思科 ASA 系列常规操作 ASDM 配置指南

软件版本 7.4
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。

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 ASDM 配置指南

关于本指南

文档目标

本指南旨在帮助您使用或自适应安全设备管理器 (ASDM) 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。

本指南中，术语 “ASA”一般适用于所支持的型号，除非另有说明。

备注 ASDM 支持许多 ASA 版本。ASDM 文档和联机帮助涵盖 ASA 支持的所有最新功能。如果您运行的是旧版 ASA 软件，本文档可能包含您的版本中不支持的功能。请参阅每章的功能历史记录表以确定功能的添加时间。有关每个 ASA 版本所支持的 ASDM 最低版本，请参阅《*思科 ASA 系列兼容性*》。

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。

备注 ASDM 支持许多 ASA 版本。ASDM 文档和联机帮助涵盖 ASA 支持的所有最新功能。如果您运行的是旧版 ASA 软件，本文档可能包含您的版本中不支持的功能。请参阅每章的功能历史记录表以确定功能的添加时间。有关每个 ASA 版本支持的最低 ASDM 版本的信息，请参阅《思科 ASA 兼容性》。另请参阅特殊、弃用和传统服务，第 1-16 页。

ASDM 要求

ASDM 客户端操作系统和浏览器要求

下表列出支持的建议用于 ASDM 的客户端操作系统和 Java。

表 1-1　　操作系统和浏览器要求

操作系统	浏览器				Java SE 插件
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows （英文版和日文版）： • 8 • 7 • 服务器 2008 • 服务器 2012	是	是	不支持	是	7.0 或更高版本
Apple OS X 10.4 及更高版本	不支持	是	是	是 （仅限 64 位版本）	7.0 或更高版本
Red Hat Enterprise Linux 5（GNOME 或 KDE）： • “桌面” (Desktop) • 带工作站选项的桌面版	N/A	是	N/A	是	7.0 或更高版本

Java 和浏览器兼容性

下表列出了 Java、 ASDM 和浏览器兼容性的兼容性警告。

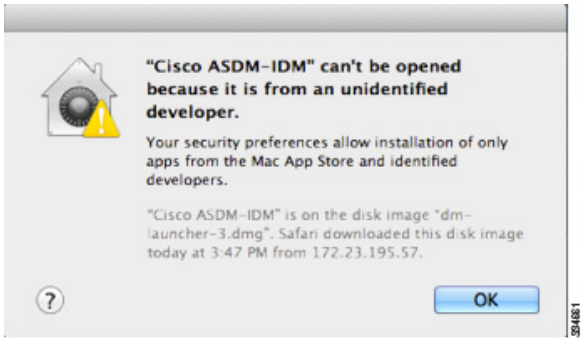
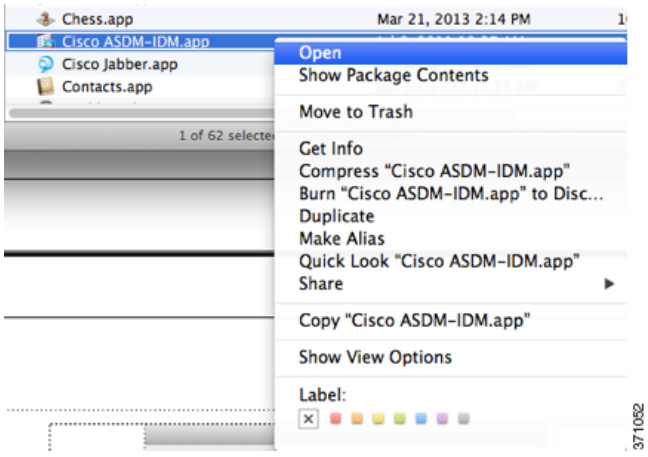
表 1-2　　Java 与 ASDM 兼容性相关注意事项

