禁用	*可选许可证：可用*
UC 代理总会话数	1000	
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。		
AnyConnect 高级版对等体数 （最大数量）	300	
	共享许可证：不支持	
高级 终端评估	启用	
适用于思科 VPN 电话的 AnyConnect	启用	
AnyConnect Essentials	不支持	
适用于移动设备的 AnyConnect	启用	

表 3-5　　ASA 5516-X 许可证功能 （续）

许可证	基础许可证	
其他 VPN 许可证		
VPN 对等体总数 （包括所有类型）	300	
其他 VPN 对等体数	300	
VPN 负载均衡	启用	
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	
所有类型的最大接口数	1,116	
安全情景	2	*可选许可证：* *5*
群集	不支持	
最大 VLAN 数量	150	

ASA 5525-X

表 3-6　　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*						
并发防火墙连接数	500,000							
GTP/GPRS	禁用	*可选许可证：可用*						
UC 代理总会话数	2	*可选许可证：*	*24*	*50*	*100*	*250*	*500*	*750*	*1000*
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。								
AnyConnect 高级版对等体数 （最大数量）	750							
	可选共享许可证：我们建议升级到 AnyConnect Plus 或 Apex 许可，从而替换共享服务器功能。							
高级 终端评估	启用							
适用于思科 VPN 电话的 AnyConnect	启用							
AnyConnect Essentials	禁用							
适用于移动设备的 AnyConnect	启用							
其他 VPN 许可证								
VPN 对等体总数 （包括所有类型）	750							
其他 VPN 对等体数	750							
VPN 负载均衡	启用							
通用许可证								
加密	基本 (DES)	*可选许可证：强 (3DES/AES)*						

表 3-6　　ASA 5525-X 许可证功能 （续）

许可证	基础许可证									
故障转移	主用/备用或主用/主用									
所有类型的最大接口数	1316									
安全情景	2	*可选许可证：*	*5*	*10*	*20*					
群集	2									
IPS 模块	禁用	*可选许可证：可用*								
最大 VLAN 数量	200									

ASA 5545-X

表 3-7　　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*								
并发防火墙连接数	750,000									
GTP/GPRS	禁用	*可选许可证：可用*								
UC 代理总会话数	2	*可选许可证：*	*24*	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。										
AnyConnect 高级版对等体数 （最大数量）	2500									
	可选共享许可证：我们建议升级到AnyConnect Plus 或Apex 许可，从而替换共享服务器功能。									
高级 终端评估	启用									
适用于思科 VPN 电话的 AnyConnect	启用									
AnyConnect Essentials	禁用									
适用于移动设备的 AnyConnect	启用									
其他 VPN 许可证										
VPN 对等体总数 （包括所有类型）	2500									
其他 VPN 对等体数	2500									
VPN 负载均衡	启用									
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									
所有类型的最大接口数	1716									
安全情景	2	*可选许可证：*	*5*	*10*	*20*	*50*				
群集	2									
IPS 模块	禁用	*可选许可证：可用*								
最大 VLAN 数量	300									

ASA 5555-X

表 3-8　　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*							
并发防火墙连接数	1,000,000								
GTP/GPRS	禁用	*可选许可证：可用*							
UC 代理总会话数	2	*可选许可证：*							
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。									
AnyConnect 高级版对等体数 （最大数量）	5000								
	可选共享许可证：我们建议升级到 AnyConnect Plus 或 Apex 许可，从而替换共享服务器功能。								
高级 终端评估	启用								
适用于思科 VPN 电话的 AnyConnect	启用								
AnyConnect Essentials	禁用								
适用于移动设备的 AnyConnect	启用								
其他 VPN 许可证									
VPN 对等体总数 （包括所有类型）	5000								
其他 VPN 对等体数	5000								
VPN 负载均衡	启用								
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								
所有类型的最大接口数	2516								
安全情景	2	*可选许可证：*	*5*	*10*	*20*	*50*	*100*		
群集	2								
IPS 模块	禁用	*可选许可证：可用*							
最大 VLAN 数量	500								

带 SSP-10 的 ASA 5585-X

您可以在同一机箱中使用两个相同级别的 SSP。不支持混合级别的 SSP （例如，不支持混用 SSP-10 和 SSP-20）。每个 SSP 均作为独立设备，可单独配置和管理。如果需要，可以将两个 SSP 用作故障切换对。

表 3-9　　带 SSP-10 的 ASA 5585-X 许可证功能

许可证	基础许可证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*							
并发防火墙连接数	1,000,000								
GTP/GPRS	禁用	*可选许可证：可用*							
UC 代理总会话数	2	*可选许可证：*							
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。									
AnyConnect 高级版对等体数 （最大数量）	5000								
	可选共享许可证：我们建议升级到AnyConnect Plus 或Apex 许可，从而替换共享服务器功能。								
高级 终端评估	启用								
适用于思科 VPN 电话的 AnyConnect	启用								
AnyConnect Essentials	禁用								
适用于移动设备的 AnyConnect	启用								
其他 VPN 许可证									
VPN 对等体总数 （包括所有类型）	5000								
其他 VPN 对等体数	5000								
VPN 负载均衡	启用								
通用许可证									
10 GE I/O	**基础许可证**：禁用；光纤接口在 1 GE 的速度下工作					**增强型安全许可证**：启用；光纤接口在 10 GE 的速度下工作			
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								
所有类型的最大接口数	4612								
安全情景	2	*可选许可证：*		*5*	*10*	*20*	*50*	*100*	
群集	禁用	*可选许可证：适用于 16 台设备*							
最大 VLAN 数量	1024								

带 SSP-20 的 ASA 5585-X

您可以在同一机箱中使用两个相同级别的 SSP。不支持混合级别的 SSP （例如，不支持混用 SSP-20 和 SSP-40）。每个 SSP 均作为独立设备，可单独配置和管理。如果需要，可以将两个 SSP 用作故障切换对。

表 3-10　　带 SSP-20 的 ASA 5585-X 许可证功能

许可证	基础许可证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*									
并发防火墙连接数	2,000,000										
GTP/GPRS	禁用	*可选许可证：可用*									
UC 代理总会话数	2	*可选许可证：*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。											
AnyConnect 高级版对等体数 （最大数量）	10,000										
	可选共享许可证：我们建议升级到 AnyConnect Plus 或 Apex 许可，从而替换共享服务器功能。										
高级 终端评估	启用										
适用于思科 VPN 电话的 AnyConnect	启用										
AnyConnect Essentials	禁用										
适用于移动设备的 AnyConnect	启用										
其他 VPN 许可证											
VPN 对等体总数 （包括所有类型）	10,000										
其他 VPN 对等体数	10,000										
VPN 负载均衡	启用										
通用许可证											
10 GE I/O	**基础许可证**：禁用；光纤接口在 1 GE 的速度下工作					**增强型安全许可证**：启用；光纤接口在 10 GE 的速度下工作					
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										
所有类型的最大接口数	4612										
安全情景	2	*可选许可证：*		*5*	*10*	*20*	*50*	*100*	*250*		
群集	禁用	*可选许可证：适用于 16 台设备*									
最大 VLAN 数量	1024										

1. 利用可覆盖 10,000 个会话的 UC 许可证，会话总数合计可达到 10,000，但是电话代理会话的最大数量为 5000。

带 SSP-40 和 SSP-60 的 ASA 5585-X

您可以在同一机箱中使用两个相同级别的 SSP。不支持混合级别的 SSP （例如，不支持混用 SSP-40 和 SSP-60）。每个 SSP 均作为独立设备，可单独配置和管理。如果需要，可以将两个 SSP 用作故障切换对。

表 3-11　　带 SSP-40 和 SSP-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*									
并发防火墙连接数	**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*									
UC 代理总会话数	2	*可选许可证：*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。											
AnyConnect 高级版对等体数 （最大数量）	10,000										
	可选共享许可证：我们建议升级到AnyConnect Plus 或Apex 许可，从而替换共享服务器功能。										
高级 终端评估	启用										
适用于思科 VPN 电话的 AnyConnect	启用										
AnyConnect Essentials	禁用										
适用于移动设备的 AnyConnect	启用										
其他 VPN 许可证											
VPN 对等体总数 （包括所有类型）	10,000										
其他 VPN 对等体数	10,000										
VPN 负载均衡	启用										
通用许可证											
10 GE I/O	启用；光纤接口在 10 GE 的速度下工作										
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										
所有类型的最大接口数	4612										
安全情景	2	*可选许可证：*		*5*	*10*	*20*	*50*	*100*	*250*		
群集	禁用	*可选许可证：适用于 16 台设备*									
最大 VLAN 数量	1024										

1. 利用可覆盖 10,000 个会话的 UC 许可证，会话总数合计可达到 10,000，但是电话代理会话的最大数量为 5000。

ASA 服务模块

表 3-12　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*									
并发防火墙连接数	10,000,000										
GTP/GPRS	禁用	*可选许可证：可用*									
UC 代理总会话数	2	*可选许可证：*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。											
AnyConnect 高级版对等体数 （最大数量）	10,000										
	可选共享许可证：我们建议升级到 AnyConnect Plus 或 Apex 许可，从而替换共享服务器功能。										
高级 终端评估	启用										
适用于思科 VPN 电话的 AnyConnect	启用										
AnyConnect Essentials	禁用										
适用于移动设备的 AnyConnect	启用										
其他 VPN 许可证											
VPN 对等体总数 （包括所有类型）	10,000										
其他 VPN 对等体数	10,000										
VPN 负载均衡	启用										
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*				
群集	不支持										
最大 VLAN 数量	1000										

1. 利用可覆盖 10,000 个会话的 UC 许可证，会话总数合计可达到 10,000，但是电话代理会话的最大数量为 5000。

许可证说明

下表包含有关许可证的其他信息。

表 3-13　许可证说明

许可证	备注
AnyConnect Essentials	**备注**　此许可证是传统许可证。我们建议您升级到 AnyConnect Plus 或 Apex 许可证。 AnyConnect 基础版会话包含以下 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 高级版许可证而不是 AnyConnect 基础版许可证。 **备注**　借助 AnyConnect 基础版许可证， VPN 用户可以使用 Web 浏览器来进行登录，然后下载并启动 (WebLaunch) AnyConnect 客户端。 AnyConnect 客户端软件提供一系列相同的客户端功能，无论是通过此许可证还是通过 AnyConnect 高级版许可证启用。 在特定 ASA 上， AnyConnect 基础版许可证不能和以下许可证同时处于活动状态：AnyConnect 高级版许可证 （所有类型）或高级终端评估许可证。但是，您可以在同一网络中的不同 ASA 上运行 AnyConnect 基础版和 AnyConnect 高级版许可证。 默认情况下，ASA 使用 AnyConnect 基础版许可证，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，以使用其他许可证。
适用于思科 VPN 电话的 AnyConnect	**备注**　此许可证是传统许可证。我们建议您升级到 AnyConnect Plus 或 Apex 许可证，包括此许可证。 通过结合使用 AnyConnect 高级版许可证，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。

表 3-13　　许可证说明 （续）

许可证	备注
适用于移动设备的 AnyConnect	**备注**　此许可证是传统许可证。我们建议您升级到 AnyConnect Plus 或 Apex 许可证，包括此许可证。 此许可证为运行 Windows Mobile 5.0、6.0 和 6.1 的触摸屏移动设备提供对 AnyConnect 客户端的访问。如果希望对 AnyConnect 2.3 及更高版本的移动访问提供支持，我们建议您使用此许可证。此许可证要求激活以下任一许可证，以指定允许的 SSL VPN 会话的总数：AnyConnect 基础版或 AnyConnect 高级版。 **移动安全评估支持** 实施远程访问控制和从移动设备收集安全评估数据要求在 ASA 上安装一个 AnyConnect Mobile 许可证和一个 AnyConnect 基础版或 AnyConnect 高级版许可证。根据您安装的许可证，可以获得以下功能。 • AnyConnect 高级版许可证功能 – 根据 DAP 属性和所有其他现有终端属性，在受支持的移动设备上实施 DAP 策略。这包括允许或拒绝来自移动设备的远程访问。 • AnyConnect 基础版许可证功能 – 逐个组启用或禁用移动设备访问，以及使用 ASDM 配置该功能。 – 通过 CLI 或 ASDM 显示有关已连接移动设备的信息，这些移动设备并不具有实施 DAP 策略或者拒绝或允许对其进行远程访问的能力。
AnyConnect Premium	**备注**　此许可证是传统许可证。我们建议您升级到 AnyConnect Plus 或 Apex 许可证，包括此许可证。 AnyConnect 高级版会话包括以下 VPN 类型： • SSL VPN • 无客户端 SSL VPN • 使用 IKEv2 的 IPsec 远程访问 VPN
共享 AnyConnect 高级版	**备注**　此许可证是传统许可证。我们建议您升级到 AnyConnect Plus 或 Apex 许可证，从而替代共享许可证功能。 通过共享许可证， ASA 可以充当多个客户端 ASA 的共享许可证服务器。共享许可证池非常大，但是每一个 ASA 使用的最大会话数不能超过为永久许可证列出的最大数量。
僵尸网络流量过滤器	要下载动态数据库，需要强加密 (3DES/AES) 许可证。
加密	无法禁用 DES 许可证。如果您安装有 3DES 许可证，则 DES 仍然可用。要在希望仅使用强加密时防止使用 DES，请务必将所有相关命令都配置为仅使用强加密。

所有类型的最大接口数	最大整合接口数；例如， VLAN 接口、物理接口、冗余接口、网桥组接口和 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，即使 GigabitEthernet 0/0 接口被定义为 port-channel 1 的一部分，以下两个接口也要计数：
	`interface gigabitethernet 0/0`
	
	和
	`interface port-channel 1`

表 3-13　　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 侧的 IPS 签名订用。 请参阅以下准则： • 要购买 IPS 签名订用，您需要具有预装了 IPS 的 ASA（部件号必须包含“IPS”，例如 ASA5515-IPS-K9）；您不能为非 IPS 部件号 ASA 购买 IPS 签名订用。 • 为进行故障切换，需要在两台设备上均具有 IPS 签名订用；由于此订用不是 ASA 许可证，因此在故障切换中不会进行共享。 • 为进行故障切换，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 模块许可证在故障切换集群许可证中进行技术共享。但是，由于 IPS 签名订用要求，您必须为故障切换中的每台设备购买单独的 IPS 模块许可证。
其他 VPN	其他 VPN 会话包括以下 VPN 类型： • 使用 IKEv1 的 IPsec 远程访问 VPN • 使用 IKEv1 的 IPsec 站点间 VPN • 使用 IKEv2 的 IPsec 站点间 VPN 此许可证包含在基础许可证中。
VPN （会话）总数 （包括所有类型）	• 虽然最大总 VPN 会话数累计超过最大 VPN AnyConnect 会话数和其他 VPN 会话数，但是合并会话数不应超过 VPN 会话限制。如果超过最大 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，然后从门户启动 AnyConnect 客户端会话，总计使用的是 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，则会使用 2 个会话。

表 3-13　　许可证说明 （续）

许可证	备注
UC 代理总会话数	加密语音检测的每个 TLS 代理会话都会计入 UC 许可证限制。 使用 TLS 代理会话的其他应用不计入 UC 限制，例如 Mobility Advantage 代理就不需要许可证。 某些 UC 应用可能会对连接使用多个会话。例如，如果使用主用和备用思科统一通信管理器配置电话，由于有 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** 窗格来独立设置 TLS 代理限制。要查看型号的限制，请输入 **tls-proxy maximum-sessions ?** 命令。当应用高于默认 TLS 代理限制的 UC 许可证时， ASA 会将 TLS 代理限制自动设置为与 UC 限制相匹配。TLS 代理限制优先于 UC 许可证限制；如果将 TLS 代理限制设置为低于 UC 许可证，则可能无法使用 UC 许可证中的所有会话。 **备注**　对于以 “K8” 结尾的许可证部件号 （例如，用户数少于 250 的许可证）， TLS 代理会话数限制为 1000。对于以 “k9” 结尾的许可证部件号 （例如，用户数为 250 或更多的许可证）， TLS 代理限制取决于配置，最高值为型号限制。K8 和 K9 是指许可证是否有出口限制：K8 不受限制， K9 受限制。 如果清除配置（例如，使用 **clear configure all** 命令），则 TLS 代理限制会设置为型号的默认值；如果此默认值低于 UC 许可证限制，则您会看到要求使用 **tls-proxy maximum-sessions** 命令再次提高限制的错误消息 （在 ASDM 中，使用 **TLS Proxy** 窗格）。如果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，则会在辅助设备上自动生成 **clear configure all** 命令，因此，您可能会在辅助设备上看到警告消息。由于配置同步会恢复在主设备上设置的 TLS 代理限制，因此可以忽略该警告。 您也可能为连接使用 SRTP 加密会话： • 对于 K8 许可证， SRTP 会话数限制为 250。 • 对于 K9 许可证，没有限制。 **备注**　只有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式，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 上安装用于设置合适的 vCPU 数量的型号许可证。在安装许可证之前，吞吐量限制为 100 kbps，以便您可以执行初步连接测试。需要安装型号许可证才能正常运行。

最大 VLAN 数量	对于根据 VLAN 限制计数的接口，您必须向其分配 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。

关于 PAK 许可证

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

- 预安装许可证，第 3-17 页
- 永久许可证，第 3-17 页
- 基于时间的许可证，第 3-17 页
- 共享型 AnyConnect 高级版许可证 （AnyConnect 3 和更早版本），第 3-20 页
- 故障切换或 ASA 集群许可证，第 3-20 页
- 无负载加密型号，第 3-23 页
- 许可证常见问题解答，第 3-23 页

预安装许可证

默认情况下， ASA 随附已安装的许可证。此许可证可能是基础许可证，您要向其添加更多许可证，或者其可能已经安装所有许可证，具体取决于您的订购以及供应商为您安装的内容。

相关主题

监控 PAK 许可证，第 3-33 页

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，则 ASA 会将永久许可证和基于时间的许可证合并为运行许可证。

相关主题

如何合并永久许可证和基于时间的许可证，第 3-18 页

基于时间的许可证

除永久许可证以外，您还可以购买基于时间的许可证，或者接收具有时间限制的评估许可证。例如，您可能订购有效期为 1 年的僵尸网络流量过滤器基于时间的许可证。

- 基于时间的许可证激活准则，第 3-18 页
- 基于时间的许可证计时器工作方式，第 3-18 页
- 如何合并永久许可证和基于时间的许可证，第 3-18 页
- 堆叠基于时间的许可证，第 3-19 页
- 基于时间的许可证到期，第 3-19 页

基于时间的许可证激活准则

- 您可以安装多个基于时间的许可证，包括同一功能的多个许可证。但是，每个功能一次只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，如果安装 3000 个会话的统一通信许可证和 2000 个会话的统一通信许可证，则其中仅有一个许可证可处于活动状态。
- 如果激活在密钥中具有多个功能的评估许可证，则无法为所包含的其中一个功能也同时激活另一基于时间的许可证。例如，如果评估许可证包含僵尸网络流量过滤器和 1000 个会话 AnyConnect 统一通信许可证，则无法也激活独立的基于时间的 2000 个会话统一通信许可证。

基于时间的许可证计时器工作方式

- 当在 ASA 上激活基于时间的许可证时，其计时器便开始倒计时。
- 如果在基于时间的许可证超时之前停止对其进行使用，则计时器会停止。仅当重新激活基于时间的许可证时，计时器才会再次启动。
- 如果基于时间的许可证处于活动状态，并且您关闭 ASA，则计时器会停止倒计时。仅当 ASA 正在运行时，基于时间的许可证才会倒计时。系统时钟设置不影响许可证；只有 ASA 正常运行时间会计入许可证持续时间。

如何合并永久许可证和基于时间的许可证

激活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合并形成运行许可证。永久许可证与基于时间的许可证的合并方式取决于许可证的类型。下表列出了每个功能许可证的合并规则。

备注　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，也会继续倒计时。

表 3-14　基于时间的许可证合并规则

基于时间的功能	合并许可证规则
AnyConnect 高级版会话	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，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	基于时间的许可证会话会添加到永久会话中，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，则只要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	基于时间的许可证情景会添加到永久情景中，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，则只要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。
其他所有	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。对于具有数字层的许可证，将使用较高的值。通常，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。

相关主题

监控 PAK 许可证，第 3-33 页

堆叠基于时间的许可证

在许多情况下，您可能需要续订基于时间的许可证，并从旧许可证无缝过渡到新许可证。对于只有基于时间的许可证时才可提供的功能，在应用新许可证之前，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，也不必担心因为提前安装新许可证而损失许可证时间。

当安装与已安装的许可证相同的基于时间的许可证时，许可证会进行合并，并且持续时间等于合并后的持续时间。

例如：

1. 您安装有 52 周的僵尸网络流量过滤器许可证，并且该许可证已使用 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。当安装第二个许可证时，许可证合并具有 79 周的持续时间 （52 周加上 27 周）。

同样：

1. 您安装有 8 周的 1000 个会话统一通信许可证，并且该许可证已使用 2 周 （剩余 6 周）。
2. 然后，您又安装了另一个 8 周 1000 个会话许可证，许可证合并具有 14 周 1000 个会话 （8 周加上 6 周）。

如果许可证不同 （例如， 1000 个会话统一通信许可证和 2000 个会话许可证），则许可证*不会*合并。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。

虽然不同的许可证不会合并，但当前许可证到期时， ASA 会自动激活同一功能的已安装许可证（如果适用）。

相关主题

- 激活或停用密钥，第 3-26 页
- 基于时间的许可证到期，第 3-19 页

基于时间的许可证到期

当某个功能的当前许可证到期时， ASA 会自动激活同一功能的已安装许可证 （如果适用）。如果没有其他适用于此功能的基于时间的许可证，则会使用永久许可证。

如果为某个功能安装了多个额外的基于时间的许可证，则 ASA 会使用其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。

例如，您有一个基于时间的 2000 个会话统一通信许可证 （活动）、一个基于时间的 1000 个会话统一通信许可证 （非活动）以及一个永久的 500 个会话统一通信许可证。当 2000 个会话许可证到期时，ASA 会激活 1000 个会话许可证。在 1000 个会话许可证到期后，ASA 会使用 500 个会话永久许可证。

相关主题

激活或停用密钥，第 3-26 页

共享型 AnyConnect 高级版许可证 （AnyConnect 3 和更早版本）

备注　AnyConnect 4 及更高版本的许可不支持 ASA 上的共享许可证功能。AnyConnect 许可证可进行共享，并且不再需要共享服务器或参与者许可证。

共享许可证允许您购买大量 AnyConnect 高级版会话，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，并将其余设备配置为共享许可参与者）。

故障切换或 ASA 集群许可证

除一些例外情况之外，故障切换和集群设备不要求每台设备上具有相同的许可证。对于早期版本，请参阅您的版本的许可文档。

- 故障切换许可证要求和例外情况，第 3-20 页
- ASA 集群许可证要求和例外，第 3-21 页
- 如何合并故障切换或 ASA 集群许可证，第 3-21 页
- 故障切换或 ASA 集群设备之间的通信丢失，第 3-22 页
- 升级故障切换对，第 3-23 页

故障切换许可证要求和例外情况

故障切换设备不要求每个设备上具有同一许可证。通常，您仅为主设备购买许可证；对于主用/备用故障切换，辅助设备会在变为主用状态时继承主许可证。如果您在两台设备上都有许可证，则这两个许可证会合并为一个运行故障切换集群许可证。此规则存在一些例外情况。有关故障切换的具体许可要求，请参阅下表。

型号	许可证要求
ASA 5506-X 系列	• 主用/备用 - 增强型安全许可证。 • 主用/主用 - 不支持。 **备注**　每台设备必须拥有相同的加密许可证。
ASA 5512-X 至 ASA 5555-X	• ASA 5512-X - 增强型安全许可证。 • 其他型号 - 基础许可证。 **备注**　每台设备必须拥有相同的加密许可证；每台设备必须拥有相同的 IPS 模块许可证。您还需要两台设备的 IPS 侧均有 IPS 签名订用。请参阅以下准则： – 要购买 IPS 签名订用，您需要具有预装了 IPS 的 ASA（部件号必须包含“IPS”，例如 ASA5515-IPS-K9）；您不能为非 IPS 部件号 ASA 购买 IPS 签名订用。 – 您需要在两台设备上均有 IPS 签名订用；由于此订用不是 ASA 许可证，因此在故障切换中不会进行共享。 – 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 模块许可证在故障切换集群许可证中进行技术共享。但是，由于 IPS 签名订用要求，您必须为故障切换中的每台设备购买单独的 IPS 模块许可证。

型号	许可证要求
ASAv	• 主用/备用 - 标准和高级版许可证。 • 主用/主用 - 不支持。 **备注**　备用设备要求具有与主设备相同的型号许可证；每台设备必须拥有相同的加密许可证。
所有其他型号	基础许可证。 **备注**　每台设备必须拥有相同的加密许可证。

备注　需要有效的永久密钥；在极少数情况下，可以删除身份验证密钥。如果密钥全部由 0 组成，则需要重新安装有效的身份验证密钥，然后才能启用故障切换。

ASA 集群许可证要求和例外

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。

此准则也存在例外。有关集群的精确许可要求，请参阅下表。

型号	许可证要求
ASA 5585-X	集群许可证。 **备注**　每台设备都必须有相同的加密许可证；每台设备都必须有相同的 10 GE I/O/增强型安全许可证 （带有 SSP-10 和 SSP-20 的 ASA 5585-X）。
ASA 5512-X	增强型安全许可证。 **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。 **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。

如何合并故障切换或 ASA 集群许可证

对于故障切换对或 ASA 集群，每台设备上的许可证会合并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，则合并的许可证使用以下规则：

- 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合并，最高值为平台限制。如果正在使用的所有许可证都基于时间，则许可证将同时倒计时。

  例如，对于故障切换：

  – 您有两台 ASA，各自安装有 10 个 AnyConnect 高级版会话；这些许可证会合并，从而拥有总共 20 个 AnyConnect 高级版会话。

  – 您有两台各有 500 个 AnyConnect 高级版会话的 ASA 5525-X；由于平台限制为 750，因此合并后的许可证允许使用 750 个 AnyConnect 高级版会话。

注意　在上述示例中，如果 AnyConnect 高级版许可证基于时间，则可能要禁用其中一个许可证，以便不会 “浪费”一个 500 个会话的许可证，由于平台限制，您只能使用其中的 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；合并后的许可证允许使用 30 个情景。对于主用/主用故障切换，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，总共 30 个情景。

  例如，对于 ASA 集群：

  - 您有四台带 SSP-10 的 ASA 5585-X ASA，三台设备各有 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，因此合并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，三台设备各有 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，因此这些许可证将进行合并，从而拥有总共 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证 （并且没有数字层），持续时间是所有许可证的合并后的持续时间。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/主用故障切换和 ASA 集群，即使所有设备都以主用状态在运行也如此。

  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，则合并后的持续时间为 96 周。

相关主题

监控 PAK 许可证，第 3-33 页

故障切换或 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合并的运行许可证。

如果在 30 天的宽限期内恢复通信，则对于基于时间的许可证，将从主/主许可证中减去耗用时间；如果主/主许可证已到期，则仅在此时辅助/从属许可证才会开始倒计时。

如果在 30 天内没有恢复通信，则对于基于时间的许可证，将从所有设备许可证 （如果已安装）中减去耗用时间。它们会被视为独立许可证，不会受益于合并后的许可证。耗用时间包括 30 天的宽限期。

例如：

1. 您在两台设备上都安装有 52 周的僵尸网络流量过滤器许可证。合并后的运行许可证允许总共 104 周的持续时间。
2. 这两台设备作为故障切换设备/ASA 集群运行 10 周，因此合并后的许可证会剩余 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），则辅助/从属设备会继续使用合并后的许可证，并继续从 94 周倒计时。
4. 基于时间的许可证的行为取决于恢复通信的时间：

- 在 30 天内 - 从主/主设备许可证中减去耗用时间。在这种情况下，通信将在 4 周后恢复。因此，将从主/主许可证中减去 4 周，总共剩余 90 周 （主设备上剩余 38 周，辅助设备上剩余 52 周）。
- 在 30 天后 - 从两台设备的许可证中减去耗用时间。在这种情况下，通信将在 6 周后恢复。因此，将从主/主许可证和辅助/从属许可证中减去 6 周，总共剩余 84 周 （主/主设备上剩余 36 周，辅助/从属设备上剩余 46 周）。

升级故障切换对

由于故障切换对不要求在两台设备上具有同一许可证，因此可以将新许可证应用于每台设备而不会产生任何停机时间。如果应用要求重新加载的永久许可证，则可以在重新加载时故障切换到另一台设备。如果两台设备都需要重新加载，则可以将其分开重新加载，以便不会产生停机时间。

相关主题

表 3-15，第 3-26 页

无负载加密型号

您可以购买一些具有无负载加密功能的型号。如要出口至某些国家/地区，则在思科 ASA 系列上不能启用负载加密。ASA 软件可感知无负载加密型号，并会禁用以下功能：

- 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，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）。

当您查看许可证时，将不会列出 VPN 许可证和统一通信许可证。

相关主题

监控 PAK 许可证，第 3-33 页

许可证常见问题解答

问 我是否可以激活多个基于时间的许可证，例如， AnyConnect 高级版和僵尸网络流量过滤器？

答 是的。对于每个功能，您可以一次使用一个基于时间的许可证。

问 我是否可以“堆叠”基于时间的许可证，以便在时间限制解除时，将自动使用下一个许可证？

答 是的。对于相同的许可证，当安装多个基于时间的许可证时，时间限制会合并。对于不相同的许可证（例如，1000 个会话 AnyConnect 高级版许可证和 2500 个会话许可证），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。

问 我是否可以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？

答 是的。激活永久许可证不会影响基于时间的许可证。

问 对于故障切换，我是否可以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？

答 否。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由两台备用服务器组成的一个单独故障切换对中。

问 我是否需要为故障切换对中的辅助设备购买相同的许可证？

答 否。从版本 8.3(1) 开始，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，如果您为版本 8.3 之前的软件购买了匹配的许可证），这些许可证会合并为运行故障切换集群许可证，其数量最高值为型号限制。

问 除共享型 AnyConnect 高级版许可证之外，我是否可以使用基于时间的或永久的 AnyConnect 高级版许可证？

答 是的。仅在本地安装的许可证 （基于时间的许可证或永久许可证）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 高级版许可证；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适用于本地 AnyConnect 高级版会话；不能将其添加到共享许可池供参与者使用。

PAK 许可证准则

情景模式规定

在多情景模式下，请在系统执行空间中应用激活密钥。

故障切换准则

请参阅故障切换或 ASA 集群许可证，第 3-20 页。

型号准则

- 仅在 ASAv 上支持智能许可。
- 在 ASAv、 ASA 5506-X、 ASA 5508-X 和 ASA 5516-X 上不支持智能许可。

升级和降级准则

如果从任何之前版本升级到最新版本，则您的激活密钥保持兼容。但如果要维护降级功能，则可能会遇到问题：

- 降级到版本 8.1 或更早版本 - 在升级后，如果激活在*版本 8.2 之前*引入的其他功能许可证，则执行降级后激活密钥会继续与早期版本兼容。但是，如果激活在*版本 8.2 或更高版本*中引入的功能许可证，则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：
  - 如果以前输入了早期版本的激活密钥，则 ASA 会使用该密钥 （没有您在版本 8.2 或更高版本中激活的任何新许可证）。
  - 如果您有新系统且没有早期的激活密钥，则需要请求与早期版本兼容的新激活密钥。
- 降级到版本 8.2 或更早版本 - 版本 8.3 中引入了更稳健的基于时间的密钥用法以及故障切换许可证变更：
  - 如果您有多个基于时间的激活密钥处于活动状态，则在降级后，只有最新激活的基于时间的密钥可以处于活动状态。所有其他密钥都会变为非活动状态。如果最后的基于时间的许可证是用于版本 8.3 中引入的功能，则该许可证即使无法在早期版本中使用，也仍会保持活动状态。重新输入永久密钥或有效的基于时间的密钥。
  - 如果在故障切换对上有不匹配的许可证，则降级将禁用故障切换。即使密钥匹配，所使用的许可证也将不再是合并许可证。
  - 如果您安装有一个基于时间的许可证，但是它用于版本 8.3 中引入的功能，则在降级之后，该基于时间的许可证保持活动状态。您需要重新输入永久密钥，以禁用该基于时间的许可证。

其他准则

- 激活密钥不会存储在配置文件中；它会以隐藏文件的形式存储在闪存中。
- 激活密钥会绑定到设备的序列号。功能许可证无法在设备之间转移 （除非发生硬件故障）。如果您由于硬件故障而必须更换设备，并且思科 TAC 涵盖该设备，请联系思科许可团队，以便将您的现有许可证转移至新的序列号。思科许可团队将要求您提供产品许可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来获取退款或已升级的许可证。
- 在单个设备上，无法将用于同一功能的两个单独许可证合并；例如，如果您购买了一个 25 个会话 SSL VPN 许可证，此后又购买了 50 个会话许可证，则无法使用 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合并区分开来）。
- 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 高级版许可证，此许可证与以下许可证不兼容：AnyConnect 高级版许可证、共享型 AnyConnect 高级版许可证以及高级终端评估许可证。默认情况下，如果安装了 AnyConnect 高级版许可证 （如果其适用于您的型号），则会使用该许可证，而不是上述许可证。您可以依次使用 **webvpn** 和 **no anyconnect-essentials** 命令在配置中禁用 AnyConnect 基础版许可证，以恢复使用其他许可证。

配置 PAK 许可证

本节介绍如何获取激活密钥以及如何将其激活。您也可以停用密钥。

- 获取激活密钥，第 3-25 页
- 激活或停用密钥，第 3-26 页

获取激活密钥

要获得激活密钥，您需要产品授权密钥，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，则可以为高级终端评估和额外的 AnyConnect 高级版会话购买单独的密钥。

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

操作步骤

步骤 1　获取 ASA 的序列号，方法是输入以下命令。

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

步骤 2　如果您尚未向 Cisco.com 注册，请创建帐户。

步骤 3　请转至以下许可网站：

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

系统会自动生成激活密钥，并将其发送到您提供的邮件地址。此密钥包含迄今为止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执行步骤 4。输入所有产品授权密钥后，所提供的最终激活密钥会包含已注册的所有永久功能。

激活或停用密钥

本节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。

准备工作

- 如果您已处于多情景模式下，请在系统执行空间中输入激活密钥。
- 某些永久许可证会在激活后要求重新加载 ASA。下表列出了要求重新加载的许可证。

表 3-15　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 vCPU 许可证。

操作步骤

步骤 1　将激活密钥应用于 ASA：

activation-key *key* [**activate** | **deactivate**]

示例：

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

key 是包括五个元素的十六进制字符串，各元素之间以空格分隔。前导 0x 说明符是可选的；假设所有值都是十六进制。

您可以安装一个永久密钥和多个基于时间的密钥。如果输入新的永久密钥，则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。如果不输入任何值，则 **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。如果您是第一次输入密钥，之后指定 **deactivate**，则在 ASA 上安装的密钥处于不活动状态。

步骤 2　（可能需要。）重新加载 ASA：

reload

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 ASA。如果您需要重新加载，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.
```

相关主题

- 基于时间的许可证，第 3-17 页
- 表 3-15，第 3-26 页

配置共享许可证 （AnyConnect 3 或更早版本）

备注　AnyConnect 4 及更高版本的许可不支持 ASA 上的共享许可证功能。AnyConnect 许可证可进行共享，并且不再需要共享服务器或参与者许可证。

本节介绍如何配置共享许可服务器和参与者。

- 关于共享许可证，第 3-27 页
- 配置共享许可服务器，第 3-31 页
- 配置共享许可备用服务器 （可选），第 3-32 页
- 配置共享许可参与者，第 3-33 页

关于共享许可证

共享许可证允许您购买大量 AnyConnect 高级版会话，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，并将其余设备配置为共享许可参与者）。

- 关于共享许可服务器和参与者，第 3-27 页
- 参与者和服务器之间的通信问题，第 3-28 页
- 有关共享许可备用服务器，第 3-28 页
- 故障切换和共享许可证，第 3-29 页
- 最大参与者数量，第 3-30 页

关于共享许可服务器和参与者

以下步骤说明共享许可证的工作方式：

1. 决定哪一台 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 （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。只能指定一台备用服务器。

   注意　共享许可备用服务器仅需要参与者许可证。

4. 请在共享许可服务器上配置一个共享密钥；具有该共享密钥的所有参与者都可以使用共享许可证。
5. 将 ASA 配置为参与者时，它通过发送有关自身的信息 （包括本地许可证和型号信息）向共享许可服务器注册。

   注意　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. 共享许可服务器会使用参与者应轮询服务器的频率的有关信息进行响应。
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，从而获取更多会话（以 50 个会话为增量）。

8. 共享许可服务器使用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。

注意　共享许可服务器也可以参与共享许可证池。它进行参与既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，则服务器通过提供尽可能多的可用会话进行响应。
   b. 参与者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. 当参与者的负载减少时，它会向服务器发送消息，以释放共享会话。

备注　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也如此。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。
- 如果在 24 小时的时间到期之前且服务器使参与者会话到期之后，参与者与服务器重新连接，则参与者需要为会话发送新的请求；服务器通过可向该参与者发送尽可能多的会话进行响应。

有关共享许可备用服务器

共享许可备用服务器必须先成功向主共享许可服务器注册，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。

当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发出会话，而且现有会话将会超时。请务必在此 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。

当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。

备注　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，直至达到 30 天。此外，如果此后主服务器停止运行任意时长，则备用服务器的运行限制会逐日缩短。当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。

故障切换和共享许可证

本节介绍共享许可证如何与故障切换交互。

- 故障切换和共享许可证服务器，第 3-29 页
- 故障切换和共享许可证参与者，第 3-30 页

故障切换和共享许可证服务器

本节介绍主服务器和备用服务器如何与故障切换交互。由于共享许可服务器也会与 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，因此您可能需要为主共享许可服务器和备用共享许可服务器配置故障切换，以便提高可靠性。

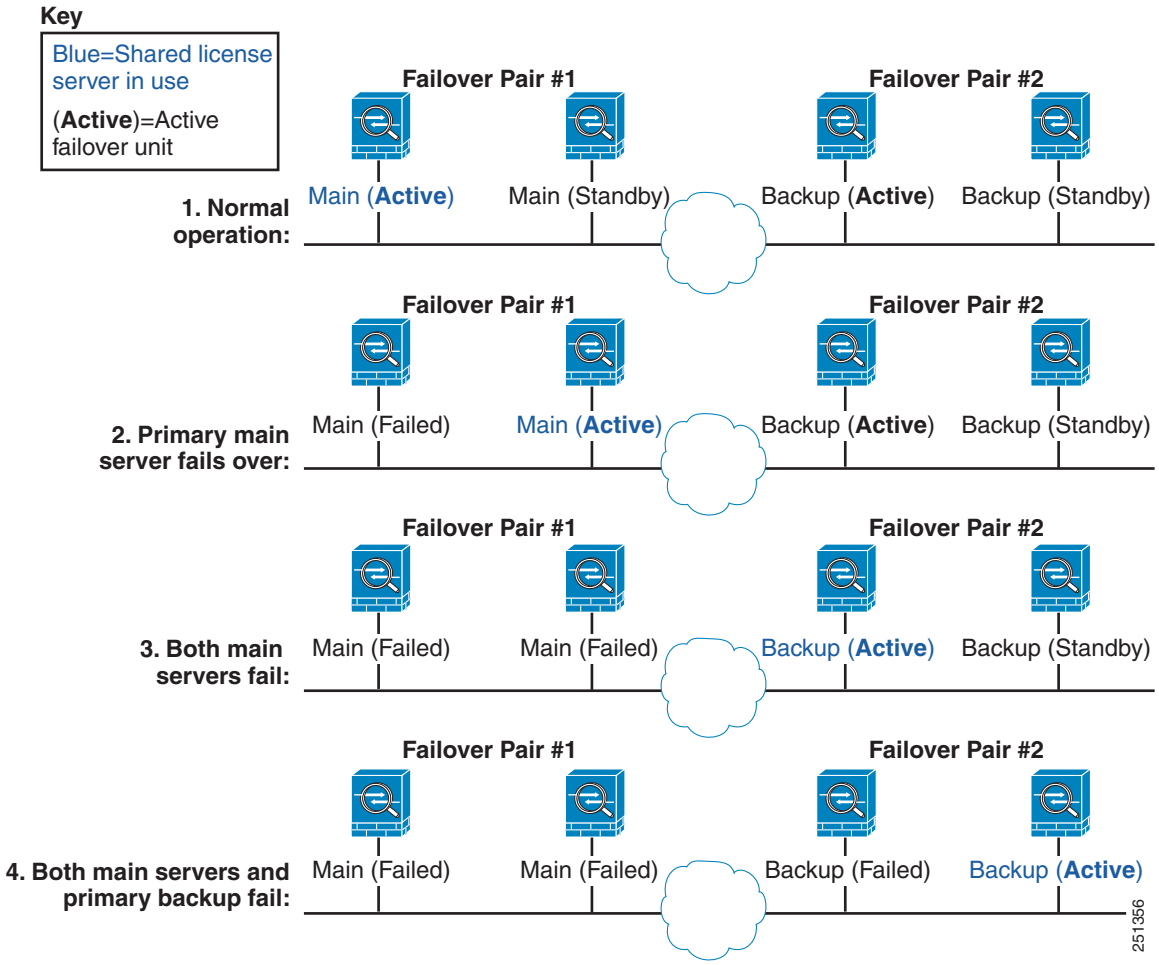
备注　备用服务器机制独立于故障切换，但与其兼容。

仅在单情景模式下支持共享许可证，因此不支持主用/主用故障切换。

对于主用/备用故障切换，主设备将充当主共享许可服务器，发生故障切换后，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。相反，您可以视需要让另一对设备充当备用服务器。

例如，您具有包含 2 个故障切换对的网络。第 1 对包含主许可服务器。第 2 对包含备用服务器。第 1 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。绝不会使用第 2 对中的备用服务器。仅当第 1 对中的两台设备均发生故障时，第 2 对中的备用服务器才会用作共享许可服务器。如果第 1 对保持故障状态，并且第 2 对中的主设备发生故障，则第 2 对中的备用设备将会用作共享许可服务器 （请参阅图 3-1）。

图 3-1　故障切换和共享许可证服务器



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。

相关主题

有关共享许可备用服务器，第 3-28 页

故障切换和共享许可证参与者

对于参与者对，两台设备均会使用单独的参与者 ID 向共享许可服务器注册。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。此转移请求用于将来自先前主用设备的共享会话移至新的主用设备。

最大参与者数量

ASA 不限制共享许可证的参与者数量；但是，超大共享网络可能会潜在影响许可服务器的性能。在这种情况下，您可以增大参与者刷新之间的延迟，也可以创建两个共享网络。

配置共享许可服务器

本节介绍如何将 ASA 配置为共享许可服务器。

准备工作

服务器必须具有共享许可服务器密钥。

操作步骤

步骤 1　设置共享密钥：

license-server secret *secret*

示例：

```
ciscoasa(config)# license-server secret farscape
```

secret 是由 4 至 128 个 ASCII 字符组成的字符串。拥有此密钥的任何参与者都可以使用许可服务器。

步骤 2　（可选）设置刷新间隔：

license-server refresh-interval *seconds*

示例：

```
ciscoasa(config)# license-server refresh-interval 100
```

间隔介于 10 和 300 秒之间；此值会提供给参与者，用于设置其应与服务器通信的频率。默认值为 30 秒。

步骤 3　（可选）设置服务器侦听来自参与者的 SSL 连接的端口。

license-server port *port*

示例：

```
ciscoasa(config)# license-server port 40000
```

port 介于 1 和 65535 之间。默认值为 TCP 端口 50554。

步骤 4　（可选）确定备用服务器 IP 地址和序列号：

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
```

如果备用服务器属于某个故障切换对，请另外确定备用设备序列号。只能确定 1 台备用服务器及其可选的备用设备。

步骤 5　使此设备成为共享许可服务器：

license-server enable *interface_name*

示例：

```
ciscoasa(config)# license-server enable inside
```

指定参与者与服务器进行连接的接口。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
```

配置共享许可备用服务器 （可选）

本节介绍如何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。

准备工作

备用服务器必须具有共享许可参与者密钥。

操作步骤

步骤 1　确定共享许可服务器 IP 地址和共享密钥：

license-server address *address* **secret** *secret* [**port** *port*]

示例：

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

如果更改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　使此设备成为共享许可备用服务器：

license-server backup enable *interface_name*

示例：

```
ciscoasa(config)# license-server backup enable inside
```

指定参与者与服务器进行连接的接口。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密钥，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
```

配置共享许可参与者

本节介绍如何配置共享许可参与者才能与共享许可服务器进行通信。

准备工作

参与者必须具有共享许可参与者密钥。

操作步骤

步骤 1　确定共享许可服务器 IP 地址和共享密钥：

license-server address *address* **secret** *secret* [**port** *port*]

示例：

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

如果更改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）如果配置了备用服务器，请输入备用服务器地址：

license-server backup address *address*

示例：

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

示例

以下示例设置许可服务器 IP 地址和共享密钥，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 PAK 许可证

本节介绍如何查看许可证信息。

- 查看当前许可证，第 3-33 页
- 监控共享许可证，第 3-43 页

查看当前许可证

本节介绍如何查看您的当前许可证，以及与基于时间的激活密钥对应的许可证的剩余时间。

准备工作

如果您拥有的是无负载加密型号，则在查看许可证时，将不会列出 VPN 许可证和统一通信许可证。有关详情，请参见无负载加密型号，第 3-23 页。

操作步骤

步骤 1　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 （包括永久许可证和活动的基于时间的许可证）：

show activation-key [**detail**]

detail 关键字还显示非活动的基于时间的许可证。

对于故障切换或集群设备，该命令还显示 “集群”许可证，该许可证包括所有设备的密钥。

示例

示例 3-1　　独立设备运行 show activation-key 命令时的输出

以下是独立设备运行 **show activation-key** 命令时的样本输出，其中显示运行许可证 （包括永久许可证和活动的基于时间的许可证）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 3-2　　独立设备运行 show activation-key detail 时的输出

以下是独立设备运行 **show activation-key detail** 命令时的样本输出，其中显示运行许可证（合并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 3-3　　故障切换对中的主设备运行 show activation-key detail 时的输出

以下是主故障切换设备运行 **show activation-key detail** 命令时的样本输出，其中显示：

- 主设备许可证 （合并的永久许可证和基于时间的许可证）。
- “故障切换集群”许可证 （来自主设备和辅助设备的合并许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主许可证和辅助许可证组合的值以粗体显示。
- 主设备永久许可证。
- 主设备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 3-4　　故障切换对中的辅助设备运行 show activation-key detail 时的输出

以下是辅助故障切换设备运行 **show activation-key detail** 命令时的样本输出，其中显示：

- 辅助设备许可证 （合并的永久许可证和基于时间的许可证）。
- “故障切换集群”许可证 （来自主设备和辅助设备的合并许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主许可证和辅助许可证组合的值以粗体显示。
- 辅助设备永久许可证。
- 辅助设备安装的基于时间的许可证 （活动和非活动）。此设备没有任何基于时间的许可证，因此在此样本输出中不会显示任何内容。

```
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 3-5　　没有许可证的 ASAv 独立设备运行 show activation-key 时的输出

部署了 1 个 vCPU 的 ASAv 的以下输出，显示了空白激活密钥、未许可状态以及一条表示安装 1 个 vCPU 许可证的消息。

备注　命令输出显示 “This platform has an ASAv VPN Premium license.”此消息指出 ASAv 可执行负载加密的条件；并不是指 ASAv 标准和高级版许可证。

```
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 3-6　　有 4 个 vCPU 标准许可证的 ASAv 独立设备运行 show activation-key 时的输出

备注 命令输出显示 “This platform has an ASAv VPN Premium license.”此消息指出 ASAv 可执行负载加密的条件；并不是指 ASAv 标准和高级版许可证。

```
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 3-7　　有 4 个 vCPU 高级许可证的 ASAv 独立设备运行 show activation-key 时的输出

备注 命令输出显示 “This platform has an ASAv VPN Premium license.”此消息指出 ASAv 可执行负载加密的条件；并不是指 ASAv 标准和高级版许可证。

```
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 3-8　　故障切换对中的 ASA 服务模块主要设备运行 show activation-key 时的输出

以下是主故障切换设备运行 **show activation-key** 命令时的样本输出，其中显示：

- 主设备许可证 （合并的永久许可证和基于时间的许可证）。
- “故障切换集群”许可证 （来自主设备和辅助设备的合并许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主许可证和辅助许可证组合的值以粗体显示。
- 主设备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 3-9　　故障切换对中的 ASA 服务模块辅助设备运行 show activation-key 时的输出

以下是辅助故障切换设备运行 **show activation-key** 命令时的样本输出，其中显示：

- 辅助设备许可证 （合并的永久许可证和基于时间的许可证）。
- “故障切换集群”许可证 （来自主设备和辅助设备的合并许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主许可证和辅助许可证组合的值以粗体显示。
- 辅助设备安装的基于时间的许可证 （活动和非活动）。此设备没有任何基于时间的许可证，因此在此样本输出中不会显示任何内容。

```
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 3-10　　集群运行 show activation-key 时的输出

```
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

要监控共享许可证，，然后输入以下命令之一。

- **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。

以下是许可证参与者上 **show shared license** 命令的样本输出：

```
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
```

以下是许可证服务器上 **show shared license detail** 命令的样本输出：

```
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
...
```

- **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。

PAK 许可证历史记录

功能名称	平台版本	说明
增加了连接数和 VLAN 数量	7.0(5)	提高了以下限制： • ASA5510 基础许可证连接数从 32000 增加到 50000；VLAN 数从 0 增加到 10。 • ASA5510 基础许可证连接数从 64000 增加到 130000；VLAN 数从 10 增加到 25。 • ASA5520 连接数从 130000 增加到 280000；VLAN 数从 25 增加到 100。 • ASA5540 连接数从 280000 增加到 400000；VLAN 数从 100 增加到 200。
SSL VPN 许可证	7.1(1)	引入了 SSL VPN 许可证。
增加了 SSL VPN 许可证数量	7.2(1)	为 ASA 5550 和更高版本引入了 5000 用户 SSL VPN 许可证。
ASA 5510 上的基础许可证增加了接口数	7.2(2)	对于 ASA 5510 上的基础许可证，最大接口数从 3 加管理接口数增加到无限个。
增加了 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 个故障切换；1 个限用于备用接口）增加到 20 个全功能接口。此外，中继端口数量也从 1 增加到 8。现在有 20 个全功能接口，您不需要使用 backup interface 命令禁用备用 ISP 接口的功能；您可以为其使用全功能接口。备用接口命令对于 Easy VPN 配置仍非常有用。 以下型号的 VLAN 数量限制也有所增加：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。 **备注**　接口名称仍为 Ethernet 0/0 和 Ethernet 0/1。 使用 **speed** 命令可更改接口上的速度，使用 **show interface** 命令可查看为每个接口当前配置的速度。

功能名称	平台版本	说明
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，远程计算机将对一系列规模大幅扩展的防病毒软件和反间谍软件应用、防火墙、操作系统以及相关更新进行扫描。它还会扫描您指定的所有注册表项、文件名和进程名称，并将扫描结果发送至 ASA。ASA 使用用户登录凭据和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，您可以进行相关配置，以尝试对不合规计算机进行更新 （使其符合版本要求），从而增强主机扫描。 思科可通过独立于思科安全桌面的软件包，对主机扫描所支持的应用和版本的列表进行及时更新。
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。
适用于移动设备的 AnyConnect 许可证	8.0(3)	引入了适用于移动设备的 AnyConnect 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。
增加了 ASA 5580 的 VLAN 数量	8.1(2)	在 ASA 5580 上支持的 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测应用会在其连接中使用 TLS 代理会话。根据 UC 许可证限制对每个 TLS 代理会话进行计数。所有这些应用都在 UC 代理伞状结构下获得许可，并且可以混合搭配使用。 此功能在版本 8.1 中不可用。
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 基础版许可证	8.2(1)	引入了 AnyConnect 基础版许可证。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 高级版许可证而不是 AnyConnect 基础版许可证。 **备注**　借助 AnyConnect 基础版许可证， VPN 用户可以使用 Web 浏览器来进行登录，然后下载并启动 (WebLaunch) AnyConnect 客户端。 AnyConnect 客户端软件提供一系列相同的客户端功能，无论是通过此许可证还是通过 AnyConnect 高级版许可证启用。 在特定 ASA 上， AnyConnect 基础版许可证不能和以下许可证同时处于活动状态：AnyConnect 高级版许可证 （所有类型）或高级终端评估许可证。但是，您可以在同一网络中的不同 ASA 上运行 AnyConnect 基础版和 AnyConnect 高级版许可证。 默认情况下， ASA 使用 AnyConnect 基础版许可证，但您可以通过使用 **webvpn**，然后使用 **no anyconnect-essentials** 命令将其禁用以使用其他许可证。

功能名称	平台版本	说明
SSL VPN 许可证更改为 AnyConnect 高级版 SSL VPN 版本许可证	8.2(1)	SSL VPN 许可证的名称更改为 AnyConnect 高级版 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。
10 GE I/O 许可证 （用于带 SSP-20 的 ASA 5585-X）	8.2(3)	引入了 10 GE I/O 许可证 （用于带 SSP-20 的 ASA 5585-X），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。 **备注**　在 8.3(x) 版本中不支持 ASA 5585-X。
10 GE I/O 许可证 （用于带 SSP-10 的 ASA 5585-X）	8.2(4)	引入了 10 GE I/O 许可证 （用于带 SSP-10 的 ASA 5585-X），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。 **备注**　在 8.3(x) 版本中不支持 ASA 5585-X。
不相同的故障切换许可证	8.3(1)	不再要求每个设备上的故障切换许可证相同。来自主设备和辅助设备的合并许可证是同时用于这两种设备的许可证。 修改了以下命令：**show activation-key** 和 **show version**。
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以堆叠。在许多情况下，您可能需要续订基于时间的许可证，并从旧许可证无缝过渡到新许可证。对于只有基于时间的许可证时才可提供的功能，在应用新许可证之前，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，也不必担心因为提前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。
基于时间的许可证以正常运行时间为基础	8.3(1)	基于时间的许可证现在根据 ASA 的总正常运行时间进行倒计时；系统时钟不会影响许可证。
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，每个功能一次只能有一个许可证处于活动状态。 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。 修改了以下命令：**activation-key [activate | deactivate]**。
AnyConnect 高级版 SSL VPN 版本许可证更改为 AnyConnect 高级版 SSL VPN 许可证	8.3(1)	AnyConnect 高级版 SSL VPN 版本许可证的名称更改为 AnyConnect 高级版 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，则会禁用统一通信、强加密 VPN 和强加密管理协议。 **备注**　仅在 8.3(x) 版本中支持此专用映像；要在 8.4(1) 及更高版本中获得无负载加密支持，您需要购买专用硬件版本的 ASA。

功能名称	平台版本	说明
增加了 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 增加到 100。对于带 SSP-20 和更高版本的 ASA 5580 和 5585-X，最大数量从 50 增加到 250。
增加了 ASA 5580 和 5585-X 的 VLAN 数量	8.4(1)	对于 ASA 5580 和 5585-X，最大 VLAN 数量从 250 增加到 1024。
增加了 ASA 5580 和 5585-X 的连接数	8.4(1)	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 高级版 SSL VPN 许可证更改为 AnyConnect 高级版许可证	8.4(1)	AnyConnect 高级版 SSL VPN 许可证的名称更改为 AnyConnect 高级版许可证。许可证信息显示从 “SSL VPN Peers” 更改为 “AnyConnect Premium Peers”。
增加了 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。
增加了 ASA 5580 的其他 VPN 会话数	8.4(1)	其他 VPN 会话限制从 5,000 增加到 10,000。
使用 IKEv2 的 IPsec 远程访问 VPN	8.4(1)	向 AnyConnect 基础版和 AnyConnect 高级版许可证中添加了使用 IKEv2 的 IPsec 远程访问 VPN。 **备注**　在我们对 ASA 上的 IKEv2 的支持中存在以下限制：目前不支持重复的安全关联。 IKEv2 站点间会话已添加到其他 VPN 许可证 （以前为 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)	对于附带无负载加密功能的型号 （例如 ASA 5585-X），ASA 软件会禁用统一通信和 VPN 功能，从而使 ASA 可供出口到特定国家/地区。
适用于 SSP-20 和 SSP-40 的双 SSP	8.4(2)	对于 SSP-40 和 SSP-60，您可以在同一机箱中使用两个相同级别的 SSP。不支持混合级别的 SSP （例如，不支持混用 SSP-40 和 SSP-60）。每个 SSP 均作为独立设备，可单独配置和管理。如果需要，可以将两个 SSP 用作故障切换对。当在机箱中使用两个 SSP 时不支持 VPN；但请注意，VPN 并没有被禁用。
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)	为 ASA 5580 和 5585-X 添加了集群许可证。
在 ASASM 上支持 VPN	9.0(1)	ASASM 现在支持所有 VPN 功能。
在 ASASM 上支持统一通信	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 现在支持所有 SSP 型号使用双 SSP （在同一机箱中，您可以使用两个相同级别的 SSP）。使用双 SSP 时，现在支持 VPN。

功能名称	平台版本	说明
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 ASAv4 与 ASAv30 标准和高级版型号许可证	9.2(1)	ASAv 随附简化的许可方案：标准或高级版级别的 ASAv4 和 ASAv30 永久许可证。无可用的附加许可证。



适用于 ASAv 的智能软件许可

通过思科智能软件许可，您可以集中购买和管理许可证池。与产品授权密钥 (PAK) 许可证不同，智能许可证未绑定到特定序列号。您可以轻松部署或停用 ASAv，而不必管理每台设备的许可证密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。

- 支持的许可证，第 4-1 页
- 关于智能软件许可，第 4-4 页
- 智能软件许可必备条件，第 4-6 页
- 智能软件许可准则，第 4-6 页
- 智能软件许可的默认设置，第 4-6 页
- 配置智能软件许可，第 4-7 页
- 管理智能软件许可，第 4-8 页
- 监控智能软件许可，第 4-9 页
- 智能软件许可历史记录，第 4-11 页

支持的许可证

本节列出可用于 ASAv 的许可证授权。

- ASAv5 和 ASAv10，第 4-2 页
- ASAv30，第 4-3 页
- 许可证说明，第 4-4 页

ASAv5 和 ASAv10

表 4-1　　ASAv5 和 ASAv10 许可证功能

许可证	标准许可证
防火墙许可证	
僵尸网络流量过滤器	支持
并发防火墙连接数	100,000
GTP/GPRS	支持
公司间媒体引擎	支持
UC 电话代理会话数， UC 代理会话总数	500
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。	
AnyConnect 高级版对等体数 （最大数量）	250
	共享许可证：不支持
高级 终端评估	启用
适用于思科 VPN 电话的 AnyConnect	启用
AnyConnect Essentials	禁用
适用于移动设备的 AnyConnect	启用
其他 VPN 许可证	
VPN 对等体总数 （包括所有类型）	250
其他 VPN 对等体数	250
VPN 负载均衡	启用
通用许可证	
吞吐量级别	ASAv5：100 Mbps ASAv10：1 Gbps
加密	强 (3DES/AES)
故障转移	现用/备用
所有类型的最大接口数	716
安全情景	不支持
群集	不支持
最大 VLAN 数量	50
RAM，vCPU 数量，vCPU 频率限制	2 GB， 1 个 vCPU， 5000 MHz

ASAv30

表 4-2　　ASAv30 许可证功能

许可证	标准许可证
防火墙许可证	
僵尸网络流量过滤器	支持
并发防火墙连接数	500,000
GTP/GPRS	支持
公司间媒体引擎	支持
UC 电话代理会话数， UC 代理会话总数	1000
VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。购买 AnyConnect 许可证时，请参阅以下最大值。	
AnyConnect 高级版对等体数 （最大数量）	750
	共享许可证：不支持
高级 终端评估	启用
适用于思科 VPN 电话的 AnyConnect	启用
AnyConnect Essentials	禁用
适用于移动设备的 AnyConnect	启用
其他 VPN 许可证	
VPN 对等体总数 （包括所有类型）	750
其他 VPN 对等体数	750
VPN 负载均衡	启用
通用许可证	
吞吐量级别	2 Gbps
加密	强 (3DES/AES)
故障转移	现用/备用
所有类型的最大接口数	1316
安全情景	不支持
群集	不支持
最大 VLAN 数量	200
RAM，vCPU 数量，vCPU 频率限制	8 GB， 4 个 vCPU， 20000 MHz **备注**　如果选择部署 2 个或 3 个 vCPU，请参阅以下值： 2 个 vCPU - 4 GB RAM， 10000 MHz 的 vCPU 频率限制， 250,000 个并发防火墙连接。 3 个 vCPU - 4 GB RAM， 15000 MHz 的 vCPU 频率限制， 350,000 个并发防火墙连接。

许可证说明

下表包含有关许可证的其他信息。

表 4-3　　许可证说明

许可证	备注
AnyConnect Premium	VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。 AnyConnect 高级版会话包括以下 VPN 类型： • SSL VPN • 无客户端 SSL VPN • 使用 IKEv2 的 IPsec 远程访问 VPN
加密	无法禁用 DES 许可证。虽然安装了 3DES 许可证，但是 DES 仍然可用。要在希望仅使用强加密时防止使用 DES，请务必将所有相关命令都配置为仅使用强加密。

所有类型的最大接口数	最大整合接口数；例如， VLAN 接口、物理接口、冗余接口、网桥组接口和 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，即使 GigabitEthernet 0/0 接口被定义为 port-channel 1 的一部分，以下两个接口也要计数：
	`interface gigabitethernet 0/0`
	和
	`interface port-channel 1`

其他 VPN	其他 VPN 会话包括以下 VPN 类型： • 使用 IKEv1 的 IPsec 远程访问 VPN • 使用 IKEv1 的 IPsec 站点间 VPN • 使用 IKEv2 的 IPsec 站点间 VPN
VPN （会话）总数 （包括所有类型）	• 虽然最大总 VPN 会话数累计超过最大 VPN AnyConnect 会话数和其他 VPN 会话数，但是合并会话数不应超过 VPN 会话限制。如果超过最大 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，然后从门户启动 AnyConnect 客户端会话，总计使用的是 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，则会使用 2 个会话。

最大 VLAN 数量	对于根据 VLAN 限制计数的接口，您必须向其分配 VLAN。例如：
	`interface gigabitethernet 0/0.100`
	`  vlan 100`

关于智能软件许可

本节介绍如何结合使用智能软件许可与 ASAv。

- 智能软件管理器和帐户，第 4-5 页
- 按虚拟帐户管理的许可证和设备，第 4-5 页
- 设备注册和令牌，第 4-5 页
- 与许可证颁发机构的定期通信，第 4-5 页
- 不合规状态，第 4-5 页

智能软件管理器和帐户

为 ASAv 购买一个或多个许可证时，可在思科智能软件管理器中对其进行管理：

http://tools.cisco.com/rhodui/index

通过智能软件管理器，您可以为组织创建一个主帐户。

默认情况下，许可证分配给主帐户下的*默认虚拟帐户*。作为帐户管理员，您可以选择创建其他虚拟帐户；例如，您可以为区域、部门或子公司创建帐户。通过多个虚拟帐户，您可以更轻松地管理大量许可证和设备。

按虚拟帐户管理的许可证和设备

仅当虚拟帐户的 ASAv 可以使用分配给该帐户的许可证时，才能按虚拟帐户对许可证和设备进行管理。如果您需要其他许可证，则可以从另一个虚拟帐户传输未使用的许可证。您还可以在虚拟帐户之间传输 ASAv。

设备注册和令牌

对于每个虚拟帐户，您可以创建注册令牌。默认情况下，此令牌有效期为 30 天。当部署每个 ASAv 或注册现有 ASAv 时，请输入此令牌 ID 以及授权级别。如果现有令牌已过期，则可以创建新的令牌。

在完成部署后或在现有 ASAv 上手动配置这些参数后启动时， ASAv 会向思科许可证颁发机构进行注册。当 ASAv 向令牌注册时，许可证颁发机构会为设备与许可证颁发机构之间的通信颁发 ID 证书。此证书有效期为 1 年，但需要每 6 个月续签一次。

与许可证颁发机构的定期通信

ASAv 每 30 天与许可证颁发机构进行通信。如果您在智能软件管理器中进行更改，则可以刷新 ASAv 上的授权，以使更改立即生效。或者，也可以等待 ASAv 按计划通信。

您可以随意配置 HTTP 代理。ASAv 必须可以直接访问互联网，或者至少每 90 天通过 HTTP 代理访问互联网。常规许可证通信每 30 天进行一次，但如果 ASAv 具有宽限期，则会最多运行 90 天，而不会进行自动通报。您必须在 90 天截止前与许可证颁发机构联系。

备注　不支持离线许可。

不合规状态

ASAv 在以下情况下可能会处于不合规状态：

- 过度使用 - 当 ASAv 使用不可用的许可证时。
- 许可证到期 - 当基于时间的许可证到期时。
- 通信不畅 - 当 ASAv 无法访问许可证颁发机构以重新获得授权时。

在 90 天过后进行重新授权尝试时， ASAv 将严格限制速率，直至您能够成功地重新获得授权为止。

Smart Call Home 基础设施

默认情况下， Smart Call Home 配置文件在名为 “License”的配置中。此配置文件可指定许可证颁发机构的 URL。您无法删除此配置文件。请注意，许可证配置文件的唯一可配置选项是许可证颁发机构的目标地址 URL。除非获得思科 TAC 的指示，否则不应更改许可证颁发机构 URL。

您无法为智能软件许可禁用 Smart Call Home；例如，即使使用 no service call-home 命令禁用 Smart Call Home，也不会禁用智能软件许可。

除非您专门配置其他 Smart Call Home 功能，否则不会开启这些功能。

智能软件许可必备条件

- 在思科智能软件管理器上创建主帐户：

  http://tools.cisco.com/rhodui/index
- 从思科软件中心购买一个或多个 ASAv 许可证。
- 确保可从 ASAv 访问互联网或访问 HTTP 代理，以使 ASAv 能够访问许可证颁发机构。不支持离线许可。
- 配置 DNS 服务器，以使 ASA 能够解析许可证颁发机构服务器的名称。请参阅配置 DNS 服务器，第 16-13 页。

智能软件许可准则

故障转移

您必须使用同一型号许可证部署两台设备。

其他准则

您不能将基于 PAK 的许可用于 ASAv。仅支持智能软件许可。如果升级现有 PAK 许可的 ASAv，则以前安装的激活密钥将被忽略，但会保留在设备上。如果将 ASAv 降级，则将恢复激活密钥。

智能软件许可的默认设置

- ASAv 默认配置包括名为 “License”的 Smart Call Home 配置文件，该文件用于指定许可证颁发机构的 URL。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

- 在部署 ASAv 时，您可设置功能层和吞吐量级别。此时仅标准级别可用。

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
```

- 此外，在配置过程中，您还可以选择配置 HTTP 代理。

```
call-home
  http-proxy ip_address port port
```

配置智能软件许可

在部署 ASAv 时，设备向许可证颁发机构注册，并会根据部署时输入的值来启用智能软件许可。如果需要为现有 ASAv 更改许可证授权或配置智能软件许可，请执行以下任务：

步骤 1　（可选）配置 HTTP 代理，第 4-7 页。

步骤 2　设置智能许可证授权，第 4-7 页。

步骤 3　向许可证颁发机构注册 ASAv，第 4-8 页。

（可选）配置 HTTP 代理

如果您的网络使用 HTTP 代理进行互联网访问，则必须为智能软件许可配置代理地址。此代理一般也用于 Smart Call Home。

操作步骤

步骤 1　指定 HTTP 代理 URL：

```
call-home
  http-proxy ip_address port port
```

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

设置智能许可证授权

要请求许可证授权，请执行以下程序。

操作步骤

步骤 1　进入许可证智能配置模式：

```
license smart
```

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

步骤 2　设置功能层：

```
feature tier standard
```

仅标准层可用。

步骤 3　设置吞吐量级别：

```
throughput level {100M | 1G | 2G}
```

示例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

步骤 4　退出许可证智能模式以应用更改：

exit

示例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

在通过以下方式退出许可证智能配置模式之前，更改将不会生效：明确退出该模式（**exit** 或 **end**）或输入使您进入其他模式的任何命令。

向许可证颁发机构注册 ASAv

当注册 ASAv 时，许可证颁发机构会为 ASAv 与许可证颁发机构之间的通信颁发 ID 证书。它还会将 ASAv 分配到相应的虚拟帐户。通常，此程序是一次性实例。但是，如果 ID 证书由于诸如通信问题等原因而到期，则稍后可能需要重新注册 ASAv。

操作步骤

步骤 1　在智能软件管理器中，为要将此 ASAv 添加到的虚拟帐户请求并复制注册令牌。

步骤 2　在 ASAv 中输入注册令牌：

license smart register idtoken *id_token* [**force**]

示例：

```
ciscoasa# license smart register idtoken
YjE3Njc5MzYtMGQzMi00OTA4LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQkd
YRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

使用 **force** 关键字注册已注册但可能与许可证颁发机构不同步的 ASAv。例如，如果从智能软件管理器中意外删除了 ASAv，请使用 **force**。

ASAv 尝试向许可证颁发机构注册并请求对已配置的许可证授权进行授权。

管理智能软件许可

您可能需要从帐户取消注册 ASAv，或者手动更新 ID 证书或许可证授权。

- 取消注册 ASAv，第 4-9 页
- 更新 ID 证书或许可证授权，第 4-9 页

取消注册 ASAv

对 ASAv 取消注册会从帐户中删除 ASAv。系统会删除 ASAv 中的所有许可证授权和证书。您可能希望取消注册来为新的 ASAv 释放许可证。或者，也可以从智能软件管理器删除 ASAv。

操作步骤

步骤 1　取消注册 ASAv：

```
license smart deregister
```

更新 ID 证书或许可证授权

默认情况下， ID 证书每 6 个月自动更新，许可证授权每 30 天更新。如果您访问互联网的时间有限，或者在例如智能软件管理器中进行了任何许可更改，则可能要为其中任一项手动更新注册。

操作步骤

步骤 1　更新 ID 证书：

```
license smart renew id
```

步骤 2　更新许可证授权：

```
license smart renew auth
```

监控智能软件许可

您可以监控许可证功能、状态和证书，以及启用调试消息。

- 查看当前许可证，第 4-9 页
- 查看智能许可证状态，第 4-10 页
- 显示 ID 证书信息，第 4-10 页
- 调试智能软件许可，第 4-11 页

查看当前许可证

请参阅以下命令以查看许可证：

- **show activation-key**, **show license features**

  以下示例显示仅有基础许可证 （无最新许可证授权）的 ASAv：

```
Serial Number:  9AAHGX8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured
```

```
Licensed features for this platform:
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
```

- **show license entitlement**

  显示有关每个使用中的授权及其句柄 （即整数 ID）、计数、标签、执行模式 （例如，合规、不合规等）、版本和授权请求时间的详细信息。

查看智能许可证状态

请参阅以下命令以查看许可证状态：

- **show license all**

  显示智能软件许可的状态、智能代理版本、 UDI 信息、智能代理状态、全局合规状态、授权状态、许可证书信息和计划智能代理任务。

- **show license registration**

  显示当前智能许可证注册状态。

- **show license pool**

  显示此设备分配到的授权池。

显示 ID 证书信息

请参阅以下命令以查看许可证 ID 证书：

- **show license cert**

  显示 ID 证书内容、颁发日期和到期日期。

调试智能软件许可

请参阅以下用于调试集群的命令：

- **debug license agent** {**error** | **trace** | **debug** | **all**}

  从智能代理打开调试。

- **debug license** *level*

  打开各种级别的智能软件许可管理器调试。

智能软件许可历史记录

功能名称	平台版本	说明
面向 ASAv 的思科智能软件许可	9.3(2)	通过智能软件许可，您可以购买和管理许可证池。与 PAK 许可证不同，智能许可证未绑定到特定序列号。您可以轻松部署或停用 ASAv，而不必管理每台设备的许可证密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。 引入了以下命令：**clear configure license**、 **debug license agent**、 **feature tier**、 **http-proxy**、 **license smart**、 **license smart deregister**、 **license smart register**、 **license smart renew**、 **show license**、 **show running-config license**、 **throughput level**



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下的工作方式。本章还包含有关自定义透明防火墙操作的信息。

可以在多情景模式下为每个情景独立设置防火墙模式。

- 关于防火墙模式，第 5-1 页
- 默认设置，第 5-6 页
- 防火墙模式准则，第 5-6 页
- 设置防火墙模式，第 5-7 页
- 为透明防火墙配置 ARP 检测，第 5-8 页
- 自定义透明防火墙的 MAC 地址表，第 5-9 页
- 监控透明防火墙，第 5-10 页
- 防火墙模式示例，第 5-11 页
- 防火墙模式历史记录，第 5-22 页

关于防火墙模式

- 关于路由防火墙模式，第 5-1 页
- 关于透明防火墙模式，第 5-2 页

关于路由防火墙模式

在路由模式下，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。

关于透明防火墙模式

通常情况下，防火墙是一个路由跃点，并充当与其中一个被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 “嵌入式防火墙”或 “隐藏防火墙”，而不被视为已连接设备的路由器跃点。

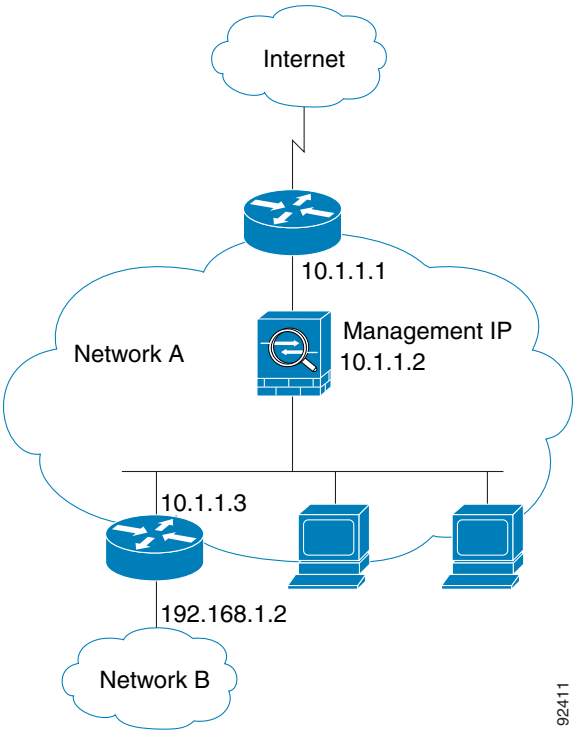
- 在网络中使用透明防火墙，第 5-2 页
- 网桥组，第 5-3 页
- 管理接口，第 5-3 页
- 允许第 3 层流量，第 5-3 页
- 允许的 MAC 地址，第 5-4 页
- 路由模式下不允许通过流量，第 5-4 页
- BPDU 处理，第 5-4 页
- MAC 地址与路由查找，第 5-4 页
- ARP 检测，第 5-5 页
- MAC 地址表，第 5-5 页

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，因此可以将透明防火墙轻松引入到现有网络中。

图 5-1 显示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

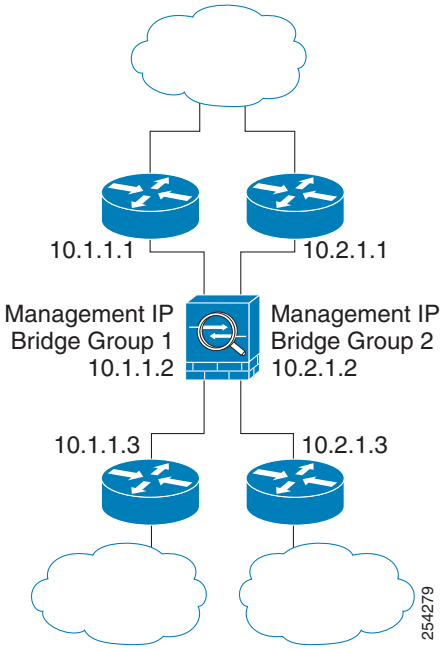


网桥组

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。网桥组的流量相互分离；流量不会路由至 ASA 中的另一个网桥组，并且流量必须退出 ASA 后才能通过外部路由器路由回 ASA 中的另一个网桥组。虽然每个网桥组的桥接功能是独立的，但所有网桥组之间可共享很多其他功能。例如，所有网桥组都共享系统日志服务器或 AAA 服务器的配置。为完全分离安全策略，请在每个情景中对一个网桥组使用安全情景。

图 5-2 显示连接到 ASA 的两个网络，后者具有两个网桥组。

图 5-2　　具有两个网桥组的透明防火墙网络



备注　每个网桥组都需要一个管理 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 地址必须与已连接网络位于同一子网上。有关其他管理方法，请参阅管理接口，第 5-3 页。

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

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

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。

注意　可使用访问规则允许广播和组播流量通过。有关详情，请参阅防火墙配置指南。

- 允许 ARP 双向通过透明防火墙，而无需 ACL。ARP 流量可通过 ARP 检测进行控制。
- 允许 IPv6 邻居发现和路由器请求数据包双向通过透明防火墙，而无需 ACL。
- 对于从低安全性接口传播到高安全性接口的第 3 层流量，要求低安全性接口上有扩展 ACL。有关详情，请参阅防火墙配置指南。

允许的 MAC 地址

允许以下目标 MAC 地址通过透明防火墙。系统会丢弃此列表中未列出的任何 MAC 地址。

- 实际广播目标 MAC 地址等于 FFFF.FFFF.FFFF
- IPv4 组播 MAC 地址的范围是 0100.5E00.0000 至 0100.5EFE.FFFF
- IPv6 组播 MAC 地址的范围是 3333.0000.0000 至 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 至 0900.07FF.FFFF

路由模式下不允许通过流量

在路由模式下，某些类型的流量无法通过 ASA，即使在 ACL 中允许其通过也如此。但是，透明防火墙可使用扩展 ACL（用于 IP 流量）或 EtherType 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）可使用 EtherType ACL 配置为通过。

备注　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 EtherType 的任何数据包通过。BPDU 和 IS-IS 除外，它们受支持。

允许路由模式下通过流量的功能

对于透明防火墙不直接支持的功能，您可以允许流量通过，以便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 EtherType ACL 配置为拒绝 BPDU。如果使用故障切换功能，则可能要阻止 BPDU，以防止交换机端口在拓扑结构更改时进入阻止状态。有关详情，请参见故障切换的透明防火墙模式要求，第 7-14 页。

MAC 地址与路由查找

当 ASA 在透明模式下运行时，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，则必须使用静态路由，以便 ASA 可以访问该子网。
- 在 NAT 启用的情况下距离 ASA 至少一跳的流量 - 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距离 ASA 至少一跳的情况下的 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，则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
  - Skinny (SCCP)

ARP 检测

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

当启用 ARP 检测查时，ASA 将所有 ARP 数据包中的 MAC 地址、IP 地址和源接口与 ARP 表中的静态条目进行比较，并执行下列操作：

- 如果 IP 地址、 MAC 地址和源接口与 ARP 条目匹配，则数据包可以通过。
- 如果 MAC 地址、 IP 地址或接口之间不匹配，则 ASA 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，则可以将 ASA 设置为从所有接口向外转发数据包 （泛洪），或者丢弃数据包。

注意　即使此参数设置为 flood，专用管理接口 （如果有）也绝不会以泛洪方式传输数据包。

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；网关路由器使用网关路由器 MAC 地址进行响应。但是，攻击者使用攻击者 MAC 地址 （而不是路由器 MAC 地址）将其他 ARP 响应发送到主机。这样，攻击者即可在所有主机流量转发到路由器之前将其拦截。

ARP 检测确保只要静态 ARP 表中的 MAC 地址和相关 IP 地址正确，攻击者就无法利用攻击者 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 地址与源接口相关联，以便 ASA 可了解如何将要发送到设备的任何数据包从正确的接口发出。

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，则 ASA 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 为目标 IP 地址生成 ARP 请求，以便 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，以便 ASA 可了解哪个接口接收 ping 应答。

系统会丢弃原始数据包。

默认设置

默认模式为路由模式。

透明模式默认设置

- 默认情况下，允许所有 ARP 数据包通过 ASA。
- 如果启用 ARP 检测，则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，并且 ASA 会将对应的条目添加到 MAC 地址表中。

防火墙模式准则

情景模式规定

根据情景设置防火墙模式。

透明防火墙准则

- 在透明防火墙模式下，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 的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时所需的路由）仅适用于来自一个网桥组网络的管理流量。这是因为默认路由会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，则需要指定静态路由来确定预期会发出管理流量的网络。

有关详细准则，请参阅路由模式和透明模式接口准则，第 13-4 页。

IPv6 规定

支持 IPv6。

其他准则和限制

- 更改防火墙模式时， ASA 会清除运行配置，因为许多命令不会在这两种模式下同时受到支持。启动配置会保持不变。如果重新加载而不保存，则会加载启动配置，且模式会恢复为原始设置。有关备份配置文件的信息，请参阅设置防火墙模式，第 5-7 页。
- 如果将文本配置下载到 ASA 且使用 **firewall transparent** 命令来更改模式，请确保将该命令放在配置的顶部；ASA 会在读取命令后立即更改模式并继续读取下载的配置。如果此命令显示在配置的后面部分，则 ASA 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，请参阅设置 ASA 映像、 ASDM 和启动配置，第 33-18 页。

透明模式下不支持的功能

表 5-1 列出透明模式下不支持的功能。

表 5-1　透明模式下不支持的功能

功能	描述
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 中继不是必需的，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向另一个方向传输。
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 中允许组播流量通过，从而允许此类流量通过 ASA。
QoS	-
针对直通流量终止 VPN	透明防火墙仅支持用于管理连接的站点间 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，但其不会终止非管理连接。无客户端 SSL VPN 也不受支持。
统一通信	-

设置防火墙模式

备注　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

更改模式时， ASA 会清除运行配置 （有关详细信息，请参阅防火墙模式准则，第 5-6 页）。

- 如果您已经具有填充的配置，请务必在更改模式之前备份配置；在创建新配置时，可以使用此备份作为参考。请参阅备份和恢复配置或其他文件，第 33-22 页。
- 在控制台端口处使用 CLI 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，并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。

操作步骤

备注　要将防火墙模式设置为透明模式，并要在清除配置后配置 ASDM 管理访问，请参阅配置 ASDM 访问，第 2-7 页。

步骤 1　将防火墙模式设置为透明：

firewall transparent

示例：

```
ciscoasa(config)# firewall transparent
```

要将模式更改为路由模式，请输入 **no firewall transparent** 命令。

备注　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

要配置 ARP 检测，请执行以下步骤：

步骤 1　根据添加静态 ARP 条目，第 5-8 页中所述添加静态 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，因此该功能需要静态 ARP 条目。

步骤 2　根据启用 ARP 检测，第 5-9 页中所述启用 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。尽管主机通过 IP 地址标识数据包目标，但是以太网上数据包的实际传递仍然依赖于以太网 MAC 地址。当路由器或主机要在直连网络上传递数据包时，它会发送 ARP 请求，要求获取与 IP 地址关联的 MAC 地址，然后根据 ARP 响应将数据包传递到该 MAC 地址。主机或路由器会保留 ARP 表，因此不必对需要传递的每个数据包都发送 ARP 请求。只要在网络上发送 ARP 响应，便会动态更新 ARP 表，但如果一段时间未使用条目，则它会超时。如果条目不正确 （例如，给定 IP 地址的 MAC 地址发生更改），则该条目在可以更新之前会超时。

备注　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）。

操作步骤

步骤 1　添加静态 ARP 条目：

arp *interface_name ip_address mac_address*

示例：

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

这允许来自外部接口上 IP 地址为 10.1.1.1、 MAC 地址为 0009.7cbe.2100 的路由器的 ARP 响应。

启用 ARP 检测

本节介绍如何启用 ARP 检测。

操作步骤

步骤 1　启用 ARP 检测：

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

示例：

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

flood 关键字用于将不匹配的 ARP 数据包转发出所有接口，**no-flood** 关键字用于丢弃不匹配的数据包。默认设置是以泛洪方式传输不匹配的数据包。要通过 ASA 的 ARP 仅限于静态条目，请将此命令设置为 **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。

- 添加静态 MAC 地址，第 5-9 页
- 设置 MAC 地址超时，第 5-10 页
- 禁用 MAC 地址获悉，第 5-10 页

添加静态 MAC 地址

通常，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，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与静态条目不匹配的接口发送流量，则 ASA 会丢弃这些流量并生成系统消息。当添加静态 ARP 条目时（请参阅添加静态 ARP 条目，第 5-8 页），静态 MAC 地址条目会自动添加到 MAC 地址表中。

要将静态 MAC 地址添加到 MAC 地址表，请执行以下步骤。

操作步骤

步骤 1　添加静态 MAC 地址条目：

mac-address-table static *interface_name mac_address*

示例：

```
ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100
```

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。要更改超时，请执行以下步骤：

操作步骤

步骤 1　设置 MAC 地址条目超时：

mac-address-table aging-time *timeout_value*

示例：

```
ciscoasa(config)# mac-address-table aging-time 10
```

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 地址获悉

默认情况下，每个接口会自动获悉进入流量的 MAC 地址，并且 ASA 会将对应的条目添加到 MAC 地址表中。如有必要，可以禁用 MAC 地址获悉；然而除非将 MAC 地址静态添加到表中，否则没有流量可以通过 ASA。

要禁用 MAC 地址获悉，请执行以下步骤：

操作步骤

步骤 1　禁用 MAC 地址获悉：

mac-learn *interface_name* **disable**

示例：

```
ciscoasa(config)# mac-learn inside disable
```

此命令的 **no** 形式会重新启用 MAC 地址获悉。

clear configure mac-learn 命令会在所有接口上重新启用 MAC 地址获悉。

监控透明防火墙

命令	目的
show arp-inspection	监控 ARP 检测。显示所有接口上的 ARP 检测的当前设置。
show mac-address-table [*interface_name*]	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。

示例

以下是 **show mac-address-table** 命令 （用于显示整个 MAC 地址表）的样本输出：

```
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 （用于显示内部接口的 MAC 地址表）的样本输出：

```
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。

- 路由防火墙模式下数据通过 ASA 的方式，第 5-11 页
- 数据通过透明防火墙的方式，第 5-17 页

路由防火墙模式下数据通过 ASA 的方式

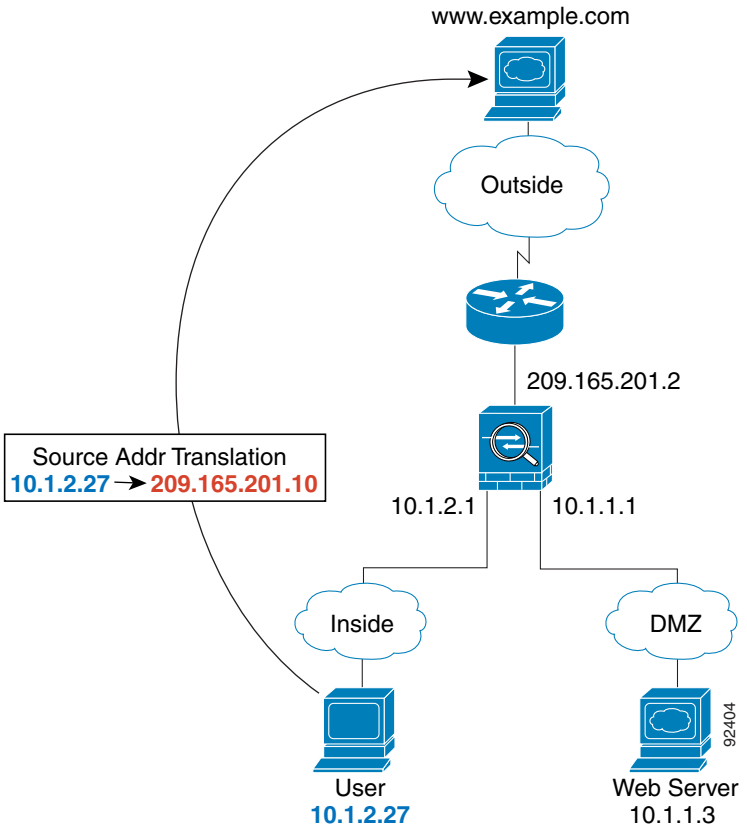
本节介绍路由防火墙模式下数据通过 ASA 的方式。

- 内部用户访问 Web 服务器，第 5-12 页
- 外部用户访问 DMZ 上的 Web 服务器，第 5-13 页
- 内部用户访问 DMZ 上的 Web 服务器，第 5-14 页
- 外部用户尝试访问内部主机，第 5-15 页
- DMZ 用户尝试访问内部主机，第 5-16 页

内部用户访问 Web 服务器

图 5-3 显示内部用户访问外部 Web 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）验证数据包是否获得允许。

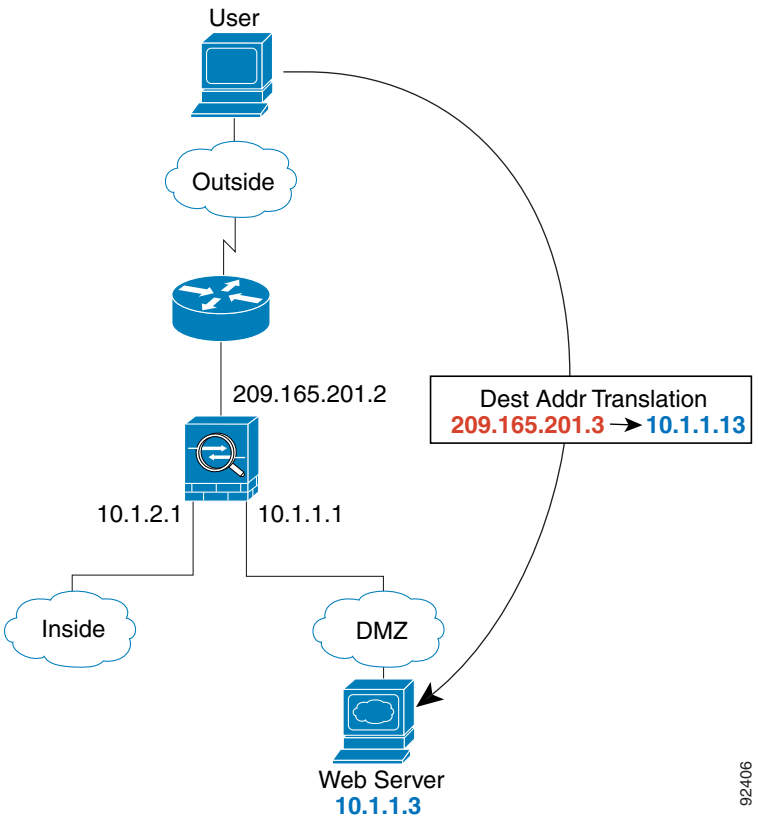
   对于多情景模式， ASA 会首先将数据包分类到一个情景中。
3. ASA 将本地源地址 (10.1.2.27) 转换为位于外部接口子网上的全局地址 209.165.201.10。

   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，则可简化路由。
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. 当 www.example.com 响应请求时，数据包会通过 ASA，由于已建立会话，因此数据包会绕过许多与新连接关联的查找。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 Web 服务器

图 5-4 显示访问 DMZ Web 服务器的外部用户。

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）：

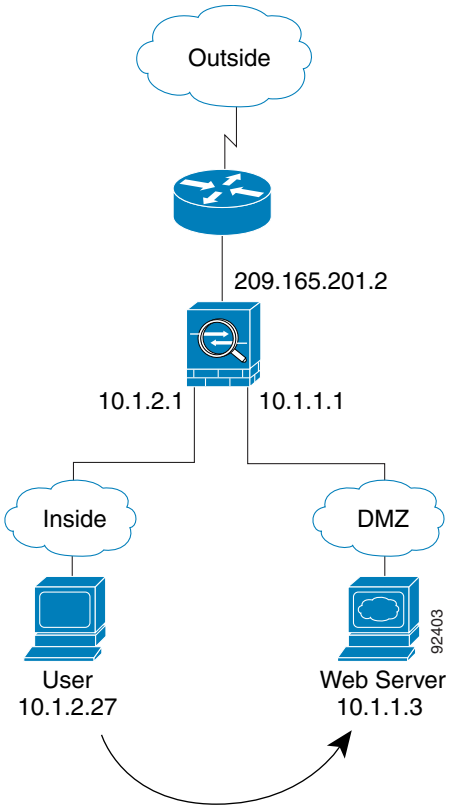
1. 外部网络上的用户使用位于外部接口子网上的全局目标地址 209.165.201.3 从 DMZ Web 服务器请求访问网页。
2. ASA 接收数据包并将目标地址逆向转换为本地地址 10.1.1.3。
3. 由于它是新会话，因此 ASA 会根据安全策略条款 （访问列表、过滤器、 AAA）验证数据包是否获得允许。

   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 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 Web 服务器响应请求时，数据包会通过 ASA，由于已建立会话，因此数据包会绕过许多与新连接关联的查找。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 Web 服务器

图 5-5 显示访问 DMZ Web 服务器的内部用户。

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）：

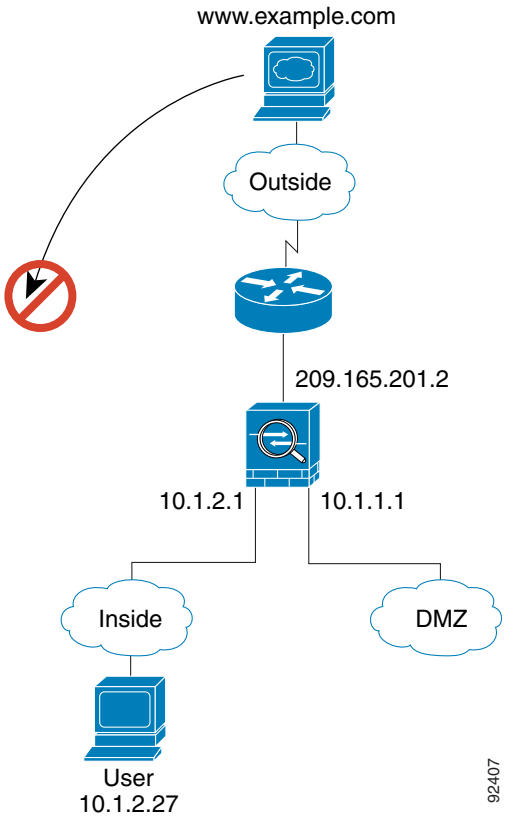
1. 内部网络上的用户使用目标地址 10.1.1.3 从 DMZ Web 服务器请求访问网页。
2. ASA 接收数据包；由于是新会话，因此 ASA 会根据安全策略条款 （访问列表、过滤器、AAA）验证数据包是否获得允许。

   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 Web 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许多与新连接关联的查找。
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） 验证数据包是否获得允许。

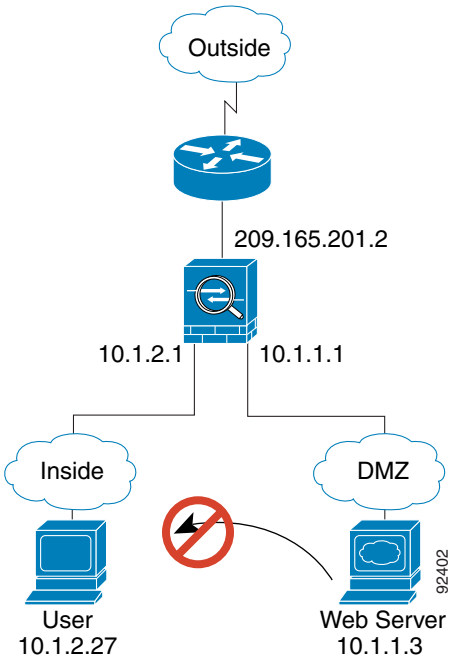
3. 系统会拒绝数据包，而 ASA 则丢弃数据包并记录连接尝试情况。

   如果外部用户尝试攻击内部网络，则 ASA 会采用多种技术来确定数据包对于已建立的会话是否有效。

DMZ 用户尝试访问内部主机

图 5-7 显示 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）：

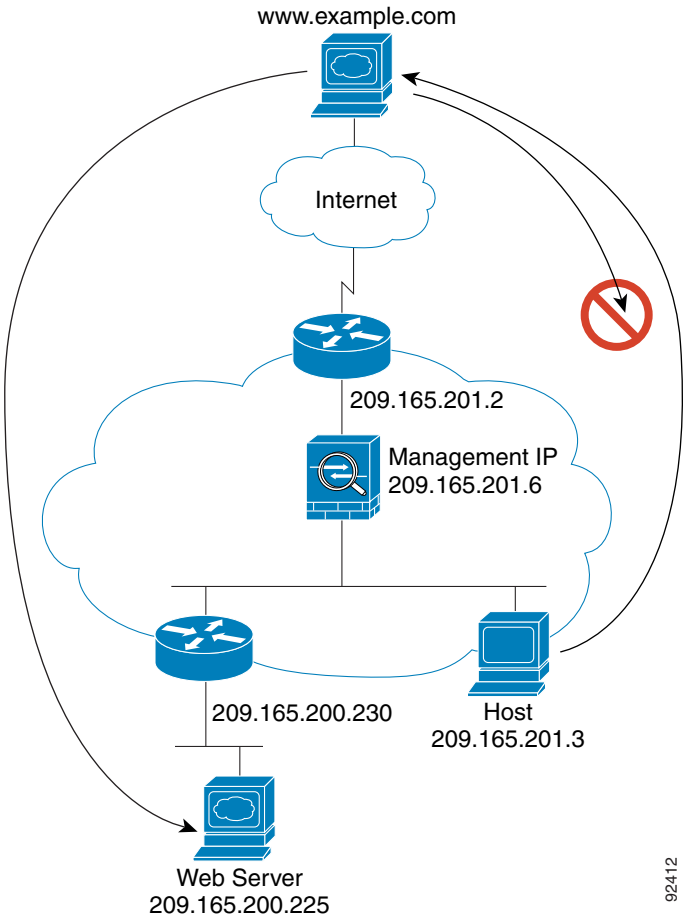
1. DMZ 网络上的用户尝试访问内部主机。由于 DMZ 不必路由互联网上的流量，因此专用寻址方案不会防止路由。
2. ASA 接收数据包，由于是新会话，因此 ASA 会根据安全策略 （访问列表、过滤器、 AAA）验证数据包是否获得允许。

   系统会拒绝数据包，而 ASA 则丢弃数据包并记录连接尝试情况。

数据通过透明防火墙的方式

图 5-8 显示包含公共 Web 服务器的内部网络上的典型透明防火墙实施。ASA 具有访问列表，以便内部用户可访问互联网资源。通过其他访问列表，外部用户只能访问内部网络上的 Web 服务器。

图 5-8　典型透明防火墙数据路径



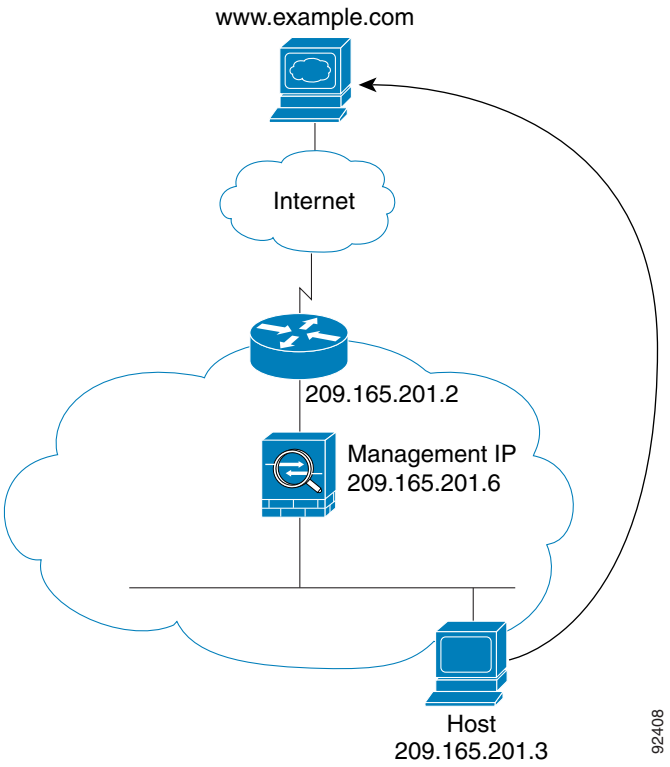
本节介绍数据如何通过 ASA。

- 内部用户访问 Web 服务器，第 5-18 页
- 内部用户使用 NAT 访问 Web 服务器，第 5-19 页
- 外部用户访问内部网络上的 Web 服务器，第 5-20 页
- 外部用户尝试访问内部主机，第 5-21 页

内部用户访问 Web 服务器

图 5-9 显示内部用户访问外部 Web 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，并在需要时将源 MAC 地址添加到 MAC 地址表中。由于它是新会话，因此会根据安全策略条款 （访问列表、过滤器、 AAA）验证数据包是否获得允许。

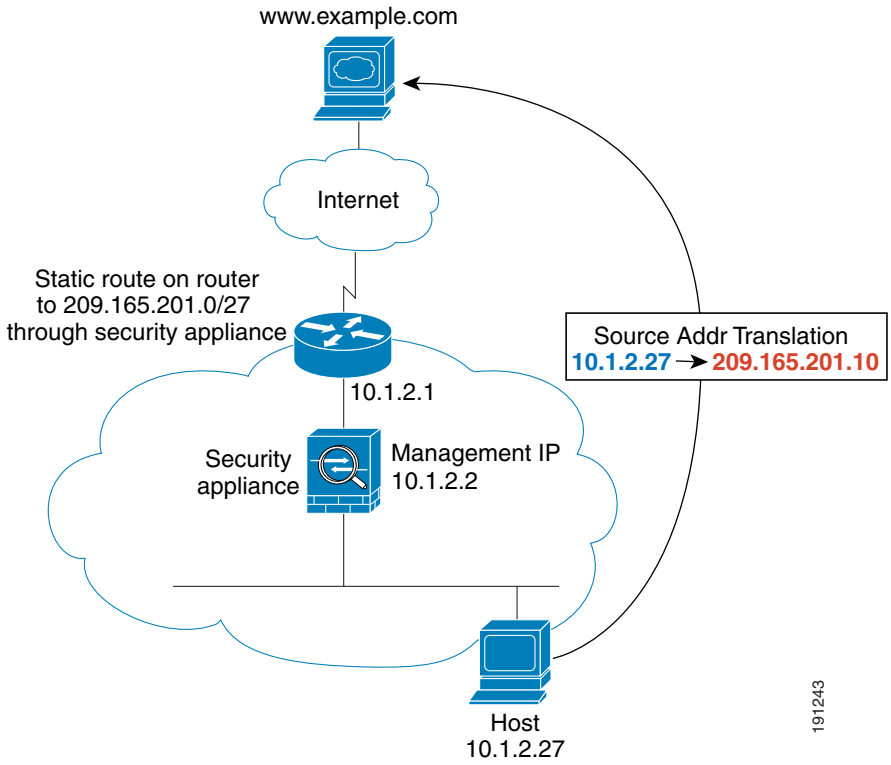
   对于多情景模式， ASA 会首先将数据包分类到一个情景中。
3. ASA 记录有关会话已建立的信息。
4. 如果目标 MAC 地址在其表中，则 ASA 会将数据包从外部接口转发出去。目标 MAC 地址是上游路由器的地址 (209.165.201.2)。

   如果目标 MAC 地址不在 ASA 表中，则 ASA 会通过发送 ARP 请求或 ping 来尝试发现 MAC 地址。系统会丢弃第一个数据包。
5. Web 服务器响应请求；由于已建立会话，因此数据包会绕过许多与新连接关联的查找。
6. ASA 将数据包转发给内部用户。

内部用户使用 NAT 访问 Web 服务器

图 5-10 显示内部用户访问外部 Web 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，并在需要时将源 MAC 地址添加到 MAC 地址表中。由于它是新会话，因此会根据安全策略条款 （访问列表、过滤器、 AAA）验证数据包是否获得允许。

   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。

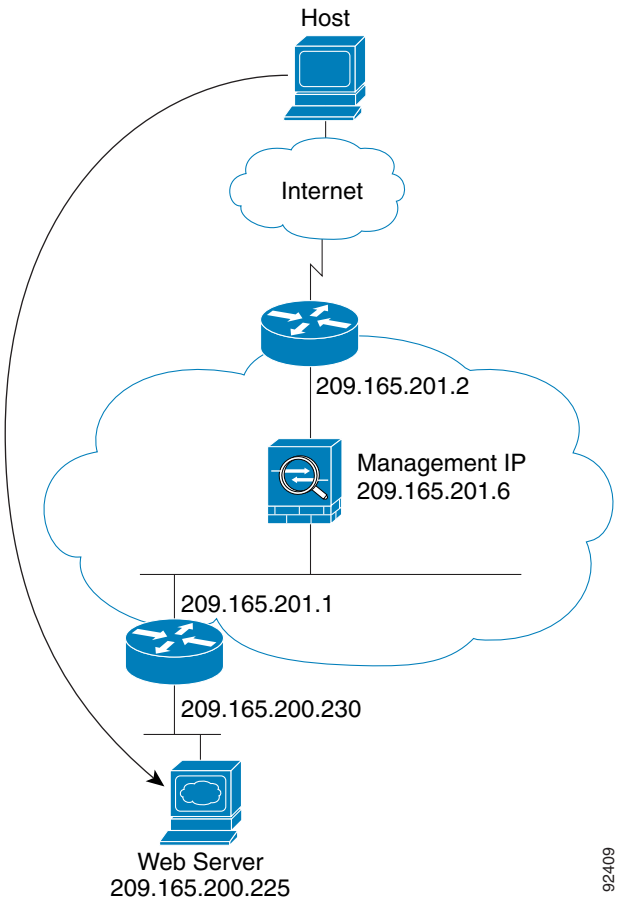
   由于映射地址与外部接口不在同一网络上，因此请确保上游路由器具有至映射网络 （指向 ASA）的静态路由。
4. 然后， ASA 会记录有关会话已建立的信息，并从外部接口转发数据包。
5. 如果目标 MAC 地址在其表中，则 ASA 会将数据包从外部接口转发出去。目标 MAC 地址是上游路由器的地址 (10.1.2.1)。

   如果目标 MAC 地址不在 ASA 表中，则 ASA 会通过发送 ARP 请求和 ping 来尝试发现 MAC 地址。系统会丢弃第一个数据包。
6. Web 服务器响应请求；由于已建立会话，因此数据包会绕过许多与新连接关联的查找。
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 Web 服务器

图 5-11 显示访问内部 Web 服务器的外部用户。

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 Web 服务器请求访问网页。
2. ASA 接收数据包，并在需要时将源 MAC 地址添加到 MAC 地址表中。由于它是新会话，因此会根据安全策略条款 （访问列表、过滤器、 AAA）验证数据包是否获得允许。

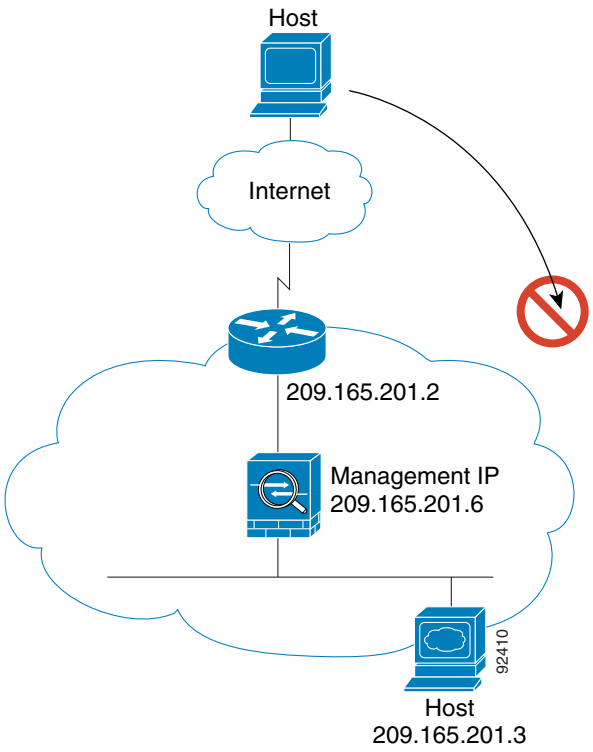
   对于多情景模式， ASA 会首先将数据包分类到一个情景中。
3. ASA 记录有关会话已建立的信息。
4. 如果目标 MAC 地址在其表中，则 ASA 会将数据包从内部接口转发出去。目标 MAC 地址是下游路由器的地址 (209.165.201.1)。

   如果目标 MAC 地址不在 ASA 表中，则 ASA 会通过发送 ARP 请求和 ping 来尝试发现 MAC 地址。系统会丢弃第一个数据包。
5. Web 服务器响应请求；由于已建立会话，因此数据包会绕过许多与新连接关联的查找。
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，并在需要时将源 MAC 地址添加到 MAC 地址表中。由于它是新会话，因此会根据安全策略条款 （访问列表、过滤器、 AAA）验证数据包是否获得允许。

   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，因此会拒绝数据包，并且 ASA 会丢弃数据包。
4. 如果外部用户尝试攻击内部网络，则 ASA 会采用多种技术来确定数据包对于已建立的会话是否有效。

防火墙模式历史记录

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 2 层防火墙，充当 “嵌入式防火墙”或 “隐藏防火墙”，并且不会被视为所连接设备的路由器跃点。 引入了以下命令：**firewall transparent** 和 **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。 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。 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。网桥组流量相互分隔。在单情景模式和多情景模式的每个情景中，最多可配置 8 个网桥组，每组最多 4 个接口。 **备注**　尽管您可以在 ASA 5505 上配置多个网桥组，但在 ASA 5505 上的透明模式下数据接口数限制为两个意味着只能有效地使用 1 个网桥组。 引入了以下命令：**interface bvi**、 **bridge-group** 和 **show bridge-group**。
针对未连接的子网添加 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，否则不建议启用此功能。这项功能让针对 ASA 发动拒绝服务 (DoS) 攻击变得更容易；任何接口上的用户都可发送许多 ARP 应答，并且用虚假条目造成 ASA ARP 表过载。 如果您使用以下对象，则可能要使用此功能： • 辅助子网。 • 用于流量转发的相邻路由上的代理 ARP。 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
在多情景模式下支持混合防火墙模式	8.5(1)/9.0(1)	可以在多情景模式下为每个情景独立设置防火墙模式，因此某些情景可在透明模式下运行，而另一些情景则可在路由模式中运行。 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 个增加到 250 个网桥组。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。 修改了以下命令：**interface bvi** 和 **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。

- 关于安全情景，第 6-1 页
- 多情景模式许可，第 6-12 页
- 多情景模式准则，第 6-13 页
- 多情景模式默认设置，第 6-14 页
- 配置多情景，第 6-14 页
- 在情景与系统执行空间之间切换，第 6-21 页
- 管理安全情景，第 6-22 页
- 监控安全情景，第 6-25 页
- 多情景模式示例，第 6-35 页
- 多情景模式的历史记录，第 6-37 页

关于安全情景

可以将一个 ASA 分区成多台虚拟设备，这些虚拟设备称为安全情景。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。有关在多情景模式下不支持的功能，请参阅多情景模式准则，第 6-13 页。

本节提供安全情景的概述。

- 安全情景的常见用途，第 6-2 页
- 情景配置文件，第 6-2 页
- ASA 如何对数据包进行分类，第 6-3 页
- 级联安全情景，第 6-6 页
- 对安全情景的管理访问，第 6-7 页
- 关于资源管理，第 6-8 页
- 关于 MAC 地址，第 6-11 页

安全情景的常见用途

您可能希望在以下情况下使用多安全情景：

- 您作为运营商，希望向众多客户销售安全服务。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。
- 您所在的组织是一家大型企业或大学校园，并且希望保持各部门完全分隔。
- 您所在的组织是一家企业，需要为不同部门提供不同的安全策略。
- 您具有需要多个 ASA 的网络。

情景配置文件

本节介绍 ASA 如何实施多情景模式配置。

- 情景配置，第 6-2 页
- 系统配置，第 6-2 页
- 管理情景配置，第 6-2 页

情景配置

对于每个情景， ASA 包含一个配置，该配置确定安全策略、接口以及可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

系统管理员通过在系统配置 （与单模式配置类似的启动配置）中配置每个情景配置位置、分配的接口以及其他情景运行参数，从而添加并管理情景。系统配置可标识 ASA 的基本设置。系统配置本身并不包含任何网络接口或网络设置；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*的某个情景。系统配置中包含一个仅用于故障切换流量的专用故障切换接口。

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，当用户登录到管理情景时，该用户将具有系统管理员权限并可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，由于登录到管理情景会授予用户针对所有情景的管理员权限，因此可能需要将对管理情景的访问限定于适当的用户。管理情景必须驻留在闪存中，而不是远程位置。

如果您的系统已处于多情景模式下，或者您从单模式进行转换，则管理情景会自动在内部闪存中创建名为 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 如何对数据包进行分类

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

- 有效分类器条件，第 6-3 页
- 分类示例，第 6-4 页

备注　如果目标 MAC 地址为组播或广播 MAC 地址，则数据包会复制并传递到每个情景。

有效分类器条件

本节介绍分类器使用的条件。

- 唯一接口，第 6-3 页
- 唯一 MAC 地址，第 6-3 页
- NAT 配置，第 6-3 页

备注　对于以接口为目标的管理流量，使用接口 IP 地址进行分类。

不使用路由表对数据包进行分类。

唯一接口

如果仅有一个情景与传入接口相关联，则 ASA 会将数据包分类至该情景。在透明防火墙模式下，要求情景具有唯一接口，因此总是使用此方法对数据包进行分类。

唯一 MAC 地址

如果多情景共享一个接口，则分类器在每个情景中使用分配给该接口的唯一 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，会启用 MAC 地址自动生成。在配置每个接口时，您也可以手动设置 MAC 地址。

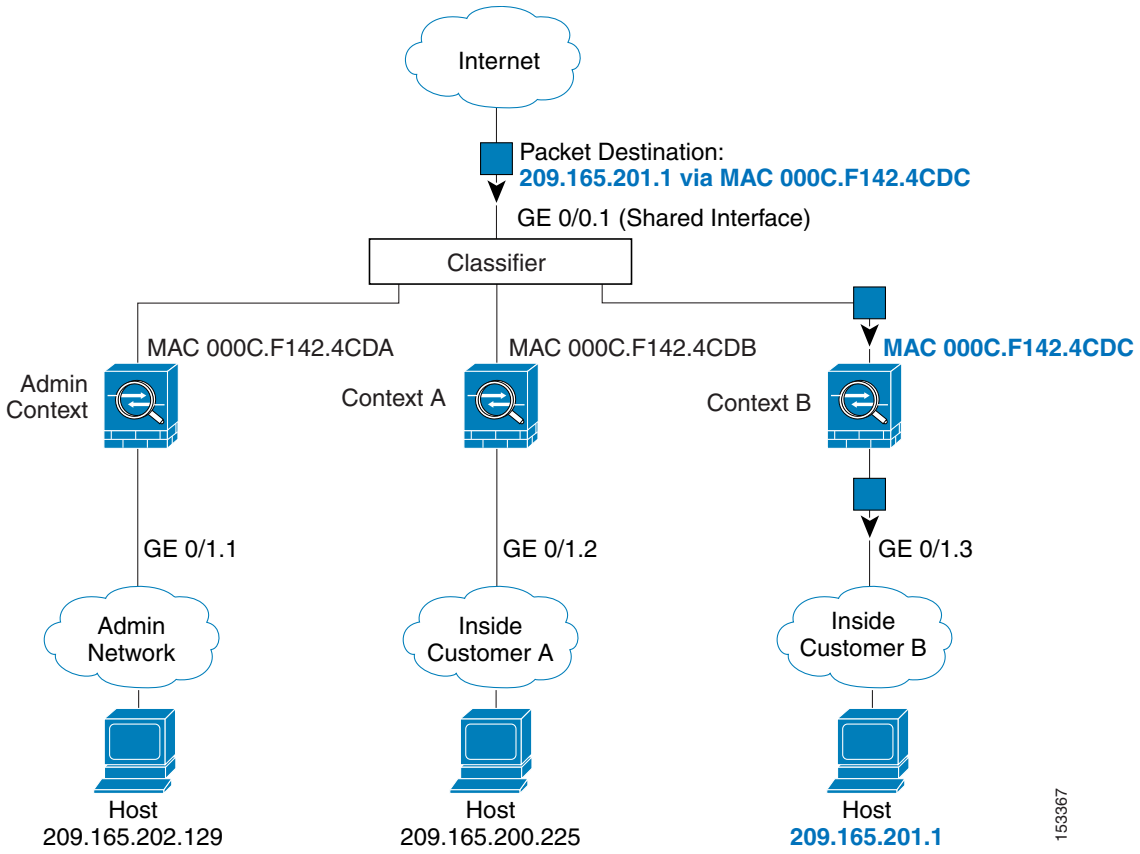
NAT 配置

如果禁用唯一 MAC 地址，则 ASA 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 配置的完整性如何，都可以进行流量分类。

分类示例

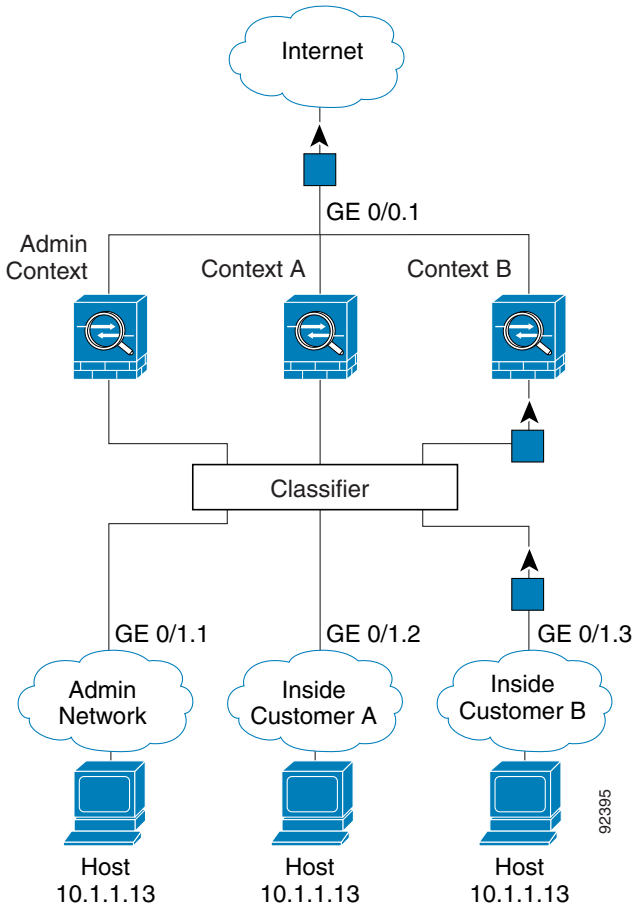
图 6-1 展示了多情景共享一个外部接口。因为情景 B 包含路由器将数据包发送到的 MAC 地址，因此分类器会将该数据包分配至情景 B。

图 6-1　使用 MAC 地址通过共享接口进行数据包分类



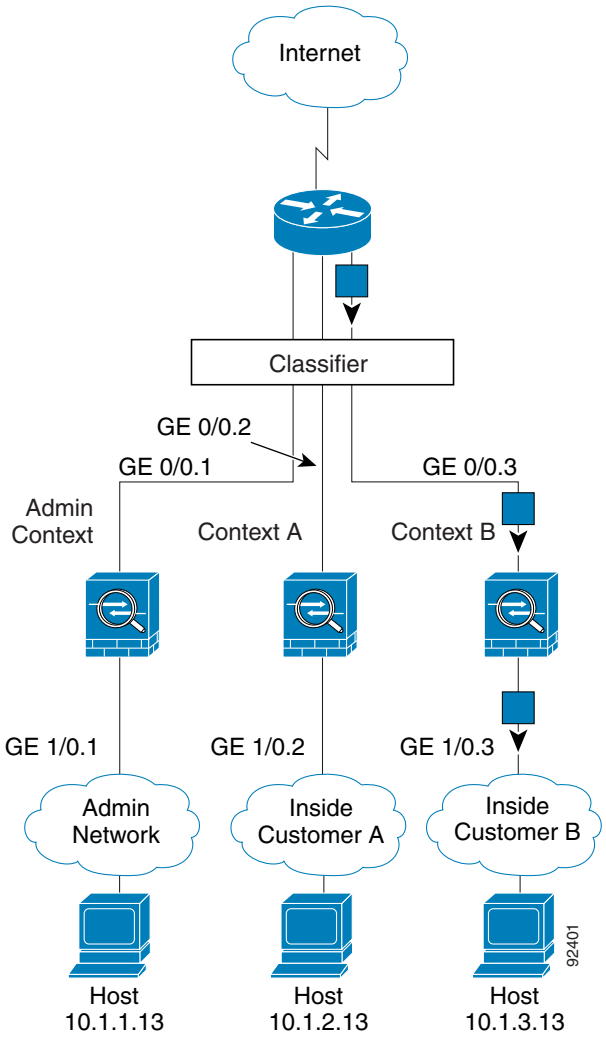
请注意，必须对所有新的传入流量加以分类，即使其来自内部网络。图 6-2 展示了情景 B 内部网络上的主机访问互联网。由于传入接口是分配至情景 B 的千兆以太网 0/1.3，因此分类器会将数据包分配至情景 B。

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 展示了来自互联网并以情景 B 内部网络上的主机为目标的数据包。由于传入接口是分配至情景 B 的千兆以太网 1/0.3，因此分类器会将数据包分配至情景 B。

图 6-3　透明防火墙情景



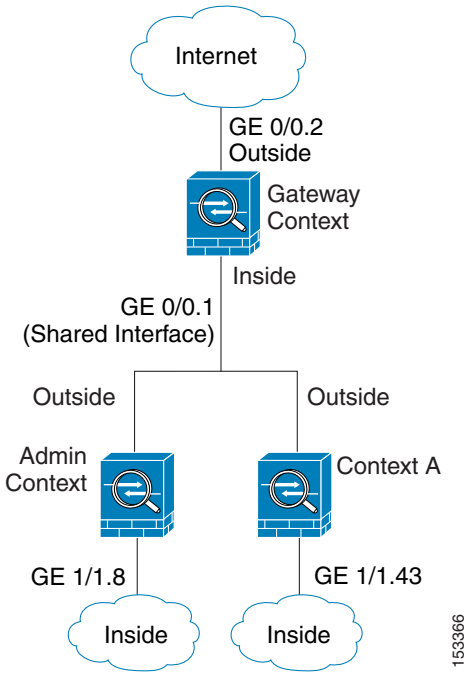
级联安全情景

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。如果您希望通过在顶级情景中配置共享参数，从而简化某些情景的配置，则可能要使用级联情景。

备注　级联情景要求每个情景接口具有唯一 MAC 地址（默认设置）。由于在不具有 MAC 地址的共享接口上对数据包进行分类存在限制，我们不建议在不具有唯一 MAC 地址的情况下使用级联情景。

图 6-4 展示了在网关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 提供多情景模式下的系统管理员访问，以及单个情景的管理员访问。以下章节描述了以系统管理员身份或以情景管理员身份进行登录：

- 系统管理员访问，第 6-7 页
- 情景管理员访问，第 6-8 页

系统管理员访问

您可以通过两种方式以系统管理员身份访问 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 （对于运行时命令而言）。

- 使用 Telnet、 SSH 或 ASDM 访问管理情景。

  要启用 Telnet、 SSH 和 ASDM 访问，请参阅第 32 章 “管理访问”。

作为系统管理员，您可以访问所有情景。

当您从管理情景切换到系统情景时，您的用户名会更改为默认用户名 “enable_15”。如果在该情景中配置了命令授权，则需要为 “enable_15” 用户配置授权权限，也可以使用已为其提供足够权限的其他名称登录。要使用新用户名登录，请输入 **login** 命令。例如，使用用户名 “admin” 登录管理情景。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具有最高权限的 “admin” 用户。当从管理情景切换到情景 A 时，用户名会更改为 enable_15，因此您必须输入 **login** 命令，以 “admin” 身份再次登录。当切换到情景 B 时，必须再次输入 **login** 命令来以 “admin” 身份登录。

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 来访问情景。如果您登录到一个非管理情景，则只能访问该情景的配置。您可以提供该情景的单独登录。要启用 Telnet、SSH 和 ASDM 访问以及配置管理身份验证，请参阅第 32 章 “管理访问”。

关于资源管理

默认情况下，除非实施了每个情景的最大访问限制，否则所有安全情景均可无限制地访问 ASA 的资源；唯一的例外是 VPN 资源，默认情况下会禁止访问此类资源。例如，如果您发现一个或者多个情景使用了过多资源，并且导致其他情景出现拒绝连接的情况，则您可以配置资源管理来限制每个情景对资源的使用。对于 VPN 资源，您必须将资源管理配置为允许任何 VPN 隧道。

- 资源类，第 6-8 页
- 资源限制，第 6-8 页
- 默认类，第 6-9 页
- 使用超订用资源，第 6-9 页
- 使用不受限制资源，第 6-10 页

资源类

ASA 通过向资源类分配情景来管理资源。每个情景使用由类设置的资源限制。要使用某个类的设置，请在定义情景时向该类分配情景。所有未分配给其他类的情景都属于默认类；您不必主动向默认类分配情景。只能将情景分配给一个资源类。此规则的例外是，在成员类中未定义的限制继承自默认类；因此，一个情景实际可能是默认类和另一个类的成员。

资源限制

您可以将单一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，而是会由 ASA 为情景设置最大限制。如果您超订用资源或允许某些资源不受限制，则少数情景可能会 “用尽” 这些资源，从而潜在影响为其他情景提供服务。VPN 资源类型除外，您不能超订用此类资源，因此，分配给每个情景的资源量可以得到保证。为应对 VPN 会话数临时激增超过所分配数量的情况， 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*超订用，并按照先到先得原则供情景使用。

默认类

所有未分配给其他类的情景都属于默认类；您不必主动向默认类分配情景。

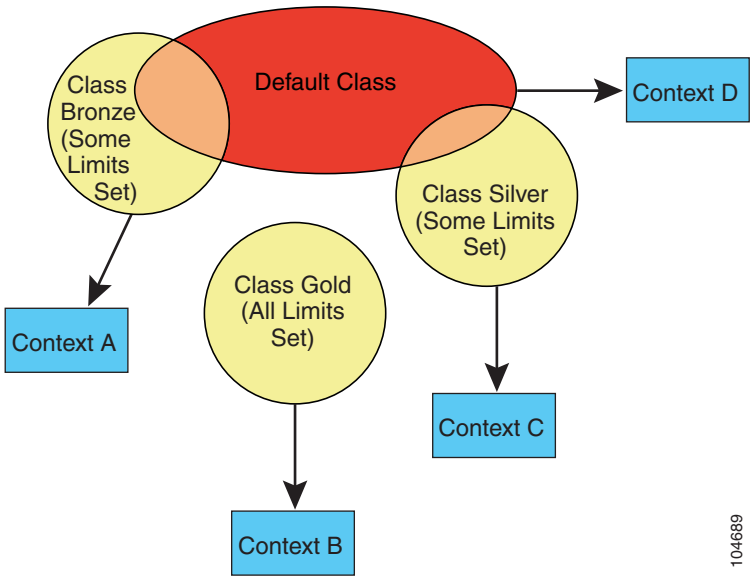
如果某个情景属于除默认类以外的类，则其类设置始终覆盖默认类设置。但是，如果另一个类具有任何未定义的设置，则成员情景为这些限制使用默认类。例如，如果创建的类对所有并发连接具有 2% 的限制，但没有任何其他限制，则所有其他限制都继承自默认类。相反地，如果创建对所有资源都有限制的类，则该类不使用默认类中的任何设置。

对于大多数资源，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 - 65535 个条目。（每个情景的最大值。）
- VPN 站点间隧道 - 0 个会话。（您必须将该类手动配置为允许任何 VPN 会话。）

图 6-5 展示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；其他限制继承自默认类。情景 B 不会从默认类继承任何限制，因为所有限制都在其类（Gold 类）中进行设置。情景 D 未分配给某个类，因此会默认成为默认类的成员。

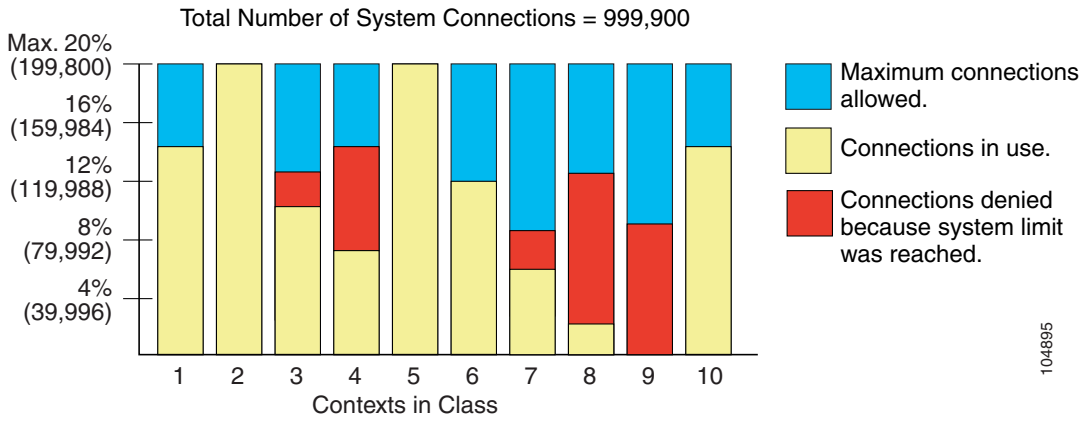
图 6-5　　资源类



使用超订用资源

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）来超订用 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 个情景分配给该类（总计 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希望设置的 20%。（请参阅图 6-6。）

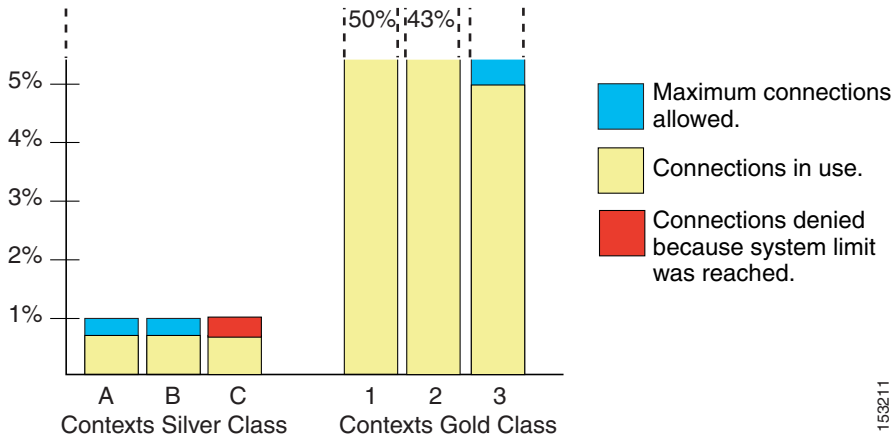
图 6-6　资源超订用



使用不受限制资源

通过 ASA 可分配对某个类中的一个或多个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%）；但是，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 无法达到其 3% 的合并限制。（请参阅图 6-7。）设置不受限制的访问与超订用 ASA 类似，不同之处在于，您对于超订用系统的程度所拥有的控制能力相对较弱。

图 6-7　不受限制资源



关于 MAC 地址

为了允许情景共享接口， ASA 会在默认情况下向每个共享情景接口分配虚拟 MAC 地址。要自定义或禁用自动生成，请参阅自动将 MAC 地址分配给情景接口，第 6-21 页。

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该接口的唯一 MAC 地址，则可尝试可能不会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 ASA 如何对数据包进行分类，第 6-3 页。

在出现生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突这种极少发生的情况下，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，请参阅配置 MTU 和 TCP MSS，第 14-5 页。

- 默认 MAC 地址，第 6-11 页
- 与手动 MAC 地址的交互，第 6-11 页
- 故障切换 MAC 地址，第 6-11 页
- MAC 地址格式，第 6-12 页

默认 MAC 地址

默认情况下会启用自动 MAC 地址生成。ASA 根据接口 (ASA 5500-X) 或背板 (ASASM) 中 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，并且该物理接口的所有子接口都使用同一固化 MAC 地址。
- 对于 ASASM - 所有 VLAN 接口都使用派生自背板 MAC 地址的同一 MAC 地址。

另请参阅 MAC 地址格式，第 6-12 页。

备注　（8.5(1.6) 及更早版本）为了保持故障切换对的无中断升级功能，在重新加载时， ASA 不会转换现有传统自动生成配置 （如果已启用故障切换）。但是，我们强烈建议您在使用故障切换时，手动将生成方法更改为前缀方法，对于 ASASM 尤其如此。如果不使用前缀方法，则安装在不同插槽编号中的 ASASM 在故障切换时会发生 MAC 地址更改，并且会出现流量中断。升级后，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。有关传统方法的详细信息，请参阅 《命令参考》中的 **mac-address auto** 命令。

与手动 MAC 地址的交互

如果您手动分配 MAC 地址，并且同时启用自动生成，则会使用手动分配的 MAC 地址。如果您随后删除了手动 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）以 A2 开头，因此如果您同时希望使用自动生成，则不能使用以 A2 开头的手动 MAC 地址。

故障切换 MAC 地址

为了使用故障切换， 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切换，并且备用设备成为主用设备，则新的主用设备会开始使用主用 MAC 地址，以最大限度地减少网络中断。有关详细信息，请参阅 MAC 地址格式，第 6-12 页一节。

MAC 地址格式

ASA 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) 中 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，地址完全相同，但内部计数器会加 1。

如何使用前缀的示例如下：如果将前缀设置为 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 的本地形式匹配：

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

对于前缀 1009 (03F1)， MAC 地址为：

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

备注　没有前缀的 MAC 地址格式为传统版本，在较新的 ASA 版本中不再支持。有关传统格式的详细信息，请参阅 《命令参考》中的 **mac-address auto** 命令。

多情景模式许可

型号	许可证要求
ASA 5506-X	不支持。
ASA 5508-X	增强型安全许可证：2 个情景。 *可选许可证：5 个情景。*
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 5516-X	增强型安全许可证：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。*
ASA 5585-X，带 SSP-10	基础许可证：2 个情景。 *可选许可证：5、 10、 20、 50 或 100 个情景。*

型号	许可证要求
ASA 5585-X，带 SSP-20、 SSP-40 和 SSP-60	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

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

多情景模式准则

故障切换准则

仅在多情景模式下支持主用/主用模式故障切换。

IPv6 规定

支持 IPv6。

备注　不支持跨情景 IPv6 路由。

不支持的功能

多情景模式不支持以下功能：

- RIP
- OSPFv3。 （支持 OSPFv2。）
- 组播路由
- 威胁检测
- 统一通信
- QoS
- 远程接入 VPN。 （支持站点间 VPN）。

其他准则

- 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。

- 如果将情景配置存储在闪存的根目录中，则在某些型号上可能会用尽该目录中的空间，即使有可用内存也是如此。在这种情况下，请为配置文件创建子目录。背景：某些型号（如 ASA 5585-X）使用 FAT 16 文件系统的内部闪存，并且，如果您未使用兼容 8.3 格式的短名称，或使用大写字符，则只能存储少于 512 个的文件和文件夹，因为文件系统会用尽所有插槽来存储长文件名（请参阅 http://support.microsoft.com/kb/120138/en-us）。

多情景模式默认设置

- 默认情况下， ASA 处于单情景模式下。
- 请参阅默认类，第 6-9 页。
- 请参阅默认 MAC 地址，第 6-11 页。

配置多情景

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。请参阅启用或禁用多情景模式，第 6-14 页。

步骤 2　（可选）配置用于资源管理的类。请参阅配置用于资源管理的类，第 6-15 页。**注意**：要支持 VPN，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”。
- ASASM - ASASM 快速入门指南。

步骤 4　配置安全情景。请参阅配置安全情景，第 6-18 页。

步骤 5　（可选）自定义 MAC 地址分配。请参阅自动将 MAC 地址分配给情景接口，第 6-21 页。

步骤 6　完成情景中的接口配置。请参阅第 13 章 “路由模式和透明模式接口”。

启用或禁用多情景模式

根据您从思科订购多情景模式的方式，ASA 可能已面向多个安全情景进行过配置。如果您需要从单模式转换为多模式，请遵循本节中的程序。

- 启用多情景模式，第 6-14 页
- 恢复单情景模式，第 6-15 页

启用多情景模式

当您从单模式转换为多模式时， ASA 会将运行配置转换为两个文件：一个是包含系统配置的新启动配置，另一个是包含管理情景的 admin.cfg（位于内部闪存的根目录中）。原始运行配置另存为 old_running.cfg （位于内部闪存的根目录中）。系统不会保存原始启动配置。ASA 自动向系统配置中添加一个管理情景的条目，名称为 “admin”。

必备条件

备份启动配置。当您从单模式转换为多模式时，ASA 会将运行配置转换为两个文件。系统不会保存原始启动配置。请参阅 备份和恢复配置或其他文件，第 33-22 页。

操作步骤

步骤 1　切换到多情景模式：

mode multiple

示例：

```
ciscoasa(config)# mode multiple
```

系统会提示您重新启动 ASA。

恢复单情景模式

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，请执行以下步骤：

准备工作

在系统执行空间中执行此程序。

操作步骤

步骤 1　将原始运行配置的备份版本复制到当前启动配置：

copy disk0:old_running.cfg startup-config

示例：

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

步骤 2　将模式设置为单模式：

mode single

示例：

```
ciscoasa(config)# mode single
```

系统会提示您重新启动 ASA。

配置用于资源管理的类

要在系统配置中配置某个类，请执行以下步骤：您可以通过重新输入带有新值的命令来更改特定资源限制的值。

准备工作

- 在系统执行空间中执行此程序。
- 表 6-1 列出资源类型和限制。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限制	系统限制[1]	说明
asdm	并发	1 （最小值） 5 （最大值）	32	ASDM 管理会话。 **备注** 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 （仅当进行更改时才存在）。例如，系统限制为 32 个 ASDM 会话表示 HTTPS 会话数限制为 64。
conns[2]	并发或速率	N/A	并发连接数：有关适用于您的型号的连接限制，请参阅每个型号支持的功能许可证，第 3-1 页。 速率：N/A	任意两台主机之间的 TCP 或 UDP 连接数，包括一台主机和多台其他主机之间的连接。
hosts	并发	N/A	N/A	可以通过 ASA 连接的主机数。
inspects	速率	N/A	N/A	每秒应用检测数。
mac-addresses	并发	N/A	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	N/A	N/A	动态路由数。
vpn burst other	并发	N/A	您的型号的其他 VPN 会话数量减去分配给**vpn other** 的所有情景的会话数的总和。	允许的站点间 VPN 会话数超过分配给具有 **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，而您为具有**vpn other** 的所有情景分配了 4000 个会话，则其余 1000 个会话可用于**vpn burst other**。与**vpn other** （保证会话可分配给相应的情景）不同的是， **vpn burst other** 可以超订用；突发池按照先到先得的原则供所有情景使用。
vpn other	并发	N/A	有关适用于您的型号的其他 VPN 会话数的信息，请参阅每个型号支持的功能许可证，第 3-1 页。	站点间 VPN 会话数。不能超订用此资源；所有情景分配的总和不得超过型号限制。为此资源分配的会话数保证可供相应情景使用。
ssh	并发	1 （最小值） 5 （最大值）	100	SSH 会话数。
syslogs	速率	N/A	N/A	每秒系统日志消息数。
telnet	并发	1 （最小值） 5 （最大值）	100	Telnet 会话数。
xlates[2]	并发	N/A	N/A	网络地址转换数。

1. 如果此列的值为 N/A，则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. 对于值小于 xlates 或 conns 的任一限制，会生成相应的系统日志消息。例如，如果将 xlates 限制设置为 7 并将 conns 限制设置为 9，则 ASA 仅会生成系统日志消息 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'”）。

操作步骤

步骤 1　指定类名并进入类配置模式：

class *name*

示例：

```
ciscoasa(config)# class gold
```

name 是最大长度为 20 个字符的字符串。要设置默认类的限制，请输入 **default** 作为名称。

步骤 2　设置资源类型的资源限制：

limit-resource [**rate**] *resource_name number*[**%**]

示例：

```
ciscoasa(config-class)# limit-resource rate inspects 10
```

- 要获得资源类型列表，请参阅表 6-1。如果指定 **all**，则会将所有资源都配置为相同的值。如果还指定了特定资源的值，则该限制会覆盖为 **all** 设置的限制。
- 输入 **rate** 参数以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**，从而将资源设置为不受限制或使用系统限制 （如果适用）。对于 VPN 资源， **0** 表示将限制设置为无。
- 对于没有系统限制的资源，不能设置百分比 (**%**)；只能设置绝对值。

示例

例如，要将默认类的连接数限制设置为 10% 而非不受限制，并允许使用 5 个站点间 VPN 隧道（其中两个隧道预留用于 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。

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。

准备工作

- 在系统执行空间中执行此程序。
- 对于 ASASM，请根据 ASASM 快速入门指南将 VLAN 分配给交换机上的 ASASM。
- 对于 ASA 5500-X，请根据第 9 章 “基本接口配置”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，如果清除了配置），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
  ```

  虽然此情景在配置中尚不存在，但是可以随后输入 **context** *name* 命令来继续进行管理情景配置。

操作步骤

步骤 1　添加或修改情景：

context *name*

示例：

```
ciscoasa(config)# context administrator
```

name 是最大长度为 32 个字符的字符串。此名称区分大小写，因此您可以具有名为 “customerA” 和 “CustomerA” 的两个情景。您可以使用字母、数字或连字符，但名称不能以连字符开头或结尾。

备注　“System” 或 “Null”（采用大写或小写字母）是保留名称，因此不能使用。

步骤 2　（可选）添加此情景的说明：

description *text*

示例：

```
ciscoasa(config-ctx)# description Administrator Context
```

步骤 3　指定可在情景中使用的接口：

要分配接口，请执行以下操作：

allocate-interface *interface_id* [*mapped_name*] [**visible** | **invisible**]

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
```

备注　请勿在接口类型和端口号之间包含空格。

- 多次输入这些命令可指定不同的范围。如果使用此命令的 **no** 形式删除分配，则会从运行配置中删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；但是，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。
- 如果需要，可以在路由模式下将相同接口分配给多情景。透明模式不允许使用共享接口。
- *mapped_name* 是接口的字母数字别名，可在情景中用于替代接口 ID。如果不指定映射名称，则会在情景中使用接口 ID。出于安全目的，您可能不希望情景管理员知道情景使用的是哪些接口。映射名称必须以字母开头，以字母或数字结尾，并且内部字符只能是字母、数字或下划线。例如，可以使用以下名称：**int0**、**inta**、**int_0**
- 如果指定子接口的范围，则可以指定匹配的映射名称的范围。关于范围，请遵循以下准则：
  - 映射名称必须由后跟数字部分的字母部分组成。映射名称的字母部分必须与范围的两端均匹配。例如，输入以下范围：**int0-int10**。例如，如果输入 `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与子接口范围包含相同的数字数量。例如，两个范围均包括 100 个接口：**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100**。例如，如果输入 `gig0/0.`**100**`-gig0/0.`**199** `int`**1**`-int`**15**，则命令将会失败。
- 如果设置了映射的名称，则指定 **visible** 可在 **show interface** 命令中查看实际接口 ID。默认关键字 **invisible** 仅显示映射名称。

步骤 4　确定系统从中下载情景配置的 URL：

config-url *url*

示例：

```
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
```

步骤 5　（可选）将情景分配给资源类：

如果不指定类，则情景属于默认类。只能将情景分配给一个资源类。

member *class_name*

示例：

```
ciscoasa(config-ctx)# member gold
```

步骤 6　（可选）如果您已安装 IPS 模块，请将 IPS 虚拟传感器分配给此情景。

allocate-ips *sensor_name* [*mapped_name*] [**default**]

示例：

```
ciscoasa(config-ctx)# allocate-ips sensor1 highsec
```

有关虚拟传感器的详细信息，请参阅 《防火墙配置指南》。

- 当添加情景 URL 时，系统会立即加载该情景，以便在配置可用的情况下情景正常运行。
- 输入 **allocate-interface** 命令，然后再输入 **config-url** 命令。如果先输入 **config-url** 命令，则 ASA 会立即加载情景配置。如果情景包含引用 （尚未配置的）接口的任何命令，则这些命令将会失败。

- 文件名无需文件扩展名，不过，我们建议使用 “.cfg”作为文件扩展名。服务器必须能够从管理情景进行访问。如果配置文件不可用，则会显示以下警告消息：

```
WARNING: Could not fetch the URL url
INFO: Creating context with default config
```

- 对于非 HTTP(S) URL 位置，在指定 URL 之后，即可切换到该情景，在 CLI 中对其进行配置，然后输入 **write memory** 命令将文件写入到该 URL 位置。（HTTP(S) 是只读的）。
- 管理情景文件必须存储在内部闪存上。
- 可用的 URL 类型包括：**disk***number*（适用于闪存）、 **ftp**、 **http**、 **https** 或 **tftp**。
- 要更改 URL，请重新输入带有新 URL 的 **config-url** 命令。有关更改 URL 的详细信息，请参阅更改安全情景 URL，第 6-23 页。

步骤 7　（可选）将情景分配给主用/主用故障切换中的一个故障切换组。

join-failover-group {**1** | **2**)

示例：

```
ciscoasa(config-ctx)# join-failover-group 2
```

默认情况下，情景处于组 1 中。管理情景必须始终处于组 1 中。

有关故障切换组的详细信息，请参阅配置可选故障切换参数，第 7-32 页。

步骤 8　（可选）为此情景启用云网络安全：

scansafe [**license** *key*]

示例：

```
ciscoasa(config-ctx)# scansafe
```

如果不指定**许可证**，则情景将使用在系统配置中配置的许可证。ASA 将身份验证密钥发送到 云 Web 的安全 代理服务器，指出请求来自哪个组织。身份验证密钥是一个 16 字节的十六进制数。

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
```

自动将 MAC 地址分配给情景接口

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，请参阅关于 MAC 地址，第 6-11 页（尤其是从早期 ASA 版本升级时）。另请参阅查看分配的 MAC 地址，第 6-33 页。

准备工作

- 当在情景中为接口配置 **nameif** 命令时，会立即生成新的 MAC 地址。如果在配置情景接口后启用此功能，则在启用之后，会立即为所有接口生成 MAC 地址。如果禁用此功能，则每个接口的 MAC 地址会恢复为默认 MAC 地址。例如， GigabitEthernet0/1 的子接口恢复为使用 GigabitEthernet0/1 的 MAC 地址。
- 在出现生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突这种极少发生的情况下，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，请参阅配置 MTU 和 TCP MSS，第 14-5 页。

操作步骤

步骤 1　自动向每个情景接口分配专用 MAC 地址：

mac-address auto [**prefix** *prefix*]

示例：

```
ciscoasa(config)# mac-address auto prefix 19
```

如果不输入前缀，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 *prefix* 是介于 0 和 65535 之间的十进制值。此前缀会转换为一个四位数的十六进制数字，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MAC 地址格式，第 6-12 页。

在情景与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。您在配置模式下编辑或在 **copy** 或 **write** 命令中使用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 （系统配置以及所有情景配置）。系统仅显示当前配置。

操作步骤

步骤 1　切换到情景：

```
changeto context name
```

提示符切换到 ciscoasa/*name*#

步骤 2　切换到系统执行空间：

```
changeto system
```

提示符切换到 ciscoasa#

管理安全情景

本节介绍如何管理安全情景。

- 删除安全情景，第 6-22 页
- 更改管理情景，第 6-23 页
- 更改安全情景 URL，第 6-23 页
- 重新加载安全情景，第 6-24 页

删除安全情景

除非您使用 **clear context** 命令删除所有情景，否则无法删除当前管理情景。

备注　如果使用故障切换，则从主用设备上删除情景到在备用设备上删除该情景之间存在一定延迟。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不一致；此错误是临时的，可以忽略。

准备工作

在系统执行空间中执行此程序。

操作步骤

步骤 1　删除单个情景：

```
no context name
```

此外，还会删除所有情景命令。系统不会从配置 URL 位置中删除情景配置文件。

步骤 2　删除所有情景 （包括管理情景）：

```
clear context
```

系统不会从配置 URL 位置中删除情景配置文件。

更改管理情景

系统配置本身并不包含任何网络接口或网络设置；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某个情景。

管理情景与任何其他情景一样，不同之处在于，当用户登录到管理情景时，该用户将具有系统管理员权限并可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，由于登录到管理情景会授予用户针对所有情景的管理员权限，因此可能需要将对管理情景的访问限定于适当的用户。

准备工作

- 可以将任何情景设置为管理情景，只要配置文件存储在内部闪存中即可。
- 在系统执行空间中执行此程序。

操作步骤

步骤 1　设置管理情景：

admin-context *context_name*

示例：

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

连接到管理情景的所有远程管理会话 （如 Telnet、 SSH 或 HTTP）都会终止。必须重新连接到新的管理情景。

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。

准备工作

- 在没有通过新的 URL 重新加载配置的情况下，不能更改安全情景 URL。ASA 会将新的配置与当前的运行配置合并。
- 重新输入同一 URL 也可将已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到运行配置中。
  - 如果配置相同，则不会发生任何更改。
  - 如果命令冲突或命令影响情景的运行，则合并的影响取决于命令。可能会发生错误，也可能出现意外结果。如果运行配置为空 （例如，如果服务器不可用且从未下载配置），则使用新的配置。
- 如果您不想合并配置，可清除运行配置 （该操作通过情景中断所有通信），然后从新的 URL 重新加载配置。
- 在系统执行空间中执行此程序。

操作步骤

步骤 1　（可选，前提是您不需要执行合并）切换到情景并清除配置：

```
changeto context name
clear configure all
```

示例：

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(config)# clear configure all
```

如果要执行合并，请跳至步骤 2。

步骤 2　切换到系统执行空间：

```
changeto system
```

示例：

```
ciscoasa/ctx1(config)# changeto system
ciscoasa(config)#
```

步骤 3　进入要更改的情景的情景配置模式。

```
context name
```

示例：

```
ciscoasa(config)# context ctx1
```

步骤 4　输入新的 URL。系统会立即加载情景，以便其正常运行。

```
config-url new_url
```

示例：

```
ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg
```

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。

- 从系统配置中删除情景。

  此操作会清除其他属性，例如，可能有助于故障排除的内存分配。但是，将情景添加回系统要求重新指定 URL 和接口。

- 通过清除配置重新加载，第 6-25 页
- 通过删除并重新添加情景重新加载，第 6-25 页

通过清除配置重新加载

要通过清除情景配置并从 URL 重新加载配置来重新加载情景，请执行以下步骤。

操作步骤

步骤 1　切换到要重新加载的情景：

changeto context *name*

示例：

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(comfig)#
```

步骤 2　清除运行配置：

clear configure all

此命令会清除所有连接。

步骤 3　重新加载配置：

copy startup-config running-config

示例：

```
ciscoasa/ctx1(config)# copy startup-config running-config
```

ASA 会通过系统配置中指定的 URL 复制配置。不能在情景中更改此 URL。

通过删除并重新添加情景重新加载

要通过删除情景然后重新添加来重新加载该情景，请执行以下章节中的步骤：

1. 删除安全情景，第 6-22 页。
2. 配置安全情景，第 6-18 页

监控安全情景

本节介绍如何查看和监控情景信息。

- 查看情景信息，第 6-26 页
- 查看资源分配，第 6-27 页
- 查看资源使用情况，第 6-30 页
- 监控情景中的 SYN 攻击，第 6-31 页
- 查看分配的 MAC 地址，第 6-33 页

查看情景信息

从系统执行空间中，您可以查看情景列表，包括名称、分配的接口和配置文件 URL。

从系统执行空间中，输入以下命令可查看所有情景：

操作步骤

步骤 1　显示所有情景：

show context [*name* | **detail**| **count**]

如果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，请参阅以下样本输出。

count 选项用于显示情景的总数。

以下是 **show context** 命令的样本输出。以下样本输出显示三个情景：

```
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 显示每个字段的说明。

表 6-2　show context 字段

字段	说明
Context Name	列出所有情景名称。名称中带有星号 (*) 的情景是管理情景。
Interfaces	分配给情景的接口。
URL	ASA 从中加载情景配置的 URL。

以下是 **show context detail** 命令的样本输出：

```
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
```

请参阅 《命令参考》以获取有关 **detail** 输出的详细信息。

以下是 **show context count** 命令的样本输出：

```
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。

要查看资源分配，请输入以下命令：

操作步骤

步骤 1　显示资源分配：

show resource allocation [**detail**]

此命令显示资源分配情况，但不显示实际正在使用的资源。有关实际资源使用情况的详细信息，请参阅查看资源使用情况，第 6-30 页。

detail 参数用于显示其他信息。有关详细信息，请参阅以下样本输出。

以下样本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 显示每个字段的说明。

表 6-3　show resource allocation 字段

字段	说明
Resource	可限制的资源的名称。
Total	跨所有情景分配的资源总量。此数量是每秒的并发实例或实例的绝对数量。如果在类定义中指定了百分比，则 ASA 会在显示该值时将百分比转换为绝对数量。
% 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，则此列将显示 N/A。

以下是 **show resource allocation detail** 命令的样本输出：

```
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 显示每个字段的说明。

表 6-4　　show resource allocation detail 字段

字段	说明
Resource	可限制的资源的名称。
Class	每个类 （包括默认类）的名称。 All contexts 字段显示所有类的全部值。
Mmbrs	分配给每个类的情景数量。
Origin	资源限制的源，如下所示： • A - 使用 **all** 选项设置此限制，而不是将其设置为单独资源。 • C - 此限制派生自成员类。 • D - 此限制未在成员类中定义，而是派生自默认类。对于分配给默认类的情景，值将会是 “C” 而不是 “D”。 ASA 可以将 “A” 和 “C” 或 “D” 结合使用。
Limit	每个情景的资源限制，显示为绝对数量。如果在类定义中指定了百分比，则 ASA 会在显示该值时将百分比转换为绝对数量。
Total	跨类中的所有情景分配的资源总量。此数量是每秒的并发实例或实例的绝对数量。如果资源不受限制，则显示为空白。
% 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，则显示为空白。如果资源没有系统限制，则此列将显示 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。

操作步骤

步骤 1　查看每个情景的资源使用情况：

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* 关键字可显示对指定资源的使用排名前 *n* 的用户的情景。对于此选项，必须指定单个资源类型，而不能指定 **resource all**。
- **summary** 选项用于显示所有情景的综合使用情况。
- **system** 选项用于显示所有情景的综合使用情况，但显示的是资源的系统限制，而不是综合情景限制。
- 对于 **resource** *resource_name*，请参阅表 6-1 以获取可用资源名称。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，包括无法管理的那些资源。例如，可以查看 TCP 拦截次数。
- **counter** *counter_name* 是以下关键字之一：
  - **current** - 显示活动并发实例数或资源的当前使用率。
  - **denied** - 显示由于超过 Limit 列中所示的资源限制而被拒绝的实例的数量。
  - **peak** - 显示自上一次清除统计信息（使用 **clear resource usage** 命令或由于设备重启）以来，峰值并发实例数或资源的峰值使用率。
  - **all** -（默认）显示所有统计信息。
- *count_threshold* 设置一个数值，如果超过此数值，则会显示资源。默认值为 1。如果资源的使用率低于所设置的数字，则不会显示资源。如果为计数器名称指定 **all**，则 *count_threshold* 适用于当前使用情况。
- 要显示所有资源，请将 *count_threshold* 设置为 **0**。

以下是 **show resource usage context** 命令的样本输出，其中显示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
```

以下是 **show resource usage summary** 命令的样本输出，其中显示所有情景和所有资源的资源使用情况。以下样本显示 6 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** 命令的样本输出，其中显示 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，因此总共限制为 125 个连接。系统限制仅为 100 个链接，因此会显示系统限制。

```
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** 命令的样本输出，其中显示所有情景的资源使用情况，但是该命令显示的是系统限制，而不是综合情景限制。**counter all 0** 选项用于显示当前未使用的资源。Denied statistics 显示由于系统限制而拒绝资源的次数，如适用。

```
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 Cookie 算法防止 TCP SYN 泛洪攻击。SYN 泛洪攻击包含一系列通常源于欺骗性 IP 地址的 SYN 数据包。SYN 数据包的持续泛滥使服务器 SYN 队列始终保持充满状态，致使其无法处理连接请求。当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 收到来自客户端的 ACK 后，即可对客户端进行身份验证，并且允许连接到服务器。

请使用以下命令监控 SYN 攻击：

操作步骤

步骤 1　监控各个情景的攻击速率：

show perfmon

步骤 2　监控 TCP 拦截对于各个情景使用的资源量：

```
show resource usage detail
```

步骤 3　监控 TCP 拦截对于整个系统使用的资源量：

```
show resource usage summary detail
```

以下是 **show perfmon** 命令的样本输出，其中显示名为 admin 的情景的 TCP 拦截速率。

```
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
```

以下是 **show resource usage detail** 命令的样本输出，其中显示 TCP 拦截对各个情景使用的资源量。（**粗体**形式的样本文本显示 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
```

以下样本输出显示 TCP 拦截对整个系统使用的资源量。（**粗体**形式的样本文本显示 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。

- 查看系统配置中的 MAC 地址，第 6-34 页
- 查看情景中的 MAC 地址，第 6-35 页

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。

准备工作

如果您手动向接口分配 MAC 地址，但也启用了自动生成，则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 地址也如此。如果随后删除手动 MAC 地址，则会使用所显示的自动生成的地址。

操作步骤

步骤 1　从系统执行空间显示分配的 MAC 地址：

show running-config all context [*name*]

查看分配的 MAC 地址必须使用 **all** 选项。虽然 **mac-address auto** 命令仅在全局配置模式下可由用户配置，但是该命令在情景配置模式下会与分配的 MAC 地址一起显示为只读条目。只有在情景中使用 **nameif** 命令配置的已分配接口会具有分配的 MAC 地址。

示例

show running-config all context admin 命令的以下输出显示了分配给 Management0/0 接口的主用 MAC 地址和备用 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 （主用 MAC 地址和备用 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，因此没有为其生成 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。

操作步骤

步骤 1　显示情景中的每个接口正在使用的 MAC 地址：

show interface | include (Interface)|(MAC)

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
...
```

备注　**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，则只能查看系统配置中未使用的自动生成地址。

多情景模式示例

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% 而非不受限制，并将 VPN 其他会话连接数限制设置为 10 且 VPN 突发连接数限制为 5。
- 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，该情景将属于默认资源类。
- 从 FTP 服务器添加两个情景，作为 gold 资源类的一部分。

```
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
```

多情景模式的历史记录

表 6-5　　多情景模式的历史记录

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。 引入了以下命令：**context**、 **mode** 和 **class**。
自动 MAC 地址分配	7.2(1)	引入了将 MAC 地址自动分配给情景接口的功能。 引入了以下命令：**mac-address auto**。
资源管理	7.2(1)	引入了资源管理。 引入了以下命令：**class**、 **limit-resource** 和 **member**。
适用于 IPS 的虚拟传感器	8.0(2)	运行 IPS 软件版本 6.0 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 分配给一个或多个虚拟传感器，也可以将多个安全情景分配给同一虚拟传感器。 引入了以下命令：**allocate-ips**。
自动 MAC 地址分配增强功能	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)，并在故障切换对中为主设备和辅助设备 MAC 地址使用不同方案。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；如果您还希望手动分配 MAC 地址，则手动 MAC 地址不能以 A2 开头。 修改了以下命令：**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。
默认情况下会启用自动 MAC 地址分配。	8.5(1)	现在，默认情况下会启用自动 MAC 地址分配。 修改了以下命令：**mac-address auto**。

表 6-5　　多情景模式的历史记录 （续）

功能名称	平台版本	功能信息
自动生成 MAC 地址前缀	8.6(1)	在多情景模式下， ASA 现在会将自动 MAC 地址生成配置转换为使用默认前缀。ASA 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，系统自动执行此转换。前缀生成方法提供许多好处，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。如果要更改前缀，可以使用自定义前缀重新配置此功能。传统的 MAC 地址生成方法不再可用。 **备注**　为了保持故障切换对的无中断升级功能， ASA 在重新加载时 （如果已启用故障切换）*不会*转换现有配置中的 MAC 地址方法。但是，我们强烈建议您在使用故障切换时，手动将生成方法更改为前缀方法，对于 ASASM 尤其如此。如果不使用前缀方法，则安装在不同插槽编号中的 ASASM 在故障切换时会发生 MAC 地址更改，并且会出现流量中断。升级后，要使用 MAC 地址生成的前缀方法，请重新启用 MAC 地址生成来使用前缀。 修改了以下命令：**mac-address auto**。
安全情景中的动态路由	9.0(1)	现在，在多情景模式下支持 EIGRP 和 OSPFv2 动态路由协议。不支持 OSPFv3、 RIP 和组播路由。
用于路由表条目的新资源类型	9.0(1)	系统创建了新的资源类型 routes，用于设置每个情景中的最大路由表条目数。 修改了以下命令：**limit-resource**、 **show resource types**、 **show resource usage** 和 **show resource allocation**。
多情景模式下的站点间 VPN	9.0(1)	现在，在多情景模式下支持站点间 VPN 隧道。
用于站点间 VPN 隧道的新资源类型	9.0(1)	系统创建了新的资源类型 （即 vpn other 和 vpn burst other），用于设置每个情景中站点间 VPN 隧道的最大数量。 修改了以下命令：**limit-resource**、 **show resource types**、 **show resource usage** 和 **show resource allocation**。



通过故障切换实现高可用性

本章介绍如何配置主用/备用或主用/主用故障切换以实现思科 ASA 的高可用性。

- 关于故障切换，第 7-1 页
- 故障切换许可，第 7-22 页
- 故障切换准则，第 7-23 页
- 故障切换的默认设置，第 7-24 页
- 配置主用/备用故障切换，第 7-24 页
- 配置主用/主用故障切换，第 7-28 页
- 配置可选故障切换参数，第 7-32 页
- 管理故障切换，第 7-38 页
- 监控故障切换，第 7-43 页
- 故障切换历史记录，第 7-45 页

关于故障切换

配置故障切换需要通过专用故障切换链路和状态链路 （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切换条件。如果符合这些条件，将执行故障切换。

- 故障切换模式，第 7-2 页
- 故障切换系统要求，第 7-2 页
- 故障切换和状态故障切换链路，第 7-3 页
- 故障切换中的 MAC 地址和 IP 地址，第 7-8 页
- ASA 服务模块的机箱内和机箱间模块的布置，第 7-8 页
- 无状态故障切换和状态故障切换，第 7-12 页
- 故障切换的透明防火墙模式要求，第 7-14 页
- 故障切换运行状况监控，第 7-16 页
- 故障切换时间，第 7-17 页
- 配置同步，第 7-17 页
- 关于主用/备用故障切换，第 7-19 页
- 关于主用/主用故障切换，第 7-20 页

故障切换模式

ASA 支持两种故障切换模式：主用/主用故障切换和主用/备用故障切换。每种故障切换模式都有自己确定和执行故障切换的方法。

- 在主用/备用故障切换中，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。发生故障切换时，主用设备会故障切换到备用设备，后者随即变为主用状态。您可以将主用/备用故障切换用于单情景或多情景模式下的 ASA。
- 在主用/主用故障切换配置下，两台 ASA 都可以传送网络流量。主用/主用故障切换仅适用于多情景模式下的 ASA。在主用/主用故障切换中，您可将 ASA 上的安全情景划分为 2 个*故障切换组*。故障切换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。发生故障切换时，会在故障切换组级别进行。

两种故障切换模式都支持状态或无状态故障切换。

故障切换系统要求

本部分介绍，在故障切换配置下，对于 ASA 的硬件、软件和许可证要求。

- 硬件要求，第 7-2 页
- 软件要求，第 7-2 页
- 许可证要求，第 7-3 页

硬件要求

故障切换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。

如果您在故障切换配置中，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

故障切换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。但是，您可以在升级过程中临时使用不同的软件版本；例如，可以将一台设备从 8.3(1) 版本升级到 8.3(2) 版本，并使故障切换保持主用状态。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。
- 安装有相同的 AnyConnect 映像。如果在执行无中断升级时，故障切换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”。

相关主题

升级故障转移对或 ASA 集群，第 33-4 页

许可证要求

故障切换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切换集群许可证。

相关主题

故障切换或 ASA 集群许可证，第 3-20 页

故障切换和状态故障切换链路

故障切换链路和可选的状态故障切换链路是两台设备之间的专用连接。

- 故障切换链路，第 7-3 页
- 状态故障切换链路，第 7-4 页
- 避免中断故障切换和数据链路，第 7-5 页

注意 除非您使用 IPsec 隧道或故障切换密钥保护通信，否则所有信息会以明文形式通过故障切换和状态链路发送。如果使用 ASA 端接 VPN 隧道，则此信息包括用于建立隧道的任何用户名、密码和预共享密钥。以明文发送此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 隧道或故障切换密钥来保护故障切换通信。

故障切换链路

故障切换对中的两台设备会不断地通过故障切换链路进行通信，以便确定每台设备的运行状态。

- 故障切换链路数据，第 7-3 页
- 故障切换链路接口，第 7-4 页
- 连接故障切换链路，第 7-4 页

故障切换链路数据

以下信息将通过故障切换链路传输：

- 设备状态 （主用或备用）
- Hello 消息 (keep-alives)
- 网络链路状态
- MAC 地址交换
- 配置复制和同步

故障切换链路接口

您可以将任意未使用的接口 （物理、冗余或 EtherChannel）用作故障切换链路；但是，您不能指定当前已配置名称的接口。故障切换链路接口不会配置为常规网络接口；该接口仅会因为故障切换而存在。此接口仅可用于故障切换链路 （或者也用于状态链路）。ASA 不支持在用户数据和故障切换链路之间共享接口，即使为用户数据和故障切换配置了不同的子接口。必须将独立的物理、 EtherChannel 或冗余接口用于故障切换链路。

对于用作故障切换链路的冗余接口，请参见以下因提供更多冗余而带来的优势：

- 当故障切换设备启动时，它会在成员接口之间轮流检测主用设备。
- 如果故障切换设备在其中一个成员接口上停止从对等体接收保持连接消息，它将切换到另一个成员接口。

对于用作故障切换链路的 EtherChannel，要阻止无序数据包，仅使用 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。您不能在 EtherChannel 配置用作故障切换链路时对其进行修改。

连接故障切换链路

您可以使用以下两种方法之一连接故障切换链路：

- 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 的故障切换接口。
- 使用以太网电缆直接连接设备，无需外部交换机。

如果不在设备之间使用交换机，当接口出现故障时，两台对等体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。

状态故障切换链路

要使用状态故障切换，必须配置状态故障切换链路，以便传送连接状态信息。

您有三种可用于状态链路的接口选项。

- 专用接口 （推荐），第 7-4 页
- 共享故障切换链路，第 7-5 页
- 共享常规数据接口 （不推荐），第 7-5 页

备注　请勿将管理接口用于状态链路。

专用接口 （推荐）

您可以将专用接口 （物理、冗余或 EtherChannel）用于状态链路。对于用作状态链路的 EtherChannel，要阻止无序数据包，仅使用 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。

可以使用以下两种方法之一连接专用的状态链路：

- 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 的故障切换接口。
- 使用以太网电缆直接连接设备，无需外部交换机。

  如果不在设备之间使用交换机，当接口出现故障时，两台对等体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。

使用长距离故障切换时，为实现最佳性能，故障切换链路的延迟应低于 10 毫秒且不超过 250 毫秒。如果延迟超过 10 毫秒，重新传输故障切换消息会导致一些性能降级。

共享故障切换链路

如果您没有足够的接口，可能有必要共享故障切换链路。如果您将故障切换链路用作状态链路，则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状态链路。

共享常规数据接口 （不推荐）

与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，接口上可能会发送大量状态故障切换流量，导致该网段出现性能问题。

仅单情景路由模式支持将数据接口用作状态链路。

避免中断故障切换和数据链路

我们建议，让故障切换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。如果故障切换链路发生故障， ASA 可使用数据接口来确定是否需要进行故障切换。随后，故障切换操作会被暂停，直到故障切换链路恢复正常。

请参阅以下连接情景，以设计具有弹性的故障切换网络。

情景 1 - 不推荐

如果单台交换机或一组交换机用于连接两台 ASA 之间的故障切换和数据接口，则交换机或交换机间链路发生故障时，两台 ASA 都都将处于主用状态。因此，不推荐使用下图中显示的 2 种连接方法。

图 7-1　使用单台交换机进行连接 - 不推荐

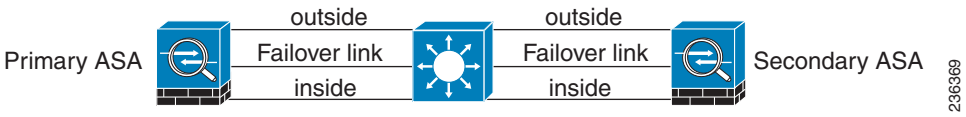
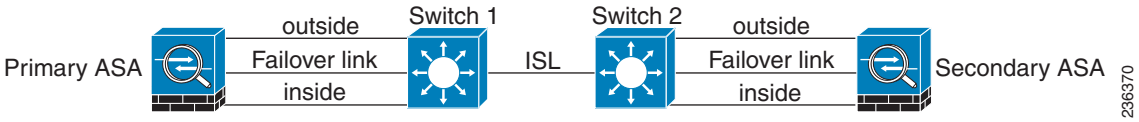


图 7-2　使用两台交换机进行连接 - 不推荐



情景 2 - 推荐

我们不推荐让故障切换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切换链路，如下图所示。

图 7-3　使用不同的交换机进行连接

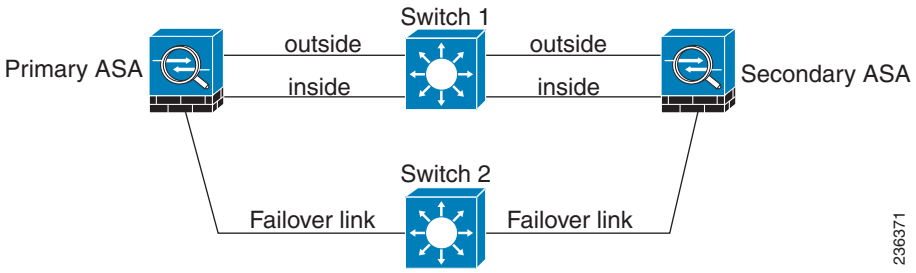
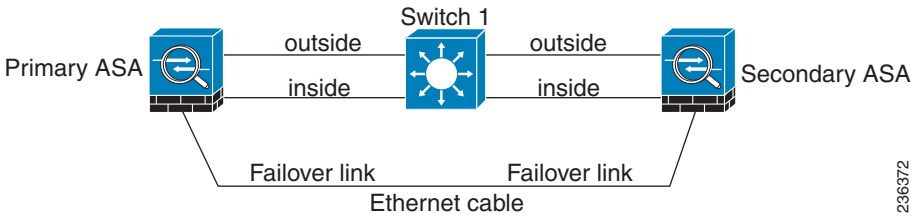


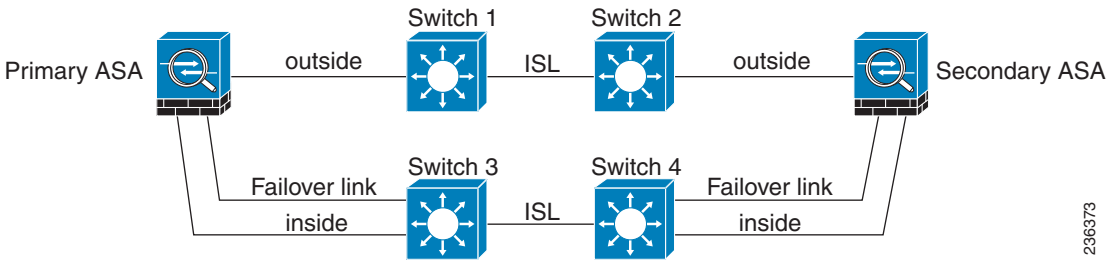
图 7-4　使用电缆进行连接



情景 3 - 推荐

如果 ASA 数据接口连接到多台交换机，则故障切换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，如下图所示。

图 7-5　使用安全的交换机进行连接



情景 4 - 推荐

最可靠的故障切换配置使用故障切换链路上的冗余接口，如下图所示。

图 7-6　使用冗余接口进行连接

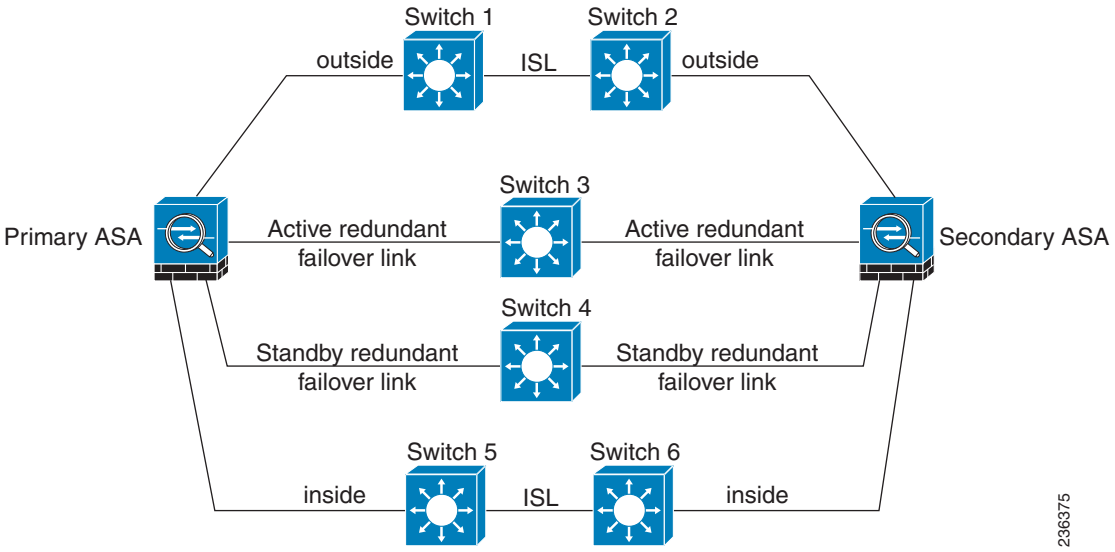
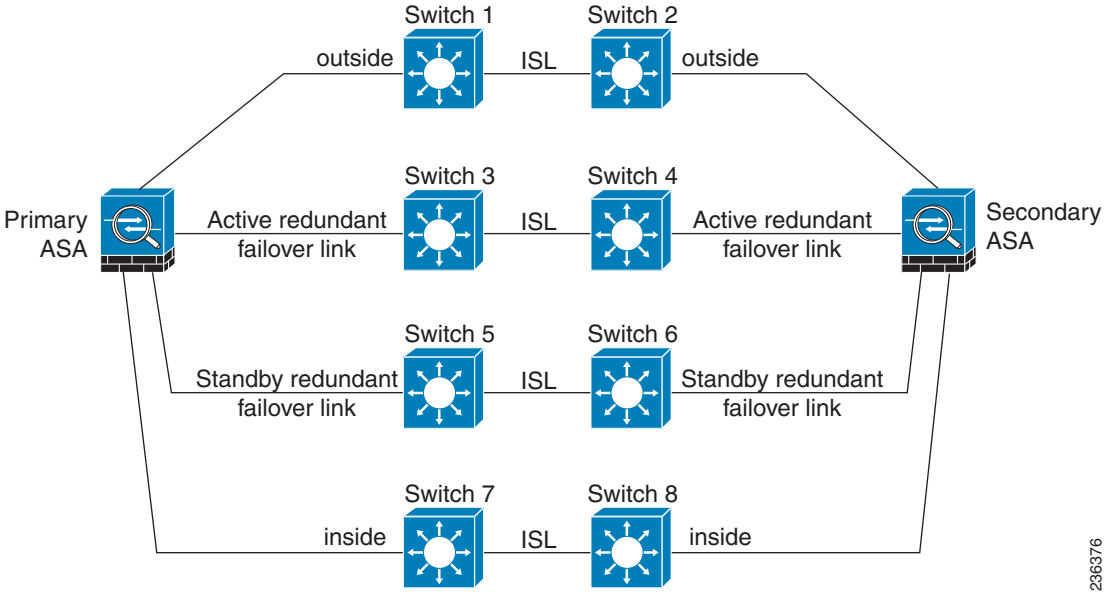


图 7-7　使用交换机间链路进行连接



故障切换中的 MAC 地址和 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. 当主设备或故障切换组进行故障切换时，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。

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。在多情景模式下， ASA 会默认生成虚拟的主用和备用 MAC 地址。在单情景模式下，您可以手动配置虚拟 MAC 地址。

如果您没有配置虚拟 MAC 地址，则可能需要清除连接的路由器上的 ARP 表，以便恢复流量。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。

进行故障切换时，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状态链路的情况。

相关主题

- 关于 MAC 地址，第 6-11 页
- 配置主用/主用故障切换，第 7-28 页

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。

- 机箱内故障切换，第 7-8 页
- 机箱间故障切换，第 7-9 页

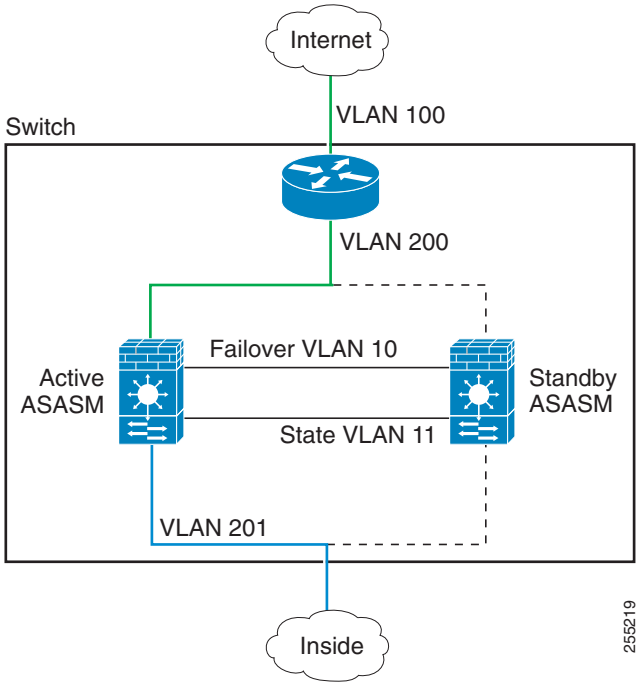
机箱内故障切换

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。

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。

下图显示典型的交换机内配置。

图 7-8　　交换机内故障切换



机箱间故障切换

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切换，但是，它可以协调地配合交换机故障切换操作。请参阅交换机文档，以便配置交换机的故障切换。

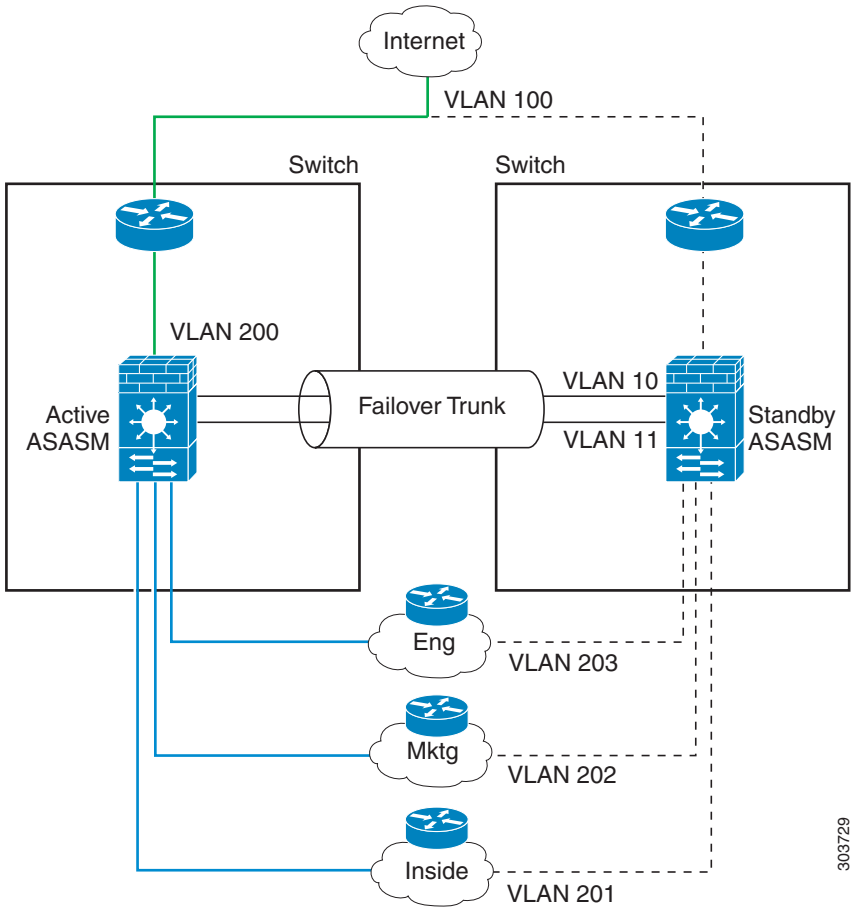
要在 ASASM 之间实现最佳的故障切换通信可靠性，我们建议您在两台交换机之间配置 EtherChannel Trunk 端口，以便承载故障切换和状态 VLAN。

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呼叫数据包。

下图显示典型的交换机和 ASASM 冗余配置。两台交换机之间的 Trunk 会承载故障切换 ASASM VLAN （VLAN 10 和 11）。

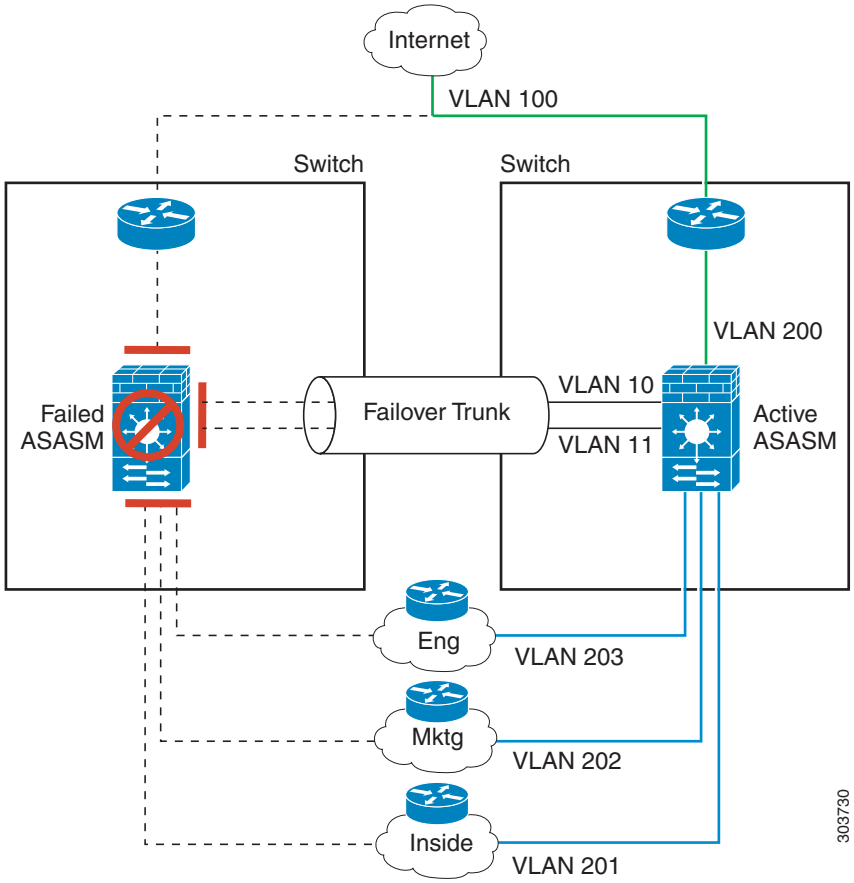
备注　ASASM 故障切换与交换机故障切换操作无关；但是，ASASM 可在任何一种交换机故障切换情景下工作。

图 7-9　　正常操作


Internet
VLAN 100
Switch
Switch
VLAN 200
Active
ASASM
Failover Trunk
VLAN 10
VLAN 11
Standby
ASASM
Eng
VLAN 203
Mktg
VLAN 202
Inside
VLAN 201
303729

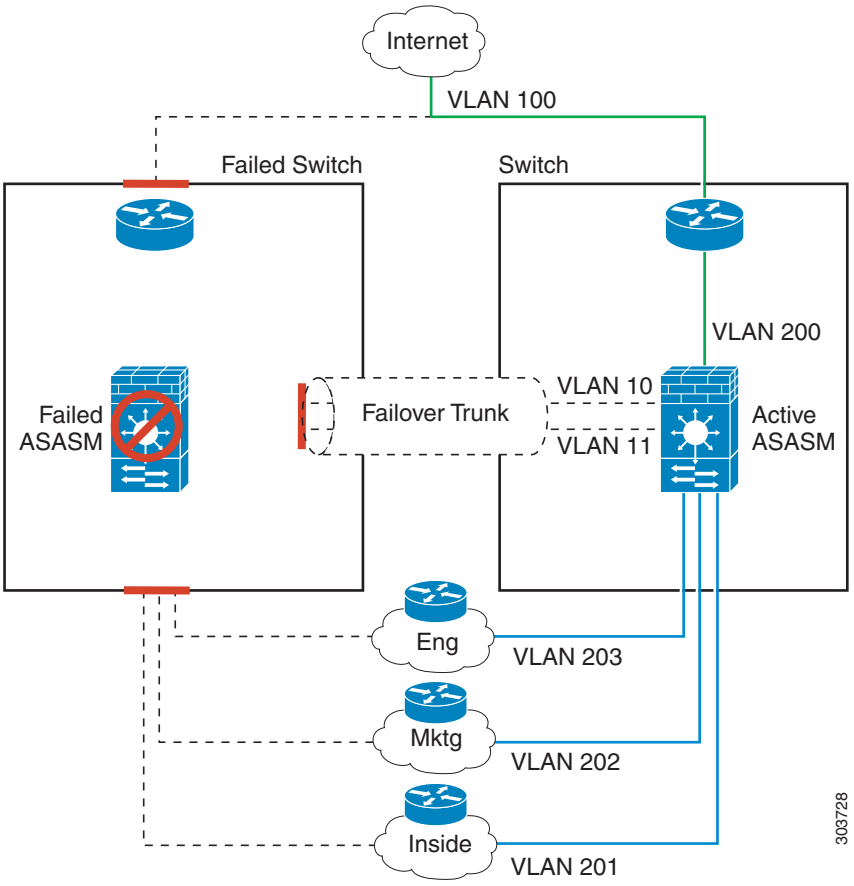
如果主 ASASM 发生故障，则辅助 ASASM 会变为主用状态，并成功穿过防火墙 VLAN。

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 均会故障切换到其辅助设备。

图 7-11　　交换机故障



无状态故障切换和状态故障切换

ASA 支持主用/备用和主用/主用模式下的两种类型的故障切换，即无状态故障切换和状态故障切换。

- 无状态故障切换，第 7-13 页
- 状态故障切换，第 7-13 页

备注　无客户端 SSL VPN 的某些配置元素 （如书签和自定义）使用 VPN 故障切换子系统，该子系统是状态故障切换的一部分。您必须使用状态故障切换，在同步故障切换对中的成员之间同步这些元素。不推荐将无状态故障切换用于无客户端 SSL VPN。

无状态故障切换

发生故障切换时，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。

备注　无客户端 SSL VPN 的某些配置元素 （如书签和自定义）使用 VPN 故障切换子系统，该子系统是状态故障切换的一部分。您必须使用状态故障切换，在同步故障切换对中的成员之间同步这些元素。不推荐将无状态 （常规）故障切换用于无客户端 SSL VPN。

状态故障切换

启用状态故障切换时，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/主用故障切换中，在主用和备用故障切换组之间传送此信息。发生故障切换之后，相同的连接信息在新主用设备上可用。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。

- 支持的功能，第 7-13 页
- 不支持的功能，第 7-14 页

支持的功能

启用状态故障切换时，以下状态信息会传送到备用 ASA：

- NAT 转换表
- TCP 连接状态
- TCP 连接状态
- ARP 表
- 第 2 层网桥表 （在透明防火墙模式下运行时）
- HTTP 连接状态 （如果启用了 HTTP 复制） - 默认情况下，启用了状态故障切换时， ASA 不会复制 HTTP 会话信息。因为 HTTP 会话通常短暂的且由于 HTTP 客户端通常重试失败的连接尝试，无法进行复制 HTTP 会话提高系统性能，而不会造成严重的数据或失去连接。
- 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 - 状态故障切换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。发生故障切换事件时，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。进行故障切换后，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。计时器到期后，过时的路由条目 （由代编号确定）将从表中删除。于是 RIB 将包含新主用设备上的最新的路由协议转发信息。

注意　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。

- 思科 IP SoftPhone 会话 - 如果在活动 Cisco IP SoftPhone 会话期间发生故障切换，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 - 进行故障切换后， 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，在故障切换过程中可能会丢失数据包，并且无法从数据包丢失中恢复。

不支持的功能

启用状态故障切换时，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
- 需进行高级 TCP 状态跟踪的应用检测 - 不会自动复制这些连接的 TCP 状态。如果这些连接复制到备用设备，将会尽力尝试重新建立 TCP 状态。
- TCP 状态绕行连接
- DHCP 服务器地址租用
- 组播路由
- 模块的状态信息，如 ASA FirePOWER 模块。
- 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。必须重新建立呼叫。
- 选定的无客户端 SSL VPN 功能：
  - 智能隧道
  - 端口转发
  - 插件
  - Java 小程序
  - IPv6 无客户端或 Anyconnect 会话
  - Citrix 身份验证 （Citrix 用户在故障切换后必须重新进行身份验证）

故障切换的透明防火墙模式要求

使用透明防火墙模式时，故障切换存在特殊的注意事项。

- 设备 ASAv 的透明模式要求，第 7-14 页
- ASA 服务模块的透明模式要求，第 7-15 页

设备 ASAv 的透明模式要求

当主用设备故障切换到备用设备时，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到 STP 转发模式。该端口仍会参与 STP。因此，如果端口是环路的一部分，则端口最终会转换为 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切换功能或 STP 稳定性。

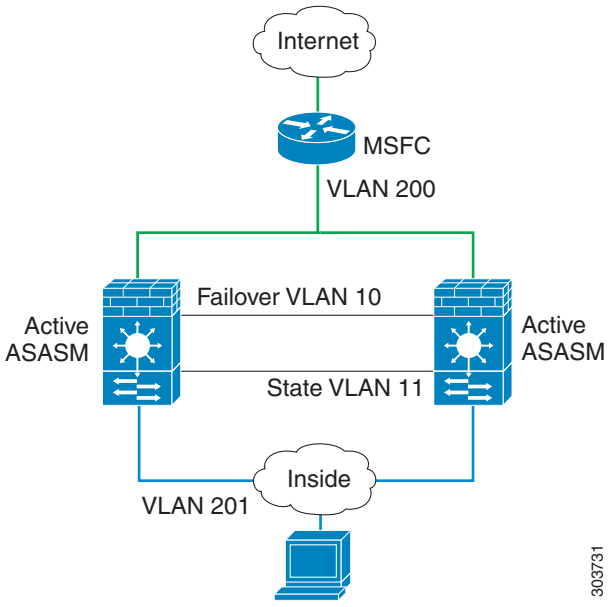
- 禁用接口监控。
- 将接口保持时间增大到一个高值，这将允许 STP 在 ASA 进行故障切换之前融合。
- 降低 STP 计时器的值，以 STP 在接口保持时间之内融合。

ASA 服务模块的透明模式要求

当您在透明模式下使用故障切换时，为避免出现环路，应允许 BPDU 通过 （默认），并且必须使用支持 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切换链路。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。要断开环路，需要桥接 VLAN 200 和 VLAN 201 之间发送的 BPDU。

图 7-12　透明模式环路



故障切换运行状况监控

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。

- 设备运行状况监控，第 7-16 页
- 接口监控，第 7-16 页

设备运行状况监控

ASA 会通过 Hello 消息监控故障切换链路，进而确定其他设备的运行状况。当设备在故障切换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（包括故障切换链路）上发送接口 LANTEST 消息，以验证对等体是否响应。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 在故障切换链路上收到响应，则不会进行故障切换。
- 如果 ASA 在故障切换链路上未收到响应，但在数据接口上收到响应，则设备不会进行故障切换。故障切换链路会标记为发生故障。您应尽快恢复故障切换链路，因为当故障切换切换发生故障时，设备无法故障切换到备用设备。
- 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，并将另一台设备分类为故障设备。

接口监控

您最多可以监控 250 个接口（在多模式下，会在所有情景之间进行分配）。您应监控重要的接口。例如，在多模式下，您可以配置一个用于监控共享接口的情景：因为接口是共享的，所有情景都可以从监控中受益。

当设备在 2 个轮询期内，未在受监控的接口上收到 Hello 消息，将运行接口测试。如果对于某个接口，所有接口测试均失败，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阈值，则会进行故障切换。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，并且不会计入故障切换限制。

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。

如果有服务模块（例如 ASA FirePOWER SSP），则 ASA 也会通过背板接口监控模块的运行状况。模块故障被视为设备故障，会触发故障切换。此设置可配置。

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)。

备注　如果故障设备未恢复，并且您认为其应未发生故障，则可通过输入 **failover reset** 命令重置状态。但是，如果故障切换条件仍然存在，设备将再次失败。

接口测试

ASA 使用以下接口测试：

1. 链路打开/关闭测试 - 接口状态测试。如果链路打开/关闭测试表明接口已关闭，则 ASA 认为其发生了故障。如果状态为打开，则 ASA 会执行网络活动测试。

2. 网络活动测试 - 收到的网络活动的测试。此测试旨在使用 LANTEST 消息生成网络流量，以确定发生故障的设备 （如有）。测试开始时，每台设备会清除其接口的收到的数据包计数。在测试期间 （最多 5 秒），一旦设备收到数据包，则接口会被视为正常运行。如果一台设备收到流量，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。如果任何设备都未收到流量，则 ASA 会开始 ARP 测试。
3. ARP 测试 - 读取设备 ARP 缓存，以获取 10 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，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 ASA 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。如果未收到任何流量，测试将通过 ARP 测试再次开始。

接口状态

受监控接口可以具有以下状态：

- Unknown - 初始状态。此状态也可能意味着状态无法确定。
- Normal - 接口正在接收流量。
- Testing - 接口上有 5 个轮询时间未收听到 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 - 在接口上没有收到流量，但在对等体接口上收听到流量。

故障切换时间

下表显示了最小、默认和最大故障切换时间。

表 7-1　　ASA 故障切换时间

故障切换条件	最低	默认	最大值
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

故障切换包含各种类型的配置同步。

- 运行配置复制，第 7-18 页
- 文件复制，第 7-18 页
- 命令复制，第 7-18 页

运行配置复制

当故障切换对中的一台或两台设备启动时，系统会执行运行配置复制。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切换命令除外），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”；完成时， ASA 显示消息 “End Configuration Replication to mate”。根据配置的大小，复制可能需要几秒到几分钟。

在备用设备上，配置仅存在于运行内存中。您应根据保存配置更改，第 2-18 页将配置保存到闪存中。

备注　在复制过程中，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。

备注　**crypto ca server** 命令和相关子命令不会同步到故障切换对等体。

文件复制

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

  ASA 使用存储在 cache:/stc/profiles 中的 AnyConnect 客户端配置文件的缓存文件，而不是存储在闪存文件系统中的文件。要将 AnyConnect 客户端配置文件复制到备用设备，请执行以下其中一项操作：
  - 在主用设备上输入 **write standby** 命令。
  - 在主用设备上重新应用配置文件。
  - 重新加载备用设备。
- 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。不必将主用配置保存到闪存才能复制命令。

在主用/主用故障切换中，在系统执行空间中输入的命令会从其上的故障切换组 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不同步。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*复制到备用 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/备用故障切换

主用/备用故障切换允许您使用备用 ASA 来接管故障设备的功能。主用设备出现故障时将变为备用状态，同时备用设备变为主用状态。

备注　对于多情景模式， ASA 可以故障切换整台设备 （包括所有情景），但不能对各个情景单独进行故障切换。

- 主/辅助角色和主用/备用状态，第 7-19 页
- 启动时的主用设备确定，第 7-19 页
- 故障切换事件，第 7-20 页

主/辅助角色和主用/备用状态

故障切换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 （即，使用哪一个 IP 地址以及哪一台设备会主动传送流量）有关。

但是，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差别：

- 如果两台设备同一时间启动 （并且运行状况相同），则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，辅助设备处于主用状态，而且无法通过故障切换链路获取主设备的 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

主用设备按以下方式确定：

- 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。

故障切换事件

在主用/备用故障切换中，故障切换会在设备级别进行。即使在多情景模式下运行的系统上，您也无法对个别情景或一组情景进行故障切换。

下表显示了每个故障事件的故障切换操作。对于每种故障事件，该表显示了故障切换策略 （故障切换或禁用故障切换）、主用设备执行的操作、备用设备执行的操作，以及有关故障切换条件和操作的所有特别说明。

表 7-2　故障切换事件

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	成为主用设备 将主用设备标记为发生故障	在任何受监控接口或故障切换链路上，均未收到 Hello 消息。
以前的主用设备恢复	禁用故障切换	成为备用设备	无需操作	无。
备用设备发生故障 （电源或硬件）	禁用故障切换	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切换，即使超过接口故障阈值也是如此。
故障切换链路在运行过程中发生故障	禁用故障切换	将故障切换链路标记为发生故障	将故障切换链路标记为发生故障	您应尽快恢复故障切换链路，因为当故障切换链路发生故障时，设备无法故障切换到备用设备。
故障切换链路在启动时发生故障	禁用故障切换	将故障切换链路标记为发生故障	成为主用设备	如果故障切换链路在启动时发生故障，则两台设备都会成为主用设备。
状态链路发生故障	禁用故障切换	无需操作	无需操作	如果发生故障切换，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	成为主用设备	无。
备用设备上的接口故障超过阈值	禁用故障切换	无需操作	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切换，即使超过接口故障阈值也是如此。

关于主用/主用故障切换

本部分介绍主用/主用故障切换。

- 主用/主用故障切换概述，第 7-21 页
- 故障切换组的主/辅助角色和主用/备用状态，第 7-21 页
- 故障切换事件，第 7-21 页

主用/主用故障切换概述

在主用/主用故障切换配置下，两台 ASA 都可以传送网络流量。主用/主用故障切换仅适用于多情景模式下的 ASA。在主用/主用故障切换中，您可将 ASA 上的安全情景最多划分为 2 个故障切换组。

故障切换组就是一个或多个安全情景的逻辑组。您可以将故障切换组指定为在主 ASA 上处于主用状态，并将故障切换组 2 指定为在辅助 ASA 上处于主用状态。发生故障切换时，会在故障切换组级别进行。例如，根据接口故障模式，故障切换组 1 可能会故障切换到辅助 ASA，相应地，故障切换组 2 可能故障切换到主 ASA。在以下情况下可能发生此事件：故障切换组 1 中的接口在主 ASA 上发生故障，但在辅助 ASA 上正常工作，而故障切换组 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切换组 1 的成员。默认情况下，所有未分配的安全情景也是故障切换组 1 的成员。如果希望使用主用/主用故障切换，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切换组 2。

备注　配置主用/主用故障切换时，请确保两台设备的整合流量在每台设备的处理能力之内。

备注　需要时，可将两个故障切换组分配到一台 ASA，但您将无法利用具有两台主用 ASA 的优势。

故障切换组的主/辅助角色和主用/备用状态

就像在主用/备用故障切换中一样，主用/主用故障切换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/备用故障切换的是，当两台设备同时启动时，此指定不指示哪一台设备会成为主用设备。相反，主设备/辅助设备指定会做两件事：

- 两台设备同时启动时，主设备会提供运行配置。
- 配置中的每个故障切换组都配置了主设备或辅助设备首选项。

启动时的故障切换组主用设备确定

故障切换组在其上变为主用状态的的设备按以下方式确定：

- 一台设备启动时，如果对等设备不可用，则两个故障切换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 （而且两个故障切换组都处于主用状态），则故障切换组将在主用设备上保持主用状态，而无论故障切换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：
  - 发生故障切换。
  - 您手动强制执行故障切换。
  - 您为故障切换组配置了抢占，这导致故障切换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，每个故障切换组都会在其首选设备上变为主用状态。

故障切换事件

在主用/主用故障切换配置中，故障切换会在故障切换组级别，而不是系统级别进行。例如，如果您将两个故障切换组指定为主设备上的主用故障切换组，并且故障切换组 1 发生故障，则故障切换组 2 会在主设备上保持主用，而故障切换组 1 则会在辅助设备上变为主用状态。

由于故障切换组可以包含多个情景，并且每个情景可以包含多个接口，因此有可能单个情景中的所有接口都发生故障而不导致相关故障切换组发生故障。

下表显示了每个故障事件的故障切换操作。对于每种故障事件，给出了策略 （是否发生故障切换）、主用故障切换组的操作和备用故障切换组的操作。

表 7-3　　故障切换事件

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	成为主用设备 将主用设备标记为发生故障	故障切换对中的一台设备发生故障时，该设备上的所有主用故障切换组都会被标记为发生故障，并在对等设备上变为主用状态。
主用故障切换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	成为主用设备	无。
备用故障切换组上的接口故障超过阈值	禁用故障切换	无需操作	将备用组标记为发生故障	备用故障切换组标记为发生故障后，主用故障切换组不会尝试进行故障切换，即使超过接口故障阈值也是如此。
以前的主用故障切换组恢复	禁用故障切换	无需操作	无需操作	除非配置了故障切换组抢占，否则故障切换组会在其当前设备上保持主用状态。
故障切换链路在启动时发生故障	禁用故障切换	成为主用设备	成为主用设备	如果故障切换链路在启动时发生故障，则两台设备上的故障切换组都会变为主用状态。
状态链路发生故障	禁用故障切换	无需操作	无需操作	如果发生故障切换，状态信息会过时，而且会话会被终止。
故障切换链路在运行过程中发生故障	禁用故障切换	不适用	不适用	每台设备都会将故障切换链路标记为发生故障。您应尽快恢复故障切换链路，因为当故障切换链路发生故障时，设备无法故障切换到备用设备。

故障切换许可

故障切换设备不要求每个设备上具有同一许可证。如果您在两台设备上都有许可证，则这两个许可证会合并为一个运行故障切换集群许可证。此规则存在一些例外情况。有关故障切换的具体许可要求，请参阅下表。

型号	许可证要求
ASA 5506-X 系列	• 主用/备用 - 增强型安全许可证。 • 主用/主用 - 不支持。 **备注**　每台设备必须拥有相同的加密许可证。

型号	许可证要求
ASA 5512-X 至 ASA 5555-X	• ASA 5512-X - 增强型安全许可证。 • 其他型号 - 基础许可证。 **备注**　每台设备必须拥有相同的加密许可证；每台设备必须拥有相同的 IPS 模块许可证。您还需要两台设备的 IPS 侧均有 IPS 签名订用。请参阅以下准则： – 要购买 IPS 签名订用，您需要具有预装了 IPS 的 ASA（部件号必须包含“IPS”，例如 ASA5515-IPS-K9）；您不能为非 IPS 部件号 ASA 购买 IPS 签名订用。 – 您需要在两台设备上均有 IPS 签名订用；由于此订用不是 ASA 许可证，因此在故障切换中不会进行共享。 – 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 模块许可证在故障切换集群许可证中进行技术共享。但是，由于 IPS 签名订用要求，您必须为故障切换中的每台设备购买单独的 IPS 模块许可证。
ASAv	• 主用/备用 - 标准和高级版许可证。 • 主用/主用 - 不支持。 **备注**　备用设备要求具有与主设备相同的型号许可证；每台设备必须拥有相同的加密许可证。
所有其他型号	基础许可证。 **备注**　每台设备必须拥有相同的加密许可证。

故障切换准则

情景模式

- 仅多情景模式支持主用/主用模式。
- 对于多情景模式，请在系统执行空间中执行所有步骤，除非另外说明。
- 如果您尝试同时在两个或更多情景中进行配置更改， ASA 故障切换复制将会失败。变通方案是在每个情景中连续进行配置更改。

型号支持

对于 ASA 5506W-X，必须为内部 GigabitEthernet 1/9 接口禁用接口监控。这些接口将无法进行通信以执行默认接口监控检查，由于预期的接口通信故障，导致交换机在主用和备用之间来回切换。

其他准则

- 发生故障切换事件时，在连接到 ASA 故障切换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。
- 您最多可以在一台设备上监控跨所有情景的 250 个接口。
- 对于主用/主用故障切换，不应在相同 ASR 组中配置相同情景中的两个接口。
- 对于主用/主用故障切换，最多可以定义两个故障切换组。
- 对于主用/主用故障切换，删除故障切换组时，必须最后删除故障切换组 1。故障切换组 1 始终包含管理情景。未分配到故障切换组的所有情景将默认分配到故障切换组 1。不能删除已显式分配了情景的故障切换组。

相关主题

故障切换配置中的自动更新服务器支持，第 33-38 页

故障切换的默认设置

默认情况下，故障切换策略包含以下内容：

- 在状态故障切换中不进行 HTTP 复制。
- 单个接口故障导致故障切换。
- 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 地址在多情景模式下启用；在单情景模式下禁用。
- 监控所有物理接口，或者对于 ASASM，监控所有 VLAN 接口。

配置主用/备用故障切换

- 为主用/备用故障切换配置主设备，第 7-24 页
- 为主用/备用故障切换配置辅设备，第 7-27 页

为主用/备用故障切换配置主设备

遵循本节介绍的步骤，配置主用/备用故障切换配置中的主设备。这些步骤提供了在主设备上启用故障切换所需的最小配置。

准备工作

- 为除故障切换和状态链路外的所有接口配置备用 IP 地址。
- 请勿为故障切换和状态链路配置 **nameif**。
- 对于多情景模式，请在系统执行空间中完成本程序。要从该情景切换到系统执行空间，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　指定要用作故障切换链路的接口：

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* 可指定 VLAN ID。

步骤 3　为故障切换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　启用故障切换链路：

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，指定与故障切换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* 可指定 VLAN ID。

步骤 6　如果您指定了单独的状态链路，可以将主用和备用 IP 地址分配给状态链路：

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
```

此地址应处于不同于故障切换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。

如果您将共享状态链路，请跳过此步骤。

步骤 7　如果您指定了单独的状态链路，请启用状态链路。

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，以加密故障切换和状态链路上的通信：

- （首选）在设备之间的故障切换和状态链路上建立 IPsec LAN 到 LAN 隧道，以加密所有的故障切换通信：

  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。

  如果使用主密码 （请参阅配置主密码，第 16-10 页），则该密钥会在配置中加密。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密密钥。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 ****；这种遮掩密钥无法复制。

  如果您未配置故障切换和状态链路加密，故障切换通信 （包括在命令复制过程中发送的配置中的所有密码或密钥）将采用明文形式。

  不能同时使用 IPsec 加密和传统 **failover key** 加密。如果同时配置两种方法，将使用 IPsec。但是，如果使用主密码 （请参阅配置主密码，第 16-10 页），则在配置 IPsec 加密之前，必须先使用 **nofailover key** 命令删除故障切换密钥。

  故障切换 LAN 到 LAN 隧道不计入 IPsec （其他 VPN）许可证。

- （可选）对故障切换和状态链路上的故障切换通信进行加密：

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  示例：

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  可以使用 1 到 63 个字符的 *shared_secret*，或者 32 个字符的 **hex** *key*。对于 *shared_secret*，您可以任意组合使用数字、字母或标点符号。该共享密钥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。

  如果使用主密码 （请参阅配置主密码，第 16-10 页），则共享密钥或十六进制密钥会在配置中加密。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密的共享密钥或十六进制密钥。默认情况下使用 **0**，表明未加密的密码。

  failover key 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。

  如果您未配置故障切换和状态链路加密，故障切换通信 （包括在命令复制过程中发送的配置中的所有密码或密钥）将采用明文形式。

步骤 9　启用故障切换：

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切换参数：

```
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 folink 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
```

相关主题

- 第 13 章 “路由模式和透明模式接口”

为主用/备用故障切换配置辅设备

在辅助设备上只需要配置故障切换链路。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，该命令可确定每台设备是主设备，还是辅助设备。

准备工作

- 请勿为故障切换和状态链路配置 **nameif**。
- 对于多情景模式，请在系统执行空间中完成本程序。要从该情景切换到系统执行空间，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。请参阅为主用/备用故障切换配置主设备，第 7-24 页。

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　故障切换配置同步之后，会将配置保存到闪存：

```
ciscoasa(config)# write memory
```

配置主用/主用故障切换

- 为主用/主用故障切换配置主设备，第 7-28 页
- 为主用/主用故障切换配置辅助设备，第 7-31 页

为主用/主用故障切换配置主设备

遵循本节介绍的步骤，配置主用/主用故障切换配置中的主设备。这些步骤提供了在主设备上启用故障切换所需的最小配置。

准备工作

- 根据启用或禁用多情景模式，第 6-14 页启用多情景模式。
- 根据第 13 章“路由模式和透明模式接口”，为除故障切换和状态链路外的所有接口配置备用 IP 地址。
- 请勿为故障切换和状态链路配置 **nameif**。
- 在系统执行空间中完成本程序。要从该情景切换到系统执行空间，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　指定要用作故障切换链路的接口：

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* 可指定 VLAN ID。

步骤 3　为故障切换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　启用故障切换链路：

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，指定与故障切换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* 可指定 VLAN ID。

步骤 6　如果您指定了单独的状态链路，可以将主用和备用 IP 地址分配给状态链路：

此地址应处于不同于故障切换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状态链路，请启用状态链路：

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，以加密故障切换和状态链路上的通信：

- （首选）在设备之间的故障切换和状态链路上建立 IPsec LAN 到 LAN 隧道，以加密所有的故障切换通信：

  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。

  如果使用主密码 （请参阅配置主密码，第 16-10 页），则该密钥会在配置中加密。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密密钥。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 ****；这种遮掩密钥无法复制。

  如果您未配置故障切换和状态链路加密，故障切换通信 （包括在命令复制过程中发送的配置中的所有密码或密钥）将采用明文形式。

  不能同时使用 IPsec 加密和传统 **failover key** 加密。如果同时配置两种方法，将使用 IPsec。但是，如果使用主密码 （请参阅配置主密码，第 16-10 页），则在配置 IPsec 加密之前，必须先使用 **nofailover key** 命令删除故障切换密钥。

  故障切换 LAN 到 LAN 隧道不计入 IPsec （其他 VPN）许可证。

- （可选）对故障切换和状态链路上的故障切换通信进行加密：

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  示例：

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  可以使用 1 到 63 个字符的 *shared_secret*，或者 32 个字符的 **hex** *key*。

  对于 *shared_secret*，您可以任意组合使用数字、字母或标点符号。该共享密钥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。

  如果使用主密码 （请参阅配置主密码，第 16-10 页），则共享密钥或十六进制密钥会在配置中加密。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密的共享密钥或十六进制密钥。默认情况下使用 **0**，表明未加密的密码。

  failover key 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。

  如果您未配置故障切换和状态链路加密，故障切换通信 （包括在命令复制过程中发送的配置中的所有密码或密钥）将采用明文形式。

步骤 9　创建故障切换组 1：

```
failover group 1
```

默认情况下，此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。如果需要非标准配置，则可以使用 **primary** 或 **secondary** 子命令视需要指定不同的设备首选项。

步骤 10　创建故障切换组 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切换组：

```
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切换组 1。管理情景始终是故障切换组 1 的成员；您不能将其分配给组 2。

步骤 12　启用故障切换：

```
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切换参数：

```
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 folink 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/主用故障切换配置辅助设备

在辅助设备上只需要配置故障切换链路。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，该命令可确定每台设备是主设备，还是辅助设备。

准备工作

- 根据启用或禁用多情景模式，第 6-14 页启用多情景模式。
- 请勿为故障切换和状态链路配置 **nameif**。
- 在系统执行空间中完成本程序。要从该情景切换到系统执行空间，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。请参阅为主用/主用故障切换配置主设备，第 7-28 页。

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　故障切换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，可强行要求故障切换组 2 在辅助设备上处于主用状态：

```
failover active group 2
```

配置可选故障切换参数

您可以视需要自定义故障切换设置。

- 配置故障切换条件和其他设置，第 7-32 页
- 配置接口监控，第 7-35 页
- 配置非对称路由数据包支持 （主用/主用模式），第 7-35 页

配置故障切换条件和其他设置

有关您可在本节中更改的许多参数的默认设置，请参阅故障切换的默认设置，第 7-24 页。对于主用/主用模式，您可以设置每个故障切换组的大多数条件。

准备工作

在多情景模式下，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/主用模式下，您可以为系统设置此速率；但不能为每个故障切换组设置此速率。

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切换。但是，当网络临时堵塞时，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切换通信的呼叫数据包，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/主用模式下，您可以为系统设置此速率；但不能为每个故障切换组设置此速率。

failover replication rate *conns*

示例：

```
ciscoasa(config)# failover replication rate 20000
```

步骤 3　禁用在备用设备或情景中直接进行任何配置更改的功能：

默认情况下，允许备用设备/情景上进行配置，但系统会显示一条警告消息。

failover standby config-lock

步骤 4　（仅主用/主用模式）指定要自定义的故障切换组：

failover group {**1** | **2**}

示例：

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

步骤 5　（仅主用/主用模式）为故障切换组 1 配置故障切换抢占：

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，则两个故障切换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，此命令会使故障切换组自动在该设备上变为主用状态。

您可以输入可选的 *delay* 值，该值指定故障切换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。

如果启用状态故障切换，则抢占会延迟，直到连接从当前处于主用状态的故障切换组所在的设备中复制为止。

步骤 6　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

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 7　设置接口发生故障时的故障切换阈值：

- 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，一个接口故障会导致故障切换。

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 8　更改接口轮询和保持时间：

- 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，则介于 500 和 999 毫秒之间。保持时间确定，从一个呼叫数据包丢失，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。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切换条件，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 9　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 将需要输入 000C.F142.4CDE。

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。

您也可以使用其他命令或方法设置 MAC 地址，但是我们建议只使用一种方法。如果使用多种方法设置 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 10　（仅主用/主用模式）视需要为其他故障切换组，重复本程序。

配置接口监控

默认情况下，会在所有物理接口或所有 VLAN 接口 （对于 ASASM）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，以免影响故障切换策略。

准备工作

- 您最多可以在一台设备上监控 250 个接口 （跨多情景模式下的所有情景）。
- 在多情景模式下，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）触发故障切换，则可以使用 **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/主用故障切换下运行时，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/主用故障切换对中的两台 ASA 连接到不同的运营商，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。如果没有找到匹配项，数据包会被丢弃。如果找到匹配项，则会进行以下的操作：

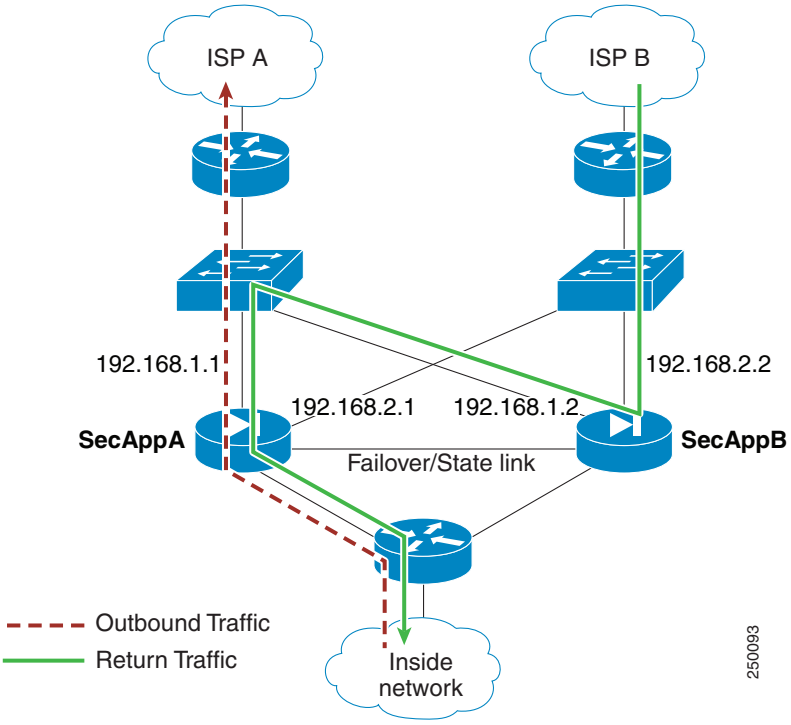
- 如果传入流量来自对等设备，第 2 层报头的部分或全部内容会被重写，数据包会被重定向到另一设备。只要会话处于活动状态，此重定向即可继续。

- 如果传入流量来自相同设备上的不同接口，第 2 层报头的部分或全部内容会被重写，数据包会被重新注入数据流。

备注　此功能不提供非对称路由；它会将非对称路由数据包恢复到正确接口。

下图显示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，返回流量会使用主用 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。状态故障切换会将会话信息从 SecAppA 复制到 SecAppB。
5. 第 2 层报头会使用接口 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。

准备工作

- 状态故障切换 - 将主用故障切换组中的接口上的会话的状态信息，传送给备用故障切换组。
- 复制 HTTP - HTTP 会话状态信息不会传送给备用故障切换组，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，执行本程序。

- 您无法在一个情景中同时配置 ASR 组和流量区域。如果在情景中配置一个区域，任何情景接口都不能属于 ASR 组。

操作步骤

步骤 1　在主设备上，指定要允许非对称路由数据包的接口：

interface *phy_if*

示例：