Java 版本	条件	备注
7 Update 51	ASDM Launcher 需要可信证书	要继续使用 Launcher，请执行以下其中一项操作： • 将 Java 升级到 Java 8 或降级到 Java 7 update 45 或更低版本。 • 在 ASA 上安装由已知 CA 颁发的可信证书。 • 安装自签证书并使用 Java 进行注册。请参阅为 ASDM 安装身份证书。 • 或者，使用 Java Web Start。 **注意：**Java 7 update 51 不支持 ASDM 7.1(5) 及更低版本。如果您已升级 Java，并且无法再启动 ASDM 以将其升级到 7.2 版本或更高版本，则可以使用 CLI 升级 ASDM，也可以在 Java 控制面板中为每个要使用 ASDM 管理的 ASA 添加安全性异常。请参阅 “解决方法”一节，网址： http://java.com/en/download/help/java_blocked.xml 添加安全性异常后，启动旧版本 ASDM，然后升级到 7.2 或更高版本。
	在极少数情况下，使用 Java Web Start 时无法加载在线帮助	在极少数情况下，启动在线帮助时，浏览器窗口会加载，但内容无法显示。浏览器报告以下错误：“Unable to connect”。 解决方法： • 使用 ASDM Launcher 或： • 清除 Java 运行时参数中的 **-Djava.net.preferIPv6Addresses=true** 参数： a. 启动 Java 控制面板。 b. 点击 **Java** 选项卡。 c. 点击 **View**。 d. 清除以下参数：**-Djava.net.preferIPv6Addresses=true** e. 点击 **OK**，然后点击 **Apply**，再次点击 **OK**。
7 Update 45	使用不可信证书时， ASDM 将显示一条有关缺失 “权限”属性的黄色警告	由于 Java 中存在的一个漏洞，因此，如果没有在 ASA 上安装可信证书，您将会在 JAR 清单中看到指示缺少权限属性的黄色警告。**可忽略此警告**；ASDM 7.2 或更高版本包含 “权限”属性。为了防止出现该警告，请安装可信证书 （由已知 CA 颁发）；或者依次选择 **Configuration > Device Management > Certificates > Identity Certificates** 以在 ASA 上生成自签证书。启动 ASDM，当出现证书警告时，选中 **Always trust connections to websites** 复选框。

表 1-2　Java 与 ASDM 兼容性相关注意事项（续）

Java 版本	条件	备注
7	ASA 需要有强加密许可证 (3DES/AES)	ASDM 需要一个与 ASA 的 SSL 连接。您可以向思科申请一个 3DES 许可证： 1. 转至 www.cisco.com/go/license。 2. 点击 **Continue to Product License Registration**。 3. 在许可门户中，点击文本字段旁边的 **Get Other Licenses**。 4. 从下拉列表中选择 **IPS、 Crypto、 Other...**。 5. 将 **ASA** 键入至 **Search by Keyword** 字段。 6. 在 **Product** 列表中选择 **Cisco ASA 3DES/AES License**，然后点击 **Next**。 7. 输入 ASA 的序列号，然后按照提示为 ASA 申请 3DES/AES 许可证。
全部	• 自签证书或不可信证书 • IPv6 • Firefox 和 Safari	如果 ASA 使用自签证书或不可信证书，当使用 HTTPS 通过 IPv6 浏览时， Firefox 和 Safari 将无法添加安全性异常。请访问 https://bugzilla.mozilla.org/show_bug.cgi?id=633001。此警告会影响从 Firefox 或 Safari 到 ASA 的所有 SSL 连接 （包括 ASDM 连接）。要避免此警告，请为 ASA 配置由可信证书颁发机构颁发的正确证书。
	• ASA 上的 SSL 加密必须包括 RC4-MD5 和 RC4-SHA1，*或者*在 Chrome 中禁用 SSL 虚假启动。 • Chrome	如果更改 ASA 上的 SSL 加密以排除 RC4-MD5 和 RC4-SHA1 算法（默认情况下已启用这些算法）， Chrome 将由于 Chrome “SSL 虚假启动”功能而无法启动 ASDM。我们建议重新启用其中一种算法（参阅 **Configuration > Device Management > Advanced > SSL Settings** 窗格）；您也可以根据 Run Chromium with flags 使用 **--disable-ssl-false-start** 标签在 Chrome 中禁用 SSL 虚假启动。
	服务器专用 IE9	对于服务器专用 Internet Explorer 9.0，“Do not save encrypted pages to disk”选项在默认情况下处于启用状态 （请参阅 Tools > Internet Options > Advanced）。此选项会导致初始 ASDM 下载失败。请务必禁用此选项以允许 ASDM 下载。
	OS X	在 OS X 上，第一次运行 ASDM 时，系统可能会提示您安装 Java；根据需要按照提示进行安装。安装完成后， ASDM 将启动。