```
primary/admin(config)# interface gigabitethernet 0/0
```

步骤 2　设置接口的 ASR 组编号：

asr-group *num*

示例：

```
primary/admin(config-ifc)# asr-group 1
```

num 的有效值范围为 1 到 32。

步骤 3　在辅助设备上，指定要允许非对称路由数据包的类似接口：

interface *phy_if*

示例：

```
secondary/ctx1(config)# interface gigabitethernet 0/1
```

步骤 4　设置接口的 ASR 组编号，以匹配主设备接口：

asr-group *num*

示例：

```
secondary/ctx1(config-ifc)# asr-group 1
```

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 的设备是故障切换对中的主设备。

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 情景配置

```
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 情景配置

```
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
```

管理故障切换

本节介绍如何在启用故障切换后管理故障切换设备，包括如何更改故障切换设置和如何强制从一台设备故障切换到另一台设备。

- 强制故障切换，第 7-39 页
- 禁用故障切换，第 7-39 页
- 恢复故障设备，第 7-40 页
- 重新同步配置，第 7-40 页
- 测试故障切换功能，第 7-41 页
- 远程命令执行，第 7-41 页

强制故障切换

要强制要求备用设备成为主用设备，请执行以下程序。

准备工作

在多情景模式下，请在系统执行空间中执行本程序。

操作步骤

步骤 1　在*备用*设备上输入时，可以强制故障切换。备用设备将成为主用设备。

如果指定 **group** *group_id*，则在指定主用/主用故障切换组的*备用*设备上输入此命令时，将强制进行故障切换。备用设备将成为故障切换组的主用设备。

- 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 group 1
  ```

步骤 2　在*主用*设备上输入时，可以强制故障切换。主用设备将成为备用设备。

如果指定 **group** *group_id*，在指定故障切换组的*主用*设备上输入时，此命令将强制进行故障切换。主用设备将成为故障切换组的备用设备。

- 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 group 1
  ```

禁用故障切换

在一台或两台设备上禁用故障切换，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。对于主用/主用故障切换对，故障切换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。

禁用故障切换时，请参阅以下特征：

- 备用设备/情景保持备用模式，以便两台设备都不开始传输流量 （这称为假备用状态）。
- 备用设备/情景继续使用其备用 IP 地址，即使它不再连接到主用设备/情景也是如此。
- 备用设备/情景继续侦听故障切换链路上的连接。如果在主用设备/情景上重新启用故障切换，则备用设备/情景会在重新同步其他配置后恢复普通备用状态。
- 要真正禁用故障切换，请将禁用故障切换配置保存到启动配置，然后重新加载。

准备工作

在多情景模式下，请在系统执行空间中执行本程序。

操作步骤

步骤 1　禁用故障切换：

```
no failover
```

步骤 2　要完全禁用故障切换，请保存配置并重新加载：

```
write memory
reload
```

步骤 3

恢复故障设备

要将故障设备恢复到无故障状态，请执行以下程序。

准备工作

在多情景模式下，请在系统执行空间中执行本程序。

操作步骤

步骤 1　将故障设备恢复为无故障状态：

- 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 group 1
  ```

将故障设备恢复到无故障状态，不会自动使其成为主用设备；恢复后的设备将保持在备用状态，直到故障切换 （强制或自然）使其变为主用状态。例外情况是，配置了故障切换抢占的故障切换组 （仅主用/主用模式）。如果故障切换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，则该故障切换组将变为主用状态。

如果指定 **group** *group_id*，此命令会将发生故障的主用/主用故障切换组恢复到无故障状态。

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切换命令除外），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，该命令只会复制情景配置。

复制命令会存储在运行配置中。

测试故障切换功能

要测试故障切换功能，请执行以下程序。

操作步骤

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，从而强制进行故障切换：

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** 命令检查故障切换状态。

步骤 5　完成后，您可以在新的主用设备上输入以下命令，从而将设备恢复到主用状态：

主用/备用模式：

```
ciscoasa(config)# no failover active
```

主用/主用模式：

```
ciscoasa(config)# failover active group group_id
```

备注　当 ASA 接口发生故障时，对于故障切换而言，仍然会将其视为设备问题。如果 ASA 检测到接口发生故障，将立即进行故障切换，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 （尽管其未收到对等体的呼叫数据包）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，以阻止对等体收到彼此的呼叫数据包。

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切换对等体。

- 发送命令，第 7-42 页
- 更改命令模式，第 7-42 页
- 安全注意事项，第 7-43 页
- 远程命令执行的限制，第 7-43 页

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，因此可以使用 **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，则可以使用 **failover exec active** 命令向主用设备发送配置更改。这些更改随后会复制到备用设备。请勿使用 **failover exec** 命令向备用设备或情景发送配置命令；这些配置更改不会复制到主用设备，而且两个配置将不再同步。

configuration、exec 和 **show** 命令的输出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。

您必须拥有足够在本地设备上执行命令的权限才能在对等设备上执行命令。

操作步骤

步骤 1　如果您处于多情景模式下，请使用 **changeto context** *name* 命令更改要配置的情景。您无法使用 **failover exec** 命令更改故障切换对等体上的情景。

步骤 2　使用以下命令，将命令发送到指定的故障切换设备：

```
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也是如此。使用 **mate** 关键字，以在故障切换对等体上执行命令。

导致命令模式更改的命令不会更改当前会话的提示。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，请参阅更改命令模式，第 7-42 页。

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下启动。您可以使用 **failover exec** 命令发送适当的命令（如 **interface** 命令）来更改该命令模式。当使用 **failover exec** 更改模式时，会话提示不会更改。

例如，如果您登录到故障切换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下输入。

以下示例显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)#
```

更改设备当前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下执行。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** 命令可显示指定设备上的命令模式，通过 **failover exec** 命令发送的命令在该设备中执行。**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
Active unit Failover EXEC is at interface sub-command mode

ciscoasa(config)# sh failover exec standby
Standby unit Failover EXEC is at config mode

ciscoasa(config)# sh failover exec mate
Active unit Failover EXEC is at interface sub-command mode
```

安全注意事项

failover exec 命令使用故障切换链路向对等设备发送命令以及接收对等设备命令执行的输出。您应在故障切换链路上启用加密，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：

- 如果使用零停机时间升级程序升级一台设备，但不升级另一台设备，则两台设备都必须运行支持 **failover exec** 命令的软件，该命令才能工作。
- 命令补全和情景帮助不适用于 *cmd_string* 参数中的命令。
- 在多情景模式下，只能向对等设备上的对等情景发送命令。要将命令发送到不同情景，必须在所登录的设备上切换到该情景。
- 不能通过 **failover exec** 命令使用以下命令：
  - **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 exec** 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切换对等体上的全局配置模式。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。但是，使用 **failover exec** 为对等体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。
- 需要用户输入或确认的命令必须使用 **/nonconfirm** 选项。

监控故障切换

- 故障切换消息，第 7-44 页
- 监控故障切换状态，第 7-44 页

故障切换消息

发生故障切换时，两台 ASA 都会发送系统消息。

- 故障切换系统日志消息，第 7-44 页
- 故障切换调试消息，第 7-44 页
- SNMP 故障切换陷阱，第 7-44 页

故障切换系统日志消息

ASA 发出一系列与优先级为 2 的故障切换有关的系统日志消息，指示一个严重情况。要查看这些信息，请参阅 《系统日志消息指南》。要启用日志记录，请参阅第 36 章 “日志记录”。

备注　在故障切换过程中，故障切换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。

故障切换调试消息

要查看调试消息，请输入 **debug fover** 命令。有关详情，请参阅命令参考。

备注　由于调试输出在 CPU 进程中分配的高优先级，它可能会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 故障切换陷阱

要接收故障切换的 SNMP 系统日志陷阱，请将 SNMP 代理配置为发送 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。有关详情，请参见第 37 章 “SNMP”。

监控故障切换状态

要监控故障切换状态，请输入以下其中一个命令：

- **show failover**

  显示有关设备的故障切换状态的信息。

- **show failover group**

  显示有关故障切换组的故障切换状态的信息。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**

  显示有关受监控接口的信息。

- **show running-config failover**

  显示运行配置中的故障切换命令。

故障切换历史记录

表 7-4　　故障切换历史记录

功能名称	版本	功能信息
主用/备用故障切换	7.0(1)	引入了此功能。
主用/主用故障切换	7.0(1)	引入了此功能。
故障切换密钥支持使用十六进制值	7.0(4)	现在可以指定十六进制值用于故障切换链路加密。 修改了以下命令：**failover key hex**。
支持故障切换密钥的主密码	8.3(1)	故障切换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。 **备注**　**failover key** 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。 修改了以下命令：**failover key [0 | 8]**。
添加了故障切换的 IPv6 支持。	8.2(2)	修改了以下命令：**failover interface ip**、**show failover**、**ipv6 address**、**show monitor-interface**。
支持 IPsec LAN 到 LAN 隧道加密故障切换和状态链路通信。	9.1(2)	现在可以将 IPsec LAN 到 LAN 隧道用于故障切换和状态链路加密，而不是对故障切换密钥使用专有加密（**failover key** 命令）。 **备注**　故障切换 LAN 到 LAN 隧道不计入 IPsec（其他 VPN）许可证。 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切换，则可以禁用模块监控。 修改了以下命令：**monitor-interface service-module**
锁定故障切换对中的备用设备或备用情景上的配置更改	9.3(2)	现在可以锁定备用设备（主用/备用故障切换）或备用情景（主用/主用故障切换）上的配置更改，因此，除了正常的配置同步之外，将无法在备用设备上做出更改。 引入了以下命令：**failover standby config-lock**



ASA 集群

通过集群，您可以将多台 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。

备注 使用集群时，有些功能不受支持。请参阅集群不支持的功能，第 8-23 页。

- 关于 ASA 集群，第 8-1 页
- ASA 集群的许可，第 8-29 页
- ASA 集群的必备条件，第 8-29 页
- ASA 集群准则，第 8-30 页
- ASA 集群的默认设置，第 8-33 页
- 配置 ASA 集群，第 8-33 页
- 管理 ASA 集群成员，第 8-49 页
- 监控 ASA 集群，第 8-53 页
- ASA 集群示例，第 8-58 页
- ASA 集群历史记录，第 8-69 页

关于 ASA 集群

本节介绍集群架构及其工作原理。

- ASA 集群如何融入网络中，第 8-2 页
- 性能比例因子，第 8-2 页
- 集群成员，第 8-2 页
- 集群接口，第 8-4 页
- 集群控制链路，第 8-5 页
- ASA 集群中的高可用性，第 8-8 页
- 配置复制，第 8-9 页
- ASA 集群管理，第 8-10 页
- 负载均衡方法，第 8-11 页
- 站点间集群，第 8-16 页

- ASA 集群如何管理连接，第 8-20 页
- ASA 功能和集群，第 8-22 页

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。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

- ASA 集群的许可，第 8-29 页
- 集群控制链路，第 8-5 页
- ASA 集群管理，第 8-10 页
- 跨网络 EtherChannel （推荐），第 8-11 页
- 基于策略的路由 （仅适用于路由防火墙模式），第 8-15 页
- 等价多路径路由 （仅适用于路由防火墙模式），第 8-16 页

性能比例因子

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。

- 引导程序配置，第 8-3 页
- 主设备和从属设备角色，第 8-3 页
- 主设备选举，第 8-3 页

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*从属*设备加入集群。

主设备和从属设备角色

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属设备。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。

您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，配置将被复制到从属设备。如果是接口等物理资产，主设备的配置将被镜像到所有从属设备。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，则从属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

- 集群的集中功能，第 8-23 页

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. 当为设备启用集群（或当设备首次启动时已启用集群）时，设备会每 3 秒广播一个选举请求。
2. 具有较高优先级的任何其他设备都会响应选举请求；优先级设置在 1 和 100 之间，其中 1 为最高优先级。
3. 如果某设备在 45 秒后未收到另一个具有较高优先级的设备的响应，则该设备会成为主设备。

   注意　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，则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。

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

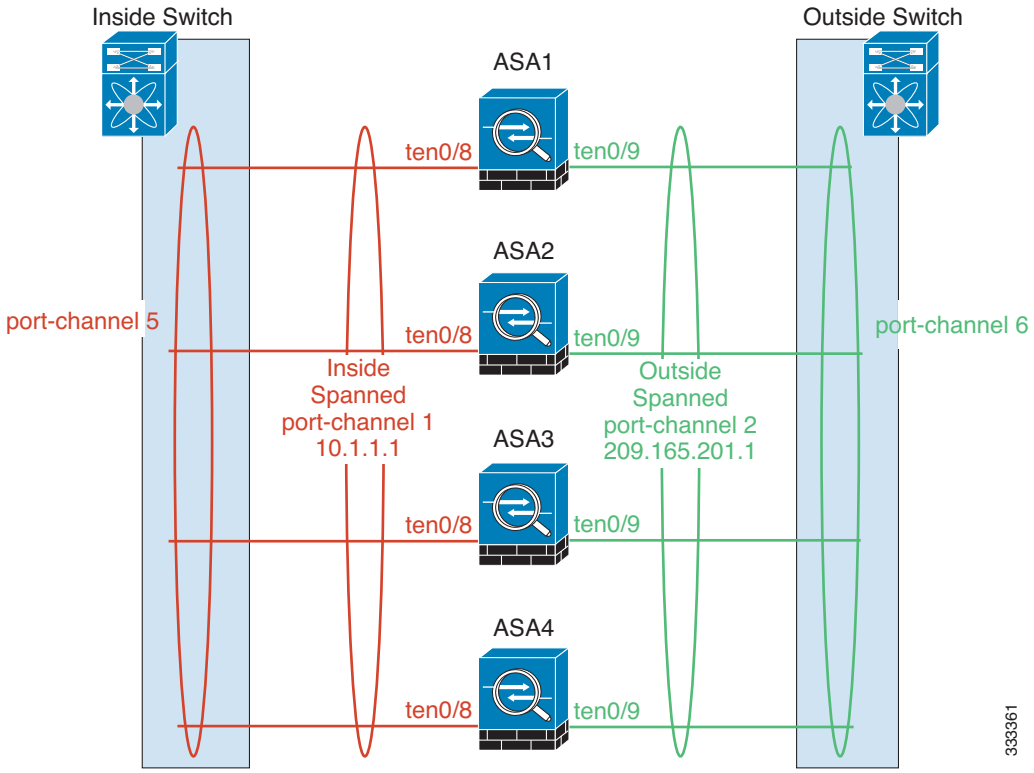
- 集群的集中功能，第 8-23 页

集群接口

您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）

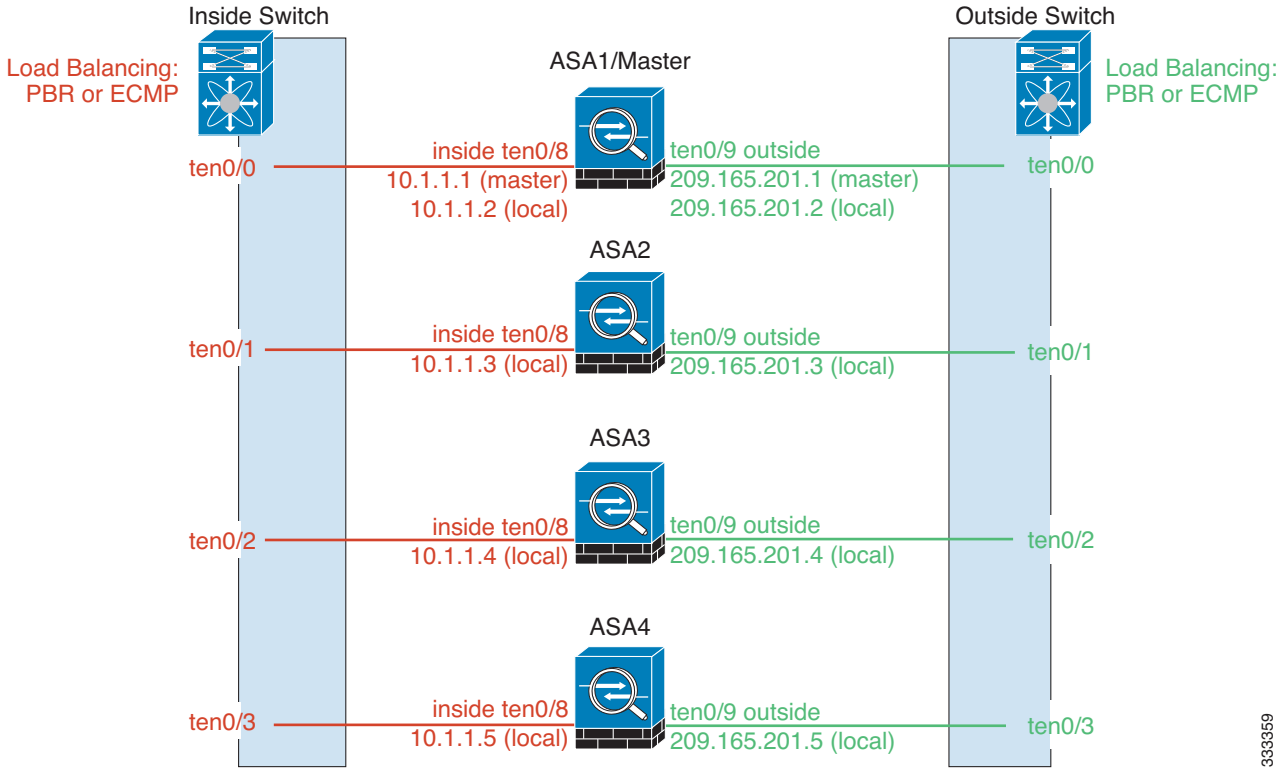
您可以将每台设备的一个或多个接口分组为跨集群中所有设备的 EtherChannel。EtherChannel 汇聚通道中所有可用活动接口上的流量。在路由模式和透明防火墙模式下都可以配置跨网络 EtherChannel。在路由模式下， EtherChannel 被配置为只有一个 IP 地址的路由接口。在透明模式下， IP 地址被分配到网桥组而非接口。负载均衡属于 EtherChannel 固有的基本操作。



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。

备注　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

- 负载均衡方法，第 8-11 页

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。

- 集群控制链路流量概述，第 8-5 页
- 集群控制链路接口和网络，第 8-6 页
- 调整集群控制链路的吞吐量大小，第 8-6 页
- 集群控制链路冗余，第 8-7 页
- 集群控制链路可靠性，第 8-7 页
- 集群控制链路故障，第 8-7 页

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

- 集群成员，第 8-2 页
- 配置复制，第 8-9 页
- 设备运行状况监控，第 8-8 页
- 数据路径连接状态复制，第 8-9 页
- 在集群中再均衡新的 TCP 连接，第 8-22 页

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，您不能将模块接口用于集群控制链路；但是，可以使用 ASA 5585-X 网络模块上的接口。

您可以使用 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，我们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

- 集群控制链路冗余，第 8-7 页
- 调整集群控制链路的吞吐量大小，第 8-6 页

调整集群控制链路的吞吐量大小

您应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，您可以将 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效率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。

备注 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。

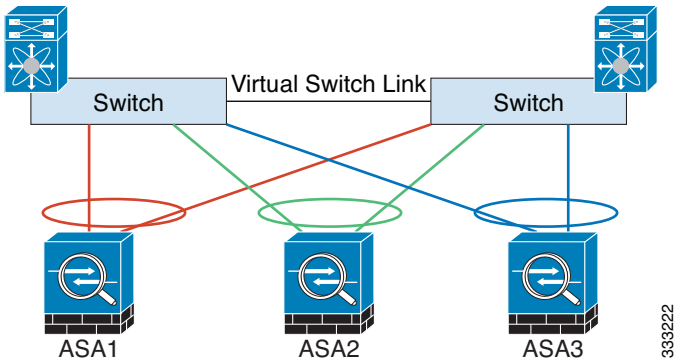
相关主题

- 站点间集群，第 8-16 页

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，则您可以将同一个 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。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，没有数据包无序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。

备注 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

重新加入集群，第 8-9 页

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。

- 设备运行状况监控，第 8-8 页
- 接口监控，第 8-8 页
- 设备或接口故障，第 8-8 页
- 数据路径连接状态复制，第 8-9 页

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 消息来监控每台从属设备。每台从属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。

当您启用运行状况监控时，默认情况下会监控所有物理接口 （包括主要的 EtherChannel 和冗余接口类型）；您可以选择按接口禁用监控。

设备或接口故障

启用运行状况监控时，如果某台设备或其受监控的接口发生故障，将从集群中删除该设备。如果特定逻辑接口的所有物理接口在特定设备上发生故障，但在其他设备上的同一逻辑接口下仍有活动端口，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。

备注　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

重新加入集群，第 8-9 页

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，您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，您必须在控制台端口上通过输入 **cluster** *name*，然后输入 **enable** 来手动启用集群。
- 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

- 配置主设备引导程序设置，第 8-42 页

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

交通	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) 和身份防火墙。
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 集群的优势之一是易于管理。本节介绍如何管理集群。

- 管理网络，第 8-10 页
- 管理接口，第 8-10 页
- 主设备管理与从属设备管理，第 8-10 页
- RSA 密钥复制，第 8-11 页
- ASDM 连接证书 IP 地址不匹配，第 8-11 页

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。

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。要管理单个成员，您可以连接到本地 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，您只能配置一个 IP 地址，该 IP 地址始终属于主设备。您无法使用 EtherChannel 接口直接连接到从属设备；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，您可以使用设备本地 EtherChannel 进行管理。

主设备管理与从属设备管理

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属设备复制到主设备。

如果需要，您可以直接监控从属设备。虽然可以从主设备执行文件管理，但您也可以在从属设备上执行 （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属设备。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，您无需更新缓存的 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 地址使用自签名证书。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。但是，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 18 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。

- 跨网络 EtherChannel （推荐），第 8-11 页
- 基于策略的路由 （仅适用于路由防火墙模式），第 8-15 页
- 等价多路径路由 （仅适用于路由防火墙模式），第 8-16 页

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 汇聚通道中所有可用活动接口上的流量。

- 跨网络 EtherChannel 的优势，第 8-11 页
- 最大吞吐量准则，第 8-12 页
- 负载均衡，第 8-12 页
- EtherChannel 冗余，第 8-12 页
- 连接到 VSS 或 vPC，第 8-12 页

跨网络 EtherChannel 的优势

我们优先推荐 EtherChannel 负载均衡方法，因其具有以下优势：

- 发现故障的速度更快。
- 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

EtherChannel，第 10-2 页

最大吞吐量准则

要实现最大吞吐量，我们建议采取以下措施：

- 使用 “对称”的负载均衡散列算法，亦即来自两个方向的数据包具有相同的散列值，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散列算法。
- 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散列算法都相同。

负载均衡

EtherChannel 链路使用专有散列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。

备注 在 ASA 上，请勿更改默认的负载均衡算法。在交换机上，我们建议使用以下其中一种算法：**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。如果您配置了 NAT，则转发和返回数据包具有不同的 IP 地址和/或端口。返回流量将根据散列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

- 自定义 EtherChannel，第 10-9 页
- 负载均衡，第 10-4 页
- NAT 和集群，第 8-27 页

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

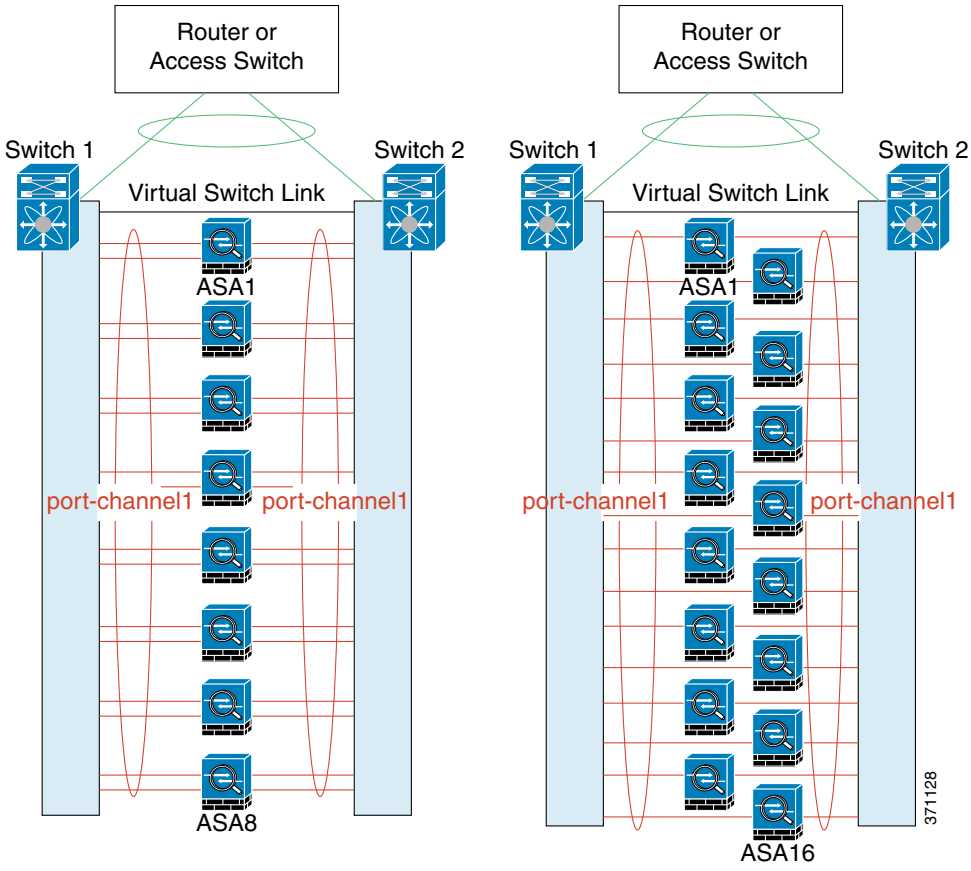
您可以在跨网络 EtherChannel 中包含每台 ASA 的多个接口。每台 ASA 有多个接口，对于连接到 VSS 或 vPC 中两台交换机的情况特别有用。

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）。

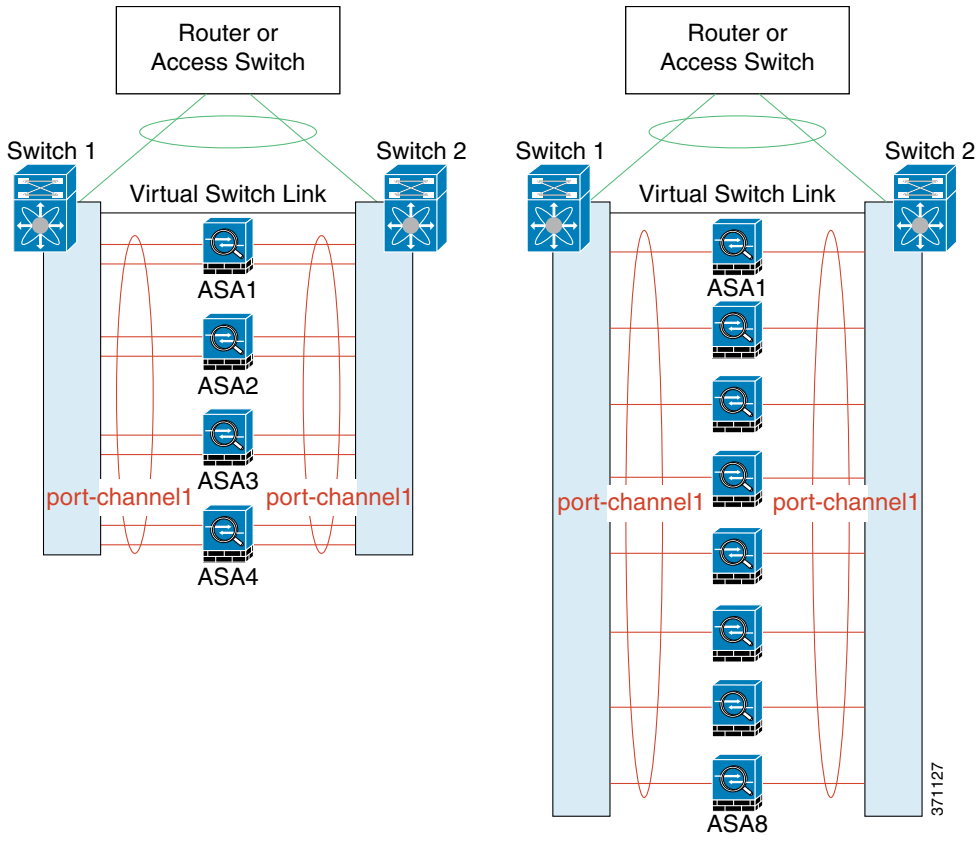
对于支持 EtherChannel 中有 8 条活动链路的交换机，在连接到 VSS/vPC 中的两台交换机时，最多可在跨网络 EtherChannel 中配置 16 条活动链路。

如果您要在跨网络 EtherChannel 中使用 8 条以上的活动链路，则无法同时使用备用链路；要支持 9 至 32 条活动链路，需要您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。

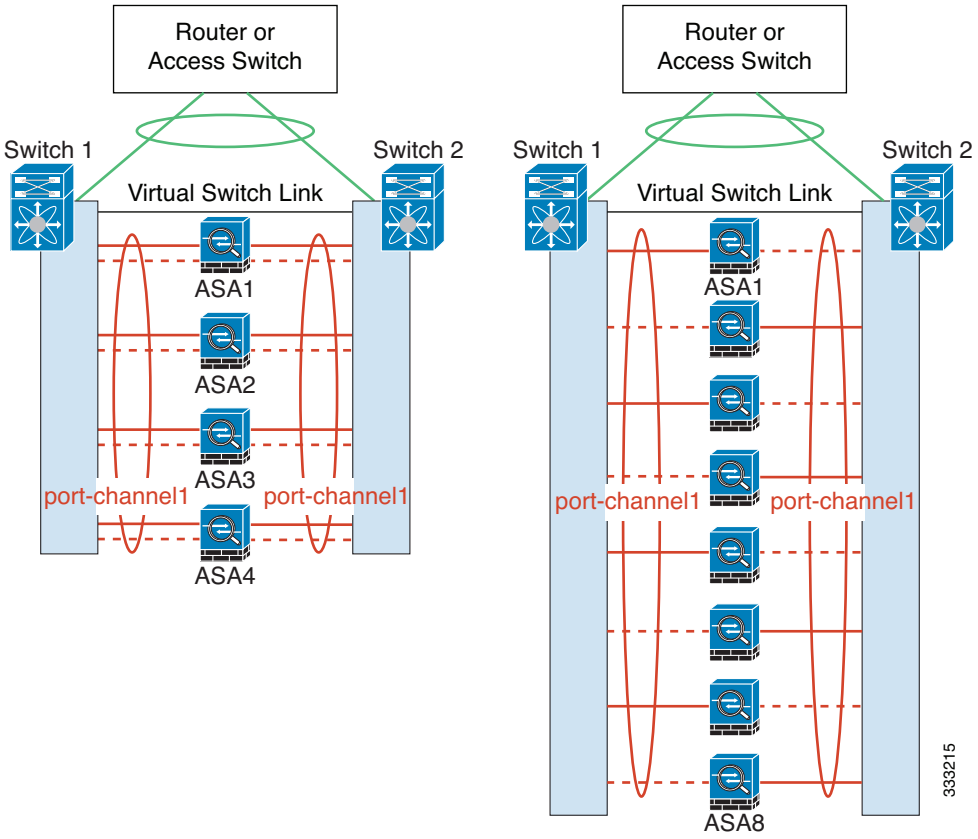
下图所示为 8-ASA 集群和 16-ASA 集群中有 32 条活动链路的跨网络 EtherChannel。



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。活动链路显示为实线，非活动链路显示为虚线。 cLACP 负载均衡可以自动选择 8 条最佳链路作为 EtherChannel 中的活动链路。如图所示， cLACP 可以帮助实现链路级负载均衡。



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，我们建议使用此方法。与跨网络 EtherChannel 相比，此方法也可以提供额外调整选项。

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。要实现最佳性能，我们建议您通过配置 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 的可访问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

备注　如果您使用此负载均衡方法，则可以使用设备本地 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，我们建议使用此方法。与跨网络 EtherChannel 相比，此方法也可以提供额外调整选项。

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/或源和目标端口的散列值将数据包发送到下一跃点。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。

备注　如果您使用此负载均衡方法，则可以使用设备本地 EtherChannel 作为独立接口。

站点间集群

对于站点间安装，您只要遵循以下准则就可以充分发挥 ASA 集群的作用。

- 站点间集群准则，第 8-16 页
- 确定数据中心互联的规格，第 8-17 页
- 站点间集群示例，第 8-18 页

站点间集群准则

请参阅有关站点间集群的以下准则：

- 在以下接口和防火墙模式下，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**	N/A
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，没有数据包无序或丢弃数据包的情况；例如，您应使用专用链路。
- 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，如果集群布置于内部和外部路由器对之间 （AKA 南北插入），您必须确保两个内部路由器共享一个 MAC 地址，两个外部路由器共享一个 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。

- 对于透明模式，如果集群布置于每个站点上的数据网络和网关路由器之间，用作内部网络之间的防火墙 （AKA 东西插入），则每个网关路由器都应使用 HSRP 等第一跳冗余协议 (FHRP) 在每个站点提供相同的虚拟 IP 和 MAC 地址目标。数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术扩展到多个站点。您需要创建过滤器，阻止发往本地网关路由器的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的网关路由器，则您需要删除所有过滤器，使流量能够成功到达另一站点的网关。

相关主题

- 在集群中再均衡新的 TCP 连接，第 8-22 页
- 连接角色，第 8-21 页

确定数据中心互联的规格

您应在数据中心互联 (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：

$$\frac{\text{每个站点的集群成员数量}}{2} \times \text{每个成员的集群控制链路规格}$$

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 4 个站点的 2 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 6 个站点的 3 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)）。

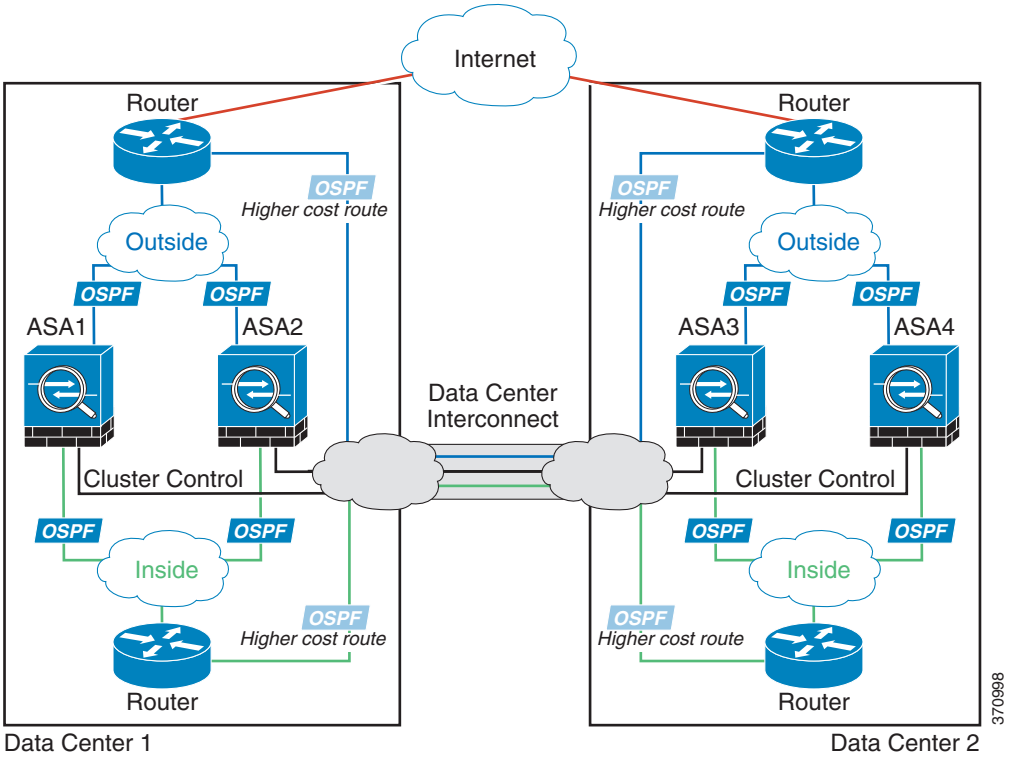
站点间集群示例

以下示例显示支持的集群部署。

- 独立接口路由模式南北站点间集群示例，第 8-18 页
- 跨网络 EtherChannel 透明模式南北站点间集群示例，第 8-19 页
- 跨网络 EtherChannel 透明模式东西站点间集群示例，第 8-20 页

独立接口路由模式南北站点间集群示例

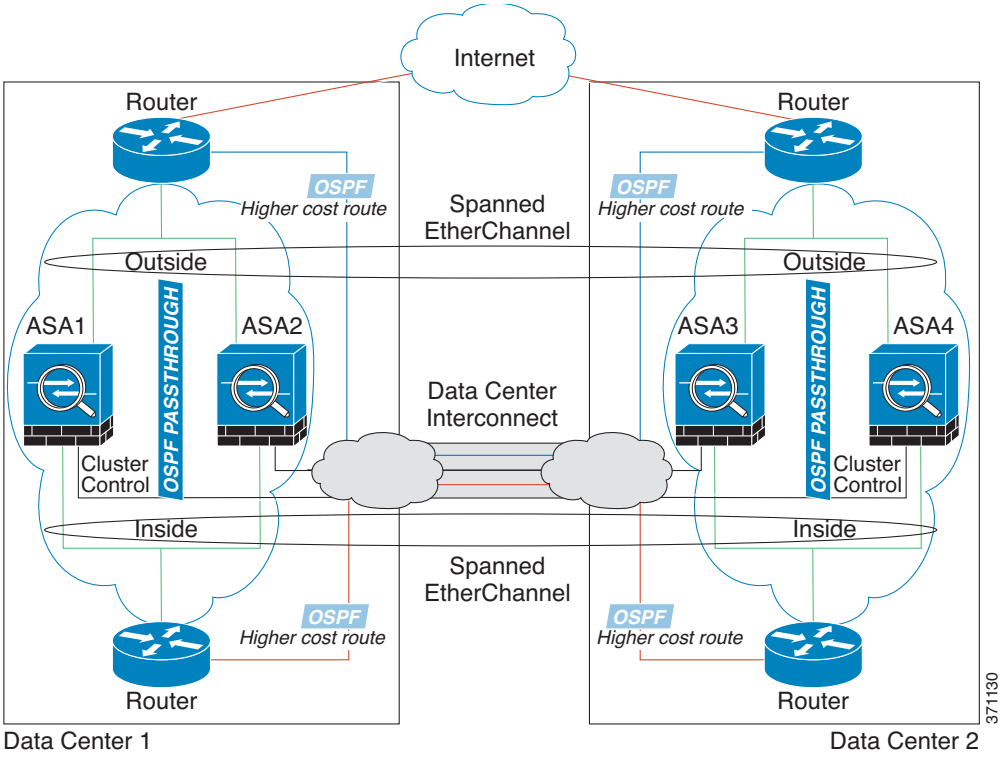
以下示例显示了分别位于 2 个布置于内部和外部路由器（南北插入）之间的数据中心的 2 个 ASA 集群成员。集群成员由集群控制链路通过 DCI 连接。位于每个数据中心的内部和外部路由器使用 OSPF 和 PBR 或 ECMP 在集群成员之间对流量执行负载均衡。通过指定 DCI 中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有 ASA 集群成员都中断连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的 ASA 集群成员。



跨网络 EtherChannel 透明模式南北站点间集群示例

以下示例显示了分别位于 2 个布置于内部和外部路由器（南北插入）之间的数据中心的 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。每个 ASA EtherChannel 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均使用 OSPF（可通过透明的 ASA）。不同于 MAC，所有路由器上的路由器 IP 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。



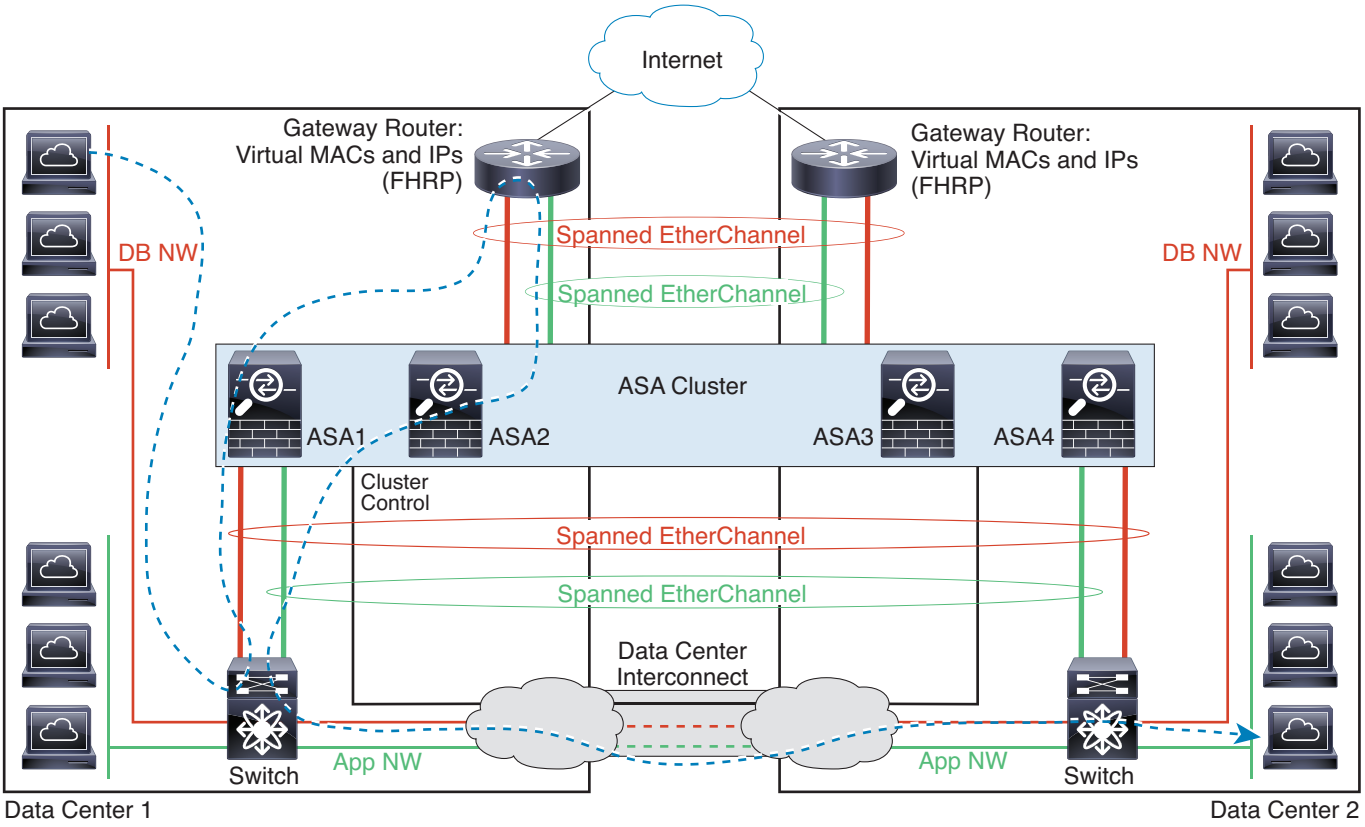
位于每个站点的交换机的实施可包括：

- 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，您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 视作站点本地的 EtherChannel。

跨网络 EtherChannel 透明模式东西站点间集群示例

以下示例显示了分别位于 2 个置于每个站点上的网关路由器和两个内部网络之间的数据中心的 2 个 ASA 集群成员，以及应用网络和数据库网络（东西插入）。集群成员由集群控制链路通过 DCI 连接。每个站点上的集群成员使用面向内部与外部应用网络和数据库网络的跨网络 EtherChannel 连接到本地交换机。每个 ASA EtherChannel 跨越集群中的所有 ASA。

每个站点上的网关路由器使用 FHRP（例如 HSRP）在每个站点上提供相同的目标虚拟 MAC 和 IP 地址。数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术在站点之间扩展。您必须添加过滤器，阻止发往网关路由器的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的网关路由器，则您必须删除过滤器，使流量能够发送到另一站点的网关路由器。



有关 vPC/VSS 选项的详细信息，请参阅跨网络 EtherChannel 透明模式南北站点间集群示例，第 8-19 页。

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。

- 连接角色，第 8-21 页
- 新连接所有权，第 8-21 页
- 数据流示例，第 8-22 页
- 在集群中再均衡新的 TCP 连接，第 8-22 页

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 端口的散列值选择导向者，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。一个连接了可以有多个转发者；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

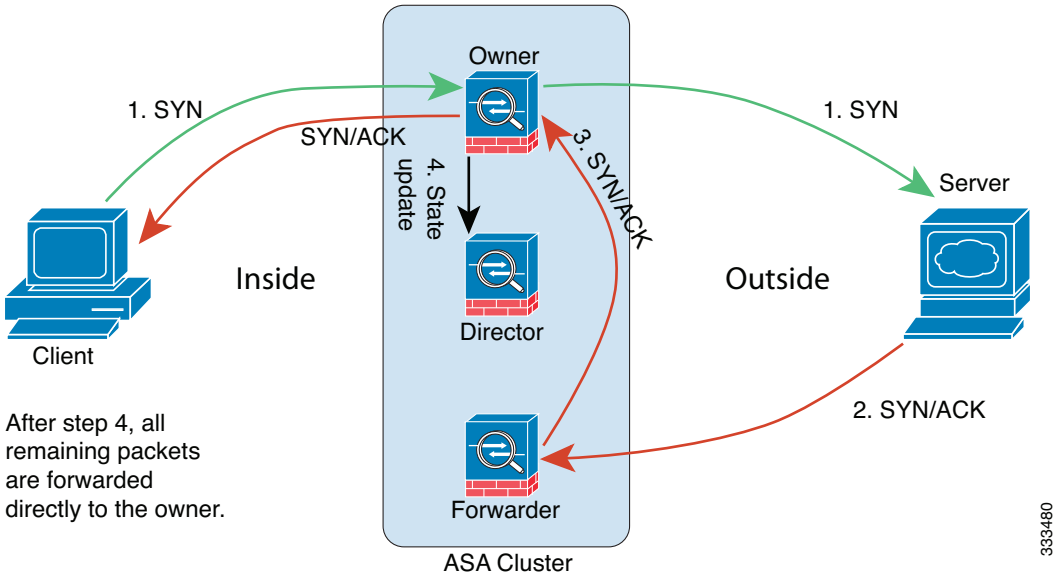
通过负载均衡将新连接定向到集群成员时，该连接的两个方向都由此设备所有。如果该连接有任何数据包到达其他设备，这些数据包都会通过集群控制链路被转发到所有者设备。为了获得最佳性能，对于要到达同一台设备的流量的两个方向以及要在设备之间均摊的流量，都需要执行适当的外部负载均衡。如果反向流量到达其他设备，会被重定向回原始设备。

相关主题

- 负载均衡方法，第 8-11 页

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，您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。现有流量将不会移至其他设备。

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。

- 集群不支持的功能，第 8-23 页
- 集群的集中功能，第 8-23 页

- 应用到单台设备的功能，第 8-24 页
- 动态路由和集群，第 8-25 页
- 组播路由和集群，第 8-26 页
- NAT 和集群，第 8-27 页
- 用于网络访问的 AAA 和集群，第 8-27 页
- 系统日志与 NetFlow 和集群，第 8-28 页
- SNMP 和集群，第 8-28 页
- VPN 和集群，第 8-28 页
- FTP 和集群，第 8-28 页
- 思科 TrustSec 和集群，第 8-28 页

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 穿透
  - MGCP
  - MMP
  - RTSP
  - SCCP （瘦客户端）
  - WAAS
  - WCCP
- 僵尸网络流量过滤器
- 自动更新服务器
- DHCP 客户端、服务器和代理。支持 DHCP 中继。
- 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。

备注　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 组播控制平面协议的处理 （数据平面转发分布于整个集群中）
- PIM 组播控制平面协议的处理 （数据平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。
- 筛选服务

相关主题

- 调整集群控制链路的吞吐量大小，第 8-6 页
- 在集群中再均衡新的 TCP 连接，第 8-22 页

应用到单台设备的功能

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。但是，该策略是在每台设备上独立执行。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 - 多情景模式下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。您负责使用 FireSIGHT 管理中心将集群中 ASA FirePOWER 模块上的策略保持一致。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。

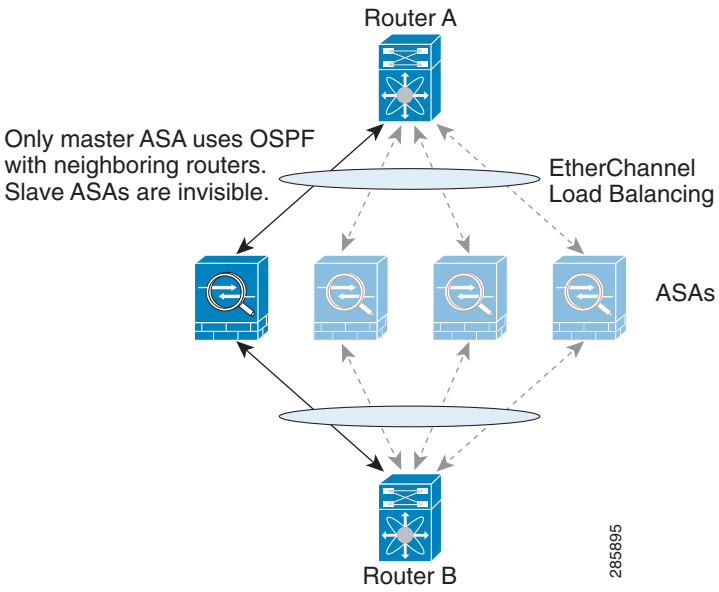
动态路由和集群

- 跨网络 EtherChannel 模式下的动态路由，第 8-25 页
- 独立接口模式下的动态路由，第 8-26 页

跨网络 EtherChannel 模式下的动态路由

在跨网络 EtherChannel 模式下，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属设备。如果路由数据包到达从属设备，会被重定向到主设备。

图 8-1　　跨网络 EtherChannel 模式下的动态路由



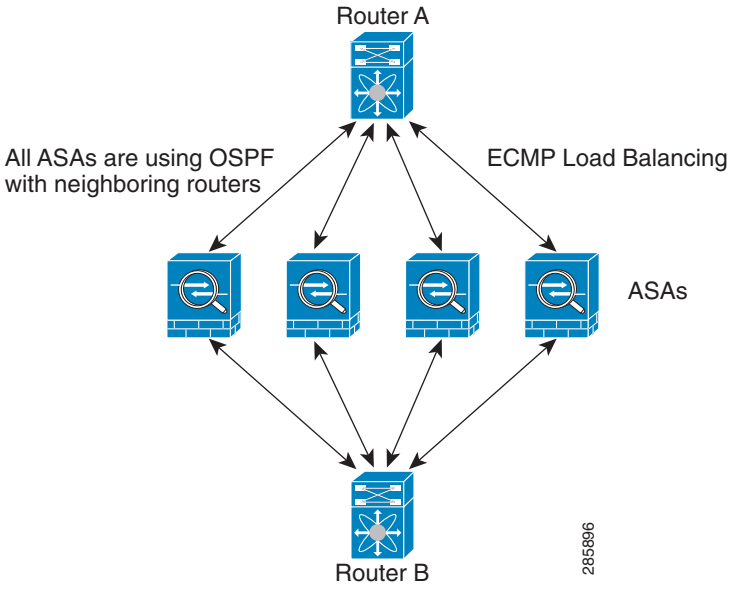
当从属设备成员从主设备获知路由后，每台设备将独立作出转发决定。

OSPF LSA 数据库不会从主设备同步到从属设备。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。请参阅 OSPF 无中断转发功能，解决中断问题。

独立接口模式下的动态路由

在独立接口模式下，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　　独立接口模式下的动态路由



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。

- 跨网络 EtherChannel 模式下的组播路由，第 8-26 页
- 独立接口模式下的组播路由，第 8-26 页

跨网络 EtherChannel 模式下的组播路由

在跨网络 EtherChannel 模式下，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，每台从属设备都可以转发组播数据包。

独立接口模式下的组播路由

在独立接口模式下，设备并不单独处理组播。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，请考虑以下准则：

- 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 回复。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属设备。当从属设备收到需要动态 NAT 的连接而转换项不在表中时，将向主设备请求该转换项。从属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，它允许每台从属设备成为 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 或瘦客户端等需要多会话 PAT 的流量，您可以禁用每会话 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

SIP 检测和集群

控制流可以在任何设备上创建 （由于负载均衡），但其子数据流必须驻留在同一设备上。

不支持 TLS 代理配置。

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属设备。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

- 在非 EMBLEM 格式系统日志消息中包含设备 ID，第 36-15 页

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。

您应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。

备注　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 连接都将断开， VPN 用户将遇到服务中断。选举出新的主设备后，您必须重新建立 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，您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 数据通道和控制通道流量由不同的集群成员所有，则数据通道所有者会将空闲超时更新定期发送到控制通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，则控制通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签 (SGT) 信息。然后，主设备将向从属设备提供 SGT，从属设备可根据安全策略为 SGT 作出匹配项决定。

ASA 集群的许可

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。

此准则也存在例外。有关集群的精确许可要求，请参阅下表。

型号	许可证要求
ASA 5585-X	集群许可证，最多可支持 16 台设备。 **备注**　每台设备都必须有相同的加密许可证；每台设备都必须有相同的 10 GE I/O/增强型安全许可证 （带有 SSP-10 和 SSP-20 的 ASA 5585-X）。
ASA 5512-X	增强型安全许可证，支持 2 台设备。 **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。 **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 集群的必备条件

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下，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下，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。

交换机必备条件

- 请务必完成交换机配置后再在 ASA 上配置集群。
- 有关支持的交换机列表，请参阅思科 ASA 兼容性。

ASA 必备条件

- 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。
  - 从属设备加入集群后，其管理接口配置将替换为从主设备复制的配置。
- 要在集群控制链路上使用巨型帧 （推荐），您必须在启用集群之前启用巨型帧保留。

其他必备条件

我们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

- ASA 集群准则，第 8-30 页
- 启用巨帧支持，第 9-7 页
- 引导程序配置，第 8-3 页

ASA 集群准则

情景模式

每台成员设备上的模式必须匹配。

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匹配。

故障切换

集群不支持故障切换。

IPv6

集群控制链路只有在使用 IPv4 时才受支持。

模式

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，我们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，您可以选择在连接到 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，您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，我们建议使用以下其中一种 EtherChannel 负载均衡算法：**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，则交换机上的 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。
- 您应在所有面向集群的 EtherChannel 接口上为思科 Nexus 交换机禁用 LACP Graceful Convergence 功能。

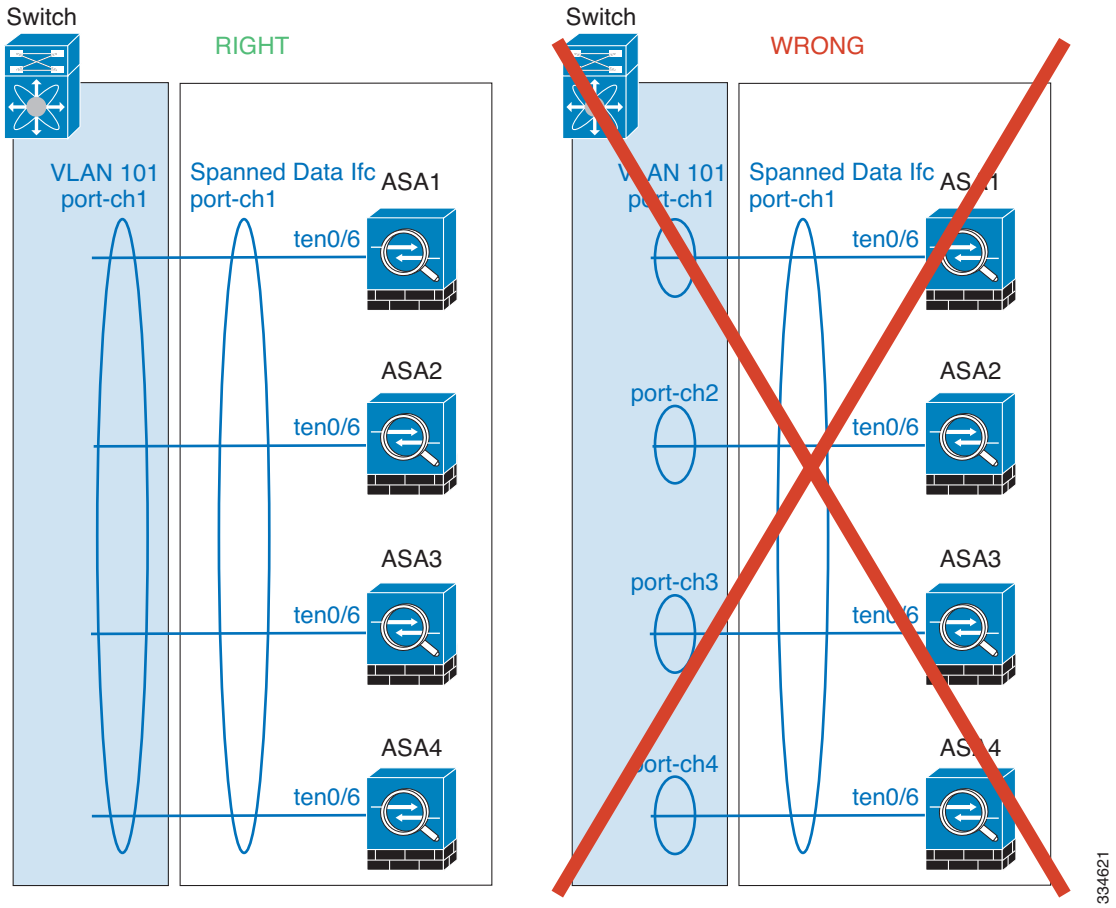
- 有些交换机不支持 LACP 动态端口优先级 （活动链路和备用链路）。您可以禁用动态端口优先级，使跨网络 EtherChannel 具有更高兼容性。
- 集群控制链路路径上的网络要素不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。
- 端口通道绑定中断时间不得超过配置的 keepalive 间隔。
- 在 Supervisor 2T EtherChannel 上，默认的散列值分配算法是自适应算法。为了避免在 VSS 设计中出现非对称流量，请将连接到 ASA 的端口通道上的散列算法更改为固定算法：

  ```
  router(config)# port-channel id hash-distribution fixed
  ```

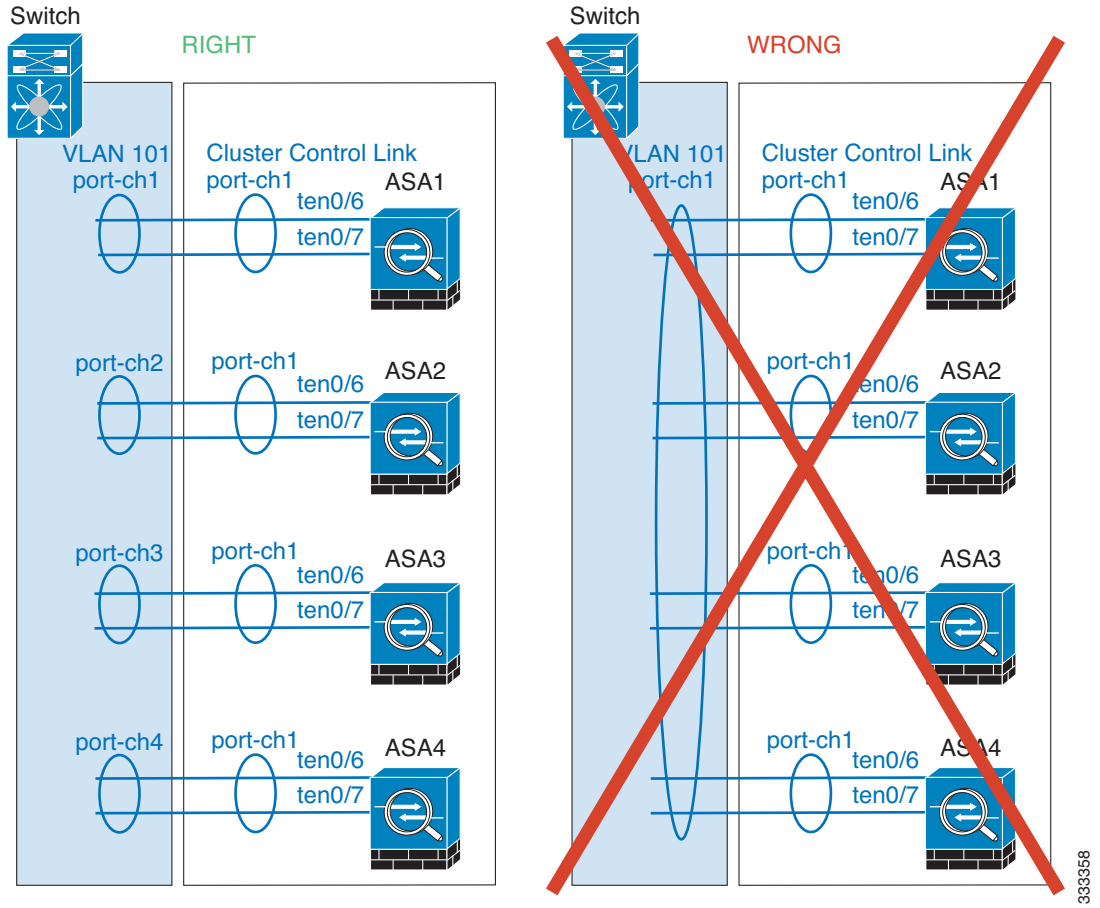
  请勿全局更改算法；您可能需要对 VSS 对等链路使用自适应算法。

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 配置 - 请务必为跨网络 EtherChannel 和设备本地 EtherChannel 适当地配置交换机。
  - 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。



其他准则

- 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），您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，您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，您需要重新建立 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，我们建议您限制 ICMP 错误信息。
- 我们不支持独立接口模式下的 VXLAN。仅跨网络 EtherChannel 模式支持 VXLAN。

相关主题

- 调整集群控制链路的吞吐量大小，第 8-6 页
- 引导程序配置，第 8-3 页

- 集群不支持的功能，第 8-23 页
- 配置 EtherChannel，第 10-8 页
- EtherChannel 接口和冗余接口准则，第 10-4 页

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。
- 默认情况下，集群运行状况检查功能处于启用状态，保持时间为 3 秒。默认情况下，在所有接口上启用接口运行状况监控。
- 默认情况下，连接再均衡处于禁用状态。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

备注　要启用或禁用集群，您必须使用控制台连接 （适用于 CLI）或 ASDM 连接。

要配置集群，请执行以下任务：

步骤 1　根据 ASA 集群的必备条件，第 8-29 页和 ASA 集群准则，第 8-30 页，在交换机和 ASA 上完成所有预配置。

步骤 2　使用电缆连接集群设备并配置上游和下游设备，第 8-33 页。

步骤 3　每台设备上配置主设备集群接口模式，第 8-35 页。您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　在主设备上配置接口，第 8-36 页。如果接口未准备好加入集群，则您无法启用集群。

步骤 5　配置主设备引导程序设置，第 8-42 页。

步骤 6　配置从属设备引导程序设置，第 8-47 页。

步骤 7　在主设备上配置安全策略。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。配置将被复制到从属设备。

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。

备注　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。

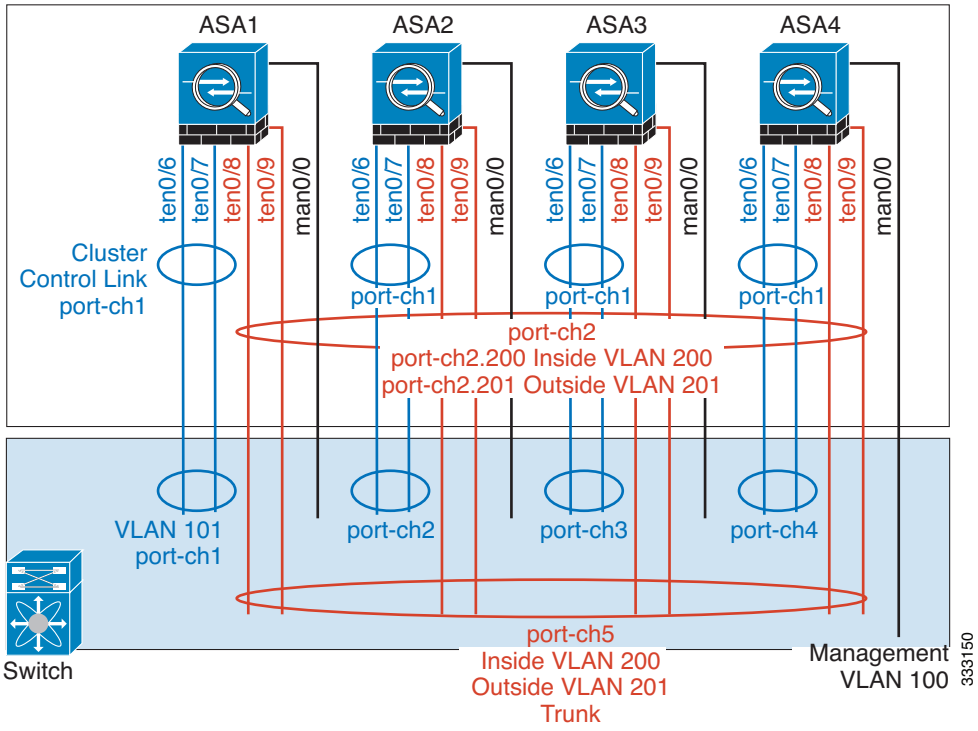
示例

备注　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 的优势。
- 1 个管理接口。

将一台交换机用于内部和外部网络。



目的	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。

目的	逐一连接 4 台 ASA 上的接口	连接到交换机端口
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。

每台设备上配置主设备集群接口模式

您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

- 您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 模式下亦如此。即使是在透明防火墙模式下，管理接口也可以是独立接口。
- 在跨网络 EtherChannel 模式下，如果将管理接口配置为独立接口，您将无法为管理接口启用动态路由。您必须使用静态路由。
- 在多情景模式下，您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，您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，您可以重新运行 **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。如果您不想清除配置，则可以键入 **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*，您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，您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。您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 模式下也可以是独立接口。

- 配置独立接口（管理接口的推荐配置），第 8-36 页
- 配置跨网络 EtherChannel，第 8-38 页

相关主题

- 集群接口，第 8-4 页

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 模式下，我们建议将管理接口配置为独立接口。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下。
- 对于多情景模式，请在每个情景下执行本程序。如果您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，则此 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；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。在透明模式下，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 是长度最多为 48 个字符的文本字符串，并且不区分大小写。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；您必须手动配置 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

- 管理接口，第 8-10 页
- 每台设备上配置主设备集群接口模式，第 8-35 页
- 负载均衡方法，第 8-11 页
- 配置 EtherChannel，第 10-8 页
- 启用巨帧支持，第 9-7 页
- 配置 VLAN 子接口和 802.1Q 中继，第 11-3 页
- 安全级别，第 13-1 页

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

- 您必须处于跨网络 EtherChannel 接口模式下。
- 对于多情景模式，请在系统执行空间中开始本程序。如果您尚未进入情景配置模式，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 - 我们建议不要在 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）。如果您需要使用这些设置，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，我们建议使用以下其中一种算法：**source-dest-ip** or **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，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。

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的交换机（1 还是 2）。此外，您还必须在步骤 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 1 至步骤 3，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。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实现均衡。在启用负载均衡之前，您必须在 **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方式，因为通道组中所有接口的这些参数都必须匹配。

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
```

本程序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 是长度最多为 48 个字符的文本字符串，并且不区分大小写。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，执行以下其中一项操作。

- 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。您不能将同一接口分配至多个网桥组。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。在多情景模式下，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，您只需为共享接口手动设置 MAC 地址即可。请注意，您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 以 000C.F142.4CDE 的形式输入。

如果您还要使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。

相关主题

- 每台设备上配置主设备集群接口模式，第 8-35 页
- 配置网桥组，第 13-8 页
- 配置主设备引导程序设置，第 8-42 页
- 配置 EtherChannel，第 10-8 页
- EtherChannel 接口和冗余接口准则，第 10-4 页
- 连接到 VSS 或 vPC，第 8-12 页
- 启用物理接口和配置以太网参数，第 9-6 页
- 配置 VLAN 子接口和 802.1Q 中继，第 11-3 页

- 配置安全情景，第 6-18 页
- 安全级别，第 13-1 页
- ASA 集群准则，第 8-30 页

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。您添加到集群的后续设备将成为从属设备。

准备工作

- 您必须使用控制台端口来启用或禁用集群。您不能使用 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程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。
- 我们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。

如果您有足够的接口，我们建议您将多个集群控制链路接口合并到 EtherChannel 中。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属设备；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，您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*

我们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。由于集群控制链路是单独、稳定的网络，因此无需 LACP 流量开销。**注意：**我们建议将*数据* EtherChannel 设置为 Active 模式。

c. 启用接口：

```
no shutdown
```

您只需要启用接口；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
```

将 MTU 设置为 64 到 65,535 字节之间的值。默认 MTU 为 1500 字节。

我们建议将 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程序。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。您只能为每台设备配置一个集群组。集群的所有成员必须使用同一名称。

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。每台设备必须拥有唯一的名称。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
```

不允许子接口和管理接口。

指定 IP 地址的 IPv4 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。此命令不会影响数据路径流量，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 0.8 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。如果设备在保持期内未接收到来自对等设备的任何 keepalive 消息，则对等设备被视为无响应或无法工作。如果将集群控制链路配置为 EtherChannel （推荐）且它连接到 VSS 或 vPC 对，则您可能需要启用 **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。如果您将 ASA 保持时间超时设置为一个较低值 （如 0.8 秒），则可将 ASA 从集群中匿名删除， ASA 会将 keepalive 消息发送到这些 EtherChannel 接口之一。当您启用 **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。如果特定逻辑接口的所有物理接口在特定设备上发生故障，但在其他设备上的同一逻辑接口下仍有活动端口，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。

默认情况下，为所有接口启用运行状况检查。您可以使用此命令的 **no** 形式将其禁用。要按接口禁用监控，请参见 **no health-check monitor-interface** 命令。

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、添加额外的交换机形成 VSS 或 vPC），您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，您可以重新启用运行状况检查功能。

步骤 9　（可选）在接口上禁用接口运行状况检查：

no health-check monitor-interface *interface_id*

示例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management0/0
```

您可能想禁用不重要的接口（例如管理接口）的运行状况检查。您可以指定任何端口通道 ID、冗余 ID 或单一物理接口 ID。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

步骤 10　（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
```

默认情况下，此命令处于禁用状态。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 11　（可选）启用从属设备到主设备的控制台复制：

console-replicate

默认情况下，此功能处于禁用状态。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，从属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 12　（可选）禁用 LACP 中的动态端口优先级：

clacp static-port-priority

某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 13　（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。ASA集群中的在 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属设备；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 输入为 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，即最高优先级。该优先级需要高于交换机上的优先级。

此命令并非引导程序配置的一部分，而是从主设备复制到从属设备上的。但是，在启用集群后无法更改此值。

步骤 14　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。系统会提示您删除不兼容命令。如果您选择 **No**，则不会启用集群。使用 **noconfirm** 关键字可绕过确认步骤并自动删除不兼容命令。

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。

要禁用集群，请输入 **no enable** 命令。

注意　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，然后为名为 “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

- 启用巨帧支持，第 9-7 页
- 在主设备上配置接口，第 8-36 页
- 调整集群控制链路的吞吐量大小，第 8-6 页

- 主设备选举，第 8-3 页
- 接口监控，第 8-8 页
- 退出集群，第 8-50 页

配置从属设备引导程序设置

执行以下程序配置从属设备。

准备工作

- 您必须使用控制台端口来启用或禁用集群。您不能使用 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程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。
- 我们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），可以作为从属设备加入集群 （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。

每台设备必须拥有唯一的名称。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 IP 地址的 IPv4 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属设备不可能在任何当前选举中成为主设备。从属设备的配置将被同步自主设备的配置覆盖。

要禁用集群，请输入 **no enable** 命令。

注意　如果禁用集群，所有数据接口将关闭，只有管理接口会处于活动状态。

示例

以下示例包括对从属设备 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

- 启用巨帧支持，第 9-7 页
- 主设备选举，第 8-3 页
- 退出集群，第 8-50 页

管理 ASA 集群成员

部署集群后，您可以更改配置和管理集群成员。

- 成为非活动成员，第 8-49 页
- 停用成员，第 8-50 页
- 退出集群，第 8-50 页
- 更改主设备，第 8-52 页
- 在集群范围内执行命令，第 8-52 页

成为非活动成员

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。

备注　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程序。如果您尚未进入情景配置模式，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

- 退出集群，第 8-50 页

停用成员

要从任何设备停用成员，请执行以下步骤。

备注 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。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程序。如果您尚未进入情景配置模式，请输入 **changeto system** 命令。

操作步骤

步骤 1 从集群中删除设备：

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。如果在从属设备上输入此命令来删除主设备，将会选举新的主设备。

要查看成员名称，请输入 **cluster remove unit ?**，或者输入 **show cluster info** 命令。

相关主题

- 退出集群，第 8-50 页

退出集群

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　对于从属设备，禁用集群：

cluster group *cluster_name*
no enable

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

在从属设备上启用集群时，您无法进行配置更改。

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　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，请使用本节中的程序。但是请注意，对集中功能而言，如果使用本程序强制更改主设备，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。

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程序。如果您尚未进入情景配置模式，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。

要查看成员名称，请输入 **cluster master unit ?**（可查阅除当前设备之外的所有名称），或输入 **show cluster info** 命令。

相关主题

- 成为非活动成员，第 8-49 页
- 集群的集中功能，第 8-23 页

在集群范围内执行命令

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** 命令以收集所有输出并将其显示在当前设备的控制台上。其他命令，如 **capture** 和 **copy**，也可在整个集群范围内执行。

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
```

要查看成员名称，请输入 **cluster exec unit ?**（可查阅除当前设备之外的所有名称），或输入 **show cluster info** 命令。

示例

要同时将同一捕获文件从集群中的所有设备复制到 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
```

多个 PCAP 文件 （一个文件来自一个设备）将复制到 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。在本示例中， asa1 和 asa2 是集群设备名称。

以下是 **cluster exec show port-channel** 摘要命令的输出示例，显示了集群内每个成员的 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。

- 监控集群状态，第 8-53 页
- 在集群范围捕获数据包，第 8-54 页
- 监控集群资源，第 8-54 页
- 监控集群流量，第 8-55 页
- 监控集群路由，第 8-57 页
- 配置集群日志记录，第 8-57 页
- 监控集群接口，第 8-57 页
- 调试集群，第 8-58 页

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

要支持集群范围的故障排除，您可以使用 **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属设备上将自动启用此功能。

相关主题

- 捕获数据包，第 35-1 页

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*]

显示整个集群的聚合数据。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)
```

  要对连接流进行故障排除，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。寻找具有以下标志的流：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*]

  显示整个集群的聚合数据。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
```

  要显示所有设备上正在使用的连接的聚合计数，请输入：

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     c12(LOCAL):********************************************************
  100 in use, 100 most used
```

```
cl1:********************************************************************
100 in use, 100 most used
```

- **show asp cluster counter**

  此命令对于数据路径故障排除非常有用。

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

- 在非 EMBLEM 格式系统日志消息中包含设备 ID，第 36-15 页

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。

- ASA 和交换机配置示例，第 8-58 页
- 单臂防火墙，第 8-61 页
- 流量分离，第 8-63 页
- 包含备用链路 （传统的 8 主用/8 备用）的跨网络 EtherChannel，第 8-65 页

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

- ASA 配置，第 8-59 页
- 思科 IOS 交换机配置，第 8-60 页

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 从属设备引导程序配置

```
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
```

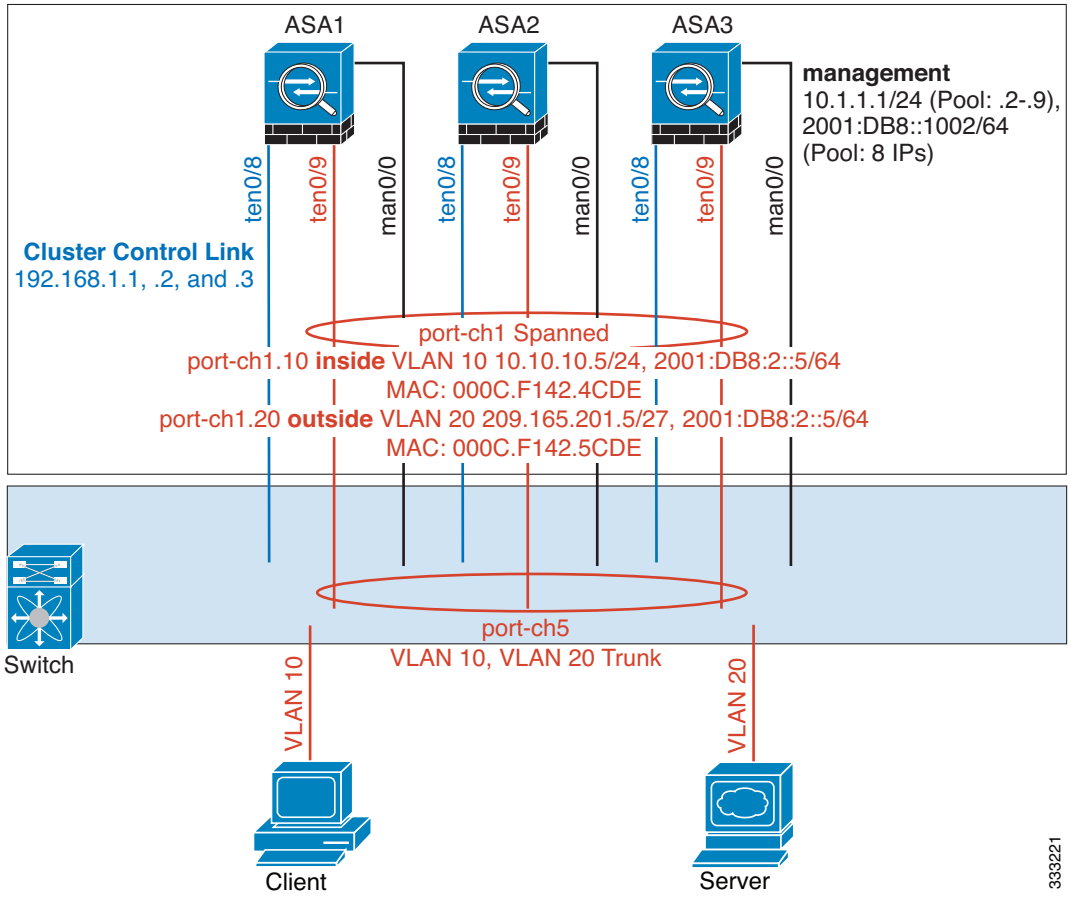
思科 IOS 交换机配置

```
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侧分组为一个 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 从属设备引导程序配置

```
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 从属设备引导程序配置

```
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
```

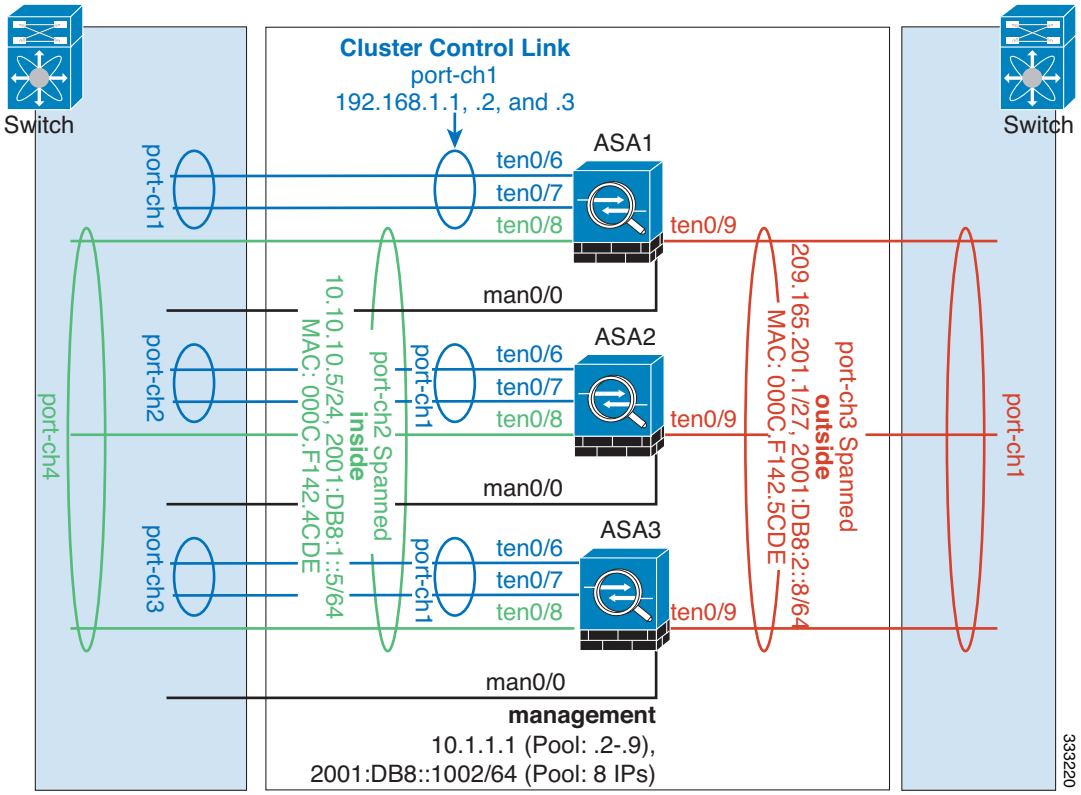
主设备接口配置

```
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 从属设备引导程序配置

```
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 从属设备引导程序配置

```
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

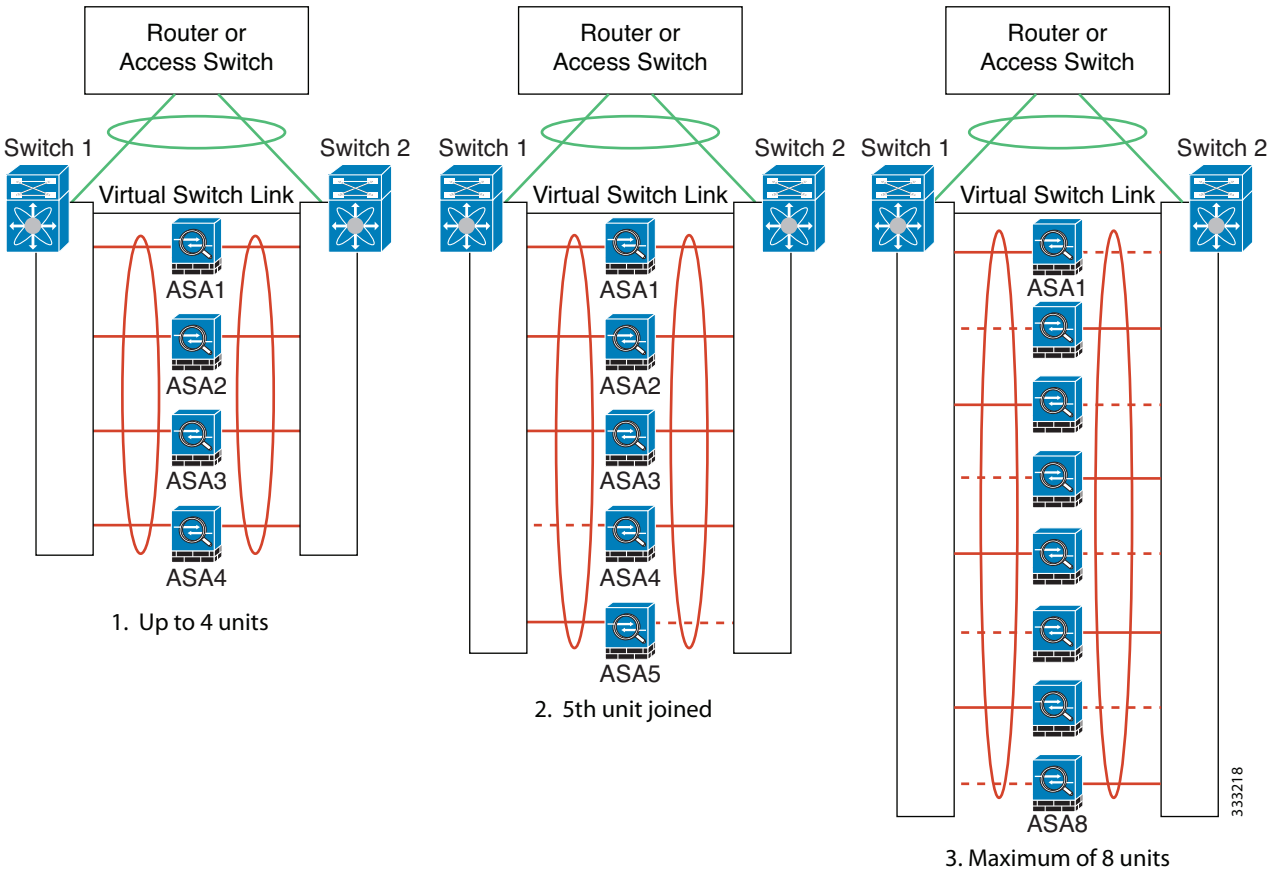
interface tengigabitethernet 0/8
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    port-channel span-cluster
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    ipv6 address 2001:DB8:1::5/64
    mac-address 000C.F142.4CDE

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
```

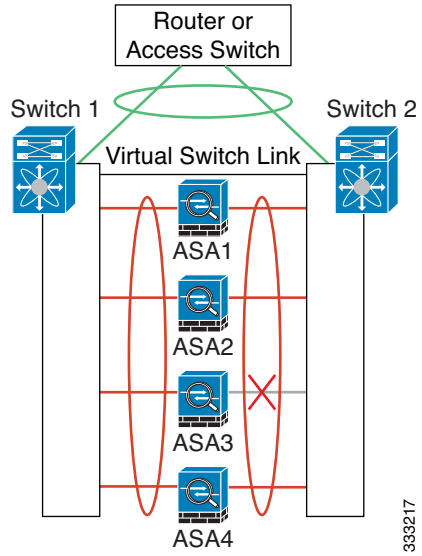
包含备用链路 （传统的 8 主用/8 备用）的跨网络 EtherChannel

在传统的 EtherChannel 中，最大活动端口数限制为 8 个来自交换机侧的端口。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。如果您使用 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，排序位置较低的端口是 “主” 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的情况：

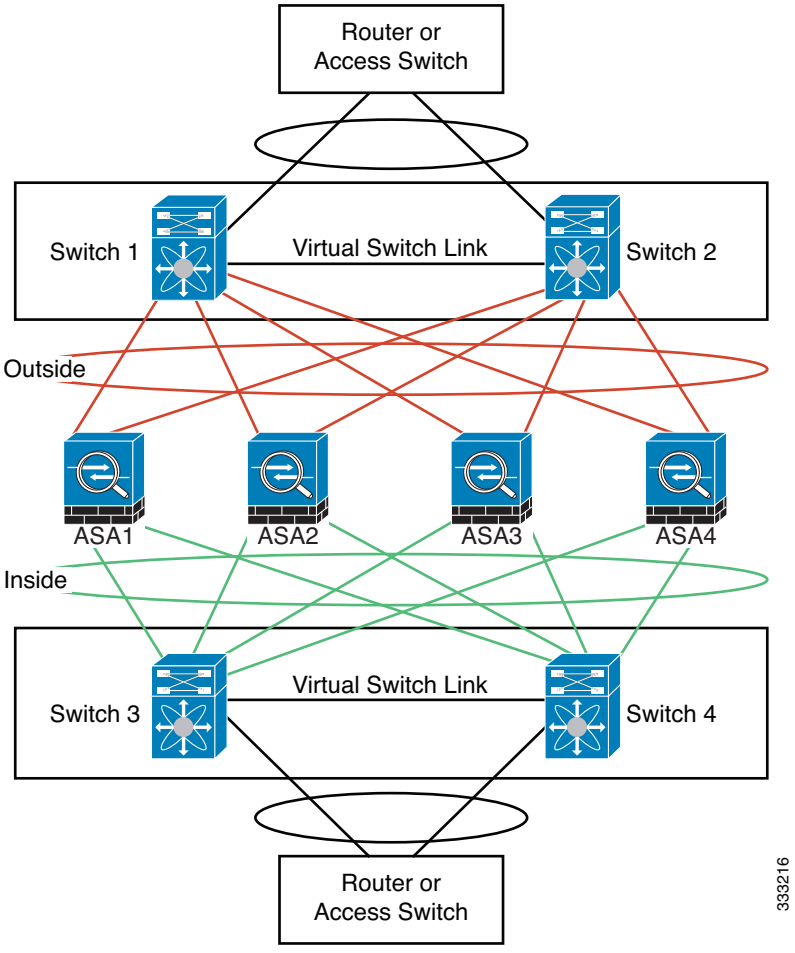


此时的处理原则是，首先将通道中的活动端口数增加到最大值，其次是保持活动的主端口数与活动的辅助端口数之间的均衡。请注意，当第 5 台设备加入集群时，流量并未在所有设备之间达到均衡。

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 从属设备引导程序配置

```
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 从属设备引导程序配置

```
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 从属设备引导程序配置

```
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，您可以将多台 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。 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。 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）且它连接到 VSS 或 vPC 对，则您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。如果您将 ASA 保持时间超时设置为一个较低值（如 0.8 秒），则可将 ASA 从集群中匿名删除，ASA 会将 keepalive 消息发送到这些 EtherChannel 接口之一。当您启用 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。 修改了以下命令：**health-check** [**vss-enabled**]

功能名称	平台版本	功能信息
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。 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)	在透明防火墙模式下使用跨网络 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下使用跨网络 EtherChannel 的站点间集群。 未修改任何命令。
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。您还应遵循以下准则： • 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。 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，您现在可以在跨网络 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。 **备注**　如果您要在跨网络 EtherChannel 中使用 8 条以上的活动链路，则无法同时使用备用链路；要支持 9 至 32 条活动链路，需要您禁用允许使用备用链路的 cLACP 动态端口优先级。 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。 未修改任何命令。
BGP 对 ASA 集群的支持	9.3(1)	增加了对 BGP 用于 ASA 集群的支持。 引入了以下命令：**bgp router-id clusterpool**
通过在内部网络之间设置 ASA 集群防火墙，进行透明模式的站点间部署	9.3(2)	您现在可以在每个站点上的内部网络和网关路由器之间部署透明模式的集群 （AKA 东西插入），并在站点之间扩展内部 VLAN。建议使用重叠传输虚拟化 (OTV)，但您可以使用任何可确保网关路由器的重叠 MAC 地址和 IP 地址在站点之间不泄漏的方法。使用 HSRP 等第一跃点冗余协议 (FHRP) 为网关路由器提供相同的虚拟 MAC 和 IP 地址。

功能名称	平台版本	功能信息
按接口启用和禁用 ASA 集群运行状况监控	9.4(1)	您现在可以按接口启用或禁用运行状况监控。默认情况下，运行状况监控在所有端口通道冗余接口和单一物理接口上处于启用状态。运行状况监控不在 VLAN 子接口或虚拟接口 （例如， VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。您可能想禁用不重要的接口 （例如管理接口）的运行状况检查。 引入了以下命令：**health-check monitor-interface**。
DHCP 中继的 ASA 集群支持	9.4(1)	现在可以在 ASA 集群上配置 DHCP 中继。通过使用客户端 MAC 地址散列，使客户端 DHCP 请求在集群成员中实现了负载均衡。仍然不支持 DHCP 客户端和服务器功能。 未修改任何命令。
ASA 集群中的 SIP 检测支持	9.4(1)	您现在可以在 ASA 集群上配置 SIP 检测。控制流可以在任何设备上创建 （由于负载均衡），但其子数据流必须驻留在同一设备上。不支持 TLS 代理配置。 引入了以下命令：**show cluster service-policy**



第 3 部分

接口



基本接口配置

本章介绍基本接口配置，包括以太网设置和巨帧配置。

备注 在多情景模式下，请在系统执行空间中完成本节所述的所有任务。要从情景切换到系统执行空间，请输入 **changeto system** 命令。

备注 对于 ASA 服务模块接口，请参阅 《ASA 服务模块 快速入门指南》。

- 关于基本接口配置，第 9-1 页
- 基本接口配置许可，第 9-4 页
- 基本接口配置的相关准则，第 9-5 页
- 基本接口配置的默认设置，第 9-5 页
- 启用物理接口和配置以太网参数，第 9-6 页
- 监控接口，第 9-8 页
- 基本接口示例，第 9-9 页
- 基本接口配置历史记录，第 9-9 页

关于基本接口配置

本节介绍接口功能与特殊接口。

- Auto-MDI/MDIX 功能，第 9-1 页
- 管理接口，第 9-2 页

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。

管理接口

管理接口是一个仅用于管理流量的独立接口，具体情况视型号而定。

- 管理接口概述，第 9-2 页
- 管理插槽/端口接口，第 9-2 页
- 将任何接口用于管理专用流量，第 9-3 页
- 用于透明模式的管理接口，第 9-3 页
- 不支持冗余管理接口，第 9-3 页
- 除 ASA 5585-X 以外的所有型号上的管理接口，第 9-3 页

管理接口概述

您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）

您可能需要按照第 32 章 “管理访问”中所述配置对接口的管理访问。

管理*插槽/端口*接口

下表列出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	Management 0/1	Management 1/0	Management 1/1	可针对直通流量进行配置	允许子接口
ASA 5506-X	否	否	否	**是**	否	否
ASA 5508-X	否	否	否	**是**	否	否
ASA 5512-X	**是**	否	否	否	否	否
ASA 5515-X	**是**	否	否	否	否	否
ASA 5516-X	否	否	否	**是**	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
ASA 5585-X	**是**	**是**	**是** 如果在插槽 1 中安装了 SSP，则 Management 1/0 和 1/1 接口仅在插槽 1 中提供对 SSP 的管理访问。	**是**	**是**	**是**
ASASM	否	否	否	否	N/A	N/A
ASAv	**是**	否	否	否	否	否

备注　如果您安装了一个模块，则该模块的管理接口仅提供对该模块的管理访问。对于安装了软件模块的型号，软件模块与 ASA 使用相同的物理管理接口。

将任何接口用于管理专用流量

若想将任何接口 （包括 EtherChannel 接口）用作管理专用接口，您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

在透明防火墙模式下，除了允许的最大数量的直通流量接口，您还可以将管理接口 （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。您不能将任何其他接口类型用作管理接口。

在多情景模式下，您无法跨情景共享任何接口，包括管理接口。要为每个情景提供管理，您可以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， ASA 5555-X 不允许管理接口上有子接口，因此为了针对每个情景进行管理，您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。

备注　在透明防火墙模式下，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

冗余接口不支持管理*插槽/端口*接口作为成员。您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。

除 ASA 5585-X 以外的所有型号上的管理接口

管理接口具有以下特征：

- 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
- 软件模块共享管理接口。ASA 和模块支持单独的 MAC 地址和 IP 地址。您必须在模块操作系统中执行模块 IP 地址的配置。但是，物理特征 （例如启用接口）在 ASA 上进行配置。

基本接口配置许可

型号	许可证要求
ASA 5506-X 系列	所有类型的接口： 基础许可证：536 增强型安全许可证：636
ASA 5508-X	所有类型的接口： 基础许可证：716
ASA 5512-X	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	所有类型的接口： 基础许可证：916
ASA 5516-X	所有类型的接口： 基础许可证：716
ASA 5525-X	所有类型的接口： 基础许可证：1316
ASA 5545-X	所有类型的接口： 基础许可证：1716
ASA 5555-X	所有类型的接口： 基础许可证：2516
ASA 5585-X	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
ASAv5 和 ASAv10	所有类型的接口： 标准许可证和高级许可证：716
ASAv30	所有类型的接口： 标准许可证和高级许可证：1316

备注 所有类型的接口均包括最大数量的组合接口；例如， VLAN 接口、 VXLAN 接口、物理接口、冗余接口、网桥组接口和 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，即使 GigabitEthernet 0/0 接口被定义为 port-channel 1 的一部分，以下两个接口也要计数：
interface gigabitethernet 0/0
和
interface port-channel 1

基本接口配置的相关准则

防火墙模式

对于多情景透明模式，每个情景必须使用不同的接口；您不能在情景之间共享一个接口。

故障切换

您不能与数据接口共享一个故障切换接口或状态接口。

其他准则

有些管理相关服务在启用非管理接口和 ASA 实现 “系统就绪”状态之前不可用。在 “系统就绪”状态下， ASA 会生成以下系统日志消息：

```
%ASA-6-199002: Startup completed.  Beginning operation.
```

基本接口配置的默认设置

本节列出了接口的默认设置 （如果没有出厂默认配置）。

接口的默认状态

接口的默认状态取决于类型和情景模式。

在多情景模式下，默认启用所有已分配的接口，而不考虑接口在系统执行空间中的状态。但是，要使流量通过该接口，还必须在系统执行空间中启用该接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

在单模式下或在系统执行空间中，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，要使流量通过冗余接口，还必须启用成员物理接口。
- VLAN 子接口 - 已启用。但是，要使流量通过子接口，还必须启用物理接口。
- VXLAN VNI 接口 - 已启用。
- EtherChannel 端口通道接口 - 已启用。但是，要使流量通过 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。您可以将 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。

启用物理接口和配置以太网参数

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 （如有）
- 启用暂停帧以进行流量控制

准备工作

对于多情景模式，请在系统执行空间中完成本程序。要从情景切换到系统执行空间，请输入 **changeto system** 命令。

操作步骤

步骤 1　指定要配置的接口：

interface *physical_interface*

示例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID 包含类型、插槽和端口号，格式为 *type*[*slot*/]*port*。

物理接口类型包括：

- **gigabitethernet**
- **tengigabitethernet**
- **management**

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）将媒体类型设置为 SFP （如果适用于所用的型号）：

media-type sfp

要恢复默认 RJ-45，请输入 **media-type rj45** 命令。

步骤 3　（可选）设置速度：

speed {**auto** | **10** | **100** | **1000** | **nonegotiate**}

示例：

```
ciscoasa(config-if)# speed 100
```

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** 命令可禁用链路协商。

步骤 4　（可选）设置 RJ-45 接口的双工：

duplex {**auto** | **full** | **half**}

示例：

```
ciscoasa(config-if)# duplex full
```

auto 设置是默认设置。EtherChannel 接口的双工设置必须为 **full** 或 **auto**。

步骤 5　（可选）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：

flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

示例：

```
ciscoasa(config-if)# flowcontrol send on 95 200 10000
```

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。根据 FIFO 缓冲区的使用率， NIC 硬件会自动生成暂停 (XOFF) 和 XON 帧。如果缓冲区的使用率超过高水位标记，系统会发送暂停帧。默认的 *high_water* 值为 128 KB （10 千兆以太网）和 24 KB （千兆以太网）；您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，如果缓冲区使用率降低至低于最低限的水平，则可发送 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）；您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 到期后恢复流量，具体由暂停帧中的计时器值控制。默认的 *pause_time* 值为 26624；您可以将此值设置为介于 0 到 65535 之间的值。如果缓冲区使用率持续高于高水位标记，则将重复发送暂停帧，但受暂停刷新阈值控制。

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?
```

要在没有提示的情况下更改参数，请使用 **noconfirm** 关键字。

注意　系统仅支持 802.3x 中定义的流量控制帧。系统不支持基于优先级的流量控制。

步骤 6　启用接口：

no shutdown

```
ciscoasa(config-if)# no shutdown
```

要禁用接口，请输入 **shutdown** 命令。如果输入 **shutdown** 命令，则还可关闭所有子接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

启用巨帧支持

巨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。您可以通过增加用于处理以太网帧的内存量对所有接口启用巨帧支持。为巨帧分配较多内存可能会有碍于最大限度地利用其他功能 （例如 ACL）。

准备工作

- 在多情景模式下，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 的值传输巨帧的每个接口设置 MTU；例如，使用 **mtu** 命令将该值设置为 9198。在多情景模式下，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。

操作步骤

步骤 1　启用巨帧支持：

jumbo-frame reservation

示例

以下示例启用巨帧保留，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
```

相关主题

- 关于高级接口配置，第 14-1 页
- 配置 MTU 和 TCP MSS，第 14-5 页

监控接口

请参阅以下命令：

- **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。

基本接口示例

请参阅以下配置示例。

- 物理接口参数示例，第 9-9 页
- 多情景模式示例，第 9-9 页

物理接口参数示例

以下示例在单模式下配置物理接口的参数：

```
interface gigabitethernet 0/1
    speed 1000
    duplex full
    no shutdown
```

多情景模式示例

以下示例在多情景模式下配置用于系统配置的接口参数，并将千兆以太网 0/1.1 子接口分配到 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
```

基本接口配置历史记录

表 9-2　　接口历史记录

功能名称	版本	功能信息
ASA 5510 上的基础许可证增加了接口数	7.2(2)	对于 ASA 5510 上的基础许可证，最大接口数从 3 加管理接口数增加到无限个。
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)。接口名称将仍为 Ethernet 0/0 和 Ethernet 0/1。使用 **speed** 命令可更改接口上的速度，使用 **show interface** 命令可查看为每个接口当前配置的速度。

表 9-2　　接口历史记录 （续）

功能名称	版本	功能信息
对 ASA 5580 的巨型数据包支持	8.1(1)	思科 ASA 5580 支持巨帧。巨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。您可以通过增加用于处理以太网帧的内存量对所有接口启用巨帧支持。为巨帧分配较多内存可能会有碍于最大限度地利用其他功能 （例如 ACL）。 ASA 5585-X 也支持此功能。 引入了以下命令：**jumbo-frame reservation**。
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)	您现在可以为流量控制启用暂停 (XOFF) 帧。 ASA 5585-X 也支持此功能。 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)	您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。 修改了以下命令：**flowcontrol**。



EtherChannel 接口和冗余接口

本章介绍如何配置 EtherChannel 接口和冗余接口。

备注 在多情景模式下，请在系统执行空间中完成本节所述的所有任务。要从情景切换到系统执行空间，请输入 **changeto system** 命令。

备注 有关具有特殊要求的 ASA 集群接口，请参阅第 8 章 “ASA 集群”。

- 关于 EtherChannel 接口和冗余接口，第 10-1 页
- EtherChannel 接口和冗余接口准则，第 10-4 页
- EtherChannel 接口和冗余接口的默认设置，第 10-6 页
- 配置冗余接口，第 10-6 页
- 配置 EtherChannel，第 10-8 页
- 监控 EtherChannel 接口和冗余接口，第 10-11 页
- EtherChannel 接口和冗余接口的示例，第 10-11 页
- EtherChannel 接口和冗余接口历史记录，第 10-12 页

关于 EtherChannel 接口和冗余接口

本节介绍 EtherChannel 接口和冗余接口。

- 冗余接口，第 10-1 页
- EtherChannel，第 10-2 页

冗余接口

逻辑冗余接口包括一对物理接口：主用接口和备用接口。当主用接口发生故障时，备用接口将变为主用接口并开始传递流量。您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切换，但如果需要，您可以配置冗余接口以及设备级故障切换。

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 地址会发生更改，以与当前最先列出的接口的 MAC 地址相匹配。或者，您可以向冗余接口分配 MAC 地址，该地址的使用与成员接口 MAC 地址无关。如果主用接口故障切换到备用接口，则系统会维护同一 MAC 地址，以便流量不会中断。

相关主题

- 配置 MTU 和 TCP MSS，第 14-5 页
- 配置多情景，第 6-14 页

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，以便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。

您最多可配置 48 个 EtherChannel。

- 通道组接口，第 10-2 页
- 连接到另一台设备上的 EtherChannel，第 10-2 页
- 链路汇聚控制协议，第 10-3 页
- 负载均衡，第 10-4 页
- EtherChannel MAC 地址，第 10-4 页

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，您最多可以将 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都必须属于同一类型且具有相同速度。添加到通道组的第一个接口确定正确的类型和速度。

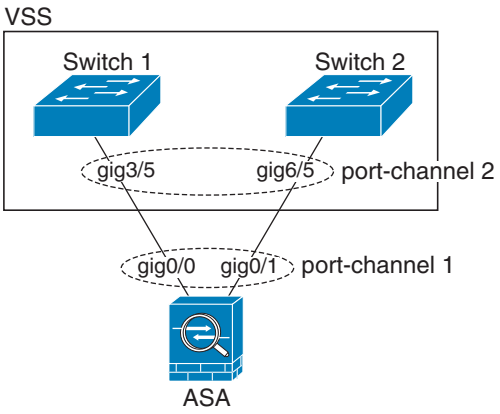
EtherChannel 汇聚通道中所有可用活动接口上的流量。系统根据源或目标 MAC 地址、 IP 地址、 TCP 端口号、 UDP 端口号和 VLAN 编号使用专有散列算法来选择接口。

连接到另一台设备上的 EtherChannel

ASA EtherChannel 连接到的设备还必须支持 802.3ad EtherChannel；例如，可以连接到 Catalyst 6500 交换机或 Cisco Nexus 7000。

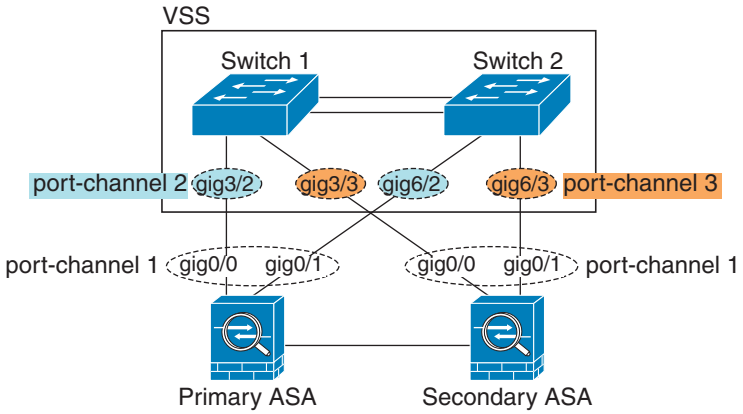
如果交换机属于虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 的一部分，则可以将同一 EtherChannel 内的 ASA 接口连接到 VSS/vPC 中的单独交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台单独的交换机的行为就像一台交换机一样。

图 10-1　　连接到 VSS/vPC



如果您在主用/备用故障切换部署中使用 ASA，则需要在 VSS/vPC 中的交换机上创建单独的 EtherChannel，为每个 ASA 创建一个。在每个 ASA 上，您可以将一个 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），但单个 EtherChannel 并不可取，因为您不希望将流量发送到备用 ASA。

图 10-2　　主用/备用故障切换和 VSS/vPC



链路汇聚控制协议

链路汇聚控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

您可以将 EtherChannel 中的每个物理接口配置为：

- Active - 发送并接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- Passive - 接收 LACP 更新。备用 EtherChannel 只能与主用 EtherChannel 建立连接。
- On - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。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 地址进行散列处理来将数据包分发给 EtherChannel 中的接口（此条件可配置）。在模数运算中，将得到的散列值除以主用链路数，得到的余数确定哪个接口拥有流量。*hash_value* **mod** *active_links* 结果为 0 的所有数据包都发往 EtherChannel 中的第一个接口，结果为 1 的发往第二个接口，结果为 2 的数据包发往第三个接口，依此类推。例如，如果您有 15 个主用链路，则模数运算的值为 0 到 14。如果有 6 个主用链路，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，而 EtherChannel 中的每个 ASA 又有 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未由备用接口替代，则流量会在剩余的链路之间重新均衡。该故障会在第 2 层的生成树和第 3 层的路由表中被屏蔽，因此故障切换对其他网络设备是透明的。

相关主题

- 自定义 EtherChannel，第 10-9 页

EtherChannel MAC 地址

属于通道组一部分的所有接口都共享同一 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。

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。在多情景模式下，您可以将唯一 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更改的情况下，我们建议手动或在多情景模式下自动配置唯一 MAC 地址。如果删除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址会更改为下一个编号最小的接口，从而导致流量中断。

EtherChannel 接口和冗余接口准则

故障切换

- 如果要将冗余接口或 EtherChannel 接口用作故障切换链路，您必须在故障切换对中的两台设备上预配置要使用的接口；不能在主设备上配置该接口并期望它会复制到辅助设备，因为*复制需要使用故障切换链路本身*。
- 如果将冗余接口或 EtherChannel 接口用于状态链路，则无需特殊配置；可以照常从主设备复制配置。
- 您可以使用 **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。如果主用成员接口故障切换到备用接口，则此活动不会在监控设备级故障切换时导致冗余接口或 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 接口用于故障切换或状态链路，然后防止无序数据包，则仅会使用 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。您不能在 EtherChannel 配置用作故障切换链路时对其进行修改。要更改配置，您需要在进行更改时关闭 EtherChannel 或临时禁用故障切换；执行上述任一操作均可在这段时间内阻止进行故障切换。

型号支持

- 仅在 ASA 设备上支持 EtherChannel；在 ASAv 或 ASASM 上不支持 EtherChannel。
- ASASM 上不支持冗余接口。

集群

- 如果要将冗余接口或 EtherChannel 接口用作集群控制链路，您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*。
- 要配置跨网络 EtherChannel 或单个集群接口，请参阅有关集群的章节。

冗余接口

- 您最多可以配置 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。
- 您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。您不能在冗余接口和 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，则可以在 ASA 上配置这两种接口。
- 如果关闭主用接口，则备用接口变为主用接口。
- 冗余接口不支持管理*插槽/端口*接口作为成员。您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。

EtherChannel

- ASAv 上不支持 EtherChannel。
- 您最多可配置 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，您最多可以将 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，其余接口可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都必须属于同一类型且具有相同速度。添加到通道组的第一个接口确定正确的类型和速度。
- ASA EtherChannel 连接到的设备还必须支持 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 标签的 LACPDU。如果使用思科 IOS **vlan dot1Q tag native** 命令在相邻交换机上启用本地 VLAN 标签，则 ASA 将会丢弃已标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标签。在多情景模式下，在数据包捕获中不包含这些消息，因此您无法轻易对问题进行诊断。
- 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 EtherChannel 接口，而不是成员物理接口。
- 您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。您不能在冗余接口和 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，则可以在 ASA 上配置这两种接口。

EtherChannel 接口和冗余接口的默认设置

本节列出了接口的默认设置 （如果没有出厂默认配置）。

接口的默认状态

接口的默认状态取决于类型和情景模式。

在多情景模式下，默认启用所有已分配的接口，而不考虑接口在系统执行空间中的状态。但是，要使流量通过该接口，还必须在系统执行空间中启用该接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

在单模式下或在系统执行空间中，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，要使流量通过冗余接口，还必须启用成员物理接口。
- EtherChannel 端口通道接口 - 已启用。但是，要使流量通过 EtherChannel 接口，还必须启用通道组物理接口。

配置冗余接口

逻辑冗余接口包括一对物理接口：主用接口和备用接口。当主用接口发生故障时，备用接口将变为主用接口并开始传递流量。您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切换，但如果需要，您可以配置冗余接口以及故障切换。

本节介绍如何配置冗余接口。

- 配置冗余接口，第 10-6 页
- 更改主用接口，第 10-7 页

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。

准备工作

- 您最多可以配置 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 会根据其成员接口的物理类型继承默认延迟值。
- 两个成员接口均必须为相同的物理类型。例如，均是千兆以太网接口。
- 如果已为物理接口配置了名称，则不能将该物理接口添加到冗余接口。您必须先在 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格中使用 **no nameif** 命令。
- 对于多情景模式，请在系统执行空间中完成本程序。要从情景切换到系统执行空间，请输入 **changeto system** 命令。

注意　如果使用的是配置中已有的物理接口，则删除名称将会清除引用该接口的任何配置。

操作步骤

步骤 1　添加逻辑冗余接口：

interface redundant *number*

示例：

```
ciscoasa(config)# interface redundant 1
```

number 参数是介于 1 和 8 之间的整数。

要配置冗余接口的逻辑参数 （例如名称），您需要先向该接口至少添加一个成员接口。

步骤 2　将第一个成员接口添加到冗余接口：

member-interface *physical_interface*

示例：

```
ciscoasa(config-if)# member-interface gigabitethernet 0/0
```

冗余接口不支持管理*插槽/端口*接口作为成员。

添加该接口后，将会删除其任何配置 （例如 IP 地址）。

步骤 3　将第二个成员接口添加到冗余接口：

member-interface *physical_interface*

示例：

```
ciscoasa(config-if)# member-interface gigabitethernet 0/1
```

确保第二个接口的物理类型与第一个接口相同。

要删除成员接口，请输入 **no member-interface** *physical_interface* 命令。您不能从冗余接口中同时删除两个成员接口；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
```

更改主用接口

默认情况下，主用接口 （如果可用）是配置中列出的第一个接口。

操作步骤

步骤 1　要查看哪个接口是主用接口，请：

```
ciscoasa# show interface redundantnumber detail | grep Member
```

示例：

```
ciscoasa# show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

步骤 2　更改主用接口：

```
ciscoasa# redundant-interface redundantnumber active-member physical_interface
```

redundant*number* 参数是冗余接口 ID，例如 **redundant1**。

physical_interface 是设为主用的成员接口的 ID。

配置 EtherChannel

本节介绍如何创建 EtherChannel 端口通道接口，如何向 EtherChannel 分配接口，以及如何自定义 EtherChannel。

- 将接口添加到 EtherChannel，第 10-8 页
- 自定义 EtherChannel，第 10-9 页

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。

准备工作

- 您最多可配置 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，您最多可以将 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，其余接口可在出现接口故障的情况下用作备用链路。
- 要为集群配置跨网络 EtherChannel，请参阅有关集群的章节而不是此程序。
- 通道组中的所有接口都必须具有相同的类型、速度和双工。不支持半双工。
- 如果已为物理接口配置了名称，则不能将该物理接口添加到通道组。您必须先在 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格中使用 **no nameif** 命令。
- 对于多情景模式，请在系统执行空间中完成本程序。要从情景切换到系统执行空间，请输入 **changeto system** 命令。

注意　如果使用的是配置中已有的物理接口，则删除名称将会清除引用该接口的任何配置。

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，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。

在透明模式下，如果使用多个管理接口创建通道组，则可以将 EtherChannel 用作管理专属接口。

步骤 2　将此物理接口分配到 EtherChannel：

channel-group *channel_id* **mode** {**active** | **passive** | **on**}

示例：

```
ciscoasa(config-if)# channel-group 1 mode active
```

channel_id 是介于 1 和 48 之间的整数。如果此通道 ID 的端口通道接口尚未存在于配置中，则将添加一个端口通道接口：

interface port-channel *channel_id*

我们建议使用 **active** 模式。

步骤 3　（可选）为通道组中的物理接口设置优先级：

lacp port-priority *number*

示例：

```
ciscoasa(config-if)# lacp port-priority 12345
```

优先级 *number* 是介于 1 和 65535 之间的整数。默认值为 32768。数字越大，优先级越低。如果分配的接口多于可用的接口，则 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相同，则优先级由接口 ID（插槽/端口）确定。最低的接口 ID 具有最高优先级。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 也如此），请将此命令设置为具有较低的值。例如，要在千兆以太网 0/7 之前将千兆以太网 1/3 设为主用，请在 1/3 接口上将 **lacp port-priority** 值设置为 12345；在 0/7 接口上设置为默认值 32768。

如果 EtherChannel 另一端的设备端口存在优先级冲突，则会使用系统优先级来确定使用哪些端口优先级。请参阅 **lacp system-priority** 命令。

步骤 4　对于要添加到通道组中的每个接口，请重复步骤 1 至步骤 3。

通道组中的每个接口都必须具有相同的类型和速度。不支持半双工。如果添加不匹配的接口，则该接口将处于暂停状态。

相关主题

- 链路汇聚控制协议，第 10-3 页
- 自定义 EtherChannel，第 10-9 页

自定义 EtherChannel

本节介绍如何设置 EtherChannel 中的最大接口数，用于使 EtherChannel 成为主用接口所需的最小操作接口数、负载均衡算法以及其他可选参数。

操作步骤

步骤 1　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。如果尚未添加接口，则此命令会创建端口通道接口。

您需要先向端口通道接口添加至少一个成员接口，然后才能为其配置逻辑参数（例如名称）。

步骤 2　指定通道组中允许的最大主用接口数：

lacp max-bundle *number*

示例：

```
ciscoasa(config-if)# lacp max-bundle 6
```

number 介于 1 和 16 之间。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　指定使端口通道接口变成主用接口所需的最小主用接口数：

port-channel min-bundle *number*

示例：

```
ciscoasa(config-if)# port-channel min-bundle 2
```

number 介于 1 和 16 之间。默认值为 1。如果通道组中的主用接口数小于此值，则端口通道接口将会发生故障，并可能会触发设备级故障切换。

步骤 4　配置负载均衡算法：

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
```

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**) 来均衡接口上的数据包负载。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，则分配给 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。

步骤 5　设置 LACP 系统优先级：

lacp system-priority *number*

示例：

```
ciscoasa(config)# lacp system-priority 12345
```

number 介于 1 和 65535 之间。默认值为 32768。数字越大，优先级越低。对于 ASA 而言，此命令是全局命令。

如果 EtherChannel 另一端的设备端口存在优先级冲突，则会使用系统优先级来确定使用哪些端口优先级。有关 EtherChannel 内的接口优先级，请参阅 **lacp port-priority** 命令。

步骤 6　（可选）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，请参阅启用物理接口和配置以太网参数，第 9-6 页。此方法提供了设置这些参数的快捷方式，因为通道组中所有接口的这些参数都必须匹配。

相关主题

- 负载均衡，第 10-4 页
- 将接口添加到 EtherChannel，第 10-8 页

监控 EtherChannel 接口和冗余接口

请参阅以下命令：

- **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，以详细的单行摘要形式显示 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散列结果和成员接口。

EtherChannel 接口和冗余接口的示例

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 的优先级设置为高于其他接口。

```
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
```

EtherChannel 接口和冗余接口历史记录

表 10-1　　EtherChannel 接口和冗余接口历史记录

功能名称	版本	功能信息
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。当主用接口发生故障时，备用接口将变为主用接口并开始传递流量。您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切换，但如果需要，您可以配置冗余接口以及故障切换。您最多可以配置 8 个冗余接口对。
EtherChannel 支持	8.4(1)	您可以为八个主用接口各配置多达 48 个 802.3ad EtherChannel。 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**。 **备注**　ASA 5505 不支持 EtherChannel。
一个 EtherChannel 中支持 16 个主用链路	9.2(1)	现在，一个 EtherChannel 中最多可以配置 16 个主用链路。以前，可以有 8 个主用链路和 8 个备用链路。确保交换机可以支持 16 个主用链路（例如，可使用带有 F2 系列 10 千兆以太网模块的思科 Nexus 7000）。 **备注**　如果从较低的 ASA 版本进行升级，则为了实现兼容，可将最大主用接口数设置为 8（**lacp max-bundle** 命令）。 修改了以下命令：**lacp max-bundle** 和 **port-channel min-bundle**。



VLAN 接口

本章说明如何配置 VLAN 子接口。

备注 在多情景模式下，请在系统执行空间中完成本节所述的所有任务。要从情景切换到系统执行空间，请输入 **changeto system** 命令。

- 关于 VLAN 接口，第 11-1 页
- VLAN 接口许可，第 11-1 页
- VLAN 接口准则，第 11-2 页
- VLAN 接口的默认设置，第 11-2 页
- 配置 VLAN 子接口和 802.1Q 中继，第 11-3 页
- 监控 VLAN 接口，第 11-4 页
- VLAN 接口示例，第 11-4 页
- VLAN 接口历史记录，第 11-4 页

关于 VLAN 接口

通过 VLAN 子接口，您可以将物理接口、冗余接口或 EtherChannel 接口划分为标记有不同 VLAN ID 的多个逻辑接口。具有一个或多个 VLAN 子接口的接口会自动配置为 802.1Q 中继。由于 VLAN 允许您在给定的物理接口上分离流量，因此您可以增加可供网络使用的接口数，而无需添加额外的物理接口或 ASA。此功能非常有助于您在多情景模式下向每个情景分配唯一接口。

VLAN 接口许可

型号	许可证要求
ASA 5506-X 系列	基础许可证：5 增强型安全许可证：30
ASA 5508-X	基础许可证：50

型号	许可证要求
ASA 5512-X	基础许可证：50 增强型安全许可证：100
ASA 5515-X	基础许可证：100
ASA 5516-X	基础许可证：50
ASA 5525-X	基础许可证：200
ASA 5545-X	基础许可证：300
ASA 5555-X	基础许可证：500
ASA 5585-X	基础许可证和增强型安全许可证：1024
ASAv5 和 ASAv10	标准许可证和高级许可证：50
ASAv30	标准许可证和高级许可证：200

备注　对于根据 VLAN 限制计数的接口，您必须向其分配 VLAN。例如：
interface gigabitethernet 0/0.100
vlan 100

VLAN 接口准则

型号支持

VLAN 子接口在 ASASM 上不受支持；ASASM 接口已是从交换机分配的 VLAN 接口。

其他准则

- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常表明也不希望物理接口传递流量，因为物理接口会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 接口才能使子接口传递流量，请通过省略 **nameif** 命令来确保物理接口、冗余接口或 EtherChannel 接口不传递流量。如果要使物理接口、冗余接口或 EtherChannel 接口传递未标记的数据包，您可以照常配置 **nameif** 命令。
- （除 ASA 5585-X 以外的所有型号）无法在管理接口上配置子接口。
- ASA 不支持动态中继协议 (DTP)，因此您必须无条件地将连接的交换机端口配置到中继上。

VLAN 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）。

接口的默认状态

接口的默认状态取决于类型和情景模式。

在多情景模式下，默认启用所有已分配的接口，而不考虑接口在系统执行空间中的状态。但是，要使流量通过该接口，还必须在系统执行空间中启用该接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

在单模式下或在系统执行空间中，接口具有以下默认状态：

- 物理接口 - 已禁用。
- VLAN 子接口 - 已启用。但是，要使流量通过子接口，还必须启用物理接口。

配置 VLAN 子接口和 802.1Q 中继

向物理接口、冗余接口或 EtherChannel 接口添加 VLAN 子接口。

准备工作

对于多情景模式，请在系统执行空间中完成本程序。要从情景切换到系统执行空间，请输入 **changeto system** 命令。

操作步骤

步骤 1　指定新的子接口：

interface {*physical_interface* | **redundant** *number* | **port-channel** *number*}.*subinterface*

示例：

```
ciscoasa(config)# interface gigabitethernet 0/1.100
```

redundant *number* 参数是冗余接口 ID，例如 **redundant 1**。

port-channel *number* 参数是 EtherChannel 接口 ID，例如 **port-channel 1**。

subinterface ID 是介于 1 和 4294967293 之间的整数。

步骤 2　指定子接口的 VLAN：

vlan *vlan_id*

示例：

```
ciscoasa(config-subif)# vlan 101
```

vlan_id 是介于 1 和 4094 之间的整数。某些 VLAN ID 可能是连接的交换机中的保留 VLAN ID，因此请查看交换机文档以了解详细信息。

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。您无法将 VLAN 分配给物理接口。每个子接口必须有一个 VLAN ID，然后才能传递流量。要更改 VLAN ID，您无需使用 **no** 选项删除旧 VLAN ID；您可以输入带有不同 VLAN ID 的 **vlan** 命令，ASA 会更改旧的 ID。

相关主题

- VLAN 接口许可，第 11-1 页

监控 VLAN 接口

请参阅以下命令：

- **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。

VLAN 接口示例

以下示例在单模式下配置子接口的参数：

```
interface gigabitethernet 0/1.1
    vlan 101
    no shutdown
```

VLAN 接口历史记录

表 11-1　　VLAN 接口历史记录

功能名称	版本	功能信息
增加了 VLAN 数量	7.0(5)	提高了以下限制： • ASA5510 基础许可证的 VLAN 数量从 0 增加到 10。 • ASA5510 增强型安全许可证 VLAN 数量从 10 增加到 25。 • ASA5520 VLAN 数量从 25 增加到 100。 • ASA5540 VLAN 数量从 100 增加到 200。
增加了 VLAN 数量	7.2(2)	提高了以下型号的 VLAN 限制：ASA 5510 （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）。
增加了 ASA 5580 的 VLAN 数量	8.1(2)	在 ASA 5580 上支持的 VLAN 数量从 100 增加到 250。



VXLAN 接口

本章介绍如何配置虚拟可扩展局域网 (VXLAN) 接口。VXLAN 作为第 3 层物理网络之上的第 2 层虚拟网络，可对第 2 层网络进行扩展。

- 关于 VXLAN 接口，第 12-1 页
- VXLAN 接口准则，第 12-6 页
- VXLAN 接口的默认设置，第 12-6 页
- 配置 VXLAN 接口，第 12-6 页
- 监控 VXLAN 接口，第 12-10 页
- VXLAN 接口示例，第 12-11 页
- VXLAN 接口的历史记录，第 12-15 页

关于 VXLAN 接口

VXLAN 提供与 VLAN 相同的以太网第 2 层网络服务，但其可扩展性和灵活性更为出色。与 VLAN 相比， VXLAN 提供以下优势：

- 可在整个数据中心中灵活部署多租户网段。
- 更高的可扩展性可提供更多的第 2 层网段，最多可达 1600 万个 VXLAN 网段。

本节介绍 VXLAN 如何工作。有关详细信息，请参阅 RFC 7348。

- VXLAN 封装，第 12-1 页
- VXLAN 隧道终端，第 12-2 页
- VTEP 源接口，第 12-2 页
- VNI 接口，第 12-2 页
- 对等体 VTEP，第 12-3 页
- VXLAN 使用案例，第 12-3 页

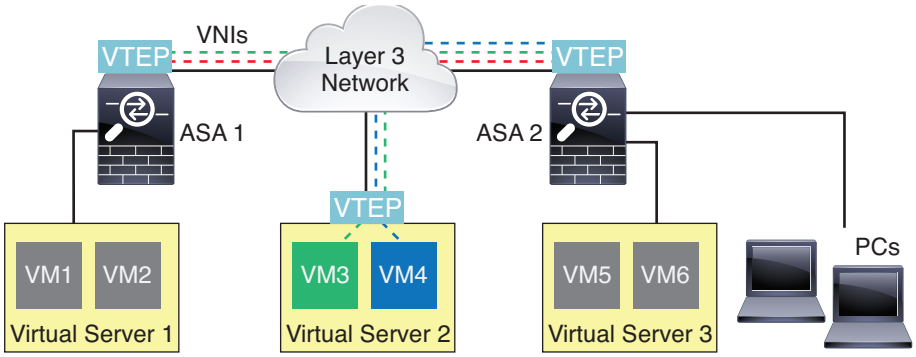
VXLAN 封装

VXLAN 是在第 3 层网络上的第 2 层重叠方案，使用 MAC Address-in-User 数据报协议 (MAC-in-UDP) 的封装方式。原始第 2 层帧已添加 VXLAN 报头，然后放入 UDP-IP 数据包中。

VXLAN 隧道终端

VXLAN 隧道终端 (VTEP) 设备执行 VXLAN 封装和解封。每个 VTEP 有两种接口类型：一个或多个虚拟接口称为 VXLAN 网络标识符 (VNI) 接口，您可以向其应用安全策略；以及称为 VTEP 源接口的常规接口，用于为 VTEP 之间的 VNI 接口建立隧道。VTEP 源接口连接到传输 IP 网络，进行 VTEP 至 VTEP 通信。

下图显示两个 ASA 和充当第 3 层网络中的 VTEP 的虚拟服务器 2，用于在站点之间扩展 VNI 1、2 和 3 网络。ASA 充当 VXLAN 和非 VXLAN 网络之间的网桥或网关。



VTEP 之间的底层 IP 网络与 VXLAN 重叠无关。封装的数据包根据外部 IP 地址报头路由，该报头具有初始 VTEP（用作源 IP 地址）和终止 VTEP（作为目标 IP 地址）。当远程 VTEP 未知时，目标 IP 地址可以是组播组。默认情况下，目标端口是 UDP 端口 4789（用户可配置）。

VTEP 源接口

VTEP 源接口是一个计划要与所有 VNI 接口相关联的常规 ASA 接口（物理、冗余、EtherChannel 接口，甚至 VLAN 接口）。每个 ASA/安全情景可以配置一个 VTEP 源接口。

尽管并未将 VTEP 源接口限制为全部用于传输 VXLAN 流量，但是可以实现该用途。如果需要，可以使用该接口传输常规流量，并将一个安全策略应用于传输此类流量的该接口。但是，对于 VXLAN 流量，必须对 VNI 接口应用所有安全策略。VTEP 接口仅作为物理端口。

在透明防火墙模式下， VTEP 源接口不是 BVI 的一部分，并且类似于对待管理接口的方式，不为该源接口配置 IP 地址。

VNI 接口

VNI 接口类似于 VLAN 接口：它们是虚拟接口，通过使用标记，实现网络流量在给定物理接口上的分离。将安全策略直接应用于每个 VNI 接口。

所有 VNI 接口都与同一 VTEP 接口相关联。

VXLAN 数据包处理

进出 VTEP 源接口的流量取决于 VXLAN 处理，特别是封装或解封。

封装处理包括以下任务：

- VTEP 源接口通过 VXLAN 报头封装内部 MAC 帧。
- UDP 校验和字段设置为零。

- 外部帧源 IP 设置为 VTEP 接口 IP。
- 外部帧目标 IP 通过远程 VTEP IP 查找确定。

解封；ASA 仅在以下条件下解封 VXLAN 数据包：

- VXLAN 数据包是目标端口设置为 4789 （用户可配置该值）的 UDP 数据包。
- 入口接口是 VTEP 源接口。
- 入口接口 IP 地址与目标 IP 地址相同。
- VXLAN 数据包格式符合标准。

对等体 VTEP

当 ASA 将数据包发送到对等体 VTEP 之后的设备时， ASA 需要两条重要的信息：

- 远程设备的目标 MAC 地址
- 对等体 VTEP 的目标 IP 地址

有两种方法使 ASA 可以找到此信息：

- 可以在 ASA 上静态配置单个对等体 VTEP IP 地址。

  无法手动定义多个对等体。

  然后， ASA 将已封装 VXLAN 的 ARP 广播发送到 VTEP，以获取终端节点 MAC 地址。
- 可以在每个 VNI 接口 （或者总的来说，在 VTEP 上）配置组播组。

  ASA 通过 VTEP 源接口发送 IP 组播数据包内已封装 VXLAN 的 ARP 广播数据包。对此 ARP 请求的响应使 ASA 可以获取远程终端节点的远程 VTEP IP 地址和目标 MAC 地址。

ASA 维护目标 MAC 地址到 VNI 接口的远程 VTEP IP 地址的映射。

VXLAN 使用案例

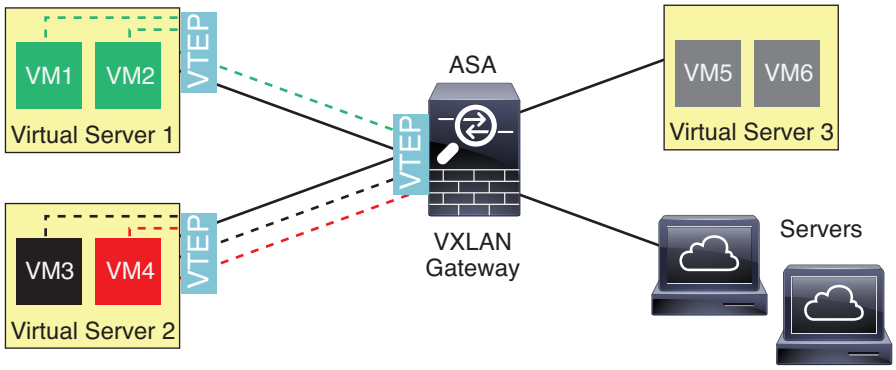
本节介绍在 ASA 上实施 VXLAN 的使用案例。

- VXLAN 网桥或网关概述，第 12-3 页
- VXLAN 网桥 （透明模式），第 12-4 页
- VXLAN 网关 （路由模式），第 12-4 页
- VXLAN 域之间的路由器，第 12-5 页

VXLAN 网桥或网关概述

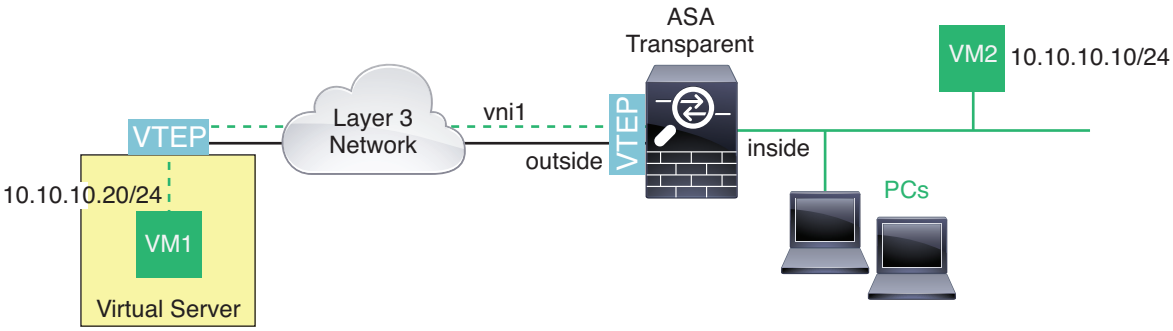
每个 ASA VTEP 都可作为终端节点 （例如 VM、服务器和 PC）和 VXLAN 重叠网络之间的网桥或网关。对于通过 VTEP 源接口借助 VXLAN 封装接收的传入帧，ASA 去掉 VXLAN 报头，并基于内部以太网帧的目标 MAC 地址，将传入帧转发到连接非 VXLAN 网络的物理接口。

ASA 始终会处理 VXLAN 数据包；而不仅仅是在两个其他 VTEP 之间转发未处理的 VXLAN 数据包。



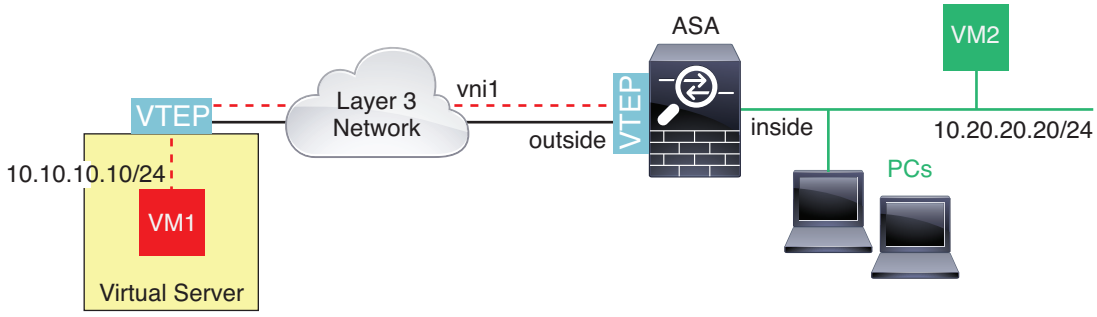
VXLAN 网桥 （透明模式）

在透明防火墙模式下， ASA 可以作为处于同一网络中 （远程） VXLAN 网段和本地网段之间的 VXLAN 网桥。在这种情况下，网桥虚拟接口 (BVI) 的一个成员是常规接口，而另一个成员是 VNI 接口。



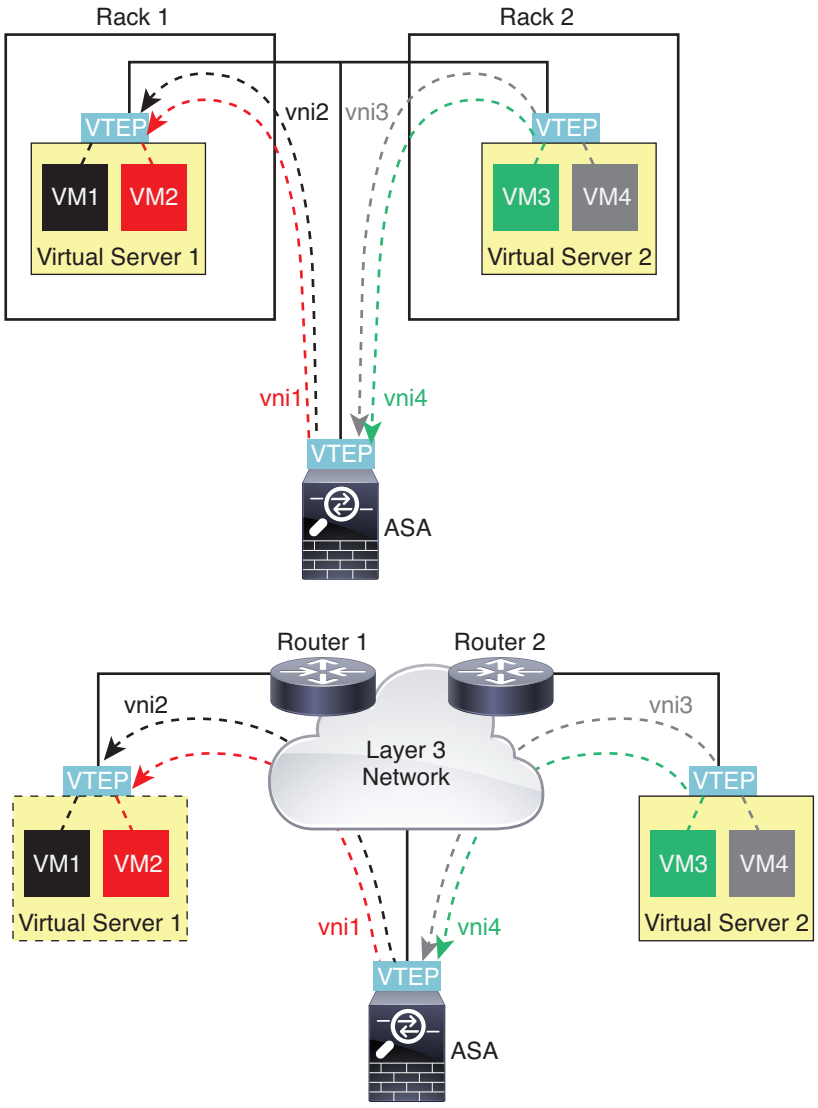
VXLAN 网关 （路由模式）

ASA 可充当 VXLAN 和非 VXLAN 域之间的路由器，用于连接不同网络上的设备。



VXLAN 域之间的路由器

借助通过 VXLAN 扩展的第 2 层域，虚拟机可以指向一个 ASA 作为其网关，即使 ASA 位于不同机架中，甚至当 ASA 位于第 3 层网络上很远的位置也是如此。



请参阅有关此场景的以下注释：

1. 对于从 VM3 到 VM1 的数据包，目标 MAC 地址为 ASA MAC 地址，因为 ASA 是默认网关。
2. 虚拟服务器 2 上的 VTEP 源接口接收来自 VM3 的数据包，然后使用 VNI 3 的 VXLAN 标签封装数据包，并将数据包发送到 ASA。
3. 当 ASA 接收数据包时，会解封数据包以获得内部帧。
4. ASA 使用内部帧进行路由查找，然后发现目标位于 VNI 2 上。如果尚不具有 VM1 的映射，ASA 会在 VNI 2 上的组播组 IP 上发送封装的 ARP 广播。

注意　ASA 必须使用动态 VTEP 对等体发现，因为 ASA 在此场景下有多个 VTEP 对等体。

5. ASA 再次使用 VXLAN 标签为 VNI 2 封装数据包，并且将数据包发送到虚拟服务器 1。在封装之前， ASA 将内部帧目标 MAC 地址更改为 VM1 的 MAC 地址 （ASA 可能需要组播封装的 ARP，以获取 VM1 MAC 地址）。
6. 当虚拟服务器 1 接收 VXLAN 数据包时，该虚拟服务器会解封数据包并向 VM1 提供内部帧。

VXLAN 接口准则

IPv6

- VNI 接口支持 IPv6 流量，但 VTEP 源接口 IP 地址只支持 IPv4。
- 不支持 IPv6 OSPF 接口设置。

群集

在单个接口模式下， ASA 集群不支持 VXLAN。仅跨网络 EtherChannel 模式支持 VXLAN。

路由

- VNI 接口仅支持静态路由；不支持动态路由协议。
- 不支持基于策略的路由。

VXLAN 接口的默认设置

默认启用 VNI 接口。

配置 VXLAN 接口

要配置 VXLAN，请执行下列步骤：

步骤 1　配置 VTEP 源接口，第 12-6 页。

步骤 2　配置 VNI 接口，第 12-8 页。

步骤 3　（可选）更改 VXLAN UDP 端口，第 12-9 页。

配置 VTEP 源接口

每个 ASA 或每个安全情景可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)；此时， VXLAN VTEP 是唯一受支持的 NVE。

准备工作

对于多情景模式，请在情景执行空间完成本节所述的任务。输入 **changeto context** *name* 命令以更改为要配置的情景。

操作步骤

步骤 1　（透明模式）将源接口指定为仅 NVE：

```
interface id
  nve-only
```

示例：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
```

可以通过此设置配置接口的 IP 地址。此命令对于路由模式为可选命令，在此模式下，此设置限制到 VXLAN 的流量并且仅限制此接口上的通用管理流量。

步骤 2　配置源接口名称和 IPv4 地址。

示例 （路由模式）：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

示例 （透明模式）：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

步骤 3　指定 NVE 实例：

```
nve 1
```

只能指定一个 NVE 实例，其中 ID 为 1。

注意　默认情况下，系统会为 NVE 实例添加 **encapsulation vxlan** 命令；无需显式添加该命令。

步骤 4　指定在步骤 2 中配置的源接口名称：

```
source-interface interface_name
```

示例：

```
ciscoasa(cfg-nve)# source-interface outside
```

步骤 5　（多情景模式；对于单情景模式为可选）手动指定对等体 VTEP IP 地址：

```
peer ip ip_address
```

示例：

```
ciscoasa(cfg-nve)# peer ip 10.1.1.2
```

如果指定对等体 IP 地址，则无法使用组播组发现。在多情景模式中不支持组播，因此只能选择手动配置。只能为 VTEP 指定一个对等体。

步骤 6　（可选；仅限单情景模式）为所有关联的 VNI 接口指定默认组播组：

```
default-mcast-group mcast_ip
```

示例：

```
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

如果每个 VNI 接口未配置组播组，则使用该组。如果配置一个 VNI 接口级别的组，则该组将覆盖此设置。

配置 VNI 接口

添加 VNI 接口，将其与 VTEP 源接口相关联，并配置基本的接口参数。

操作步骤

步骤 1　创建 VNI 接口：

interface vni *vni_num*

示例：

```
ciscoasa(config)# interface vni 1
```

将 ID 设置为 1 和 10000 之间的整数。此 ID 仅为内部接口标识符。

步骤 2　指定 VXLAN 网段 ID：

segment-id *id*

示例：

```
ciscoasa(config-if)# segment-id 1000
```

将 ID 设置为 1 和 16777215 之间的整数。网段 ID 用于 VXLAN 标记。

步骤 3　（透明模式）指定要与此接口关联的网桥组：

bridge-group *number*

示例：

```
ciscoasa(config-if)# bridge-group 1
```

请参阅配置透明模式接口，第 13-8 页，以配置 BVI 接口并将常规接口关联到此网桥组。

步骤 4　将此接口与 VTEP 源接口相关联：

vtep-nve 1

步骤 5　为接口命名：

nameif *vni_interface_name*

示例：

```
ciscoasa(config-if)# nameif vxlan1000
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。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，因为该命令会导致删除所有引用该名称的命令。

步骤 6　（路由模式）分配 IPv4 和/或 IPv6 地址：

ip address {*ip_address* [*mask*] [**standby** *ip_address*] | **dhcp** [**setroute**] | **pppoe** [**setroute**]}

ipv6 address {**autoconfig** | *ipv6-address/prefix-length* [**standby** *ipv6-address*]}

示例：

```
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

步骤 7　设置安全级别：

security-level *level*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 为 0 （最低）到 100 （最高）之间的整数。

步骤 8　（单情景模式）设置组播组地址：

mcast-group *multicast_ip*

示例：

```
ciscoasa(config-if)# mcast-group 236.0.0.100
```

如果没有为 VNI 接口设置组播组，请使用源自 VTEP 源接口配置的默认组 （如果有）。如果手动设置 VTEP 源接口的 VTEP 对等体 IP，则无法为 VNI 接口指定组播组。多情景模式下不支持组播。

（可选）更改 VXLAN UDP 端口

默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。如果网络使用非标准端口，可以对其进行更改。

准备工作

对于多情景模式，请在系统执行空间中完成此任务。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。

操作步骤

步骤 1　设置 VXLAN UDP 端口：

vxlan port *number*

示例：

```
ciscoasa(config)# vxlan port 5678
```

监控 VXLAN 接口

参阅以下命令，以监控 VTEP 和 VNI 接口。

- **show nve** [*id*] [**summary**]

  此命令显示 NVE 接口的参数、状态和统计信息，其载频接口 （源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。使用 **summary** 选项，此命令仅显示 NVE 接口的状态、NVE 接口后 VNI 的数量，以及所发现的 VTEP 数量。

  请参阅以下所示的 **show nve 1** 命令输出：

```
ciscoasa# show nve 1
ciscoasa(config-if)# show nve
nve 1, source-interface "inside" is up
IP address 15.1.2.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
6701004 packets input, 3196266002 bytes
6700897 packets output, 3437418084 bytes
1 packets dropped
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP 地址 15.1.2.3
Number of VNIs attached to nve 1: 2
VNIs attached:
vni 2: segment-id 5002, mcast-group 239.1.2.3
vni 1: segment-id 5001, mcast-group 239.1.2.3
```

  请参阅以下所示的 **show nve 1 summary** 命令输出：

```
ciscoasa# show nve 1 summary
nve 1, source-interface "inside" is up
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Default multicast group: 239.1.2.3
Number of VNIs attached to nve 1: 2
```

- **show interface vni** *id* [**summary**]

  此命令显示 VNI 接口的参数、状态和统计信息，其桥接接口 （如果已配置）的状态，以及与其关联的 NVE 接口。**summary** 选项仅显示 VNI 接口参数。

  请参阅以下所示的 **show interface vni 1** 命令输出：

```
ciscoasa# show interface vni 1
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group 239.1.3.3
Traffic Statistics for "vni-inside":
235 packets input, 23606 bytes
524 packets output, 32364 bytes
14 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 2 bytes/sec
1 minute drop rate, 0 pkts/sec
```

```
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
```

请参阅以下所示的 **show interface vni 1 summary** 命令输出：

```
ciscoasa# show interface vni 1 summary
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group not configured
```

- **show vni vlan-mapping**

  此命令显示 VNI 网段 ID 和 VLAN 接口或物理接口之间的映射。此命令仅在透明防火墙模式下有效，因为在路由模式下， VXLAN 和 VLAN 之间的映射可能会显示过多的值。

  请参阅以下所示的 **show vni vlan-mapping** 命令输出：

```
ciscoasa# show vni vlan-mapping
vni1: segment-id: 6000, interface: 'g0110', vlan 10, interface: 'g0111', vlan 11
vni2: segment_id: 5000, interface: 'g01100', vlan 1, interface: 'g111', vlan 3,
interface: 'g112', vlan 4
```

- **show arp vtep-mapping**

  此命令可显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。

  请参阅以下所示的 **show arp vtep-mapping** 命令输出：

```
ciscoasa# show arp vtep-mapping
vni-outside 192.168.1.4 0012.0100.0003 577 15.1.2.3
vni-inside 192.168.0.4 0014.0100.0003 577 15.1.2.3
```

- **show mac-address-table vtep-mapping**

  在透明模式下，此命令显示带有远程 VTEP IP 地址的 VNI 接口上的第 2 层转发表 （MAC 地址表）。

  请参阅以下所示的 **show mac-address-table vtep-mapping** 命令输出：

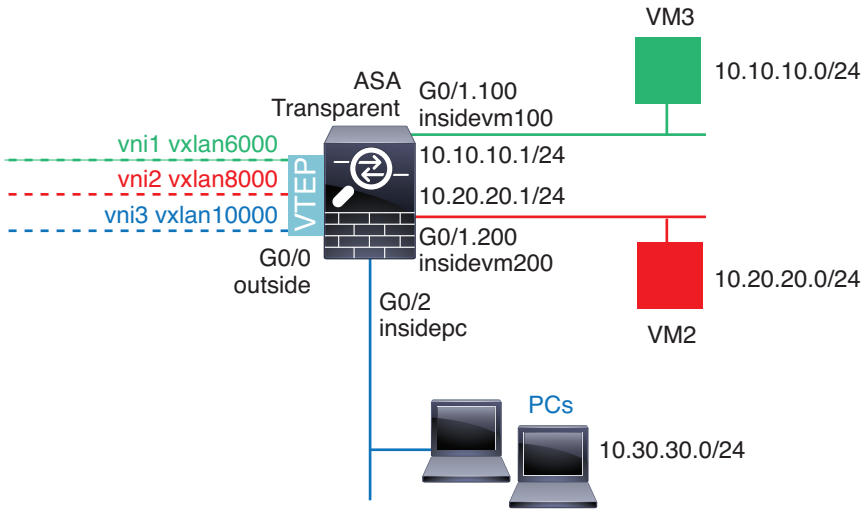
```
ciscoasa# show mac-address-table vtep-mapping
interface                  mac  address       type    Age(min)   bridge-group    VTEP
-------------------------------------------------------------------------------------
----------
vni-outside               00ff.9200.0000      dynamic      5          1      10.9.1.3
vni-inside                0041.9f00.0000      dynamic      5          1      10.9.1.3
```

VXLAN 接口示例

请参阅以下所示的 VXLAN 配置示例。

- 透明 VXLAN 网关示例，第 12-12 页
- VXLAN 路由示例，第 12-14 页

透明 VXLAN 网关示例



请参见以下有关此示例的说明：

- GigabitEthernet 0/0 上的外部接口用作 VTEP 源接口，并且连接到第 3 层网络。
- GigabitEthernet 0/1.100 上的 insidevm100 VLAN 子接口连接到 VM3 所在的 10.10.10.0/24 网络。当 VM3 与 VM1（未显示；两者均有 10.10.10.0/24 IP 地址）通信时，ASA 使用 VXLAN 标签 6000。
- GigabitEthernet 0/1.200 上的 insidevm200 VLAN 子接口连接到 VM2 所在的 10.20.20.0/24 网络。当 VM2 与 VM4（未显示；两者均有 10.20.20.0/24 IP 地址）通信时，ASA 使用 VXLAN 标签 8000。
- GigabitEthernet 0/2 上的 insidepc 接口连接到若干 PC 所在的 10.30.30.0/24 网络。当这些 PC 与属于同一网络（全部具有 10.30.30.0/24 IP 地址）的远程 VTEP 后面的 VM/PC（未显示）进行通信时，ASA 使用 VXLAN 标签 10000。

ASA 配置

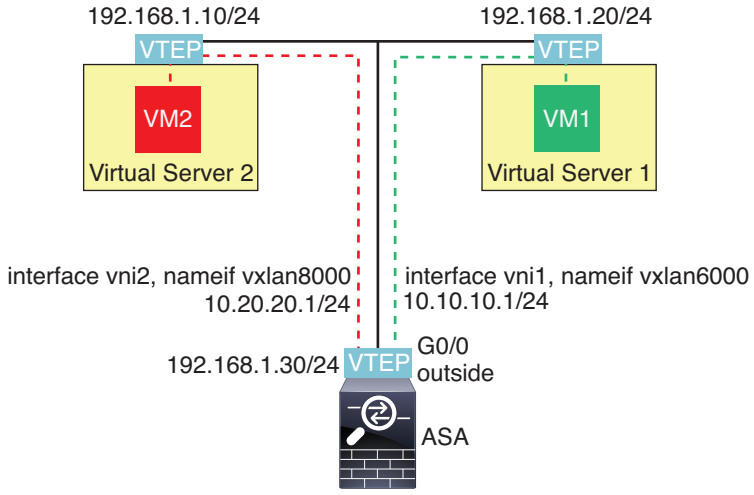
```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  bridge-group 1
  vtep-nve 1
  mcast-group 235.0.0.100
!
```

```
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  bridge-group 2
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface vni3
  segment-id 10000
  nameif vxlan10000
  security-level 0
  bridge-group 3
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface gigabitethernet0/1.100
  nameif insidevm100
  security-level 100
  bridge-group 1
!
interface gigabitethernet0/1.200
  nameif insidevm200
  security-level 100
  bridge-group 2
!
interface gigabitethernet0/2
  nameif insidepc
  security-level 100
  bridge-group 3
!
interface bvi 1
  ip address 10.10.10.1 255.255.255.0
!
interface bvi 2
  ip address 10.20.20.1 255.255.255.0
!
interface bvi 3
  ip address 10.30.30.1 255.255.255.0
```

备注

- 对于 VNI 接口 vni1 和 vni2，在封装过程中将删除内部 VLAN 标签。
- VNI 接口 vni2 和 vni3 通过组播共享封装的 ARP 的同一组播 IP 地址。系统允许此共享。
- ASA 基于以上 BVI 和网桥组配置，将 VXLAN 流量桥接到支持的非 VXLAN 接口。对于每个扩展的第 2 层网段 （10.10.10.0/24、 10.20.20.0/24 和 10.30.30.0/24）， ASA 充当网桥。
- 在网桥组中允许有多个 VNI 或多个常规接口 （VLAN 或仅物理接口）。VXLAN 网段 ID 与 VLAN ID （或物理接口）之间的转发或关联，由目标 MAC 地址和连接到目标的接口决定。
- VTEP 源接口是透明防火墙模式下，由接口配置中的 **nve-only** 所指示的第 3 层接口。VTEP 源接口不是 BVI 接口或管理接口，但是具有 IP 地址，并且使用路由表。

VXLAN 路由示例



请参见以下有关此示例的说明：

- VM1 (10.10.10.10) 通过虚拟服务器 1 进行托管，VM2 (10.20.20.20) 通过虚拟服务器 2 进行托管。
- VM1 的默认网关是 ASA，其与虚拟服务器 1 不在同一 POD，但是 VM1 并不知道该网关。VM1 只知道其默认网关 IP 地址为 10.10.10.1。同样， VM2 只知道其默认网关 IP 地址为 10.20.20.1。
- 虚拟服务器 1 和 2 上支持 VTEP 的虚拟机监控程序能够通过同一子网或通过第 3 层网络 （未显示；在这种情况下， ASA 和虚拟服务器的上行链路具有不同的网络地址）与 ASA 进行通信。
- VM1 的数据包将通过其虚拟机监控程序的 VTEP 进行封装，并通过 VXLAN 隧道发送到其默认网关。
- 当 VM1 将数据包发送到 VM2 时，对数据包而言，它将通过默认网关 10.10.10.1 进行发送。虚拟服务器 1 知道 10.10.10.1 不是本地地址，因此，VTEP 通过 VXLAN 封装数据包，并将该数据包发送到 ASA 的 VTEP。
- 数据包会在 ASA 中进行解封。在解封过程中可获取 VXLAN 网段 ID。紧接着， ASA 基于 VXLAN 网段 ID 将内部帧重新注入到相应的 VNI 接口 (vni1)。然后，ASA 进行路由查找，并通过另一个 VNI 接口 vni2 发送内部数据包。所有通过 vni2 的传出数据包都使用 VXLAN 网段 8000 进行封装，并通过 VTEP 发送到外部。
- 最终，虚拟服务器 2 的 VTEP 接收封装的数据包、解封数据包，并将数据包转发到 VM2。

ASA 配置

```
interface gigabitethernet0/0
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
  default-mcast-group 235.0.0.100
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
```

```
  vtep-nve 1
  ip address 10.20.20.1 255.255.255.0
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  vtep-nve 1
  ip address 10.10.10.1 255.255.255.0
!
```

VXLAN 接口的历史记录

表 12-1　　VXLAN 接口的历史记录

功能名称	版本	功能信息
VXLAN 支持	9.4(1)	增加了 VXLAN 支持，包括 VXLAN 隧道终端 (VTEP) 支持。每个 ASA 或安全情景可以定义一个 VTEP 源接口。 引入了以下命令：**debug vxlan**、 **default-mcast-group**、 **encapsulation vxlan**、 **inspect vxlan**、 **interface vni**、 **mcast-group**、 **nve**、 **nve-only**、 **peer ip**、 **segment-id**、 **show arp vtep-mapping**、 **show interface vni**、 **show mac-address-table vtep-mapping**、**show nve**、**show vni vlan-mapping**、 **source-interface**、 **vtep-nve** 和 **vxlan port**



路由模式和透明模式接口

本章介绍在路由或透明防火墙模式下为所有型号完成接口配置的相关任务。

- 关于路由模式和透明模式接口，第 13-1 页
- 路由模式和透明模式接口准则，第 13-4 页
- 路由模式和透明模式接口的默认设置，第 13-5 页
- 配置路由模式接口，第 13-5 页
- 配置透明模式接口，第 13-8 页
- 配置 IPv6 寻址，第 13-12 页
- 监控路由模式和透明模式接口，第 13-13 页
- 路由模式和透明模式接口示例，第 13-14 页
- 路由模式和透明模式接口历史记录，第 13-15 页

备注 对于多情景模式，请在情景执行空间完成本节所述的任务。输入 **changeto context** *name* 命令以更改为要配置的情景。

关于路由模式和透明模式接口

当 ASA 处于路由防火墙模式 （默认）下时，每个接口都是需要在唯一子网上为其设置 IP 地址的第 3 层路由接口。所有透明模式接口都属于网桥组。

- 安全级别，第 13-1 页
- 透明模式下的网桥组，第 13-2 页
- PPPoE （仅路由模式），第 13-2 页
- 双 IP 堆栈 （IPv4 和 IPv6），第 13-3 页
- IPv6，第 13-3 页

安全级别

每个接口必须具有安全级别，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）分配至级别 100。而连接到互联网的外部网络可分配至级别 0。其他网络 （例如 DMZ）可指定为介于中间的级别。您可以将多个接口分配至同一安全级别。

级别控制以下行为：

- 网络访问 - 默认情况下，默许从安全级别较高的接口访问安全级别较低的接口 （出站）。较高安全级别接口上的主机可以访问较低安全级别接口上的任何主机。您可以通过将 ACL 应用于接口来限制访问。

  如果为相同安全接口启用通信，则默许这些接口可访问安全级别相同或较低的其他接口。

- 检测引擎 - 某些应用检测引擎取决于安全级别。对于安全级别相同的接口，检测引擎应用于任一方向的流量。
  - NetBIOS 检测引擎 - 仅应用于出站连接。
  - SQL*Net 检测引擎 - 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。
- 筛选 - HTTP(S) 和 FTP 筛选仅应用于出站连接 （从高安全级别到低安全级别）。

  如果您为相同安全接口启用通信，则可以筛选任一方向的流量。

- **established** 命令 - 如果已建立从高安全级别主机到低安全级别主机的连接，则此命令允许从低安全级别主机到高安全级别主机的返回连接。

  如果您为相同安全接口启用通信，则可以为两个方向配置 **established** 命令。

相关主题

允许相同安全级别通信，第 14-6 页

透明模式下的网桥组

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。网桥组的流量相互分离；一个网桥组的流量不会路由到思科 ASA 中的其他网桥组，并且流量必须先流出 ASA，然后再由外部路由器路由回 ASA 中的其他网桥组。虽然每个网桥组的桥接功能是独立的，但所有网桥组之间可共享很多其他功能。例如，所有网桥组都共享系统日志服务器或 AAA 服务器的配置。为完全分离安全策略，请在每个情景中对一个网桥组使用安全情景。每个情景或在单模式下至少需要一个网桥组。

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 （例如系统消息或 AAA 通信）的源地址。除网桥组管理地址外，还可以选择为某些型号配置管理接口；有关详细信息，请参阅管理接口，第 9-2 页。

PPPoE （仅路由模式）

PPPoE 将以太网和 PPP 两个广泛接受的标准结合在一起，可提供将 IP 地址分配至客户端系统的身份验证方法。PPPoE 客户端通常是通过 DSL 或电缆服务等远程宽带连接来连接到 ISP 的个人计算机。ISP 部署 PPPoE 的原因在于， PPPoE 支持使用其现有远程访问基础设施进行高速宽带访问，同时也更加便于客户使用。

PPPoE 提供在以太网网络上使用点对点协议 (PPP) 实施身份验证的标准方法。利用 PPPoE， ISP 可以对 IP 地址进行经过身份验证的分配。在此类实施中， PPPoE 客户端和服务器通过在 DSL 或其他宽带连接上运行的第 2 层网桥协议实现互连。

PPPoE 由以下两个主要阶段组成：

- 主动发现阶段 - 在此阶段， PPPoE 客户端查找 PPPoE 服务器 （称为访问集中器）。在此阶段会分配会话 ID 并建立 PPPoE 层。
- PPP 会话阶段 - 在此阶段，将协商 PPP 选项并执行身份验证。完成链路设置后， PPPoE 就将用作第 2 层封装方法，允许通过 PPPoE 报头中的 PPP 链路传输数据。

在系统初始化时， PPPoE 客户端通过交换一系列数据包与访问集中器建立会话。建立会话后，就将设置 PPP 链路，包括使用密码身份验证协议 (PAP) 进行身份验证。建立 PPP 会话后，每个数据包便会封装在 PPPoE 和 PPP 报头中。

双 IP 堆栈 （IPv4 和 IPv6）

思科 ASA 支持在接口上同时配置 IPv6 和 IPv4。您无需输入任何特殊命令来执行此操作；只需照常输入 IPv4 配置命令和 IPv6 配置命令即可。请确保配置一条同时适用于 IPv4 和 IPv6 的默认路由。

IPv6

本节包含有关如何配置 IPv6 的信息。

- IPv6 寻址，第 13-3 页
- 修改的 EUI-64 接口 ID，第 13-3 页
- 在透明模式下不支持的 IPv6 命令，第 13-4 页

IPv6 寻址

您可以为 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。对于透明模式，需要为每个网桥组配置该地址，而不是逐个接口进行配置。您还可以为管理接口配置全局 IPv6 地址。
- 链路本地 - 链路本地地址是只能在直连网络上使用的专用地址。路由器不使用链路本地地址转发数据包；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，例如地址解析和邻居发现。在透明模式下，由于链路本地地址仅在网段上可用，并且绑定到接口 MAC 地址，因此，因此需要逐个接口配置链路本地地址。

至少需要配置链路本地地址， IPv6 才会起作用。如果配置全局地址，则接口上会自动配置链路本地地址，因此无需另外专门配置链路本地地址。如果不配置全局地址，则需要自动或手动配置链路本地地址。

备注　如果希望仅配置链路本地地址，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。

修改的 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）的接口标识符部分的长度为 64 位，并以修改的 EUI-64 格式进行构造。ASA 可为连接到本地链路的主机执行该要求。

在接口上启用此功能时，该接口接收的 IPv6 数据包源地址根据源 MAC 地址进行验证，以确保接口标识符使用修改的 EUI-64 格式。如果 IPv6 数据包不将修改的 EUI - 64 格式用于接口标识符，则会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会执行地址格式验证。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。从路由器背后的主机接收的数据包将无法通过地址格式验证，且会被丢弃，因为其源 MAC 地址将是路由器 MAC 地址，而不是主机 MAC 地址。

在透明模式下不支持的 IPv6 命令

以下 IPv6 命令在透明防火墙模式下不受支持，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**

路由模式和透明模式接口准则

情景模式

- 在多情景模式下，您只能配置已根据配置多情景，第 6-14 页分配给系统配置中的情景的情景接口。
- 在多情景模式下不支持 PPPoE。
- 对于透明模式下的多情景模式，每个情景必须使用不同的接口；不能跨情景共享接口。
- 对于透明模式下的多情景模式，每个情景通常使用不同子网。您可以使用重叠子网，但是从路由角度而言，需要路由器和 NAT 配置才能实现网络拓扑。

故障切换

请勿采用本章中的程序配置故障切换接口。要配置故障切换和状态链路，请参阅第 7 章 “通过故障切换实现高可用性”。

IPv6

ASA 不支持 IPv6 任播地址。

型号支持

ASASM 上不支持 PPPoE 和 DHCP。

ASASM 的 VLAN ID

您可以向配置中添加任何 VLAN ID，但是，只有通过交换机分配至 ASA 的 VLAN 才能传递流量。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，接口将更改为启动状态。有关接口状态的详细信息，请参阅 **show interface** 命令。

透明模式准则

- 您可以在单情景模式下或在多情景模式下的每个情景中配置最多 250 个网桥组。请注意，您必须至少使用 1 个网桥组；数据接口必须属于网桥组。
- 每个网桥组可包括最多 4 个接口。
- 对于 IPv4，每个网桥组都需要一个管理 IP 地址，以用于管理流量和使流量通过 ASA。
- 管理 IP 地址必须与已连接网络位于同一子网上。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。
- 透明模式下的管理接口不支持 PPPoE。

路由模式和透明模式接口的默认设置

默认安全级别

默认安全级别为 0。如果将一个接口指定为 “inside”，且未明确设置安全级别，则 ASA 将安全级别设置为 100。

备注　如果更改接口的安全级别，且不希望等待现有连接超时后才使用新安全信息，则可使用 **clear local-host** 命令清除连接。

配置路由模式接口

要配置路由模式接口，请执行以下步骤：

步骤 1　配置常规路由模式接口参数，第 13-5 页。

步骤 2　配置 PPPoE，第 13-7 页。

步骤 3　配置 IPv6 寻址，第 13-12 页。

配置常规路由模式接口参数

此程序介绍如何设置名称、安全级别、 IPv4 地址和其他选项。

准备工作

在多情景模式下，请在情景执行空间中完成本程序。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　进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

接口 ID 可以是：

- **redundant**
- **port-channel**
- *physical* - 例如， **ethernet**、**gigabitethernet**、**tengigabitethernet**、**management**。请参阅您的型号的硬件安装指南以获取接口名称。
- *physical.subinterface* - 例如， **gigabitethernet0/0.100**。
- **vni**
- **vlan**
- *mapped_name* - 适用于多情景模式。

步骤 2　为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。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，因为该命令会导致删除所有引用该名称的命令。

步骤 3　使用以下其中一种方法设置 IP 地址。

- 手动设置 IP 地址：

  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
  ```

  注意　如果您使用故障切换，则必须手动设置 IP 地址和备用地址；不支持 DHCP 和 PPPoE。

  ip_address 和 *mask* 参数分别用于设置接口 IP 地址和子网掩码。

  standby *ip_address* 参数用于故障切换。

- 从 DHCP 服务器获取 IP 地址。

  ip address dhcp [**setroute**]

  示例：

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  借助于关键字 **setroute**， ASA 可使用 DHCP 服务器提供的默认路由。

  重新输入此命令，以重置 DHCP 租用并请求新的租用。

  如果不是在使用 **no shutdown** 命令启用接口后再输入 **ip address dhcp** 命令，则可能不会发送某些 DHCP 请求。

- 从 PPPoE 服务器获取 IP 地址：

  ip address pppoe [**setroute**]

  示例：

  ```
  ciscoasa(config-if)# ip address pppoe setroute
  ```

  或者，您可以通过手动输入 IP 地址来启用 PPPoE：

  ip address *ip_address mask* **pppoe**

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.78 255.255.255.0 pppoe
  ```

  setroute 选项用于在 PPPoE 客户端尚未建立连接时设置默认路由。当使用 **setroute** 选项时，在配置中不能有静态定义的路由。

  注意　如果在两个接口上启用 PPPoE （例如主接口和备用接口），并且不配置双 ISP 支持，则 ASA 只能通过第一个接口发送流量来获取 IP 地址。

步骤 4　设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 是介于 0 （最低）和 100 （最高）之间的整数。 .

步骤 5　（可选）将接口设置为管理专属模式，以便其不允许流量通过。

management-only

默认情况下，管理接口配置为管理专属。除 ASA 5585-X 以外，您无法在管理接口上禁用 **management-only**。

management-only 命令不支持用于冗余接口。

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下为情景配置进行参数配置。接口 ID 是一个映射名称。

```
ciscoasa/contextA(config)# interface int1
ciscoasa/contextA(config-if)# nameif outside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
```

相关主题

- 配置 MTU 和 TCP MSS，第 14-5 页
- 配置 IPv6 寻址，第 13-12 页
- 启用物理接口和配置以太网参数，第 9-6 页
- 配置 PPPoE，第 13-7 页

配置 PPPoE

如果使用 PPPoE 进行 IP 寻址，请配置用于向访问集中器进行 ASA 身份验证的用户名和密码。

操作步骤

步骤 1　定义要用于 PPPoE 的 VPDN 组：

vpdn group *group_name* **request dialout pppoe**

示例：

```
ciscoasa(config)# vpdn group pppoe-sbc request dialout pppoe
```

步骤 2　如果 ISP 要求身份验证，请选择身份验证协议：

vpdn group *group_name* **ppp authentication** {**chap** | **mschap** | **pap**}

示例：

```
ciscoasa(config)# vpdn group pppoe-sbc ppp authentication chap
```

针对 ISP 所使用的身份验证类型输入相应的关键字：

使用 CHAP 或 MS-CHAP 时，用户名可能是指远程系统名称，而密码可能是指 CHAP 密钥。

步骤 3　将 ISP 分配的用户名关联到 VPDN 组：

vpdn group *group_name* **localname** *username*

示例：

```
ciscoasa(config)# vpdn group pppoe-sbc localname johncrichton
```

步骤 4　为 PPPoE 连接创建用户名和密码对：

vpdn username *username* **password** *password* [**store-local**]

示例：

```
ciscoasa(config)# vpdn username johncrichton password moya
```

store-local 选项可将用户名和密码存储在 ASA 上的 NVRAM 中的特殊位置；如果某自动更新服务器将 **clear config** 命令发送到 ASA，然后连接中断，则 ASA 可以从 NVRAM 读取用户名和密码，并向访问集中器重新进行身份验证。

配置透明模式接口

要配置网桥组和关联接口，请执行以下步骤。

步骤 1　配置网桥组，第 13-8 页。

步骤 2　配置常规透明模式接口参数，第 13-9 页。

步骤 3　配置管理接口，第 13-10 页。

步骤 4　配置 IPv6 寻址，第 13-12 页。

配置网桥组

每个网桥组都需要一个管理 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 地址必须与已连接网络位于同一子网上。对于 IPv4 流量，需要管理 IP 地址来传递任何流量。对于 IPv6 流量，您必须至少配置链路本地地址以传递流量，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。

备注　对于单独的管理接口 （适用于受支持的型号），会向配置中自动添加无法配置的网桥组 (ID 301)。此网桥组未包含在网桥组限制中。

操作步骤

步骤 1　创建网桥组：

interface bvi *bridge_group_number*

示例：

```
ciscoasa(config)# interface bvi 1
```

bridge_group_number 是介于 1 和 250 之间的整数。

步骤 2　指定网桥组的管理 IP 地址：

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
```

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（分别用于上游路由器、下游路由器和透明防火墙）的其他子网，例如 /30 子网 (255.255.255.252)。ASA 将所有 ARP 数据包丢弃到子网中的第一个和最后一个地址或从中丢弃所有 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 会将 ARP 请求从下游路由器丢弃到上游路由器。

standby 关键字和地址用于故障切换。

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
```

配置常规透明模式接口参数

本程序介绍如何为每个透明接口设置名称、安全级别和网桥组。

准备工作

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入 **changeto context** *name* 命令。
- 请勿对管理接口执行此程序；要配置管理接口，请参阅配置管理接口，第 13-10 页。

操作步骤

步骤 1　进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

接口 ID 可以是：

- **redundant**
- **port-channel**
- *physical* - 例如，**ethernet**、**gigabitethernet**、**tengigabitethernet**、**management**。请参阅您的型号的硬件安装指南以获取接口名称。
- *physical*.*subinterface* - 例如， **gigabitethernet0/0.100**。
- **vni**
- **vlan**
- *mapped_name* - 适用于多情景模式。

步骤 2　向网桥组分配接口：

bridge-group *number*

示例：

```
ciscoasa(config-if)# bridge-group 1
```

number 是介于 1 和 100 之间的整数。最多可将四个接口分配到网桥组。您不能将同一接口分配至多个网桥组。

步骤 3　为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。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，因为该命令会导致删除所有引用该名称的命令。

步骤 4　设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 是介于 0 （最低）和 100 （最高）之间的整数。

配置管理接口

您可以在单情景模式下或每个情景中配置一个与网桥组接口分离的管理接口。

准备工作

- 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。此网桥组未包含在网桥组限制中。
- 如果您的型号不包含管理接口，则必须从数据接口管理透明防火墙；请跳过此程序。（例如，在 ASASM 上。）
- 在多情景模式下，您无法跨情景共享任何接口，包括管理接口。您必须连接到数据接口。

- 在多情景模式下，请在情景执行空间中完成本程序。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　进入接口配置模式：

interface {{**port-channel** *number* | **management** *slot*/*port*}[.*subinterface*] | *mapped_name*}

示例：

```
ciscoasa(config)# interface management 0/0.1
```

port-channel *number* 参数是 EtherChannel 接口 ID，例如 **port-channel 1**。EtherChannel 接口只能拥有管理成员接口。

冗余接口不支持管理*插槽*/*端口*接口作为成员。您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。

在多情景模式下，如已使用 **allocate-interface** 命令分配一个接口，请输入 *mapped_name* 命令。

步骤 2　为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif management
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。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，因为该命令会导致删除所有引用该名称的命令。

步骤 3　使用以下其中一种方法设置 IP 地址。

- 手动设置 IP 地址：

  要用于故障切换，您必须手动设置 IP 地址和备用地址；不支持 DHCP。

  ip_address 和 *mask* 参数分别用于设置接口 IP 地址和子网掩码。

  standby *ip_address* 参数用于故障切换。

  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
  ```

- 从 DHCP 服务器获取 IP 地址。

  ip address dhcp [**setroute**]

  示例：

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  借助于关键字 **setroute**， ASA 可使用 DHCP 服务器提供的默认路由。

  重新输入此命令，以重置 DHCP 租用并请求新的租用。

  如果不是在使用 **no shutdown** 命令启用接口后再输入 **ip address dhcp** 命令，则可能不会发送某些 DHCP 请求。

步骤 4　设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 100
```

number 是介于 0 （最低）和 100 （最高）之间的整数。

相关主题

管理接口，第 9-2 页

配置 IPv6 寻址

要为任何路由模式接口以及为透明模式网桥组接口和管理接口配置全局 IPv6 地址，请执行以下步骤。

备注　配置全局地址将自动配置链路本地地址，因此无需单独对其进行配置。

备注　要配置 IPv6 邻居发现，请参阅第 27 章 “IPv6 邻居发现”。

准备工作

在多情景模式下，请在情景执行空间中完成本程序。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　进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

在透明模式下，指定网桥组或管理接口。

示例：

```
ciscoasa(config)# interface bvi 1
```

步骤 2　使用以下其中一种方法设置 IP 地址。

- （仅限路由模式）在接口上启用无状态自动配置：

  ipv6 address autoconfig

  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 自动生成接口的链路本地地址。

注意　尽管 RFC 4862 明确要求配置为无状态自动配置的主机不发送路由器通告消息，但在此情况下， ASA 确实会发送路由器通告消息。要抑制消息，请参阅 **ipv6 nd suppress-ra** 命令。

- 向接口分配全局地址：

  ipv6 address *ipv6-address/prefix-length* [**standby** *ipv6-address*]

  示例：

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
  ```

  分配全局地址时，将自动为接口创建链路本地地址。

  standby 指定由辅助设备或故障切换对中的故障切换组使用的接口地址。

- （仅限路由模式）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，向接口分配全局地址。

  ipv6 address *ipv6-prefix/prefix-length* **eui-64**

  示例：

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98::/48 eui-64
  ```

  分配全局地址时，将自动为接口创建链路本地地址。

  您无需指定备用地址；系统将自动生成接口 ID。

步骤 3　（可选）在本地链路上的 IPv6 地址中，强制使用修改的 EUI-64 格式的接口标识符。

ipv6 enforce-eui64 *if_name*

示例：

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

if_name 参数即是 **nameif** 命令指定的接口名称，可对该名称启用地址格式执行。

监控路由模式和透明模式接口

您可以监控接口统计信息、状态、 PPPoE 。

- 接口统计信息，第 13-13 页
- PPPoE，第 13-14 页

接口统计信息

- **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。

PPPoE

- **show ip address** *interface_name* **pppoe**

  显示当前 PPPoE 客户端配置信息。

- **debug pppoe {event | error | packet}**

  启用 PPPoE 客户端调试。

- **show vpdn session [l2tp | pppoe] [id** *sess_id* **| packets | state | window]**

  查看 PPPoE 会话的状态。

  以下示例显示此命令提供的信息：

```
ciscoasa# show vpdn

Tunnel id 0, 1 active sessions
     time since change 65862 secs
     Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
     6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
     Session state is SESSION_UP
       Time since event change 65865 secs, interface outside
       PPP interface id is 1
       6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
```

路由模式和透明模式接口示例

以下透明模式示例包括两个网桥组，每组三个接口，以及一个管理专属接口：

```
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
```

路由模式和透明模式接口历史记录

表 13-1　　透明模式下的接口历史记录

功能名称	平台版本	功能信息
透明模式的 IPv6 支持	8.2(1)	为透明防火墙模式引入了 IPv6 支持。
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。网桥组流量相互分隔。在单情景模式或每个情景中最多可配置八个网桥组，每组四个接口。 引入了以下命令：**interface bvi** 和 **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 个增加到 250 个网桥组。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。 修改了以下命令：**interface bvi** 和 **bridge-group**。



高级接口配置

本章介绍如何为接口配置 MAC 地址，如何设置最大传输单元 (MTU)，如何设置最大 TCP 分片大小 (TCP MSS)，以及如何允许相同安全级别通信。设置正确的 MTU 和最大 TCP 分片大小是实现最佳网络性能的关键。

- 关于高级接口配置，第 14-1 页
- 配置 MAC 地址，第 14-5 页
- 配置 MTU 和 TCP MSS，第 14-5 页
- 允许相同安全级别通信，第 14-6 页

备注 对于多情景模式，请在情景执行空间完成本节所述的任务。输入 **changeto context** *name* 命令以更改为要配置的情景。

关于高级接口配置

本节介绍高级接口设置。

- 关于 MAC 地址，第 14-1 页
- 关于 MTU，第 14-2 页
- 关于 TCP MSS，第 14-3 页
- 接口间通信，第 14-3 页
- 接口间通信 （路由防火墙模式），第 14-4 页

关于 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。

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首个物理接口的 MAC 地址。如果更改配置中成员接口的顺序，则 MAC 地址会更改以匹配目前列出的第一个接口的 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。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。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。在多情景模式下，您可以将唯一 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更改的情况下，我们建议手动或在多情景模式下自动配置唯一 MAC 地址。如果删除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址会更改为下一个编号最小的接口，从而导致流量中断。

在多情景模式下，如果在情景之间共享接口，则可以将唯一 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。尽管可以使用不具有唯一 MAC 地址的共享接口，但有一些限制。您可以手动分配每个 MAC 地址，或者为情景中的共享接口自动生成 MAC 地址。如果自动生成 MAC 地址，则可以使用本程序覆盖生成的地址。

对于单情景模式，或者多情景模式下不共享的接口，您可能想要给子接口分配唯一 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。

相关主题

- ASA 如何对数据包进行分类，第 6-3 页
- 自动将 MAC 地址分配给情景接口，第 6-21 页

关于 MTU

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 标签的帧大小。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 标签（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。

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。

备注　只要有内存空间， ASA 就可接收大于所配置的 MTU 的帧。

- 默认 MTU，第 14-2 页
- 路径 MTU 发现，第 14-2 页
- MTU 和巨帧，第 14-3 页

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 标签等的 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。

MTU 和巨帧

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。
- 适应巨帧 - 如果启用巨帧，最多可以将 MTU 设置为 9198 字节。

关于 TCP MSS

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。

您可以在 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 会假定 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，第 14-3 页
- VPN 和非 VPN 流量的 TCP MSS，第 14-3 页

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。

VPN 和非 VPN 流量的 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，如果使用巨帧并将 MTU 设置为较大的值，则需要将 TCP MSS 设置为符合新的 MTU。

接口间通信

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，则仅可以为每个级别 （0 到 100）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。

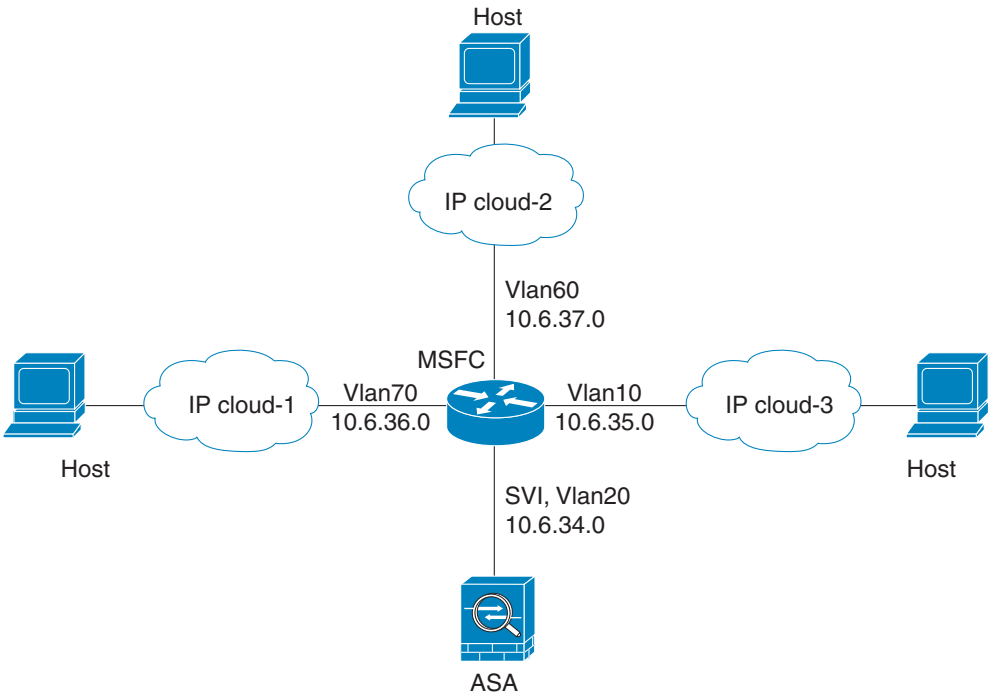
如果启用同一安全级别接口通信，则仍可以照常配置不同安全级别的接口。

接口间通信（路由防火墙模式）

接口间通信可能对从某一接口流入、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，流量必须先流入 ASA，然后流出，再流入另一个分支节点。

备注　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 的非对称路由情况。

对于 ASASM，在启动此功能之前，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。下图显示了同一接口上的主机需要在其上进行通信的网络。



以下示例配置显示了思科 IOS **route-map** 命令，它们用于在图中显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
```

配置 MAC 地址

如果需要手动分配 MAC 地址，可以使用本程序完成。

准备工作

在多情景模式下，请在情景执行空间中完成本程序。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　进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

步骤 2　向此接口分配专用 MAC 地址：

mac-address *mac_address* [**standby** *mac_address*]

示例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

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 以 000C.F142.4CDE 的形式输入。

如果您还要使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。

如需与故障切换配合使用，请设置**备用** MAC 地址。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

配置 MTU 和 TCP MSS

准备工作

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入 **changeto context** *name* 命令。
- 要将 MTU 增加到 1500 以上，请按照启用巨帧支持，第 9-7 页启用巨帧。在 ASASM 上，巨帧默认受支持；无需启用它们。

操作步骤

步骤 1　将 MTU 设置在 300 到 9198 字节之间 （对于 ASAv，设为 9000）。

mtu *interface_name bytes*

示例：

```
ciscoasa(config)# mtu inside 9200
```

默认值为 1500 字节。

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。

对于支持巨帧的型号，如果为任何接口输入的值大于 1500，则需启用巨帧支持。请参阅启用巨帧支持，第 9-7 页。

步骤 2　以字节为单位设置 TCP 最大分片大小，范围在 48 和任何最大值之间：

```
sysopt connection tcpmss [minimum] bytes
```

示例：

```
ciscoasa(config)# sysopt connection tcpmss 8500
ciscoasa(config)# sysopt connection tcpmss minimum 1290
```

默认值为 1380 字节。您可以禁用此功能，只需将字节数设置为 **0**。

对于 **minimum** 关键字，请将最大分片大小设置为不小于 48 和 65535 之间的*字节数*。默认情况下， minimum 功能已禁用 （设置为 0）。

示例

以下示例将启用巨帧、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
```

以下示例将启用巨帧、增加所有接口上的 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
```

允许相同安全级别通信

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。

操作步骤

步骤 1　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 inter-interface
```

步骤 2　启用连接到同一接口的主机之间的通信：

```
same-security-traffic permit intra-interface
```



流量区域

您可以向*流量区域*分配多个接口，让现有流中的流量在该区域内的任何接口流出或流入 ASA。此功能允许 ASA 上的等价多路径 (ECMP) 路由以及多个接口分担流向 ASA 的外部流量负载均衡。

- 关于流量区域，第 15-1 页
- 流量区域的前提条件，第 15-7 页
- 流量区域准则，第 15-8 页
- 配置流量区域，第 15-9 页
- 监控流量区域，第 15-10 页
- 流量区域示例，第 15-12 页
- 流量区域历史记录，第 15-14 页

关于流量区域

本节介绍应如何使用网络中的流量区域。

- 未划分区域的行为，第 15-2 页
- 为什么使用区域？第 15-2 页
- 每区域连接和路由表，第 15-4 页
- ECMP 路由，第 15-4 页
- 基于接口的安全策略，第 15-5 页
- 流量区域支持的服务，第 15-6 页
- 安全级别，第 15-6 页
- 流量的主接口和当前接口，第 15-6 页
- 加入或离开区域，第 15-6 页
- 区域内流量，第 15-6 页
- 流向设备的流量和流出设备的流量，第 15-6 页
- 区域中的重叠 IP 地址，第 15-7 页

未划分区域的行为

自适应安全算法在决定是允许还是拒绝流量时会考虑数据包的状态。流量的执行参数之一是流入和流出同一端口的流量。任何流入其他接口的现有流量都将被 ASA 丢弃。

通过流量区域，您可以将多个接口集合在一起，这样流入或流出区域中*任意*接口的流量都将执行自适应安全算法安全检查。

相关主题

状态检测概述，第 1-10 页

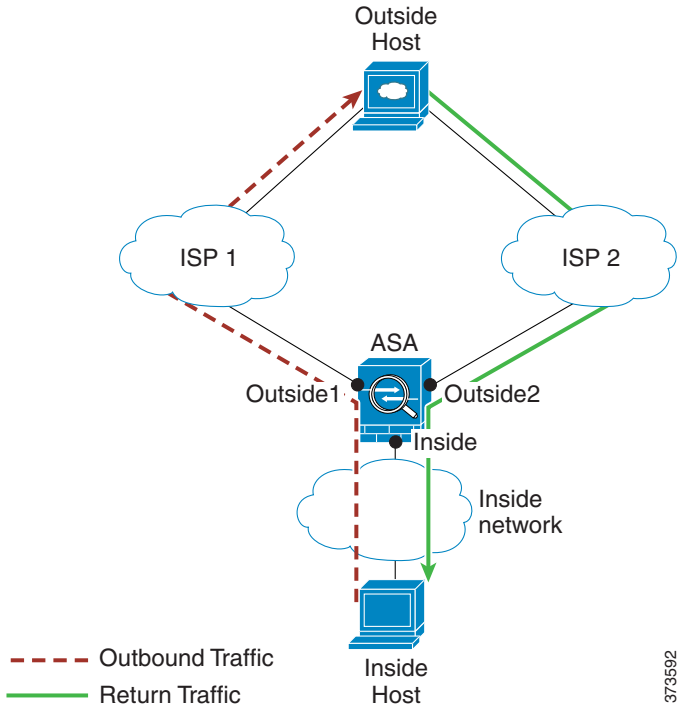
为什么使用区域？

您可以使用区域来支持几种路由情景。

- 非对称路由，第 15-2 页
- 丢失的路由，第 15-3 页
- 负载均衡，第 15-4 页

非对称路由

在以下场景中，通过 Outside1 接口上的 ISP 1 在内部主机和外部主机之间建立了连接。由于目标网络上的非对称路由，从 Outside2 接口上的 ISP 2 返回已到达的流量。

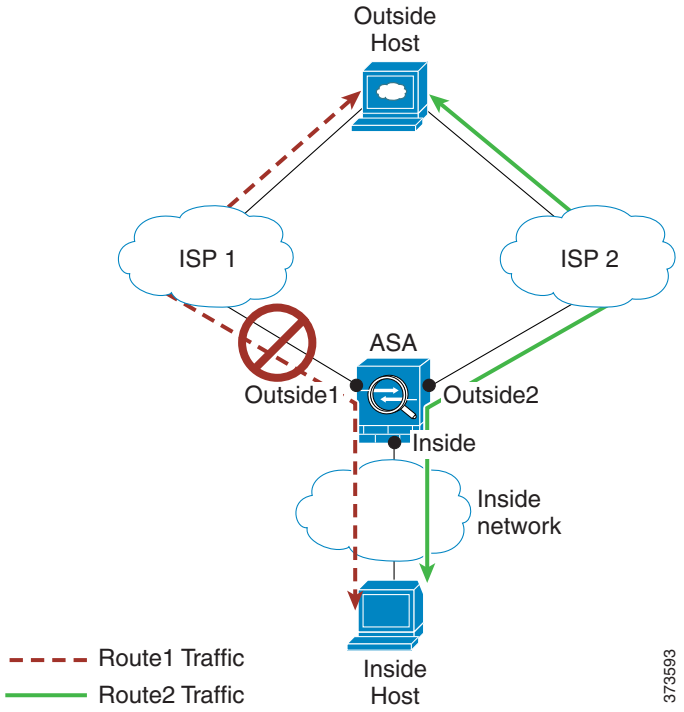


因未划分区域出现的问题：ASA 针对每个接口维护连接表。返回到达 Outside2 的流量时，它不会匹配连接表，并且将被丢弃。

通过划分区域解决问题：ASA 针对每个区域维护连接表。如果您将 Outside1 和 Outside2 集合到一个区域中，当返回到达 Outside2 的流量时，它将匹配每区域连接表，并且允许连接。

丢失的路由

在以下场景中，通过 Outside1 接口上的 ISP 1 在内部主机和外部主机之间建立了连接。由于 Outside1 和 ISP 1 之间的路由已丢失或移动，流量需要通过 ISP 2 采取不同的路由。

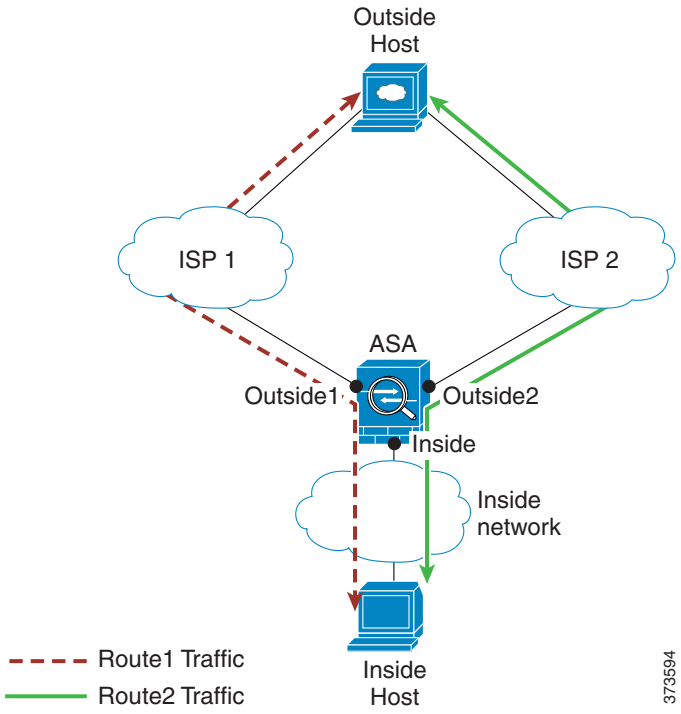


因未划分区域出现的问题：内部主机和外部主机之间的连接将被删除；您必须使用新的次优路由建立新连接。对于 UDP，新路由将在单次丢包之后使用；但对于 TCP，需要重新建立新连接。

通过划分区域解决问题：ASA 检测到丢失的路由，并通过 ISP2 将流量切换到新路径。流量将被无缝转发，无任何丢包现象。

负载均衡

在以下场景中，通过 Outside1 接口上的 ISP 1 在内部主机和外部主机之间建立了连接。借助通过 Outside2 上的 ISP 2 的等价路由建立了第二个连接。



因未划分区域出现的问题：无法进行跨接口负载均衡；您只能在一个接口上通过等价路由进行负载均衡。

通过划分区域解决问题：ASA 在区域中的所有接口上跨最多 8 个等价路由对连接进行负载均衡。

每区域连接和路由表

ASA 维护每区域连接表，使流量能够到达任何一个区域接口。此外，ASA 还维护每区域路由表，提供 ECMP 支持。

ECMP 路由

ASA 支持等价多路径 (ECMP) 路由。

- 未划分区域的 ECMP 支持，第 15-5 页
- 划分区域的 ECMP 支持，第 15-5 页
- 如何对连接进行负载均衡，第 15-5 页
- 回退到另一区域中的路由，第 15-5 页

未划分区域的 ECMP 支持

如果没有区域，每个接口最多支持 3 个等价静态或动态路由。例如，您可以在指定不同网关的外部接口上配置三个默认路由：

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

在这种情况下，流量在外部接口上的 10.1.1.2、 10.1.1.3 和 10.1.1.4 之间进行负载均衡。流量基于散列源和目标 IP 地址的算法在指定网关之间进行分发。

不支持跨多个接口执行 ECMP，因此您不能在不同接口上定义到同一目标的路由。使用上述任一路由配置时，不允许使用以下路由：

```
route outside2 0 0 10.2.1.1
```

划分区域的 ECMP 支持

如果有区域，在一个区域中最多可以跨 8 个接口配置最多 8 个等价静态或动态路由。例如，您可以在区域中跨三个接口配置三个默认路由：

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

同样，动态路由协议可以自动配置等价路由。ASA 使用更稳健的负载均衡机制跨接口对流量进行负载均衡。

当某条路由丢失时， ASA 将流量无缝移至其他路由。

如何对连接进行负载均衡

ASA 可以使用数据包六元组 （源和目标 IP 地址、源和目标端口、协议和入口接口）构成的散列跨等价路由对连接进行负载均衡。除非路由丢失，否则连接将在其持续时间内在所选接口上保持不中断的状态。

连接中的数据包不会跨路由进行负载均衡；连接只使用一个路由，除非此路由丢失。

ASA 执行负载均衡时，不考虑接口带宽或其他参数。您应确保同一区域中的所有接口都有相同的特性，例如 MTU、带宽等。

用户不能配置负载均衡算法。

回退到另一区域中的路由

当路由在某个接口上丢失时，如果区域中没有其他路由可用，则 ASA 将使用来自其他接口/区域的路由。如果使用此备用路由，可能会发生丢包现象，就像使用未划分区域的路由支持一样。

基于接口的安全策略

区域允许流量进出区域中的任何接口，但安全策略 （访问规则、 NAT 等）本身仍然应用于每个接口，而非每个区域。如果为区域中的所有接口配置相同的安全策略，则可对该流量成功实施 ECMP 和负载均衡。有关所需并行接口配置的详细信息，请参阅流量区域的前提条件，第 15-7 页。

流量区域支持的服务

区域支持以下服务：

- 访问规则
- NAT
- 服务规则， QoS 流量管制除外。
- 路由

虽然没有完整的划分区域支持，但您还可以配置流向设备的流量和流出设备的流量，第 15-6 页中列出的流向设备服务和流出设备服务。

请勿为流量区域中的接口配置其他服务 （例如， VPN 或 Botnet 流量过滤器）；它们可能不会按预期运行或扩展。

备注　有关如何配置安全策略的详细信息，请参阅流量区域的前提条件，第 15-7 页。

安全级别

添加到区域的第一个接口决定区域的安全级别。所有其他接口必须具有相同的安全级别。要更改区域中接口的安全级别，除了一个接口之外，所有其他接口都必须删除，然后更改安全级别，再重新添加接口。

流量的主接口和当前接口

每个连接流都是在初始入口和出口接口的基础上构建的。这些接口是*主*接口。

如果由于路由更改或非对称路由而使用新的出口接口，则新接口为*当前*接口。

加入或离开区域

将接口分配到区域时，该接口上的所有连接都会删除。必须重新建立连接。

如果从区域删除某个接口，以该接口为主接口的连接都会删除。必须重新建立连接。如果该接口是当前接口， ASA 会将连接移回主接口。区域路由表也会刷新。

区域内流量

要允许流量在同一区域中*流入*一个接口和*流出*另一个接口，请启用 **same-security permit intra-interface** 命令，此命令允许流量流入和流出同一接口，并启用 **same-security permit inter-interface** 命令，此命令允许在安全级别相同的接口之间路由流量。否则，流量不能在同一区域中的两个接口之间路由。

流向设备的流量和流出设备的流量

- 您不能向区域添加管理专用接口或管理访问接口。
- 对于区域中常规接口上的管理流量，仅支持对现有流量进行非对称路由；无 ECMP 支持。

- 您只能在一个区域接口上配置管理服务，但要利用非对称路由支持，需要在所有接口上配置管理服务。即使所有接口上的配置是并行的，也不支持 ECMP。
- ASA 支持在区域中运行以下流向设备服务和流出设备服务：
  - Telnet
  - SSH
  - HTTPS
  - SNMP
  - Syslog
  - BGP

区域中的重叠 IP 地址

对于未划分区域的接口，只要您正确配置 NAT， ASA 就支持接口上的重叠 IP 地址网络。但是，不支持同一区域中的接口上的重叠网络。

流量区域的前提条件

- 配置所有接口参数，包括名称、 IP 地址和安全级别。注意，安全级别必须匹配区域中的所有接口。您应根据带宽和其他第 2 层属性计划同类接口的集合。
- 配置以下服务以便在所有区域接口上匹配：
  - 访问规则 - 将同一访问规则应用到所有区域成员接口，或者使用全局访问规则。

    例如：

    ```
    access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
    access-group ZONE1 in interface outside1
    access-group ZONE1 in interface outside2
    access-group ZONE1 in interface outside3
    ```

  - NAT - 在区域的所有成员接口上配置相同的 NAT 策略，或者使用全局 NAT 规则（换句话说，使用 “any”表示 NAT 规则中的区域接口）。

    不支持接口 PAT。

    例如：

    ```
    object network WEBSERVER1
      host 10.9.9.9 255.255.255.255
      nat (inside,any) static 209.165.201.9
    ```

    注意　使用接口特定 NAT 和 PAT 池时， ASA 无法在原始接口发生故障的情况下切换连接。

    如果使用的是接口特定 PAT 池，则来自同一主机的多个连接可能会对不同接口进行负载均衡，并使用不同的映射 IP 地址。在此情况下，使用多个并发连接的互联网服务或许无法正确工作。

  - 服务规则 - 使用全局服务策略，或向区域中的每个接口分配相同策略。

    不支持 QoS 流量管制。

例如：

```
service-policy outside_policy interface outside1
service-policy outside_policy interface outside2
service-policy outside_policy interface outside3
```

注意　对于 VoIP 检测，区域负载均衡会造成无序数据包增加。发生这种情况的原因是，后面的数据包可能先于前面的采用不同路径的数据包到达 ASA。无序数据包的特征包括：

- 中间节点 （防火墙和 IDS）和接收端节点 （如果使用查询）上的内存利用率更高。
- 视频或语音质量差。

为减少这些影响，我们建议 IP 地址仅用于 VoIP 流量的负载分配。

- 配置路由时着眼于 ECMP 区域功能。

流量区域准则

防火墙模式

仅支持路由防火墙模式。不支持透明防火墙模式。

故障切换

- 您不能将故障切换或状态链路添加到区域。
- 在主用/主用故障切换模式下，您可以在每个情景中将接口分配给非对称路由 (ASR) 组。此服务允许在对等设备上的类似接口返回的流量恢复到原始设备。您无法在一个情景中同时配置 ASR 组和流量区域。如果在情景中配置一个区域，任何情景接口都不能属于 ASR 组。有关 ASR 组的详细信息，请参阅配置非对称路由数据包支持 （主用/主用模式），第 7-35 页。
- 仅将每个连接的主接口复制到备用设备；不复制当前接口。如果备用设备变为主用状态，它将根据需要分配一个新的当前接口。

群集

- 您不能将集群控制链路添加到区域。

其他准则

- 您最多可以创建 256 个区域。
- 您可以将以下类型的接口添加到区域：
  - 物理
  - VLAN
  - 以太网通道
  - 冗余
- 您不能添加以下类型的接口：
  - 管理专用
  - 管理访问
  - 故障切换或状态链路
  - 集群控制链路

  - EtherChannel 或冗余接口中的成员接口
  - VNI；此外，如果常规数据接口被标记为 nve-only，它不能成为区域的成员。
- 接口只能是一个区域的成员。
- 每个区域最多可包含 8 个接口。
- 对于 ECMP，在所有区域接口上，每个区域最多可以添加 8 个等价路由。您也可以将单个接口上的多个路由配置为 8 路由限制的一部分。

配置流量区域

配置已命名区域，并向该区域分配接口。

操作步骤

步骤 1　添加区域：

```
zone name
```

例如：

```
zone outside
```

区域名称的最大长度为 48 个字符。

步骤 2　向区域添加接口：

```
interface id
  zone-member zone_name
```

例如：

```
interface gigabitethernet0/0
  zone-member outside
```

步骤 3　向区域添加更多接口；确保它们与您添加的第一个接口具有相同的安全级别。

例如：

```
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

示例

以下示例配置具有 4 个成员接口的外部区域：

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

监控流量区域

本节介绍如何监控流量区域。

- 区域信息，第 15-10 页
- 区域连接，第 15-10 页
- 区域路由，第 15-11 页

区域信息

- **show zone** [*name*]

  显示区域 ID、情景、安全级别和成员。

  请参阅以下所示的 **show zone** 命令的输出：

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

- **show nameif zone**

  显示接口名称和区域名称。

  请参阅以下所示的 **show nameif zone** 命令的输出：

```
ciscoasa# show nameif zone
Interface               Name                    zone-name    Security
GigabitEthernet0/0      inside-1                inside-zone    100
GigabitEthernet0/1.21   inside                  inside-zone    100
GigabitEthernet0/1.31   4                                      0
GigabitEthernet0/2      outside                 outside-zone   0
Management0/0           lan                                    0
```

区域连接

- **show conn** [**long** | **detail**] [**zone** *zone_name* [**zone** *zone_name*] [...]]

  show conn zone 命令可显示区域的连接。**long** 和 **detail** 关键字可显示用于构建连接的主接口和用于转发流量的当前接口。

  请参阅以下所示的 **show conn long zone** 命令的输出：

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080 inside-zone:inside1(inside2):
10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

- **show asp table zone**

  显示用于调试的加速安全路径表。

- **show local-host** [**zone** *zone_name* [**zone** *zone_name*] [...]]

  显示区域内本地主机的网络状态。

请参阅以下所示的 **show local-host zone** 命令的输出。首先列出的是主接口，当前接口用括号括起来。

```
ciscoasa# show local-host zone outside-zone

Zone:outside-zone: 4 active, 5 maximum active, 0 denied
local host: <10.122.122.1>,
    TCP flow count/limit = 3/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
    TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

区域路由

- **show route zone**

  显示区域接口的路由。

  请参阅以下所示的 **show route zone** 命令的输出：

```
ciscoasa# show route zone

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 not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

- **show asp table routing**

  显示用于调试的加速安全路径表，并显示与每个路由关联的区域。

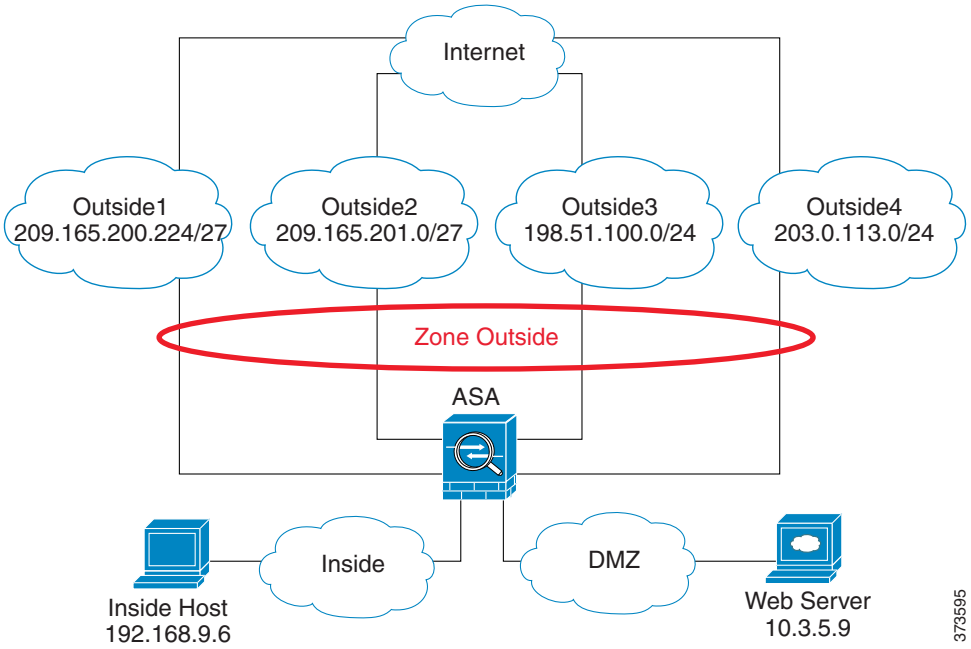
  请参阅以下所示的 **show asp table routing** 命令的输出：

```
ciscoasa# show asp table routing
route table timestamp: 60
in   255.255.255.255 255.255.255.255 identity
in   10.1.0.1       255.255.255.255 identity
in   10.2.0.1       255.255.255.255 identity
in   10.6.6.4         255.255.255.255 identity
in   10.4.4.4         255.255.255.255 via 10.4.0.10 (unresolved, timestamp: 49)
in   172.0.0.67       255.255.255.255 identity
in   172.0.0.0       255.255.255.0   wan-zone:outside2
in   10.85.43.0      255.255.255.0   via 10.4.0.3 (unresolved, timestamp: 50)
in   10.85.45.0      255.255.255.0   via 10.4.0.20 (unresolved, timestamp: 51)
in   192.168.0.0        255.255.255.0   mgmt
in   192.168.1.0       255.255.0.0     lan-zone:inside
out  255.255.255.255 255.255.255.255 mgmt
out  172.0.0.67       255.255.255.255 mgmt
```

```
out   172.0.0.0         255.255.255.0   mgmt
out   10.4.0.0        240.0.0.0       mgmt
out   255.255.255.255 255.255.255.255 lan-zone:inside
out   10.1.0.1        255.255.255.255 lan-zone:inside
out   10.2.0.0        255.255.0.0     lan-zone:inside
out   10.4.0.0        240.0.0.0       lan-zone:inside
```

流量区域示例

以下示例将 4 个 VLAN 接口分配给了外部区域，并且配置了 4 个默认等价路由。为内部接口配置了 PAT， Web 服务器在使用静态 NAT 的 DMZ 接口上可用。




```
interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch

zone outside

interface gigabitethernet0/0.101
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
```

```
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/1.201
  vlan 201
  nameif outside3
  security-level 0
  ip address 198.51.100.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/1.202
  vlan 202
  nameif outside4
  security-level 0
  ip address 203.0.113.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/2.301
  vlan 301
  nameif inside
  security-level 100
  ip address 192.168.9.1 255.255.255.0
  no shutdown

interface gigabitethernet0/2.302
  vlan 302
  nameif dmz
  security-level 50
  ip address 10.3.5.1 255.255.255.0
  no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
  host 10.3.5.9 255.255.255.255
  nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
  subnet 192.168.9.0 255.255.255.0
  nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87
# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99
route inside 209.165.202.130 255.255.255.255 192.168.9.99

# The global service policy
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
```

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

流量区域历史记录

功能名称	平台版本	说明
流量区域	9.3(2)	您可以将接口集合到一个流量区域以实现流量负载均衡（使用等价多路径 (ECMP) 路由）、路由冗余以及多个接口之间的非对称路由。 **备注**　您不能将安全策略应用于已命名的区域；安全策略是基于接口的策略。当区域中的接口配置了相同的访问规则、 NAT 和服务策略时，负载均衡和非对称路由将能够正常工作。 引入或修改了以下命令：**zone**、 **zone-member**、 **show running-config zone**、 **clear configure zone**、 **show zone**、 **show asp table zone**、 **show nameif zone**、 **show conn long**、 **show local-host zone**、 **show route zone**、 **show asp table routing**、 **clear conn zone**、 **clear local-host zone**



第 4 部分

基本设置



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。

- 设置主机名、域名及启用密码和 Telnet 密码，第 16-1 页
- 恢复启用密码和 Telnet 密码，第 16-3 页
- 设置日期和时间，第 16-7 页
- 配置主密码，第 16-10 页
- 配置 DNS 服务器，第 16-13 页
- 调整 ASP （加速安全路径）性能和行为，第 16-14 页
- 监控 DNS 缓存，第 16-15 页
- 基本设置历史记录，第 16-15 页

设置主机名、域名及启用密码和 Telnet 密码

在设置主机名、域名及启用密码和 Telnet 密码之前，请检查以下要求：

准备工作

- 在多情景模式下，可在系统和情景执行空间中配置主机名和域名。
- 启用密码和 Telnet 密码可在每个情景中设置；此类密码在系统中不可用。在多情景模式下发起从交换机到 ASASM 的会话时， ASASM 使用管理员情景中设置的登录密码。
- 要从系统切换至情景配置，请输入 **changeto context** *name* 命令。

要设置主机名、域名及启用密码和 Telnet 密码，请执行以下步骤。

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
```

此名称最多可包含 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。如果建立与多台设备的会话，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到非限定名称。例如，如果将域名设置为“example.com”，并通过非限定名称“jupiter”指定系统日志服务器，则 ASA 将名称限定为“jupiter.example.com”。

步骤 3　更改启用密码。默认情况下，启用密码为空。

如果没有配置启用身份验证，则可使用启用密码进入特权 EXEC 模式。如果没有配置 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。可以在密码中使用除问号和空格以外的任意字符。

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*

密码以加密形式保存在配置中，因此在输入原始密码后无法查看原始密码。输入不含密码的 **enable password** 命令，将密码设置为默认的空密码。

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，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* 是一个区分大小写的密码，最多由 16 个字母数字和特殊字符组成。可以在密码中使用除问号和空格以外的任意字符。

密码以加密形式保存在配置中，因此在输入原始密码后无法查看原始密码。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 **encrypted** 关键字一起输入 **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

配置访问特权 EXEC 模式的身份验证，第 32-13 页）

恢复启用密码和 Telnet 密码

忘记启用密码或 Telnet 密码时，可恢复这些密码。程序因设备类型不同而异。必须使用 CLI 执行该任务。

恢复 ASA 上的密码

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，然后重新启动。

步骤 3　启动后，当系统提示进入 ROMMON 模式时按下 **Escape** 键。

步骤 4　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　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，并询问是否要更改该值：

```
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，请按 **Enter** 键。

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-X、 ASA 5508-X 和 5516-X 上的密码

要恢复 ASA 5506-X、 ASA 5508-X 和 ASA 5516-X 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，然后重新启动。

步骤 3　启动后，当系统提示进入 ROMMON 模式时按下 **Escape** 键。

步骤 4　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，请按 **Enter** 键。

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

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 **Enter** 键。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到运行的配置。

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

备注　无法在 ASAv 上禁用密码恢复。

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** 命令可防止在配置保持不变的情况下进入 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 模式并维护现有配置，所以该擦除可防止恢复密码。但是，禁用密码恢复可以防止未授权用户查看配置或插入不同的密码。在此情况下，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。更改设置的唯一方法是在 CLI 提示符下输入命令。使用不同版本的命令加载新配置不会更改设置。如果在将 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。如果使用故障切换，并且备用设备配置为忽略启动配置，则当 **no service password recovery** 命令复制到备用设备时，配置寄存器会发生相同的更改。

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

备注　请勿设置 ASASM 的日期和时间；其可从主机交换机接收这些设置。

设置时区和夏令时日期

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，时区为 UTC，夏令时日期范围从四月第一个星期日的凌晨 2:00 到十月最后一个星期日的凌晨 2:00。

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。默认的循环日期范围是从三月第二个星期日的凌晨 2:00 到十一月第一个星期日的凌晨 2:00。

- 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 表示太平洋夏令时间。

  day 值设置一月中的第几天，从 1 到 31。例如，可用 April 1 或 1 April 形式输入月份和日期，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 形式输入月份和日期，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。年范围为 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，该值为 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 表示太平洋夏令时间。

  week 值用 1 到 4 之间的整数或 “first”或 “last”这样的词指定某月中的第几周。例如，如果某天刚好跨在第五周，则用 “last”来指定。

  weekday 值指定星期几：星期一、星期二、星期三等等。

  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，该值为 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，例如验证 CRL，其包括精确时间戳。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

在多情景模式下，只能在系统配置中设置时间。

要使用 NTP 服务器设置日期和时间，请执行以下步骤：

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 和 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* 参数是一个最长为 32 个字符的字符串。

步骤 4　标识 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* 关键字参数对标识 NTP 数据包的传出接口（如果不想使用路由表中的默认接口）。由于在多情景模式下系统不包含任何接口，请指定在管理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** 关键字将此 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。如果多台服务器准确度相似，则 **prefer** 关键字指定使用这些服务器中的哪台服务器。但是，如果某台服务器的准确度明显高于首选服务器，则 ASA 将使用这台更准确的服务器。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 会使用最准确的服务器。

手动设置日期和时间

在手动设置日期和时间之前，请检查以下要求：

准备工作

在多情景模式下，只能在系统配置中设置时间。

要手动设置日期和时间，请执行以下步骤：

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 表示下午 8:54。

day 值设置一月中的第几天，从 1 到 31。例如，可用 april 1 或 1 april 形式输入月份和日期，具体取决于标准日期格式。

month 值设置月份。根据标准日期格式，可用 april 1 或 1 april 形式输入月份和日期。

year 值以四位数字格式设置年份，例如， 2004。有效范围为 1993 到 2035。

默认时区为 UTC。如果输入 **clock set** 命令后，使用 **clock timezone** 命令更改时区，则时间自动调整到新的时区。

此命令将时间设置在硬件芯片中，不在配置文件中保存时间。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。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，而无需更改任何功能。使用主密码的功能包括：

- OSPF
- EIGRP
- VPN 负载均衡
- VPN （远程访问和站点间）
- 故障转移
- AAA 服务器
- 记录
- 共享许可证

备注　如果已启用故障切换，但未设置故障切换共享密钥，则在更改主密码时会显示错误消息，通知您必须输入故障切换共享密钥，以防主密码更改以纯文本形式发送。

添加或更改主密码

在添加或更改主密码之前，请检查以下要求：

准备工作

该程序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。

要添加或更改主密码，请执行以下步骤：

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 和 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。如果未在命令中输入新密码，则系统会提示您输入。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
Old key: bumblebee
New key: haverford
Confirm key: haverford
```

注意　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
```

只要启用密码加密且有可用的主密码，所有用户密码均将被加密。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，则该命令将预期该密码在未来可用。

如果稍后使用 **no password encryption aes** 命令禁用密码加密，所有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，在多情景模式下，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，但也未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。

示例

以下示例显示不存在上一个密钥：

```
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
Old key: 12345678
```

在以下示例中，输入不包含参数的命令，以便系统提示您输入密钥。由于密钥已经存在，系统将提示您输入。

```
ciscoasa(config)# key config-key password-encryption
Old key: 12345678
New key: 23456789
Confirm key: 23456789
```

在以下示例中，因为不存在密钥，所以系统不会提示您提供密钥。

```
ciscoasa(config)# key config-key password-encryption
New key: 12345678
Confirm key: 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该主密码。如果不知道密码，请参阅删除主密码，第 16-12 页。
- 此程序只能在安全会话中进行；即可通过 Telnet、 SSH，或通过 HTTPS 连接 ASDM。

要禁用主密码，请执行以下步骤：

操作步骤

步骤 1　删除主密码。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

Warning! You have chosen to revert the encrypted passwords to plain text. This operation
will expose passwords in the configuration and therefore exercise caution while viewing,
storing, and copying configuration.

Old key: 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
```

包含密码的非易失存储器将被 0xFF 模式擦除并覆盖。

在多情景模式下，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下输入 **write memory** 命令，但也未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。

删除主密码

无法恢复主密码。如果主密码丢失或未知，则可删除该主密码。

要删除主密码，请执行以下步骤：

操作步骤

步骤 1　删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。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。

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 （例如 **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。

备注　ASA 有限支持使用 DNS 服务器，具体取决于功能。例如，大多数命令要求您输入 IP 地址，只有当手动配置 **name** 命令将名称与 IP 地址相关联，并通过 **name** 命令启用名称后，才能够使用名称。

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，以便能够到达 DNS 服务器。

要配置 DNS 服务器，请执行以下步骤：

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　指定一台或多台 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
```

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。

- 选择规则引擎事务提交模型，第 16-14 页
- 启用 ASP 负载均衡，第 16-15 页

选择规则引擎事务提交模型

默认情况下，当更改基于规则的策略 （例如访问规则）时，更改会立即生效。但是，这种即时性将稍微降低性能。对于每秒高连接环境的大量规则列表而言，例如当您更改具有 25,000 条规则的策略而 ASA 每秒处理 18,000 个连接时，性能降低更加明显。

由于规则引擎要编译规则以实现更快的规则查找，所以性能会受到影响。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。

您可以更改此行为，以便规则引擎在实施规则更改时使用交易模式，并在新规则编译并可用之前继续使用旧规则。通过交易模式，在规则编译期间性能应不会下降。下表解释了行为差异。

模型	编译前	编译中	编译后
默认	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。

交易模式的另一个优势是，当替换接口上的 ACL 时，在删除旧的 ACL 和应用新的 ACL 之间没有间隙。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交易模式，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。

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
- 单核无法承受负载的相对严重过载接口接收环造成溢出。

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** 命令输出远小于 100%，则此命令可在数据包属于许多无关的连接时帮助您提高吞吐量。**auto** 选项使 ASA 能够自动打开和关闭每数据包负载均衡。

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
```

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 服务器中动态了解的条目，以及使用 **name** 命令手动输入的名称和 IP 地址。

基本设置历史记录

功能名称	平台版本	说明
主密码	8.3(1)	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，而无需更改任何功能。 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)	已修改了 **show password encryption** 命令。

功能名称	平台版本	说明
删除默认 Telnet 密码	9.0(2)/9.1(2)	为了提高 ASA 管理访问的安全性，已删除 Telnet 的默认登录密码；使用 Telnet 登录之前必须手动设置密码。 **备注**　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，当清除了密码时，ASA 恢复默认设置“cisco”。现在，当清除密码时，密码也被删除。 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。 修改了以下命令：**passwd**。
ASP 负载均衡	9.3(2)	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，从而降低丢包率并提高吞吐量。 引入了以下命令：**asp load-balance per-packet-auto**。



DHCP 和 DDNS 服务

本章介绍如何配置 DHCP 服务器和 DHCP 中继以及动态 DNS (DDNS) 更新方法。

- 关于 DHCP 和 DDNS，第 17-1 页
- DHCP 和 DDNS 服务准则，第 17-3 页
- 配置 DHCP 服务器，第 17-4 页
- 配置 DDNS，第 17-11 页
- 监控 DHCP 和 DDNS 服务，第 17-16 页
- DHCP 和 DDNS 服务历史记录，第 17-17 页

关于 DHCP 和 DDNS

本节介绍 DHCP 客户端和服务器如何使用 DHCP 中继代理协同运行，以及 DDNS 如何与 DHCP 集成。

关于 DHCP 服务器

DHCP 为 DHCP 客户端提供网络配置参数，如 IP 地址。思科 ASA 可以为连接到 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继消息。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（即在链路上）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

您可以配置 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。

您可以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。

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

- 配置 DHCP 服务器，第 17-4 页

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执行这些更新。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 和 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。

DHCP 和 DDNS 服务准则

本节介绍在配置 DHCP 和 DDNS 服务之前应检查的准则和限制。

防火墙模式

在透明防火墙模式下不支持。

IPv6

不支持接口专用 DHCP 中继服务器的 IPv6。

DHCP 服务器

- 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。
- 如果也启用 DHCP 服务器，则不能启用中继代理。
- ASA DHCP 服务器不支持 BOOTP 请求。在多情景模式下，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 会向 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 会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 会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，则服务器会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

- 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接口专用服务器的组合，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 的接口专用服务器。
- 如果也启用 DHCP 服务器功能，则不能启用中继代理。

- 如果已启用 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 无法访问或拒绝，则绑定解除。
- 您不能启用接口上作为 DHCP 代理服务运行的 DHCP 中继服务。必须先删除 VPN DHCP 配置，否则系统将显示错误消息。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。
- 在透明防火墙模式下， 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。要在透明模式下允许 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。
- 当 ASA 将 DHCP 中继到 DHCP 服务器时，它使用面向 DHCP 服务器的接口地址而非面向 DHCP 客户端的地址 (GIADDR) 获取数据包。此地址在与 EasyVPN 部署结合使用时会出现问题，因为它可能不是唯一的，而且 DHCP 流量必须通过 VPN 隧道路由。ASA EasyVPN 服务器不支持多个具有相同地址的对等体。为纠正这一问题，ASA 应使用 DHCP 服务器向其发送响应的地址获取数据包 (GIADDR)。部署 DHCP 中继时，此地址必须是唯一的。

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。请参阅启用 DHCP 服务器，第 17-4 页。

步骤 2　配置高级 DHCP 选项。请参阅 配置高级 DHCP 选项，第 17-6 页。

步骤 3　配置 DHCPv4 中继代理或 DHCPv6 中继代理。请参阅配置 DHCPv4 中继代理，第 17-9 页或配置 DHCPv6 中继代理，第 17-11 页。

启用 DHCP 服务器

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，供其在指定的时间段内使用。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 和 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。

您可以使用高级 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 服务器来发现域，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

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

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

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
```

备注　ASA 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。

下表显示 **dhcpd option** 命令不支持的 DHCP 选项。

表 17-1　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
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 用于配置思科 IP 电话。有关配置这些选项的详细信息，请参阅使用 DHCP 服务器配置思科 IP 电话，第 17-8 页。

使用 DHCP 服务器配置思科 IP 电话

思科 IP 电话从 TFTP 服务器下载其配置。当思科 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。

备注　思科 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。

任意选项编号

要发送用于任意选项编号的信息，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

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

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 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

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。您可以配置以下类型的服务器：

- 接口专用 DHCP 服务器 - DHCP 请求进入特定接口后， ASA 仅向接口专用服务器中继请求。
- 全局 DHCP 服务器 - DHCP 请求进入未让接口专用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。如果接口有接口专用服务器，则将不使用全局服务器。

操作步骤

步骤 1　执行以下两项操作或其中之一：

- 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。您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
```

通过此操作，客户端可以将其默认路由设置为指向 ASA，即使 DHCP 服务器指定了另一个路由器也如此。

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）执行以下其中一项操作：

- 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 参数可以是链路范围的单播、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）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 （以秒为单位）。

ipv6 dhcprelay timeout *seconds*

示例：

```
ciscoasa(config)# ipv6 dhcprelay timeout 25
```

seconds 参数的有效值范围为 1 到 3600。默认值为 60 秒。

配置 DDNS

本节介绍如何配置 DDNS。

为静态 IP 地址更新 A 和 PTR RR

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

要配置 DHCP 客户端以请求其更新 A 和 PTR RR 并且 DHCP 服务器执行这些请求，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

要将 DHCP 客户端配置为包括 FQDN 选项 （该选项指示 DHCP 服务器不执行 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

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

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 DDNS 更新方法。

ddns both

示例：

```
ciscoasa(DDNS-update-method)# ddns both
```

步骤 3　配置接口。

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 DHCP 和 DDNS 服务

本节介绍监控 DHCP 和 DDNS 服务的程序。

监控 DHCP 服务

请参阅以下用于监控 DHCP 服务的命令：

- **show running-config dhcpd**

  此命令可显示当前 DHCP 配置。
- **show running-config dhcprelay**

  此命令可显示当前 DHCP 中继服务状态。
- **show ipv6 dhcprelay binding**

  此命令可显示中继代理创建的中继绑定条目。
- **show ipv6 dhcprelay statistics**

  此命令可显示 IPv6 的 DHCP 中继代理统计信息。
- **clear config ipv6 dhcprelay**

  此命令可清除 IPv6 DHCP 中继配置。

监控 DDNS 状态

请参阅以下用于监控 DDNS 状态的命令：

- **show running-config ddns**

  此命令可显示当前 DDNS 配置。
- **show running-config dns server-group**

  此命令可显示当前 DNS 服务器组的状态。

DHCP 和 DDNS 服务历史记录

表 17-2　DHCP 和 DDNS 服务历史记录

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。 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**。
DDNS	7.0(1)	引入了此功能。 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 for IPv6 (DHCPv6)	9.0(1)	增加了对 IPv6 的支持。 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。每接口 DHCP 中继不支持 IPv6。 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。 引入或修改了以下命令：**dhcprelay information trusted**、 **dhcprelay information trust-all**、 **show running-config dhcprelay**。

表 17-2　　DHCP 和 DDNS 服务历史记录 （续）

功能名称	平台版本	说明
DHCP 重新绑定功能	9.1(4)	在 DHCP 重新绑定阶段，客户端会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，客户端不会重新绑定到备用服务器。 未引入或修改任何命令。
IPv6 的 DHCP 监控	9.4(1)	现在可监控 IPv6 的 DHCP。



第 18 章

数字证书

本章介绍如何配置数字证书。

- 关于数字证书，第 18-1 页
- 数字证书准则，第 18-8 页
- 监控数字证书，第 18-39 页
- 证书管理历史记录，第 18-41 页

关于数字证书

数字证书是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、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。

如果使用数字证书进行身份验证，则 ASA 上必须存在至少一个身份证书及其颁发 CA 证书。此配置允许多个身份、根和证书层次结构。ASA 根据 CRL（也称为权限吊销列表）评估第三方证书，从身份证书一直到从属证书颁发机构链。

以下是几种不同类型的可用数字证书的说明：

- CA 证书用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。
- CA 还会颁发身份证书，这是特定系统或主机的证书。
- 代码签名证书是用于创建数字签名以签署代码的特殊证书，经过签署的代码会透露证书源。

本地 CA 在 ASA 上集成独立的证书颁发机构功能，并且会部署证书，对已颁发的证书提供安全的吊销检查。本地 CA 凭借通过网站登录页面进行的用户注册提供安全、可配置的内部机构进行证书身份验证。

备注 CA 证书和身份证书适用于站点间 VPN 连接和远程访问 VPN 连接。本文档中的程序是指 ASDM GUI 中使用的远程访问 VPN。

数字证书是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、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。

如果使用数字证书进行身份验证，则 ASA 上必须存在至少一个身份证书及其颁发 CA 证书。此配置允许多个身份、根和证书层次结构。以下是几种不同类型的可用数字证书的说明：

- CA 证书用于签署其他证书。它是自签名证书，也称为根证书。
- 由另一个 CA 证书颁发的证书称为从属证书。

CA 负责管理证书请求和颁发数字证书。数字证书包括用于识别用户或设备的信息，例如名称、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 （例如 VeriSign），也可以是组织内建立的私有 （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

通过公钥加密实现的数字签名为设备和用户提供了一种身份验证方法。在 RSA 加密系统等公钥加密中，每位用户都有一个包含公钥和私钥的密钥对。这一对密钥相互补充，用其中一个密钥加密的任何内容都可用另一个密钥解密。

简言之，使用私钥加密数据时会形成一个签名。此签名附加在数据中并发送给接收者。接收者对数据应用发送者的公钥。如果随数据一起发送的签名与对数据应用公钥的结果一致，就会确立消息的有效性。

此过程的前提是接收者拥有发送者的公钥副本而且非常确定此密钥属于发送者，而不是伪装成发送者的其他人。

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 Web 浏览器都使用若干 CA 的根证书进行配置。对于 VPN，作为 IPsec 组件的 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，会向 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执行一些公钥加密，从而自行向远程对等体进行身份验证。每个对等体发送由 CA 颁发的唯一证书。此过程之所以适用，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 的对等体吊销证书。已吊销的证书无法被其他对等体识别为有效证书。已吊销的证书列于 CRL 中，每个对等体在接受来自其他对等体的证书之前都可能会检查这些证书。

某些 CA 会在其实施过程中使用 RA。RA 是一种用作 CA 的代理的服务器，以便 CA 功能可以在 CA 不可用时继续使用。

密钥对

密钥对是具有以下特征的 RSA 密钥：

- 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 密钥的最大密钥模数长度为 2048 位。默认大小为 1024。许多使用 RSA 密钥对超过 1024 位的身份证书的 SSL 连接可能会在 ASA 上造成较高的 CPU 使用率，从而拒绝无客户端登录。
- 对于签名操作，受支持的最大密钥长度为 4096 位。我们建议使用至少 2048 位的密钥长度。
- 您可以生成一个用于签名和加密的通用 RSA 密钥对，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，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

通过信任点，您可以管理并跟踪 CA 和证书。信任点表示 CA 或身份对。信任点包括 CA 的身份、CA 特定配置参数，以及与一个已注册身份证书的关联。

定义信任点之后，您可以在要求指定 CA 的命令中根据名称对其进行引用。您可以配置多个信任点。

备注　如果思科 ASA 具有多个共享同一 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。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。对于站点间 VPN，您必须注册每个 ASA。对于远程访问 VPN，则必须注册每个 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 只需要允许它访问即可。为使 ASA 提供此服务，用户必须在 ASA 发送注册请求之前使用 AAA 支持的任何方法进行身份验证。您还可以使用主机扫描和动态访问策略执行注册资格规则。

ASA 仅对 AnyConnect SSL 或 IKEv2 VPN 会话支持此功能。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 （无客户端启动的 AnyConnect）则支持该代理。

ASA 不支持证书的轮询。

ASA 支持此功能的负载均衡。

吊销检查

颁发证书后，该证书在固定时期内有效。有时， CA 会在此时期到期前吊销证书，例如，因为安全问题、名称更改或关联。CA 会定期发布签署的已吊销证书列表。启用吊销检查可强制 ASA CA 在每次使用证书进行身份验证时检查并确定其未吊销该证书。

启用吊销检查后，ASA 会在 PKI 证书验证过程中使用 CRL 检查和/或 OCSP 检查证书吊销状态。仅当第一种方法返回错误时 （例如，指示服务器不可用时），才会使用 OCSP。

通过 CRL 检查， ASA 可检索、分析、缓存 CRL，从而提供已吊销 （和未吊销）证书及其证书序列号的完整列表。ASA 根据 CRL （也称为权限吊销列表）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吊销状态检查方法，此方法通过验证机构对证书状态进行本地化，而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 标准的第三方 CA 供应商，包括但不限于：

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft 证书服务
- 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)吊销。CRL 配置是信任点配置的一部分。

进行证书身份验证时，您可以使用 **revocation-check crl** 命令将 ASA 配置为强制进行 CRL 检查。您也可以使用 **revocation-check crl none** 命令将 CRL 检查设为可选检查，从而在 CA 无法提供更新后的 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 的时间超过配置的 CRL 缓存时间时，ASA 会认为该 CRL 的版本过旧而不可靠（即 “过时”）。下次证书身份验证要求检查过时 CRL 时， ASA 会尝试检索更新版本的 CRL。

ASA 缓存 CRL 的时间由以下两个因素确定：

- 使用 **cache-time** 命令指定的分钟数。默认值为 60 分钟。
- 检索到的 CRL 中的 NextUpdate 字段，CRL 中可能没有该字段。您可使用 **enforcenextupdate** 命令控制 ASA 是否需要和使用 NextUpdate 字段。

ASA 通过以下方式使用这两个因素：

- 如果不需要 NextUpdate 字段，则 ASA 会在经过由 **cache-time** 命令定义的时间长度后将 CRL 标记为过时。
- 如果需要 NextUpdate 字段，则 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 分钟内过时。

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 来为新检索的 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) 吊销。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 即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吊销状态，并且可帮助组织进行大型 PKI 安装部署和扩展安全网络。

备注　ASA 允许 OCSP 响应有五秒钟的时间偏差。

进行证书身份验证时，您可以使用 **revocation-check ocsp** 命令将 ASA 配置为强制进行 OCSP 检查。您也可以使用 **revocation-check ocsp none** 命令将 OCSP 检查设为可选检查，从而在验证机构无法提供更新后的 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。

备注　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。然后，在客户端证书验证信任点配置 **match certificate** 命令，以使用包含自签名 OCSP 响应方证书的信任点验证响应方证书。使用同一程序配置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 会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吊销状态检查。但是，如果此扩展不存在，则 ASA 会尝试使用信任点中指定的同一方法检查吊销状态。如果响应方证书无法验证，则吊销检查失败。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吊销检查。
- 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 文件存储

ASA 使用本地 CA 数据库访问和实施用户信息、已颁发的证书和吊销列表。此数据库默认驻留在本地闪存中，也可以配置为驻留在已安装并可供 ASA 访问的外部文件系统上。

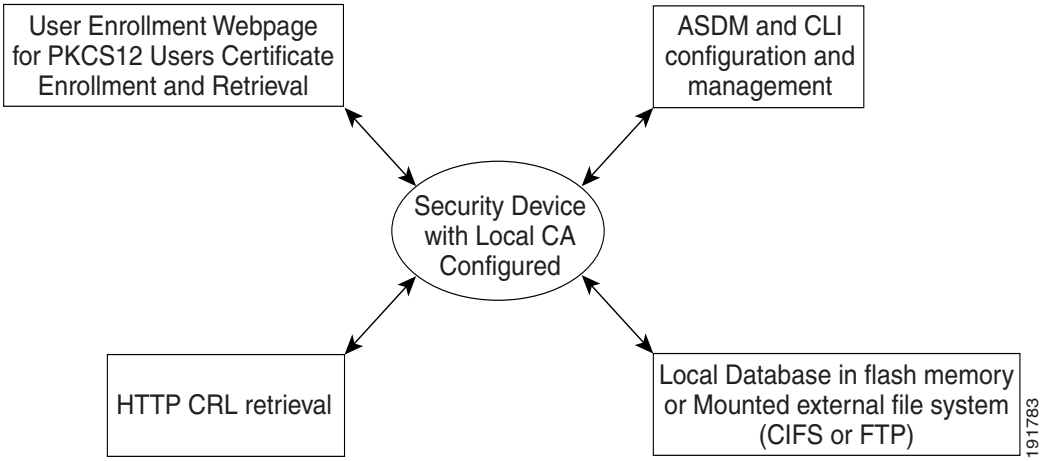
可存储在本地 CA 用户数据库中的用户数不受限制；但是，如果出现闪存存储问题，将生成系统日志以提示管理员采取行动，并且本地 CA 可能会禁用，直到存储问题得到解决。闪存可存储不超过 3500 个用户的数据库；但如果数据库的用户数超过 3500，则需要外部存储器。

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以及由本地 CA 管理员提供的一次性密码以验证其注册资格。

下图显示本地 CA 服务器位于 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 18-1　　本地 CA



证书和用户登录凭证

下一节介绍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。

在所有情况下， 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进行启用
  - 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进行启用
  - 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何 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进行启用
  - 使用用户名和密码作为凭证
- 授权
  - 通过授权服务器组设置进行启用
  - 使用用户名作为凭证

如果禁用身份验证但启用授权，则 ASA 将使用主 DN 字段进行授权。

- 身份验证
  - 通过身份验证服务器组设置进行禁用 （设置为 None）
  - 未使用凭证
- 授权
  - 通过授权服务器组设置进行启用
  - 使用证书主 DN 字段的用户名值作为凭证

备注　如果证书中不存在主 DN 字段，则 ASA 使用辅助 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 DN = EA （邮件地址）并且辅助 DN = CN （公用名），则授权请求中使用的用户名将是 anyuser@example.com。

数字证书准则

本节介绍在配置数字证书之前应检查的准则和限制。

情景模式准则

- 对于第三方 CA，仅在单情景模式下受支持。

故障切换准则

- 在有状态的故障切换中不支持复制会话。
- 对于本地 CA，不支持故障切换。

IPv6 规定

不支持 IPv6。

本地 CA 证书

- 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。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。证书具有生效日期和时间以及到期日期和时间。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，则注册失败。
- 在本地 CA 证书到期前 30 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到时间进行本地 CA 滚动更新。新的本地 CA 证书必须在当前证书到期前导入到所有必要的设备上。如果管理员未通过将滚动更新证书安装为新的本地 CA 证书作出响应，则验证可能会失败。
- 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。

以下示例显示 base 64 编码的本地 CA 证书：

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

SCEP 代理支持

- 终端必须运行的是 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 身份验证和证书身份验证。
- 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下。

本地 CA 证书数据库

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 证书和密钥对的存档。
- 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。

其他准则

- 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。
- 启用故障切换时，无法配置本地 CA。您只能为无故障切换的独立 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，该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 2048 位的密钥长度。
- **lifetime ca-certificate** 命令在第一次生成本地 CA 服务器证书时 （即，最初配置本地 CA 服务器并发出 **no shutdown** 命令时）生效。当 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，
- 您应将 ASA 配置为使用身份证书保护流向管理接口的 ASDM 流量和 HTTPS 流量。每次重新启动后都会重新生成使用 SCEP 自动生成的身份证书，因此请确保手动安装您自己的身份证书。本程序仅适用于 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 （Subject Name 中的序列号）使用 PrintableString 格式的证书。如果序列号格式使用编码 （例如 UTF8），则证书授权将失败。
- 仅当在 ASA 上导入证书参数时，才对证书参数使用有效的字符和值。

- 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，则 ASA 会拒绝已导入的证书。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
```

配置密钥对

要创建或删除密钥对，请执行以下步骤：

操作步骤

步骤 1　生成一个通用 RSA 密钥对。

crypto key generate rsa

示例：

```
ciscoasa/contexta(config)# crypto key generate rsa
```

默认密钥模数长度为 1024。要指定其他模数长度大小，请使用 **modulus** 关键字。

注意　许多使用 RSA 密钥对超过 1024 位的身份证书的 SSL 连接可能会在 ASA 上造成较高的 CPU 使用率，从而拒绝无客户端登录。

步骤 2　（可选）向每个密钥对分配标签。

crypto key generate rsa label *key-pair-label*

示例：

```
ciscoasa/contexta(config)# crypto key generate rsa label exchange
```

该标签由使用密钥对的信任点引用。如果未分配标签，则密钥对将自动标记为 *Default-RSA-Key*。

步骤 3　验证已生成的密钥对。

show crypto key *name of key*

示例：

```
ciscoasa/contexta(config)# show crypto key examplekey
```

步骤 4　保存已生成的密钥对。

write memory

示例：

```
ciscoasa(config)# write memory
```

步骤 5　如有必要，请删除现有密钥对，以便可以生成新的密钥对。

crypto key zeroize rsa

示例：

```
ciscoasa(config)# crypto key zeroize rsa
```

步骤 6　（可选）存档本地 CA 服务器证书和密钥对。

copy

示例：

```
ciscoasa# copy LOCAL-CA-SERVER_0001.pl2 tftp://10.1.1.22/user6/
```

此命令使用 FTP 或 TFTP 从 ASA 复制本地 CA 服务器证书和密钥对及所有文件。

注意　确保尽可能经常备份所有本地 CA 文件。

示例

以下示例显示如何删除密钥对：

```
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

要配置信任点，请执行以下步骤：

操作步骤

步骤 1　创建对应于 ASA 需要从其接收证书的 CA 的信任点。

crypto ca trustpoint *trustpoint-name*

示例：

```
ciscoasa/contexta(config)# crypto ca trustpoint Main
```

您可以进入 crypto ca trustpoint 配置模式，该模式控制可从步骤 3 开始配置的 CA 特定信任点参数。

注意　当尝试连接时，在尝试从信任点检索 ID 证书的过程中会出现表示信任点不包含 ID 证书的警告。

步骤 2　选择以下选项之一：

- 通过指定信任点请求使用 SCEP 进行自动注册并配置注册 URL。

  enrollment url *url*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment url
http://10.29.67.142:80/certsrv/mscep/mscep.dll
```

- 通过将从 CA 收到的证书粘贴到终端，请求使用指定信任点手动注册。

  enrollment terminal

  示例：

  ```
  ciscoasa/contexta(config-ca-trustpoint)# enrollment terminal
  ```

步骤 3　指定可用的 CRL 配置选项。

revocation-check crl 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
```

注意　要启用必需或可选的 CRL 检查，请确保在获得证书后为 CRL 管理配置信任点。

步骤 4　进入 CRL 配置模式。

crl configure

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# crl configure
```

步骤 5　在注册过程中，要求 CA 在证书的 Subject Alternative Name 扩展中包含指定的邮件地址。

email *address*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# email example.com
```

步骤 6　（可选）指定重试周期（以分钟为单位），且仅应用于 SCEP 注册。

enrollment retry period

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 5
```

步骤 7　（可选）指定允许的最大重试次数，且仅应用于 SCEP 注册。

enrollment retry count

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 2
```

步骤 8　在注册过程中，要求 CA 在证书的 Subject Alternative Name 扩展中包含指定的完全限定域名。

fqdn *fqdn*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# fqdn example.com
```

步骤 9　在注册过程中，要求 CA 在证书中包含 ASA 的 IP 地址。

ip-address *ip-address*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# ip-address 10.10.100.1
```

步骤 10　指定要认证其公钥的密钥对。

keypair *name*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# keypair exchange
```

步骤 11　配置 OCSP URL 覆盖和信任点以用于验证 OCSP 响应方证书。

match certificate map-name override ocsp

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# match certificate examplemap override ocsp
```

步骤 12　在 OCSP 请求上禁用随机数扩展。随机数扩展以加密方式将请求与响应绑定以避免重放攻击。

ocsp disable-nonce

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp disable-nonce
```

步骤 13　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。

ocsp url

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp url
```

步骤 14　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吊销请求进行身份验证。

password *string*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# password mypassword
```

步骤 15　设置一种或多种吊销检查方法：CRL、 OCSP 和随机数。

revocation check

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# revocation check
```

步骤 16　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.”）。

subject-name *X.500 name*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# myname X.500 examplename
```

步骤 17　在注册过程中，要求 CA 在证书中包含 ASA 序列号。

serial-number

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# serial number JMX1213L2A7
```

步骤 18　保存运行配置。

write memory

示例：

```
ciscoasa/contexta(config)# write memory
```

为信任点配置 CRL

要在证书身份验证过程中使用强制或可选 CRL 检查，您必须为每个信任点配置 CRL。要为信任点配置 CRL，请执行以下步骤：

操作步骤

步骤 1　针对要修改其 CRL 配置的信任点进入 crypto ca trustpoint 配置模式。

crypto ca trustpoint *trustpoint-name*

示例：

```
ciscoasa (config)# crypto ca trustpoint Main
```

注意　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　针对当前信任点进入 crl 配置模式。

crl configure

示例：

```
ciscoasa(config-ca-trustpoint)# crl configure
```

提示　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，可以随时重新输入此命令来重新启动该程序。

步骤 3　选择下列其中一项来配置检索策略：

- CRL 仅从已通过身份验证的证书中指定的 CRL 分发点进行检索。

  policy cdp

  示例：

  ```
  ciscoasa(config-ca-crl)# policy cdp
  ```

注意　证书中指定的分发点不支持 SCEP 检索。

要继续，请转至步骤 5。

- CRL 仅从您配置的 URL 中进行检索。

  policy static

  示例：

  ```
  ciscoasa(config-ca-crl)# policy static
  ```

  要继续，请转至步骤 4。

- CRL 仅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 中进行检索。

  policy both

  示例：

  ```
  ciscoasa(config-ca-crl)# policy both
  ```

  要继续，请转至步骤 4。

步骤 4　如果您在配置 CRL 策略时使用关键字 **static** 或 **both**，则必须为 CRL 检索配置 URL。您最多可以输入五个 URL，级别为 1 至 5。*n* 参数是分配给 URL 的级别。

url *n url*

示例：

```
ciscoasa (config-ca-crl)# url 2 http://www.example.com
```

要删除 URL，请使用 **no url** *n* 命令。

步骤 5　指定 HTTP、 LDAP 或 SCEP 作为 CRL 检索方法。

protocol http | ldap | scep

示例：

```
ciscoasa(config-ca-crl)# protocol http
```

步骤 6　为当前信任点配置 ASA 缓存 CRL 的时间长度。*refresh-time* 参数是 ASA 将 CRL 视为过时之前等待的分钟数。

cache-time *refresh-time*

示例：

```
ciscoasa(config-ca-crl)# cache-time 420
```

步骤 7　选择如下选项之一：

- 要求 CRL 中有 NextUpdate 字段。这是默认设置。

  enforcenextupdate

  示例：

  ```
  ciscoasa(config-ca-crl)# enforcenextupdate
  ```

- 允许 CRL 中没有 NextUpdate 字段。

  no enforcenextupdate

示例：

```
ciscoasa(config-ca-crl)# no enforcenextupdate
```

步骤 8　如果 LDAP 指定为检索协议，则向 ASA 表明 LDAP 服务器身份。您可以按 DNS 主机名或按 IP 地址指定服务器。如果服务器侦听端口上的 LDAP 查询，则您还可以提供端口号，而不是使用默认端口号 389。

ldap-defaults *server*

示例：

```
ciscoasa (config-ca-crl)# ldap-defaults ldap1
```

注意　如果使用主机名而非 IP 地址来指定 LDAP 服务器，请确保您已将 ASA 配置为使用 DNS。

步骤 9　如果 LDAP 服务器需要凭证，则允许 CRL 检索。

ldap-dn *admin-DN password*

示例：

```
ciscoasa (config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering c00lRunZ
```

步骤 10　从指定信任点所代表的 CA 检索当前 CRL 并测试当前信任点的 CRL 配置。

crypto ca crl request *trustpoint*

示例：

```
ciscoasa (config-ca-crl)# crypto ca crl request Main
```

步骤 11　保存运行配置。

write memory

示例：

```
ciscoasa (config)# write memory
```

导出或导入信任点配置

要导出信任点配置，请执行以下步骤：

操作步骤

步骤 1　以 PKCS12 格式导出带有所有关联密钥和证书的信任点配置。

crypto ca export *trustpoint*

示例：

```
ciscoasa(config)# crypto ca export Main
```

ASA 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，请确保该文件处于安全位置。

示例

以下示例显示使用密码 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---
```

要导入信任点配置，请执行以下步骤：

步骤 1　导入与信任点配置关联的密钥对和已颁发证书。

crypto ca import *trustpoint* **pkcs12**

示例：

```
ciscoasa(config)# crypto ca import Main pkcs12
```

ASA 提示您以 base64 格式将文本粘贴到终端。系统将向与信任点一起导入的密钥对分配与所创建的信任点名称相匹配的标签。

注意　如果 ASA 具有共享同一 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。通过使用创建的规则，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。

要配置 CA 证书映射规则，请执行以下步骤：

操作步骤

步骤 1　针对要配置的规则进入 CA 证书映射配置模式，并指定规则索引编号。

crypto ca certificate map *sequence-number*

示例：

```
ciscoasa(config)# crypto ca certificate map 1
```

步骤 2　指定所有已签发证书的可分辨名称。它同时也是自签名 CA 证书的使用者名称 DN。

issuer-name *DN-string*

示例：

```
ciscoasa(config-ca-cert-map)# issuer-name cn=asa.example.com
```

使用逗号分隔属性-值对。使用引号将任何包含逗号的值引起来。issuer-name 必须少于 500 个字母数字字符。默认 issuer-name 是 cn=*hostame.domain-name*。

步骤 3　指定 ASA 可应用于证书的 **Subject** 字段中找到的值的测试。

subject-name attr *tag* **eq | co | ne | nc** *string*

示例：

```
ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
```

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。以下是有效的运算符：

- 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　保存运行配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

手动获取证书

准备工作

您必须已从信任点代表的 CA 获取 base-64 编码的 CA 证书。

要手动获取证书，请执行以下步骤：

操作步骤

步骤 1　导入已配置的信任点的 CA 证书。

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
```

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。

步骤 2　使用信任点注册 ASA。

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
```

此命令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不同的 RSA 密钥，则 **crypto ca enroll** 命令显示两个证书请求，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** 命令显示一个证书请求。

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。确保证书采用 base-64 格式。

步骤 3　导入从 CA 收到的每个证书并确保以 base-64 格式将证书粘贴到终端。

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
```

步骤 4　通过显示为 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。

show crypto ca server certificate

示例：

```
ciscoasa(config)# show crypto ca server certificate Main
```

步骤 5　保存运行配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

步骤 6　对于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

本节介绍如何使用 SCEP 自动获取证书。

准备工作

您必须已从信任点代表的 CA 获取 base-64 编码的 CA 证书。

要使用 SCEP 自动获取证书，请执行以下步骤：

操作步骤

步骤 1　获取已配置的信任点的 CA 证书。

crypto ca authenticate *trustpoint*

示例：

```
ciscoasa/contexta(config)# crypto ca authenticate Main
```

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。

步骤 2　使用信任点注册 ASA。此命令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。

crypto ca enroll *trustpoint*

示例：

```
ciscoasa/contexta(config)# crypto ca enroll Main
```

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，则会重新发送证书请求。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 （包括字符的大小写）不同，则系统将显示警告。要解决此问题，请退出注册过程，进行任何必要的更正，然后重新输入 **crypto ca enroll** 命令。

注意　如果 ASA 在您发出 **crypto ca enroll** 命令后但在收到证书前重新启动，请重新输入 **crypto ca enroll** 命令并通知 CA 管理员。

步骤 3　通过显示为 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。

show crypto ca server certificate

示例：

```
ciscoasa/contexta(config)# show crypto ca server certificate Main
```

步骤 4　保存运行配置。

write memory

示例：

```
ciscoasa/contexta(config)# write memory
```

为 SCEP 请求配置代理支持

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：

操作步骤

步骤 1　进入 tunnel-group ipsec-attributes 配置模式。

tunnel-group *name* **ipsec-attributes**

示例：

```
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
```

步骤 2　启用客户端服务。

crypto ikev2 enable outside client-services port *portnumber*

示例：

```
ciscoasa(config-tunnel-ipsec)# crypto ikev2 enable outside client-services
```

默认端口号为 443。

注意　仅当支持 IKEv2 时，才需要此命令。

步骤 3　进入 tunnel-group general-attributes 配置模式。

tunnel-group *name* **general-attributes**

示例：

```
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
```

步骤 4　为隧道组启用 SCEP 注册。

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.
```

步骤 5　进入 group-policy attributes 配置模式。

group-policy *name* **attributes**

示例：

```
ciscoasa(config)# group-policy FirstGroup attributes
```

步骤 6　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。

scep-forwarding-url value *URL*

示例：

```
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
```

URL 是 CA 上的 SCEP URL。

步骤 7　当证书不适用于 SCEP 代理的 WebLaunch 支持时，请提供通用辅助密码。

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
```

您必须使用 **hide** 关键字支持 SCEP 代理。

例如，证书对于请求该证书的终端不可用。终端获得证书后，AnyConnect 会断开连接，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。

步骤 8　隐藏 AnyConnect VPN 会话的辅助预填写用户名。

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
```

尽管从更早版本继承了 **ssl-client** 关键字，但此命令用于支持使用 IKEv2 或 SSL 的 AnyConnect 会话。

您必须使用 **hide** 关键字支持 SCEP 代理。

步骤 9　当证书不可用时，请提供用户名。

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
```

启用本地 CA 服务器

本节介绍如何启用本地 CA 服务器。

准备工作

启用本地 CA 服务器之前，您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。

要启用本地 CA 服务器，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　启用本地 CA 服务器。

no shutdown

示例：

```
ciscoasa(config-ca-server)# no shutdown
```

此命令用于生成本地 CA 服务器证书、密钥对和必要的数据库文件，并将本地 CA 服务器证书和密钥对存档在 PKCS12 文件中。您必须输入由 8 至 65 个字母数字组成的密码。初始启动后，您可以禁用本地 CA，无需提示输入密码。

步骤 3　保存配置，以确保在重新启动后本地 CA 证书和密钥对不会丢失。

write memory

示例：

```
ciscoasa(config)# write memory
```

示例

以下示例启用本地 CA 服务器：

```
ciscoasa(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样本输出：

```
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

要配置本地 CA 服务器，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　指定 SMTP 发件人地址，即本地 CA 在向用户发送用于为注册邀请提供一次性密码 (OTP) 时用作发件人地址的有效邮件地址。

smtp from-address *e-mail_address*

示例：

```
ciscoasa(config-ca-server) # smtp from-address SecurityAdmin@example.com
```

步骤 3　（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。

subject-name-default *dn*

示例：

```
ciscoasa(config-ca-server)# subject-name-default cn=engineer, o=asc systems, c=” US”
```

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。如果您未指定使用者名称 DN，则必须在每次将向用户数据库中添加用户时指定要包含在用户证书中的准确使用者名称 DN。

注意　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 后将不能更改颁发者名称和密钥长度服务器值。

步骤 4　在 ASA 上创建自签名证书并将其与本地 CA 关联。

no shutdown

示例：

```
ciscoasa(config-ca-server)# no shutdown
```

自签名证书密钥用法扩展具有密钥加密、密钥签名、 CRL 签名和证书签名功能。

注意　在生成自签名的本地 CA 证书后，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吊销或恢复权限。

示例

以下示例显示如何使用所有必需参数的预定义默认值来配置本地 CA 服务器：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp from-address SecurityAdmin@example.com
ciscoasa(config-ca-server)# subject-name-default cn=engineer, o=asc Systems, c=US
ciscoasa(config-ca-server)# no shutdown
```

自定义本地 CA 服务器

要配置自定义本地 CA 服务器，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　指定没有默认值的参数。

issuer-name *DN-string*

示例：

```
ciscoasa(config-ca-server)# issuer-name cn=xx5520,cn=30.132.0.25,ou=DevTest,ou=QA,o=ASC
Systems
```

步骤 3　自定义显示在从本地 CA 服务器发送的所有邮件的使用者字段中的文本

smtp subject *subject-line*

示例：

```
ciscoasa(config-ca-server)# smtp subject Priority E-Mail: Enclosed Confidential
Information is Required for Enrollment
```

步骤 4　**指定**要用作由本地 CA 服务器生成的所有邮件的 From: 字段的邮件地址。

smtp from-address *e-mail_address*

示例：

```
ciscoasa(config-ca-server)# smtp from-address SecurityAdmin@example.com
```

步骤 5　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。

subject-name-default *dn*

示例：

```
ciscoasa(config-ca-server)# subject-name default cn=engineer, o=ASC Systems, c=US
```

默认使用者名称 DN 变成由本地 CA 服务器颁发的所有用户证书中的用户名的一部分。

允许的 DN 属性关键字如下：

- C = 国家/地区
- CN = 公用名
- EA = 邮件地址
- L = 地区
- O = 组织名称
- OU = 组织单位
- ST = 省/自治区/直辖市
- SN = 姓
- ST = 省/自治区/直辖市

注意　如果未指定 subject-name-default 作为标准使用者名称默认值，则每次添加用户时都必须指定 DN。

禁用本地 CA 服务器

要禁用本地 CA 服务器，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　禁用本地 CA 服务器。

shutdown

示例：

```
ciscoasa(config-ca-server)# shutdown
INFO: Local CA Server has been shutdown.
```

此命令用于禁用网站注册，允许您修改本地 CA 服务器配置，并存储当前配置以及关联文件。初始启动后，您可以重新启用本地 CA，无需提示输入密码。

删除本地 CA 服务器

要删除现有的已启用或已禁用的本地 CA 服务器，请执行以下步骤：

操作步骤

步骤 1　输入以下其中一个命令，可删除现有的已启用或已禁用的本地 CA 服务器：

- **no crypto ca server**

  示例：

  ```
  ciscoasa(config)# no crypto ca server
  ```

- **clear configure crypto ca server**

  示例：

  ```
  ciscoasa(config)# clear config crypto ca server
  ```

备注　删除本地 CA 服务器将会从 ASA 中删除配置。配置删除后，无法恢复。

确保同时还删除关联的本地 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 CA 证书有效期

要配置本地 CA 服务器证书有效期，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　确定要在证书中包含的到期日期。本地 CA 证书的默认有效期是三年。

lifetime ca-certificate *time*

示例：

```
ciscoasa(config-ca-server)# lifetime ca-certificate 365
```

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)。

步骤 3　（可选）将本地 CA 证书的有效期重置为默认值三年。

no lifetime ca-certificate

示例：

```
ciscoasa(config-ca-server)# no lifetime ca-certificate
```

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.
```

注意　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 证书在到期前导入到所有所需的设备上。

配置用户证书有效期

要配置用户证书有效期，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　设置希望用户证书保持有效的时间长度。

lifetime certificate *time*

示例：

```
ciscoasa(config-ca-server)# lifetime certificate 60
```

注意　在用户证书到期之前，本地 CA 服务器将自动启动证书续签处理，在证书到期日期前几天向用户授予注册权限，设置续签提醒，并发送包含用于证书续签的注册用户名和 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

要配置 CRL 有效期，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　设置希望 CRL 保持有效的时间长度。

lifetime crl *time*

示例：

```
ciscoasa(config-ca-server)# lifetime crl 10
```

本地 CA 将在每次吊销或取消吊销用户证书时更新和重新颁发 CRL，但如果未发生吊销变更，则会在每个 CRL 有效期到期后自动重新颁发一次 CRL。如果未指定 CRL 有效期，则默认有效期为六小时。

步骤 3　可随时强制颁发 CRL，这会立即更新和重新生成当前 CRL，以覆盖现有 CRL。

crypto ca server crl issue

示例：

```
ciscoasa(config-ca-server)# crypto ca server crl issue
A new CRL has been issued.
```

注意　除非 CRL 文件已被错误地删除或已损坏且必须重新生成，否则请勿使用此命令。

配置服务器密钥长度

要配置服务器密钥长度，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　指定在用户证书注册时生成的公钥和私钥的长度。

keysize server

示例：

```
ciscoasa(config-ca-server)# keysize server 2048
```

密钥对长度选项包括 512、 768、 1024、 2048 位，默认值是 1024 位。

注意　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都将失效。要更改本地 CA 密钥长度，必须删除当前本地 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样本输出。

```
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

要配置外部本地 CA 文件存储，请执行以下步骤：

操作步骤

步骤 1　访问特定文件系统类型的配置模式。

mount *name* **type**

示例：

```
ciscoasa(config)# mount mydata type cifs
```

步骤 2　安装 CIFS 文件系统。

mount *name* **type cifs**

示例：

```
ciscoasa(config-mount-cifs)# mount mydata type cifs
server 10.1.1.10 share myshare
domain example.com
username user6
password ********
status enable
```

注意　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　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 4　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。

database path *mount-name directory-path*

示例：

```
ciscoasa(config-ca-server)# database path mydata:newuser
```

此命令用于建立服务器路径，然后指定用于存储和检索的本地 CA 文件或文件夹名称。要将本地 CA 文件存储返回到 ASA 闪存，请使用 **no database path** 命令。

注意　要保护存储在外部服务器上的本地 CA 文件，需要受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　保存运行配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

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，用户信息会自动保存到启动配置的默认位置。

示例

以下示例显示出现在闪存或外部存储器中的本地 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)
```

下载并存储 CRL

要下载并存储 CRL，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　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。

publish-crl interface *interface* **port** *portnumber*

示例：

```
ciscoasa(config-ca-server)# publish-crl outside 70
```

接口和可选端口选择如下：

- inside - 接口名称/GigabitEthernet0/1
- management - 接口名称/Management0/0
- outside - 接口名称/GigabitEthernet0/0
- 端口号范围可以是 1 至 65535。TCP 端口 80 是 HTTP 默认端口号。

注意　如果您未指定此命令，则无法从 CDP 位置访问 CRL，因为需要此命令才能打开接口以下载 CRL 文件。

可以将 CDP URL 配置为使用接口的 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，当请求传入时， ASA 会将路径 /user8/my_crl_file 与已配置的 CDP URL 进行匹配。如果路径匹配， ASA 将返回存储的 CRL 文件。

注意　协议必须是 HTTP，因此所显示的前缀为 http://。

步骤 3　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 位置为 http://*hostname.domain*/+CSCOCA+/asa_ca.crl。

cdp-url *url*

示例：

```
ciscoasa(config-ca-server)# cdp-url http://172.16.1.1/pathname/myca.crl
```

本地 CA 将在每次吊销或取消吊销用户证书时更新和重新颁发 CRL。如果未发生吊销变更，则会在每个 CRL 有效期到期后重新颁发一次 CRL。

如果此命令设置为直接从本地 CA ASA 提供 CRL，请参阅下载并存储 CRL，第 18-32 页以了解有关打开接口上的端口以便从该接口访问 CRL 的说明。

其他设备也存在 CRL，用以验证由本地 CA 颁发的证书的吊销情况。此外，本地 CA 会跟踪其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）检索吊销状态来验证用户证书时，将执行吊销检查。

设置注册参数

要设置注册参数，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　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。

otp expiration *timeout*

示例：

```
ciscoasa(config-ca-server)# otp expiration 24
```

注意　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　指定已注册的用户可以检索 PKCS12 注册文件的小时数。

enrollment-retrieval *timeout*

示例：

```
ciscoasa(config-ca-server)# enrollment-retrieval 120
```

当用户已成功注册时，此时间期限开始。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

要添加有资格在本地 CA 数据库注册的用户，请执行以下步骤：

操作步骤

步骤 1　将新用户添加到本地 CA 数据库。

crypto ca server user-db add *username* [**dn** *dn*] [**email** *emailaddress*]

示例：

```
ciscoasa(config-ca-server)# crypto ca server user-db add user1 dn user1@example.com,
Engineer, Example Company, US, email user1@example.com
```

username 参数是包含 4 至 64 个字符的字符串，它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以进行注册邀请。

dn 参数是可分辨名称，即 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 参数是要向其发送 OTP 和通知的新用户的邮件地址。

步骤 2　向新添加的用户提供用户权限。

crypto ca server user-db allow *user*

示例：

```
ciscoasa(config-ca-server)# crypto ca server user-db allow user
```

步骤 3　通知本地 CA 数据库中的用户注册和下载用户证书，该证书自动通过邮件将 OTP 发送给该用户。

crypto ca server user-db email-otp *username*

示例：

```
ciscoasa(config-ca-server)# crypto ca server user-db email-otp exampleuser1
```

注意　当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中指定邮件地址。

步骤 4　显示已颁发的 OTP。

crypto ca server user-db show-otp

示例：

```
ciscoasa(config-ca-server)# crypto ca server user-db show-otp
```

步骤 5　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 *timeout*

示例：

```
ciscoasa(config-ca-server)# otp expiration 24
```

此命令定义 OTP 对用户注册有效的时间。此时间期限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段内返回以根据需要多次下载 PKCS12 文件。此时间段到期后， PKCS12 文件将自动从存储器中删除且不再可供下载。

注意　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。

续签用户

要指定续签通知的时间，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　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)。

renewal-reminder *time*

示例：

```
ciscoasa(config-ca-server)# renewal-reminder 7
```

如果证书到期，则其将会失效。续签通知及将通知以邮件形式发送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，则系统日志消息将向您通报续签要求。

ASA 自动向任何持有即将到期的有效证书的用户授予证书续签权限，只要这些用户仍存在于用户数据库中即可。因此，如果管理员不想允许某用户自动续签，则必须在续签时间段之前从数据库中删除该用户。

恢复用户

要恢复用户和由本地 CA 服务器颁发的之前已吊销的证书，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　恢复用户和取消吊销由本地 CA 服务器颁发的之前已吊销的证书。

crypto ca server unrevoke *cert-serial-no*

示例：

```
ciscoasa(config-ca-server)# crypto ca server unrevoke 782ea09f
```

本地 CA 保留当前 CRL 和所有已吊销用户证书的序列号。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。按证书序列号吊销（或取消吊销）任意当前证书时， CRL 自动反映这些更改。

删除用户

要按用户名从用户数据库中删除用户，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　从用户数据库中删除用户，并允许吊销已颁发给用户的任意有效证书。

crypto ca server user-db remove *username*

示例：

```
ciscoasa(config-ca-server)# crypto ca server user-db remove user1
```

吊销证书

要吊销用户证书，请执行以下步骤：

操作步骤

步骤 1　进入 local ca server 配置模式。

crypto ca server

示例：

```
ciscoasa(config)# crypto ca server
```

步骤 2　输入十六进制格式的证书序列号。

crypto ca server revoke *cert-serial-no*

示例：

```
ciscoasa(config-ca-server)# crypto ca server revoke 782ea09f
```

此命令用于在本地 CA 服务器上的证书数据库中和自动重新颁发的 CRL 中将证书标记为已吊销。

注意　如果需要吊销 ASA 的证书，则还需要密码，因此请确保记录密码并将其存储在安全位置。

配置证书身份验证和续签提醒

存储证书链

当配置了定期证书身份验证时，ASA 存储从客户端收到的证书链并定期重新对其进行身份验证。在普通会话建立过程中执行的所有 PKI 检查（包括签名验证、吊销检查、有效日期、密钥用法检查等）都会按配置的间隔重复执行。如果定期身份验证失败，则会注销 VPN 会话。如果成功，则会话继续。定期证书身份验证不是强制性的，并且默认情况下已禁用。

备注　当前支持 IKEv2 的以下功能：如果使用即将到期的证书启动会话，则证书到期后，系统随即会注销该会话。此功能照常继续运行。

限制

定期证书身份验证不适用于任何其他非 VPN 会话/连接。所有 VPN 会话都支持定期证书身份验证（IKEv1 RA 和 L2L、IKEv2 RA 和 L2L [包括基于第三方标准的 SSL 客户端和无客户端]，以及 L2TP 和 EZVPN）。

缓存 CRL

ASA 会将证书验证过程中收到的 CRL 缓存一段时间（持续时间可配置），并在该段时间内将其重用于验证其他证书。通过缓存，无需在每次连接尝试时都重复向服务器请求 CRL 并进行验证，从而实现性能优势。定期证书验证类似于普通证书验证。

吊销检查

可以使用 *none* 选项配置 ASA 来进行吊销检查以及 CRL 或 OCSP 检查：

```
revocation-check [crl] [ocsp] [none]
```

如果缓存中没有 CRL，则配置有 *none* 选项的第一个连接将生成 CRL 的请求，而无需等待响应。系统会在未进行吊销状态检查的情况下成功建立第一个此类连接。在缓存中没有 CRL 的第一个连接始终跳过吊销检查。如果 CRL 下载失败，或者 CRL/OCSP 服务器无法访问，则保留原始行为并保持连接。普通身份验证和定期身份验证之间的区别在于，通过定期重复身份验证，系统始终会尝试检索 CRL 并等待其响应。如果无法检索 CRL，则使用收到的 CRL 检查证书时，行为类似于普通身份验证，并且允许连接。当禁用吊销检查时，定期验证会执行通常在会话建立过程中执行的所有其他检查。

本地 CA

使用由本地 CA 颁发的证书的 VPN 会话还可以执行定期证书验证，包括吊销检查，就像对待第三方 CA 颁发的证书一样。

非活动会话

在 IKEv2 或 SSL 隧道发生故障后， AnyConnect 会话可能会进入非活动状态。会话会继续存在，以允许在不重新进行身份验证的情况下恢复会话。与普通会话类似，非活动会话使用初始连接过程中提供的证书继续执行定期身份验证。非活动会话也可以根据定期身份验证结果进行注销。

故障切换

客户端证书在会话初始化过程中同步到备用设备。主用和备用设备将维护和管理各自的独立数据库，以在会话启动和关闭时存储这些证书。数据库经过优化可避免存储重复的 CA 证书。因为 ID 证书通常对于每个会话都是唯一的，所以系统不会对 ID 证书执行重复检查。

集群

集群仅支持 L2L VPN。此外，系统仅会建立到主设备的 VPN 会话且不会将其同步到任何其他设备。如果主设备发生故障，则需要重新建立会话。

设置证书到期提醒 （用于身份证书或 CA 证书）

ASA 每隔 24 小时检查一次信任点中的所有 CA 和 ID 证书是否到期。如果证书即将到期，则会将一条系统日志作为警报发出。

系统提供 CLI 来配置提醒和循环间隔。默认情况下，在到期前 60 天开始提醒并且每 7 天循环提醒一次。您可以通过使用以下命令配置提醒发送间隔和发送第一个提醒时的到期前天数：

```
[no] crypto ca alerts expiration [begin <days before expiration>] [repeat <days>]
```

无论提醒如何配置，系统都会在到期前的最后一周内每天发送提醒。此外，还添加了以下 show 和 clear 命令：

```
clear conf crypto ca alerts
show run crypto ca alerts
```

除了续签提醒之外，如果系统在配置中找到已到期证书，则每天会生成一次系统日志，以通过续签证书或删除已到期证书来调整配置。

例如，假设到期提醒配置为在到期前 60 天开始，此后每 6 天重复提醒一次。如果 ASA 在到期前 40 天重新启动，则系统当日会发送提醒，并在第 36 天发送下一个提醒。

备注　对于信任池证书不会执行到期检查。本地 CA 信任点会被视为也需要进行到期检查的普通信任点。

启用/禁用定期证书验证

您可以在 group-policy attributes 配置模式下启用/禁用定期证书验证：

```
[no] periodic-authentication certificate <time in hours> | none
```

默认情况下会禁用定期证书验证 （periodic-authentication certificate 设置为 none）。

如果启用，您可以配置介于 1 和 168 小时之间的间隔。

执行基本约束

基本约束扩展可确定 CA 证书的使用者，以及包含此证书的有效证书路径的最大深度。cA 布尔值指示已认证公钥是否用于验证证书签名。如果未断言 cA 布尔值，则不得断言密钥用法扩展中的 keyCertSign 位。如果在版本 3 中不存在基本约束扩展，或者扩展存在但未断言 cA 布尔值，则已认证公钥不得用于验证证书签名。

默认情况下，不带有 CA 标志证书不能作为 CA 证书安装在 ASA 上。系统会提供 CLI 按钮来允许为现有客户安装这些证书：

```
ciscoasa(config-ca-trustpoint)# ca-check
ciscoasa (config-ca-trustpoint)# show run crypto ca trustpoint new
crypto ca trustpoint new
enrollment terminal
crl configure

ciscoasa (config-ca-trustpoint)# no ca-check
ciscoasa (config-ca-trustpoint)# show run crypto ca trustpoint new
crypto ca trustpoint new
enrollment terminal
no ca-check
crl configure
```

监控数字证书

请参阅以下用于监控数字证书状态的命令：

- **show crypto ca server**

  此命令显示本地 CA 配置和状态。

- **show crypto ca server cert-db**

  此命令显示由本地 CA 颁发的用户证书。

- **show crypto ca server certificate**

  此命令以 base 64 格式显示控制台上的本地 CA 证书以及滚动更新证书 （可用时），包括用于在新证书导入到其他设备时对其进行验证的滚动更新证书指纹。

- **show crypto ca server crl**

  此命令显示 CRL。

- **show crypto ca server user-db**

  此命令显示用户及其状态，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。仅显示已注册并持有有效证书的用户。
  - expired。仅显示持有已到期证书的用户。
  - 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**

  此命令显示符合注册条件的用户。
- **show crypto ca server user-db enrolled**

  此命令显示具有有效证书的已注册用户。
- **show crypto ca server user-db expired**

  此命令显示具有过期证书的用户。
- **show crypto ca server user-db on-hold**

  此命令显示无证书且不允许注册的用户。
- **show crypto key** *name of key*

  此命令显示您已生成的密钥对。
- **show running-config**

  此命令显示本地 CA 证书映射规则。

示例

以下示例显示 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
```

以下示例显示本地 CA CRL：

```
ciscoasa(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
```

以下示例显示一个暂停用户：

```
ciscoasa(config)# show crypto ca server user-db on-hold
username: wilma101
email:    <None>
dn:       <None>
allowed:  <not allowed>
notified: 0
ciscoasa(config)#
```

以下示例显示 **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
```

证书管理历史记录

表 18-1　　证书管理历史记录

功能名称	平台版本	说明
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者证书）是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、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)	引入了以下命令： **issuer-name** *DN-string?***revocation-check crl none**、**revocation-check crl**、 **revocation-check none**。 废弃了以下命令：**crl** {**required** | **optional** | **nocheck**}。

表 18-1　　证书管理历史记录 （续）

功能名称	平台版本	说明
证书管理	8.0(2)	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)	引入了此功能，可从第三方 CA 对设备证书进行安全部署。 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 5 部分

IP 路由



第 19 章

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。所谓路由是指通过网络将信息从源发送到目标的活动。在途中通常会经过至少一个中间节点。路由涉及两个基本活动：确定最佳路由路径和通过网络传输数据包。

- 路径确定，第 19-1 页
- 支持的路由类型，第 19-2 页
- 路由在 ASA 中的工作方式，第 19-3 页
- 支持的互联网路由协议，第 19-4 页
- 路由表，第 19-5 页
- 禁用代理 ARP 请求，第 19-8 页
- 显示路由表，第 19-9 页

路径确定

路由协议使用指标来评估传播数据包的最佳路径。指标是一种测量标准，例如供路由算法用于确定目标的最佳路径的路径带宽。为帮助执行确定路径的过程，路由算法会初始化和维护其中包含路由信息的路由表。路由信息根据所使用的路由算法而异。

路由算法使用各种信息来填充路由表。目标或下一跳关联告知路由器，可以通过将数据包发送到特定路由器 （表示通往最终目标的下一跳）来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。路由器通过比较指标来确定最佳路由，而这些指标根据所使用的路由算法的设计而异。

路由器互相进行通信，并通过传输各种消息来维护其路由表。路由更新消息是通常由路由表的全部或部分内容组成的消息。通过分析来自所有其他路由器的路由更新，路由器可以构建详细的网络拓扑图。链路状态通告 （路由器之间发送的另一种消息）用于告知其他路由器发送方链路的状态。链路信息还可用于构建完整网络拓扑图，以使路由器能够确定通向网络目标的最佳路径。

备注 在多情景模式下，仅主用/主用故障切换支持非对称路由。

支持的路由类型

路由器可以使用多种路由类型。ASA 使用以下路由类型：

- 静态与动态，第 19-2 页
- 单路径与多路径，第 19-2 页
- 平面与分层，第 19-2 页
- 链路状态与距离矢量，第 19-3 页

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。除非网络管理员修改这些映射，否则映射不会发生更改。使用静态路由的算法设计简单，并且在网络流量相对可预测且网络设计相对简单的环境下适用。

由于静态路由系统无法对网络更改作出反应，因此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，则路由软件会重新计算路由并发出新的路由更新消息。这些消息会渗入网络，促使路由器重新运行其算法并相应地更改其路由表。

可以酌情使用静态路由对动态路由算法进行补充。例如，可以将必备路由器 （所有无法路由的数据包都发送到该路由器）指定为所有无法路由的数据包的存储库，从而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个路径。与单路径算法不同，这些多路径算法允许流量在多条线路上多路复用。多路径算法的优势在于显著提高吞吐量和可靠性，通常称为负载共享。

平面与分层

某些路由算法在平面空间中运行，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。在分层路由系统中，某些路由器形成实际上的路由主干。来自非主干路由器的数据包会传播到主干路由器，在此数据包通过主干进行发送，直至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播到最终目标。

路由系统往往指定逻辑节点组，称为域、自治系统或区域。在分层系统中，某个域中的一些路由器可以与其他域中的路由器进行通信，而其他路由器只能与其本域中的路由器进行通信。在超大网络中，还可能存在其他分层级别，其中位于最高分层级别的路由器形成路由主干。

分层路由的主要优点在于，它会模仿大多数公司的组织，从而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知道其域中的其他路由器即可，因此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。

链路状态与距离矢量

链路状态算法 （也称最短路径优先算法）将路由信息以泛洪形式发送给互联网络中的所有节点。但是，每条路由器仅发送用于说明其自身链路状态的路由表部分。在链路状态算法中，每条路由器在其路由表中构建整个网络的情景。距离矢量算法（也称为 Bellman-Ford 算法）要求每条路由器仅向其邻居发送其路由表的全部或部分内容。实质上，链路状态算法会四处发送小的更新，而距离矢量算法只将较大的更新发送给相邻路由器。距离矢量算法仅知道其邻居。通常，链路状态算法与 OSPF 路由协议结合使用。

路由在 ASA 中的工作方式

ASA 同时使用路由表和 XLATE 表来决定路由。为了处理目标 IP 转换流量，即未转换流量，ASA 会搜索现有 XLATE 或静态转换来选择传出接口。

- 传出接口选择过程，第 19-3 页
- 下一跳选择过程，第 19-3 页
- ECMP 路由，第 19-4 页

传出接口选择过程

选择过程遵循以下步骤：

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，并且系统会创建 XLATE，而不使用路由表。
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 通过查询路由以选择传出接口来处理此数据包，然后执行源 IP 转换 （如有必要）。

   对于常规动态出站 NAT，将会使用路由表，然后创建 XLATE 来对初始传出数据包进行路由。仅使用现有 XLATE 转发传入返回数据包。对于静态 NAT，始终使用现有 XLATE 或静态转换规则来转发目标转换的传入数据包。

下一跳选择过程

在使用之前描述的任何方法选择传出接口之后，要另外执行路由查询，以找到属于之前选择的传出接口的合适下一跳。如果路由表中没有明确属于所选接口的路由，则会丢弃数据包并生成 6 级系统日志消息 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也如此。如果找到属于所选传出接口的路由，则会将数据包转发到相应的下一跳。

只有在使用单个传出接口可提供能够多个下一跳时，才能在 ASA 上实现负载共享。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 创建后发生更改 （例如路由摆动），则仍然使用原先的 XLATE 而非路由表转发目标转换流量，直至 XLATE 超时。如果从旧接口中删除旧路由并通过路由进程将其附加到另一个接口，则流量会转发到错误的接口，或者被丢弃并生成 6 级系统日志消息 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，可能会发生同样的问题。可能会使用错误的传出接口转发回目标转换返回数据包。

在某些安全流量配置中，几乎任何流量都可能根据流量中初始数据包的方向进行源转换或目标转换，因此很可能会发生该问题。当在路由摆动后发生该问题时，可使用 **clear xlate** 命令手动解决或通过 XLATE 超时自动解决该问题。如有必要，可以减小 XLATE 超时。为保证极少出现该问题，请确保在 ASA 上及其周围不存在路由摆动。也就是说，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 进行转发。

ECMP 路由

ASA 支持等价多路径 (ECMP) 路由。

如果没有区域，每个接口最多支持 3 个等价静态或动态路由。例如，您可以在指定不同网关的外部接口上配置三个默认路由：

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

在这种情况下，流量在外部接口上的 10.1.1.2、 10.1.1.3 和 10.1.1.4 之间进行负载均衡。流量基于散列源和目标 IP 地址的算法在指定网关之间进行分发。

不支持跨多个接口执行 ECMP，因此您不能在不同接口上定义到同一目标的路由。使用上述任一路由配置时，不允许使用以下路由：

```
route outside2 0 0 10.2.1.1
```

如果有区域，在一个区域中最多可以跨 8 个接口配置最多 8 个等价静态或动态路由。例如，您可以在区域中跨三个接口配置三个默认路由：

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

同样，动态路由协议可以自动配置等价路由。ASA 使用更稳健的负载均衡机制跨接口对流量进行负载均衡。

当某条路由丢失时， ASA 将流量无缝移至其他路由。

支持的互联网路由协议

ASA 支持多种互联网路由协议。本节对每种协议进行简单介绍。

- 增强型内部网关路由协议 (EIGRP)

  EIGRP 是思科专有协议，用于提供与 IGRP 路由器的兼容性和无缝互操作性。通过自动重分发机制，可将 IGRP 路由导入到增强型 IGRP，反之亦然，从而可以将增强型 IGRP 逐渐添加到现有 IGRP 网络。

  有关配置 EIGRP 的详细信息，请参阅配置 EIGRP，第 25-2 页。

- 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) 工作小组开发的面向互联网协议 (IP) 网络的路由协议。OSPF 使用链路状态算法构建和计算所有到达已知目标的最短路径。OSPF 区域中的每条路由器包含相同的链路状态数据库，该数据库是由每条路由器可使用的接口和可访问邻居组成的列表。

  有关配置 OSPF 的详细信息，请参阅配置 OSPFv2，第 24-5 页。

- 路由信息协议 (RIP)

  RIP 是一种使用跳数作为指标的距离矢量协议。RIP 广泛用于路由全局互联网中的流量，并且是一种内部网关协议 (IGP)，意味着在单个自治系统内执行路由。

  有关配置 RIP 的详细信息，请参阅传统功能指南。

- 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，并且是互联网运营商 (ISP) 之间所使用的协议。客户连接到 ISP，然后 ISP 使用 BGP 交换客户路由和 ISP 路由。在自治系统 (AS) 之间使用 BGP 时，该协议称为外部 BGP (EBGP)。如果运营商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

  有关配置 BGF 的详细信息，请参阅配置 BGP，第 23-3 页。

路由表

- 如何填充路由表，第 19-5 页
- 如何制定转发决策，第 19-7 页
- 动态路由和故障切换，第 19-7 页
- 动态路由和集群，第 19-7 页
- 多情景模式下的动态路由，第 19-8 页

如何填充路由表

ASA 路由表可由静态定义的路由、直连路由以及通过 RIP、EIGRP、OSPF 和 BGP 路由协议发现的路由进行填充。由于 ASA 除具有路由表中的静态路由和已连接路由外，还可以运行多条路由协议，因此可通过多种方式发现或输入同一路由。当在路由表中放入同一目标的两条路由时，将按如下确定保留在路由表中的路由：

- 如果两个路由具有不同的网络前缀长度 （网络掩码），则会将两个路由都视为唯一并输入到路由表中。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，但由于两条路由具有不同的前缀长度 （子网掩码），因此均会安装在路由表中。这两条路由被视为不同目标，数据包转发逻辑会确定使用哪条路由。

- 如果 ASA 从单个路由协议 （例如 RIP）获悉通向同一目标的多条路径，则会在路由表中输入具有更佳指标的路由 （由路由协议确定）。

  指标是与特定路由关联的值，从最高优先到最低优先进行排序。用于确定指标的参数根据路由协议而异。具有最低指标的路径选择作为最佳路径并安装在路由表中。如果有多个指标相等的通向同一目标的路径，则会在这些等价路径上进行负载均衡。

- 如果 ASA 从多个路由协议获悉目标，则会比较路由的管理距离，并在路由表中输入管理距离较短的路由。

路由的管理距离

您可以更改由路由协议发现或重分发到路由协议中的路由的管理距离。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，则会将具有较短*默认*管理距离的路由输入到路由表中。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。

管理距离是 ASA 在有两个或多个通向同一目标 （来自两个不同路由协议）的路由时，用于选择最佳路径的路由参数。由于路由协议具有基于不同于其他协议的算法的指标，因此并非总能够确定通向由不同路由协议生成的同一目标的两条路由的最佳路径。

每个路由协议使用管理距离值划分优先级。表 19-1 显示 ASA 支持的路由协议的默认管理距离值。

表 19-1　　受支持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
Unknown	255

管理距离值越小，协议的优先等级越高。例如，如果 ASA 从 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）均收到通向特定网络的路由，则 ASA 会选择 OSPF 路由，因为 OSPF 具有更高的优先级。在这种情况下，路由器会将 OSPF 版本的路由添加到路由表。

在本示例中，如果 OSPF 派生路由的源丢失 （例如，由于电源关闭），则 ASA 会使用 RIP 派生路由，直至 OSPF 派生路由再次出现。

管理距离是一项本地设置。例如，如果您使用 **distance-ospf** 命令更改通过 OSPF 获取的路由的管理距离，则该更改仅会影响输入了该命令的 ASA 上的路由表。在路由更新中不会通告管理距离。

管理距离不影响路由进程。EIGRP、 OSPF、 RIP 和 BGP 路由进程仅通告路由进程已发现或重分发到路由进程中的路由。例如，即使在 ASA 路由表中使用 OSPF 路由进程发现的路由，RIP 路由进程也会通告 RIP 路由。

备用路由

当由于安装另一条路由而导致初始尝试将路由安装在路由表中失败时，系统会注册备用路由。如果安装在路由表中的路由失败，则路由表维护进程会呼叫已注册备用路由的每个路由协议进程，并请求它们重新在路由表中安装此路由。如果有多个协议为失败路由注册了备用路由，则根据管理距离选择优先路由。

鉴于以上过程，当动态路由协议发现的路由失败时，您可以创建安装在路由表中的浮动静态路由。浮动静态路仅仅是配置有比 ASA 上运行的动态路由协议更大的管理距离的静态路由。当动态路由进程发现的对应路由失败时，会在路由表中安装静态路由。

如何制定转发决策

系统按如下制定转发决策：

- 如果目标不匹配路由表中的条目，则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，则会丢弃数据包。
- 如果目标匹配路由表中的单个条目，则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，并且所有条目都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在路由表中共存。
- 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 的数据包到达在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 位对比 19 位）。在转发数据包时，较长前缀始终优先于较短的前缀。

动态路由和故障切换

当路由表在主用设备上发生更改时，备用设备上的动态路由会进行同步，意味着主用设备上的所有添加、删除或更改都会立即传播到备用设备。如果在主设备进入主用状态一段时间之后，备用设备也进入主用状态，则路由在故障切换批量同步进程中会同步，因此主用/备用故障切换对上的路由表应看似相同。

动态路由和集群

动态路由完全集成在集群中，并且路由会跨设备进行共享。路由表条目也会集群中跨设备进行复制。

当设备从从属设备过渡到主设备时，RIB 表的初始序号（32 位序列号）会递增。在过渡后，新的主设备最初拥有的 RIB 表条目是先前主设备的镜像。此外，在新的主设备上会启动再收敛计时器。当 RIB 表的初始序号递增时，所有现有条目都被视为过时。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条目表明它们已经刷新并会同步到所有从属设备。在再收敛计时器到期后，会删除 RIB 表中的旧条目。OSPF 路由、RIP 路由以及 EIGRP 路由的 RIB 表条目会同步到从属设备。

仅当某台设备加入集群时，才会从主设备到加入设备进行批量同步。

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传输将这些更新发送到所有从属设备。从属设备在收到集群路由更新消息后会更新其 RIB 表。

对于受支持的动态路由协议（OSPF、RIP 和 EIGRP），来自从属设备上跨网络 EtherChannel 接口的路由数据包会转发给主设备。只有主设备才能发现和处理动态路由协议数据包。当从属设备请求执行批量同步时，将会复制所有通过跨网络 EtherChannel 接口获悉的路由条目。

当通过主设备上的跨网络 EtherChannel 接口获悉新的路由条目时，会将新条目广播到所有从属设备。因网络拓扑更改而修改现有路由条目时，修改后的条目也会同步到所有从属设备。因网络拓扑更改而删除现有路由条目时，已删除的条目也会同步到所有从属设备。

在多情景模式下，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。

如果配置单独接口，则还必须配置路由器 ID 池设置。

多情景模式下的动态路由

在多情景模式下，每个情景维护单独的路由表和路由协议数据库。因而您可以在每个情景中独立配置 OSPFv2 和 EIGRP。您可以在某些情景中配置 EIGRP，并在相同或不同的情景中配置 OSPFv2。在混合情景模式下，您可以在处于路由模式下的情景中启用任何动态路由协议。在多情景模式下，不支持 RIP 和 OSPFv3。

下表列出了 EIGRP 及 OSPFv2 的属性、用于将路由分发到 OSPFv2 和 EIGRP 进程中的路由映射、以及在 OSPFv2 中用于筛选路由更新 （多情景模式下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。	N/A
在系统情景中禁用。		N/A
两个情景可能使用相同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。	N/A
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 OSPP 实例。	N/A
支持跨共享接口的 EIGRP 实例交互。	支持跨共享接口的 OSPFv2 实例交互。	N/A
在单模式下可用的所有 CLI 在多情景模式下也可用。		
每个 CLI 仅在对其进行了使用的情景中起作用。		

路由资源管理

资源类 （称为*路由*）指定可存在于情景中的路由表条目的最大数量。这可解决一个情景影响另一个情景中的可用路由表条目的问题，您也可以对每个情景的最大路由条目数进行更好的控制。

由于没有明确的系统限制，因此只能为此资源限制指定绝对值，不能使用百分比限制。此外，每个情景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（已连接、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，并会生成系统日志消息。

禁用代理 ARP 请求

当主机将 IP 流量发送到同一以太网网络上的其他设备时，该主机需要知道该设备的 MAC 地址。ARP 是一个第 2 层协议，用于将 IP 地址解析为 MAC 地址。主机发送 ARP 请求，询问“谁有此 IP 地址？”拥有该 IP 地址的设备回答“我有该 IP 地址；这是我的 MAC 地址。”

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 地址也如此。当配置 NAT 并指定与 ASA 接口处于相同网络的映射地址时，ASA 使用代理 ARP。流量可到达主机的唯一方法是， ASA 使用代理 ARP 来声明 MAC 地址已分配到目标映射地址。

在极少数情况下，您可能要为 NAT 地址禁用代理 ARP。

如果 VPN 客户端地址池与现有网络重叠，则 ASA 默认在所有接口上发送代理 ARP 请求。如果有另一个接口位于同一个第 2 层域中，则该接口将会看到 ARP 请求，并以自身接口的 MAC 地址进行回应。结果将是面向内部主机的 VPN 客户端的返回流量转至错误的接口并被丢弃。在这种情况下，您应在不需要代理 ARP 请求的接口上禁用代理 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
```

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
```



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。

- 关于静态路由和默认路由，第 20-1 页
- 静态路由和默认路由准则，第 20-3 页
- 配置默认路由和静态路由，第 20-3 页
- 监控静态路由或默认路由，第 20-7 页
- 静态路由或默认路由示例，第 20-7 页
- 静态路由和默认路由的历史记录，第 20-7 页

关于静态路由和默认路由

要将流量路由到非连接的主机或网络，必须使用静态路由或动态路由定义到主机或网络的路由。通常，您必须配置至少一个静态路由：所有流量的默认路由 （不是通过其他方式路由到默认网络网关），通常是指下一跳路由器。

- 默认路由，第 20-1 页
- 静态路由，第 20-2 页
- 使用到 null0 接口的路由将不必要的流量转发到 “黑洞”，第 20-2 页
- 路由优先级，第 20-2 页
- 透明防火墙模式路由，第 20-2 页
- 等价多路径路由，第 20-2 页
- 静态路由跟踪，第 20-2 页

默认路由

最简单的方法是配置一个默认路由，将所有流量都发送到上游路由器，从而依靠该路由器来为您路由流量。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。默认静态路由是以 0.0.0.0/0 作为目标 IP 地址的静态路由。

静态路由

在以下情况下，您可能希望在单情景模式中使用静态路由：

- 网络使用不同的路由器发现协议，例如 BGP、 EIGRP、 RIP 或 OSPF。
- 网络规模较小，并且可以轻松管理静态路由。
- 不希望流量或 CPU 开销与路由协议相关联。
- 在某些情况下，仅使用默认路由并不足够。默认网关可能无法到达目标网络，因此还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法将直接流量定向到未直接与 ASA 连接的任何内部网络。

使用到 null0 接口的路由将不必要的流量转发到 “黑洞”

通过访问规则，您可以根据其报头中包含的信息过滤数据包。到 null0 接口的静态路由是访问规则的补充性解决方案。您可以使用 null0 路由将不必要或不需要的流量转发到 “黑洞”，从而丢弃该流量。

静态 null0 路由具有良好的性能配置文件。您还可以使用静态 null0 路由防止产生路由环路。BGP 可以利用静态 null0 路由进行远程触发黑洞路由。

路由优先级

- 标识具体目标的路由优先于默认路由。
- 当存在通向同一目标的多个路由 （静态或动态）时，路由的管理距离即可确定优先级。静态路由设置为 1，因此其通常是优先级最高的路由。
- 当您具有多个管理距离相同的通向同一目标的静态路由时，请参阅 ECMP 路由，第 19-4 页。
- 对于来自具有 Tunneled 选项的隧道的新流量，此路由覆盖任何其他已配置或已知悉的默认路由。

透明防火墙模式路由

在透明防火墙模式中，对于源自 ASA 并要发往非直连网络的流量，您需要配置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。如果存在无法通过单个默认路由进行访问的服务器，则必须配置静态路由。

等价多路径路由

ASA 支持等价多路径 (ECMP) 路由。有关详情，请参见 ECMP 路由，第 19-4 页。

静态路由跟踪

使用静态路由的一个问题是，缺乏用于确定路由处于开启还是关闭状态的内在机制。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，才会从路由表中删除静态路由。

静态路由跟踪功能提供在主路由发生故障的情况下跟踪静态路由的可用性和安装备用路由的方法。例如，您可以定义一个到 ISP 网关的默认路由和一个到辅助 ISP 的备用默认路由，以防止主要 ISP 变得不可用。

静态路由和默认路由准则

防火墙模式

在透明防火墙模式中不支持静态路由跟踪。

IPv6

- ASDM 透明模式不支持 IPv6 静态路由。
- IPv6 不支持静态路由跟踪。

群集

在集群中，仅在主设备上支持静态路由监控。

配置默认路由和静态路由

您至少应配置一个默认路由。您可能还需要配置静态路由。

- 配置默认路由，第 20-3 页
- 配置静态路由，第 20-4 页
- 跟踪静态路由，第 20-5 页

配置默认路由

默认路由是以 0.0.0.0/0 作为目标 IP 地址的静态路由。

准备工作

请参阅有关 Tunneled 选项的以下准则：

- 请勿在隧道路由的传出接口上启用单播 RPF （**ip verify reverse-path** 命令），因为此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，因为此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。
- 不能使用 tunneled 选项定义多个默认路由。
- 不支持隧道流量的 ECMP。

操作步骤

步骤 1　添加一个默认路由。

IPv4：

```
route if_name 0.0.0.0 0.0.0.0 gateway_ip [distance | tunneled]
```

IPv6：

ipv6 route *if_name* **::/0** *next_hop_ipv6_addr* [*distance* | **tunneled**]

示例：

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.4
ciscoasa(config)# route inside 0.0.0.0 0.0.0.0 10.1.2.3 tunneled
ciscoasa(config)# ipv6 route inside ::/0 3FFE:1100:0:CC00::1
```

if_name 是要通过其发送特定流量的接口。

distance 参数是路由的管理距离，该值介于 1 和 254 之间。如果未指定值，则默认值为 **1**。管理距离是用于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，这使其优先于动态路由协议所发现的路由，但不优先于直连路由。OSPF 所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，则静态路由优先。已连接的路由始终优先于静态路由或动态发现的路由。

注意　如果您在具有不同指标的不同接口上同时配置两个默认路由，则从具有更高指标的接口到 ASA 的连接会失败，但是从具有较低指标的接口到 ASA 的连接则会如预期成功。

您可以使用 **tunneled** 关键字为隧道路由定义单独的默认路由以及标准默认路由。使用 **tunneled** 选项创建默认路由时，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会发送到该路由。

提示　您可以为目标网络地址和掩码输入 **0 0** 而非 **0.0.0.0 0.0.0.0**，如下例所示：

```
ciscoasa(config)# route outside 0 0 192.168.2.4
```

配置静态路由

静态路由用于定义为特定目标网络发送流量的位置。

操作步骤

步骤 1　添加一个静态路由：

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
```

if_name 是要通过其发送特定流量的接口。要将不必要的流量转发到 “黑洞”，请输入 **null0** 接口。

dest_ip 和 *mask* 参数表示目标网络的 IP 地址，*gateway_ip* 参数是下一跳路由器的地址。为静态路由指定的地址是在进入 ASA 并执行 NAT 之前的数据包内的地址。

distance 参数是路由的管理距离。如果未指定值，则默认值为 **1**。管理距离是用于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，这使其优先于动态路由协议所发现的路由，但不优先于直连路由。OSPF 所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，则静态路由优先。已连接的路由始终优先于静态路由或动态发现的路由。

示例

以下示例显示 3 个通向同一网关的网络和另一个通向不同网关的网络的静态路由。

```
route outside 10.10.10.0 255.255.255.0 192.168.1.1
route outside 10.10.20.0 255.255.255.0 192.168.1.1
route outside 10.10.30.0 255.255.255.0 192.168.1.1
route inside 10.10.40.0 255.255.255.0 10.1.1.1
```

跟踪静态路由

静态路由跟踪功能提供在主路由发生故障的情况下跟踪静态路由的可用性和安装备用路由的方法。例如，您可以定义一个到 ISP 网关的默认路由和一个到辅助 ISP 的备用默认路由，以防止主要 ISP 变得不可用。

- 关于静态路由跟踪，第 20-5 页
- 配置静态路由跟踪，第 20-5 页

关于静态路由跟踪

ASA 通过将静态路由与 ASA 使用 ICMP 回应请求监控的目标网络上的监控目标主机相关联来实施静态路由跟踪。如果在指定时间内没有收到回应回复，则主机将被视为关闭，并且会从路由表中删除关联路由。使用具有较高指标的未跟踪备用路由替代已删除的路由。

选择监控目标时，您需要确保它能够响应 ICMP 回应请求。该目标可以是您选择的任何网络对象，但是应考虑使用以下对象：

- ISP 网关 （用于支持双 ISP）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，例如 ASA 需要与之进行通信的 AAA 服务器。
- 目标网络上的持久网络对象

备注　可能会在夜间关闭的 PC 不是一个理想选择。

您可以为静态定义的路由或通过 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。

配置静态路由跟踪

要配置静态路由跟踪，请完成以下步骤：

准备工作

以下对象支持静态路由跟踪：

- IPv4 流量。
- 路由防火墙模式。

操作步骤

步骤 1　定义监控进程：

sla monitor *sla_id*

示例：

```
ciscoasa(config)# sla monitor 5
ciscoasa(config-sla-monitor)#
```

步骤 2　指定监控协议、被跟踪网络上的目标主机，以及访问网络所通过的接口。

type echo protocol ipicmpecho *target_ip* **interface** *if_name*

示例：

```
ciscoasa(config-sla-monitor)# type echo protocol ipicmpecho 172.29.139.134
ciscoasa(config-sla-monitor-echo)#
```

target_ip 参数是可用性受到跟踪进程监控的网络对象的 IP 地址。当该对象可用时，跟踪进程路由会添加到路由表中。当该对象不可用时，跟踪进程删除该路由并改用备用路由进行替代。

步骤 3　（可选）配置监控选项。请参阅 《命令参考》以了解下列命令：**frequency**、 **num-packets**、 **request-data-size**、 **threshold**、 **timeout** 和 **tos**。

步骤 4　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 life forever start-time now
```

通常，您将可以使用 **sla monitor schedule** *sla_id* **life forever start-time now** 命令实施监控安排，并且允许监控配置确定进行测试的频率。

不过，您可以将监控进程安排在未来开始并仅在指定时间发生。

步骤 5　将被跟踪的静态路由与 SLA 监控进程相关联：

track *track_id* **rtr** *sla_id* **reachability**

示例：

```
ciscoasa(config)# track 6 rtr 5 reachability
```

参数 *track_id* 是使用该命令分配的跟踪号。参数 *sla_id* 是 SLA 进程的 ID 号。

步骤 6　跟踪以下路由类型之一：

- 静态路由：

  route *if_name dest_ip mask gateway_ip* [*distance*] **track** *track_id*

  示例：

  ```
  ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 track 6
  ```

  不能使用 **tunneled** 选项。

- 通过 DHCP 获取的默认路由：

  ```
  interface interface_id
    dhcp client route track track_id
    ip address dhcp setroute
  ```

- 通过 PPPoE 获取的默认路由：

```
interface interface_id
  pppoe client route track track_id
  ip address pppoe setroute
```

步骤 7　创建一个未进行跟踪的备用路由。

备用路由是与被跟踪路由通向同一目标的静态路由，但是通过不同的接口或网关。您必须为此路由分配比被跟踪路由更大的管理距离 （指标）。

监控静态路由或默认路由

- **show route**

  显示路由表。

静态路由或默认路由示例

以下示例显示如何创建静态路由，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，定义三个用于将流量定向到 dmz 接口上的三个不同网关的等价静态路由，并为隧道流量和常规流量各添加一个默认路由。

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
route inside 0 0 10.1.2.45 tunneled
```

静态路由和默认路由的历史记录

表 20-1　　静态路由和默认路由的功能历史记录

功能名称	平台版本	功能信息
静态路由跟踪	7.2(1)	静态路由跟踪功能提供在主路由发生故障的情况下跟踪静态路由的可用性和安装备用路由的方法。 引入了以下命令：**clear configure sla**、 **frequency**、 **num-packets**、 **request-data-size**、 **show sla monitor**、 **show running-config sla**、 **sla monitor**、 **sla monitor schedule**、 **threshold**、 **timeout**、 **tos**、 **track rtr**
使用静态 null0 路由将流量转发到 “黑洞”	9.2(1)	向 null0 接口发送流量会导致丢弃发往指定网络的数据包。此功能有助于为 BGP 配置远程触发黑洞 (RTBH)。 修改了以下命令：**route**。



基于策略的路由

本章介绍如何配置思科 ASA 以支持基于策略的路由 (PBR)。以下部分介绍基于策略的路由、PBR 准则和 PBR 配置。

- 关于基于策略的路由，第 21-1 页
- 基于策略的路由的准则，第 21-3 页
- 配置基于策略的路由，第 21-4 页
- 基于策略的路由示例，第 21-6 页
- 基于策略的路由的历史记录，第 21-13 页

关于基于策略的路由

典型的路由系统和协议根据流量的目标来路由流量。通过基于目标的路由系统，难以更改特定流量的路由行为。使用基于策略的路由 (PBR)，可以根据除目标网络以外的多个不同条件来定义路由行为。这些条件包括源网络或目标网络、源地址或目标地址、源端口或目标端口、协议、数据包大小和数据包分类等等。

PBR 能够通过在网络边缘分类和标记流量，然后在整个网络中使用 PBR 沿特定路径路由已标记的流量来实施服务质量 (QoS)。

这允许将源自不同来源的数据包路由到不同的网络，即使在目标相同时也如此，并且在互连多个专用网络时非常有用。

为什么使用基于策略的路由？

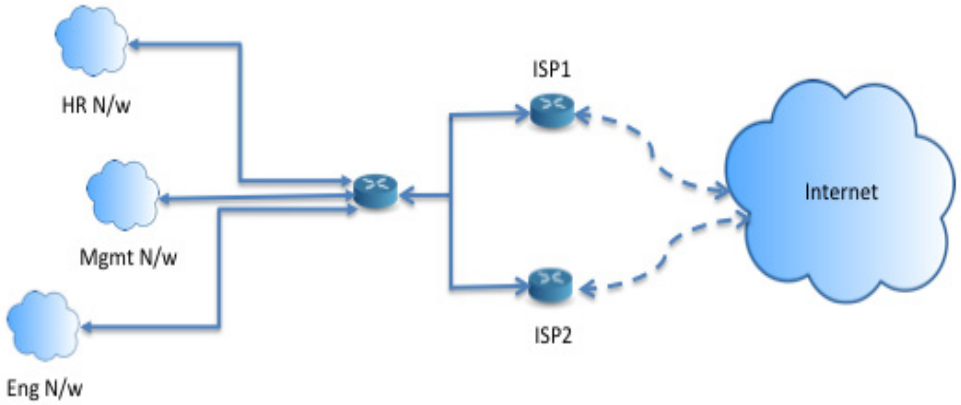
假设某公司在不同位置之间具有两个链路，一个是高带宽低延迟的昂贵链路，另一个是低带宽而延迟较高的价格更低廉链路。在使用传统路由协议时，依据带宽和/或延迟 （使用 EIGRP 或 OSPF）特征获取的节约指标，较高带宽链路会通过其发送的大部分流量。PBR 允许您通过高带宽/低延迟链路路由更高优先级的流量，并通过低带宽/高延迟链路发送所有其他流量。

以下列出了基于策略的路由的一些应用：

- 同等访问和基于源的路由
- 服务质量
- 成本节约
- 负载分担

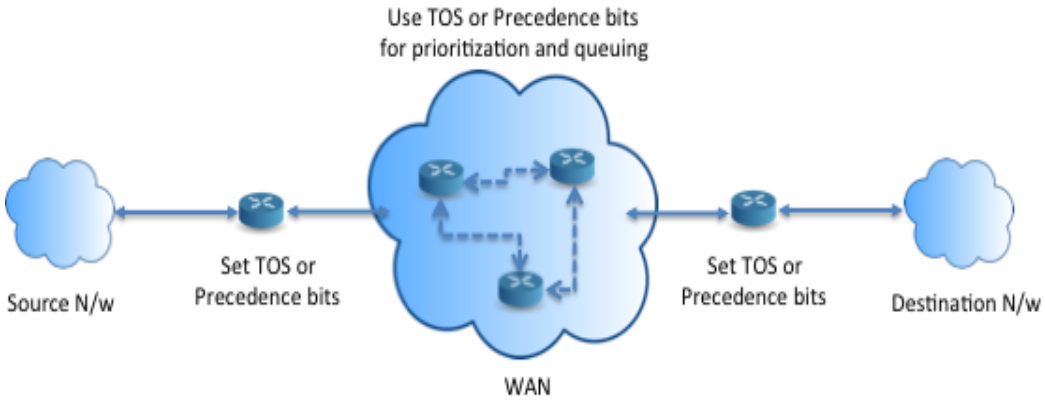
同等访问和基于源的路由

在此拓扑中，来自人力资源网络和管理网络的流量可配置为通过 ISP-1，来自工程网络的流量可配置为通过 ISP-2。因此，基于策略的路由使网络管理员能够提供同等访问和基于源的路由，如下所示。



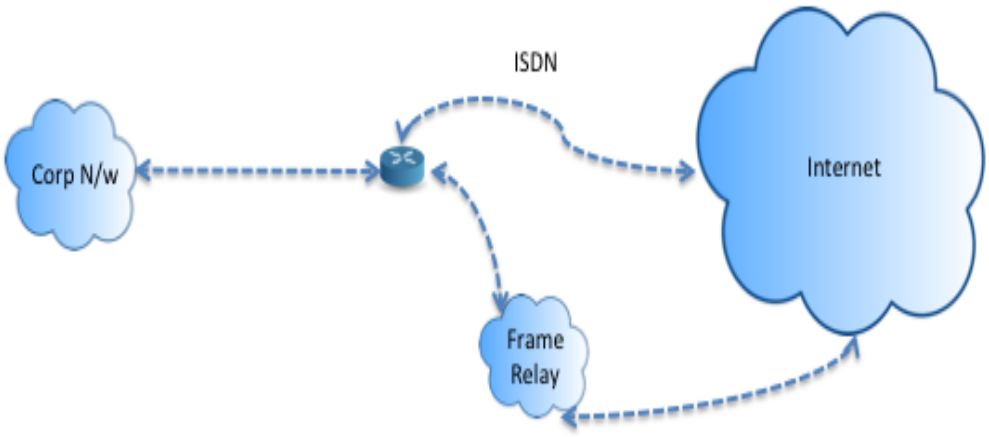
服务质量

通过标记使用基于策略的路由的数据包，网络管理员可以在网络边界对各种服务级别的网络流量进行分类，然后使用优先级、自定义或加权公平排队 （如下图所示）在网络核心中实施这些服务级别。此设置无需在主干网络核心中的每个 WAN 接口对流量进行明确分类，从而能够提升网络性能。



成本节约

组织可以通过按如下定义拓扑，将与特定活动关联的批处理流量定向为在短时间内使用较高带宽的高成本链路，并将较低带宽的低成本链路上的基本连接继续用于交互式流量。



负载分担

除 ECMP 负载均衡提供的动态负载共享功能外，网络管理员现在还可以实施策略来根据流量特征在多个路径之间分发流量。

例如，在同等访问和基于源的路由场景所描绘的拓扑中，管理员可以配置基于策略的路由来对从人力资源网络至 ISP1 的流量和从工程网络至 ISP2 的流量进行负载共享。

PBR 的实施

ASA 使用 ACL 来匹配流量，然后对流量执行路由操作。具体而言，配置指定用于进行匹配的 ACL 的路由映射，然后为该流量指定一个或多个操作。最后，将路由映射与接口相关联，在该接口上要对所有传入流量应用 PBR。

基于策略的路由的准则

防火墙模式

仅在路由防火墙模式中受支持。不支持透明防火墙模式。

群集

- 支持集群。
- 在集群场景中，如果没有静态或动态路由，但已启用 ip-verify-reverse 路径，那么可能会丢弃非对称流量。因此建议禁用 ip-verify-reverse 路径。

其他准则

- 所有现有路由映射相关的配置限制和局限性都将继续适用。

配置基于策略的路由

路由映射由一个或多个路由映射语句组成。每个语句都具有序列号，以及 permit 或 deny 语句。每个映射语句都包含 match 和 set 命令。match 命令表示要对数据包应用的匹配条件。set 命令表示要对数据包采取的操作。

- 在路由映射同时配置有 IPv4 和 IPv6 match/set 子句时或在使用了与 IPv4 和 IPv6 流量匹配的统一 ACL 时，将根据目标 IP 版本应用 set 操作。
- 当多个下一跳或接口配置为 set 操作时，所有这些选项都相继进行评估，直到找到有效的可用选项。在已配置的多个选项之间将不进行负载均衡。
- 在将具有包含 IPv6 地址的匹配 ACL 的路由映射附加到接口时，将丢弃所有 IPv6 相关 ACL 并发出警告。
- Verify-availability 选项使用跟踪对象来跟踪配置和验证已配置的下一跳的状态。由于在多模式下不支持跟踪对象配置，因此我们也将不支持 verify-availability 选项。

操作步骤

步骤 1　定义访问列表：

access-list *access_list_name* {**permit** | **deny**} **ip** {any4|ip_address...}

示例：

```
ciscoasa(config)# access-list testacl permit ip 10.1.1.0 255.255.255.0 20.1.1.0
255.255.255.0
```

步骤 2　创建路由映射条目：

route-map *name* {**permit** | **deny**} [*sequence_number*]

示例：

```
ciscoasa(config)# route-map testmap {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。

备注　当配置的路由映射不带允许或拒绝操作且没有序列号时，默认情况下将假设操作为允许且序列号为 10

步骤 3　使用访问列表定义要应用的匹配条件：

match ip-address <*access-list name*> [*access-list name*]

示例：

```
ciscoasa(config-route-map)# match ip-address testacl
```

步骤 4　指示用于输出为策略路由传递路由映射匹配子句的数据包的目标位置：

set ip default next-hop [*ip_address/ ipv6_address*]

示例：

```
ciscoasa(config-route-map)# set ip default next-hop 10.86.118.3
```

步骤 5　配置一个或多个操作：

- 设置递归下一跳 IP 地址：

  set ip next-hop recursive *ip_address*

  示例：

  ```
  ciscoasa(config-route-map)# set ip next-hop recursive 10. 86.118.1
  ```

- 验证路由映射的下一跳是否是思科发现协议 (CDP) 邻居，然后再策略路由至这些下一跳：

  set ip next-hop verify-availability *next-hop-address sequence number* **track** *object*

  示例：

  ```
  ciscoasa(config-route-map)# set ip next-hop verify-availability 10.86.118.3 56 track
  10
  ```

- 设置数据包的输出接口：

  set interface *interface_name*
  或
  set interface null0

  示例：

  ```
  ciscoasa(config-route-map)# set interface GigabitEthernet0/0
  ```

- 在 IP 报头中设置不分段 (DF) 位值：

  ```
  set ip df {0|1}
  ```

  示例：

  ```
  ciscoasa(config-route-map)# set ip df 0
  ```

- 通过在数据包中设置差分服务代码点 (DSCP) 或 IP 优先值对 IP 流量进行分类：

  set ip dscp *new-dscp*

  示例：

  ```
  ciscoasa(config-route-map)# set ip dscp af33
  ```

注意　当配置了多个 set 操作时， PBR 将按以下顺序对其进行评估：
set ip next-hop verify-availability
set ip next-hop
set ip next-hop recursive
set interface
set ip default next-hop
set default interface

步骤 6　配置接口并进入接口配置模式：

interface *physical_interface*

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
```

步骤 7　为通过框的流量配置基于策略的路由：

policy-route route-map *route-map_name*

示例：

```
ciscoasa(config-if)# policy-route route-map testmap
```

基于策略的路由示例

路由映射配置示例

在以下示例中，由于未指定操作和顺序，因此假设隐式操作为允许且序列号为 10：

```
ciscoasa(config)# route-map testmap
```

在以下示例中，由于未指定匹配条件，因此假设隐式匹配为 “any”：

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10
```

在本示例中，与 <acl> 匹配的所有流量都将通过外部接口进行策略路由和转发。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
ciscoasa(config-route-map)# set interface outside
```

在本示例中，由于未配置接口或下一跳操作，因此与 <acl> 匹配的所有流量都将根据配置修改 df 位字段和 dscp 字段，并使用普通路由进行转发

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
set ip df 1
set ip precedence af11
```

在以下示例中，与 <acl_1> 匹配的所有流量都使用下一跳 1.1.1.10 进行转发，与 <acl_2> 匹配的所有流量都使用下一跳 2.1.1.10 进行转发，并会丢弃其余流量。 “match”条件并不暗示隐式匹配 “any”。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl_1>
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address <acl_2>

ciscoasa(config-route-map)# set ip next-hop 2.1.1.10
ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# set interface Null0
```

在以下示例中，路由映射评估结果将是 (i) 路由映射操作 permit 和 acl 操作 permit 将应用 set 操作 (ii) 路由映射操作 deny 和 acl 操作 permit 将跳至普通路由查找 (iii) 路由映射操作 permit/deny 和 acl 操作 deny 将继续处理下一个路由映射条目。当没有下一个路由映射条目可用时，将不会回退到普通路由查找。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address permit_acl_1 deny_acl_2
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap deny 20
ciscoasa(config-route-map)# match ip address permit_acl_3 deny_acl_4
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10

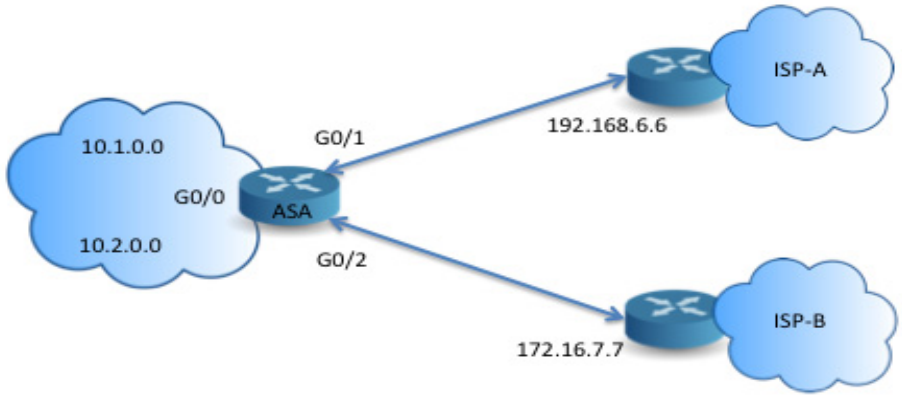
ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# match ip address deny_acl_5
ciscoasa(config-route-map)# set interface outside
```

在以下示例中，当配置了多个 set 操作时，将按照上述顺序对其进行评估。仅当 set 操作的所有选项都已评估且无法应用时，才会考虑后续 set 操作。此排序将确保首先尝试可用性最高且距离最近的下一跳，然后尝试下一个可用性最高且距离最近的下一跳，依此类推。

```
ciscoasa(config)#route-map testmap permit 10
ciscoasa(config-route-map)# match ip address acl_1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.10 1 track 1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.11 2 track 2
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.12 3 track 3
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10 2.1.1.11 2.1.1.12
ciscoasa(config-route-map)# set ip next-hop recursive 3.1.1.10
ciscoasa(config-route-map)# set interface outside-1 outside-2
ciscoasa(config-route-map)# set ip default next-hop 4.1.1.10 4.1.1.11
ciscoasa(config-route-map)# set default interface Null0
```

PBR 配置示例

本节介绍为以下场景配置 PBR 所需的全套配置：



首先，需要配置接口。

```
(config)# interface GigabitEthernet0/0
(config-if)# no shutdown
(config-if)# nameif inside
(config-if)# ip address 10.1.1.1 255.255.255.0

(config)# interface GigabitEthernet0/1
(config-if)# no shutdown
```

```
(config-if)# nameif outside-1
(config-if)# ip address 192.168.6.5 255.255.255.0

(config)# interface GigabitEthernet0/2
(config-if)# no shutdown
(config-if)# nameif outside-2
(config-if)# ip address 172.16.7.6 255.255.255.0
```

然后，需要配置访问列表来匹配流量。

```
(config)# access-list acl-1 permit ip 10.1.0.0 255.255.0.0
(config)# access-list acl-2 permit ip 10.2.0.0 255.255.0.0
```

需要通过将上述访问列表配置为匹配条件以及所需的 set 操作来配置路由匹配。

```
(config)# route-map equal-access permit 10
(config-route-map)# match ip address acl-1
(config-route-map)# set ip next-hop 192.168.6.6

(config)# route-map equal-access permit 20
(config-route-map)# match ip address acl-2
(config-route-map)# set ip next-hop 172.16.7.7

(config)# route-map equal-access permit 30
(config-route-map)# set ip interface Null0
```

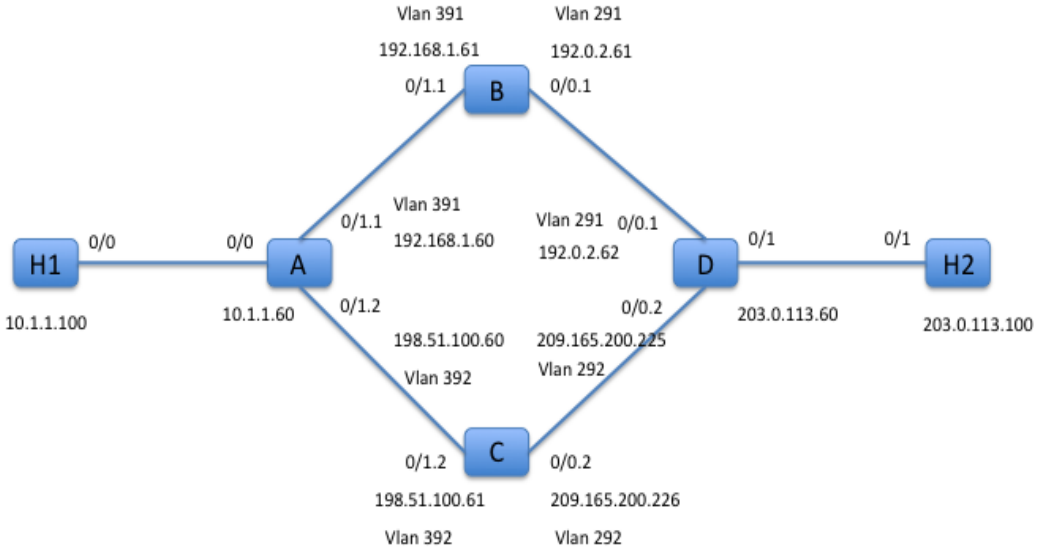
现在，此路由映射必须附加到接口。

```
(config)# interface GigabitEthernet0/0
(config-if)# policy-route route-map equal-access
```

显示策略路由配置。

```
(config)# show policy-route
Interface                   Route map
GigabitEthernet0/0   equal-access
```

操作中的基于策略的路由



我们将使用上述测试设置来配置具有不同匹配条件和 set 操作的基于策略的路由，以及了解其如何评估和应用。

首先，对设置中涉及的所有设备进行基本配置。此处，假设 A、B、C 和 D 是 ASA 设备，H1 和 H2 是 IOS 路由器。

ASA-A：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 15.1.1.60 255.255.255.0
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 25.1.1.60 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 35.1.1.60 255.255.255.0
```

ASA-B：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 45.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 25.1.1.61 255.255.255.0
```

ASA-C：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 55.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 35.1.1.61 255.255.255.0
```

ASA-D：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config) #interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif inside-1
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 45.1.1.62 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif inside-2
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 55.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
```

```
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 65.1.1.60 255.255.255.0
```

H1：

```
ciscoasa(config)# interface Loopback1
ciscoasa(config-if)# ip address 15.1.1.100 255.255.255.255

ciscoasa(config-if)# interface Loopback2
ciscoasa(config-if)# ip address 15.1.1.101 255.255.255.255

ciscoasa(config)# ip route 0.0.0.0 0.0.0.0 15.1.1.60
```

H2：

```
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# ip address 65.1.1.100 255.255.255.0

ciscoasa(config-if)# ip route 15.1.1.0 255.255.255.0 65.1.1.60
```

我们将在 ASA-A 上配置 PBR 以路由源自 H1 的流量。

ASA-A：

```
ciscoasa(config-if)# access-list pbracl_1 extended permit ip host 15.1.1.100 any

ciscoasa(config-if)# route-map testmap permit 10
ciscoasa(config-if)# match ip address pbracl_1
ciscoasa(config-if)# set ip next-hop 25.1.1.61

ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map testmap

ciscoasa(config-if)# debug policy-route
```

H1：ping 65.1.1.100 repeat 1 source loopback1

```
pbr: policy based route lookup called for 15.1.1.100/44397 to 65.1.1.100/0 proto 1
sub_proto 8 received on interface inside
pbr: First matching rule from ACL(2)
pbr: route map testmap, sequence 10, permit; proceed with policy routing
pbr: evaluating next-hop 25.1.1.61
pbr: policy based routing applied; egress_ifc = outside : next_hop = 25.1.1.61
```

数据包使用路由映射中的下一跳地址按预期进行转发。

当配置了下一跳时，将在输入路由表中执行查找，以确定到所配置的下一跳的已连接路由，并使用对应的接口。此示例的输入路由表（其中匹配的路由条目突出显示）显示如下。

```
 in   255.255.255.255 255.255.255.255 identity
 in   15.1.1.60       255.255.255.255 identity
```

```
 in   25.1.1.60       255.255.255.255 identity
 in   35.1.1.60       255.255.255.255 identity
 in   10.127.46.17    255.255.255.255 identity
 in   15.1.1.0        255.255.255.0   inside
 in   25.1.1.0        255.255.255.0   outside
 in   35.1.1.0        255.255.255.0   dmz
```

接下来，将 ASA-A 配置为从 H1 loopback2 将数据包路由出 ASA-A dmz 接口。

```
ciscoasa(config)# access-list pbracl_2 extended permit ip host 15.1.1.101 any

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address pbracl
ciscoasa(config-route-map)# set ip next-hop 35.1.1.61

ciscoasa(config)# show run route-map
!
route-map testmap permit 10
  match ip address pbracl_1
  set ip next-hop 25.1.1.61
!
route-map testmap permit 20
  match ip address pbracl
  set ip next-hop 35.1.1.61
!
```

H1：ping 65.1.1.100 repeat 1 source loopback2

错误显示如下：

```
pbr: policy based route lookup called for 15.1.1.101/1234 to 65.1.1.100/1234 proto 6
sub_proto 0 received on interface inside
pbr: First matching rule from ACL(3)
pbr: route map testmap, sequence 20, permit; proceed with policy routing
pbr: evaluating next-hop 35.1.1.61
pbr: policy based routing applied; egress_ifc = dmz : next_hop = 35.1.1.61
```

并且，从输入路由表选择的路由条目显示如下：

```
 in   255.255.255.255 255.255.255.255 identity
 in   15.1.1.60       255.255.255.255 identity
 in   25.1.1.60       255.255.255.255 identity
 in   35.1.1.60       255.255.255.255 identity
 in   10.127.46.17    255.255.255.255 identity
 in   15.1.1.0        255.255.255.0   inside
 in   25.1.1.0        255.255.255.0   outside
 in   35.1.1.0        255.255.255.0   dmz
```

基于策略的路由的历史记录

表 21-1　　路由映射的历史记录

功能名称	平台版本	功能信息
基于策略的路由	9.4(1)	基于策略的路由 (PBR) 是一种机制，基于该机制，流量可以使用 ACL，通过带有指定 QoS 的特定路径进行路由。基于数据包的第 3 层和第 4 层报头的内容， ACL 可以对流量进行分类。管理员通过此解决方案可向不同的流量提供 QoS，在低带宽、低成本永久路径与高带宽、高成本交换式路径之间分发交互式和批处理流量，并允许互联网运营商和其他组织通过明确定义的互联网连接来路由源自各类用户的流量。 引入了以下命令：**set ip next-hop verify-availability**、**set ip next-hop**、 **set ip next-hop recursive**、 **set interface**、 **set ip default next-hop**、 **set default interface**、 **set ip df**、 **set ip dscp**、 **policy-route route-map**、 **show policy-route** 和 **debug policy-route**
IPv6 支持前缀规则	9.3.2	引入了此功能。
路由映射的基于策略的路由	9.4.1	基于策略的路由 (PBR) 是一种机制，基于该机制，流量可以使用 ACL，通过带有指定 QoS 的特定路径进行路由。基于数据包的第 3 层和第 4 层报头的内容， ACL 可以对流量进行分类。管理员通过此解决方案可向不同的流量提供 QoS，在低带宽、低成本永久路径与高带宽、高成本交换式路径之间分发交互式和批处理流量，并允许互联网运营商和其他组织通过明确定义的互联网连接来路由源自各类用户的流量。 引入了以下命令：**set ip next-hop verify-availability**、**set ip next-hop**、 **set ip next-hop recursive**、 **set interface**、 **set ip default next-hop**、 **set default interface**、 **set ip df**、 **set ip dscp**、 **policy-route route-map**、 **show policy-route** 和 **debug policy-route**



路由映射

本章介绍如何为思科 ASA 配置和自定义路由映射。

- 关于路由映射，第 22-1 页
- 路由映射准则，第 22-3 页
- 定义路由映射，第 22-4 页
- 自定义路由映射，第 22-4 页
- 路由映射的配置示例，第 22-6 页
- 路由映射的功能历史记录，第 22-6 页

关于路由映射

在将路由重新分发到 OSPF、 RIP、 EIGRP 或 BGP 路由进程时会使用路由映射。在为 OSPF 路由进程生成默认路由时也会使用路由映射。路由映射定义了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。

路由映射与广为人知的 ACL 具有许多相同功能。以下是两者共有的一些特征：

- 它们都是单独语句的有序序列，各自具有允许或拒绝结果。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相关联的操作。
- 它们是通用机制 - 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 确定特定路由能够 （路由匹配 ACL permit 语句）或不能 （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，而且还会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路由。
- 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到达路由映射的结尾，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不匹配，则会拒绝路由重新分发，就如同路由映射的结尾包含 deny 语句一样。

通过动态协议 **redistribute** 命令，可以应用路由映射。在思科 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功能（请参阅定义路由映射，第 22-4 页）。如果要在重新分发期间修改路由信息，或者如果需要比 ACL 所能提供的匹配功能更强大的匹配功能，则首选路由映射。如果只是需要根据路由的前缀或掩码有选择性地允许一些路由，则建议您使用路由映射通过 **redistribute** 命令直接映射到 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有选择性地允许一些路由，则通常可以使用更多配置命令来实现相同目标。

备注　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，并且您的路由将不会重新分发。建议您以 10 为间隔对子句进行编号，为将来需要插入子句的情况保留编号空间。

- Permit 和 Deny 子句，第 22-2 页
- Match 和 Set 子句值，第 22-2 页
- BGP Match 和 BGP Set 子句，第 22-3 页
- 路由映射准则，第 22-3 页

Permit 和 Deny 子句

路由映射可以具有 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，将应用以下规则：

- 如果在使用了 permit 子句的路由映射中使用 ACL，则会重新分发 ACL 允许的路由。
- 如果在路由映射 deny 子句中使用 ACL，则不会重新分发 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，则无法找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具有两种类型的值：

- match 值用于选择应该应用此子句的路由。
- set 值用于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，则根据 permit 或 deny 子句的指示重新分发或拒绝路由，并且可能会由从 ASDM 中 Set Value 选项卡或从 **set** 命令设置的值修改其某些属性。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，直至发现子句的 **match** 命令或者根据 ASDM 中的 Match Clause 选项卡设置的 match 子句与路由匹配，或者直至到达路由映射的末尾。

如果存在下列条件中的一个，则每个子句中的 match 值或 set 值可能会缺失或多次重复：

- 如果子句中存在多个 **match** 命令或 ASDM 中的 Match Clause 值，则所有命令或值针对给定路由均成功才能使该路由与子句匹配（换句话说，针对多个 match 命令应用逻辑 AND 算法）。
- 如果 **match** 命令或 ASDM 中的 Match Clause 值在一个命令中引用多个对象，则其中一个命令或值应匹配（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 为允许，即允许路由。
- 如果 **match** 命令或 ASDM 中的 Match Clause 值不存在，则所有路由都与子句匹配。在上述示例中，到达子句 30 的所有路由都匹配；因此，永远不会到达路由映射的末尾。

- 如果 **set** 命令或 ASDM 中的 Set Value 在路由映射 permit 子句中不存在，则会重新分发路由而不修改其当前属性。

备注　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 - 没有要修改的消息。

如果路由映射子句不包含 **match** 或 **set** 命令或 ASDM 中的 Match Value 或 Set Value 选项卡中没有设置 match 值或 set 值，则该子句会执行操作。空 permit 子句允许重新分发剩余路由而不进行修改。空 deny 子句不允许重新分发其他路由 （如果路由映射进行完整扫描但找不到显式匹配，这将是默认操作）。

BGP Match 和 BGP Set 子句

除上述的 match 值和 set 值以外， 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，则根据 permit 或 deny 子句的指示重新分发或拒绝路由，并且可能会由从 ASDM 中 BGP Set Value 选项卡或从 **set** 命令设置的值修改其某些属性。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，直至发现子句的 **match** 命令根据 ASDM 中的 BGP Match Clause 选项卡的设置与路由匹配，或者直至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。不支持透明防火墙模式。

其他准则

路由映射不支持其中包含用户、用户组和完全限定域名对象的 ACL。

定义路由映射

当指定允许将来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

本节介绍如何自定义路由映射。

- 定义路由以匹配特定目标地址，第 22-4 页
- 为路由操作配置指标值，第 22-5 页

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　匹配包含目标网络并与标准 ACL 或前缀列表相匹配的所有路由：

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　匹配具有指定指标的任何路由：

match metric *metric_value*

示例：

```
ciscoasa(config-route-map)# match metric 200
```

metric_value 范围可在 0 到 4294967295 之间。

步骤 4　匹配包含下一跳路由器地址并与标准 ACL 相匹配的任何路由：

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　匹配已由与标准 ACL 相匹配的路由器通告的任何路由：

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**]}

为路由操作配置指标值

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要对路由执行的操作。要为路由操作配置指标值，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　为路由映射设置指标值：

set metric *metric_value*

示例：

```
ciscoasa(config-route-map)# set metric 200
```

metric_value 参数范围可在 0 到 294967295 之间。

步骤 3　为路由映射设置指标类型：

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 将这些路由作为指标为 5 且指标类型为 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指标值将 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 22-1　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)	引入了此功能。 引入了以下命令：**route-map**。
增强了对静态和动态路由映射的支持	8.0(2)	添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）的状态故障切换以及常规路由相关操作的调试	8.4(1)	引入了以下命令：**debug route** 和 **show debug route**。 修改了以下命令：**show route**。

表 22-1　　路由映射的功能历史记录 （续）

功能名称	平台版本	功能信息
多情景模式下的动态路由	9.0(1)	在多情景模式下支持路由映射。
支持 BGP	9.2(1)	引入了此功能。 引入以下命令：**router bgp**
IPv6 支持前缀规则	9.3.2	引入了此功能。



BGP

本章介绍如何配置思科 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。

- 关于 BGP，第 23-1 页
- BGP 准则，第 23-3 页
- 配置 BGP，第 23-3 页
- 监控 BGP，第 23-27 页
- BGP 配置示例，第 23-29 页
- BGP 历史记录，第 23-31 页

关于 BGP

BGP 是一种自治系统间路由协议。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，并且是互联网运营商 (ISP) 之间所使用的协议。

- 何时使用 BGP，第 23-1 页
- 路由表更改，第 23-2 页

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) 在其网络内交换路由信息。客户连接到 ISP，然后 ISP 使用 BGP 交换客户路由和 ISP 路由。在自治系统 (AS) 之间使用 BGP 时，该协议称为外部 BGP (EBGP)。如果运营商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

现在，可以使用 BGP 在 IPv6 网络中携带 IPv6 前缀的路由信息。

备注 当 BGPv6 ASA 加入集群时，它会在启用日志记录级别 7 时生成软回溯。

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 路由器仅会向其邻居发送已更改的路由。BGP 路由器不会发送定期路由更新，并且 BGP 路由更新仅对到达目标网络的最佳路径进行通告。

当存在多个到达某个特定目标的路由时，通过 BGP 获悉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，可在路由选择过程中使用：

- Weight - 这是思科定义的路由器本地属性。权重属性不会向相邻路由器进行通告。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。
- Local preference - 本地优先属性用于从本地 AS 中选择出口点。与权重属性不同，本地优先属性在整个本地 AS 中传播。如果有多个来自 AS 的出口点，则使用具有最高本地优先属性的出口点作为特定路由的出口点。
- Multi-exit discriminator - 多出口鉴别器 (MED) 或指标属性用作对外部 AS 进入正在对该指标进行通告的 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 属性选择路由，所以它仅作为建议。首选 MED 指标较低的路由。
- Origin - 源属性表示 BGP 获悉特定路由的方式。源属性可能具有下面三个可能值中的一个，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，会设置该值。
  - EGP - 此路由通过外部边界网关协议 (EBGP) 获悉。
  - Incomplete - 路由源未知或通过其他方式获悉。当路由重新分发到 BGP 时，可能会出现源不完整的情况。
- AS_path - 当路由通告通过一个自治系统时，会在按顺序排列的 AS 编号列表中添加 AS 编号，标识路由通告已经穿越的 AS。仅将拥有最短 AS_path 列表的路由添加至 IP 路由表中。
- Next hop - 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 下一跳地址会携带至本地 AS 中。
- Community - 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）。路由映射用于设置社区属性。预定义的社区属性如下：
  - no-export - 不向 EBGP 对等体通告相应路由。
  - no-advertise - 不向任何对等体进行通告。
  - internet - 此路由向互联网社区进行通告；网络中的所有路由器均属于此类型。

BGP 路径选择

BGP 可能会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。选择此路径后， 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 按显示的顺序使用以下条件为目标选择路径：

- 如果路径指定的下一跳不可访问，则放弃更新。
- 首选权重最高的路径。
- 如果权重相同，则首选具有最高本地优先值的路径。
- 如果本地优先值相同，则首选 BGP 在此路由器上运行所发起的路径。
- 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）。
- 首选具有由 BGP 路由器 ID 指定的最低 IP 地址的路径。
- 如果多个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下受到支持。

防火墙模式准则

不支持透明防火墙模式。仅在路由器模式下支持 BGP。

故障切换准则

在单情景模式和多情景模式下支持状态故障切换。

备注　启用集群时，不支持故障切换。

集群准则

仅在 L2 （以太网信道类型）和 L3 （单个接口类型）集群模式下支持 BGP。

注意　在用户情景中删除并重新应用 BGP 配置时，允许有 60 秒的延迟，从而使从属/备用 ASA 装置同步。

IPv6 规定

支持 IPv6。IPv6 地址系列不支持平稳重启。

配置 BGP

本节介绍如何在系统中启用和配置 BGP 进程。

操作步骤

步骤 1　在 CLI 中，启用 BGP 并配置常规 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　添加并配置策略列表。

步骤 4　添加并配置 AS 路径过滤器。

步骤 5　添加并配置社区规则。

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 路由进程和配置常规 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 的有有效值为从 1 到 4294967295 和 1.0 到 XX.YY。

步骤 2　丢弃 as-path 分段超过指定值的路由。

bgp maxas-limit *number*

示例：

```
ciscoasa(config-router)# bgp maxas-limit 15
```

参数 *number* 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 能够自动发现每个 BGP 会话的最佳 TCP 路径 MTU：

bgp transport path-mtu-discovery

步骤 5　使 BGP 能够在用于到达对等体的链接中断时，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到期：

bgp fast-external-fallover

步骤 6　如果外部 BGP (eBGP) 对等体未在传入路由的 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 对等体接收的更新。

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）更改为点分表示法。

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 （以秒为单位）。默认值为 60 秒。
- *holdtime* - ASA 在未接收到 keepalive 消息后声明对等体处于失效状态的间隔 （以秒为单位）。默认值为 180 秒。
- （可选） *min-holdtime* - ASA 未从邻居接收到 keepalive 消息后声明邻居处于失效状态的间隔（以秒为单位）。

步骤 9　启用 BGP 平稳重启功能：

bgp graceful-restart [**restart-time** *seconds*|**stalepath-time** *seconds*][**all**]

示例：

```
ciscoasa(config-router)# bgp graceful-restart restart-time 200
```

- **restart-time** - ASA 等待能够平稳重启的邻居在重新启动事件发生后恢复正常操作的最大时间段 （以秒为单位）。默认值为 120 秒。有效值范围为 1 至 3600 秒。
- **stalepath-time** - ASA 为重新启动对等体保留过时路径的最大时间段 （以秒为单位）。此计时器到期后，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。有关最佳路径的详细信息，请参阅 BGP 路径选择，第 23-2 页。

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　更改默认本地优先值：

bgp default local-preference *number*

示例：

```
ciscoasa(config-router)# bgp default local-preference 500
```

参数 *number* 是介于 0 与 4294967295 之间的任意值。值越大，表示优先级越高。

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，并将最佳路径切换到路由器 ID 最低的路由：

bgp bestpath compare-routerid

步骤 5 选择相邻 AS 通告的最佳 MED 路径：

bgp deterministic-med

步骤 6 将缺少 MED 属性的路径设置为最不优先考虑的路径：

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，将评估并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预先存在的匹配共存，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，从而可创建 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 分发使其下一跳脱离其中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 通过匹配以下任一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** - 表示要求精确匹配。所有社区以及仅指定社区必须存在。

步骤 6 重新分发带指定指标的路由：

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 路径过滤器允许您使用访问列表来过滤路由更新消息，并且查看更新消息中的单个前缀。如果更新消息中的前缀与过滤条件相匹配，则会过滤掉或接受该单个前缀，具体视过滤器条目已配置为执行的操作内容而定。本节介绍配置 AS 路径过滤器所需的步骤。

备注　**as-path 访问列表**不同于常规防火墙 ACL。

操作步骤

步骤 1　在全局配置模式下，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 路径访问列表编号。有效值范围为 1 至 500。
- *regexp* - 用于定义 AS 路径过滤器的正则表达式。自治系统编号的表示范围为 1 至 65535。

配置社区规则

社区是指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的匹配子句中使用的社区组。如同访问列表一样，可以创建一系列社区列表。系统会检查语句，直至找到匹配项为止。只要满足一个语句，便会结束测试。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，以确定社区的一个或多个允许或拒绝组。
- （可选） *community-number* - 以 1 至 4294967200 的 32 位数字表示的社区。可以输入单个社区，也可以输入以空格分隔的多个社区。

- *AA:NN* - 以 4 字节新社区格式输入的自治系统号和网络号。该值使用两个以冒号分隔的 2 字节编号进行配置。可以为每个 2 字节编号输入 1 至 65535 的数字。可以输入单个社区，也可以输入以空格分隔的多个社区。
- （可选） **internet** - 指定互联网社区。系统向所有对等体 （内部和外部）通告具有此社区的路由。
- （可选） **no-advertise** - 指定无通告社区。系统不向任何对等体 （内部或外部）通告具有此社区的路由。
- （可选） **no-export** - 指定无导出社区。系统仅向同一自治系统中的对等体或仅向联盟内的其他子自治系统通告具有此社区的路由。不会向外部对等体通告这些路由。
- （可选）**expanded**- 配置一个从 100 至 500 的扩展社区列表号，以确定社区的一个或多个允许或拒绝组。
- *regexp* - 用于定义 AS 路径过滤器的正则表达式。自治系统编号的表示范围为 1 至 65535。

注意 正则表达式只能用于扩展社区列表。

配置 IPv4 地址系列设置

可以从 BGP 配置设置中的 IPv4 系列选项来设置 BGP 的 IPv4 设置。IPv4 系列部分包括以下子部分：常规设置、聚合地址设置、过滤设置和邻居设置。其中每个子部分都支持您自定义特定于 IPv4 系列的参数。

本节介绍如何自定义 BGP IPv4 系列设置。

- 配置 IPv4 系列常规设置，第 23-8 页
- 配置 IPv4 系列聚合地址设置，第 23-10 页
- 配置 IPv4 系列过滤设置，第 23-11 页
- 配置 IPv4 系列 BGP 邻居设置，第 23-12 页
- 配置 IPv4 网络设置，第 23-16 页
- 配置重新分发设置，第 23-17 页
- 配置路由注入设置，第 23-18 页

配置 IPv4 系列常规设置

本节介绍配置常规 IPv4 设置所需的步骤。

操作步骤

步骤 1 启用 BGP 路由进程，从而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 IP 版本 4 (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，即使未指定也如此。

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，则会自动分配路由器 ID。

步骤 4　（可选）在单个接口 (L3) 模式下配置 IP 地址集群池：

bgp router-id *cluster-pool*

示例：

```
ciscoasa(config-router-af)# bgp router-id cp
```

注意　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是外部路由。此参数值的范围为 1 至 255。
- *internal-distance* - 内部 BGP 路由的管理距离。从本地自治系统中的对等设备获悉的路由是内部路由。此参数值的范围为 1 至 255。
- *local-distance* - 本地 BGP 路由的管理距离。本地路由是指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。此参数值的范围为 1 至 255。

步骤 6　使用 BGP 获悉的路由更新 IP 路由表时，修改指标和标签值。

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　将子网路由配置为自动汇总到网络级路由中

auto-summary

步骤 9　抑制未装载至路由信息库 (RIB) 中的路由的通告：

bgp suppress-inactive

步骤 10 在 BGP 与内部网关协议 (IGP) 系统之间同步：

synchronization

步骤 11 将 iBGP 配置为重新分发到 IGP 中，例如 OSPF：

bgp redistribute-internal

步骤 12 为下一跳验证配置 BGP 路由器扫描间隔：

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。此关键字与关键字 **delay** 结合用于更改下一跳跟踪延迟。此关键字与关键字 **enable** 结合用于启用下一跳地址跟踪。
- **delay** - 更改前后两次对路由表中安置的已更新下一跳路由进行检查的延迟间隔。
- *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
```

参数 *number_of_paths* 指定安置到路由表中的路由的数量。有效值介于 1 和 8 之间。

备注 如果未使用关键字 **ibgp**，则参数 *number_of_paths* 会控制并行 EBGP 路由的最大数量。

配置 IPv4 系列聚合地址设置

本节介绍将特定路由定义为聚合成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 IP 版本 4 (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，即使未指定也如此。

步骤 3 在 BGP 数据库中创建聚合条目：

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* - 聚合地址。
- *mask* - 聚合掩码。
- *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 源社区所用路由的路由映射的名称。
- （可选） **Attribute-map** *map-name* - 指定用于设置聚合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 IP 版本 4 (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，即使未指定也如此。

步骤 3 过滤在传入 BGP 更新中接收或在传出 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，从而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 IP 版本 4 (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，即使未指定也如此。

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) 平稳重启功能：

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 平稳重启功能。

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* - 扩展访问列表的编号。扩展访问列表号的范围为 1300 至 2699。
- *access-list-number* - 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* - 整数，用于指定路由器开始生成警告消息时所达到的最大值的百分比。范围为 1 至 100，默认值为 75 （百分比）。
- （可选） *restart interval* - 整数值 （以秒为单位），用于指定 BGP 邻居重新启动前的时间间隔。
- （可选） **warning-only** - 允许路由器在超过最大前缀数量时生成日志消息，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，以用作该邻居的默认路由：

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 设置前后两次发送 BGP 路由更新的最小间隔：

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 （以秒为单位）。有效值范围为 0 至 600。

步骤 14 通告 BGP 表中与已配置的路由映射相匹配的路由：

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是否对通告映射路由进行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是否对通告映射路由进行通告的非存在映射的名称。
- （可选） **check all paths** - 使具有 BGP 表中的前缀的存在映射可检查所有路径。

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（以秒为单位）。默认值为 60 秒。有效值范围为 0 至 65535。
- *holdtime* - ASA 在未接收到 keepalive 消息后声明对等体处于失效状态的间隔 （以秒为单位）。默认值为 180 秒。
- *min holdtime* - ASA 在未接收到 keepalive 消息后声明对等体处于失效状态的最小间隔 （以秒为单位）。

步骤 17 在两个 BGP 对等体之间的 TCP 连接上启用消息摘要 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，其长度最大为 25 个字符；未启用 **service password-encryption** 命令时，其长度最大为 81 个字符。此字符串包含任意字母数字字符，包括空格。

备注 第一个字符不能为数字。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到 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 将路由器配置为 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 接受并尝试建立与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 至 255 跳。

步骤 21 禁用连接验证可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，并且配置用于分隔两个外部 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* 是用于分隔 eBGP 对等体的跳数。TTL 值由路由器根据已配置的 hop-count 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* 是分配给邻居连接的权重。有效值范围为 0 至 65535。

步骤 24 将 ASA 配置为仅接受特定 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。版本可以设置为 2，以强制软件仅对指定邻居使用版本 2。默认使用版本 4，如有要求，可以动态地协商降至版本 2。

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 （**active** 或 **passive**）。
- **path-mtu-discovery** - 启用 TCP 传输路径最大传输单位 (MTU) 发现。默认情况下会启用 TCP 路径 MTU 发现。
- （可选） **disable -** 禁用 TCP 路径 MTU 发现。

步骤 26 为从外部边界网关协议 (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。此参数值的范围是从 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

本节介绍定义要由 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 IP 版本 4 (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，即使未指定也如此。

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其他路由域重新分发到 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 IP 版本 4 (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，即使未指定也如此。

步骤 3 将路由从其他路由域重新分发到 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。它可以是以下协议之一：Connected、 EIGRP、 OSPF、 RIP 或 Static。
- （可选） *process-id* - 特定路由进程的名称。
- （可选） *metric* - 已重新分发的路由的指标。
- （可选） *map-tag* - 已配置的路由映射的标识符。

备注 应检查路由映射，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 IP 版本 4 (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，即使未指定也如此。

步骤 3 配置有条件的路由注入，以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* - 用于指定要注入本地 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聚合路由的属性。

配置 IPv6 地址系列设置

可以从 BGP 配置设置中的 IPv6 系列选项来设置 BGP 的 IPv6 设置。IPv6 系列部分包括以下子部分：常规设置、聚合地址设置和邻居设置。其中每个子部分都支持您自定义特定于 IPv6 系列的参数。

本节介绍如何自定义 BGP IPv6 系列设置。

- 配置 IPv6 系列常规设置，第 23-19 页
- 配置 IPv6 系列聚合地址设置，第 23-20 页
- 配置 IPv6 系列 BGP 邻居设置，第 23-21 页
- 配置 IPv6 网络设置，第 23-25 页

- 配置重新分发设置，第 23-17 页
- 配置路由注入设置，第 23-18 页

配置 IPv6 系列常规设置

本节介绍配置常规 IPv6 设置所需的步骤。

操作步骤

步骤 1　启用 BGP 路由进程，从而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 IP 版本 6 (IPv6) 地址前缀配置路由会话：

address-family ipv6 [unicast]

步骤 3　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是外部路由。此参数值的范围为 1 至 255。
- *internal-distance* - 内部 BGP 路由的管理距离。从本地自治系统中的对等设备获悉的路由是内部路由。此参数值的范围为 1 至 255。
- *local-distance* - 本地 BGP 路由的管理距离。本地路由是指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。此参数值的范围为 1 至 255。

步骤 4　（可选）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 5　（可选）抑制未装载至路由信息库 (RIB) 中的路由的通告：

bgp suppress-inactive

步骤 6　在 BGP 与内部网关协议 (IGP) 系统之间同步：

synchronization

步骤 7　将 iBGP 配置为重新分发到 IGP 中，例如 OSPF：

bgp redistribute-internal

步骤 8　为下一跳验证配置 BGP 路由器扫描间隔：

bgp scan-time *scanner-interval*

示例：

```
ciscoasa(config-router-af)# bgp scan-time 15
```

参数 *scanner-interval* 的有效值范围为 5 至 60 秒。默认值为 60 秒。

步骤 9 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
```

参数 *number_of_paths* 的有效值介于 1 与 8 之间。

如果未使用关键字 **ibgp**，则参数 *number_of_paths* 会控制并行 EBGP 路由的最大数量。

配置 IPv6 系列聚合地址设置

本节介绍将特定路由定义为聚合成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 IP 版本 6 (IPv6) 地址前缀配置路由会话：

address-family ipv6 unicast

步骤 3 在 BGP 数据库中创建聚合条目：

aggregate-address *ipv6-address/cidr* [**as-set**][**summary-only**][**suppress-map** *map-name*][**advertise-map** *ipv6-map-name*][**attribute-map** *map-name*]

示例：

```
ciscoasa(config-router-af) aggregate-address 2000::1/8 summary-only
```

- *address* - 聚合 IPv6 地址。
- （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 源社区所用路由的路由映射的名称。
- （可选） **attribute-map** *map-name* - 指定用于设置聚合路由属性的路由映射的名称。

步骤 4 设置 BGP 路由的聚合时间间隔：

bgp aggregate-timer *seconds*

示例：

```
ciscoasa(config-router-af)bgp aggregate-timer 20
```

配置 IPv6 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，从而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 IP 版本 6 (IPv6) 地址前缀配置路由会话：

address-family ipv6 [**unicast**]

步骤 3　向 BGP 邻居表添加条目：

neighbor *ipv6-address* **remote-as** *autonomous-number*

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 remote-as 3
```

参数 *ipv6-address* 指定可用于到达指定网络的下一跳的 IPv6 地址。此下一跳的 IPv6 地址不需要直接连接；为查找直接连接的下一跳的 IPv6 地址，需要执行递归。当指定接口类型和接口号时，您可以根据需要指定数据包输出到的下一跳的 IPv6 地址。使用链路本地地址作为下一跳 （链路本地下一跳也必须是相邻设备）时，必须指定接口类型和接口号。

注意　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。

步骤 4　（可选）禁用邻居或对等组：

neighbor *ipv6-address* **shutdown**

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 shutdown 3
```

步骤 5　与 BGP 邻居交换信息：

neighbor *ipv6-address* **activate**

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 activate
```

步骤 6　将路由映射应用于传入或传出路由：

neighbor {*ipv6-address*} **route-map** *map-name* {**in**|**out**}

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 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 7 按前缀列表中的指定分发 BGP 邻居信息：

neighbor {*ipv6-address*} **prefix-list** *prefix-list-name* {**in**|**out**}

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 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 8 设置过滤器列表：

neighbor {*ipv6-address*} **filter-list** *access-list-name* {**in**|**out**}

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 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 9 控制可以从邻居接收的前缀的数量：

neighbor {*ipv6-address*} **maximum-prefix** *maximum* [*threshold*][**restart** *restart interval*][**warning-only**]

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 maximum-prefix 7 75 restart 12
```

- *maximum* - 从此邻居允许的前缀的最大数量。
- （可选） *threshold* - 整数，用于指定路由器开始生成警告消息时所达到的最大值的百分比。范围为 1 至 100，默认值为 75 （百分比）。
- （可选） *restart interval* - 整数值 （以秒为单位），用于指定 BGP 邻居重新启动前的时间间隔。
- （可选） **warning-only** - 允许路由器在超过最大前缀数量时生成日志消息，而不是终止对等。

步骤 10 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，以用作该邻居的默认路由：

neighbor {*ipv6-address*} **default-originate** [**route-map** *map-name*]

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 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 11 设置前后两次发送 BGP 路由更新的最小间隔：

neighbor {*ipv6-address*} **advertisement-interval** *seconds*

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 advertisement-interval 15
```

参数 *seconds* 是时间 （以秒为单位）。有效值范围为 0 至 600。

步骤 12 从出站路由更新中删除专用自治系统号：

neighbor {*ipv6-address*} **remove-private-as**

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 remove-private-as
```

步骤 13 通告 BGP 表中与已配置的路由映射相匹配的路由：

neighbor {*ipv6-address*} **advertise-map** *map-name* {**exist-map** *map-name* |**non-exist-map** *map-name*}[**check-all-paths**]

示例：

```
ciscoasa(config-router-af)# neighbor 2000::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是否对通告映射路由进行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是否对通告映射路由进行通告的非存在映射的名称。
- （可选） **check all paths** - 使具有 BGP 表中的前缀的存在映射可检查所有路径。

步骤 14 为特定 BGP 对等体或对等组设置计时器。

neighbor {*ipv6-address*} **timers** *keepalive holdtime min holdtime*

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 timers 15 20 12
```

- *keepalive* - ASA 向其对等体发送 keepalive 消息的频率（以秒为单位）。默认值为 60 秒。有效值范围为 0 至 65535。
- *holdtime* - ASA 在未接收到 keepalive 消息后声明对等体处于失效状态的间隔 （以秒为单位）。默认值为 180 秒。
- *min holdtime* - ASA 在未接收到 keepalive 消息后声明对等体处于失效状态的最小间隔 （以秒为单位）。

步骤 15 在两个 BGP 对等体之间的 TCP 连接上启用消息摘要 5 (MD5) 身份验证：

neighbor {*ipv6-address*} **password** *string*

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 password test
```

参数 *string* 是区分大小写的密码，启用 **service password-encryption** 命令时，其长度最大为 25 个字符；未启用 **service password-encryption** 命令时，其长度最大为 81 个字符。此字符串包含任意字母数字字符，包括空格。

备注 第一个字符不能为数字。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 16 指定应将社区属性发送到 BGP 邻居：

neighbor {*ipv6-address*} **send-community** [**standard**]

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 send-community
```

- （可选）关键字 **standard** - 仅发送标准社区。

步骤 17 将路由器配置为 BGP 发言邻居或对等组的下一跳：

neighbor {*ipv6-address*}**next-hop-self**

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 next-hop-self
```

步骤 18 接受并尝试建立与未直接连接的网络上的外部对等体的 BGP 连接：

neighbor {*ipv6-address*} **ebgp-multihop** [*ttl*]

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 ebgp-multihop 5
```

参数 *ttl* 指定生存时间，范围为 1 至 255 跳。

步骤 19 禁用连接验证可与使用环回接口的单跳对等体建立 eBGP 对等会话：

neighbor {*ipv6-address*} **disable-connected-check**

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 disable-connected-check
```

步骤 20 保护 BGP 对等会话，并且配置用于分隔两个外部 BGP (eBGP) 对等体的最大跳数。

neighbor {*ipv6-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* 是用于分隔 eBGP 对等体的跳数。TTL 值由路由器根据已配置的 hop-count 参数计算得出。有效值范围为 1 至 254。

步骤 21 向邻居连接分配权重：

neighbor {*ipv6-address*} **weight** *number*

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 weight 30
```

参数 *number* 是分配给邻居连接的权重。有效值范围为 0 至 65535。

步骤 22 将 ASA 配置为仅接受特定 BGP 版本：

neighbor {*ipv6-address*} **version** *number*

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 version 4
```

参数 *number* 指定 BGP 版本号。默认为版本 4。目前仅支持 BGP 版本 4。

步骤 23 为 BGP 会话启用 TCP 传输会话选项：

neighbor {*ipv6-address*} **transport** {**connection-mode**{**active**|**passive**}|
path-mtu-discovery[**disable**]}

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 transport connection-mode active
```

- **connection-mode** - - 连接类型 （**active** 或 **passive**）。
- **path-mtu-discovery** - 启用 TCP 传输路径最大传输单位 (MTU) 发现。默认情况下会启用 TCP 路径 MTU 发现。

- （可选） **disable -** 禁用 TCP 路径 MTU 发现。

步骤 24 为从外部边界网关协议 (eBGP) 邻居接收的路由自定义 AS_PATH 属性：

neighbor {*ipv6-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。此参数值的范围是从 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。

注意 BGP 预置路由穿越的每个 BGP 网络的自治系统号，以维护网络可达性信息和防止路由环路。此命令应配置为仅用于自治系统迁移，并且在完成迁移后应将其删除。此程序应仅由经验丰富的网络操作员尝试执行。配置不当可能会造成路由环路

配置 IPv6 网络设置

本节介绍定义要由 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 IP 版本 6 (IPv6) 地址前缀配置路由会话：

address-family ipv6 [**unicast**]

步骤 3 指定将由 BGP 路由进程通告的网络：

network {*ipv6 network/ prefix length*} [**route-map** *route-map name*]

示例：

```
ciscoasa(config-router-af)# network 2001:1/64 route-map test_route_map
```

- *ipv6 network/prefix length* - BGP 将通告的网络。
- （可选） *route-map name* - 已配置的路由映射的标识符。应检查路由映射，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其他路由域重新分发到 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 IP 版本 6 (IPv6) 地址前缀配置路由会话：

address-family ipv6 [**unicast**]

示例：

```
ciscoasa(config-router)# address-family ipv6[unicast]
```

步骤 3　将路由从其他路由域重新分发到 BGP 自治系统：

redistribute *protocol* [*process-id*][*autonomous-num*][**metric** *metric value*][**match**{**internal**|**external1**|**external2**|**NSSA external 1**|**NSSA external 2**}][**route-map** [map-tag]][subnets]

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。它可以是以下协议之一：Connected、 EIGRP、 OSPF、 RIP 或 Static。
- （可选） *process-id* - 对于 OSPF 协议，这是将会从其重新分发路由的相应 OSPF 进程 ID。这可以标识路由进程。该值采用非零十进制数字的形式。

注意　系统会为其他协议自动填充该值。

- （可选） *metric metric value* - 当在同一路由器上从一个 OSPF 进程重新分发到另一个 OSPF 进程时，如果未指定指标值，则指标将从一个进程携带至另一个进程。将其他进程重新分发到 OSPF 进程时，如果未指定指标值，则默认指标为 20。默认值为 0。
- （可选）match *internal* | *external1* | *external2* | *NSSA external 1* | *NSSA external 2* - 适用于将 OSPF 路由重新分发到其他路由域所依据的条件。它可以是下列类型之一：
  - *internal* - 特定自治系统的内部路由。
  - *external 1* - 自治系统的外部路由，但可以作为 OSPF Type 1 外部路由导入 BGP。
  - *external 2* - 自治系统的外部路由，但可以作为 OSPF Type 2 外部路由导入 BGP。
  - *NSSA external 1* - 自治系统的外部路由，但可以作为 OSPF NSSA Type 1 外部路由器导入 BGP。
  - *NSSA external 2* - 自治系统的外部路由，但可以作为 OSPF NSSA Type 2 外部路由器导入 BGP。
- （可选） *map-tag* - 已配置的路由映射的标识符。

备注　应检查路由映射，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 IP 版本 6 (IPv6) 地址前缀配置路由会话：

```
address-family ipv6 [unicast]
```

示例：

```
ciscoasa(config-router)# address-family ipv6 [unicast]
```

步骤 3 配置有条件的路由注入，以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* - 用于指定要注入本地 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聚合路由的属性。

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。

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**

  显示带有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 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*

  显示与指定的过滤器列表相符的路由。
- **show bgp injected-paths**

  显示 BGP 路由表中所有注入的路径。
- **show bgp ipv4 unicast**

  显示 IP 版本 4 (IPv4) BGP 路由表中的单播会话条目。
- **show bgp ipv6 unicast**

  显示 IPv6 边界网关协议 (BGP) 路由表中的条目。
- **show bgp ipv6 community**

  显示属于指定 IPv6 边界网关协议 (BGP) 社区的路由。
- **show bgp ipv6 community-list**

  显示 IPv6 边界网关协议 (BGP) 社区列表允许的路由。
- **show bgp ipv6 filter-list**

  显示与指定的 IPv6 过滤器列表相符的路由。
- **show bgp ipv6 inconsistent-as**

  显示源自治系统不一致的 IPv6 边界网关协议 (BGP) 路由。
- **show bgp ipv6 neighbors**

  显示到邻居的 IPv6 边界网关协议 (BGP) 连接的相关信息。
- **show bgp ipv6 paths**

  显示数据库中的所有 IPv6 边界网关协议 (BGP) 路径。
- **show bgp ipv6 prefix-list**

  显示与前缀列表相匹配的路由。
- **show bgp ipv6 quote-regexp**

  显示与作为引用字符串的自治系统路径正则表达式相匹配的 IPv6 边界网关协议 (BGP) 路由。
- **show bgp ipv6 regexp**

  显示与自治系统路径正则表达式相匹配的 IPv6 边界网关协议 (BGP) 路由。
- **show bgp ipv6 route-map**

  显示无法安置在路由表中的 IPv6 边界网关协议 (BGP) 路由。
- **show bgp ipv6 summary**

  显示所有 IPv6 边界网关协议 (BGP) 连接的状态。
- **show bgp neighbors** *ip_address*

  显示到邻居的 BGP 和 TCP 连接的相关信息
- **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]

  显示与指定的前缀列表相匹配的路由。

- **show bgp regexp** *regexp*

  显示与自治系统路径正则表达式相匹配的路由。
- **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**

  显示多情景模式下的系统情景特定 BGP 配置。

  此命令可用于多情景模式下的所有用户情景。
- **show bgp update-group**

  显示有关 BGP 更新组的信息。

备注　要禁用 BGP Log 消息，请在路由器配置模式下输入 **no bgp log-neighbor-changes**。这会禁用邻居变更消息的日志记录。请在 BGP 路由进程的路由器配置模式下输入此命令。
默认情况下，已记录邻居变更。

BGP 配置示例

此示例显示如何通过各种可选进程启用和配置 BGPv4。

步骤 1　定义要路由从一个路由协议重新分发到另一个路由协议的条件，或者启用策略路由

```
ciscoasa(config)# route-map mymap2 permit 10
```

步骤 2　重新分发具有路由地址或与已指定的某个访问列表传递的数据包相匹配的任何路由：

```
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

步骤 3　指示用于输出为策略路由传递路由映射匹配子句的数据包的目标位置：

```
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下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
```

此示例显示如何通过各种可选进程启用和配置 BGPv6。

步骤 1 定义要路由从一个路由协议重新分发到另一个路由协议的条件，或者启用策略路由

```
ciscoasa(config)# route-map mymap1 permit 10
```

步骤 2 重新分发具有路由地址或与已指定的某个访问列表传递的数据包相匹配的任何路由：

```
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

步骤 3 指示用于输出为策略路由传递路由映射匹配子句的数据包的目标位置：

```
ciscoasa(config-route-map)# set ipv6 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下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 进入地址系列配置模式，以使用标准 IP 版本 6 (IPv6) 地址前缀配置路由会话：

```
address-family ipv6 [unicast]
```

步骤 7 向 BGP 邻居表添加条目：

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 remote-as 64600
```

步骤 8 将路由映射应用于传入或传出路由：

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 route-map mymap1 in
```

BGP 历史记录

表 23-1 列出各种功能变更以及实施相应功能变更的平台版本。

表 23-1 BGP 的功能历史记录

功能名称	平台版本	功能信息
BGP 支持	9.2(1)	系统添加了以下支持：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。 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**。 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**。
BGP 对 ASA 集群的支持	9.3(1)	我们添加了对 L2 和 L3 集群的支持。 引入了以下命令：**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。 引入了以下命令：**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。 引入了以下命令：**neighbor advertise-map**

表 23-1 BGP 的功能历史记录

功能名称	平台版本	功能信息
IPv6 的 BGP 支持	9.3(2)	我们添加了对 IPv6 的支持。 引入了以下命令：**address-family ipv6**、 **ipv6 prefix-list**、 **ipv6 prefix-list description**、 **ipv6 prefix-list sequence-number**、 **match ipv6 next-hop**、 **match ipv6 route-source**、 **match ipv6- address prefix-list**、 **set ipv6-address prefix -list**、 **set ipv6 next-hop**、 **set ipv6 next-hop peer-address** 修改了以下命令：**bgp router-id**



OSPF

本章介绍如何将思科 ASA 配置为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：

- 关于 OSPF，第 24-1 页
- OSPF 准则，第 24-4 页
- 配置 OSPFv2，第 24-5 页
- 配置 OSPF 快速呼叫数据包，第 24-6 页
- 自定义 OSPFv2，第 24-7 页
- 配置 OSPFv3，第 24-17 页
- 配置平稳重启，第 24-35 页
- OSPFv2 示例，第 24-39 页
- OSPFv3 示例，第 24-40 页
- 监控 OSPF，第 24-41 页
- 其他参考资料，第 24-44 页
- OSPF 历史记录，第 24-44 页

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所有到达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。

相比 RIP， OSPF 具有以下优点：

- 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。
- 路由决策基于开销，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开销。可以配置开销来指定首选路径。

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 不允许重叠地址），则可能要运行两个进程。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。

您可以将路由从一个 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 筛选。

OSPF 支持 MD5 和明文邻居身份验证。如有可能，应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。

在使用 NAT 的情况下，如果 OSPF 在公共区域和专用区域中运行，并且如果要求地址筛选，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 筛选，您可以具有单独的以 ASA 为 ABR 的专用和公共区域。可以将 3 类 LSA（区域间路由）从一个区域筛选到另一个区域，借此能够将 NAT 和 OSPF 配合使用而不通告专用网络。

备注 只能筛选 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到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。

您可以同时在 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。

OSPF 支持快速呼叫数据包

OSPF 支持快速呼叫数据包的功能提供了一种在小于 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。

OSPF 支持快速呼叫数据包的必备条件

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 OSPF 支持快速呼叫数据包的信息

以下各节介绍与 OSPF 支持快速呼叫数据包相关的概念：

- OSPF 呼叫间隔和停顿间隔
- OSPF 快速呼叫数据包
- OSPF 快速呼叫数据包的优势

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结合用于保持连接。如果路由器在停顿间隔内没有从邻居接收到呼叫数据包，则将声明该邻居关闭。

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。要了解快速呼叫数据包，您应已了解 OSPF 呼叫数据包与停顿间隔之间的关系。请参阅 OSPF 呼叫间隔和停顿间隔，第 24-3 页。

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，它在分片上都必须一致。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片便无需相同。

OSPF 快速呼叫数据包的优势

OSPF 快速呼叫数据包功能的优势是 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，您可以在 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 分片中尤其有用。

OSPFv2 与 OSPFv3 之间的实施差异

OSPFv3 不向后兼容 OSPFv2。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：

- 按链路进行协议处理。
- 删除寻址语义。
- 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 支持单情景模式和多情景模式。

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。

故障切换准则

OSPFv2 和 OSPFv3 支持状态故障切换。

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。
- 在跨接口模式下，管理专属接口上不支持动态路由。
- 在单个接口模式下，请确保将主设备和从属设备建立为 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。
- 在单个接口模式下，只能在主设备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 路由器配置模式下是可选的。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设备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，将删除整个配置，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。
- 当某个设备作为从属设备进入集群时，我们建议为 **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。从属设备仍然从主设备继承路由器配置。
- 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，路由器进程仅在主设备上处于活动状态，在从属设备上处于暂停状态。各集群设备具有同一路由器 ID，因为已从主设备对配置进行同步。因此，在角色更改过程中，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设备上都处于活动状态。各集群设备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。

其他准则

- OSPFv2 和 OSPFv3 在接口上支持多个实例。
- OSPFv3 在非集群环境中通过 ESP 报头支持加密。
- 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 平稳重启和 IETF NSF 平稳重启机制。
- OSPFv3 根据 RFC 5187 定义支持平稳重启机制。

配置 OSPFv2

本节介绍如何在 ASA 上启用 OSPFv2 进程。

启用 OSPFv2 后，您需要定义路由映射。有关详细信息，请参阅定义路由映射，第 22-4 页。然后，生成默认路由。有关详细信息，请参阅配置静态路由，第 20-4 页。

为 OSPFv2 进程定义路由映射后，您可以根据特定需要对其进行自定义。要了解任何在 ASA 上自定义 OSPFv2 进程，请参阅自定义 OSPFv2，第 24-7 页。

要启用 OSPFv2，您需要创建 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。

您最多可以启用两个 OSPFv2 进程实例。每个 OSPFv2 进程具有其自己的关联区域和网络。

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。您最多可以使用两个进程。

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。您可以将区域 ID 指定为十进制数字或 IP 地址。有效十进制值范围为 0 到 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

本节介绍如何配置 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 参数表示端口通道接口号。

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 参数表示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 OSPF 支持快速呼叫数据包功能。由于乘数设置为 5，因此每秒将发送五个呼叫数据包。

自定义 OSPFv2

本节介绍如何自定义 OSPFv2 进程。

- 将路由重新分发到 OSPFv2 中，第 24-7 页
- 将路由重新分发到 OSPFv2 中时配置路由汇总，第 24-9 页
- 配置 OSPFv2 区域之间的路由汇总，第 24-9 页
- 配置 OSPFv2 接口参数，第 24-10 页
- 配置 OSPFv2 区域参数，第 24-13 页
- 配置 OSPFv2 NSSA，第 24-13 页
- 为集群配置 IP 地址池 （OSPFv2 和 OSPFv3），第 24-15 页
- 定义静态 OSPFv2 邻居，第 24-15 页
- 配置路由计算计时器，第 24-16 页
- 记录邻居启动或关闭，第 24-16 页

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。

备注 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，必须先生成默认路由。请参阅配置静态路由，第 20-4 页，然后根据定义路由映射，第 22-4 页定义路由映射。

要将静态路由、已连接路由、 RIP 路由或 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。您最多可以使用两个进程。

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
```

您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 的指标相匹配来显示从 OSPF 进程 1 到 OSPF 进程 2 中的路由重新分发。ASA 将这些路由作为指标为 5 且指标类型为 1 类的外部 LSA 重新分发。

步骤 5　将路由从一个 RIP 路由进程重新分发到另一个 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　将路由从一个 EIGRP 路由进程重新分发到另一个 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 中时配置路由汇总

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，您可以将 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。标签值可用作用于通过路由映射控制重新分发的值。

要配置路由汇总，可以执行以下操作：

- 添加路由汇总地址，第 24-9 页

添加路由汇总地址

要在一个汇总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。您最多可以使用两个进程。

步骤 2　设置汇总地址：

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，汇总地址 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 区域之间的路由汇总

路由汇总是通告地址的整合。此功能导致通过区域边界路由器向其他区域通告单个汇总路由。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，则可以将区域边界配置为通告汇总路由，包括该区域内属于指定范围的所有单独网络。

要定义汇总路由的地址范围，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。您最多可以使用两个进程。

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，您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** 和 **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。您最多可以使用两个进程。

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。可以为每个接口的每个网络指定单独的密码。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开销：

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。

建议不要每个接口保留多个密钥。每次添加新密钥时，应删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。删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。范围是从 1 到 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，您必须手动定义 OSPF 邻居；无法实现动态邻居发现。有关详情，请参见定义静态 OSPFv2 邻居，第 24-15 页。此外，您只能在该接口上定义一个 OSPF 邻居。

配置 OSPFv2 区域参数

您可以配置多个 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汇总路由分配特定开销。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。要利用 OSPF 末节区域支持，必须在末节区域中使用默认路由。要进一步减少发送到末节区域中的 LSA 数量，您可以在 ABR 上使用 **area stub** 命令的 **no-summary** 关键字，以防止其将汇总链路通告 （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。您最多可以使用两个进程。

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。在转换过程中支持汇总和筛选。

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 （例如 RIP）并使用其处理重新分发。在使用 NSSA 的情况下，您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：

- 您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。您最多可以使用两个进程。

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　设置汇总地址并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，汇总地址 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。

注意　OSPF 不支持汇总地址 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

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。

备注　如果使用的是集群，则无需指定路由器 ID 的 IP 地址池。如果不配置 IP 地址池，则 ASA 使用自动生成的路由器 ID。

定义静态 OSPFv2 邻居

您需要定义静态 OSPFv2 邻居来通过点对点非广播网络通告 OSPFv2 路由。通过此功能，您可以跨现有 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 20 章“静态路由和默认路由”。

操作步骤

步骤 1　创建 OSPFv2 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。您最多可以使用两个进程。

步骤 2　定义 OSPFv2 邻近区域：

neighbor *addr* [**interface** *if_name*]

示例：

```
ciscoasa(config-rtr)# neighbor 255.255.0.0 [interface my_interface]
```

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。

配置路由计算计时器

您可以配置 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。

操作步骤

步骤 1 创建 OSPFv2 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。您最多可以使用两个进程。

步骤 2 配置路由计算时间：

timers throttle spf *spf-start spf-hold spf-maximum*

示例：

```
ciscoasa(config-router)# timers throttle spf 500 500 600
```

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 0 到 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。

如果要在不开启 **debug ospf adjacency** 命令的情况下了解 OSPFv2 邻居是启动还是关闭，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。

操作步骤

步骤 1　创建 OSPFv2 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。您最多可以使用两个进程。

步骤 2　为启动或关闭的邻居配置日志记录：

log-adj-changes [**detail**]

配置 OSPFv3

本节介绍如何配置 OSPFv3 路由进程。

- 启用 OSPFv3，第 24-18 页
- 配置 OSPFv3 接口参数，第 24-18 页
- 配置 OSPFv3 路由器参数，第 24-23 页
- 配置 OSPFv3 区域参数，第 24-25 页
- 配置 OSPFv3 被动接口，第 24-27 页
- 配置 OSPFv3 管理距离，第 24-27 页
- 配置 OSPFv3 计时器，第 24-28 页
- 定义静态 OSPFv3 邻居，第 24-30 页
- 重置 OSPFv3 默认参数，第 24-30 页
- 发送系统日志消息，第 24-31 页
- 抑制系统日志消息，第 24-32 页
- 计算汇总路由开销，第 24-32 页
- 生成到 OSPFv3 路由域中的默认外部路由，第 24-32 页
- 配置 IPv6 汇总前缀，第 24-33 页
- 重新分发 IPv6 路由，第 24-34 页

启用 OSPFv3

要启用 OSPFv3，您需要创建 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。

操作步骤

步骤 1 创建 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config)# ipv6 router ospf 10
```

process_id 参数是此路由进程的内部使用的标签，可以是任何正整数。此标签不必与任何其他设备上的标签匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 启用接口：

interface *interface_name*

示例：

```
ciscoasa(config)# interface Gigabitethernet0/0
```

步骤 3 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。

ipv6 ospf *process-id* **area** *area_id*

示例：

```
ciscoasa(config)# ipv6 ospf 200 area 100
```

配置 OSPFv3 接口参数

如有必要，您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。

操作步骤

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 10
```

process_id 参数是此路由进程的内部使用的标签，可以是任何正整数。此标签不必与任何其他设备上的标签匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 创建 OSPFv3 区域：

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
```

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。您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 指定在 OSPF 接口上发送数据包的开销：

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
```

interface-cost 参数指定表示为链路状态指标的无符号整数值，其值的范围可以为 1 至 65535。默认开销基于带宽。

步骤 4 筛选到 OSPFv3 接口的传出 LSA：

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
```

默认情况下，所有传出 LSA 都泛洪至该接口。

步骤 5 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）：

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
```

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。

步骤 6 指定接口的加密类型：

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
```

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 （例如 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。

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。

步骤 7 指定减少到接口的 LSA 泛洪：

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
```

步骤 8 指定接口上发送的呼叫数据包之间的间隔 （以秒为单位）：

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
```

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。

步骤 9 接收到 DBD 数据包后，禁用 OSPF MTU 不匹配检测：

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
```

默认情况下， OSPF MTU 不匹配检测已启用。

步骤 10 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：

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
```

point-to-point non-broadcast 关键字可将网络类型设置为点对点非广播。**broadcast** 关键字可将网络类型设置为广播。

步骤 11 设置路由器优先级，这有助于为网络确定指定的路由器：

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
```

有效值范围为 0 到 255。

步骤 12 配置与非广播网络的 OSPFv3 路由器互连：

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
```

步骤 13　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）：

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
```

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。有效值的范围为 1 到 65535 秒。默认值为 5 秒。

步骤 14　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）：

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
```

有效值的范围为 1 到 65535 秒。默认值为 1 秒。

配置 OSPFv3 路由器参数

操作步骤

步骤 1　启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config)# ipv6 router ospf 10
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，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。您最多可以使用两个进程。

步骤 2 配置 OSPFv3 区域参数：

中转区

示例：

```
ciscoasa(config-rtr)# area 10
```

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。

步骤 3 将命令设置为其默认值：

default

示例：

```
ciscoasa(config-rtr)# default originate
```

originate 参数分发默认路由。

步骤 4 控制默认信息的分发：

default-information

步骤 5 根据路由类型定义 OSPFv3 路由管理距离：

distance

示例：

```
ciscoasa(config-rtr)# distance 200
```

支持的参数包括值为 1 至 254 的管理距离和 OSPFv3 距离的 **ospf**。

步骤 6 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：

ignore

示例：

```
ciscoasa(config-rtr)# ignore lsa
```

步骤 7 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：

log-adjacency-changes

示例：

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

通过 **detail** 参数，将会记录所有状态更改。

步骤 8 抑制在接口上发送和接收路由更新：

passive-interface [*interface_name*]

示例：

```
ciscoasa(config-rtr)# passive-interface inside
```

interface_name 参数指定 OSPFv3 进程运行所在的接口的名称。

步骤 9 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** - 指定已连接路由。
- **ospf** - 指定 OSPFv3 路由。
- **static** - 指定静态路由。

redistribute

示例：

```
ciscoasa(config-rtr)# redistribute ospf
```

步骤 10　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，请参阅为集群配置 IP 地址池 （OSPFv2 和 OSPFv3），第 24-15 页。

router-id

示例：

```
ciscoasa(config-rtr)# router-id 10.1.1.1
```

步骤 11　配置有效值为 0 至 128 的 IPv6 地址汇总：

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
```

X:X:X:X::X/ 参数指定 IPv6 前缀。

步骤 12　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。

timers

示例：

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

配置 OSPFv3 区域参数

操作步骤

步骤 1　启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config)# ipv6 router ospf 1
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，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。您最多可以使用两个进程。

步骤 2 设置 NSSA 区域或末节区域的汇总默认开销：

area *area-id* **default-cost** *cost*

示例：

```
ciscoasa(config-rtr)# area 1 default-cost nssa
```

步骤 3 仅汇总与边界路由器的地址和掩码匹配的路由：

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
```

- *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 类汇总 LSA。
- **not-advertise** 关键字将地址范围状态设置为 DoNotAdvertise。
- 抑制 3 类汇总 LSA，并保持向其他网络隐藏组件网络。
- **cost** *cost* 关键字/参数对指定汇总路由的指标或开销，它在 OSPF SPF 计算过程中用于确定到达目标的最短路径。
- 有效值范围为 0 到 16777215。

步骤 4 指定 NSSA 区域：

area *area-id* **nssa**

示例：

```
ciscoasa(config-rtr)# area 1 nssa
```

步骤 5 指定末节区域：

area *area-id* **stub**

示例：

```
ciscoasa(config-rtr)# area 1 stub
```

步骤 6 定义虚拟链路及其参数：

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
```

- *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。对于连接到公用网络的所有路由器和接入服务器，值必须相同。有效值范围为 1 到 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）。对于连接到公用网络的所有路由器和接入服务器，值必须相同。有效值范围为 1 到 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

操作步骤

步骤 1　启用 OSPFv3 路由进程：

ipv6 router ospf *process_id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符，在本地进行分配，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。您最多可以使用两个进程。

步骤 2　抑制在接口上发送和接收路由更新：

passive-interface [*interface_name*]

示例：

```
ciscoasa(config-rtr)# passive-interface inside
```

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

操作步骤

步骤 1　启用 OSPFv3 路由进程：

ipv6 router ospf *process_id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符，在本地进行分配，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。您最多可以使用两个进程。

步骤 2 设置 OSPFv3 路由的管理距离：

distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*

示例：

```
ciscoasa(config-rtr)# distance ospf external 200
```

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

您可以为 OSPFv3 设置 LSA 到达计时器、 LSA 步调设置计时器和调速计时器。

操作步骤

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，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。您最多可以使用两个进程。

步骤 2 设置 ASA 接受来自 OSPF 邻居的同一 LSA 的最小间隔：

timers lsa arrival *milliseconds*

示例：

```
ciscoasa(config-rtr)# timers lsa arrival 2000
```

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）。范围是从 0 到 6,000,000 毫秒。默认值为 1000 毫秒。

步骤 3 配置 LSA 泛洪数据包步调设置：

timers pacing flood *milliseconds*

示例：

```
ciscoasa(config-rtr)# timers lsa flood 20
```

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）。可配置范围是从 5 到 100 毫秒。默认值为 33 毫秒。

步骤 4 更改将 OSPFv3 LSA 收集到组中并刷新、校验和或老化的间隔：

timers pacing lsa-group *seconds*

示例：

```
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

seconds 参数指定将 LSA 分组、刷新、校验和或老化的间隔秒数。范围是从 10 到 1800 秒。默认值为 240 秒。

步骤 5　配置 LSA 重新传输数据包步调：

timers pacing retransmission *milliseconds*

示例：

```
ciscoasa(config-rtr)# timers pacing retransmission 100
```

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）。可配置范围是从 5 到 200 毫秒。默认值为 66 毫秒。

步骤 6　配置 OSPFv3 LSA 调速：

timers throttle lsa *milliseconds1 milliseconds2 milliseconds3*

示例：

```
ciscoasa(config-rtr)# timers throttle lsa 500 6000 8000
```

- *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，如果最短或最长时间小于第一次出现的值，则 OSPFv3 会自动更正为第一次出现的值。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。
- 对于 *milliseconds1*，默认值为 0 毫秒。
- 对于 *milliseconds2* 和 *milliseconds3*，默认值为 5000 毫秒。

步骤 7　配置 OSPFv3 SPF 调速：

timers throttle spf *milliseconds1 milliseconds2 milliseconds3*

```
ciscoasa(config-rtr)# timers throttle spf 5000 12000 16000
```

- *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 限制，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 会自动更正为 *milliseconds2* 值。
- 对于 *milliseconds1*， SPF 调速的默认值为 5000 毫秒。
- 对于 *milliseconds2* 和 *milliseconds3*， SPF 调速的默认值为 10000 毫秒。

定义静态 OSPFv3 邻居

您需要定义静态 OSPFv3 邻居来通过点对点非广播网络通告 OSPF 路由。通过此功能，您可以跨现有 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 20 章“静态路由和默认路由”。

操作步骤

步骤 1 启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config)# ipv6 router ospf 1
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，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。您最多可以使用两个进程。

步骤 2 配置与非广播网络的 OSPFv3 路由器互连。

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
```

重置 OSPFv3 默认参数

要将 OSPFv3 参数还原为其默认值，请执行以下步骤：

操作步骤

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符，在本地进行分配，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。您最多可以使用两个进程。

步骤 2 将可选参数还原为其默认值：

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
```

- **area** 关键字指定 OSPFv3 区域参数。**auto-cost** 关键字根据带宽指定 OSPFv3 接口开销。
- **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指标。
- **discard-route** 关键字可启用或禁用丢弃安装路由。**distance** 关键字指定管理距离。
- **distribute-list** 关键字可筛选路由更新中的网络。
- **ignore** 关键字可忽略特定事件。**log-adjacency-changes** 关键字可记录邻接状态中的记录。
- **maximum-paths** 关键字可通过多个路径转发数据包。
- **passive-interface** 关键字可在接口上抑制路由更新。
- **redistribute** 关键字可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 汇总前缀。
- **timers** 关键字指定 OSPFv3 计时器。

发送系统日志消息

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。

操作步骤

步骤 1　启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，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。您最多可以使用两个进程。

步骤 2　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：

log-adjacency-changes [**detail**]

示例：

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

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

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：

操作步骤

步骤 1 启用 OSPFv2 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config-if)# router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符，在本地进行分配，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。您最多可以使用两个进程。

步骤 2 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：

ignore lsa mospf

示例：

```
ciscoasa(config-rtr)# ignore lsa mospf
```

计算汇总路由开销

操作步骤

步骤 1 恢复用于根据 RFC 1583 计算汇总路由开销的方法：

compatible rfc1583

示例：

```
ciscoasa (config-rtr)# compatible rfc1583
```

生成到 OSPFv3 路由域中的默认外部路由

操作步骤

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，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。您最多可以使用两个进程。

步骤 2　生成到 OSPFv3 路由域中的默认外部路由：

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
```

- **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指标。
- 如果不使用 **default - metric** 命令指定值，则默认值为 10。有效十进制值范围为 0 到 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。有效值可以是以下其中一项：
  - 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 汇总前缀

操作步骤

步骤 1　启用 OSPFv3 路由进程：

ipv6 router ospf
process-id

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符，在本地进行分配，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。您最多可以使用两个进程。

步骤 2　配置 IPv6 汇总前缀：

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
```

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签值。此关键字仅适用于 OSPFv3。

重新分发 IPv6 路由

操作步骤

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，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。您最多可以使用两个进程。

步骤 2 将 IPv6 路由从一个 OSPFv3 进程重新分发到另一个 OSPFv3 进程中：

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
```

- *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，如果未指定指标值，则会将指标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，如果未指定指标值，则默认指标为 20。
- **metric transparent** 关键字导致 RIP 使用重新分发的路由的路由表指标为 RIP 指标。
- **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。有效值可以是以下其中一项：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其中一项：内部 （适用于小于 63 的 IS-IS 指标）或外部 （适用于大于 64 且小于 128 的 IS-IS 指标）。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其中一个选项配合使用：**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 到 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筛选。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签，则不会导入任何路由。*map-tag* 参数标识已配置的路由映射。

配置平稳重启

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) 功能允许在恢复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，在故障切换 (HA) 模式中主用设备崩溃而备用设备接管，在集群模式中主设备崩溃而从属设备被选为新的主设备），或者已计划无中断软件升级。

在 OSPFv2 和 OSPFv3 上均支持平稳重启。通过使用 NSF Cisco（RFC 4811 和 RFC 4812）或 NSF IETF (RFC 3623)，您可以在 OSPFv2 上配置平稳重启。您可以使用 graceful-restart (RFC 5187) 在 OSPFv3 上配置平稳重启。

配置 NSF 平稳重启功能涉及两个步骤；配置功能和将设备配置为支持 NSF 功能或 NSF 感知。支持 NSF 功能的设备可以向邻居表明其自己的重启活动，而支持 NSF 感知的设备可以帮助重新启动邻居。

根据某些条件，可以将设备配置为支持 NSF 功能的设备或 NSF 感知的设备：

- 设备可以配置为 NSF 感知的设备，而与其所处的模式无关。
- 设备必须处于 Failover 或 Spanned Etherchannel (L2) 集群模式下才能配置为支持 NSF 功能的设备。
- 为使设备支持 NSF 功能或 NSF 感知，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。

备注　如果为 OSPFv2 配置了快速呼叫，则在主用设备重新加载且备用设备激活时不会发生平稳重启。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

思科 NSF 平稳重启机制取决于 LLS 功能，因为它会发送含有呼叫数据包中设置的 RS 位的 LLS 块来表示重启活动。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 来表示重启活动。要配置功能，请输入以下命令：

操作步骤

步骤 1　创建 OSPF 路由进程并针对要重新分发的 OSPF 进程进入路由器配置模式。

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。您最多可以使用两个进程。

步骤 2 支持使用 LLS 数据块或不透明 LSA 来启用 NSF：

```
capability {lls|opaque}
```

示例：

```
ciscoasa(config-router)# capability lls
```

lls 关键字用于启用思科 NSF 平稳重启机制的 LLS 功能。

opaque 关键字用于启用 IETF NSF 平稳重启机制的不透明 LSA 功能。

为 OSPFv2 配置平稳重启

对于 OSPFv2、思科 NSF 和 IETF NSF，存在两种平稳重启机制。一次只能为 ospf 实例配置其中一种平稳重启机制。支持 NSF 感知的设备既可以配置为思科 NSF 助手，也可以配置为 IETF NSF 助手，但是一次只能在思科 NSF 或 IETF NSF 模式中为 ospf 实例配置支持 NSF 功能的设备。

为 OSPFv2 配置思科 NSF 平稳重启

为 OSPFv2 配置思科 NFS 平稳重启 （适用于支持 NSF 功能的设备或 NSF 感知的设备）。

操作步骤

步骤 1 在支持 NSF 功能的设备上启用思科 NSF：

```
nsf cisco [enforce global]
```

示例：

```
ciscoasa(config-router)# nsf cisco
```

enforce global 关键字在检测到非 NSF 感知邻居的设备时会取消 NSF 重新启动。

步骤 2 （可选）在支持 NSF 感知的设备上启用思科 NSF 助手模式。

```
capability {lls|opaque}
```

示例：

```
ciscoasa(config-router)# capability lls
```

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 平稳重启

为 OSPFv2 配置思科 IETF NSF 平稳重启 （支持 NSF 功能的设备或 NSF 感知的设备）。

操作步骤

步骤 1　在支持 NSF 功能的设备上启用 IETF NSF：

nsf ietf [**restart interval** *seconds*]

示例：

```
ciscoasa(config-router)# nsf ietf restart interval 80
```

restart interval *seconds* 指定平稳重启间隔的长度 （以秒为单位）。有效值为 1 到 1800 秒。默认值为 120 秒。

使用小于邻接启动所需的时间的值来配置重启间隔时，可能会终止平稳重启。例如，不支持低于 30 秒的重启间隔。

步骤 2　在支持 NSF 感知设备上启用 IETF NSF 助手模式：

nsf ietf helper [**strict-lsa-checking**]

示例：

```
ciscoasa(config-router)# nsf ietf helper
```

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，或者如果在启动平稳重启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。

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 配置平稳重启

为 OSPFv3 配置 NSF 平稳重启功能涉及两个步骤：将一个设备配置为支持 NSF 功能，然后将另一个设备配置为支持 NSF 感知。

操作步骤

步骤 1　在未配置有显式 IPv6 地址的接口上启用 IPv6 处理：

interface *physical_interface*
ipv6 enable

示例：

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

physical_interface 参数标识参与 OSPFv3 NSF 的接口。

步骤 2 在支持 NSF 功能的设备上为 OSPFv3 启用 graceful-restart：

graceful-restart [**restart interval** *seconds*]

示例：

```
ciscoasa(config-router)# graceful-restart restart interval 80
```

restart interval *seconds* 指定平稳重启间隔的长度 （以秒为单位）。有效值为 1 到 1800 秒。默认值为 120 秒。

使用小于邻接启动所需的时间的值来配置重启间隔时，可能会终止平稳重启。例如，不支持低于 30 秒的重启间隔。

步骤 3 在支持 NSF 感知的设备上为 OSPFv3 启用 graceful-restart：

graceful-restart helper [**strict-lsa-checking**]

示例：

```
ciscoasa(config-router)# graceful-restart helper strict-lsa-checking
```

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，或者如果在启动平稳重启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。

默认情况下会启用平稳重启助手模式。

删除 OSPF 配置

删除 OSPFv2 配置。

操作步骤

步骤 1 删除已启用的整个 OSPFv2 配置。

clear configure router ospf *pid*

示例：

```
ciscoasa(config)# clear configure router ospf 1000
```

清除配置后，您必须使用 **router ospf** 命令重新配置 OSPF。

删除 OSPFv3 配置。

操作步骤

步骤 1 删除已启用的整个 OSPFv3 配置。

clear configure ipv6 router ospf *process-id*

示例：

```
ciscoasa(config)# clear configure ipv6 router ospf 1000
```

清除配置后，您必须使用 **ipv6 router ospf** 命令重新配置 OSPFv3。

OSPFv2 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 要清除 OSPFv2 配置，请输入以下命令：

```
ciscoasa(config)# clear configure router ospf pid
```

OSPFv3 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信息，例如 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。

要监控或显示各种 OSPFv2 路由统计信息，请输入以下其中一个命令：

命令	目的
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 OSPFv2 数据库相关的信息列表。

命令	目的
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。
show ospf [*process-id*] **summary-address**	显示在 OSPFv2 进程下配置的所有汇总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。

要监控或显示各种 OSPFv3 路由统计信息，请输入以下其中一个命令：

命令	目的
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 OSPFv3 数据库相关的信息列表。

命令	目的
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。
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 统计信息。
show ipv6 ospf [*process-id*] **summary-prefix**	显示在 OSPFv3 进程下配置的所有汇总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 流量相关的统计信息。
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。

其他参考资料

RFC

RFC	标题
2328	OSPFv2
4552	OSPFv3 身份验证
5340	IPv6 的 OSPF

OSPF 历史记录

表 24-1 OSPF 的功能历史记录

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。 引入了以下命令：**route ospf**

表 24-1　　OSPF 的功能历史记录 （续）

功能名称	平台版本	功能信息
多情景模式下的动态路由	9.0(1)	在多情景模式中支持 OSPFv2 路由。
群集		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。 引入或修改了以下命令：**show route cluster**、 **show ipv6 route cluster**、**debug route cluster**、 **router-id cluster-pool**。
OSPFv3 支持 IPv6		IPv6 支持 OSPFv3 路由。 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 24-1 OSPF 的功能历史记录 （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。 修改了以下命令：**ospf dead-interval**
计时器		添加了新 OSPF 计时器；弃用了旧 OSPF 计时器。 引入了以下命令：**timers lsa arrival**、 **timers pacing**、 **timers throttle** 删除了以下命令：**Timers spf**、 **timers lsa-grouping-pacing**
使用访问列表筛选路由		现在支持使用 ACL 筛选路由。 引入了以下命令：**distribute-list** 引入了以下屏幕：
OSPF 监控增强功能		添加了其他 OSPF 监控信息。 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。 添加了以下命令：**redistribute bgp**
OSPF 支持不间断转发 (NSF)	9.3(1)	添加了对 NSF 的 OSPFv2 和 OSPFv3 支持。 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) 配置思科 ASA，以路由数据、执行身份验证和重新分发路由信息。

- 关于 EIGRP，第 25-1 页
- EIGRP 准则，第 25-2 页
- 配置 EIGRP，第 25-2 页
- 自定义 EIGRP，第 25-4 页
- EIGRP 的监控，第 25-17 页
- EIGRP 示例，第 25-17 页
- EIGRP 历史记录，第 25-18 页

关于 EIGRP

EIGRP 是思科开发的增强版的 IGRP。与 IGRP 和 RIP 不同， EIGRP 不发送定期路由更新。仅在网络拓扑发生更改时才会发送 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 的路由器会存储所有邻居路由表，以便可以迅速适应备用路由。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。这些查询会传播直至找到备用路由为止。对可变长度子网掩码功能的支持允许在网络号边界自动汇总路由。此外，还可以将 EIGRP 配置为在任何接口的任何位边界汇总。EIGRP 不会定期更新。相反，它仅在路由指标发生更改时才发送部分更新。部分更新的传播是自动绑定的，以便仅对需要该信息的路由器进行更新。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 用于动态获悉直连网络中其他路由器的过程。EIGRP 路由器发出组播 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出。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 中配置呼叫间隔以配置一个邻居，则发送到该邻居的 Hello 消息将作为单播消息发送。路由更新和确认消息作为单播消息发出。

一旦邻居关系建立后，除非网络拓扑发生更改，否则便不会交换路由更新。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 预期可收到来自该邻居的 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 将目标的所有路由都保存在拓扑表中，而不只是保存最低成本路由。最低成本路由会插入到路由表中。其他路由则保留在拓扑表中。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。后继路由是指用于进行数据包转发的具有到达目标的最低成本路径的邻居路由器。可行性计算可确保路径不是路由环路的一部分。

如果在拓扑表中找不到可行后继路由，则必须进行路由重新计算。在路由重新计算期间， DUAL 会查询 EIGRP 邻居获取路由，该邻居反过来又会查询其邻居。当路由器没有可用于路由的可行后继路由时，会返回一个无法访问消息。

在路由重新计算期间，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，则会将路由标记为陷入主动状态。系统会删除拓扑表中作为可行性后继路由指向无响应邻居的所有路由。

备注 如果没有 GRE 隧道，则 EIGRP 邻居关系就不会通过 IPSec 隧道受到支持。

EIGRP 准则

防火墙模式准则

仅在路由防火墙模式中受支持。不支持透明防火墙模式。

故障切换准则

在单情景模式和多情景模式下支持状态故障切换。

IPv6 规定

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，只能在主设备共享接口上的两个情景之间建立 EIGRP 邻接关系。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。

其他准则

- 由于不支持组播流量的情景间交换，因此 EIGRP 实例不能跨共享接口相互建立邻接关系。
- 最多支持一个 EIGRP 进程。

配置 EIGRP

本节介绍如何在系统中启用 EIGRP 进程。启用 EIGRP 后，请参阅以下各节了解如何在系统中自定义 EIGRP 进程。

- 启用 EIGRP，第 25-3 页
- 启用 EIGRP 末节路由，第 25-3 页

启用 EIGRP

只能在 ASA 中启用一个 EIGRP 路由进程。

要启用 EIGRP，请执行以下步骤：

操作步骤

步骤 1　创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp *as-num*

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2　配置参与 EIGRP 路由的接口和网络：

network *ip-addr* [*mask*]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

可以使用此命令配置一个或多个 **network** 语句。

已定义网络范围内的直接网络和静态网络由 ASA 通告。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅为 EIGRP 配置接口，第 25-6 页。

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路由器。通常情况下，除了发送末节路由器的默认路由以外，分布路由器不需要发送任何其他信息。

只有指定的路由会从末节路由器传播到分布路由器。作为末节路由器， ASA 使用消息“inaccessible”来响应对汇总、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。将 ASA 配置为末节后，它会向所有相邻路由器发送特定对等体信息包，报告自己的状态为末节路由器。收到通知其末节状态数据包的任何邻居都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不会查询该对等体。末节路由器依赖于分布路由器将正确的更新发送到所有对等体。

要启用 ASA 作为 EIGRP 末节路由进程，请执行以下步骤：

操作步骤

步骤 1　创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp *as-num*

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2　配置参与 EIGRP 路由的接口和网络：

network *ip-addr* [*mask*]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

可以使用此命令配置一个或多个 **network** 语句。

已定义网络范围内的直接网络和静态网络由 ASA 通告。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅配置被动接口，第 25-7 页一节。

步骤 3　配置末节路由进程：

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]}
```

必须指定哪些网络由末节路由进程向分布路由器通告。静态网络和已连接网络不会自动重新分发到末节路由进程。

备注　末节路由进程不维护完整的拓扑表。末节路由至少需要分布路由器的一个默认路由，以做出路由决策。

自定义 EIGRP

本节介绍如何自定义 EIGRP 路由。

- 为 EIGRP 路由进程定义网络，第 25-5 页
- 为 EIGRP 配置接口，第 25-6 页
- 配置被动接口，第 25-7 页
- 在接口上配置汇总汇聚地址，第 25-8 页
- 更改接口延迟值，第 25-8 页

- 在接口上启用 EIGRP 身份验证，第 25-9 页
- 定义 EIGRP 邻居，第 25-10 页
- 将路由重新分发到 EIGRP 中，第 25-11 页
- 在 EIGRP 中过滤网络，第 25-12 页
- 自定义 EIGRP 呼叫间隔和保持时间，第 25-13 页
- 禁用自动路由汇总，第 25-14 页
- 在 EIGRP 中配置默认信息，第 25-15 页
- 禁用 EIGRP 水平分割，第 25-16 页
- 重新启动 EIGRP 进程，第 25-16 页

为 EIGRP 路由进程定义网络

通过网络表，可指定 EIGRP 路由进程所使用的网络。对于参与 EIGRP 路由的接口，它必须位于网络条目定义的地址范围内。对于要通告的直连网络和静态网络，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掩码。

要添加或定义网络，请执行以下步骤：

操作步骤

步骤 1　创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp *as-num*

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2　配置参与 EIGRP 路由的接口和网络：

network *ip-addr* [*mask*]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

可以使用此命令配置一个或多个 **network** 语句。

已定义网络范围内的直接网络和静态网络由 ASA 通告。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅配置被动接口，第 25-7 页。

为 EIGRP 配置接口

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，您可以配置其中包含该接口所连接网络的 **network** 命令，并使用 **passive-interface** 命令阻止该接口发送或接收 EIGRP 更新。

要为 EIGRP 配置接口，请执行以下步骤：

操作步骤

步骤 1　创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp *as-num*

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2　配置参与 EIGRP 路由的接口和网络：

```
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
```

可以使用此命令配置一个或多个 network 语句。

已定义网络范围内的直接网络和静态网络由 ASA 通告。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅为 EIGRP 路由进程定义网络，第 25-5 页。

步骤 3　控制默认候选路由信息的发送或接收：

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}
```

输入 **no default-information in** 命令会导致在收到的路由中阻止候选默认路由位。

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。

有关详细信息，请参阅在 EIGRP 中配置默认信息，第 25-15 页。

步骤 4　启用 EIGRP 数据包的 MD5 身份认证：

authentication mode eigrp *as-num* **md5**

示例：

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

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 会返回以下错误消息：

```
% Asystem(100) specified does not exist
```

有关详细信息，请参阅在接口上启用 EIGRP 身份验证，第 25-9 页。

步骤 5　设置延迟值：

delay *value*

示例：

```
ciscoasa(config-if)# delay 200
```

输入的*value* 参数以 10 倍微秒数为单位。要设置延迟 2000 毫秒，请输入 200 作为 *value* 的值。

要查看分配给接口的延迟值，请使用 **show interface** 命令。

有关详细信息，请参阅更改接口延迟值，第 25-8 页。

步骤 6　更改呼叫间隔：

hello-interval eigrp *as-num seconds*

示例：

```
ciscoasa(config)# hello-interval eigrp 2 60
```

有关详细信息，请参阅自定义 EIGRP 呼叫间隔和保持时间，第 25-13 页。

步骤 7　更改保持时间：

hold-time eigrp *as-num seconds*

示例：

```
ciscoasa(config)# hold-time eigrp 2 60
```

有关详细信息，请参阅自定义 EIGRP 呼叫间隔和保持时间，第 25-13 页。

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。要配置被动接口，请执行以下步骤：

操作步骤

步骤 1　创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp *as-num*

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2　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 **network** 语句。

```
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
```

已定义网络范围内的直接网络和静态网络由 ASA 通告。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅为 EIGRP 路由进程定义网络，第 25-5 页。

步骤 3　阻止接口发送或接收 EIGRP 路由消息。

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}
```

使用 **default** 关键字可禁用所有接口上的 EIGRP 路由更新。按 **nameif** 命令中定义的内容指定接口名称，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。

在接口上配置汇总汇聚地址

可以逐个接口配置汇总地址。如果要创建不会出现在网络号边界上的汇总地址，或者要在自动路由汇总禁用的情况下在 ASA 上使用汇总地址，则需要手动定义汇总地址。如果路由表中存在任何更具体的路由，则 EIGRP 将使用与所有更具体路由的最小值相等的指标从接口通告汇总地址。

要创建汇总地址，请执行以下操作：

操作步骤

步骤 1　针对正在更改 EIGRP 所使用的延迟值的接口，进入接口配置模式：

interface *phy_if*

示例：

```
ciscoasa(config)# interface inside
```

步骤 2　创建汇总地址：

summary-address eigrp *as-num address mask* [*distance*]

示例：

```
ciscoasa(config-if)# summary-address eigrp 2 address mask [20]
```

默认情况下，所定义的 EIGRP 汇总地址的管理距离为 5。可以通过在 **summary-address** 命令中指定可选的 *distance* 参数来更改该值。

更改接口延迟值

接口延迟值用于 EIGRP 距离计算。可以逐个接口修改该值。

要更改接口延迟值，请执行以下步骤：

操作步骤

步骤 1　针对正在更改 EIGRP 所使用的延迟值的接口，进入接口配置模式：

interface *phy_if*

示例：

```
ciscoasa(config)# interface inside
```

步骤 2　设置延迟值：

delay *value*

示例：
```
ciscoasa(config-if)# delay 200
```

输入的*value* 参数以 10 倍微秒数为单位。要设置延迟 2000 毫秒，请输入 200 作为 *value* 的值。

注意　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 路由身份验证提供对来自 EIGRP 路由协议的路由更新的 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。

系统会逐个接口配置 EIGRP 路由身份验证。必须使用相同的身份验证模式和密钥来配置接口上为 EIGRP 消息身份验证配置的所有 EIGRP 邻居，才能建立邻接关系。

备注　必须先启用 EIGRP，然后才能启用 EIGRP 路由身份验证。

要在接口上启用 EIGRP 身份验证，请执行以下步骤：

操作步骤

步骤 1　创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp *as-num*

示例：
```
hostname(config)# router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2　配置参与 EIGRP 路由的接口和网络：

network *ip-addr* [*mask*]

示例：
```
hostname(config)# router eigrp 2
hostname(config-router)# network 10.0.0.0
255.0.0.0
```

- 可以使用此命令配置一个或多个 network 语句。
- 已定义网络范围内的直接网络和静态网络由 ASA 通告。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。
- 如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅配置 EIGRP，第 25-2 页。

步骤 3　针对正在配置 EIGRP 消息身份验证的接口，进入接口配置模式：

interface *phy_if*

示例：

```
hostname(config)# interface inside
```

步骤 4　启用 EIGRP 数据包的 MD5 身份认证：

authentication mode eigrp *as-num* **md5**

示例：

```
hostname(config)# authentication mode eigrp 2 md5
```

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 会返回以下错误消息：

```
% Asystem(100) specified does not exist
```

步骤 5　配置 MD5 算法所使用的密钥：

authentication key eigrp *as-num key* **key-id** *key-id*

示例：

```
hostname(config)# authentication key eigrp 2 cisco key-id 200
```

- *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 会返回以下错误消息：

  ```
  % Asystem(100) specified does not exist%
  ```

- *key* 参数最多可包含 16 个字符，包括字母、数字和特殊字符。在 key 参数中不允许使用空格。
- *key-id* 参数是范围可从 0 到 255 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 邻居位于整个非广播网络 （例如隧道）内，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。

要手动定义 EIGRP 邻居，请执行以下步骤：

操作步骤

步骤 1　创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp *as-num*

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2　定义静态邻居：

neighbor *ip-addr* **interface** *if_name*

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

ip-addr 参数是邻居的 IP 地址。

if-name 参数是按照 **nameif** 命令指定的接口名称，邻居通过该名称可用。可以为 EIGRP 路由进程定义多个邻居。

将路由重新分发到 EIGRP 中

您可以将 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 配置中的 **network** 语句范围内，则无需将其重新分发。

备注　仅适用于 RIP：开始此程序之前，必须创建路由映射，以进一步定义将指定路由协议中的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 22 章 “路由映射”。

要将路由重新分发到 EIGRP 路由进程，请执行以下步骤：

操作步骤

步骤 1　创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp *as-num*

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2　（可选）指定应该应用于已重新分发到 EIGRP 路由进程的路由的默认指标：

default-metric *bandwidth delay reliability loading mtu*

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# default-metric bandwidth delay reliability loading mtu
```

如果未在 EIGRP 路由器配置中指定默认指标，则必须在每个 **redistribute** 命令中指定指标值。如果在 **redistribute** 命令中指定 EIGRP 指标且在 EIGRP 路由器配置中有 **default-metric** 命令，则使用 **redistribute** 命令中的指标。

步骤 3　将已连接路由重新分发到 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]
```

如果在 EIGRP 路由器配置中没有 **default-metric** 命令，则必须在 **redistribute** 命令中指定 EIGRP 指标值。

步骤 4　将静态路由重新分发到 EIGRP 路由进程：

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]
```

步骤 5　将路由从 OSPF 路由进程重新分发到 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]
```

步骤 6　将路由从 RIP 路由进程重新分发到 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]
```

在 EIGRP 中过滤网络

备注　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，创建一个标准 ACL，以定义要从发送或接收更新中过滤的路由。

要在 EIGRP 中过滤网络，请执行以下步骤：

操作步骤

步骤 1　创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp *as-num*

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2　配置参与 EIGRP 路由的接口和网络：

```
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
```

可以使用此命令配置一个或多个 network 语句。

已定义网络范围内的直接网络和静态网络由 ASA 通告。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅为 EIGRP 配置接口，第 25-6 页。

步骤 3　过滤 EIGRP 路由更新中发送的网络：

```
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]
```

可以指定接口，以将过滤器仅应用于由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。

步骤 4　过滤 EIGRP 路由更新中接收的网络：

```
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]
```

可以指定接口，以将过滤器仅应用于由该特定接口接收的更新。

自定义 EIGRP 呼叫间隔和保持时间

ASA 定期发送 Hello 数据包，以发现邻居以及获悉邻居何时变得无法访问或失效。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 可访问的时间长度。如果邻居在通告的保持时间内未收到 Hello 数据包，则将 ASA 视为无法访问。默认情况下，通告的保持时间是 15 秒 （呼叫间隔的三倍）。

Hello 时间间隔和通告的保持时间均逐个接口进行配置。我们建议将保持时间至少设置为呼叫间隔的三倍。

要配置呼叫间隔和通告保持时间，请执行以下步骤：

操作步骤

步骤 1　进入输入接口配置模式（针对正在配置呼叫间隔或通告保持时间的接口）：

interface *phy_if*

示例：

```
ciscoasa(config)# interface inside
```

步骤 2　更改呼叫间隔：

hello-interval eigrp *as-num seconds*

示例：

```
ciscoasa(config)# hello-interval eigrp 2 60
```

步骤 3　更改保持时间：

hold-time eigrp *as-num seconds*

示例：

```
ciscoasa(config)# hold-time eigrp 2 60
```

禁用自动路由汇总

默认情况下已启用自动路由汇总。EIGRP 路由进程在网络号边界上汇总。如果存在非连续网络，这可能会引起路由问题。

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汇总地址 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，则它们也会汇总为 192.168.0.0。为防止可能出现的将流量路由到错误位置，应在创建冲突性汇总地址的路由器上禁用自动路由汇总。

操作步骤

步骤 1　创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp *as-num*

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2　禁用自动路由汇总：

no auto-summary

示例：

```
ciscoasa(config-router)# no auto-summary
```

自动汇总地址的默认管理距离为 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。如果将 ASA 配置为禁止接收默认信息，则会导致在收到的路由中阻止候选默认路由位。如果将 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。

操作步骤

步骤 1　创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp *as-num*

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2　配置参与 EIGRP 路由的接口和网络：

```
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
```

可以使用此命令配置一个或多个 network 语句。

已定义网络范围内的直接网络和静态网络由 ASA 通告。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅为 EIGRP 配置接口，第 25-6 页。

步骤 3　控制默认候选路由信息的发送或接收：

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}
```

注意　输入 **no default-information in** 命令会导致在收到的路由中阻止候选默认路由位。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

水平分割用于控制 EIGRP 更新和查询数据包的发送。在接口上启用水平分割时，不会为以此接口为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降低路由环路的可能性。

默认情况下，所有接口上均启用水平分割。

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，可能出现此行为不如人意的情况。对于这些情况，包括配置了 EIGRP 的网络，可能要禁用水平分割。

如果在某个接口上禁用水平分割，则必须同时在该接口上的所有路由器和接入服务器禁用水平分割。

要禁用 EIGRP 水平分割，请执行以下步骤：

操作步骤

步骤 1　针对正在更改 EIGRP 所使用的延迟值的接口，进入接口配置模式：

interface *phy_if*

示例：

```
ciscoasa(config)# interface phy_if
```

步骤 2　禁用水平分割：

no split-horizon eigrp *as-number*

示例：

```
ciscoasa(config-if)# no split-horizon eigrp 2
```

重新启动 EIGRP 进程

您可以重新启动 EIGRP 进程，也可以清除重分发计数器或清除计数器。

操作步骤

步骤 1　重新启动 EIGRP 进程，或者清除重分发计数器或清除计数器：

clear eigrp pid {**1-65535** | **neighbors** | **topology** | **events)**}

示例：

```
ciscoasa(config)# clear eigrp pid 10 neighbors
```

EIGRP 的监控

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。

要监控或禁用各种 EIGRP 路由统计信息，请输入下面的一个命令：

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。
show eigrp [*as-number*] **traffic**	显示 EIGRP 流量统计信息。
show mfib cluster	显示有关转发条目和接口的 MFIB 信息。
show route cluster	显示有关集群的其他路由同步详细信息。
禁用 EIGRP 日志记录消息	
no eigrp log-neighbor-changes	禁用邻居变更消息的日志记录。在路由器配置模式下为 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。

备注　默认情况下，会记录邻居变更消息和邻居警告消息。

EIGRP 示例

以下示例显示如何通过各种可选进程启用和配置 EIGRP：

步骤 1　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　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　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　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　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 历史记录

表 25-1　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)	对于使用增强型内部网关路由协议 (EIGRP) 来路由数据、执行身份验证和重新分发及监控路由信息，添加了相应的支持。 引入了以下命令：**route eigrp**。
多情景模式下的动态路由	9.0(1)	在多情景模式下支持 EIGRP 路由。
群集	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。 引入或修改了以下命令：**show route cluster**、 **debug route cluster**、**show mfib cluster**、**debug mfib cluster**。
EIGRP 自动汇总	9.2(1)	默认情况下，现已针对 EIGRP 禁用 Auto-Summary 字段。



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。

- 关于组播路由，第 26-1 页
- 组播路由准则，第 26-3 页
- 启用组播路由，第 26-3 页
- 自定义组播路由，第 26-4 页
- 组播路由示例，第 26-14 页
- 组播路由历史记录，第 26-15 页

关于组播路由

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。

备注 组播路由同时支持 UDP 和非 UDP 传输。但是，非 UDP 传输没有进行快速路径优化。

- 末节组播路由，第 26-2 页
- PIM 组播路由，第 26-2 页
- 组播组概念，第 26-2 页
- 集群，第 26-2 页

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 同时支持 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 选举过程来构建。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。

备注　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。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，并希望接收发送到此组的流量。

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，从属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，重定向到主设备较为常见。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。从属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”。

组播路由准则

情景模式准则

在单情景模式中受支持。在多情景模式下，不支持非共享接口和共享接口。

防火墙模式准则

仅在路由防火墙模式中受支持。不支持透明防火墙模式。

IPv6 规定

不支持 IPv6。

其他准则

在集群中，对于 IGMP 和 PIM，仅在主设备上支持此功能。

启用组播路由

默认情况下，在 ASA 上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。

备注　组播路由仅支持 UDP 传输层。

操作步骤

步骤 1　启用组播路由：

```
multicast-routing
```

示例：

```
ciscoasa(config)# multicast-routing
```

组播路由表中的条目数量受 ASA 的 RAM 容量限制。

表 26-1 列出了基于 ASA 上 RAM 容量的特定组播表的最大条目数。一旦达到这些限制，将会丢弃所有新条目。

表 26-1　　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。

- 配置末节组播路由和转发 IGMP 消息，第 26-4 页
- 配置静态组播路由，第 26-4 页
- 配置 IGMP 功能，第 26-5 页
- 配置 PIM 功能，第 26-9 页
- 配置双向邻居过滤器，第 26-13 页
- 配置组播边界，第 26-14 页

配置末节组播路由和转发 IGMP 消息

备注　不同时支持末节组播路由和 PIM。

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。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。

操作步骤

步骤 1　配置末节组播路由和转发 IGMP 消息：

igmp forward interface *if_name*

示例：

```
ciscoasa(config-if)# igmp forward interface interface1
```

配置静态组播路由

配置静态组播路由可以分离组播流量与单播流量。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。

操作步骤

步骤 1　配置静态组播路由：

```
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]
```

步骤 2　配置末节区域的静态组播路由：

```
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]
```

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) 将其组成员身份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 消息来识别组成员身份。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处于活动状态或非活动状态的组。

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。

备注　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。

- 禁用接口上的 IGMP，第 26-6 页
- 配置 IGMP 组成员身份，第 26-6 页
- 配置静态加入的 IGMP 组，第 26-6 页
- 控制对组播组的访问，第 26-7 页
- 限制接口上的 IGMP 状态数量，第 26-8 页
- 修改发送到组播组的查询消息，第 26-8 页
- 更改 IGMP 版本，第 26-9 页

禁用接口上的 IGMP

您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。

操作步骤

步骤 1　禁用接口上的 IGMP：

no igmp

示例：

```
ciscoasa(config-if)# no igmp
```

要重新启用接口上的 IGMP，请使用 **igmp** 命令。

备注　接口配置中仅显示 **no igmp** 命令。

配置 IGMP 组成员身份

您可以将 ASA 配置成为组播组的成员。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。

备注　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，请参阅配置静态加入的 IGMP 组，第 26-6 页。

操作步骤

步骤 1　将 ASA 配置为组播组的成员：

igmp join-group *group-address*

示例：

```
ciscoasa(config-if)# igmp join-group mcast-group
```

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。您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。

操作步骤：

步骤 1　将 ASA 配置为静态加入到接口上的组播组：

igmp static-group

示例：

```
ciscoasa(config-if)# igmp static-group group-address
```

group-address 参数是该组的 IP 地址。

控制对组播组的访问

您可以通过使用访问控制列表控制对组播组的访问。

操作步骤

步骤 1　为组播流量创建标准 ACL：

access-list *name* **standard** [**permit | deny]** *ip_addr mask*

示例：

```
ciscoasa(config)# access-list acl1 standard permit 192.52.662.25
```

您可以为一个 ACL 创建多个条目。您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。

步骤 2　创建扩展 ACL：

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
```

dst_ip_addr 参数是被允许或拒绝的组播组的 IP 地址。

步骤 3　将 ACL 应用于接口：

igmp access-group *acl*

示例：

```
ciscoasa(config-if)# igmp access-group acl
```

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

您可以对每个接口限制 IGMP 成员身份报告造成的 IGMP 状态数量。超出所配置限制的成员身份报告不会输入到 IGMP 缓存中，多余成员身份报告的流量不会转发。

操作步骤：

步骤 1　限制接口上的 IGMP 状态数量：

igmp limit *number*

示例：

```
ciscoasa(config-if)# igmp limit 50
```

有效值的范围为 0 到 500，默认值为 500。

将此值设置为 0 可防止添加获悉的组，但仍允许手动定义成员身份 （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

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 上存储的成员身份信息。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主机查询的响应，它就会删除该组。

备注　**igmp query-timeout** 和 **igmp query-interval** 命令需要 IGMP V2。

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：

操作步骤

步骤 1　设置查询间隔时间 （以秒为单位）：

igmp query-interval *seconds*

示例：

```
ciscoasa(config-if)# igmp query-interval 30
```

有效值的范围为 0 到 500；默认值为 125。

如果 ASA 不能在指定超时值 （默认值为 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　更改查询的超时值：

igmp query-timeout *seconds*

示例：

```
ciscoasa(config-if)# igmp query-timeout 30
```

有效值的范围为 0 到 500；默认值为 225。

步骤 3　更改最大查询响应时间：

igmp query-max-response-time *seconds*

示例：

```
ciscoasa(config-if)# igmp query-max-response-time 30
```

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。

要控制在接口上运行的 IGMP 版本，请执行以下步骤。

操作步骤

步骤 1　控制要在接口上运行的 IGMP 版本：

igmp version {**1** | **2**}

示例：

```
ciscoasa(config-if)# igmp version 2
```

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。

备注　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。

- 启用和禁用接口上的 PIM，第 26-10 页
- 配置静态交汇点地址，第 26-10 页
- 配置指定路由器优先级，第 26-11 页
- 配置和筛选 PIM 注册消息，第 26-11 页

- 配置 PIM 消息间隔，第 26-12 页
- 筛选 PIM 邻居，第 26-12 页

启用和禁用接口上的 PIM

您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：

操作步骤

步骤 1　在特定接口上启用或重新启用 PIM：

pim

示例：

```
ciscoasa(config-if)# pim
```

步骤 2　在特定接口上禁用 PIM：

no pim

示例：

```
ciscoasa(config-if)# no pim
```

备注　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。

备注　ASA 不支持 Auto-RP 或 PIM BSR。您必须使用 **pim rp-address** 命令来指定 RP 地址。

您可以将 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)。

要配置 PIM PR 的地址，请执行以下步骤。

操作步骤

步骤 1　在特定接口上启用或重新启用 PIM：

pim rp-address *ip_address* [*acl*] [**bidir**]

```
ciscoasa(config)# pim rp-address 10.86.75.23 [acl1] [bidir]
```

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。请勿在使用此命令时一起使用主机 ACL。

排除 **bidir** 关键字会使组在 PIM 稀疏模式下运行。

备注　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，请执行以下步骤：

操作步骤

步骤 1　更改指定路由器优先级：

pim dr-priority *num*

示例：

```
ciscoasa(config-if)# pim dr-priority 500
```

num 参数可以是介于 1 到 4294967294 之间的任意数字。

配置和筛选 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 将会从其接受 PIM 注册消息的组播源。

要筛选 PIM 注册消息，请执行以下步骤：

操作步骤

步骤 1　配置 ASA 以筛选 PIM 注册消息：

pim accept-register {**list** *acl* | **route-map** *map-name*}

示例：

```
ciscoasa(config)# pim accept-register {list acl1 | route-map map2}
```

在此示例中， ASA 筛选 PIM 注册消息 *acl1* 和路由映射 *map2*。

配置 PIM 消息间隔

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。

要更改这些间隔时间，请执行以下步骤：

操作步骤

步骤 1　发送路由器查询消息：

pim hello-interval *seconds*

示例：

```
ciscoasa(config-if)# pim hello-interval 60
```

seconds 参数的有效值范围为 1 到 3600 秒。

步骤 2　更改 ASA 发送 PIM 加入消息或删除消息的时间 （以秒为单位）：

pim join-prune-interval *seconds*

示例：

```
ciscoasa(config-if)# pim join-prune-interval 60
```

seconds 参数的有效值范围为 10 到 600 秒。

筛选 PIM 邻居

您可以定义可成为 PIM 邻居的路由器。通过筛选可成为 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。

要定义可成为 PIM 邻居的邻居，请执行以下步骤：

操作步骤

步骤 1　使用标准 ACL 定义要加入到 PIM 的路由器：

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
```

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　筛选邻居路由器：

pim neighbor-filter pim_nbr

示例：

```
ciscoasa(config)# interface GigabitEthernet0/3
```

```
ciscoasa(config-if)# pim neighbor-filter pim_nbr
```

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 （如有）。PIM 双向邻居过滤器是定义可参与 DF 选举的邻居设备的 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 允许的邻居可参与 DF 选举过程。

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 定义可成为 ASA 的 PIM 邻居的设备。

双向 PIM 允许组播路由器保持减少的状态信息。要选择 DF，必须为 bidir 双向启用分片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 选举的路由器，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，即使分片上有非 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 选举。
- 如果一个被拒绝的邻居支持 bidir，将不会发生 DF 选举。
- 如果一个被拒绝的邻居不支持 bidir，可能会发生 DF 选举。

要定义可成为 PIM 双向邻居过滤器的邻居，请执行以下步骤：

操作步骤

步骤 1　使用标准 ACL 定义要加入到 PIM 的路由器：

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
```

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　筛选邻居路由器：

pim bidirectional-neighbor-filter pim_nbr

示例：

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidirectional neighbor-filter pim_nbr
```

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

地址范围定义了域边界，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。

您可以通过以下做法在接口上为组播地址设置使用管理性界定的边界：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性界定的地址。此地址范围可在不同组织管理的域中重复使用。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复使用。

您可以通过输入 **filter-autorp** 关键字在使用管理性界定的边界配置、检查和筛选 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 组范围通知都会被删除。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 消息转发前，将会筛选整个组范围并将其从 Auto-RP 消息中删除。

要配置组播边界，请执行以下步骤：

操作步骤

步骤 1　配置组播边界：

multicast boundary *acl* [**filter-autorp**]

示例：

```
ciscoasa(config-if)# multicast boundary acl1 [filter-autorp]
```

组播路由示例

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
```

组播路由历史记录

表 26-2　　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新发布和监控路由信息的支持。 引入了 **multicast-routing** 命令。
支持群集功能	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

- 关于 IPv6 邻居发现，第 27-1 页
- IPv6 邻居发现的必备条件，第 27-3 页
- IPv6 邻居发现准则，第 27-3 页
- IPv6 邻居发现的默认设置，第 27-4 页
- 配置 IPv6 邻居发现，第 27-5 页
- 监控 IPv6 邻居发现，第 27-11 页
- IPv6 邻居发现历史记录，第 27-11 页

关于 IPv6 邻居发现

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访问及哪些邻居不可访问，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。

- 邻居请求消息，第 27-1 页
- 邻居可访问时间，第 27-2 页
- 重复地址检测，第 27-2 页
- 路由器通告消息，第 27-2 页
- 静态 IPv6 邻居，第 27-3 页

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访问性。当节点要验证邻居的可访问性时，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。

邻居可访问时间

邻居可访问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暂停状态的接口。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保持为已配置。

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，如果是，路由器应用作默认路由器的持续时间 [以秒为单位]）。
- 主机的其他信息，例如主机在其发送的数据包中应使用的跃点限制和 MTU。
- 给定链路上邻居请求消息重新传输之间的时间。
- 节点将邻居视为可访问的时间。

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。

您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下输入。

静态 IPv6 邻居

您可以在 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 邻居发现的必备条件

请根据配置 IPv6 寻址，第 13-12 页配置 IPv6 地址。

IPv6 邻居发现准则

防火墙模式准则

透明防火墙模式下不支持以下 IPv6 邻居发现命令，因为它们需要路由器功能：

- **ipv6 nd prefix**
- **ipv6 nd ra-interval**
- **ipv6 nd ra-lifetime**
- **ipv6 nd suppress-ra**

其他准则和限制

- 时间间隔值包括在发送出此接口的所有 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。到达到期日期时，将不再通告前缀。
- 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访问。
- 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。值表示作为此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 视为此接口的默认路由器。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删除动态条目，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]）除外。
- 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 邻居发现缓存中删除静态条目；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 地址配置的故障切换 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，不可在故障切换接口上配置。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 27-1 列出 IPv6 邻居发现的默认设置。

表 27-1　　默认的 IPv6 邻居发现参数

参数	默认
邻居请求传输消息时间间隔的 *value*	邻居请求传输时间间隔为 1000 秒。
邻居可访问时间的 *value*	默认值为 0。
路由器通告传输时间间隔的 *value*	默认值为 200 秒。

表 27-1　默认的 IPv6 邻居发现参数 （续）

参数	默认
路由器有效期的 *value*	默认值为 1800 秒。
DAD 期间发送的连续邻居请求传输消息数量的 *value*	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

- 进入接口配置模式，第 27-5 页
- 配置邻居请求消息间隔，第 27-6 页
- 配置邻居可访问时间，第 27-6 页
- 配置路由器通告传输时间间隔，第 27-7 页
- 配置路由器有效期值，第 27-7 页
- 配置 DAD 设置，第 27-8 页
- 抑制路由器通告消息，第 27-8 页
- 为 IPv6 DHCP 中继配置地址配置标志，第 27-9 页
- 配置路由器通告中的 IPv6 前缀，第 27-9 页
- 配置静态 IPv6 邻居，第 27-10 页

进入接口配置模式

配置每个接口的邻居发现设置。要进入接口配置模式，请执行以下步骤。

操作步骤

步骤 1　进入接口配置模式：

interface *name*

示例：

```
hostname(config)# interface gigabitethernet 0/0
```

配置邻居请求消息间隔

要在接口上配置 IPv6 邻居请求重新传输之间的时间间隔，请以下步骤。

操作步骤

步骤 1　设置接口上 IPv6 邻居请求重新传输之间的时间间隔：

ipv6 nd ns-interval *value*

示例：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ns-interval 9000
```

值参数的有效值范围为 1000 到 3600000 毫秒。

此信息也在路由器通告消息中发送。

配置邻居可访问时间

要配置可访问性确认事件发生后远程 IPv6 节点被视为可访问的时间，请执行以下步骤：

操作步骤

步骤 1　设置远程 IPv6 节点可访问的时间：

ipv6 nd reachable-time *value*

示例：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd reachable-time 1700000
```

value 参数的有效值范围为 0 到 3600000 毫秒。

当该值为 0 时，将发送未确定的可访问时间。由接收设备来设置和跟踪可访问时间的值。

配置路由器通告传输时间间隔

要在接口上配置 IPv6 路由器通告传输之间的时间间隔，请执行以下步骤：

操作步骤

步骤 1　设置 IPv6 路由器通告传输之间的时间间隔：

ipv6 nd ra-interval [**msec**] *value*

示例：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-interval 201
```

可选 **msec** 关键字指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 到 1800 秒或 500 到 1800000 毫秒。

如果将 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，请参阅配置路由器有效期值，第 27-7 页。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。

配置路由器有效期值

要在接口上配置 IPv6 路由器通告的路由器有效期值，请执行以下步骤。

操作步骤

步骤 1　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：

ipv6 nd ra-lifetime [**msec**] *value*

示例：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-lifetime 2000
```

- 可选 **msec** 关键字指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 到 9000 秒。
- 输入 0 表示不应将 ASA 视为选定接口的默认路由器。

配置 DAD 设置

要在接口上指定 DAD 设置，请执行以下步骤。

操作步骤

步骤 1　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：

ipv6 nd dad attempts *value*

示例：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd dad attempts 20
```

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。

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。在不希望 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。

要在接口上抑制 IPv6 路由器通告的路由器有效期值，请执行以下步骤。

操作步骤

步骤 1　抑制路由器有效期值：

ipv6 nd suppress-ra *seconds*

示例：

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd suppress-ra 900
```

seconds 参数将 ASA 的有效性指定为该接口的默认路由器。有效值的范围为 0 到 9000 秒。

零值表示不应将 ASA 视为指定接口的默认路由器。

备注　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。

为 IPv6 DHCP 中继配置地址配置标志

您可以向 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。

操作步骤

步骤 1　在 IPv6 路由器通告数据包中设置托管地址配置标志：

ipv6 nd managed-config-flag

示例：

```
hostname (config-if)# ipv6 nd managed-config-flag
```

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。

步骤 2　在 IPv6 路由器通告数据包中设置其他地址配置标志：

ipv6 nd other-config-flag

示例：

```
hostname (config-if)# ipv6 nd other-config-flag
```

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

要配置包含在 IPv6 路由器通告中的 IPv6 前缀，请执行以下步骤：

操作步骤

步骤 1　配置包含在 IPv6 路由器通告中的 IPv6 前缀：

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)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

- 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* 语法指示有效期和首选项到期的日期和时间。到达此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** 关键字指示使用的默认值。

- 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无法将指定的前缀用于 IPv6 自动配置。
- 可选 **off-link** 关键字指示指定的前缀将不用于链路上确定。
- *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）。有效值的范围为 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。此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）。有效值的范围为 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）。

配置静态 IPv6 邻居

要在 IPv6 邻居发现缓存中配置静态条目，请执行以下步骤：

操作步骤

步骤 1　在 IPv6 邻居发现缓存中配置静态条目：

ipv6 neighbor *ipv6_address if_name mac_address*

示例：

```
hostname(config-if)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

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。

监控 IPv6 邻居发现

要监控 IPv6 邻居发现参数，请输入以下命令：

命令	目的
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访问时间。

IPv6 邻居发现历史记录

表 27-2　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)	引入了此功能。 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)	引入了以下命令：**ipv6 nd managed-config-flag**、 **ipv6 nd other-config-flag**。



第 6 部分

AAA 服务器和本地数据库



AAA 和本地数据库

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、执行策略、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。

本章还介绍如何为 AAA 功能配置本地数据库。对于外部 AAA 服务器，请参阅与您的服务器类型对应的章节。

- 关于 AAA 和本地数据库，第 28-1 页
- 本地数据库准则，第 28-4 页
- 向本地数据库添加用户帐户，第 28-4 页
- 生成共享密钥，第 28-7 页
- 监控本地数据库，第 28-8 页
- 本地数据库历史记录，第 28-9 页

关于 AAA 和本地数据库

本节介绍 AAA 和本地数据库。

- 身份验证，第 28-2 页
- 授权，第 28-2 页
- 记帐，第 28-2 页
- 身份验证、授权和记帐之间的交互，第 28-2 页
- AAA 服务器，第 28-2 页
- AAA 服务器组，第 28-3 页
- 关于本地数据库，第 28-3 页

身份验证

身份验证提供了一种识别用户的方法，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
- Network access
- VPN 接入

授权

授权是执行策略的过程：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
- Network access
- VPN 接入

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。身份验证用于识别用户。授权用于实施策略，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，则必须先为每种 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。可以按名称标识 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。

关于本地数据库

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。

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

对于多情景模式，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。

备注　您不能使用本地数据库进行网络访问授权。

回退支持

本地数据库可以用作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

从锁定中恢复，第 32-23 页

向本地数据库添加用户帐户

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 *username* 关键字是长度为 3 到 64 个字符的字符串，可以任意组合使用 ASCII 可打印字符 （字符代码 32-126），但是空格和问号除外。**password** *password* 关键字是长度为 3 到 32 个字符的字符串，可以任意组合使用 ASCII 可打印字符 （字符代码 32-126），但是空格和问号除外。**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。此权限级别与命令授权一起使用。

注意　如果未使用命令授权（**AAA 授权控制台 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** 关键字指示密码已加密。如果在 **username** 命令中定义了密码，则 ASA 会在将该密码保存到配置时会对其进行加密，以确保安全。当输入 **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，如果输入密码 “test”，则 **show running-config** 输出内容将与以下内容类似：

```
username user1 password DLaUiAX3178qgoB5c7iVNw== encrypted
```

只有在剪切并粘贴配置文件以在另一个 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 用户没有属性或组策略关联。您必须使用 **username attributes** 命令明确配置所有值。有关详情，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 关键字允许完全访问 **aaa authentication console LOCAL** 命令指定的所有服务。**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 ASDM 监控访问。如果使用 **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 关键字会拒绝管理访问。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

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- 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)#
```

您可以指定公共密钥文件 (PKF) 格式的密钥 （**pkf** 关键字）或 Base64 密钥 （**publickey** 关键字）。对于 **publickey**， *key* 是 Base64 编码的公共密钥。您可以使用任何可生成 SSH-RSA 原始密钥 （不带证书）的 SSH 密钥生成软件 （如 ssh keygen）生成密钥。

对于 **pkf** 密钥，系统将提示您粘贴 PKF 格式的密钥，最长 4096 位。此格式用于由于过长而无法以 Base64 格式内嵌粘贴的密钥。例如，可以使用 ssh keygen 生成 4096 位的密钥，然后将其转换为 PKF，并使用 **pkf** 关键字作为密钥提示。

注意　您可以将 **pkf** 选项与故障切换一起使用，但 PKF 密钥不会自动复制到备用系统。您必须输入 **write standby** 命令才能同步 PKF 密钥。

在 ASA 上使用 **show running-config username** 命令查看密钥时，密钥将使用 SHA-256 散列加密。即使输入 **pkf** 形式的密钥， ASA 也会对密钥进行散列处理，并将其显示为散列的 **publickey**。如果需要从 **show** 输出复制密钥，请使用 **hashed** 关键字指定 **publickey** 类型。

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。有关详情，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
```

生成共享密钥

要在 Linux 系统或 Macintosh 系统上为 SSH 生成共享密钥并将其导入，请执行以下步骤：

操作步骤

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+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 ----
jcrichton-mac:.ssh john$
```

步骤 3　将密钥复制到剪贴板。

步骤 4　连接到 ASA CLI，并将公钥添加到您的用户名：

```
ciscoasa(config)# username test attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- 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 ----
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

请查看以下用于监控本地数据库的命令：

- **show aaa-server**

  此命令可显示已配置的数据库统计信息。要清除 AAA 服务器配置，请输入 **clear aaa-server statistics** 命令。

- **show running-config aaa-server**

  此命令可显示 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。

本地数据库历史记录

表 28-1　　本地数据库历史记录

功能名称	平台版本	说明
AAA 的本地数据库配置	7.0(1)	介绍如何配置本地数据库以供 AAA 使用。 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，可以按每个用户启用公钥身份验证。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。 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。*



用于 AAA 的 RADIUS 服务器

本章介绍如何配置用于 AAA 的 RADIUS 服务器。

- 关于用于 AAA 的 RADIUS 服务器，第 29-1 页
- 用于 AAA 的 RADIUS 服务器准则，第 29-13 页
- 配置用于 AAA 的 RADIUS 服务器，第 29-13 页
- 监控用于 AAA 的 RADIUS 服务器，第 29-18 页
- 用于 AAA 的 RADIUS 服务器历史记录，第 29-19 页

关于用于 AAA 的 RADIUS 服务器

思科 ASA 支持以下符合 RFC 标准的用于 AAA 的 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、 7.x 和 8.x 中的 RSA RADIUS。
- Microsoft

支持的身份验证方法

ASA 支持下列使用 RADIUS 服务器的身份验证方法：

- 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（当启用密码管理功能时）。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。

备注 要将 MS-CHAPv2 启用为 ASA 与 RADIUS 服务器之间进行 VPN 连接所使用的协议，则必须在隧道组常规属性中启用密码管理。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，则可以通过使用 **no mschapv2-capable** 命令将该服务器配置为发送非 MS-CHAPv2 身份验证请求。

VPN 连接的用户授权

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授权 （按用户使用动态 ACL 或 ACL 名称）。要实施动态 ACL，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。设备会根据 ACL 允许或拒绝对指定服务的访问。当身份验证会话到期时， ASA 会删除 ACL。

除了 ACL 以外，ASA 还支持 VPN 远程访问和防火墙直接转发代理会话的权限授权与设置的许多其他属性。

支持的 RADIUS 属性集

ASA 支持以下 RADIUS 属性集：

- RFC 2138 中定义的身份验证属性。
- RFC 2139 中定义的记帐属性。
- RFC 2868 中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 中定义的 Microsoft VSA。
- 思科 VSA (Cisco-Priv-Level)。此属性集提供 0 至 15 级标准数字权限排名，最低级别为 1，最高级别为 15。0 级表示没有权限。1 级（登录）允许对此级别可用的命令执行特权执行访问。2 级 （启用）允许 CLI 配置权限。

支持的 RADIUS 授权属性

授权是指执行权限或属性的过程。如果已配置权限或属性，则定义为身份验证服务器的 RADIUS 服务器会执行权限或属性。这些属性具有供应商 ID 3076。

表 29-1 列出了支持的 RADIUS 用户授权属性。

备注 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 ACS 4.0 之前版本中的属性名称仍然包含 cVPN3000 前缀。ASA 基于属性数字 ID 而非属性名来执行 RADIUS 属性。

下表中列出的所有属性都是从 RADIUS 服务器发送到 ASA 的下游属性，但编号为 146、 150、 151 和 152 的属性除外，这些属性是从 ASA 发送到 RADIUS 服务器的上游属性。RADIUS 属性 146 和 150 从 ASA 发送到 RADIUS 服务器，用于身份验证请求和授权请求。以上所列的全部四个属性都是从 ASA 发送到 RADIUS 服务器，用于记帐开始请求、临时更新请求和停止请求。8.4(3) 版本引入了上游 RADIUS 属性 146、 150、 151 和 152。

在 9.0(1) 版本中，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 29-1　　支持的 RADIUS 授权属性

属性名称	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	时间范围的名称，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 本地池的名称
Allow-Network-Extension-Mode	有	64	布尔值	单值	0 = 已禁用 1 = 已启用
Authenticated-User-Idle-Timeout	有	50	整数	单值	1-35791394 分钟
Authorization-DN-Field	有	67	字符串	单值	可能的值：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	要为思科 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	要为思科 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，则 Banner2 字符串会连接到 Banner1 字符串。
Cisco-IP-Phone-Bypass	有	51	整数	单值	0 = 已禁用 1 = 已启用
Cisco-LEAP-Bypass	有	75	整数	单值	0 = 已禁用 1 = 已启用
Client Type	有	150	整数	单值	1 = 思科 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 = 已禁用 1 = 已启用

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
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 版本及更高版本，请改用此属性而非 IETF-Radius-Class。您可以使用以下其中一种格式： • *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	换行符 (\n) 分隔的 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 = 无修改 2 = 无代理 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 = 已禁用 1 = 已启用
Intercept-DHCP-Configure-Msg	有	62	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Allow-Passwd-Store	有	16	布尔值	单值	0 = 已禁用 1 = 已启用
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 = 具有有效期的 RADIUS 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	有	42	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Backup-Server-List	有	60	字符串	单值	服务器地址 （以空格分隔）
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	指定要作为防火墙策略推送到客户端的过滤器的名称

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
IPsec-Client-Firewall-Filter-Optional	有	58	整数	单值	0 = 必需 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 到 255 个字符）。
IPsec-IKE-Peer-ID-Check	有	40	整数	单值	1 = 必需 2 = 如果受对等体证书支持 3 = 不检查
IPsec-IP-Compression	有	39	整数	单值	0 = 已禁用 1 = 已启用
IPsec-Mode-Config	有	31	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP	有	34	布尔值	单值	0 = 已禁用 1 = 已启用
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 到 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 = 允许本地 LAN
IPsec-Split-Tunnel-List	有	27	字符串	单值	指定用于描述分割隧道包含列表的网络或 ACL 的名称。
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 = 已禁用 1 = 已启用
IPv6-Address-Pools	有	218	字符串	单值	IP 本地池 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 = 无状态请求 15= 40/128 位加密/无状态请求
L2TP-MPPC-Compression		38	整数	单值	0 = 已禁用 1 = 已启用

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
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 = 无状态请求 15= 40/128 位加密/无状态请求
PPTP-MPPC-Compression		37	整数	单值	0 = 已禁用 1 = 已启用
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。
Required-Client- Firewall-Vendor-Code	有	45	整数	单值	1 = 思科系统公司 （带思科集成客户端） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = 思科系统公司 （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

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
Required-Client-Firewall-Product-Code	有	46	整数	单值	思科系统公司产品： 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 = 已禁用 1 = 已启用
Require-HW-Client-Auth	有	48	布尔值	单值	0 = 已禁用 1 = 已启用
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 Session Subtype 的适用条件是 Session Type (151) 属性仅具有以下值：1、 2、 3 和 4。
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 = 思科 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 = 已禁用 1 = 已启用 2 = 自动启动

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
Smart-Tunnel-Auto-Signon-Enable	有	139	字符串	单值	智能隧道自动登录名称列表 （附带域名）
Strip-Realm	有	135	布尔值	单值	0 = 已禁用 1 = 已启用
SVC-Ask	有	131	字符串	单值	0 = 已禁用 1 = 已启用 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 家	字符串	单值	字符串 （模块的名称）
SVC-MTU	有	125	整数	单值	MTU 值 256 到 1406 个字节
SVC-Profiles	有	128	字符串	单值	字符串 （配置文件的名称）
SVC-Rekey-Time	有	110	整数	单值	0 = 已禁用 1-10080 分钟
Tunnel Group Name	有	146	字符串	单值	1 到 253 个字符
Tunnel-Group-Lock	有	85	字符串	单值	隧道组的名称或 “none”
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。 合法值为 0-11、 16-27、 32-43，以及 48-59 。
Use-Client-Address		17	布尔值	单值	0 = 已禁用 1 = 已启用
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 的名称

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
WebVPN-ActiveX-Relay	有	137	整数	单值	0 = 已禁用 Otherwise = 已启用
WebVPN-Apply-ACL	有	102	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Auto-HTTP-Signon	有	124	字符串	单值	保留
WebVPN-Citrix-Metaframe-Enable	有	101	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Content-Filter-Parameters	有	69	整数	单值	1 = Java ActiveX 2 = Java 脚本 4 = 映像 8 = 映像中的 Cookie
WebVPN-Customization	有	113	字符串	单值	自定义的名称
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 （最多 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 = 已禁用 1 = 已启用
WebVPN-File-Server-Browsing-Enable	有	96	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Entry-Enable	有	95	整数	单值	0 = 已禁用 1 = 已启用
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
WebVPN-Home-Page-Use-Smart-Tunnel	有	228	布尔值	单值	已启用 （如果无客户端主页将通过智能隧道呈现）。
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 = Deflate 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 = 已禁用。
WebVPN-Keepalive-Ignore	有	121	整数	单值	0 - 900

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
WebVPN-Macro-Substitution	有	223	字符串	单值	无限制。例如，请参阅位于以下 URL 的《*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，请参阅位于以下 URL 的《*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 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	有	98	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-HTTP-Proxy	有	99	整数	单值	0 = 已禁用 1 = 已启用
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”）。 此文本将替换无客户端门户主页上的默认字符串 “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 = 已禁用。
WebVPN Smart-Card-Removal-Disconnect	有	225	布尔值	单值	0 = 已禁用 1 = 已启用
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	智能隧道自动登录名称列表 （附带域名）
WebVPN-Smart-Tunnel-Auto-Start	有	138	整数	单值	0 = 已禁用 1 = 已启用 2 = 自动启动
WebVPN-Smart-Tunnel-Tunnel-Policy	有	227	字符串	单值	“e networkname”、“i networkname”或“a”中之一，其中 networkname 是指智能隧道网络列表的名称， e 表示不包含的隧道， i 表示指定的隧道， a 表示所有隧道。
WebVPN-SSL-VPN-Client-Enable	有	103	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSL-VPN-Client-Keep-Installation	有	105	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSL-VPN-Client-Required	有	104	整数	单值	0 = 已禁用 1 = 已启用

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
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 到 600 秒， 0 = 关闭
WebVPN-SVC-Client-DPD-Frequency	有	108	整数	单值	5 到 3600 秒， 0 = 关闭
WebVPN-SVC-DTLS-Enable	有	123	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-DTLS-MTU	有	125	整数	单值	MTU 值为 256 到 1406 个字节。
WebVPN-SVC-Gateway-DPD-Frequency	有	109	整数	单值	5 到 3600 秒， 0 = 关闭
WebVPN-SVC-Rekey-Time	有	110	整数	单值	4 到 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 （Deflate 压缩）
WebVPN-UNIX-Group-ID (GID)	有	222	整数	单值	有效 UNIX 组 ID
WebVPN-UNIX-User-ID (UID)	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 = 已禁用 1 = 已启用
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

下表列出了支持的 IETF RADIUS 属性。

表 29-2　　支持的 IETF RADIUS 属性

属性名称	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，我们建议使用 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

表 29-2　　支持的 IETF RADIUS 属性 （续）

IETF-Radius-Idle-Timeout	有	28	整数	单值	秒
IETF-Radius-Service-Type	有	6	整数	单值	秒。可能的 Service Type 值： • .Administrative - 允许用户访问配置提示符。 • .NAS-Prompt - 允许用户访问 exec 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 记帐连接断开原因代码

如果 ASA 在发送数据包时遇到连接断开问题，则会返回以下代码：

连接断开原因代码
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
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

用于 AAA 的 RADIUS 服务器准则

本节介绍您在配置用于 AAA 的 RADIUS 服务器之前应检查的准则和限制。

IPv6

AAA 服务器必须使用 IPv4 地址，但是终端可以使用 IPv6。

其他准则

- 在单模式下可以有最多 100 个服务器组，在多模式下每个情景可以有 4 个服务器组。
- 在单模式下每个组可以有最多 16 个服务器，在多模式下每个组可以有 4 个服务器。

相关主题

- 回退支持，第 28-3 页
- 组中存在多个服务器时的回退方式，第 28-4 页
- 从锁定中恢复，第 32-23 页

配置用于 AAA 的 RADIUS 服务器

本节介绍如何配置用于 AAA 的 RADIUS 服务器。

步骤 1　将 ASA 属性加载到 RADIUS 服务器。用于加载属性的方法取决于您使用的 RADIUS 服务器类型：

- 对于思科 ACS：服务器已集成这些属性。您可以跳过此步骤。
- 对于来自其他供应商的 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。要定义属性，请使用属性名称或编号、类型、值和供应商代码 (3076)。

步骤 2　添加 RADIUS 服务器组。请参阅配置 RADIUS 服务器组，第 29-13 页。

步骤 3　对于某个服务器组，向服务器组添加服务器。请参阅向组中添加 RADIUS 服务器，第 29-16 页。

配置 RADIUS 服务器组

如果您要将外部 RADIUS 服务器用于身份验证、授权或记帐，则必须先为每个 AAA 协议创建至少一个 RADIUS 服务器组，然后向每个服务器组添加一个或多个服务器。可以按名称标识 AAA 服务器组。

要添加 RADIUS 服务器组，请执行以下步骤：

操作步骤

步骤 1　确定服务器组名称和协议。

aaa-server *server_tag* **protocol radius**

示例：

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)#
```

输入 **aaa-server protocol** 命令时，会进入 AAA 服务器组配置模式。

步骤 2　将可下载的 ACL 与来自 RADIUS 数据包的思科 AV 对中收到的 ACL 合并。

merge-dacl {**before-avpair** | **after-avpair**}

示例：

```
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

默认设置为 **no merge dacl**，指定可下载的 ACL 不与思科 AV 对 ACL 合并。如果同时收到 AV 对和可下载的 ACL，将优先使用 AV 对。

before-avpair 选项指定可下载的 ACL 条目应放置在思科 AV 对条目之前。

after-avpair 选项指定可下载的 ACL 条目应放置在思科 AV 对条目之后。此选项仅适用于 VPN 连接。对于 VPN 用户，ACL 的形式可以是思科 AV 对 ACL、可下载 ACL 和在 ASA 上配置的 ACL。此选项确定是否合并可下载的 ACL 与 AV 对 ACL，不适用于在 ASA 上配置的任何 ACL。

步骤 3　指定在 ASA 尝试下一个服务器之前可向组中的 RADIUS 服务器发送的最大请求数。

max-failed-attempts *number*

示例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 参数的取值范围为 1 至 5。默认值为 3。

如果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。该服务器组仍然标记为 10 分钟（默认值）内无响应，因此该时段内其他的 AAA 请求不会尝试联系该服务器组，而是会立即使用回退方法。如果没有回退方法， ASA 会继续重试该组中的服务器。

步骤 4　指定用于重新激活组中的已失败服务器的方法（重新激活策略）。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

示例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

depletion 关键字仅在组中的所有服务器均处于非活动状态后，才重新激活已失败的服务器。

deadtime *minutes* 关键字-参数对指定介于 0 至 1440（以分钟为单位）之间的时长，该时长是禁用组中的最后一台服务器到随后重新启用所有服务器之间会经过的一段时间。默认值为 10 分钟。

timed 关键字在 30 秒的停止运行时间之后，重新激活已失败的服务器。

步骤 5　向组中的所有服务器发送记帐消息。

accounting-mode simultaneous

示例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

输入 **accounting-mode single** 命令，恢复到仅向活动服务器发送消息的默认设置。

步骤 6　确定服务器及其所属的 AAA 服务器组。

aaa-server *server_group* [*interface_name*] **host** *server_ip*

示例：

```
ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1
```

输入 **aaa-server host** 命令时，将会进入 AAA 服务器主机配置模式。

步骤 7　为 AAA 服务器组启用 RADIUS 动态授权 (CoA) 服务。

dynamic-authorization {port *port-number*}

示例：

```
ciscoasa(config-aaa-server-group)# dynamic-authorization port 1700
```

定义后会注册相应的 RADIUS 服务器组以用于 CoA 通知，且 ASA 会侦听用于从 ISE 获取 CoA 策略更新的端口。

CoA 侦听 *port-number* 的有效范围为 1 至 65535。

如果此命令的 **no** 形式中指定的端口号或接口与当前配置中的行不匹配，则会显示错误消息。

步骤 8　为 RADIUS 服务器组启用仅授权模式。

authorize-only

示例：

```
ciscoasa(config-aaa-server-group)# authorize-only
```

当此服务器组用于授权时， RADIUS 访问请求消息将会构建为“仅授权”请求，而不是现在可用的已配置的密码方法。

仅授权请求包含带有仅授权值 (17) 的服务类型属性以及访问请求内的消息身份验证器。

支持仅授权模式则无需在访问请求中包含 RADIUS 公用密码。因此，不需要在 aaa-server-host 模式下使用 radius-common-pw CLI 配置公用密码。

注意　仅授权模式是配置用于服务器组，而公用密码则是特定于主机。因此，一旦配置了仅授权模式，就会忽略为单个 AAA 服务器配置的公用密码。

步骤 9　关闭对于与特定隧道组建立的连接的 hostscan 处理。

without-csd {**anyconnect**}

示例：

```
ciscoasa(config-tunnel-webvpn)# without-csd anyconnect
```

此设置目前适用于无客户端连接和第 3 层连接。该命令已被修改为可以将此设置仅应用于 AnyConnect 连接。

示例

以下示例显示如何添加包含一台服务器的 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
```

以下示例显示如何为仅授权、动态授权 (CoA) 更新和每小时定期记帐配置 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
```

以下示例显示如何为采用 ISE 的密码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
```

以下示例显示如何为采用 ISE 的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
```

向组中添加 RADIUS 服务器

要向组中添加 RADIUS 服务器，请执行以下步骤：

操作步骤

步骤 1　确定 RADIUS 服务器及其所属的 AAA 服务器组。

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
```

输入 **aaa-server host** 命令时，将会进入 AAA 服务器主机配置模式。

步骤 2　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。

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

示例：

```
ciscoasa(config-aaa-server-host)# acl-netmask-convert standard
```

关键字 **auto-detect** 指定 ASA 应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，则会将其转换为标准网络掩码表达式。

关键字 **standard** 指定 ASA 假定来自 RADIUS 服务器的可下载 ACL 仅包含标准网络掩码表达式。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 仅包含通配符网络掩码表达式，并且在下载 ACL 后会将其全部转换为标准网络掩码表达式。

步骤 3　指定用于所有通过 ASA 访问 RADIUS 授权服务器的用户的公用密码。

radius-common-pw *string*

示例：

```
ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc
```

参数 *string* 是一个区分大小写的字母数字关键字 （最多为 127 个字符），将用作与 RADIUS 服务器进行的所有授权事务的公用密码。

步骤 4　对 RADIUS 服务器启用 MS-CHAPv2 身份验证请求。

mschapv2-capable

示例：

```
ciscoasa(config-aaa-server-host)# mschapv2-capable
```

步骤 5　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）。

timeout *hh:mm:ss*

示例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

步骤 6　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。

retry-interval *seconds*

示例：

```
ciscoasa(config-aaa-server-host)# retry-interval 8
```

参数 *seconds* 指定请求的重试间隔时间（1 到 10 秒）。这是 ASA 在重试连接请求之前等待的时间。

注意　无论您输入了哪种 retry-interval 设置，随后的重试间隔时间始终为 50 或 100 毫秒。这是预期行为。

步骤 7　向组中的所有服务器发送记帐消息。

accounting-mode simultaneous

示例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

输入 **accounting-mode single** 命令，恢复到仅向活动服务器发送消息的默认设置。

步骤 8　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。

authentication-port *port*

示例：

```
ciscoasa(config-aaa-server-host)# accounting-port 1646
```

步骤 9　将记帐端口指定为端口 1646 或者指定用于主机记帐的服务器端口。

accounting-port *port*

示例：

```
ciscoasa(config-aaa-server-host)# accounting-port 1646
```

步骤 10　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。

key

示例：

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

您配置的服务器密钥应与在 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 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)#
```

监控用于 AAA 的 RADIUS 服务器

请参阅以下命令以监控用于 AAA 的 RADIUS 服务器的状态：

- **show aaa-server**

  此命令可显示配置的 RADIUS 服务器统计信息。

- **show running-config aaa-server**

  此命令可显示 RADIUS 服务器运行配置。

- **clear aaa-server statistics**

  此命令可清除 RADIUS 服务器配置。

用于 AAA 的 RADIUS 服务器历史记录

表 29-3　　用于 AAA 的 RADIUS 服务器历史记录

功能名称	平台版本	说明
用于 AAA 的 RADIUS 服务器	7.0(1)	说明如何配置用于 AAA 的 RADIUS 服务器。 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**。
通过来自 ASA 的 RADIUS 访问请求和记帐请求数据包发送主要的供应商特定属性 (VSA)	8.4(3)	四个新 VSA - 通过来自 ASA 的 RADIUS 访问请求数据包发送 Tunnel Group Name (146) 和 Client Type (150)。通过来自 ASA 的 RADIUS 记帐请求数据包发送 Session Type (151) 和 Session Subtype (152)。为所有类型的记帐请求数据包 （Start、 Interim-Update 和 Stop）发送全部四个属性。RADIUS 服务器（例如 ACS 和 ISE）可以执行授权和策略属性，或者将这些属性用于记帐和收费。



用于 AAA 的 TACACS+ 服务器

本章介绍如何配置 AAA 中使用的 TACACS+ 服务器。

- 关于用于 AAA 的 TACACS+ 服务器，第 30-1 页
- 用于 AAA 的 TACACS+ 服务器的准则，第 30-2 页
- 配置 TACACS+ 服务器，第 30-3 页
- 监控用于 AAA 的 TACACS+ 服务器，第 30-5 页
- 用于 AAA 的 TACACS+ 服务器历史记录，第 30-5 页

关于用于 AAA 的 TACACS+ 服务器

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。

TACACS+ 属性

思科 ASA 可支持 TACACS+ 属性。TACACS+ 属性可分隔身份验证、授权和记帐功能。该协议支持两种类型的属性：强制属性和可选属性。服务器和客户端都必须能够理解强制属性，而且必须将强制属性应用于用户。可选属性是否能被理解，或是否会被使用不作要求。

备注 要使用 TACACS+ 属性，请确保您已在 NAS 上启用 AAA 服务。

下表列出适用于直接转发代理连接的受支持的 TACACS+ 授权响应属性。

表 30-1 支持的 TACACS+ 授权响应属性

属性	描述
acl	确定要应用于连接的本地配置的 ACL。
idletime	指示经过身份验证的用户会话终止前可以处于非活动状态的时长 （以分钟为单位）。
timeout	指示经过身份验证的用户会话终止前，身份验证凭据可以保持活动状态的时长 （以分钟为单位）。

下表列出支持的 TACACS+ 记帐属性。

?

表 30-2　　支持的 TACACS+ 记帐属性

属性	描述
bytes_in	指定此连接过程中传输的输入字节的数量 （仅停止记录）
bytes_out	指定此连接过程中传输的输出字节的数量 （仅停止记录）。
cmd	定义执行的命令 （仅命令记帐）。
disc-cause	指定标识连接断开原因的数值代码 （仅停止记录）。
elapsed_time	定义连接所消耗的秒数 （仅停止记录）。
foreign_ip	指定隧道连接的客户端的 IP 地址。定义用于直接转发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。定义用于直接转发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	指定此连接过程中传输的输入数据包的数量。
packs_out	指定此连接过程中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	指示客户端的 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。

用于 AAA 的 TACACS+ 服务器的准则

本节介绍您在配置用于 AAA 的 TACACS+ 服务器之前应检查的准则和限制。

IPv6

AAA 服务器必须使用 IPv4 地址，但是终端可以使用 IPv6。

其他准则

- 在单模式下可以有最多 100 个服务器组，在多模式下每个情景可以有 4 个服务器组。
- 在单模式下每个组可以有最多 16 个服务器，在多模式下每个组可以有 4 个服务器。

相关主题

- 回退支持，第 28-3 页
- 组中存在多个服务器时的回退方式，第 28-4 页
- 从锁定中恢复，第 32-23 页

配置 TACACS+ 服务器

本节介绍如何配置 TACACS+ 服务器。

步骤 1　添加 TACACS+ 服务器组。请参阅配置 TACACS+ 服务器组，第 30-3 页。

步骤 2　对于某个服务器组，向服务器组添加服务器。请参阅将 TACACS+ 服务器添加到服务器组，第 30-4 页。

配置 TACACS+ 服务器组

如果要将 TACACS+ 服务器用于身份验证、授权或记帐，则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。您可以按名称标识 TACACS+ 服务器组。

要添加 TACACS+ 服务器组，请执行以下步骤：

操作步骤

步骤 1　确定服务器组名称和协议。

aaa-server *server_tag* **protocol tacacs+**

示例：

```
ciscoasa(config)# aaa-server servergroup1 protocol tacacs+
```

输入 **aaa-server protocol** 命令时，会进入 AAA 服务器组配置模式。

步骤 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。

max-failed-attempts *number*

示例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 参数的取值范围为 1 至 5。默认值为 3。

如果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。该服务器组仍然标记为 10 分钟（默认值）内无响应，因此该时段内其他的 AAA 请求不会尝试联系该服务器组，而是会立即使用回退方法。如要将无响应时段从默认值改为其他值，请参阅下一步中的 **reactivation-mode** 命令。

如果没有回退方法， ASA 会继续重试该组中的服务器。

步骤 3　指定用于重新激活组中的已失败服务器的方法（重新激活策略）。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

示例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

depletion 关键字仅在组中的所有服务器均处于非活动状态后，才重新激活已失败的服务器。

deadtime *minutes* 关键字-参数对指定介于 0 至 1440（以分钟为单位）之间的时长，该时长是禁用组中的最后一台服务器到随后重新启用所有服务器之间会经过的一段时间。默认值为 10 分钟。

timed 关键字在 30 秒的停止运行时间之后，重新激活已失败的服务器。

步骤 4　向组中的所有服务器发送记帐消息。

accounting-mode simultaneous

示例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

如要恢复仅向活动服务器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+ 服务器添加到服务器组

要将 TACACS+ 服务器添加到服务器组，请执行以下操作：

操作步骤

步骤 1　确定 TACACS+ 服务器，以及该服务器所属的服务器组。

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
```

输入 **aaa-server host** 命令时，将会进入 AAA 服务器主机配置模式。

步骤 2　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）。

timeout *hh:mm:ss*

示例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

步骤 3　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。

server-port *port_number*

示例：

```
ciscoasa(config-aaa-server-host)# server-port 49
```

步骤 4　指定服务器密钥值，该密钥值用于面向 TACACS+ 服务器对 NAS 进行身份验证。

key

示例：

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

此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输的数据，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。

监控用于 AAA 的 TACACS+ 服务器

请参阅以下用于监控用于 AAA 的 TACACS+ 服务器的命令：

- **show aaa-server**

  此命令可显示已配置的 TACACS+ 服务器统计信息。输入 **clear aaa-server statistics** 命令可清除 TACACS+ 服务器统计信息。

- **show running-config aaa-server**

  此命令可显示 TACACS+ 服务器运行配置。输入 **clear configure aaa-server** 命令可清除 TACACS+ 服务器配置。

用于 AAA 的 TACACS+ 服务器历史记录

表 30-3　　用于 AAA 的 TACACS+ 服务器历史记录

功能名称	平台版本	说明
TACACS+ 服务器	7.0(1)	介绍如何配置用于 AAA 的 TACACS+ 服务器。 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**。



用于 AAA 的 LDAP 服务器

本章介绍如何配置 AAA 中使用的 LDAP 服务器。

- 关于 LDAP 和 ASA，第 31-1 页
- 用于 AAA 的 LDAP 服务器准则，第 31-4 页
- 配置用于 AAA 的 LDAP 服务器，第 31-4 页
- 监控用于 AAA 的 LDAP 服务器，第 31-10 页
- 用于 AAA 的 LDAP 服务器的历史记录，第 31-10 页

关于 LDAP 和 ASA

思科 ASA 与大多数 LDAPv3 目录服务器兼容，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，则可以手动对其进行配置。

如何使用 LDAP 进行身份验证

在身份验证过程中， ASA 将充当用户的 LDAP 服务器的客户端代理，并以明文形式或通过使用 SASL 协议对 LDAP 服务器执行身份验证。默认情况下，ASA 以明文形式将身份验证参数（通常是用户名和密码）传递到 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 使用从用户名和密码计算的 MD5 值来响应 LDAP 服务器。
- Kerberos - ASA 通过使用 GSSAPI Kerberos 机制发送用户名和领域来响应 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 将选择两者中较强的 Kerberos 机制。

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。

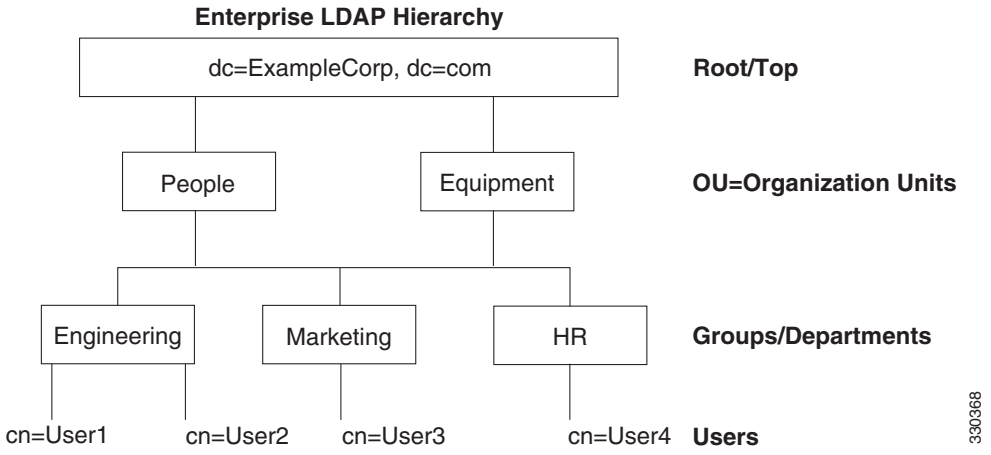
备注　有关 LDAP 协议的详细信息，请参阅 RFC 1777、 2251 和 2849。

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 的一名员工名为 Employee1。Employee1 在 Engineering 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 Engineering 部门的一名成员，该部门是一个称为 People 的组织单位的成员，而该组织单位本身是 Example Corporation 的成员。有关多级别层次结构的示例，请参阅下图。

多级别层次结构具有更多详细信息，但是，在单级别层次结构中搜索返回结果的速度更快。

图 31-1　　多级别 LDAP 层次结构



搜索 LDAP 层次结构

通过 ASA，可以在 LDAP 层次结构中定制搜索。在 ASA 上配置以下三个字段，以定义在 LDAP 层次结构中开始搜索的位置、搜索范围和查找的信息类型。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 定义服务器从 ASA 收到授权请求时应开始在 LDAP 层次结构中搜索用户信息的位置。
- Search Scope 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 下方的多个级别进行。您可以选择使服务器仅搜索其正下方的级别，否则，它可能搜索整个子树。单级别搜索速度更快，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。常用命名属性可以包括 cn （通用名称）、 sAMAccountName 和 userPrincipalName。

该图显示 Example Corporation 的样本 LDAP 层次结构。鉴于该层次结构，您能够以不同的方式定义搜索。下表显示两种样本搜索配置。

在第一个配置示例中，当 Employee1 使用所需的 LDAP 授权建立 IPsec 隧道时，ASA 将向 LDAP 服务器发送一个搜索请求，指明其应在 Engineering 组中搜索 Employee1。此搜索速度很快。

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 内搜索 Employee1。此搜索需要更长时间。

表 31-1　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	一个级别	cn=Employee1	搜索速度较快
2	dc=ExampleCorporation,dc=com	子树	cn=Employee1	搜索时间较长

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 可以使用权限较少的登录 DN 进行绑定。例如，登录 DN 可能是其 AD“Member Of”指定属于 Domain Users 的一部分的用户。对于 VPN 密码管理操作，登录 DN 需要提升的权限，而且必须是 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：

- 在端口 389 上使用未加密密码执行简单 LDAP 身份验证
- 在端口 636 上执行安全 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。

备注　作为 LDAP 客户端， ASA 不支持传输匿名绑定或请求。

LDAP 属性映射

ASA 可为以下选项使用 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），例如 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绑定到 LDAP 服务器或将其删除。您还可以显示或清除属性映射。

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，并且 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。

要正确使用属性映射功能，您需要了解 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 属性的名称及其经常映射到的用户定义的属性的类型包括：

- IETF-Radius-Class（ASA V8.2 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。组策略属性将 IETF-Radius-Class 属性替换为 ASDM V6.2/ASA V8.2 或更高版本。
- 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横幅。
- Tunneling-Protocols - 根据访问类型，允许或拒绝 VPN 远程访问会话。

注意　单一 LDAP 属性映射可以包含一个或多个属性。只能从特定 LDAP 服务器映射一个 LDAP 属性。

用于 AAA 的 LDAP 服务器准则

本节包含您在配置 AAA 的 LDAP 服务器之前应检查的准则和限制。

IPv6

AAA 服务器必须使用 IPv4 地址，但是终端可以使用 IPv6。

其他准则

- 在 ASA 上配置的用于访问 Sun 目录服务器的 DN 必须能够访问该服务器上的默认密码策略。建议使用目录管理员或具有目录管理员权限的用户作为 DN。或者，也可以将 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 V7.1.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。
- 在单模式下，最多可以有 100 个 LDAP 服务器组；在多模式下，每个情景可以有 4 个 LDAP 服务器组。
- 在单模式下，每组最多可以有 16 个 LDAP 服务器；在多模式下，每组可以有 4 个 LDAP 服务器。
- 当用户登录时，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（仅限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。

配置用于 AAA 的 LDAP 服务器

本节介绍如何配置用于 AAA 的 LDAP 服务器。

步骤 1　配置 LDAP 属性映射。请参阅配置 LDAP 属性映射，第 31-5 页。

步骤 2　添加 LDAP 服务器组。请参阅配置 LDAP 服务器组，第 31-6 页。

步骤 3　（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。请参阅使用 LDAP 为 VPN 配置授权，第 31-8 页。

配置 LDAP 属性映射

要配置 LDAP 属性映射，请执行以下步骤：

操作步骤

步骤 1　创建未填充的 LDAP 属性映射表。

ldap attribute-map *map-name*

示例：

```
ciscoasa(config)# ldap attribute-map att_map_1
```

步骤 2　将用户定义的属性名称部门映射到思科属性。

map-name *user-attribute-name Cisco-attribute-name*

示例：

```
ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class
```

步骤 3　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。

map-value *user-attribute-name Cisco-attribute-name*

示例：

```
ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1
```

步骤 4　确定服务器及其所属的 AAA 服务器组。

aaa-server *server_group* [*interface_name*] **host** *server_ip*

示例：

```
ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4
```

步骤 5　将属性映射绑定到 LDAP 服务器。

ldap-attribute-map *map-name*

示例：

```
ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1
```

示例

以下示例显示如何根据称为 accessType 的 LDAP 属性将管理会话限用于 ASA。accessType 属性可能具有下列值之一：

- VPN
- admin
- helpdesk

以下示例显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
```

以下示例说明如何显示思科 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

本节介绍如何配置 LDAP 服务器组。

准备工作

您必须先添加属性映射，然后才能向 LDAP 服务器组中添加 LDAP 服务器。

要创建和配置 LDAP 服务器组，然后向该组中添加 LDAP 服务器，请执行以下步骤：

操作步骤

步骤 1　确定服务器组名称和协议。

aaa-server *server_tag* **protocol ldap**

示例：

```
ciscoasa(config)# aaa-server servergroup1 protocol ldap
ciscoasa(config-aaa-server-group)#
```

输入 **aaa-server protocol** 命令时，会进入 AAA 服务器组配置模式。

步骤 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。

max-failed-attempts *number*

示例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

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 （仅限管理访问）配置了回退方法来配置回退机制，并且组中的所有服务器均无法响应，则将该组视为无响应，并会尝试回退方法。该服务器组仍然标记为 10 分钟 （默认值）内无响应，因此该时段内其他的 AAA 请求不会尝试联系该服务器组，而是会立即使用回退方法。如要将无响应时段从默认值改为其他值，请参阅下一步中的 **reactivation-mode** 命令。

如果没有回退方法， ASA 会继续重试该组中的服务器。

步骤 3　指定用于重新激活组中的已失败服务器的方法 （重新激活策略）。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

示例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

depletion 关键字仅在组中的所有服务器均处于非活动状态后，才重新激活已失败的服务器。

deadtime *minutes* 关键字-参数对指定介于 0 至 1440（以分钟为单位）之间的时长，该时长是禁用组中的最后一台服务器到随后重新启用所有服务器之间会经过的一段时间。默认值为 10 分钟。

timed 关键字在 30 秒的停止运行时间之后，重新激活已失败的服务器。

步骤 4　识别 LDAP 服务器以及其所属的 AAA 服务器组。

aaa-server *server_group* [*interface_name*] **host** *server_ip*

示例：

```
ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1
```

输入 **aaa-server host** 命令时，将会进入 AAA 服务器主机配置模式。根据需要，请使用主机配置模式命令进一步配置 AAA 服务器。

下表列出了可用于 LDAP 服务器的命令，以及新的 LDAP 服务器定义是否具有该命令的默认值。如果未提供默认值 （以 “-” 表示），请使用命令指定该值。

表 31-2　　主机模式命令和默认值

命令	默认值	描述
ldap-attribute-map	-	-
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 还是明文，都可以通过 SSL 来保护 ASA 与 LDAP 服务器之间的通信。如果未配置 SASL，则强烈建议通过 SSL 来保护 LDAP 通信。
ldap-scope	-	-
sasl-mechanism	-	-
server-port	389	-
server-type	autodiscovery	如果自动检测无法确定 LDAP 服务器类型，并且您知道服务器是 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 服务器组并向该组中添加 LDAP 服务器。由于示例未定义重试间隔或 LDAP 服务器侦听的端口，因此 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)#
```

使用 LDAP 为 VPN 配置授权

在 VPN 访问的 LDAP 用户身份验证成功后，ASA 将查询 LDAP 服务器，这会返回 LDAP 属性。这些属性通常包括应用到 VPN 会话的授权数据。以这种方式使用 LDAP 可一步完成身份验证和授权。

但是，有些情况下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。对于这种情况下的用户授权，您可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。

如要使用 LDAP 设置 VPN 用户授权，请执行以下步骤。

操作步骤

步骤 1　创建一个名为 remotegrp 的 IPsec 远程访问隧道组。

tunnel-group *groupname*

示例：

```
ciscoasa(config)# tunnel-group remotegrp
```

步骤 2　将服务器组和隧道组关联。

tunnel-group *groupname* **general-attributes**

示例：

```
ciscoasa(config)# tunnel-group remotegrp general-attributes
```

步骤 3　将新隧道组分配到先前创建的 AAA 服务器组以进行授权。

authorization-server-group *group-tag*

示例：

```
ciscoasa(config-general)# authorization-server-group ldap_dir_1
```

示例

虽然有可用于特定要求的其他授权相关命令和选项，但以下示例说明用于使用 LDAP 进行用户授权的命令。然后，该示例将创建一个名为 remote-1 的 IPsec 远程访问隧道组，将新隧道组分配到先前创建的 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)#
```

在完成此配置工作后，接着您可以通过输入以下命令，配置其他的 LDAP 授权参数，如目录密码、搜索目录的起点和目录搜索的范围：

```
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)#
```

监控用于 AAA 的 LDAP 服务器

有关监控用于 AAA 的 LDAP 服务器的信息，请参阅以下命令：

- **show aaa-server**

  此命令显示已配置的 AAA 服务器统计信息。使用 **clear aaa server statistics** 命令清除 AAA 服务器配置。

- **show running-config aaa-server**

  此命令可显示 AAA 服务器运行配置。使用 **clear configure aaa-server** 命令清除 AAA 服务器统计信息。

用于 AAA 的 LDAP 服务器的历史记录

表 31-3　　AAA 服务器的历史记录

功能名称	平台版本	说明
用于 AAA 的 LDAP 服务器	7.0(1)	LDAP 服务器介绍对 AAA 的支持以及如何配置 LDAP 服务器。 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**。



第 7 部分

系统管理



第 32 章

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。

- 管理访问规定，第 32-1 页
- ASDM 授权和从证书提取用户名，第 32-3 页
- 配置 ASDM、 Telnet 或 SSH 的 ASA 访问，第 32-4 页
- 为系统管理员配置 AAA，第 32-9 页
- 管理访问的历史记录，第 32-25 页

管理访问规定

本节介绍配置管理访问之前应该检查的规定和限制。

型号规定

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。

VPN 规定

备注 对于下面的配置， 192.168.10.0/24 是 AnyConnect 或 IPsec VPN 客户端的 VPN 池。每个配置都允许 VPN 客户端用户使用管理接口 IP 地址连接到与 ASA 之间的 ASDM 或 SSH 连接。

- 如要只允许 VPN 客户端用户访问 ASDM 或 HTTP（而拒绝所有其他用户的访问），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
```

- 如要只允许 VPN 客户端用户使用 SSH 访问 ASA （而拒绝所有其他用户的访问），请输入以下命令：

```
ciscoasa(config)# ssh 192.168.10.0 255.255.255.0 management_interface
```

- 只能定义一个管理访问接口。

其他规定

- 如要访问 ASA 接口进行管理访问，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。
- 除非使用 VPN 隧道中的 Telnet，否则无法使用 Telnet 访问最低安全级别的接口。
- 除了进入 ASA 时所经由的接口以外，不支持对其他接口进行管理访问。例如，如果管理主机位于外部接口上，则只能直接向外部接口发起管理连接。此规则的唯一例外是通过 VPN 连接。
- 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 实例，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 密码。
- 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。如要使用 SSH，必须使用 **aaa authentication ssh console LOCAL** 命令配置 AAA 身份验证；然后输入 **username** 命令定义本地用户。如果要使用 AAA 服务器而不是本地数据库进行身份验证，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）已删除默认 Telnet 登录密码；使用 Telnet 前必须手动设置密码。
- 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。
- 如果配置 Telnet 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。
- 启动 SSH 会话时，ASA 控制台中将显示一个圆点 (.)，然后显示以下 SSH 用户身份验证提示符：

  ```
  ciscoasa(config)#.
  ```

  显示此圆点不会影响 SSH 的功能。在进行用户身份验证之前的 SSH 密钥交换过程中生成服务器密钥或使用私有密钥解密消息时，控制台中将显示此圆点。完成这些任务可能需要两分钟或更长的时间。圆点是证实 ASA 繁忙和未暂停的进度指示器。或者，您也可以配置公共密钥而不使用密码。
- 如果无法建立到 ASA 接口的 Telnet 或 SSH 连接，请确保已根据本章中的说明启用与 ASA 的 Telnet 或 SSH。
- 从安全角度来看，横幅必须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。以下横幅设置了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。
- 在添加横幅后，如果有以下情况，可能会关闭至 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。
- 有关横幅消息的规定，请参阅 RFC 2196。

相关主题

- 设置主机名、域名及启用密码和 Telnet 密码，第 16-1 页
- 向本地数据库添加用户帐户，第 28-4 页

ASDM 授权和从证书提取用户名

在此版本之前，ASA 支持仅证书身份验证、使用在 ASDM 客户端中输入的用户名和密码的 AAA 身份验证，以及在建立 ASDM 连接的情况下的证书和 AAA 身份验证。

在此版本中，由于增加了 ASDM 授权和从证书提取用户名功能，现在支持：

- 使用来自证书的用户名的证书身份验证以及用户授权
- 使用用户提供的用户名的 AAA 身份验证以及用户授权
- 使用用户提供的用户名的证书身份验证和 AAA 身份验证以及用户授权
- 使用来自证书的用户名的具有预填充用户名的证书身份验证和 AAA 身份验证
- 使用来自证书的用户名的具有预填充用户名的证书身份验证和 AAA 身份验证以及使用同一用户名的用户授权

设置从证书提取用户名的规则

管理员可以配置从证书提取用户名的规则，并选择指定是否将从证书提取的用户名用于身份验证并在向用户显示的表单中预填充该用户名 （预填充用户名）。

```
http username-from-certificate {<primary-attr\> [<secondary-attr\>] |use-entire-name
|use-script} [pre-fill-username]
```

- primary-attr 指定要用于派生用户名的属性。 secondary-attr （可选）指定要与主要属性配合用于派生用户名的其他属性。
- 如果设置了可选的 “pre-fill-username”属性，则启用此名称用于身份验证。此用户名启用后，将连同用户输入的密码一起用于身份验证。在 ASDM 侧，如果用户名与用户最初输入的用户名不同，则会向用户显示一个新的弹出窗口，其中包含预填充的用户名。用户可以输入密码进行身份验证。

备注　**http username-from-certificate** 命令不适用于透明防火墙模式和多情景模式，也不适用于不支持 webvpn (ASA 1000v) 的平台和启用了无负载加密 (NPE) 的平台。

执行 HTTP 授权

现在，您可以配置与 LOCAL 服务器或身份验证服务器之间的所有用于授权的管理会话 （Telnet、SSH 和 HTTP）。此功能配置后，还会执行服务类型检查并根据该值授予用户完全访问权限、部分访问权限或无访问权限。

```
aaa authorization exec LOCAL| authentication-server [auto-enable]
```

在此版本中， HTTP 有自己的 CLI 命令，而且上述命令还适用于其他管理会话。 HTTP 命令为：

```
aaa authorization http console LOCAL|<aaa-server-group\>
```

此 CLI 命令可以指定授权服务器组，确保其类型是支持授权的类型。当前支持的类型包括 RADIUS、TACACS+ 和 LDAP。此外，还允许使用 LOCAL 服务器。如果升级时删除了配置中的旧命令，该命令会自动转换为新命令。

备注　同样，**aaa authorization http console** 命令既不适用于透明防火墙模式和多情景模式，也不适用于不支持 webvpn (ASA 1000v) 的平台和启用了无负载加密 (NPE) 的平台。

配置 ASDM、 Telnet 或 SSH 的 ASA 访问

本节介绍如何配置 ASDM、 Telnet 或 SSH 的 ASA 访问。

配置 Telnet 访问

如要确定允许使用 Telnet 连接至 ASA 的客户端 IP 地址，请执行以下步骤：

操作步骤

步骤 1　确定 ASA 从其接受每个地址或子网的连接的 IP 地址。

telnet *source_IP_address mask source_interface*

示例：

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

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　设置在 ASA 断开 Telnet 会话之前，会话可空闲的持续时间。

telnet timeout *minutes*

示例：

```
ciscoasa(config)# telnet timeout 30
```

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
```

配置 SSH 访问

如要确定客户端 IP 地址并定义允许使用 SSH 连接至 ASA 的用户，请执行以下步骤：

操作步骤

步骤 1　生成 SSH 必需的 RSA 密钥对 （仅适用于物理 ASA）。

crypto key generate rsa modulus *modulus_size*

示例：

```
ciscoasa(config)# crypto key generate rsa modulus 1024
```

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　将 RSA 密钥保存到永久性闪存中。

write memory

示例：

```
ciscoasa(config)# write memory
```

步骤 3　为 SSH 访问启用本地身份验证。或者，也可以配置使用 AAA 服务器的身份验证。

aaa authentication ssh console LOCAL

示例：

```
ciscoasa(config)# aaa authentication ssh console LOCAL
```

步骤 4　在本地数据库中创建可用于 SSH 访问的用户。

username *username* **password** *password*

示例：

```
ciscoasa(config)# username user1 password cisco123
```

步骤 5　确定 ASA 从其接受每个地址或子网的连接的 IP 地址，以及可在其上使用 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。

ssh *source_IP_address mask source_interface*

示例：

```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

步骤 6　（可选）设置在 ASA 断开 SSH 会话之前，会话可空闲的持续时间。

ssh timeout *minutes*

示例：

```
ciscoasa(config)# ssh timeout 30
```

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　（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。

ssh version *version_number*

示例：

```
ciscoasa(config)# ssh version 2
```

示例

以下示例显示如何生成 RAS 密钥并使内部接口上地址为 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 \qusername\q 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
```

为 ASDM

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。

如要为 ASDM 配置 HTTPS 访问，请执行以下步骤：

操作步骤

步骤 1　确定 ASA 从其接受每个地址或子网的 HTTPS 连接的 IP 地址。

http *source_IP_address mask source_interface*

示例：

```
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

步骤 2　启用 HTTPS 服务器。

http server enable [*port*]

示例：

```
ciscoasa(config)# http server enable 443
```

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　（可选）将 HTTP 请求重定向至 HTTPS 请求，使用户可以在 ASDM URL 中输入 “http://” 进入 HTTPS URL 而不会出现错误。

http redirect *interface* [*port*]

示例：

```
ciscoasa(config)# http redirect inside
```

示例

以下示例显示如何启用 HTTPS 服务器并使内部接口上地址为 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。

如要配置登录横幅，请执行以下步骤：

操作步骤

步骤 1　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**)。

banner {**exec** | **login** | **motd**} *text*

示例：

```
ciscoasa(config)# banner motd Welcome to $(hostname).
```

当用户连接至 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。

如要添加多行，请将 **banner** 命令放在每行之前。

对于横幅文本：

- 允许包含空格，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。在多情景模式下，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	（单情景和多情景模式）显示集群设备名称。集群中的每台设备都有一个唯一的名称。
context	（仅多情景模式）显示当前情景的名称。
domain	显示域名。
hostname	显示主机名。

priority	显示故障切换优先级 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** - 故障切换已启用，并且设备正在主动传输流量。 • **stby** - 故障切换已启用，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** - 故障切换未启用，并且设备正在主动传输流量。 • **stbyNoFailover** - 故障切换未启用，并且设备没有传输流量。当备用设备上存在高于阈值的接口故障时，就可能出现这种情况。 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。

如要自定义 CLI 提示符，请执行以下步骤：

操作步骤

步骤 1　通过输入以下命令自定义 CLI 提示符：

prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]}

示例：

```
ciscoasa(config)# firewall transparent
```

更改控制台超时

控制台超时设置连接可保持处于特权 EXEC 模式下或配置模式下的时间；当达到超时时间后，会话将进入用户 EXEC 模式。默认情况下，会话不会超时。此设置不会影响可与控制台端口保持连接的时间，该连接永不超时。

如要更改控制台超时，请执行以下步骤：

操作步骤

步骤 1　指定空闲时间 （以分钟为单位，范围为 0 到 60 分钟），超过此时间后特权会话将结束。默认超时时间为 0，表示会话不会超时。

console timeout *number*

示例：

```
ciscoasa(config)# console timeout 0
```

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，则可以将该接口标识为管理访问接口。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 连接到内部接口；或者，当从外部接口进入时，可以 ping 内部接口。通过以下类型的 VPN 隧道可以实现管理访问：IPsec 客户端、 IPsec 站点到站点和 AnyConnect SSL VPN 客户端。

如要配置管理接口，请执行以下步骤：

操作步骤

步骤 1　指定从另一个接口进入 ASA 时要访问的管理接口的名称。

management-access *management_interface*

示例：

```
ciscoasa(config)# management-access inside
```

为系统管理员配置 AAA

本节介绍如何为系统管理员启用身份验证和命令授权。

有身份验证和无身份验证的 CLI 访问

如何登录 ASA 取决于是否启用身份验证：

- No Authentication - 如果不对 Telnet 启用任何身份验证，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）。您将进入用户 EXEC 模式。
- Authentication - 如果根据此节启用 Telnet 或 SSH 身份验证，请输入在 AAA 服务器或本地用户数据库中所定义的用户名和密码。您将进入用户 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 enable 身份验证，则在输入 **enable** 命令时输入系统使能口令（使用 **enable password** 命令设置）。但是，如果不使用 enable 身份验证，则在输入 **enable** 命令后不再以特定用户身份登录。为了保留用户名，请使用 enable 身份验证。
- Authentication - 如果配置 enable 身份验证 （请参阅配置访问特权 EXEC 模式的身份验证，第 32-13 页）， 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 enable 身份验证，可以使用 **login** 命令而非 **enable** 命令。 **login** 保留用户名，但不需要配置开启身份验证。

有身份验证和无身份验证的 ASDM 访问

默认情况下，可以使用空的用户名和通过 **enable password** 命令设置的使能口令登录到 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使能口令来使用 ASDM。

从交换机到 ASA 服务模块的会话

对于从交换机到 ASASM 的会话（使用 **session** 命令），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），可以配置串行端口身份验证。

在多情景模式下，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。在此情况下，使用管理员情景 AAA 服务器或本地用户数据库。

支持的命令授权方法

可以使用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）用户进行 CLI 访问的身份验证时， ASA 会将该用户置于本地数据库、 RADIUS 或 LDAP 服务器所定义的权限级别中。用户可以访问分配的权限级别及以下级别的命令。请注意，所有用户首次登录时都会进入用户 EXEC 模式（命令级别为 0 或 1）。用户需要使用 **enable** 命令再次进行身份验证才能进入特权 EXEC 模式 （命令级别为 2 或更高），或使用 **login** 命令登录 （仅限本地数据库）。

注意　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。相反，输入 **enable** 命令时，您要输入系统使能口令，而 ASA 会将您置于级别 15。然后，您可以为每个级别创建使能口令，这样当您输入 **enable** *n* （2 到 15）时， ASA 就会将您置于级别 *n*。除非启用本地命令授权，否则不使用这些级别。

- TACACS+ 服务器权限级别 - 在 TACACS+ 服务器上，配置用户或组在进行 CLI 访问的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。

保留用户凭证

当用户登录到 ASA 时，该用户需要提供用于身份验证的用户名和密码。 ASA 会保留这些会话凭证，以防稍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。在特权模式下不会保留用户凭证。

- 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
用户名	是	否	否	是
密码	是	否	否	是
特权模式密码	否	否	是	否

安全情景和命令授权

以下是在多个安全情境中实施命令授权时要考虑的重点：

- 每个情景的 AAA 设置相互独立，不同情景之间不会共享这些设置。

  配置命令授权时，必须分别配置每个安全情景。此配置能够实现对不同安全情境执行不同的命令授权。

  当在安全情景之间切换时，管理员应知道登录时指定的用户名允许的命令在新情景会话中可能不同，或在新情景中可能根本未配置该命令授权。如果不知道安全情境之间的命令授权可能不同，则会使管理员感到困惑。下一点会让此行为更为复杂。

- 无论在前一个情景会话中使用哪个用户名，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，或对 enable_15 用户的授权不同于对前一个情景会话中的用户的授权，则此行为可导致混乱。

  此行为也会影响命令记帐，命令记帐仅在可以准确将每个发出的命令与特定管理员关联时才有用。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，命令记帐记录可能不容易确定谁曾经以 enable_15 用户名登录系统。如果对每个情景使用不同的记帐服务器，则跟踪使用 enable_15 用户名的用户需要关联来自多台服务器的数据。

  在配置命令授权时，请考虑以下方面：

  - 有权使用 **changeto** 命令的管理员就有权在每个其他情景中使用允许 enable_15 用户使用的所有命令。
  - 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。

备注　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。

命令特权级别

默认情况下，以下命令会分配给 0 级权限。所有其他命令会分配给 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。

配置用于 CLI 和 ASDM 访问的身份验证

本节介绍如何配置用于 CLI、 ASDM 和 enable 命令访问的身份验证。

准备工作

- 配置 Telnet、 SSH 或 HTTP 访问。
- 必须配置 SSH 身份验证才能获取 SSH 访问；无默认用户名。

如要配置用于 CLI、 ASDM 和 enable 命令访问的身份验证，请执行以下步骤：

操作步骤

步骤 1　对用户进行管理访问的身份验证。

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
```

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。**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。

HTTP 管理身份验证不支持 AAA 服务器组的 SDI 协议。

如果将 AAA 服务器组用于身份验证，可将 ASA 配置为在 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）。建议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　配置从证书提取用户名的规则：

http username-from-certificate {<*primary-attr***\> [<***secondary-attr***\>] |use-entire-name |use-script} [pre-fill-username]**

示例：

```
ciscoasa(config)# http username-from-certificate CN pre-fill-username
```

除 **aaa authentication** 命令可用于 ASDM 之外，还可使用此命令。

- primary-attr 指定要用于派生用户名的属性。 secondary-attr （可选）指定要与主要属性配合用于派生用户名的其他属性。
- 如果设置了可选的 “pre-fill-username”属性，则可将此名称用于身份验证。此用户名启用后，将连同用户输入的密码一起用于身份验证。在 ASDM 侧，如果用户名与用户最初输入的用户名不同，则会向用户显示一个新的弹出窗口，其中包含预填充的用户名。用户可以输入密码进行身份验证。

在本示例中，会执行证书身份验证。来自证书字段的 CN 将用作用户名。

配置访问特权 EXEC 模式的身份验证

选择以下选项之一用于对用户进行身份验证：

如要使用 AAA 服务器或本地数据库对用户进行身份验证，请执行以下步骤：

操作步骤

步骤 1　输入以下命令：

aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]}

示例：

```
ciscoasa(config)# aaa authentication enable console LOCAL
```

系统提示用户输入用户名和密码。

如果将 AAA 服务器组用于身份验证，可将 ASA 配置为在 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）。建议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）。

如要以本地数据库中一位用户的身份登录，请执行以下步骤：

步骤 1　输入以下命令：

login

示例：

```
ciscoasa# login
```

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。

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，因此无需为每个人提供系统使能口令。如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。

注意　如果您将可以访问 CLI 但您不希望其进入特权 EXEC 模式的用户添加到本地数据库中，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将所有本地用户都设置为 1 级，这样就可以控制谁可以使用系统使能口令访问特权 EXEC 模式。

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。用户角色的区分可防止远程访问 VPN 和网络访问用户建立到 ASA 的管理连接。

备注　串行访问未包含在管理授权内，因此如果配置 **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。

操作步骤

步骤 1　选择以下选项之一：

如要启用对本地、RADIUS、LDAP（映射的）和 TACACS+ 用户的管理授权，请输入以下命令：

备注　您可以输入用于 HTTP 的单独的授权配置。

如要在 ASA 上配置与 LOCAL 服务器或身份验证服务器之间用于授权的 Telnet 和 SSH 管理会话，请使用以下命令：

```
ciscoasa(config)# aaa authorization exec {authentication-server | LOCAL} [auto-enable]
```

备注　您可以配置任何授权服务器并将授权和身份验证设置为独立工作或一起工作。

如要在 ASA 上配置与本地服务器或身份验证服务器之间用于授权的 HTTP 管理会话，请使用以下命令：

```
ciscoasa(config)# aaa authorization http console {authentication-server | LOCAL}
```

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 （映射的）用户

  当用户通过 LDAP 进行身份验证时，可将本地 LDAP 属性及其值映射到思科 ASA 属性来提供特定授权功能。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。

  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发送时，该属性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** 命令时访问 CLI，但是如果配置 **aaa authentication http console** 命令，则拒绝 ASDM 配置访问。允许 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）用户仍可对其远程访问会话进行身份验证并终止会话。所有其他服务类型（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， ASA 将生成系统日志消息 113021。此消息用于通知用户，尝试的登录因管理权限不正确而失败。

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 service-type 和 privilege-level。

```
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 - 只允许访问 ASDM （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。
  - PASS, privilege level 2 和更高级别 - 允许在配置 **aaa authentication {telnet | ssh} console** 命令时访问 CLI，但是如果配置 **aaa authentication http console** 命令，则拒绝 ASDM 配置访问。允许 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。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）。

- 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。

为本地数据库用户配置密码策略

使用本地数据库配置用于 CLI 或 ASDM 访问的身份验证时，可以配置密码策略来要求用户在指定时间后更改密码并规定密码标准，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（例如用于网络访问的 VPN 或 AAA 流量），也不适用于通过 AAA 服务器进行身份验证的用户。

配置密码策略后，当您更改密码（自己本人的或其他用户的密码）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。

准备工作

- 配置CLI/ASDM 并启用身份验证。
- 指定本地数据库。

操作步骤

步骤 1　（可选）设置远程用户（SSH、 Telnet、 HTTP）密码到期前的间隔（以天为单位）。

password-policy lifetime *days*

示例：

```
ciscoasa(config)# password-policy lifetime 180
```

注意　控制台端口的用户不会由于密码到期而锁定。

有效值为 0 到 65536 天。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，请执行以下操作之一：

- 让另一位管理员使用 **username** 命令更改您的密码。
- 登录到物理控制台端口更改密码。

步骤 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。

password-policy minimum-changes *value*

示例：

```
ciscoasa(config)# password-policy minimum-changes 2
```

有效值为 0 到 64 个字符。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　（可选）设置密码最小长度。

password-policy minimum-length *value*

示例：

```
ciscoasa(config)# password-policy minimum-length 8
```

有效值为 3 到 64 个字符。建议最小密码长度为 8 个字符。

步骤 4　（可选）设置密码必须具有的最小大写字符数。

password-policy minimum-uppercase *value*

示例：

```
ciscoasa(config)# password-policy minimum-uppercase 3
```

有效值为 0 到 64 个字符。默认值为 0，表示无最小数。

步骤 5　（可选）设置密码必须具有的最小小写字符数。

password-policy minimum-lowercase *value*

示例：

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

有效值为 0 到 64 个字符。默认值为 0，表示无最小数。

步骤 6　（可选）设置密码必须具有的最小数字字符数。

password-policy minimum-numeric *value*

示例：

```
ciscoasa(config)# password-policy minimum-numeric 1
```

有效值为 0 到 64 个字符。默认值为 0，表示无最小数。

步骤 7　（可选）设置密码必须具有的最小特殊字符数。

password-policy minimum-special *value*

示例：

```
ciscoasa(config)# password-policy minimum-special 2
```

有效值为 0 到 64 个字符。特殊字符包括以下字符：!, @, #, $, %, ^, &, *, \q(‘ and ‘)’。默认值为 0，表示无最小数。

步骤 8　（可选）设置是否要求用户必须使用 **change-password** 命令更改密码，而不让用户使用 **username** 命令更改密码。

password-policy authenticate enable

示例：

```
ciscoasa(config)# password-policy authenticate enable
```

默认设置为禁用：用户可以使用其中任一种方法更改密码。

如果启用此功能并尝试使用 **username** 命令更改密码，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
```

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了密码有效期，则需要在旧密码到期时将用户名密码更改为新密码。如果启用密码策略身份验证，则要求用此密码更改方法。如果未启用密码策略身份验证，则既可以使用此方法也可以直接更改用户帐户。

如要更改用户名密码，请执行以下步骤：

操作步骤

步骤 1　输入以下命令：

change-password [**old-password** *old_password* [**new-password** *new_password*]]

示例：

```
ciscoasa# change-password old-password j0hncr1chton new-password a3rynsun
```

如果未在命令中输入旧密码和新密码， 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，在其中确定可供用户使用的命令。默认情况下，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。输入 **enable** 命令时（或在使用本地数据库时输入 **login** 命令时），可以进入特权 EXEC 模式并访问高级命令（包括配置命令）。

可以使用两种命令授权方法之一：

- 本地权限级别
- TACACS+ 服务器权限级别

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，每个用户可以输入分配的权限级别或以下级别的任何命令。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。

如要配置本地命令授权，请执行以下步骤：

操作步骤

步骤 1　将命令分配到权限级别。

privilege [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** *command*

示例：

```
ciscoasa(config)# privilege show level 5 command filter
```

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** - 通过这些可选关键字，可以仅仅针对命令的显示、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，要么更改为未修改的命令 （无 **show** 或 **clear** 前缀），要么更改为 **no** 形式。如果不使用其中一个关键字，则会影响命令的所有形式。
- **level** *level* - 介于 0 到 15 之间的级别。

- **mode {enable | configure}** - 如果某个命令可以在用户 EXEC 模式或特权 EXEC 模式下以及配置模式下输入，并且该命令在每个模式下执行不同的操作，则可以分别设置其在这些模式下的权限级别：
  - **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* - 将要配置的命令。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，但不能单独配置 **aaa authentication** 命令和 **aaa authorization** 命令的级别。

步骤 2　支持来自 RADIUS 的管理用户权限级别，并对进行管理访问身份验证的用户实施用户特定的访问级别。

aaa authorization exec authentication-server

示例：

```
ciscoasa(config)# aaa authorization exec authentication-server
```

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。

此命令还启用对本地、 RADIUS、 LDAP （映射的）和 TACACS+ 用户的管理授权。

使用 **aaa authorization exec LOCAL** 命令启用要从本地数据库获取的属性。

步骤 3　允许使用本地命令权限级别，可将其与本地数据库、RADIUS 服务器或 LDAP 服务器（具有映射的属性）中的用户权限级别进行核对。

aaa authorization command LOCAL

示例：

```
ciscoasa(config)# aaa authorization command LOCAL
```

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** （以 **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 filter 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。必须在用户 EXEC 模式下输入 **enable** 命令，而可在配置模式下访问的 **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** 关键字的另一个命令：**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
```

备注　最后一行用于 **configure terminal** 命令。

在 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，请参阅服务器文档了解有关命令授权支持的详细信息。

请参阅以下在思科安全 ACS 3.1 版本中配置命令的原则；其中许多原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。

注意　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，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**。

- 通过选中 **Permit Unmatched Args** 复选框，可以允许未明确拒绝的所有命令参数。

  例如，您可以仅配置 **show** 命令，那么将允许所有 **show** 命令。建议使用此方法，这样您就无需预测命令的每个变体 （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，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，这样仍能允许单独使用的 **enable**。

- 当您在命令行中缩写命令时， ASA 会将前缀和主命令扩展为全文，但对附加的参数却按照您输入的原样发送到 TACACS+ 服务器。

  例如，如果您输入 **sh log**，那么 ASA 会将整个 **show logging** 命令发送到 TACACS+ 服务器。但是，如果您输入 **sh log mess**，那么 ASA 会将 **show logging mess** 发送到 TACACS+ 服务器，而不是发送扩展后的 **show logging message** 命令。您可以配置同一个参数的多种拼法以便预测其缩写。

- 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 上输入命令， ASA 会将命令和用户名发送到 TACACS+ 服务器以确定命令是否已授权。

在启用 TACACS+ 命令授权之前，请务必以 TACACS+ 服务器上定义的用户身份登录 ASA，并确保您具有必要的命令授权来继续配置 ASA。例如，您应该以获得所有命令授权的管理员用户身份登录。否则，可能会意外锁定。

在您能肯定配置可以发挥所需作用之前，请勿保存配置。如果您因错误被锁定，通常可以通过重启 ASA 来恢复访问。如果仍然锁定，请参阅从锁定中恢复，第 32-23 页。

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您具有完全冗余的 TACACS+ 服务器系统和完全冗余的与 ASA 的连接性。例如，在您的 TACACS+ 服务器池中包括一个与接口 1 连接的服务器和另一个与接口 2 连接的服务器。您还可以将本地命令授权配置为在 TACACS+ 服务器不可用时的回退方法。在此情况下，您需要按照配置命令授权，第 32-18 页中列出的程序配置本地用户和命令权限级别。

如要使用 TACACS+ 服务器配置命令授权，请执行以下步骤：

操作步骤

步骤 1　输入以下命令：

aaa authorization command *tacacs+_server_group* [**LOCAL**]

示例：

```
ciscoasa(config)# aaa authorization command group_1 LOCAL
```

您可以将 ASA 配置为在 TACACS+ 服务器不可用时使用本地数据库作为回退方法。如要启用回退，请指定 **LOCAL** 前面的服务器组名称 （**LOCAL** 区分大小写）。建议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和命令权限级别中配置用户。

配置管理访问记帐

在 CLI 中输入 **show** 命令之外的任何命令时，可以将记帐消息发送到 TACACS+ 记帐服务器。您可以配置在用户登录时、输入 **enable** 命令时或者发出命令时记帐。

对于命令记帐，只能使用 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：

操作步骤

步骤 1　输入以下命令：

aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag*

示例：

```
ciscoasa(config)# aaa accounting telnet console group_1
```

有效的服务器组协议是 RADIUS 和 TACACS+。

步骤 2　启用命令记帐。只有 TACACS+ 服务器支持命令记帐。

aaa accounting command [**privilege** *level*] *server-tag*

示例：

```
ciscoasa(config)# aaa accounting command privilege 15 group_1
```

privilege *level* 关键字-参数对是最低权限级别，*server-tag* 参数是 ASA 应该向其发送命令记帐消息的 TACACS+ 服务器组的名称。

设置管理会话配额

您可以规定在 ASA 上允许的并发 ASDM、 SSH 和 Telnet 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。如要防止系统锁定，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，请执行以下步骤：

操作步骤

步骤 1　输入以下命令：

quota management-session *number*

示例：

```
ciscoasa(config)# quota management-session 1000
```

输入此命令的 **no** 形式将配额值设置为 0，表示没有会话限制。有效值范围为 0 到 10000。

在 SSH 会话中交换密钥

Diffie-Hellman (DH) 密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥配合使用，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。

ASA 支持使用 DH 群 1 和群 14 密钥交换方法进行密钥交换。如果未指定 DH 群密钥交换方法，则使用 DH 群 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，请执行以下步骤：

步骤 1　输入以下命令：

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
```

key-exchange 关键字指定在交换密钥时将遵循并应使用 DH 群 1 或 DH 群 14 密钥交换方法。

group 关键字表示在交换密钥时将遵循并应使用 DH 群 1 密钥交换方法或 DH 群 14 密钥交换方法。

dh-group1 关键字表示在交换密钥时将遵循并应使用 DH 群 1 密钥交换方法。由于历史遗留原因，DH 群 2 称为 DH 群 1。

dh-group14 关键字表示在交换密钥时将遵循并应使用 DH 群 14 密钥交换方法。

sha-1 关键字表示应使用 SHA - 1 加密算法。

使用 **show running-config ssh key-exchange** 命令显示当前使用的 DH 群密钥交换方法。

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。

下表列出了常见锁定条件以及如何从中恢复：

表 32-1　　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。	从交换机连接会话到 ASA。您可以从系统执行空间更改为情景并添加用户。
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，这样您就不会在服务器关闭时被锁定。	1. 如果因 ASA 上的网络配置不正确而无法访问服务器，请从交换机连接会话到 ASA。您可以从系统执行空间更改为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，这样您就不会在服务器关闭时被锁定。

表 32-1　　CLI 身份验证和命令授权锁定场景 （续）

功能	锁定条件	说明	解决方法：单模	解决方法：多模
TACACS+ 命令授权	您以没有足够权限的用户身份或不存在的用户身份登录。	启用命令授权，但是随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+ 服务器但需要立即配置 ASA，则请登录维护分区并重置密码和 **aaa** 命令。	从交换机连接会话到 ASA。您可以从系统执行空间更改为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身份登录。	启用命令授权，但是随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。	从交换机连接会话到 ASA。您可以从系统执行空间更改为情景并更改用户级别。

有关监控 SNMP 的信息，请参阅以下命令。

- **show running-config all privilege all**

  此命令显示所有命令的权限级别。

- **show running-config privilege level** *level*

  此命令显示特定权限级别的命令。 *level* 参数是介于 0 到 15 之间的整数。

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

  此命令显示特定命令的权限级别。

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
```

- **show curpriv**

  此命令显示当前登录的用户。

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
```

下表介绍了 **show curpriv** 命令输出。

表 32-2　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

管理访问的历史记录

表 32-3　管理访问的历史记录

功能名称	平台版本	说明
管理访问	7.0(1)	引入了此功能。 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**。

表 32-3　　管理访问的历史记录 （续）

功能名称	平台版本	说明
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。如要使用 SSH，必须使用 **aaa authentication ssh console LOCAL** 命令 (CLI) 或 Configuration > Device Management > Users/AAA > AAA Access > Authentication (ASDM) 配置 AAA 身份验证；然后通过输入 **username** 命令 (CLI) 或依次选择 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，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)	使用本地数据库配置用于 CLI 或 ASDM 访问的身份验证时，可以配置密码策略来要求用户在指定时间后更改密码并规定密码标准，例如最短长度和更改后的最小字符数。 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)	对于与 ASA 的 SSH 连接，您可以基于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。 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。*
支持用于 SSH 密钥交换的 Diffie-Hellman 群 14	8.4(4.1)、9.1(2)	增加了对用于 SSH 密钥交换的 Diffie-Hellman 群 14 的支持 以前只支持群　1。 引入了以下命令：**ssh key-exchange**。
支持管理会话最大数量	8.4(4.1)、9.1(2)	您可以设置并发 ASDM、 SSH 和 Telnet 会话的最大数量。 引入了以下命令：**quota management-session**、 **show running-config quota management-session**、**show quota management-session**。
对于在多情景模式下的 ASASM，支持从交换机进行 Telnet 和虚拟控制台身份验证。	8.5(1)	虽然从多情景模式下的交换机连接至 ASASM 将连接至系统执行空间，但是可以在管理员情景中配置身份验证来监管这些连接。

表 32-3　　管理访问的历史记录 （续）

功能名称	平台版本	说明
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。 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只需输入一次自己的身份验证凭证即可进入特权 EXEC 模式。**auto-enable** 选项已添加到 **aaa authorization exec** 命令中。 修改了以下命令：**aaa authorization exec**。
来自证书配置 (DoD) 的 ASDM 用户名	9.4(1)	此功能引入了从证书提取用户名并结合使用用户提供的用户名来对用户授权的能力。 弃用了以下用于 HTTP 管理会话的命令：aaa authorization exec **备注**　aaa authorization exec 命令对于 Telnet 和 SSH 会话仍然有效。 添加了以下命令：aaa authorization http console、 http username-from-certificate。 添加了以下屏幕：修改了以下屏幕：



软件和配置

本章介绍如何管理思科 ASA 软件和配置。

- 升级软件，第 33-1 页
- 管理文件，第 33-10 页
- 设置 ASA 映像、 ASDM 和启动配置，第 33-18 页
- 使用 ROM 监控加载映像，第 33-19 页
- 备份和恢复配置或其他文件，第 33-22 页
- 降级软件，第 33-35 页
- 配置自动更新，第 33-37 页
- 软件和配置的历史记录，第 33-43 页

升级软件

本节介绍如何升级单个设备、故障切换设备或集群设备。

- 升级路径，第 33-1 页
- 查看当前版本，第 33-2 页
- 从 Cisco.com 下载软件，第 33-2 页
- 升级独立设备，第 33-2 页
- 升级故障转移对或 ASA 集群，第 33-4 页

升级路径

有关版本的升级路径，请参阅下表。某些版本需要过渡升级之后才能升级到最新版本。

注意：除以下例外情况，对故障转移和 ASA 集群的零停机时间升级没有特殊要求。ASA 集群从 9.0(1) 或 9.1(1) 进行升级：由于 CSCue72961，不支持无中断升级。

当前的 ASA 版本	首先升级到：	然后升级到：
8.2(x) 及更早版本	8.4(6)	9.4(1) 或更高版本
8.3(x)	8.4(6)	9.4(1) 或更高版本

当前的 ASA 版本	首先升级到：	然后升级到：
8.4(1) 至 8.4(4)	8.4(6)、 9.0(4) 或 9.1(2)	9.4(1) 或更高版本
8.4(5) 及更高版本	—	9.4(1) 或更高版本
8.5(1)	9.0(4) 或 9.1(2)	9.4(1) 或更高版本
8.6(1)	9.0(4) 或 9.1(2)	9.4(1) 或更高版本
9.0(1)	9.0(4) 或 9.1(2)	9.4(1) 或更高版本
9.0(2) 或更高版本	—	9.4(1) 或更高版本
9.1(1)	9.1(2)	9.4(1) 或更高版本
9.1(2) 或更高版本	—	9.4(1) 或更高版本
9.2(x)	—	9.4(1) 或更高版本
9.3(x)	—	9.4(1) 或更高版本

配置迁移

根据当前版本，您在升级过程中可能需要进行一次或多次配置迁移。例如，从 8.0 升级到 9.4 时，您将需要进行以下所有迁移：

- 8.2 — 请参阅 8.2 版本说明。
- 8.3 — 请参阅 *Cisco ASA 5500 升级到 8.3 版本的迁移指南*。
- 8.4 — 请参阅 8.4 版本升级指南。
- 9.0 — 请参阅 9.0 版本升级指南。

查看当前版本

请使用 **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

尽管其他服务器类型也受支持，但此操作步骤假设您将映像存放在 TFTP 服务器。

升级独立设备

本节介绍如何安装 ASDM 和操作系统 (OS) 映像。

此操作步骤使用 TFTP。对于 FTP 或 HTTP，请参阅 **copy** 命令。

操作步骤

1. （如果要进行配置迁移）将配置显示在终端上，以便您可以备份配置：

   ```
   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。

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/asa941-smp-k8.bin disk0:/asa941-smp-k8.bin
   ```

   对于 TFTP 以外的其他方法，请参阅 **copy** 命令。

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-741.bin disk0:/asdm-741.bin
   ```

4. 如果您当前未处于全局配置模式，请访问全局配置模式：

   configure terminal

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像 URL；如要将新映像指定为第一个映像，您必须根据 6. 和 7. 删除所有现有条目，并按所需的顺序输入映像 URL。

6. 请删除所有的现有启动映像配置，以便您能够输入首选的新启动映像：

   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
   ```

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://asa941-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执行此命令。例如，您可以重新输入之前在 6. 中删除的映像。

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-741.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。

9. 将新设置保存至启动配置：

   write memory

10. 重新加载 ASA：

    reload

升级故障转移对或 ASA 集群

要执行零停机时间升级，您需要按特定顺序升级每台设备。

- 升级主用/备用故障转移对，第 33-4 页
- 升级主用/主用故障转移对，第 33-6 页
- 升级 ASA 集群，第 33-8 页

升级主用/备用故障转移对

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

1. （如果要进行配置迁移）将配置显示在终端上，以便您可以备份配置：

   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。

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/asa941-smp-k8.bin disk0:/asa941-smp-k8.bin
   ```

   对于 TFTP 以外的其他方法，请参阅 **copy** 命令。

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/asa941-smp-k8.bin
   disk0:/asa941-smp-k8.bin
   ```

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-741.bin disk0:/asdm-741.bin
   ```

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-741.bin
   disk0:/asdm-741.bin
   ```

6. 如果您当前未处于全局配置模式，请访问全局配置模式：

   configure terminal

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:/asa931-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像 URL；如要将新映像指定为第一个映像，您必须根据 8. 和 9. 删除所有现有条目，并按所需的顺序输入映像 URL。

8. 请删除所有的现有启动映像配置，以便您能够输入首选的新启动映像：

   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:/asa931-smp-k8.bin
   ```

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://asa941-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执行此命令。例如，您可以重新输入之前在 8. 中删除的映像。

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-741.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。

11. 将新设置保存至启动配置：

    write memory

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** 命令验证备用设备是否处于 Standby Ready 状态。

13. 强行要求主用设备故障转移至备用设备：

    no failover active

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

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

1. （如果要进行配置迁移）将配置显示在终端上，以便您可以备份配置：

   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。

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/asa941-smp-k8.bin disk0:/asa941-smp-k8.bin
   ```

   对于 TFTP 以外的其他方法，请参阅 **copy** 命令。

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/asa941-smp-k8.bin
   disk0:/asa941-smp-k8.bin
   ```

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-741.bin disk0:/asdm-741.bin
   ```

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-741.bin
   disk0:/asdm-741.bin
   ```

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
   ```

7. 如果您当前未处于全局配置模式，请访问全局配置模式：

   ```
   configure terminal
   ```

   示例：

   ```
   primary(config)# configure terminal
   ```

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:/asa931-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像 URL；如要将新映像指定为第一个映像，您必须根据 9. 和 10. 删除所有现有条目，并按所需的顺序输入映像 URL。

9. 请删除所有的现有启动映像配置，以便您能够输入首选的新启动映像：

   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:/asa931-smp-k8.bin
   ```

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://asa941-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执行此命令。例如，您可以重新输入之前在 9. 中删除的映像。

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-741.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。

12. 将新设置保存至启动配置：

```
write memory
```

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。

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
```

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

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

1. （如果要进行配置迁移）备份配置文件：

```
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。

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/asa941-smp-k8.bin
disk0:/asa941-smp-k8.bin
```

对于 TFTP 以外的其他方法，请参阅 **copy** 命令。

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-741.bin disk0:/asdm-741.bin
```

4. 如果您当前未处于全局配置模式，请访问全局配置模式：

```
configure terminal
```

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:/asa931-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像 URL；如要将新映像指定为第一个映像，您必须根据 6. 和 7. 删除所有现有条目，并按所需的顺序输入映像 URL。

6. 请删除所有的现有启动映像配置，以便您能够输入首选的新启动映像：

   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:/asa931-smp-k8.bin
   ```

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://asa941-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执行此命令。例如，您可以重新输入之前在 6. 中删除的映像。

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-741.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。

9. 将新设置保存至启动配置：

   write memory

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。

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。

12. 重新加载主设备：

```
reload noconfirm
```

系统将进行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

- 查看闪存中的文件，第 33-10 页
- 从闪存中删除文件，第 33-11 页
- 清除闪存文件系统，第 33-11 页
- 配置文件访问，第 33-11 页
- 将文件复制到 ASA，第 33-15 页
- 将文件复制到启动配置或运行配置，第 33-17 页

查看闪存中的文件

您可以查看闪存中的文件，并参阅有关文件的信息。

操作步骤

步骤 1　查看闪存中的文件：

dir [**disk0:** | **disk1:**]

示例：

```
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
```

对于内部闪存，请输入 **disk0:**。**disk1:** 关键字表示外部闪存。默认为内部闪存。

步骤 2　查看有关特定文件的扩展信息：

show file information [path:/]*filename*

示例：

```
hostname# show file information cdisk.bin

disk0:/cdisk.bin:
  type is image (XXX) []
  file size is 4976640 bytes version 7.0(1)
```

所列的文件大小仅用作示例。

默认路径是内部闪存的根目录 (disk0:/)。

从闪存中删除文件

您可以从闪存中删除不再需要的文件。

操作步骤

步骤 1　从闪存中删除文件：

```
hostname# delete disk0: filename
```

默认情况下，如果未指定路径，将从当前工作目录中删除文件。删除文件时，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。

清除闪存文件系统

要清除闪存文件系统，请执行以下步骤：

操作步骤

步骤 1　根据访问 ASA 服务模块控制台，第 2-2 页或访问设备控制台，第 2-1 页中的说明连接到 ASA 控制台端口。

步骤 2　关闭 ASA，然后重新启动。

步骤 3　在启动过程中，当系统提示您进入 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清除文件系统，包括隐藏的系统文件。

```
rommon #1> erase [disk0: | disk1: | flash:]
```

配置文件访问

ASA 可以使用 FTP 客户端、安全复制客户端或 TFTP 客户端。您也可以将 ASA 配置为安全复制服务器，以便能够在您的计算机上使用安全复制客户端。

- 配置 FTP 客户端模式，第 33-12 页
- 将 ASA 配置为安全复制服务器，第 33-12 页
- 配置ASA TFTP 客户端路径，第 33-14 页

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 中，客户端同时启动控制连接和数据连接。服务器 （被动模式下数据连接的接收方）通过它用于侦听特定连接的端口号进行响应。

操作步骤

步骤 1　将 FTP 模式设置为被动：

ftp mode passive

示例：

```
ciscoasa(config)# ftp mode passive
```

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。只有经允许使用 SSH 访问 ASA 的客户端才能建立安全复制连接。

准备工作

- 服务器没有目录支持。缺少目录支持会限制远程客户端访问 ASA 内部文件。
- 服务器不支持横幅或通配符。
- 根据配置 SSH 访问，第 32-4 页在 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。
- 对于多情景模式，请在系统执行空间中完成本程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。

操作步骤

步骤 1　启用 SCP 服务器：

ssh scopy enable

步骤 2　（可选）禁用 SSH 主机密钥检查：

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]?
```

默认情况下，系统会启用此选项。当启用此选项时，如果 ASA 中尚未存储主机密钥，系统会提示您接受或拒绝主机密钥。当禁用此选项时，如果以前未存储主机密钥， ASA 会自动接受主机密钥。

步骤 3　（可选）在 ASA 数据库中手动添加或删除服务器及其密钥。

```
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 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如果需要，可以手动管理密钥。

对于每个服务器，可以指定 SSH 主机的 **key-string** （公钥）或 **key-hash** （散列值）。

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 对其进行散列处理。

key-hash{**md5** | **sha256**}*fingerprint* 可用于输入已经过散列处理的密钥（使用 MD5 或 SHA-256 密钥）；例如，您从 **show** 命令输出复制的密钥。

示例

从外部主机上的客户端执行 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**，则会提示您输入密码。

以下示例为 10.86.94.170 上的服务器添加经过散列处理的主机密钥：

```
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
```

以下示例为 10.7.8.9 上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 第 2 修订版对其进行了说明。您可以将 ASA 配置为 TFTP *客户端*，以便其可以将文件复制到 TFTP *服务器*，或者从中复制文件。这样，即可备份配置文件，并将其传播到多个 ASA。

按照本节所述可以预定义 TFTP 服务器的路径，从而无需在诸如 **copy** 和 **configure net** 等命令中输入该路径。

操作步骤

步骤 1　预定义用于 **configure net** 和 **copy** 命令的 TFTP 服务器地址和文件名。

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...
```

输入命令时，可以覆盖文件名；例如，当使用 **copy** 命令时，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:** 以使用 tftp-server 值而不是 **tftp://***url*。

相关主题

将文件复制到 ASA，第 33-15 页和备份和恢复配置或其他文件，第 33-22 页

将文件复制到 ASA

本节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。

准备工作

- 对于 IPS SSP 软件模块，在将 IPS 软件下载至 disk0 之前，请确保至少 50% 的闪存可用。当安装 IPS 时， IPS 会为其文件系统保留 50% 的内部闪存。
- 您不能在闪存中的同一目录下具有两个名称相同但字母大小写不同的文件。例如，如果尝试将文件 Config.cfg 下载至包含 config.cfg 文件的位置，则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 《*Cisco 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*》。
- 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，或者将其安装在外部闪存中），请参阅设置 ASA 映像、 ASDM 和启动配置，第 33-18 页。
- 对于多情景模式，您必须处于系统执行空间中。

操作步骤

步骤 1　使用以下服务器类型之一复制文件。

- 从 TFTP 服务器进行复制：

  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 FTP 服务器进行复制：

  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 HTTP(S) 服务器进行复制：

  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 SMB 服务器进行复制：

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 SCP 服务器进行复制：

  ;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**]
  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:a9:2
b: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:2d:bf:a9:2b
:85:2e:19


Password: <type in password>
!!!!!!
6006 bytes copied in 8.160 secs (750 bytes/sec)
```

将文件复制到启动配置或运行配置

您可以将文本文件从 TFTP、FTP、SMB、HTTP(S) 或 SCP 服务器或者从闪存下载至运行配置或启动配置。

准备工作

将配置复制到运行配置时，会合并这两个配置。合并会将新配置中的所有新命令添加到运行配置中。如果配置相同，则不会发生任何更改。如果命令冲突或命令影响情景的运行，则合并的影响取决于命令。可能会发生错误，也可能出现意外结果。

操作步骤

步骤 1　要将文件复制到启动配置或运行配置，请针对相应的下载服务器，输入以下命令之一：

- 从 TFTP 服务器进行复制：

  copy [**/noconfirm**] **tftp://***server*[**/***path*]**/***src_filename* {**startup-config** | **running-config**}

  示例：

  ```
  ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config
  ```

- 从 FTP 服务器进行复制：

  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 HTTP(S) 服务器进行复制：

  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 SMB 服务器进行复制：

  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 SCP 服务器进行复制：

  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
  ```

  ;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，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
```

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
```

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
```

相关主题

设置 ASA 映像、 ASDM 和启动配置，第 33-18 页

设置 ASA 映像、 ASDM 和启动配置

如果您有多个 ASA 或具有 ASDM 映像，则应指定要启动的映像。如果不设置映像，则会使用默认启动映像，并且该映像可能不是计划使用的映像。对于启动配置，可以随意指定配置文件。

请参阅以下默认设置：

- ASA Image：
  - Physical ASA - 启动 ASA 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，以从该映像启动。请注意，如果您随后清除配置 (**clear configure all**)，则 ASAv 将还原为加载原始部署映像。
- ASDM Image on All ASAs - 启动 ASA 在内部闪存中找到的第一个 ASDM 映像，或者，如果此位置不存在映像，则在外部闪存中查找。
- Startup Configuration - 默认情况下， ASA 从隐藏文件形式的启动配置启动。

操作步骤

步骤 1　设置 ASA 启动映像位置：

boot system *url*

示例：

```
ciscoasa(config)# boot system disk:/images/asa921.bin
```

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，以指定要按顺序从中启动的不同映像；ASA 将启动其成功找到的第一个映像。当输入 **boot system** 命令时，该命令会在列表的底部添加一个条目。要对启动条目重新排序，必须使用 **clear configure boot system** 命令删除所有条目，然后按所需顺序重新输入这些条目。只能配置一个 **boot system tftp** 命令，并且该命令必须是配置的第一个命令。

注意　如果 ASA 陷入不断启动的循环中，则可以将 ASA 重新引导至 ROMMON 模式下。有关 ROMMON 模式的详细信息，请参阅查看调试消息，第 35-1 页。

步骤 2　设置要启动的 ASDM 映像：

asdm image {**disk0:/** | **disk1:/**}[*path*/]*filename*

示例：

```
ciscoasa(config)# asdm image disk0:/images/asdm721.bin
```

如果不指定要启动的映像，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。为了避免自动更新 （如已配置）发生问题，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要启动的 ASDM 映像。

步骤 3　（可选）将启动配置设置为一个已知文件，而不是默认的隐藏文件。

boot config {**disk0:/** | **disk1:/**}[*path*/]*filename*

示例：

```
ciscoasa(config)# boot config disk0:/configs/startup1.cfg
```

使用 ROM 监控加载映像

您可以使用 ROM 监控加载新的映像。

- 使用 ROM 监控加载 ASA 5500-X 系列的映像，第 33-19 页
- 使用 ROM 监控加载 ASASM 的映像，第 33-21 页
- 恢复并加载 ASA 5506W-X 无线接入点的映像，第 33-22 页

使用 ROM 监控加载 ASA 5500-X 系列的映像

要使用 TFTP 从 ROM 监控将软件映像加载到 ASA，请执行以下步骤。

步骤 1　根据访问设备控制台，第 2-1 页中的说明连接到 ASA 控制台端口。

步骤 2　关闭 ASA，然后重新启动。

步骤 3　在启动过程中，当系统提示您进入 ROMMON 模式时，请按 **Escape** 键。

步骤 4　在 ROMMOM 模式下，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：

```
rommon #1> ADDRESS=10.132.44.177
rommon #2> SERVER=10.129.0.30
rommon #3> GATEWAY=10.132.44.1
rommon #4> IMAGE=tftp-home/asa941-smp-k9.bin
rommon #5> PORT=GigabitEthernet0/0
GigabitEthernet0/0
Link is UP
MAC Address: 0012.d949.15b8
```

注意　请确保已存在网络连接。

注意　**PORT** 命令在 ASA 5506-X、 ASA 5508-X 和 ASA 5516-X 型号上被忽略，您必须从管理 1/1 接口对这些平台执行 TFTP 恢复。

步骤 5　验证您的设置：

```
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　对 TFTP 服务器执行 ping 操作：

```
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　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　通过检查 ASA 中的版本，验证是否已将正确的软件映像加载到 ASA 中：

```
ciscoasa# show version
```

使用 ROM 监控加载 ASASM 的映像

要使用 TFTP 从 ROM 监控模式将软件映像加载到 ASASM，请执行以下步骤。

操作步骤

步骤 1　根据访问 ASA 服务模块控制台，第 2-2 页中的说明连接到 ASA 控制台端口。

步骤 2　确保重新加载 ASASM 映像。

步骤 3　在启动过程中，当系统提示您进入 ROMMON 模式时，请按 **Escape** 键。

步骤 4　在 ROMMOM 模式下，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=tftp-main/asa941-smp-k9.bin
rommon #5> PORT=Data0
rommon #6> VLAN=1
Data0
Link is UP
MAC Address: 0012.d949.15b8
```

注意　请确保已存在网络连接。

步骤 5　验证您的设置：

```
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　对 TFTP 服务器执行 ping 操作：

```
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　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。

注意　ROMMON 启动完成后，您必须单独将映像下载至系统闪存；如果将模块启动至 ROMMON 模式，则重新加载后不会保留系统映像。

步骤 8　通过检查 ASA 中的版本，验证是否已将正确的软件映像加载到 ASA 中：

```
ciscoasa# show version
```

恢复并加载 ASA 5506W-X 无线接入点的映像

要使用 TFTP 将软件映像恢复并加载到 ASA5506W-X，请执行以下步骤。

操作步骤

步骤 1　向接入点 (AP) 发起会话并进入 AP ROMMON （而不是 ASA ROMMON）模式：

```
ciscoasa# hw-module module wlan recover image
```

步骤 2　按照 《思科 Aironet 无线接入点的思科 IOS 软件配置指南》中的程序执行操作。

备份和恢复配置或其他文件

我们建议您对配置和其他系统文件进行定期备份以防止系统故障。

- 执行完整系统备份或恢复，第 33-23 页
- 备份单模式配置或多模式系统配置，第 33-26 页
- 备份闪存中的情景配置或其他文件，第 33-27 页
- 备份情景中的情景配置，第 33-28 页

- 从终端显示复制配置，第 33-29 页
- 使用导出和导入命令备份其他文件，第 33-29 页
- 使用脚本备份和恢复文件，第 33-29 页

执行完整系统备份或恢复

以下程序介绍如何将配置和映像备份至 tar.gz 文件并将该文件传输到本地计算机。

- 准备工作，第 33-23 页
- 备份系统，第 33-24 页
- 恢复备份，第 33-25 页

准备工作

- 在您启动备份或恢复之前，您在备份或恢复位置应至少有 300 MB 的可用磁盘空间。
- 如果您在备份期间或之后进行任何配置更改，则这些更改将不会包含在备份中。如果在进行备份后更改配置，然后执行恢复后的，则会覆盖此配置更改。因此， ASA 的行为可能不同。
- 一次只能启动一个备份或恢复。
- 只能将配置恢复到执行原始备份时的 ASA 版本。无法使用恢复工具将配置从一个 ASA 版本迁移到另一个版本。如果需要进行配置迁移，则 ASA 会在加载新的 ASA 操作系统时自动升级常驻启动配置。
- 如果使用集群，则只能备份或恢复启动配置、运行配置和身份证书。必须为每台设备单独创建和恢复备份。
- 如果使用故障切换，则必须为主用设备和备用设备单独创建和恢复备份。
- 如果您针对 ASA 设置主口令，则需要该主口令短语来恢复您使用此程序创建的备份配置。如果您不知道 ASA 的主口令，请参阅配置主密码，第 16-10 页，以了解在继续备份之前如何重置该口令。
- 如果导入 PKCS12 数据（使用 **crypto ca trustpoint** 命令）并且信任点使用 RSA 密钥，则会为导入的密钥对分配与信任点相同的名称。由于此限制，如果在恢复 ASDM 配置后为信任点及其密钥对指定其他名称，则启动配置将与原始配置相同，但运行配置将包含其他密钥对名称。这意味着，如果对密钥对和信任点使用不同的名称，则无法恢复原始配置。要解决此问题，请确保对信任点及其密钥对使用同一名称。
- 无法使用 CLI 进行备份及使用 ASDM 进行恢复，反之亦然。
- 每个备份文件包含以下内容：
  - 运行配置
  - 启动配置
  - 所有安全映像

    思科安全桌面和主机扫描映像

    思科安全桌面和主机扫描设置

    AnyConnect (SVC) 客户端映像和配置文件

    AnyConnect (SVC) 自定义和转换
  - 身份证书 （包括绑定到身份证书的 RSA 密钥对；独立密钥除外）
  - VPN 预共享密钥

- SSL VPN 配置
- 应用配置文件自定义框架 (APCF)
- 书签
- 自定义
- 动态访问策略 (DAP)
- 插件
- 连接配置文件的预填充脚本
- 代理自动配置
- 转换表
- Web 内容
- 版本信息

备份系统

本程序介绍如何执行完整系统备份。

操作步骤

步骤 1　备份系统：

backup [**/noconfirm**] [**context** *name*] [**passphrase** *value*] [**location** *path*]

示例：

```
ciscoasa# backup location disk0:/sample-backup]
Backup location [disk0:/sample-backup]?
```

在系统执行空间中的多情景模式下，输入 **context** 关键字以备份指定的情景文件。

在 VPN 证书和预共享密钥的备份期间，需要由 **passphrase** 关键字标识的密钥才可对证书进行编码。必须提供要用于编码和解码 PKCS12 格式的证书的口令。备份仅包含绑定到证书的 RSA 密钥对，不包括任何独立证书。

备份 **location** 可以是本地磁盘或远程 URL。如果不提供位置，则会使用以下默认名称：

- 单模式 - disk0:*hostname*.backup.*timestamp*.tar.gz
- 多模式 - disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz

步骤 2　按照提示操作：

示例：

```
ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]?

Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!

Enter a passphrase to encrypt identity certificates. The default is cisco. You will be
required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!
```

```
IMPORTANT: This device uses master passphrase encryption. If this backup file is used to
restore to a device with a different master passphrase, you will need to provide the
current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

恢复备份

您可以指定要在您的本地计算机上从 zip 备份 tar.gz 文件恢复的配置和映像。

操作步骤

步骤 1　从备份文件恢复系统。

restore [**/noconfirm**] [**context** *name*] [**passphrase** *value*] [**location** *path*]

示例：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
```

步骤 2　按照提示操作：

示例：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?

Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version, some
configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption. Master passphrase
is required to restore running configuration, startup configuration and VPN pre-shared
keys.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
```

```
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to this
device, please note them for future reference.

ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside, the IP
is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside, the IP
is already used as media-termination address on interface inside.
WARNING: PAC settings will override http- and https-proxy configurations. Do not overwrite
configuration file if you want to preserve the old http- and https-proxy configurations.

Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates. The default is
cisco. If the passphrase is not correct, certificates will not be restored.

No passphrase was provided for identity certificates. Using the default value: cisco. If
the passphrase is not correct, certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

备份单模式配置或多模式系统配置

在单情景模式下或从多模式下的系统配置中，可以将启动配置或运行配置复制到外部服务器或本地闪存。

操作步骤

步骤 1　使用以下服务器类型之一来备份配置：

- 复制到 TFTP 服务器：

  copy [**/noconfirm**] {**startup-config** | **running-config**} **tftp://***server*[**/***path*]**/***dst_filename*

  示例：

  ```
  ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg
  ```

- 复制到 FTP 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
  ```

- 复制到 SMB 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
  ```

- 复制到 SCP 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
  ```

  ;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。

- 复制到本地闪存：

  copy [**/noconfirm**] {**startup-config** | **running-config**} {**disk0**|**disk1**}**:/**[*path/*]*dst_filename*

  示例：

  ```
  ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg
  ```

  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命令之一来复制本地闪存中的情景配置或其他文件。

操作步骤

步骤 1　使用以下服务器类型之一备份情景配置：

- 从闪存复制到 TFTP 服务器：

  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
  ```

- 从闪存复制到 FTP 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
```

- 从闪存复制到 SMB 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
  ```

- 从闪存复制到 SCP 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
  ```

  ;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。

- 从闪存复制到本地闪存：

  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
  ```

  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

在多情景模式下，您可以从情景中执行以下备份操作：

操作步骤

步骤 1　将运行配置复制到已连接至情景网络的启动配置服务器：

```
ciscoasa/contexta# copy running-config startup-config
```

步骤 2　将运行配置复制到已连接至情景网络的 TFTP 服务器：

```
ciscoasa/contexta# copy running-config tftp:/server[/path]/filename
```

从终端显示复制配置

操作步骤

步骤 1　将配置列显到终端：

```
ciscoasa# show running-config
```

步骤 2　请复制此命令的输出，然后将配置粘贴到文本文件。

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。

通过 CLI 可以使用 **export** 和 **import** 命令备份和恢复配置的各个元素。

要备份这些文件 （例如，使用 **import webvpn** 命令导入的那些文件或证书），请执行以下步骤：

操作步骤

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　对于要备份的文件，请运行 **export** 命令 （在本示例中为 rdp 文件）：

```
ciscoasa # export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

使用脚本备份和恢复文件

您可以使用脚本来备份和恢复 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，我们不建议对数字密钥和证书或者本地 CA 密钥执行自动备份。

本部分对此操作提供说明，并包含您可以按原样使用或根据环境要求修改后使用的样本脚本。此样本脚本特定于 Linux 系统。要将其用于 Microsoft Windows 系统，需要运用此样本的逻辑对其进行修改。

备注　或者，可以使用 **backup** 和 **restore** 命令。有关详情，请参见执行完整系统备份或恢复，第 33-23 页。

- 准备工作，第 33-30 页
- 运行脚本，第 33-30 页
- 样本脚本，第 33-30 页

准备工作

要使用脚本来备份和恢复 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，以将文件从 ASA 发送到备份站点。

另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

要运行备份和恢复脚本，请执行以下步骤：

操作步骤

步骤 1　将脚本文件下载或剪切并粘贴到系统上的任意位置。

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，可以在输入 **Perl** *scriptname* 命令时，在按 **Enter** 键之前输入选项的值。无论采用哪种方式，脚本都要求输入每个选项的值。

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 记录。您可以在日后恢复时使用这些 CLI，这在您希望仅恢复一两个文件时特别有用。

样本脚本

```
#!/usr/bin/perl
#Description: The objective of this script is to show how to back up
configurations/extensions.
# 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};
  }
}
```

降级软件

本节介绍如何降级。

- 关于激活密钥兼容性，第 33-36 页
- 执行降级，第 33-36 页

关于激活密钥兼容性

如果从任何之前版本升级到最新版本，则您的激活密钥保持兼容。但如果要维护降级功能，则可能会遇到问题：

- 降级到 8.1 版本或更早版本 - 在升级之后，如果激活在 *8.2 版本之前*引入的附加功能许可证，则激活密钥在您降级后会继续与更早版本兼容。但是，如果激活在 8.2 版本或更高版本中引入的功能许可证，则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：
  - 如果之前在更早版本中输入了激活密钥，则 ASA 会使用该密钥 （不包括在 8.2 版本或更高版本中激活的任何新许可证）。
  - 如果您有新的系统，并且没有早期的激活密钥，则需要请求与更早版本兼容的新激活密钥。
- 降级到 8.2 版本或更早版本 - 8.3 版本引入了更可靠的基于时间的密钥用法以及故障切换许可证更改：
  - 如果您有多个基于时间的激活密钥处于活动状态，则在降级后，只有最新激活的基于时间的密钥可以处于活动状态。所有其他密钥都会变为非活动状态。
  - 如果您在故障切换对上具有不匹配的许可证，则降级将会禁用故障切换。即使密钥匹配，所使用的许可证也将不再是合并许可证。

执行降级

要降级，请执行以下步骤：

操作步骤

步骤 1　降级软件：

```
ciscoasa(config)# downgrade [/noconfirm] old_image_url old_config_url [activation-key old_key]
```

例如：

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

其中 **/noconfirm** 选项用于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* 是已保存的预迁移配置的路径 （默认情况下，此配置保存在 disk0 上）。如果需要恢复至 8.3 版本之前的激活密钥，可以输入旧的激活密钥。

此命令是用于完成以下功能的快捷方式：

1. 清除引导映像配置 (**clear configure boot**)。
2. 将引导映像设置为旧映像 (**boot system**)。
3. （可选）输入新的激活密钥 (**activation-key**)。
4. 将运行配置保存到启动配置 (**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. 将旧配置复制到启动配置 (**copy** *old_config_url* **startup-config**)。
6. 重新加载 (**reload**)。

配置自动更新

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到多个 ASA，并可提供从中央位置对 ASA 的基本监控。

- 关于自动更新，第 33-37 页
- 自动更新准则，第 33-39 页
- 配置与自动更新服务器的通信，第 33-39 页
- 将客户端更新配置为自动更新服务器，第 33-40 页
- 监控自动更新状态，第 33-42 页

关于自动更新

本节介绍如何实施自动更新，以及可能需要使用自动更新的原因。

- 自动更新客户端或服务器，第 33-37 页
- 自动更新的优势，第 33-37 页
- 故障切换配置中的自动更新服务器支持，第 33-38 页

自动更新客户端或服务器

ASA 可以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 发出更新。

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，自动更新非常有用，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 （故障切换）。
- 通过开放接口提供灵活性。
- 简化用于运营商环境的安全解决方案。

自动更新规范提供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提取配置信息。自动更新服务器也可以向 ASA 发送命令，以便随时发送即时轮询请求。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。

故障切换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/备用故障切换配置下的 ASA。要在主用/备用故障切换配置上启用自动更新，请在故障切换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切换配置下的自动更新服务器支持：

- 仅在单模式下才支持主用/备用配置。
- 加载新的平台软件映像时，故障切换对会停止传递流量。
- 使用基于局域网的故障切换时，新的配置不得更改故障切换链路配置。如果更改，则设备之间的通信将会失败。
- 仅主设备会执行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。如果未处于主用状态，则 ASA 会自动故障切换至主设备。
- 仅主设备会下载软件映像或配置文件。然后，会将软件映像或配置复制到辅助设备。
- 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

以下是故障切换配置下的自动更新过程的概述。此过程假设故障切换已启用且正常运行。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，或者故障切换链路发生故障，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，则 ASA 会先故障切换至主设备，然后与自动更新服务器联系。
3. 自动更新服务器使用软件校验和与 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. 主设备将映像复制到备用设备，然后更新自身的映像。
   c. 如果两台设备都有新映像，则先重新加载辅助 （备用）设备。
   – 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. 更新过程将再次从步骤 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. 主设备会根据需要将 ASDM 映像复制到备用设备。
   c. 主设备会更新自身的 ASDM 映像。
   d. 更新过程将再次从步骤 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. 更新过程将再次从步骤 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。

自动更新准则

- 如果选择 HTTPS 作为用于与自动更新服务器进行通信的协议，则 ASA 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下受支持。

配置与自动更新服务器的通信

操作步骤

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 *url* 具有以下语法：

```
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要使用的接口。如果指定 **management-access** 命令所指定的同一接口，则自动更新请求会通过用于管理访问的相同 IPsec VPN 隧道进行传播。

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）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}
```

通过指定以下参数之一确定所使用的标识符：

- *hardware-serial* 参数指定 ASA 序列号。
- *hostname* 参数用于指定 ASA 主机名。
- **ipaddress** 关键字用于指定所指定接口的 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** 关键字用于指定所指定接口的 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** 关键字用于指定其中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到服务器的次数 （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）要计划使 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、星期六和星期日。其他可能的值为每天 （星期一到星期日）、工作日 （星期一到星期五）和周末 （星期六和星期日）。

time 参数用于以 HH:MM 格式指定开始轮询的时间。例如，8:00 表示上午 8:00，20:00 表示晚上 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。范围是从 1 到 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。范围是从 1 到 35791 分钟。

步骤 5　（可选）如果经过一段时间未联系自动更新服务器，则输入以下命令会导致其停止传递流量：

```
ciscoasa(config)# auto-update timeout period
```

period 参数用于指定介于 1 至 35791 之间的超时时段 （以分钟为单位）。默认值为永不超时（0 分钟）。要恢复默认设置，请输入此命令的 **no** 形式。

使用 **auto-update timeout** 命令确保 ASA 具有最新的映像和配置。此情况通过系统日志消息 201008 进行报告。

示例

在以下示例中， ASA 配置为在端口号 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 还配置为使用主机名作为设备 ID，并且在每个星期五和星期六晚上 10 点到晚上 11 点间的随机时间轮询自动更新服务器。在轮询尝试失败时， ASA 将尝试 10 次重新连接到自动更新服务器，并将在前后两次尝试重新连接之间等待 3 分钟，如下例所示：

```
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、更新应用到的修订版本号以及从中获得更新的 URL 或 IP 地址。

要将 ASA 配置为自动更新服务器，请执行以下步骤：

步骤 1　要启用客户端更新，请输入以下命令：

```
ciscoasa(config)# client-update enable
```

步骤 2　为您希望应用于 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映像或固件映像。可以按任意顺序输入最多四个以逗号分隔的软件映像或固件映像。

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。由于此命令也用于更新 Windows 客户端，因此客户端列表会包含多个 Windows 操作系统。

url *url-string* 参数用于指定软件/固件映像的 URL。此 URL 必须指向适合于此客户端的文件。对于所有自动更新客户端，必须使用协议 “http://” 或 “https://” 作为 URL 前缀。

为您希望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，还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，并且会忽略更新。

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)
```

监控自动更新

- 监控自动更新过程，第 33-41 页
- 监控自动更新过程，第 33-41 页

监控自动更新过程

您可以使用 **debug auto-update client** 或 **debug fover cmd-exe** 命令来显示自动更新过程中执行的操作。以下是 **debug auto-update client** 命令的样本输出。

```
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”，具体取决于哪个更新失败。*version* 是更新的版本号。*reason* 是更新失败的原因。

监控自动更新状态

请参阅以下命令来监控自动更新状态：

show auto-update

以下是 **show auto-update** 命令的样本输出：

```
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
```

软件和配置的历史记录

表 33-1　　软件和配置的历史记录

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，以将文件传输至 SCP 服务器或从中传出文件。 引入了以下命令：**ssh pubkey-chain**、 **server (ssh pubkey-chain)**、 **key-string**、 **key-hash** 和 **ssh stricthostkeycheck**。 修改了以下命令：**copy scp**。
默认情况下会启用自动更新服务器证书验证	9.2(1)	现在，默认情况下会启用自动更新服务器证书验证；对于新的配置，必须明确禁用证书验证。如果您是从较早版本升级且未启用证书验证，则不会启用证书验证，并会显示以下警告： `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.` 系统将迁移配置，以明确配置不进行证书验证： **auto-update server no-verification** 修改了以下命令：**auto-update server** {**verify-certificate** | **no-verification**}。
使用 CLI 的系统备份和恢复	9.3(2)	您现在可以使用 CLI 来备份和恢复完整系统配置，包括映像和证书。 引入了以下命令：**backup** 和 **restore**。

表 33-1　　软件和配置的历史记录 （续）

功能名称	平台版本	功能信息
恢复 ASA 5506W 配置	9.4(1)	现在支持恢复 ASA 5506W 配置。 引入了以下命令：**hw-module module wlan recover configuration**。
恢复和加载新的 ASA 5506W 映像		现在支持恢复和加载新的 ASA 5506W 映像。 引入了以下命令：**hw-module module wlan recover image**。



第 34 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)。

- 关于 EEM，第 34-1 页
- EEM 准则，第 34-2 页
- 配置 EEM，第 34-3 页
- EEM 示例，第 34-9 页
- 监控 EEM，第 34-9 页
- EEM 历史记录，第 34-10 页

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。您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。

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，除非删除并重新添加它们。
  - 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。您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

您可以使用 **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**。此值会丢弃 **action** 命令的任何输出。命令在全局配置模式下作为权限级别为 15（最高）的用户来运行。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

本节介绍在配置 EEM 之前应检查的准则和限制。

情景模式准则

不支持多情景模式。

其他准则

- 在发生崩溃过程中， 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**。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。请参阅创建事件管理器小程序并配置事件，第 34-3 页。

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。请参阅配置操作和操作输出的目标，第 34-4 页。

步骤 3　运行事件管理器小程序。请参阅运行事件管理器小程序，第 34-6 页。

步骤 4　跟踪 EEM 的内存分配和内存使用情况。请参阅跟踪内存分配和内存使用情况，第 34-6 页。

创建事件管理器小程序并配置事件

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。

要删除事件管理器小程序，请输入此命令的 **no** 形式。

步骤 2　对事件管理器小程序进行说明。

description *text*

示例：

```
ciscoasa(config-applet)# description applet1example
```

text 参数最多可包含 256 个字符。如果用引号将说明文本引起来，说明文本可包含空格。

步骤 3　要配置指定的事件，请输入以下命令之一。要删除已配置的事件，请输入相应命令的 **no** 形式。

- 要配置系统日志事件，请确定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 参数用于识别系统日志消息 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。值 0 表示未定义时间段。

- 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。
- 要将事件配置为发生一次且不会重新启动 （除非删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** 形式可删除倒数计时器事件。

注意　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。

- 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

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 的范围为 0 到 4294967295。*command* 选项的值必须位于引号中；否则，如果命令由多个单词组成，则会发生错误。命令在全局配置模式下作为权限级别为 15 （最高）的用户来运行。此命令可能不接受任何输入，因为它处于禁用状态。如果命令使 **noconfirm** 选项可用，请使用此选项。

步骤 2　选择一个可用的输出目标选项。使用相应命令的 **no** 形式可删除输出目标。

- **None** 选项会丢弃 **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
  ```

  注意　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** 选项可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

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。

跟踪内存分配和内存使用情况

要记录内存分配和内存使用情况，请执行以下步骤：

操作步骤

步骤 1　启用内存日志记录。

memory logging [1024-4194304] [**wrap**] [**size** [1-2147483647]] [**process** *process-name*] [**context** *context-name*]

示例：

```
ciscoasa(config)# memory logging 202980
```

唯一必填参数是内存日志记录缓冲区中的条目数。**wrap** 选项用于通知内存日志记录实用程序在封装时保存缓冲区。缓冲区只能保存一次。

如果内存日志记录缓冲区 wrap 多次，会被覆写。当缓冲区 wrap 时，系统会将触发器发送到事件管理器，以启用数据保存。**size** 选项用于监控特定大小。**process** 选项用于监控特定流程。

注意　Checkheaps 进程被当作一个进程完全忽略，因为它以非标准方式使用内存分配器。

context 选项按给定名称为给定虚拟情景记录内存日志记录。

要更改内存日志记录参数，必须将其禁用，然后重新启用。

步骤 2　显示内存日志记录结果。

show memory logging [**brief** | **wrap**]
show memory logging include [**address**] [**caller**] [**operator**] [**size**] [**process**] [**time**] [**context**]

示例：

```
ciscoasa# show memory logging
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] time=[13:26:33.407] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542 0x000000000131911a
0x0000000000442bfd process=[ci/console] time=[13:26:33.407] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x0000000013193e8
0x0000000000443455 0x00000000001318f5b
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542 0x000000000182774d
0x000000000182cc8a process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a 0x0000000000bff606 process=[CMGR Server Process] time=[13:26:35.964]
oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000021246ef 0x0000000001827098 0x000000000182c08d
0x000000000182c262 process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff224b9460 size=40 @ 0x00000000021246ef 0x000000000182711b 0x000000000182c08d
0x000000000182c262 process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542 0x000000000182774d
0x000000000182cc8a process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a 0x0000000000bff606 process=[CMGR Server Process] time=[13:26:38.464]
oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[ci/console] time=[13:26:38.557] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542 0x000000000131911a
0x0000000000442bfd process=[ci/console] time=[13:26:38.557] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x0000000013193e8
0x0000000000443455 0x00000000001318f5b
ciscoasa# show memory logging include process operation size
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
```

```
Number of malloc-fail                    0
Number of realloc-fail                   0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] oper=[malloc] size=72 process=[ci/console] oper=[free] size=72
process=[CMGR Server Process] oper=[malloc] size=16 process=[CMGR Server Process]
oper=[malloc] size=512 process=[CMGR Server Process] oper=[free] size=512 process=[CMGR
Server Process] oper=[malloc] size=40 process=[CMGR Server Process] oper=[free] size=16
process=[CMGR Server Process] oper=[free] size=40 process=[CMGR Server Process]
oper=[malloc] size=16 process=[CMGR Server Process] oper=[malloc] size=512 process=[CMGR
Server Process] oper=[free] size=512 process=[CMGR Server Process] oper=[malloc] size=40
process=[ci/console] oper=[malloc] size=72 process=[ci/console] oper=[free] size=72
ciscoasa# show memory logging brief
Number of free                           6
Number of calloc                         0
Number of malloc                         8
Number of realloc-new                    0
Number of realloc-free                   0
Number of realloc-null                   0
Number of realloc-same                   0
Number of calloc-fail                    0
Number of malloc-fail                    0
Number of realloc-fail                   0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
```

无需任何选项， **show memory logging** 即可显示统计信息以及记录的操作。**brief** 选项仅显示统计信息。**wrap** 选项显示封装后的缓冲区，然后清除数据，以免出现重复数据或保存重复数据。**include** 选项仅包含输出中的指定字段。您可以按任意顺序指定字段，但它们始终以下列顺序显示：

1. 流程
2. 时间
3. 情景 （除非在单模式下）
4. 操作 （free/malloc/等）
5. 地址
6. 大小
7. 主叫方

输出格式如下：

process=[XXX] time=[XXX] context=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX

最多显示 4 个主叫方地址。操作类型列于示例所示的输出 （...的数量）中。

步骤 3　响应内存日志记录包装事件。

event memory-logging-wrap

示例：

```
ciscoasa(config)# event manager applet memlog
ciscoasa(config)# event memory-logging-wrap
ciscoasa(config)# action 0 cli command "show memory logging wrap"
ciscoasa(config)# output file append disk0:/memlog.log
```

示例显示了记录所有内存分配的小程序。当为内存日志记录启用包装时，内存日志记录器向事件管理器发送事件以触发配置的小程序。

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，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

您可使用以下命令监控 EEM。

- **clear configure event manager**

  此命令可删除事件管理器的运行配置。

- **clear configure event manager applet** *appletname*

  此命令可从配置中删除已命名的事件管理器小程序。

- **show counters protocol eem**

  此命令可显示事件管理器的计数器。

- **show event manager**

  此命令可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 memory logging**、 **show memory logging include**

  这些命令可显示关于内存分配和内存使用情况的统计信息。

- **show running-config event manager**

  此命令可显示事件管理器的运行配置。

EEM 历史记录

表 34-1　　EEM 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。您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**。
EEM 的内存跟踪	9.4(1)	添加了一项新的调试功能来记录内存分配和内存使用情况，以响应内存日志记录封装事件。 引入或修改了以下命令：**memory logging**、 **show memory logging**、 **show memory logging include** 和 **event memory-logging-wrap**。



第 35 章

测试和故障排除

本章介绍如何对思科 ASA 进行故障排除和测试基本连接。

- 查看调试消息，第 35-1 页
- 捕获数据包，第 35-1 页
- 查看崩溃转储，第 35-5 页
- 查看核心转储，第 35-5 页
- ASAv 中的 vCPU 使用率，第 35-5 页
- 测试配置，第 35-6 页
- 监控性能和系统资源，第 35-16 页
- 监控连接，第 35-16 页

查看调试消息

由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 TAC 进行故障排除会话过程中使用 **debug** 命令。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。

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* 可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。在多情景模式下，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* 关键字参数对用于为特定 SGT 值指定标签，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，此值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。

要在数据层面捕获数据包，请使用 **asa_dataplane** 关键字。要筛选在 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。在单模式下，背板控制数据包会绕过访问列表，然后被捕获。在多情景模式下，只能在系统情景下捕获控制数据包。可在用户情景下捕获数据包。**access-list** 和 **match** 选项仅在用户情景下可用。

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*可以是以下其中一项：

- **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**。要永久删除捕获，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。

注意　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

要支持集群范围的故障排除，您可以使用 **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属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。

在多情景模式下，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下于集群链路上配置捕获。在系统情景下，控制层面数据包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。在用户情景下，控制层面数据包不可见。只可在此情景下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 接收到带错误格式的 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** 命令输出不会显示这些数据包。
- 您只能捕获 IP 流量；不能捕获非 IP 数据包 （如 ARP）。
- 对于多情景模式下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。
- 在多情景模式下， **copy capture** 命令仅在系统空间中可用。语法如下：

  copy /pcap capture:*Context-name*/*in-cap* **tftp**:

  其中 *in-cap* 是 *context-name* 情景下配置的捕获
- 不支持 **cluster exec capture realtime** 命令。系统会显示以下错误信息：

  ```
  Error: Real-time capture can not be run in cluster exec mode.
  ```

- 对于共享 VLAN，适用以下准则：
  - 只能为 VLAN 配置一个捕获；如果在共享 VLAN 上的多个情景中配置捕获，则仅使用最后配置的捕获。
  - 如果删除最后配置的 （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；您必须删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。唯一的例外是当您未启用 ICMP 检查时（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，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
```

- 多个 PCAP 文件 （一个文件来自一个设备）将复制到 TFTP 服务器。目标捕获文件名会自动附加设备名称，例如 filename_A.pcap、filename_B.pcap 等。在此示例中，A 和 B 是集群设备名称。如果在文件名末尾添加设备名称，将生成不同的目标名称。
- 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属设备。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
```

以下示例显示如何为集群链路中的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
```

以下示例显示如何为集群链路中的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
```

以下示例显示如何捕获某种类型的数据层面消息，如 ICMP 回送请求/响应，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。捕获与嵌入式流的五元组匹配。

虽然 UDP 数据包中的源地址和目标地址是 CCL 地址，但如果此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。也就是说，只要数据包中嵌入的地址 A 和 B 匹配，就还会捕获该数据包。

查看崩溃转储

如果 ASA 或 ASAv 崩溃，您可以查看崩溃转储信息。如果要解释崩溃转储，我们建议您联系思科 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。思科 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 利用率”和 “%CPU 使用率”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

测试配置

本节介绍如何为单模式 ASA 或每个安全情景测试连接，如何 ping ASA 接口，以及如何让一个接口上的主机 ping 到另一个接口上的主机。

- 测试基本连接：ping 地址，第 35-6 页
- 跟踪主机路由，第 35-12 页
- 跟踪数据包以测试策略配置，第 35-14 页

测试基本连接：ping 地址

ping 是一种简单命令，可用于确定特定地址是否处于活动状态以及是否做出响应。以下主题详细介绍此命令以及您可以使用此命令完成什么类型的测试。

- 使用 ping 可以完成什么测试，第 35-7 页
- 在 ICMP 和 TCP ping 之间进行选择，第 35-7 页
- 启用 ICMP，第 35-7 页
- Ping 主机，第 35-8 页
- 系统地测试 ASA 连接，第 35-9 页

使用 ping 可以完成什么测试

当您 ping 设备时，系统会向设备发送数据包并且设备会返回回复。此过程可以让网络设备相互发现、识别和测试。

您可以使用 ping 进行以下测试：

- 两个接口的环回测试 - 可以从同一个 ASA 上的一个接口发起 ping 到另一个接口，以作为外部环回测试验证每个接口的基本 “打开”状态和操作。
- Ping 到一个 ASA - 可以在另一个 ASA 上 ping 接口来验证该接口是否处于打开状态以及是否做出响应。
- 通过 ASA 执行 ping - 可以通过在 ASA 另一侧 ping 设备，通过中间 ASA 执行 ping。数据包将通过中间 ASA 的两个接口，朝每个方向传输。此操作会对中间设备的接口、操作和响应时间执行基本测试。
- 使用 ping 测试网络设备的可疑操作 - 可以从一个 ASA 接口 ping 到一台您怀疑存在功能异常的网络设备。如果接口配置正确但没有收到回送，则可能是设备存在问题。
- 使用 ping 测试中间通信 - 可以从一个 ASA 接口 ping 到已知运行正常的网络设备。如果接收到回送，任意中间设备的正确操作和物理连接都得以确认。

在 ICMP 和 TCP ping 之间进行选择

ASA 包括传统 ping，它会发送 ICMP 回送请求数据包并会在返回中获取回送回复数据包。如果所有相关网络设备都允许 ICMP 流量，这就是标准工具并且会正常运行。通过 ICMP ping，您可以 ping IPv4 或 IPv6 地址或主机名。

但是，某些网络会禁止 ICMP。如果您的网络禁止 ICMP，则可以改用 TCP ping 测试网络连接。对于 TCP ping， ping 会发送 TCP SYN 数据包，如果在响应中收到 SYN-ACK，则系统将 ping 视为成功。通过 TCP ping，您可以 ping IPv4 地址或主机名，但是不可以 ping IPv6 地址。

请记住，ICMP 或 TCP ping 成功只说明您使用的地址处于活动状态并会响应该特定类型的流量。这意味着基本连接正常工作。在设备上运行的其他策略可能会阻止特定类型的流量成功通过设备。

启用 ICMP

默认情况下，您可以从安全性高的端口 ping 到安全性低的端口。只需启用 ICMP 检测即可允许回程流量通行。如果要想从低到高进行 ping，则需要应用 ACL 来允许流量。

当 ping ASA 接口时，应用于接口的所有 ICMP 规则都必须允许回送请求数据包和回送响应数据包。ICMP 规则是可选的：如果您不配置这些规则，则系统会允许流入接口的所有 ICMP 流量。

此程序介绍要启用 ASA 接口的 ICMP ping 或通过 ASA 执行 ping，您可能需要完成的所有 ICMP 配置。

操作步骤

步骤 1　确保 ICMP 规则允许回送请求/回送响应。

ICMP 规则是可选的，应用于直接发送到接口的 ICMP 数据包。如果不应用 ICMP 规则，系统会允许所有 ICMP 访问。在这种情况下，不需要进行任何操作。

但是，如果实施 ICMP 规则，请确保在每个接口上至少包含以下命令，将 “inside”替换为设备上接口的名称。

```
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo inside
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo-reply inside
```

步骤 2　确保访问规则允许 ICMP。

当通过 ASA ping 主机时，访问规则必须允许 ICMP 流量流出和返回。访问规则必须至少允许回送请求数据包/回送回复 ICMP 数据包。您可以将这些规则添加为全局规则。

假设您已经向接口应用或全局应用访问规则，则只需将这些规则添加到相关 ACL，例如：

```
ciscoasa(config)# access-list outside_access_in extended permit icmp any any echo
ciscoasa(config)# access-list outside_access_in extended permit icmp any any echo-reply
```

或者，允许所有 ICMP 即可：

```
ciscoasa(config)# access-list outside_access_in extended permit icmp any any
```

如果您没有访问规则，则还需要允许所需的其他流量类型，因为向接口应用任何访问规则都会增加一个隐式拒绝，因此会丢弃所有其他流量。使用 **access-group** 命令，向接口应用或全局应用 ACL。

如果仅为测试目的添加规则，则可以使用 **access-list** 命令的 **no** 形式 从 ACL 删除规则。如果整个 ACL 都仅用于测试目的，请使用 **no access-group** 命令从接口删除 ACL。

步骤 3　启用 ICMP 检测。

与 ping 接口相反，通过 ASA 执行 ping 时，需要执行 ICMP 检测。检测允许返回流量 （即，回送回复数据包）返回到发起 ping 的主机，同时确保每个数据包都有一个响应，以防止特定类型的攻击。

您只要在默认全局检测策略中启用 ICMP 检测即可。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect icmp
```

Ping 主机

要 ping 任何设备，只需输入 **ping** 和 IP 地址或主机名，例如 **ping 10.1.1.1** 或 **ping www.example.com**。对于 TCP ping，应包含 **tcp** 关键字和目标端口，例如 **ping tcp www.example.com 80**。这通常可满足您需要执行的任何测试要求。

ping 成功的输出示例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

如果 ping 失败，对于每次失败尝试，系统都会输出 ? 并且成功率会显示为低于 100% （完全失败的成功率为 0%）：

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

但是，您还可以添加参数以控制 ping 的一些方面。以下是基本选项：

- ICMP ping。

  ping [*if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]

  其中：

  - *if_name* 是可用于访问主机的接口的名称。如果不在其中包含名称，系统将使用路由表确定要使用的接口。
  - *host* 是要 ping 的主机的 IPv4、 IPv6 或主机名。

  - **repeat** *count* 是要发送的数据包的数量。默认值为 5。
  - **timeout** *seconds* 是在无响应的情况下每个数据包在超时之前等待的秒数。默认值为 2。
  - **data** *pattern* 是要用于所发送数据包中的十六进制模式。默认值为 0xabcd。
  - **size** *bytes* 是所发送数据包的长度。默认值为 100 字节。
  - **validate** 表示要验证回复数据。

- TCP ping。

  ping tcp [*if_name*] *host* [*port*] [**repeat** *count*] [**timeout** *seconds*] [**source** *host ports*]

  其中：

  - *if_name* 是源借以发送 ping 的接口。如果不包含名称，系统将使用路由表。
  - *host* 是要 ping 的目标的 IPv4 地址或主机名。您不能将 TCP ping 用于 IPv6 地址。
  - *port* 是要 ping 的主机上的 TCP 端口。
  - **repeat** 和 **timeout** 与上述含义相同。
  - **source** *host port* 表示 ping 的源主机和端口。使用端口 0 可获取随机端口。

- 交互式 ping。

  ping

  输入不带参数的 ping 时，系统会提示您输入接口、目标和其他参数，包括不可用作关键字的扩展参数。如果您需要对 ping 数据包拥有广泛控制，请使用此方法。

系统地测试 ASA 连接

如果您要对 ASA 连接进行更系统的测试，可以采用以下一般程序。

准备工作

如果要查看程序中提及的系统日志消息，请启用日志记录（使用 **logging enable** 命令，或在 ASDM 中依次选择 **Configuration > Device Management > Logging > Logging Setup**）。

虽然不必要，但您还可以启用 ICMP 调试以在从外部设备 ping ASA 接口时，查看 ASA 控制台上的消息（您将无法查看通过 ASA 的 ping 的调试消息）。我们建议仅在故障排除过程中启用 ping 和调试消息，因为它们会影响性能。以下示例将启用 ICMP 调试，设置要发送到 Telnet 或 SSH 会话的系统日志消息并将它们发送到那些会话，以及启用日志记录。您也可以使用 **logging buffer debug** 命令代替 **logging monitor debug**，将日志消息发送到缓冲区，稍后使用 **show logging** 命令进行查看。

```
ciscoasa(config)# debug icmp trace
ciscoasa(config)# logging monitor debug
ciscoasa(config)# terminal monitor
ciscoasa(config)# logging enable
```

在此配置下，如果从外部主机 (209.165.201.2) 成功 ping 到 ASA 外部接口 (209.165.201.1)，您会看到以下类似内容：

```
ciscoasa(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

输出显示 ICMP 数据包长度（32 字节）、ICMP 数据包的标识符 (1) 和 ICMP 序列号（ICMP 序列号从 0 起计，每次发送请求后序列号递增）。

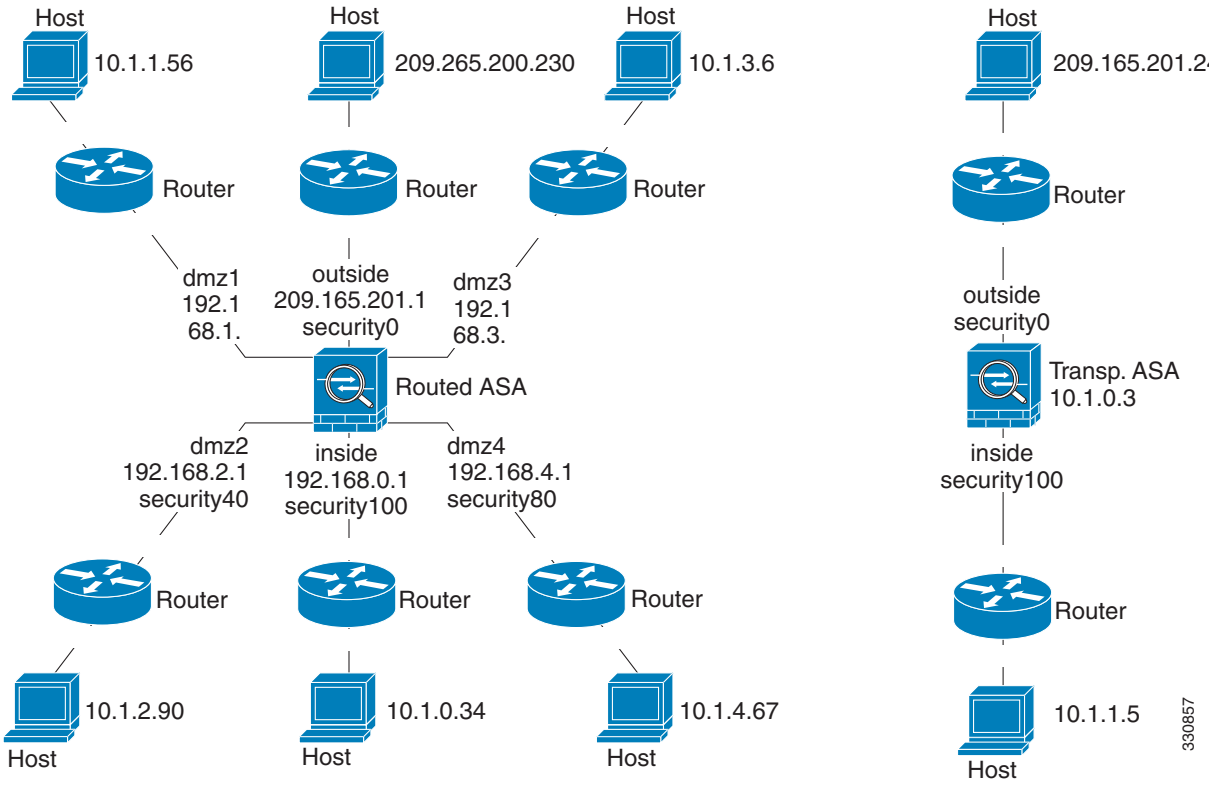
完成测试后，请禁用调试。保留此配置可能构成性能和安全风险。如果仅为了测试而启用日志记录，还可以禁用日志记录。

```
ciscoasa(config)# no debug icmp trace
ciscoasa(config)# no logging monitor debug
ciscoasa(config)# terminal no monitor
ciscoasa(config)# no logging enable
```

操作步骤

步骤 1　绘制显示接口名称、安全级别和 IP 地址的单模式 ASA 或安全情景的示意图。示意图也应包括所有直接连接的路由器和一台主机，该主机位于用于 ping ASA 的路由器的另一侧。

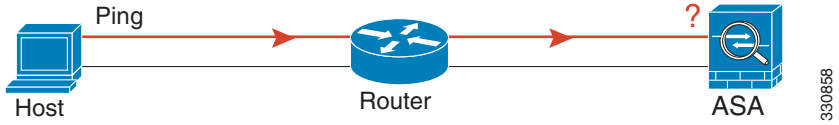
图 35-1　　接口、路由器和主机的网络图



步骤 2　从直接连接的路由器 ping 每个 ASA 接口。对于透明模式，ping 管理 IP 地址。此测试可确保 ASA 接口处于活动状态，并且接口配置正确。

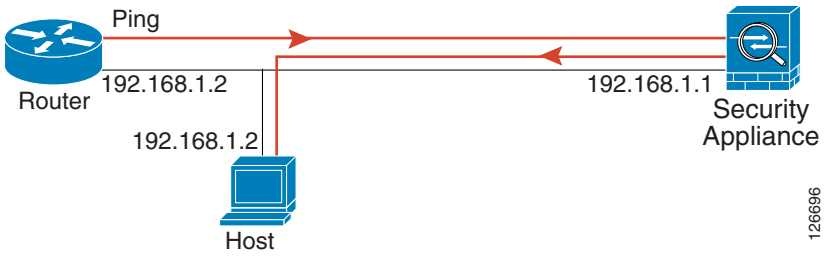
如果 ASA 接口处于非活动状态、接口配置不正确，或 ASA 与路由器之间的交换机关闭（参阅下图），ping 操作可能会失败。在这种情况下，数据包不能到达 ASA，因此调试消息或系统日志消息不会显示。

图 35-2　　ASA 接口的 ping 故障



如果 ping 回复没有返回到路由器，则可能存在交换机环路或冗余 IP 地址 （参阅下图）。

图 35-3　　IP 寻址问题引发的 ping 故障



步骤 3　从远程主机上 ping 每个 ASA 接口。对于透明模式，ping 管理 IP 地址。此测试检查直接连接的路由器是否能在主机和 ASA 之间路由数据包，以及 ASA 是否可以正确地将数据包路由回主机。

如果 ASA 没有通过中间路由器返回路由到主机， ping 操作可能失败 （参阅下图）。在这种情况下，调试消息显示 ping 成功，但系统会显示系统日志消息 110001，指示出现路由故障。

图 35-4　　ASA 没有返回路由引发的 ping 故障



步骤 4　从 ASA 接口 ping 到已知正常运行的网络设备。

- 如果没有收到 ping，传输硬件或接口配置中可能存在问题。
- 如果 ASA 接口已正确配置但没有收到来自 “已知良好的” 设备的回送回复，接口硬件的接收功能可能存在问题。如果另一个具有 “已知良好的” 接收功能的接口可以在 ping 过该 “已知良好的” 设备后收到回送，则可以确认第一个接口硬件的接收功能存在问题。

步骤 5　从一个源接口的主机或路由器 ping 另一个接口上的主机或路由器。无论要检查多少接口对，都可以重复此步骤。如果使用 NAT，测试显示 NAT 运行正常。

如果 ping 成功，系统将显示系统日志消息确认路由模式的地址转换 （305009 或 305011），并确认已创建一个 ICMP 连接 （302020）。您还可以输入 **show xlate** 或 **show conns** 命令查看此信息。

如果 NAT 配置错误， ping 操作可能会失败。在这种情况下，系统会显示系统日志消息，指示 NAT 失败 （305005 或 305006）。如果在没有静态转换的情况下从外部主机 ping 内部主机，您将会收到消息 106010。

图 35-5　　ASA 未进行地址转换引发的 ping 故障



跟踪主机路由

如果您向某个 IP 地址发送流量时遇到问题，可以跟踪主机路由以确定网络路径是否有问题。

操作步骤

步骤 1　在跟踪路由上显示 ASA，第 35-12 页。

步骤 2　确定数据包路由，第 35-13 页。

在跟踪路由上显示 ASA

默认情况下， ASA 不会在跟踪路由上显示为跃点。要使其显示，您需要减少通过 ASA 的数据包的生存时间，并且增加 ICMP 不可达消息的速率限制。

操作步骤

步骤 1　创建 L3/L4 类映射，以确定要为其自定义连接设置的流量。

class-map *name*
match *parameter*

示例：

```
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match any
```

有关匹配语句的信息，请参阅 《防火墙配置指南》中 “服务策略”章节。

步骤 2　添加或编辑用于设置要对类映射流量执行的操作的策略映射，并确定类映射。

policy-map *name*
class *name*

示例：

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class CONNS
```

在默认配置中， global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。对于类映射，请指定在本程序前面部分中创建的类。

步骤 3　减小与类匹配的数据包的生存时间 (TTL)。

set connection decrement-ttl

步骤 4　如果编辑的是现有服务策略 （例如，名为 global_policy 的默认全局策略），您即可跳过此步骤。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
ciscoasa(config)# service-policy global_policy global
```

global 关键字将策略映射应用于所有接口， **interface** 将策略应用于一个接口。仅允许存在一个全局策略。可以通过在接口应用服务策略来覆盖该接口的全局策略。每个接口只能应用一个策略映射。

步骤 5　提高 ICMP 不可达消息的速率限制，以使 ASA 显示在跟踪路由输出上。

icmp unreachable rate-limit *rate* **burst-size** *size*

示例

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

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

示例

以下示例为所有流量全局减小 TTL 并将 ICMP 不可达消息限制增至 50。

```
ciscoasa(config)# class-map global-policy
ciscoasa(config-cmap)# match any
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class global-policy
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 6
```

确定数据包路由

使用 Traceroute 帮助您确定数据包到达目标地址所要经过的路由。将 UDP 数据包发送到一个无效端口上的目标地址，跟踪路由即可启用。由于端口无效，到达目标地址过程中的路由器回应的是一个 ICMP Time Exceeded 消息，并将该错误报告给 ASA。

跟踪路由显示发送的每个探测的结果。每行输出以递增顺序对应一个 TTL 值。下表对输出符号进行了说明。

输出符号	说明
*	在超时期限内未收到对探测的响应。
nn msec	各节点指定探测数的往返时间 （以毫秒为单位）。
!N.	无法访问 ICMP 网络。
!H	无法访问 ICMP 主机。
!P	无法访问 ICMP。
!A	管理性禁止 ICMP。
?	未知 ICMP 错误。

操作步骤

步骤 1　跟踪通往目标的路由。

traceroute [*destination_ip* | *hostname*}
[**source** {*source_ip* | *source-interface*}] [**numeric**] [**timeout** *timeout_value*]
[**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

通常，您只需包含目标 IP 地址或主机名，例如 **traceroute www.example.com**。但是，如有必要，可以调整跟踪的特征：

- **source** {*source_ip* | *source-interface*} - 指定用作跟踪源的接口。您可以按名称或 IP 地址指定接口。在透明模式下，您必须使用管理地址。
- **numeric** - 表示在跟踪路由上应显示的 IP 地址。如果没有此关键字，跟踪路由不会为地址执行 DNS 查找，并且如果您配置了 DNS，跟踪路由还包含 DNS 名称。
- **timeout** *timeout_value* - 在超时之前等待响应的时间。默认值为 3 秒。
- **probe** *probe_num* - 每个 TTL 级别发送的探测数量。默认值为 3。
- **ttl** *min_ttl max_ttl* - 探测的最小和最大生存时间值。默认最小值为 1，但也可以设置更高值来阻止显示已知跃点。最大默认值为 30。当数据包到达目标地址或达到最大值时，跟踪路由终止。
- **port** *port_value* - 要使用的 UDP 端口。默认值为 33434。
- **use-icmp** - 为探测发送 ICMP 数据包而不是 UDP 数据包。

示例

```
ciscoasa# traceroute 209.165.200.225

Type escape sequence to abort.
Tracing the route to 209.165.200.225

1 10.83.194.1 0 msec 10 msec 0 msec
2 10.83.193.65 0 msec 0 msec 0 msec
3 10.88.193.101 0 msec 10 msec 0 msec
4 10.88.193.97 0 msec 0 msec 10 msec
5 10.88.239.9 0 msec 10 msec 0 msec
6 10.88.238.65 10 msec 10 msec 0 msec
7 172.16.7.221 70 msec 70 msec 80 msec
8 209.165.200.225 70 msec 70 msec 70 msec
```

跟踪数据包以测试策略配置

您可以通过根据源和目标寻址以及协议特征为数据包建模，测试您的策略配置。跟踪会执行策略查找以测试访问规则、 NAT、路由等，以便查看系统会允许还是拒绝数据包。

通过这样测试数据包，您可以看到策略结果并测试系统是否会按照需要处理要允许或拒绝的流量类型。除了验证配置之外，您还可以使用跟踪器调试意外行为，例如数据包本应被允许，但却被拒绝的情况。

操作步骤

步骤 1　该命令很复杂，因此我们将其分解为几个部分。首先从为跟踪选择接口和协议开始：

packet-tracer input *ifc_name* {**icmp** | **tcp** | **udp** | **rawip**} [**inline-tag** *tag*] ...

其中：

- **input** *ifc_name* - 开始跟踪的接口的名称。
- **icmp**、 **tcp**、 **udp**、 **rawip** - 要使用的协议。 “rawip”是原始 IP，即非 TCP/UDP 的 IP 数据包。
- **inline-tag** *tag* -（可选）。嵌入第 2 层 CMD 报头中的安全组标签值。有效值范围为 0 到 65533。

步骤 2　接下来，键入源地址和协议条件。

...{sip | **user** *username* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}...

其中：

- *sip* - 数据包跟踪的源 IPv4 或 IPv6 地址。
- **user** *username* - domain\user 格式的用户身份。跟踪中使用最近为用户映射的地址 （如有）。
- **security-group** {**name** *name* | **tag** *tag*} - 适用于 Trustsec 的基于 IP-SGT 查找的源安全组。您可以指定安全组名称或标签编号。
- **fqdn** *fqdn-string* - 源主机的完全限定域名，仅限 IPv4。

步骤 3　接下来，键入协议特征。

- ICMP - 输入 ICMP 类型 (1-255)、ICMP 代码 (0-255)，并且可以选择键入 ICMP 标识符。您必须对每个变量使用编号，例如， 8 用于表示回送。

  … type code [*ident*]...

- TCP/UDP - 输入源端口号。

  … sport ...

- Raw IP - 输入协议编号， 0-255。

  … protocol ...

步骤 4　最后，键入目标地址条件、 TCP/UDP 跟踪的目标端口和可选关键字，然后按 Enter。

...{dip | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}
dport
[**detailed**] [**xml**]

其中：

- *dip* - 数据包跟踪的目标 IPv4 或 IPv6 地址。
- **security-group** {**name** *name* | **tag** *tag*} - 适用于 Trustsec 的基于 IP-SGT 查找的目标安全组。您可以指定安全组名称或标签编号。
- **fqdn** *fqdn-string* - 目标主机的完全限定域名，仅限 IPv4。
- *dport* - TCP/UDP 跟踪的目标端口。请勿为 ICMP 或原始 IP 跟踪添加此值。
- **detailed** - 除了正常输出之外，还提供详细的跟踪结果信息。
- **xml** - 以 XML 格式显示跟踪结果。

示例

以下示例跟踪从 10.100.10.10 到 10.100.11.11 的 HTTP 端口的 TCP 数据包。结果表明隐式拒绝访问规则将丢弃该数据包。

```
ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10  80 10.100.11.11 80

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

监控性能和系统资源

您可以监控各种系统资源以确定性能或其他潜在问题。

- **show perfmon**

  显示 NAT 转换、连接、检测、URL 访问和服务器请求、AAA 和 TCP 拦截的当前和平均统计信息。

- **show memory**

  显示可用内存和已用内存。

- **show blocks**

  根据块大小显示内存块信息。

- **show cpu**

  显示 CPU 利用率。

- **show process**

  显示系统进程信息。以下是一些有用的变体：

  - **show process cpu-usage non-zero** - 显示实际正在使用 CPU 的进程，其中会过滤掉那些使用率为 0% 的进程。
  - **show process cpu-usage sorted** - 提供与进程相关的任何已配置情景消耗的 CPU 负载分解数据。

监控连接

要查看当前连接及其源、目标、协议等信息，请使用 **show conn all detail** 命令。



第 8 部分

日志记录、SNMP 和 Smart Call Home



日志记录

本章介绍如何记录系统消息并将其用于故障排除。

- 关于日志记录，第 36-1 页
- 日志记录准则，第 36-4 页
- 配置日志记录，第 36-5 页
- 监控日志，第 36-18 页
- 日志记录示例，第 36-18 页
- 日志记录的历史记录，第 36-19 页

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一种方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。思科设备可以将其日志消息发送到 UNIX 样式的系统日志服务。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打印消息。以这种形式记录日志可为日志提供受保护的长期存储。日志对常规故障排除及事件处理均有帮助。

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：覆盖缓冲区、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。

多情景模式下的日志记录

每个安全情景包含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，则只能在会话中查看与当前情景相关的消息。

请在管理情景中查看在系统执行空间中生成的系统日志消息（包括故障切换消息）以及在管理情景中生成的消息。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。

可以将 ASA 和 ASASM 配置为在每个消息中包含情景名称，从而帮助区分发送到单个系统日志服务器的情景消息。此功能有助于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 拒绝率日志记录功能显示在 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每个已建立和中断的连接，以及各连接使用的持续时间和流量。
- 协议使用情况消息显示每个连接使用的协议和端口号。
- 地址转换审计线索消息记录建立或中断的 NAT 或 PAT 连接，如果接收到从网络内部到外部环境的恶意活动报告，这些消息会有所帮助。

系统日志消息格式

系统日志消息以百分号 (%) 开头并构造如下：

```
%ASA Level Message_number: Message_text
```

字段说明如下：

ASA	由 ASA 和 ASASM 所生成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所描述情况的严重性 - 数字越小，情况越严重。
Message_number	用于标识系统日志消息的唯一六位数编号。
Message_text	用于描述情况的文本字符串。系统日志消息的这一部分有时包含 IP 地址、端口号或用户名。

严重性级别

下表列出系统日志消息严重性级别。可以为各严重性级别分配自定义颜色，更轻松地在 ASDM 日志查看器中对其进行区分。要配置系统日志消息颜色设置，请依次选择 **Tools > Preferences > Syslog** 选项卡，或者在日志查看器中，点击工具栏上的 **Color Settings**。

表 36-1　　系统日志消息严重性级别

级别号	严重级别	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。

备注　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，可以对 ASA 和 ASASM 进行配置，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）

通过创建一个在设置输出目标时可以指定的消息列表来自定义这些条件。或者，也可以将 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一个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。与 VPN 客户端功能相关联的系统日志消息范围从 611101 至 611323。

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。如果在生成系统日志消息时对象未知，则不显示特定的 *heading = value* 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，使用以下任何一个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，必须使用新命令条目来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，则消息仅记录一次。

集群

系统日志消息是在集群环境中用于记帐、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

本节介绍您在配置日志记录之前应审阅的准则和限制。

IPv6 规定

不支持 IPv6。

其他准则

- 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，您必须从其他供应商处获取 syslogd 服务器。
- 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。

- 不支持在备用 ASA 上通过 TCP 发送系统日志。
- ASA 支持在单情景模式下使用 **logging host** 命令配置 16 个系统日志服务器。在多情景模式下，限制为每个情景 4 个服务器。
- 应可以通过 ASA 和 ASASM 到达系统日志服务器。应将 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，请抑制系统日志 313001、313004 和 313005 的生成。
- 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。此默认行为是程序设计的。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
```

- 当 ASA 通过 TCP 发送系统日志时，在系统日志服务重新启动后，需要大约一分钟来启动连接。

配置日志记录

本节介绍如何配置日志记录。

步骤 1　启用日志记录。请参阅启用日志记录，第 36-6 页。

步骤 2　配置系统日志消息的输出目标。请参阅配置输出目标，第 36-6 页。

注意　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

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

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。

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。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。这两个协议的有效端口值为 1025 至 65535。默认 UDP 端口为 514。默认 UDP 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。

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保存到内部闪存。

  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

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到 ASDM

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

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

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

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来定义事件列表：

- 事件类
- 严重性
- 消息 ID

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。

注意　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 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）。

注意　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，则该消息仅记录一次。

将 EMBLEM 格式的系统日志消息生成到系统日志服务器

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。这两个协议的有效端口值为 1025 至 65535。默认 UDP 端口为 514。默认 UDP 端口为 1470。

注意　不支持在备用 ASA 上通过 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

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

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

要配置日志记录队列，请执行以下步骤：

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

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 日志记录。**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

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。

注意　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

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）。如果在多情景模式下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。

注意　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。在集群环境中， **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）

注意　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

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
```

要从系统日志消息中删除日期和时间，请输入 **no logging timestamp** 命令。

禁用系统日志消息

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
```

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

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
```

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。

在备用设备上阻止系统日志消息

要阻止在备用设备上生成特定系统日志消息，请执行以下步骤：

操作步骤

步骤 1　取消阻止以前阻止在备用设备上生成的特定系统日志消息。

logging message *syslog-id* **standby**

示例：

```
ciscoasa(config)# logging message 403503 standby
```

要阻止在备用设备上生成特定系统日志消息，请使用 **no** 形式的此命令。

使用 **logging standby** 命令确保在发生故障转移的情况下故障转移备用 ASA 的系统日志消息保持同步。

注意　使用 **logging standby** 命令会导致共享日志记录目标 （例如系统日志服务器、 SNMP 服务器和 FTP 服务器）上的流量翻倍。

限制系统日志消息生成速率

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。

  注意　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 36-2　　日志记录的历史记录

功能名称	平台版本	说明
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**。
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**。

表 36-2　　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**。
日志查看器	8.3(1)	向日志查看器中添加了源 IP 地址和目标 IP 地址。
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。
系统日志消息过滤和排序	8.4(1)	已为下列各项添加了支持： • 根据与各列对应的多个文本字符串过滤系统日志消息 • 创建自定义过滤器 • 对消息进行列排序。有关详细信息，请参阅ASDM 配置指南。 修改了以下屏幕： Monitoring > Logging > Real-Time Log Viewer > View。 Monitoring > Logging > Log Buffer Viewer > View。 此功能与所有 ASA 版本互操作。
群集	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**。
在备用设备上阻止系统日志	9.4(1)	添加了对于在故障切换配置中的备用设备上阻止生成特定系统日志消息的支持。 引入了以下命令：**logging message** *syslog-id* **standby**。



SNMP

本章介绍如何配置简单网络管理协议 (SNMP) 以监控思科 ASA。

- 关于 SNMP，第 37-1 页
- SNMP 准则，第 37-18 页
- 配置 SNMP，第 37-20 页
- 监控 SNMP，第 37-27 页
- SNMP 的示例，第 37-28 页
- SNMP 历史记录，第 37-29 页

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，并且支持同时使用所有三个版本。利用在 ASA 接口上运行的 SNMP 代理，您可以通过诸如 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，因此您无法对 SNMP 进行更改。此外，不支持 SNMP SET 请求。

您可以将 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）的从托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回复。

SNMP 术语

下表列出在使用 SNMP 时常用的术语。

表 37-1　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、故障切换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，您还可以从以下位置下载 RFC、标准 MIB 和标准陷阱：

http://www.ietf.org/

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

备注　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，我们建议在连续的轮询之间等待至少 5 秒。

在 MIB 中，并非所有 OID 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
```

备注　尽管 **oidlist** 关键字没有显示在 **show snmp-server** 命令的选项列表中，但它是可用的。但是，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。您可以使用此值标识型号。下表列出用于各型号 ASA 的 sysObjectID OID。

表 37-2 SNMP 对象标识符

产品标识符	sysObjectID	型号编号
ASA 5506 自适应安全设备	ciscoASA5506 (ciscoProducts 2114)	ASA 5506-X
ASA 5506 自适应安全设备安全情景	ciscoASA5506sc (ciscoProducts 2115)	ASA 5506-X 安全情境
ASA 5506 自适应安全设备系统情景	ciscoASA5506sy (ciscoProducts 2116)	ASA 5506-X 系统情景
ASA 5506W 自适应安全设备	ciscoASA5506W (ciscoProducts 2117)	ASA 5506W-X
ASA 5506W 自适应安全设备安全情景	ciscoASA5506Wsc (ciscoProducts 2118)	ASA 5506W-X 安全情境
ASA 5506W 自适应安全设备系统情景	ciscoASA5506Wsy (ciscoProducts 2119)	ASA 5506W-X 系统情景
ASA 5508 自适应安全设备	ciscoASA5508 (ciscoProducts 2120)	ASA 5508-X
ASA 5508 自适应安全设备安全情景	ciscoASA5508sc (ciscoProducts 2121)	ASA 5508-X 安全情境
ASA 5508 自适应安全设备系统情景	ciscoASA5508sy (ciscoProducts 2122)	ASA 5508-X 系统情景
无负载加密的 ASA 5506 自适应安全设备	ciscoASA5506K7 (ciscoProducts 2123)	无负载加密的 ASA 5506-X 自适应安全设备
无负载加密的 ASA 5506 自适应安全设备安全情景	ciscoASA5506K7sc (ciscoProducts 2124)	无负载加密的 ASA 5506-X 自适应安全设备安全情景
无负载加密的 ASA 5506 自适应安全设备系统情景	ciscoASA5506K7sy (ciscoProducts 2125)	无负载加密的 ASA 5506-X 自适应安全设备系统情景
无负载加密的 ASA 5508 自适应安全设备	ciscoASA5508K7 (ciscoProducts 2126)	无负载加密的 ASA 5508-X 自适应安全设备系统情景
无负载加密的 ASA 5508 自适应安全设备安全情景	ciscoASA5508K7sc (ciscoProducts 2127)	无负载加密的 ASA 5508-X 自适应安全设备安全情景

表 37-2 SNMP 对象标识符 （续）

无负载加密的 ASA 5508 自适应安全设备系统情景	ciscoASA5508K7sy (ciscoProducts 2128)	无负载加密的 ASA 5508-X 自适应安全设备系统情景
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
适用于 Catalyst 交换机/7600 路由器的无负载加密的 ASA 服务模块安全情景	ciscoAsaSm1K7sc (ciscoProducts 1334)	适用于 Catalyst 交换机/7600 路由器的无负载加密的自适应安全设备 (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
适用于 Catalyst 交换机/7600 路由器的无负载加密的 ASA 服务模块系统情景	ciscoAsaSm1K7sy (ciscoProducts 1335)	适用于 Catalyst 交换机/7600 路由器的无负载加密的自适应安全设备 (ASA) 服务模块系统情景
适用于 Catalyst 交换机/7600 路由器的无负载加密的 ASA 服务模块系统情景	ciscoAsaSm1K7 (ciscoProducts 1336)	适用于 Catalyst 交换机/7600 路由器的无负载加密的自适应安全设备 (ASA) 服务模块
ASA 5512	ciscoASA5512 (ciscoProducts 1407)	ASA 5512 自适应安全设备

表 37-2 SNMP 对象标识符 （续）

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
ASA5512 系统情景	ciscoASA5512sy (ciscoProducts 1415)	ASA 5512 自适应安全设备系统情景
ASA5515 系统情景	ciscoASA5515sy (ciscoProducts 1416)	ASA 5515 自适应安全设备系统情景
ASA5525 系统情景	ciscoASA5525sy (ciscoProducts1417)	ASA 5525 自适应安全设备系统情景
ASA5545 系统情景	ciscoASA5545sy (ciscoProducts 1418)	ASA 5545 自适应安全设备系统情景
ASA5555 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 安全情境	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

每个思科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 对象中返回此值。您可以使用此值标识组件的类型 （模块、电源、风扇、传感器、 CPU 等）。下表列出用于各型号 ASA 和 ASASM 的物理供应商类型值。

表 37-3 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)
适用于 Catalyst 交换机/7600 路由器的无负载加密的 ASA 服务模块	cevCat6kWsSvcAsaSm1K7 (cevModuleCat6000Type 186)
5506 自适应安全设备的加速器	cevAcceleratorAsa5506 (cevOther 10)
5506W 自适应安全设备的加速器	cevAcceleratorAsa5506W (cevOther 11)
5508 自适应安全设备的加速器	cevAcceleratorAsa5508 (cevOther 12)
无负载加密的 5506 自适应安全设备的加速器	cevAcceleratorAsa5506K7 (cevOther 13)
无负载加密的 5508 自适应安全设备的加速器	cevAcceleratorAsa5508K7 (cevOther 14)
思科自适应安全设备 (ASA) 5506 机箱	cevChassisAsa5506 (cevChassis 1600)
思科自适应安全设备 (ASA) 5506W 机箱	cevChassisAsa5506W (cevChassis 1601)

表 37-3　　物理供应商类型值 （续）

思科自适应安全设备 (ASA) 5508 机箱	cevChassisAsa5508 (cevChassis 1602)
无负载加密的思科自适应安全设备 (ASA) 5506 机箱	cevChassisAsa5506K7 (cevChassis 1603)
无负载加密的思科自适应安全设备 (ASA) 5508 机箱	cevChassisAsa5508K7 (cevChassis 1604)
5506 自适应安全设备的中央处理器	cevCpuAsa5506 (cevModuleCpuType 312)
5506W 自适应安全设备的中央处理器	cevCpuAsa5506W (cevModuleCpuType 313)
5508 自适应安全设备的中央处理器	cevCpuAsa5508 ((cevModuleCpuType 314)
无负载加密的 5506 自适应安全设备的中央处理器	cevCpuAsa5506K7 (cevModuleCpuType 315)
无负载加密的 5508 自适应安全设备的中央处理器	cevCpuAsa5508K7 (cevModuleCpuType 316)
cevModuleASA5506 类型机箱	cevModuleASA5506Type (cevModule 107)
5506 自适应安全设备现场可更换固态驱动器	cevModuleAsa5506SSD (cevModuleASA5506Type 1)
5506W 自适应安全设备现场可更换固态驱动器	cevModuleAsa5506WSSD (cevModuleASA5506Type 2)
无负载加密的 5506 自适应安全设备现场可更换固态驱动器	cevModuleAsa5506K7SSD (cevModuleASA5506Type 3)
cevModuleASA5508 类型机箱	cevModuleASA5508Type (cevModule 108)
5508 自适应安全设备现场可更换固态驱动器	cevModuleAsa5508SSD (cevModuleASA5508Type 1)
无负载加密的 5508 自适应安全设备现场可更换固态驱动器	cevModuleAsa5508K7SSD (cevModuleASA5508Type 2)
5508 自适应安全设备的机箱冷却风扇	cevFanAsa5508ChassisFan (cevFan 247)
无负载加密的 5508 自适应安全设备的机箱冷却风扇	cevFanAsa5508K7ChassisFan (cevFan 248)
5508 自适应安全设备的机箱冷却风扇传感器	cevSensorAsa5508ChassisFanSensor (cevSensor 162)
无负载加密的 5508 自适应安全设备的机箱冷却风扇传感器	cevSensorAsa5508K7ChassisFanSensor (cevSensor 163)
5506 自适应安全设备的中央处理器温度传感器	cevSensorAsa5506CpuTempSensor (cevSensor 164)
5506W 自适应安全设备的中央处理器温度传感器	cevSensorAsa5506WCpuTempSensor (cevSensor 165)
5508 自适应安全设备的中央处理器温度传感器	cevSensorAsa5508CpuTempSensor (cevSensor 166)
无负载加密的 5506 自适应安全设备的中央处理器温度传感器	cevSensorAsa5506K7CpuTempSensor (cevSensor 167)
无负载加密的 5508 自适应安全设备的中央处理器温度传感器	cevSensorAsa5508K7CpuTempSensor (cevSensor 168)
5506 自适应安全设备的加速器温度传感器	cevSensorAsa5506AcceleratorTempSensor (cevSensor 169)
5506W 自适应安全设备的加速器温度传感器	cevSensorAsa5506WAcceleratorTempSensor (cevSensor 170)
5508 自适应安全设备的加速器温度传感器	cevSensorAsa5508AcceleratorTempSensor (cevSensor 171)
无负载加密的 5506 自适应安全设备的加速器温度传感器	cevSensorAsa5506K7AcceleratorTempSensor (cevSensor 172)
无负载加密的 5508 自适应安全设备的加速器温度传感器	cevSensorAsa5508K7AcceleratorTempSensor (cevSensor 173)
5506 自适应安全设备的机箱环境温度传感器	cevSensorAsa5506ChassisTempSensor (cevSensor 174)
5506W 自适应安全设备的机箱环境温度传感器	cevSensorAsa5506WChassisTempSensor (cevSensor 175)
5508 自适应安全设备的机箱环境温度传感器	cevSensorAsa5508ChassisTempSensor (cevSensor 176)
无负载加密的 5506 自适应安全设备的机箱环境温度传感器	cevSensorAsa5506K7ChassisTempSensor (cevSensor 177)

表 37-3 物理供应商类型值 （续）

无负载加密的 5508 自适应安全设备的机箱环境温度传感器	cevSensorAsa5508K7ChassisTempSensor (cevSensor 178)
思科自适应安全设备 (ASA) 5512 自适应安全设备	cevChassisASA5512 (cevChassis 1113)
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)
5512 思科自适应安全设备的中央处理器	cevCpuAsa5512 (cevModuleCpuType 229)
无负载加密的 5512 思科自适应安全设备的中央处理器	cevCpuAsa5512K7 (cevModuleCpuType 224)
5515 思科自适应安全设备的中央处理器	cevCpuAsa5515 (cevModuleCpuType 230)
无负载加密的 5515 思科自适应安全设备的中央处理器	cevCpuAsa5515K7 (cevModuleCpuType 225)
5525 思科自适应安全设备的中央处理器	cevCpuAsa5525 (cevModuleCpuType 231)
无负载加密的 5525 思科自适应安全设备的中央处理器	cevCpuAsa5525K7 (cevModuleCpuType 226)
5545 思科自适应安全设备的中央处理器	cevCpuAsa5545 (cevModuleCpuType 232)
无负载加密的 5545 思科自适应安全设备的中央处理器	cevCpuAsa5545K7 (cevModuleCpuType 227)
5555 思科自适应安全设备的中央处理器	cevCpuAsa5555 (cevModuleCpuType 233)
无负载加密的 5555 思科自适应安全设备的中央处理器	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)
适用于 Catalyst 交换机/7600 路由器的无负载加密的思科 ASA 服务模块的 CPU	cevCpuAsaSm1K7 (cevModuleCpuType 223)

表 37-3 物理供应商类型值 （续）

5512 自适应安全设备的机箱冷却风扇	cevFanASA5512ChassisFan (cevFan 163)
无负载加密的 5512 自适应安全设备的机箱冷却风扇	cevFanASA5512K7ChassisFan (cevFan 172)
5515 自适应安全设备的机箱冷却风扇	cevFanASA5515ChassisFan (cevFan 164)
无负载加密的 5515 自适应安全设备的机箱冷却风扇	cevFanASA5515K7ChassisFan (cevFan 171)
5525 自适应安全设备的机箱冷却风扇	cevFanASA5525ChassisFan (cevFan 165)
无负载加密的 5525 自适应安全设备的机箱冷却风扇	cevFanASA5525K7ChassisFan (cevFan 170)
5545 自适应安全设备的机箱冷却风扇	cevFanASA5545ChassisFan (cevFan 166)
无负载加密的 5545 自适应安全设备的机箱冷却风扇	cevFanASA5545K7ChassisFan (cevFan 169)
无负载加密的 5545 自适应安全设备的电源风扇	cevFanASA5545K7PSFan (cevFan 161)
5545 自适应安全设备的电源风扇	cevFanASA5545PSFan (cevFan 159)
5555 自适应安全设备的机箱冷却风扇	cevFanASA5555ChassisFan (cevFan 167)
无负载加密的 5555 自适应安全设备的机箱冷却风扇	cevFanASA5555K7ChassisFan (cevFan 168)
5555 自适应安全设备的电源风扇	cevFanASA5555PSFan (cevFan 160)
无负载加密的 5555 自适应安全设备的电源风扇	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)
5545 自适应安全设备的电源装置	cevPowerSupplyASA5545PSInput (cevPowerSupply 323)
5545 自适应安全设备的电源输入状态传感器	cevPowerSupplyASA5545PSPresence (cevPowerSupply 321)
5555 自适应安全设备的电源装置	cevPowerSupplyASA5555PSInput (cevPowerSupply 324)
5555 自适应安全设备的电源输入状态传感器	cevPowerSupplyASA5555PSPresence (cevPowerSupply 322)
ASA 5585 的电源输入	cevPowerSupplyASA5585PSInput (cevPowerSupply 304)
5512 思科自适应安全设备 (ASA) 机箱风扇传感器	cevSensorASA5512ChassisFanSensor (cevSensor 120)
5512 思科自适应安全设备的机箱环境温度传感器	cevSensorASA5512ChassisTemp (cevSensor 107)
5512 思科自适应安全设备的中央处理器温度传感器	cevSensorASA5512CPUTemp (cevSensor 96)
无负载加密的 5512 思科自适应安全设备 (ASA) 机箱风扇传感器	cevSensorASA5512K7ChassisFanSensor (cevSensor 125)
无负载加密的 5512 思科自适应安全设备的中央处理器温度传感器	cevSensorASA5512K7CPUTemp (cevSensor 102)
无负载加密的 5512 自适应安全设备的机箱冷却风扇传感器	cevSensorASA5512K7PSFanSensor (cevSensor 116)
5512 自适应安全设备的机箱冷却风扇传感器	cevSensorASA5512PSFanSensor (cevSensor 119)
5515 思科自适应安全设备 (ASA) 机箱风扇传感器	cevSensorASA5515ChassisFanSensor (cevSensor 121)
5515 思科自适应安全设备的机箱环境温度传感器	cevSensorASA5515ChassisTemp (cevSensor 98)
5515 思科自适应安全设备的中央处理器温度传感器	cevSensorASA5515CPUTemp (cevSensor 97)
无负载加密的 5515 思科自适应安全设备 (ASA) 机箱风扇传感器	cevSensorASA5515K7ChassisFanSensor (cevSensor 126)

表 37-3　　物理供应商类型值 （续）

无负载加密的 5515 思科自适应安全设备的中央处理器温度传感器	cevSensorASA5515K7CPUTemp (cevSensor 103)
无负载加密的 5515 自适应安全设备的机箱冷却风扇传感器	cevSensorASA5515K7PSFanSensor (cevSensor 115)
5515 自适应安全设备的机箱冷却风扇传感器	cevSensorASA5515PSFanSensor (cevSensor 118)
5525 思科自适应安全设备 (ASA) 机箱风扇传感器	cevSensorASA5525ChassisFanSensor (cevSensor 122)
5525 思科自适应安全设备的机箱环境温度传感器	cevSensorASA5525ChassisTemp (cevSensor 108)
5525 思科自适应安全设备的中央处理器温度传感器	cevSensorASA5525CPUTemp (cevSensor 99)
无负载加密的 5525 思科自适应安全设备 (ASA) 机箱风扇传感器	cevSensorASA5525K7ChassisFanSensor (cevSensor 127)
无负载加密的 5525 思科自适应安全设备的中央处理器温度传感器	cevSensorASA5525K7CPUTemp (cevSensor 104)
无负载加密的 5525 自适应安全设备的机箱冷却风扇传感器	cevSensorASA5525K7PSFanSensor (cevSensor 114)
5525 自适应安全设备的机箱冷却风扇传感器	cevSensorASA5525PSFanSensor (cevSensor 117)
5545 思科自适应安全设备 (ASA) 机箱风扇传感器	cevSensorASA5545ChassisFanSensor (cevSensor 123)
5545 思科自适应安全设备的机箱环境温度传感器	cevSensorASA5545ChassisTemp (cevSensor 109)
5545 思科自适应安全设备的中央处理器温度传感器	cevSensorASA5545CPUTemp (cevSensor 100)
无负载加密的 5545 思科自适应安全设备 (ASA) 机箱风扇传感器	cevSensorASA5545K7ChassisFanSensor (cevSensor 128)
无负载加密的 5545 思科自适应安全设备的机箱环境温度传感器	cevSensorASA5545K7ChassisTemp (cevSensor 90)
无负载加密的 5545 思科自适应安全设备的中央处理器温度传感器	cevSensorASA5545K7CPUTemp (cevSensor 105)
无负载加密的 5545 自适应安全设备的机箱冷却风扇传感器	cevSensorASA5545K7PSFanSensor (cevSensor 113)
无负载加密的 5545 自适应安全设备的电源输入状态传感器	cevSensorASA5545K7PSPresence (cevSensor 87)
无负载加密的 5545 自适应安全设备的电源风扇温度传感器	cevSensorASA5545K7PSTempSensor (cevSensor 94)
无负载加密的 5545 自适应安全设备的电源风扇传感器	cevSensorASA5545PSFanSensor (cevSensor 89)
5545 自适应安全设备的电源输入状态传感器	cevSensorASA5545PSPresence (cevSensor 130)
5555 自适应安全设备的电源输入状态传感器	cevSensorASA5545PSPresence (cevSensor 131)
5545 自适应安全设备的电源风扇温度传感器	cevSensorASA5545PSTempSensor (cevSensor 92)
5555 思科自适应安全设备 (ASA) 机箱风扇传感器	cevSensorASA5555ChassisFanSensor (cevSensor 124)
5555 思科自适应安全设备的机箱环境温度传感器	cevSensorASA5555ChassisTemp (cevSensor 110)
5555 思科自适应安全设备的中央处理器温度传感器	cevSensorASA5555CPUTemp (cevSensor 101)
无负载加密的 5555 思科自适应安全设备 (ASA) 机箱风扇传感器	cevSensorASA5555K7ChassisFanSensor (cevSensor 129)
无负载加密的 5555 思科自适应安全设备的机箱环境温度传感器	cevSensorASA5555K7ChassisTemp (cevSensor 111)
无负载加密的 5555 思科自适应安全设备的中央处理器温度传感器	cevSensorASA5555K7CPUTemp (cevSensor 106)
无负载加密的 5555 自适应安全设备的机箱冷却风扇传感器	cevSensorASA5555K7PSFanSensor (cevSensor 112)
无负载加密的 5555 自适应安全设备的电源输入状态传感器	cevSensorASA5555K7PSPresence (cevSensor 88)

表 37-3　　物理供应商类型值 （续）

无负载加密的 5555 自适应安全设备的电源风扇温度传感器	cevSensorASA5555K7PSTempSensor (cevSensor 95)
5555 自适应安全设备的电源风扇传感器	cevSensorASA5555PSFanSensor (cevSensor 91)
5555 自适应安全设备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)
5555-X 自适应安全设备现场可更换固态驱动器	cevModuleASA5555XFRSSD (cevModuleCommonCards 396)
5545-X 自适应安全设备现场可更换固态驱动器	cevModuleASA5545XFRSSD (cevModuleCommonCards 397)
5525-X 自适应安全设备现场可更换固态驱动器	cevModuleASA5525XFRSSD (cevModuleCommonCards 398)
5515-X 自适应安全设备现场可更换固态驱动器	cevModuleASA5515XFRSSD (cevModuleCommonCards 399)
5512-X 自适应安全设备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

下表列出对指定 MIB 支持的表和对象。

表 37-4　　MIB 中受支持的表和对象

MIB 名称	支持的表和对象
CISCO-ENHANCED-MEMPOOL-MIB	cempMemPoolTable、 cempMemPoolIndex、 cempMemPoolType、 cempMemPoolName、 cempMemPoolAlternate、 cempMemPoolValid、 cempMemPoolUsed、 cempMemPoolFree、 cempMemPoolUsedOvrflw、 cempMemPoolHCUsed、 cempMemPoolFreeOvrflw、 cempMemPoolHCFree
CISCO-ENTITY-SENSOR-EXT-MIB **备注**　在适用于 Catalyst 6500 交换机/7600 路由器的 ASA 服务模块上不支持。	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB **备注**　在思科自适应安全虚拟设备 (ASAv) 上不支持。	ctsxSxpGlobalObjects、 ctsxSxpConnectionObjects、 ctsxSxpSgtObjects

表 37-4 MIB 中受支持的表和对象 （续）

DISMAN-EVENT-MIB	mteTriggerTable、 mteTriggerThresholdTable、 mteObjectsTable、 mteEventTable、 mteEventNotificationTable
DISMAN-EXPRESSION-MIB **备注** 在适用于 Catalyst 6500 交换机/7600 路由器的 ASA 服务模块上不支持。	expExpressionTable、 expObjectTable、 expValueTable
ENTITY-SENSOR-MIB **备注** 在适用于 Catalyst 6500 交换机/7600 路由器的 ASA 服务模块上不支持。	entPhySensorTable
NAT-MIB	natAddrMapTable、 natAddrMapIndex、 natAddrMapName、 natAddrMapGlobalAddrType、 natAddrMapGlobalAddrFrom、 natAddrMapGlobalAddrTo、 natAddrMapGlobalPortFrom、 natAddrMapGlobalPortTo、 natAddrMapProtocol、 natAddrMapAddrUsed、 natAddrMapRowStatus

支持的陷阱 （通知）

下表列出支持的陷阱 （通知）及其关联 MIB。

表 37-5 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。
ccmCLIRunningConfigChanged (CISCO-CONFIG-MAN-MIB)	-	**snmp-server enable traps config** 命令用于启用此陷阱的传输。
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)	-	**snmp-server enable traps entity fru-insert** 命令用于启用此通知。此陷阱不适用于 ASA 5506-X 和 ASA 5508-X。
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)	-	**snmp-server enable traps entity fru-remove** 命令用于启用此通知。此陷阱不适用于 ASA 5506-X 和 ASA 5508-X。

表 37-5 支持的陷阱（通知）（续）

ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB) **备注** 在适用于 Catalyst 6500 交换机/7600 路由器的 ASA 服务模块上不支持。	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。系统会针对电源故障发送此通知。所发送的对象会识别风扇和 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。此陷阱不适用于 ASA 5506-X 和 ASA 5508-X。 **snmp-server enable traps entity power-supply-failure** 命令用于启用电源故障陷阱的传输。此陷阱不适用于 ASA 5506-X 和 ASA 5508-X。 **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。此陷阱不适用于 ASA 5506-X 和 ASA 5508-X。 **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。此陷阱不适用于 ASA 5506-X 和 ASA 5508-X。 **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。此陷阱不适用于 ASA 5506-X 和 ASA 5508-X。 **snmp-server enable traps entity chassis-temperature** 命令用于启用机箱环境温度陷阱的传输。 **snmp-server enable traps entity accelerator-temperature** 命令用于启用机箱加速器温度陷阱的传输。此陷阱不适用于 ASA 5506-X 和 ASA 5508-X。
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。
ciscoConfigManEvent (CISCO-CONFIG-MAN-MIB)	-	**snmp-server enable traps config** 命令用于启用此陷阱的传输。

表 37-5 支持的陷阱（通知）（续）

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。
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。 **备注** 仅当创建或删除了安全情景时，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。

表 37-5　　支持的陷阱（通知）（续）

mteTriggerFired (DISMAN-EVENT-MIB) **备注**　在适用于 Catalyst 6500 交换机/7600 路由器的 ASA 服务模块上不支持。	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。
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：

- 逻辑 - 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。
- 物理 - 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。

注意　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 计数器会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。

下表中的示例显示 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。示例表明统计信息接近于为 **show traffic** 命令显示的输出。

表 37-6 物理接口和 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 版或第 2c 版中没有的安全增强功能。SNMP 第 1 版和第 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，此版本通过基于用户的安全模式 (USM) 和基于视图的访问控制模式 (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。

安全模式

为进行配置，身份验证和隐私选项会共同组成安全模式。安全模式应用于用户和组，它们分为以下三种类型：

- NoAuthPriv - 无身份验证且无隐私，意味着未对消息应用安全设置。
- 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 组配置有安全模式，并与 SNMP 视图关联。SNMP 组内的用户必须与 SNMP 组的安全模式匹配。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/安全模式对必须唯一。

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式。

SNMP 主机

SNMP 主机是 SNMP 通知和陷阱所发送到的 IP 地址。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。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。
- 您必须使用正确的安全模式创建用户和组。
- 您必须按正确的顺序删除用户、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》。

备注　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

本节介绍您在配置 SNMP 之前应查看的准则和限制。

故障切换准则

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。

其他准则

- 您必须具有 Cisco Works for Windows 或其他符合 SNMP MIB-II 标准的浏览器才能接收 SNMP 陷阱或浏览 MIB。
- 不支持基于视图的访问控制，但是 VACM MIB 可供浏览以确定默认视图设置。
- 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，您必须确保删除与该组关联的所有用户。
- 在删除用户之前，您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式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：
  - 从该组中删除用户。
  - 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，您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。
- 您最多可以添加 4000 台主机。但是，其中仅 128 台可用于陷阱。
- 支持的活动轮询目标总数为 128。
- 您可以指定网络对象以指示要添加为主机组的个别主机。
- 您可以将多个用户与一台主机关联。
- 您可以在不同的 **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会对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，则系统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。
- 集群成员不会同步其 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。
- 对版本 9.4(1)， ASA 支持每个情景使用无限数量的 SNMP 服务器陷阱主机。 **show snmp-server host** 命令输出仅显示轮询 ASA 的活动主机以及静态配置的主机。

故障排除提示

- 要确保接收来自 NMS 的传入数据包的 SNMP 进程，请输入以下命令：

```
ciscoasa(config)# show process | grep snmp
```

- 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
```

- 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。

- 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，如要帮助重现错误，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，您可能还需要使用 **icmp permit** 命令允许来自远程 SNMP 服务器的 ICMP 流量。
- 有关更多故障排除信息，请参阅以下 URL：
http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116423-troubleshoot-asa-snmp.html

配置 SNMP

本节介绍如何配置 SNMP。

步骤 1 启用 SNMP 代理和 SNMP 服务器。请参阅启用 SNMP 代理和 SNMP 服务器。，第 37-20 页。

步骤 2 配置 SNMP 陷阱。请参阅配置 SNMP 陷阱，第 37-21 页。

步骤 3 配置 SNMP 第 1 版和第 2c 版参数或 SNMP 第 3 版参数。请参阅配置 SNMP 第 1 版或第 2c 版的参数，第 37-23 页或配置 SNMP 第 3 版的参数，第 37-24 页。

启用 SNMP 代理和 SNMP 服务器。

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，SNMP 服务器已启用。

```
snmp-server enable
```

示例：

```
ciscoasa(config)# snmp-server enable
```

配置 SNMP 陷阱

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*] | **config** | **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* |*accelerator-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。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。您需要同时配置 **logging history** 命令和 **snmp-server enable traps syslog** 命令来从系统日志 MIB 生成陷阱。要恢复 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**

备注　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。

在单一模式下，所有其他陷阱在管理情景和用户环境中都可用。

在多情景模式下，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）。

accelerator-temperature 阈值陷阱仅适用于 ASA 5506-X 和 ASA 5508-X。

chassis-fan-failure 陷阱不适用于 ASA 5506-X。

config 陷阱启用 ciscoConfigManEvent 通知和 ccmCLIRunningConfigChanged 通知，在退出配置模式后会生成这些通知。

以下陷阱不适用于 ASA 5506-X 和 ASA 5508-X：**fan-failure**、 **fru-insert**、 **fru-remove**、 **power-supply**、 **power-supply-failure**、 **power-supply-presence** 和 **power-supply-temperature**。

如果 CPU 使用率大于所配置监控期的所配置阈值，则系统会生成 **cpu threshold rising** 陷阱。

当已用系统情景内存达到总系统内存的 80% 时，系统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。

注意 SNMP 不监控电压传感器。

配置 CPU 使用率阈值

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
```

要清除 CPU 利用率的阈值和监控期，请使用此命令的 **no** 形式。如果未配置 **snmp cpu threshold rising** 命令，则高阈值级别的默认值会超过 70%，临界阈值级别的默认值会超过 95%。默认监控期设置为 1 分钟。

临界 CPU 阈值级别始终保持在 95%，无法配置。高 CPU 阈值的有效阈值范围为 10% 到 94%。监控期的有效值范围为 1 到 60 分钟。

配置物理接口阀值

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%
```

要清除 SNMP 物理接口的阈值，请使用此命令的 **no** 形式。阈值定义为接口带宽利用率的百分比。有效阈值范围为 30% 到 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。

注意 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 版或第 2c 版的参数

要配置 SNMP 第 1 版或第 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，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 关键字可将 NMS 限制为仅接收陷阱。**poll** 关键字可将 NMS 限制为仅发送请求（轮询）。默认情况下， SNMP 陷阱已启用。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，您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。在使用加密的社区字符串后，对所有系统（例如 CLI、ASDM、CSM 等）仅显示加密的形式。明文密码不可见。加密的社区字符串始终由 ASA 生成；您输入的一般是明文形式。

备注　如果从版本 8.3(1) 降级到 ASA 软件的更低版本并且已配置加密密码，则必须先使用 **no key config-key password encryption** 命令将加密的密码恢复为明文，然后保存结果。

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 版或第 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，最多可包含 127 个字符。接受空格，但多个空间缩为一个空格。

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。如果在当前使用中的端口上配置 **snmp-server listen-port** 命令，系统将显示以下消息：

警告　其他功能正在使用 UDP 端口 *port*。在将 snmp-server listen-port 命令配置为使用其他端口前，向设备发送 SNMP 请求会失败。

现有 SNMP 线程会持续轮询 （每 60 秒一次），直到端口可用，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

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，系统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 版的安全模式，一个表示第 2 版的安全模式。有关安全模式的详细信息，请参阅安全模式，第 37-16 页。**auth** 关键字可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** 关键字可启用数据包加密和身份验证。**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** 关键字指定应使用 SNMP 第 3 版安全模式并允许使用 **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形式。**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。

注意　如果忘记密码，则无法将其恢复，必须重新配置用户。您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 （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，我们建议使用至少 8 个字母数字字符。

在集群中，您必须手动为 SNMPv3 用户更新每个集群的 ASA。您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。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*** | ***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 关键字可将 NMS 限制为仅接收陷阱。**poll** 关键字可将 NMS 限制为仅发送请求（轮询）。默认情况下，SNMP 陷阱已启用。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，您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。在使用加密的社区字符串后，对所有系统（例如 CLI、ASDM、CSM 等）仅显示加密的形式。明文密码不可见。加密的社区字符串始终由 ASA 生成；您输入的一般是明文形式。

注意　如果从版本 8.3(1) 降级到 ASA 软件的更低版本并且已配置加密密码，则必须先使用 **no key config-key password encryption** 命令将加密的密码恢复为明文，然后保存结果。

version 关键字指定 SNMP 陷阱版本。ASA 不支持基于 SNMP 请求的筛选 （轮询）。

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 SNMP 主机，第 37-17 页。

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，最多可包含 127 个字符。接受空格，但多个空间缩为一个空格。

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。如果在当前使用中的端口上配置 **snmp-server listen-port** 命令，系统将显示以下消息：

警告　**其他功能正在使用 UDP 端口 *port*。在将 snmp-server listen-port 命令配置为使用其他端口前，向设备发送 SNMP 请求会失败。**

现有 SNMP 线程会持续轮询 （每 60 秒一次），直到端口可用，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

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以配置的用户。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。用户列表必须具有多个用户，并且能与主机名或 IP 地址范围关联。

将用户与网络对象相关联

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。您只能将此关键字用于 SNMP 第 1 版或第 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。社区字符串最多可以包含 32 个字符。**version** 关键字可将 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 SNMP 第 3 版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，SNMP 陷阱已启用。

监控 SNMP

请参阅以下用于监控 SNMP 的信息的额命令：

- **show running-config snmp-server** [**default**]

  此命令可显示所有 SNMP 服务器配置信息。
- **show running-config snmp-server group**

  此命令可显示 SNMP 组配置设置。
- **show running-config snmp-server host**

  此命令可显示供 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**

  此命令可显示 SNMP 主机组配置。
- **show running-config snmp-server user**

  此命令可显示 SNMP 基于用户的配置设置。
- **show running-config snmp-server user-list**

  此命令可显示 SNMP 用户列表配置。

- **show snmp-server engineid**

  此命令可显示所配置的 SNMP 引擎的 ID。

- **show snmp-server group**

  此命令可显示已配置的 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**

  此命令可显示已配置的 SNMP 服务器特征。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**

  此命令可显示已配置的用户特征。

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 的示例

下节提供了可用作所有 SNMP 版本的参考的示例。

SNMP 第 1 版和第 2c 版

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

以下示例显示 ASA 如何能够使用 SNMP 第 3 版安全模式接收 SNMP 请求，该安全模式要求按以下顺序进行配置：组、用户、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 37-7 SNMP 历史记录

功能名称	平台版本	说明
SNMP 第 1 版和第 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式 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征。此外，此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。 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。 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。 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 将设置为已为接口说明设置的值。

表 37-7 SNMP 历史记录 （续）

功能名称	平台版本	说明
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.
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**。 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)	最多可以添加 4000 台主机。支持的活动轮询目标数量为 128。您可以指定网络对象以指示要添加为主机组的个别主机。您可以将多个用户与一台主机关联。 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。

表 37-7 SNMP 历史记录 （续）

功能名称	平台版本	说明
SNMP OID 和 MIB	9.2(1)	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。
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 ASA 5506-X。 ASA 5506-X 已作为新产品添加到 SNMP sysObjectID OID 表和 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的命令。 • 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。 修改了以下命令：**snmp-server enable traps**。
SNMP MIB 和陷阱	9.4(1)	ASA 5506W-X、ASA 5506H-X、ASA 5508-X、和 ASA 5516-X 已经作为新产品添加到 SNMP sysObjectID OID 表和 entPhysicalVendorType OID 表中。
每个情景的 SNMP 服务器陷阱主机数没有限制	9.4(1)	ASA 支持每个情景使用无限数量的 SNMP 服务器陷阱主机。**show snmp-server host** 命令输出仅显示正在轮询 ASA 的活动主机，以及静态配置的主机。 修改了以下命令：**show snmp-server host**。



Anonymous Reporting 和 Smart Call Home

本章介绍如何配置 Anonymous Reporting 和 Smart Call Home 服务。

- 关于 Anonymous Reporting，第 38-1 页
- 关于 Smart Call Home，第 38-2 页
- Anonymous Reporting 和 Smart Call Home 准则，第 38-6 页
- 配置 Anonymous Reporting 和 Smart Call Home，第 38-7 页
- 监控 Anonymous Reporting 和 Smart Call Home，第 38-17 页
- Smart Call Home 的示例，第 38-17 页
- Anonymous Reporting 和 Smart Call Home 的历史记录，第 38-18 页

关于 Anonymous Reporting

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，并且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 Web 服务器上存在的服务器证书并建立 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。

备注 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 要求

必须正确配置 DNS 服务器， ASA 才能访问 Cisco 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以下任务来配置 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，思科将通过提供以下服务，对系统配置问题、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。

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。
- 查看所有支持 Smart Call Home 的设备的最新资产和配置信息。

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

- 资产
- 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。
- 可以订用特定警报组。
- 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，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。
- 可以配置快照警报组，以便发送所指定的 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。

资产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、许可密钥和相关运行时间数据。
- **show inventory** - 检索并显示网络设备中安装的每款思科产品的相关资产信息。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** - 显示故障切换对中的两个装置的故障切换状态。显示的信息包括设备的主要或辅助状态、设备的主用/备用状态以及最新报告的故障切换原因。
- **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切换状态的信息。
- **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。

快照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 所存储的相应介质会话数。
- **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

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。

下表显示消息严重性级别和系统日志严重性级别之间的对应关系。

表 38-1　　消息严重性级别和系统日志级别之间的对应关系

功率水平	消息严重级别	系统日志严重级别	说明
9	巨大灾难	N/A	全网范围的灾难性故障。
8	灾难	N/A	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。严重情况；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	严重。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	警告	4	警告情况。
2	通知	5	基本通知和信息消息。可能是独立的无关紧要情况。
1	正常状态	6	信息。正常事件，表示恢复正常状态。
0	除错	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被触发时，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：

- 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。
- 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。
- 可以指定最大消息大小。默认为 3 MB。

已提供一个默认配置文件 “Cisco TAC”。默认配置文件包含一组要监控的预定义组 （诊断、环境、资产、配置和遥测）以及预定义的目标邮件地址和 HTTPS URL。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。

备注 无法更改默认配置文件的目标邮件地址或目标 URL。

在使目标配置文件订用配置、资产、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。

下表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 38-2　警报组到严重性级别订用的映射

警报组	严重级别	时间段
配置	参考	每月
诊断	信息及更高级别	N/A
环境	通知及更高级别	N/A
库存	参考	每月
快照	参考	N/A
系统日志	等效系统日志	N/A
遥感勘测	参考	每天
测试	N/A	N/A
威胁	通知	N/A

Anonymous Reporting 和 Smart Call Home 准则

本节介绍在配置 Anonymous Reporting 和 Smart Call Home 之前应查看的准则和限制。

Anonymous Reporting 准则

- 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，然后才丢弃该消息。
- 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 Smart Call Home 将保持禁用状态，即使在 Anonymous Reporting 启用后也是如此。
- 如果 Anonymous Reporting 处于启用状态，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，则可以删除信任点，但禁用 Anonymous Reporting 不会导致删除信任点。
- 如果使用的是多情景模式配置，则 **dns**、 **interface** 和 **trustpoint** 命令处于管理情景中，而 **call-home** 命令处于系统情景中。

Smart Call Home 准则

- 在多情景模式下， **subscribe-to-alert-group snapshot periodic** 命令划分成两条命令：一条命令用于从系统配置中获取信息，另一条命令用于从用户情景中获取信息。
- Smart Call Home 后台服务器只能接受 XML 格式的消息。

- 如果已启用集群功能，并且已将 Smart Call Home 配置为订用严重性级别为 “严重” 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

- DNS 要求，第 38-2 页
- 配置 DNS 服务器，第 16-13 页

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 能够监控设备，并且在存在问题时 （通常在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，可以选择 [Y]（是）、[N]（否）或 [A]（稍后询问）。如果选择 [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，则可以执行配置 Anonymous Reporting，第 38-7 页或配置 Smart Call Home，第 38-8 页中的步骤来启用 Anonymous Reporting 或 Smart Call Home。

配置 Anonymous Reporting

要配置 Anonymous Reporting，请执行以下步骤：

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 Web 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。请参阅启用 Smart Call Home，第 38-8 页。

步骤 2　配置用于将 Smart Call Home 消息传递给用户的邮件服务器。请参阅配置邮件服务器，第 38-12 页。

步骤 3　为 Smart Call Home 消息设置联系人信息。请参阅配置客户联系信息，第 38-11 页。

步骤 4　定义警报处理参数，例如可以处理的最大事件率。请参阅配置警报组订用，第 38-10 页。

步骤 5　设置警报订用配置文件。请参阅配置目标配置文件，第 38-14 页。

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。
- 要针对其接收警报的信息类别，例如配置或资产信息。

启用 Smart Call Home

要启用 Smart Call Home 并激活报障配置文件，请执行以下步骤：

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，则需要将 ASA 配置为信任该 Web 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。

备注　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。

要声明思科服务器安全认证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，请执行以下步骤：

操作步骤

步骤 1　（仅限多情景模式）在管理情景中安装证书。

changeto context *admincontext*

示例：

```
ciscoasa(config)# changeto context contextA
```

步骤 2　配置信任点并为认证登记作准备。

crypto ca trustpoint *trustpoint-name*

示例：

```
ciscoasa(config)# crypto ca trustpoint cisco
```

注意　如果使用 HTTP 作为传输方法，则必须通过信任点安装 HTTPS 所需的安全认证。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认证登记。

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，粘贴安全认证文本。

crypto ca authenticate *trustpoint*

示例：

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

步骤 5　指定安全认证文本结束，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]:
```

是

配置环境警报组和快照警报组

要配置环境警报组和快照警报组，请执行以下步骤：

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

要使目标配置文件订用警报组，请执行以下步骤：

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

要配置客户联系信息，请执行以下步骤：

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，地址是长度最多为 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 的长度最多为 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　指定思科客户 ID，此 ID 的长度最多为 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 的长度最多为 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

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。

要配置邮件服务器，请执行以下步骤：

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
```

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

要配置流量速率限制，请执行以下步骤：

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

要发送特定 Smart Call Home 通信，请执行以下步骤：

操作步骤

步骤 1　选择以下选项之一：

选项 1 - 使用配置文件配置来手动发送测试消息。

call-home test [*test-message*] **profile** *profile-name*

示例：

```
ciscoasa# call-home test [testing123] profile CiscoTAC-1
```

选项 2 - 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，则向订用了资产、配置、快照或遥测警报组的所有配置文件发送消息。

call-home send alert-group {**inventory** | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*]

示例：

```
ciscoasa# call-home send alert-group inventory
```

选项 3 - 将命令输出发送到邮件地址。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

要配置目标配置文件以进行邮件或 HTTP 传输，请执行以下步骤：

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
```

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 后台服务器，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。

要将传输方法设置为 HTTP，请参阅启用 Smart Call Home，第 38-8 页。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

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，请执行以下步骤：

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
```

重命名目标配置文件

要更改现有配置文件的名称，请执行以下步骤：

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

以下示例显示如何重命名现有配置文件：

```
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

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

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 的历史记录

表 38-3 Anonymous Reporting 和 Smart Call Home 的历史记录

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。 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)	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。 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 配置为订用严重性级别为 “严重”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 9 部分

参考



第 39 章

使用命令行界面

本章介绍如何在思科 ASA 上使用 CLI。

- 防火墙模式和安全情景模式，第 39-1 页
- 命令模式和提示，第 39-2 页
- 语法格式，第 39-3 页
- 缩写命令，第 39-3 页
- 命令行编辑，第 39-3 页
- 命令补全，第 39-3 页
- 命令帮助，第 39-3 页
- 查看运行配置，第 39-4 页
- 筛选 show 和 more 命令输出，第 39-4 页
- 命令输出分页，第 39-5 页
- 添加注释，第 39-5 页
- 文本配置文件，第 39-5 页
- 支持的字符集，第 39-7 页

备注 CLI 使用类似于思科 IOS CLI 的语法和其他约定，但是 ASA 操作系统不是思科 IOS 软件版本。请勿假定思科 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：

- 透明防火墙或路由防火墙模式

  防火墙模式确定 ASA 是作为第 2 层还是第 3 层防火墙运行。

- 多情景模式或单情景模式

  安全情景模式确定 ASA 是作为单个设备还是作为多个安全情景 （作用类似虚拟设备）运行。

有些命令仅在特定模式下可用。

命令模式和提示

ASA CLI 包含各种命令模式。有些命令只能在特定模式下输入。例如，要输入显示敏感信息的命令，您需要输入密码并进入具有更多特权的模式。然后，为确保不会意外输入配置更改，必须进入配置模式。所有较低的命令均可在较高模式下输入。例如，可以在全局配置模式下输入特权 EXEC 命令。

备注　各种类型的提示全部是默认提示，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，提示以主机名开头：

  ```
  ciscoasa
  ```

- 列显提示字符串时，系统会解析提示配置并按照设置 **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意项并且可采用任意顺序：主机、域、情景、优先级、状态。

  ```
  ciscoasa(config)# prompt hostname context priority state
  ```

- 如果您在某一情景中，则提示以主机名开头，后跟情景名称：

  ```
  ciscoasa/context
  ```

提示根据访问模式而异：

- 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均可用。在特权 EXEC 模式下输入 **configure terminal** 命令可启动全局配置模式。提示将更改为以下形式：

  ```
  ciscoasa(config)#

  ciscoasa/context(config)#
  ```

- 命令特定配置模式

  从全局配置模式下，某些命令可进入命令特定配置模式。所有用户 EXEC、特权 EXEC、全局配置和命令特定配置命令在此模式下均可用。例如， **interface** 命令会进入接口配置模式。提示将更改为以下形式：

  ```
  ciscoasa(config-if)#

  ciscoasa/context(config-if)#
  ```

语法格式

命令语法说明采用下表所列的约定。

表 39-1　　语法约定

约定	描述
粗体	粗体文本指示按字面显示输入的命令和关键字。
斜体	斜体文本指示由您提供值的参数。
[x]	方括号中包含可选元素 （关键字或参数）。
|	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

您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** （而不是输入完整命令 **write terminal**）查看配置，或者可以输入 **en** 启动特权模式并输入 **conf t** 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 使用与思科 IOS 软件相同的命令行编辑约定。您可以使用 **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。检查以前输入的命令后，您可以使用向下箭头或 **^n** 命令在列表中前移。到达想要重新使用的命令后，您可以编辑该命令或按 **Enter** 键启动该命令。您也可以使用 **^w** 删除光标左侧的字词，或使用 **^u** 删除该行。

ASA 在一条命令中最多允许 512 个字符；额外字符会被忽略。

命令补全

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 **+?**。

备注　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

要查看运行配置，请使用以下其中一个选项：

- **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。

  注意　许多关键字都显示为 *****。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

配置主密码，第 16-10 页

筛选 show 和 more 命令输出

您可以将竖线 (|) 用于任何 **show** 命令并包含过滤器选项和筛选表达式。与思科 IOS 软件类似，通过将各输出行与正则表达式匹配来执行筛选。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。

将筛选选项与 **show** 命令配合使用的语法如下：

```
ciscoasa# show command | {include | exclude | begin | grep [-v]} regexp
```

或

```
ciscoasa# more system:running-config | {include | exclude | begin | grep [-v]} regexp
```

备注　通过输入 **more** 命令，您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** 选项具有相同的效果。**exclude** 选项排除匹配正则表达式的所有输出行。带 **-v** 的 **grep** 选项具有相同的效果。**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* 替换为任何思科 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** 可转义 CLI 中的所有特殊字符，如问号 (?) 或制表符。例如，键入 **d[Ctrl+V]?g** 以在配置中输入 **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，您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，您可以选择在 More 提示出现之前要显示的行数。

启用分页后，会出现以下提示：

```
<--- More --->
```

More 提示使用类似于 UNIX **more** 命令的语法：

- 按**空格**键可查看其他屏幕。
- 按 **Enter** 键可查看下一行。
- 按 **q** 键可返回到命令行。

添加注释

您可以在某一行之前前置冒号 (:) 来创建注释。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，您可以使用 **show history** 命令或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， **write terminal** 命令不会显示注释。

文本配置文件

本节介绍如何格式化可以下载到 ASA 的文本配置文件。

- 命令与文本文件中的行的对应方式，第 39-6 页
- 命令特定配置模式命令，第 39-6 页
- 自动文本条目，第 39-6 页
- 行顺序，第 39-6 页
- 文本配置中未包含的命令，第 39-6 页
- 密码，第 39-6 页
- 多个安全情景文件，第 39-7 页

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所述命令对应的行。

在示例中，命令之前前置有 CLI 提示。以下示例中的提示为 “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：

```
context a
```

命令特定配置模式命令

命令特定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，您必须先为接口输入 **nameif** 命令，因为许多后续命令都使用该接口的名称。此外，命令特定配置模式下的命令必须紧跟在主命令之后。

文本配置中未包含的命令

有些命令不会在配置中插入行。例如， **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、启用和用户密码存储在配置中之前会自动加密。例如，密码 “cisco”的加密形式可能类似于 jMorNbK0514fadBh。您可以将配置密码以其加密形式复制到另一个 ASA，但是无法自行解密密码。

如果您在文本文件中输入了未加密的密码，则 ASA 不会在您将配置复制到 ASA 时将其自动加密。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。

多个安全情景文件

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，用于确定 ASA 的基本设置，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，它会使用指定为管理情景的情景。

每个情景都类似于一个单情景模式配置。系统配置与情景配置的不同之处在于，系统配置仅包含系统命令 （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 字符在 UTF-8 中表示为单字节字符。所有其他字符在 UTF-8 中均表示为多字节符号。

完全支持 ASCII 可打印字符 （0x20 到 0x7e）。可打印的 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 (0-255) 与 ISO 8859-1 相同。ASA CLI 最多支持 255 个 ISO 8859-1 字符 （多字节字符）。



地址、协议和端口

本章提供有关 IP 地址、协议和应用的快速参考。

- IPv4 地址和子网掩码，第 40-1 页
- IPv6 地址，第 40-4 页
- 协议和应用，第 40-9 页
- TCP 和 UDP 端口，第 40-10 页
- 本地端口和协议，第 40-13 页
- ICMP 类型，第 40-14 页

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 地址的第一个部分标识主机所在的网络，而第二个部分标识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都共享同一网络前缀，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 主机地址划分为三个不同的地址类：A 类、 B 类和 C 类。每个类在 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 至 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 至 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 至 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 个主机，因此您可以使用子网掩码将这些庞大的网络分为较小的子网。

专用网络

如果在网络上需要大量地址，但不需要在互联网上路由这些地址，则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，您可以将单个 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 类扩展网络前缀还使用第四个八位组的一部分。

如果使用二进制表示法而不是点分十进制表示法，则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，则该位会设置为 1。
- 如果该位是主机号的一部分，则会设置为 0。

示例 1：如果您有 B 类地址 129.10.0.0，并要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。该子网掩码将此 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：如果您只想将第三个八位组的一部分用于扩展网络前缀，则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。

您可以将子网掩码编写为点分十进制掩码或 */位数*（“斜杠 *位数*”）掩码。在示例 1 中，对于点分十进制掩码，您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。

您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 类网络构建成一个更大的超网。例如， 192.168.0.0/20。

确定子网掩码

请参阅下表以根据所需的主机数来确定子网掩码。

备注　子网的第一个和最后一个数字已保留，但 /32 除外，该数字用于标识单个主机。

表 40-1　　主机数、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 40-1　主机数、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 类规模和 B 类规模网络的子网掩码配合使用的网络地址。

C 类规模网络地址

对于主机数介于 2 和 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，下表显示 192.168.0.x 的 8 主机子网 (/29)。

备注　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 40-2　C 类规模网络地址

掩码为 /29 的子网 (255.255.255.248)	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 类规模网络地址

要确定将与主机数在 254 和 65,534 之间的网络的子网掩码配合使用的网络地址，您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。

要确定第三个八位组的值，请按照以下步骤操作：

步骤 1　通过用 65,536 （使用第三个和第四个八位组的地址的总数）除以所需的主机地址数，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 类规模网络上。

步骤 2　通过用 256 （第三个八位组值的数量）除以子网数量，确定第三个八位组值的倍数：

在本示例中， 256/16 = 16。

第三个八位组是 16 的倍数，从 0 开始。

下表显示网络 10.1 的 16 个子网。

备注　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 40-3　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

配置 IPv6 寻址，第 13-12 页

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

备注　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 可以通过删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。其中的数字全部为零的字段 （从左侧数起的第三和第四个字段）缩减为一个零。从左侧数起的第五个字段删除了三个前导零，仅留下了一个 8，从左侧数起的第六个字段删除了一个前导零，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 地址开头、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）。下表显示若干不同类型的 IPv6 地址的地址压缩示例。

表 40-4　　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	::

备注　两个冒号 (::) 在 IPv6 地址中只能使用一次，用以表示连续的零字段。

在处理同时包含 IPv4 和 IPv6 地址的环境时，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标识的接口。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标识的所有地址。
- **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）。

备注　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。单播地址用于标识网络节点上的接口。

全局地址

IPv6 全局单播地址的通用格式是全局路由前缀后跟子网 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。例如，具有嵌入式 IPv4 地址的 IPv6 地址即是此类型的地址。

相关主题

- IPv6 地址前缀，第 40-9 页
- 接口标识符，第 40-7 页
- 与 IPv4 兼容的 IPv6 地址，第 40-6 页

站点本地地址

站点本地地址用于在站点内寻址。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，可将站点本地地址视为专用地址。

链路本地地址

所有接口都需要有至少一个链路本地地址。您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，可将链路本地地址视为专用地址。

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。

备注　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，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。

备注　不能将未指定 IPv6 地址分配给接口。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 可由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。

备注　不能将 IPv6 环回地址分配给物理接口。将 IPv6 环回地址用作其源地址或目标地址的数据包必须保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必须是唯一的。在许多情况下，接口标识符派生自接口链路层地址。同一接口标识符可用于一个节点的多个接口上，只要这些接口连接到不同子网即可。

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。

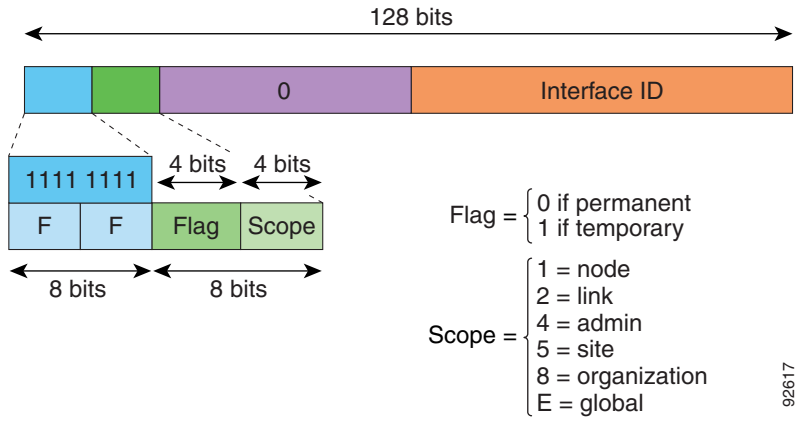
例如，具有 MAC 地址 00E0.b601.3B7A 的接口将会有一个 64 位接口 ID 02E0:B6FF:FE01:3B7A。

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标识的所有接口。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（公认）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。下图显示 IPv6 组播地址的格式。

图 40-1　　IPv6 组播地址格式



IPv6 节点 （主机和路由器）需要加入以下组播组：

- 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。

注意　请求节点地址用于邻居请求消息中。

IPv6 路由器需要加入以下组播组：

- FF01::2 （接口本地）
- FF02::2 （链路本地）
- FF05::2 （站点本地）

组播地址不应用作 IPv6 数据包中的源地址。

备注　IPv6 中没有广播地址。系统使用 IPv6 组播地址而非广播地址。

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标识为任播地址。

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。

备注　ASA 上不受支持任播地址。

必需地址

IPv6 主机必须至少配置有以下地址 （自动或手动）：

- 每个接口的链路本地地址
- 环回地址
- 全节点组播地址
- 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）：

- 必需主机地址
- 用于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 （格式为 ipv6 前缀/前缀长度）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，其中地址以十六进制的 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）的地址高位连续位的数量。例如，2001:0DB8:8086:6502::/32 是有效的 IPv6 前缀。

IPv6 前缀标识 IPv6 地址的类型。下表显示每个 IPv6 地址类型的前缀。

表 40-5　　IPv6 地址类型前缀

地址类型	二进制前缀	IPv6 表示法
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。	
任意播	取自单播地址空间。	

协议和应用

下表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 40-6　　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 40-6　　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 嵌套封装。
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 ppp 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。

您可以在 IANA 网站上在线查看协议号：

http://www.iana.org/assignments/protocol-numbers

TCP 和 UDP 端口

下表列出了文字值和端口号；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 在端口 1645 和 1646 上侦听 RADIUS。如果 RADIUS 服务器使用标准端口 1812 和 1813，则您可以将 ASA 配置为使用 **authentication-port** 和 **accounting-port** 命令侦听这些端口。
- 要分配用于 DNS 访问的端口，请使用 **domain** 文字值而不是 **dns**。如果使用 **dns**，则 ASA 会假定您意图使用 **dnsix** 文字值。

您可以在 IANA 网站上在线查看端口号：

http://www.iana.org/assignments/port-numbers

表 40-7　　端口文字值

文字	TCP 或 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收到新邮件

表 40-7　　端口文字值 （续）

文字	TCP 或 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	日间， RFC 867
discard	TCP、 UDP	9	丢弃
域	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	HTTP over SSL
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 - 打印后台处理程序
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
netbios-ssn	TCP	139	NetBIOS 会话服务

表 40-7　　端口文字值 （续）

文字	TCP 或 UDP?	值	说明
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 status
pcanywhere-data	TCP	5631	pcAnywhere data
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 （记帐）
rip	UDP	520	路由信息协议
secureid-udp	UDP	5510	SecureID over UDP
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
时间	UDP	37	时间
uucp	TCP	540	UNIX 对 UNIX 复制程序
who	UDP	513	人员
whois	TCP	43	主体
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

下表列出 ASA 为处理发往 ASA 的流量可能开放的协议、TCP 端口和 UDP 端口。除非启用此表中所列的功能和服务，否则 ASA *不*开放任何本地协议或任何 TCP 或 UDP 端口。您必须为 ASA 配置功能或服务才能开放默认的侦听协议或端口。在许多情况下，启用功能或服务后，可以配置除默认端口以外的端口。

表 40-8　　按功能和服务开放的协议和端口

功能或服务	协议	端口号	备注
DHCP	UDP	67,68	-
故障切换控制	105	N/A	-
HTTP	TCP	80	-
HTTPS	TCP	443	-
ICMP	1	N/A	-
IGMP	2	N/A	仅在目标 IP 地址 224.0.0.1 上开放协议
ISAKMP/IKE	UDP	500	可配置。
IPsec (ESP)	50	N/A	-
IPsec over UDP (NAT-T)	UDP	4500	-
IPsec over UDP （兼容思科 VPN 3000 系列）	UDP	10000	可配置。
IPsec over TCP (CTCP)	TCP	-	未使用默认端口。配置 IPsec over TCP 时，必须指定端口号。
NTP	UDP	123	-
OSPF	89	N/A	仅在目标 IP 地址 224.0.0.5 和 224.0.0.6 上开放协议
PIM	103	N/A	仅在目标 IP 地址 224.0.0.13 上开放协议
RIP	UDP	520	-
RIPv2	UDP	520	仅在目标 IP 地址 224.0.0.9 上开放端口
SNMP	UDP	161	可配置。
SSH	TCP	22	-
状态更新	8 （非安全） 9 （安全）	N/A	-
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	只能通过 VPN 隧道访问端口。

ICMP 类型

下表列出可在 ASA 命令中输入的 ICMP 类型编号和名称。

表 40-9　　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