表 1-2　　Java 与 ASDM 兼容性相关注意事项（续）

Java 版本	条件	备注
全部	OS X 10.8 及更高版本	您需要允许 ASDM 运行，因为它未使用 Apple 开发人员 ID 进行签名。如果未更改安全首选项，将会出现一个错误屏幕。  1. 要允许 ASDM 运行，请右键点击（或按住 Ctrl 键并点击）**Cisco ASDM-IDM Launcher** 图标，然后选择 **Open**。  2. 随即将会出现一个类似的错误屏幕；但您可以通过该屏幕打开 ASDM。点击 **Open**。系统将打开 ASDM-IDM Launcher。 

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/ASDM 7.4(1) 版的新功能。

表 1-3　ASA 9.4(1) 版/ASDM 7.4(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

表 1-3　　ASA 9.4(1) 版/ASDM 7.4(1) 版的新功能（续）

功能	描述
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。 未修改任何屏幕。
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。 从 **Select SIP Inspect Map** 服务策略对话框中删除了 Phone Proxy 和 UC-IME Proxy。
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。 未修改任何屏幕。
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。 未修改任何屏幕。
VXLAN 数据包检测	ASA 可检测 VXLAN 报头以强制遵守标准格式。 修改了以下屏幕：**Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > Protocol Inspection**
IPv6 的 DHCP 监控	您现在可以监控 IPv6 的 DHCP 统计信息和 DHCP 绑定。 引入了以下屏幕： **Monitoring > Interfaces > DHCP > IPV6 DHCP Statistics** **Monitoring > Interfaces > DHCP > IPV6 DHCP Binding**。
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。 未修改任何屏幕。

表 1-3　　ASA 9.4(1) 版/ASDM 7.4(1) 版的新功能（续）

功能	描述
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。 引入了以下屏幕：**Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Interface Health Monitoring**
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。 未修改任何屏幕。
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。 未修改任何屏幕。
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。 引入或修改了以下屏幕： **Configuration > Device Setup > Routing > Route Maps > Policy Based Routing** **Configuration > Device Setup > Routing > Interface Settings > Interfaces。**
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。 引入了以下屏幕： **Configuration > Device Setup > Interface Settings > Interfaces > Add > VNI Interface** **Configuration > Device Setup > Interface Settings > VXLAN**
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。 修改了以下屏幕：**Configuration > Device Management > Advanced > Embedded Event Manager > Add Event Manager Applet > Add Event Manager Applet Event。**
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。

表 1-3　　ASA 9.4(1) 版/ASDM 7.4(1) 版的新功能（续）

功能	描述
远程访问功能	
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。 修改了以下屏幕：**Configuration > Remote Access VPN > Advanced > SSL Settings**。
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 引入了以下屏幕：**Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > HTTP Cookie**。 *9.2(3) 中也包含此功能。*

表 1-3　　ASA 9.4(1) 版/ASDM 7.4(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。 未修改任何屏幕。
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。 未修改任何屏幕。
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。 修改了以下屏幕： **Configuration > Device Management > Certificate Management > Identity Certificates** **Configuration > Device Management > Certificate Management > CA Certificates**
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。 修改了以下屏幕： **Configuration > Device Management > Certificate Management > Identity Certificates** **Configuration > Device Management > Certificate Management > CA Certificates**
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。 修改了以下屏幕：**Configuration > Device Management > Certificate Management > CA Certificates**

表 1-3　　ASA 9.4(1) 版/ASDM 7.4(1) 版的新功能（续）

功能	描述
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。
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。 修改了以下屏幕：**Configuration > Site-to-Site VPN > Connection Profiles**
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。 引入了以下屏幕：**Configuration > Device Management > Management Access > HTTP Certificate Rule** 修改了以下屏幕：**Configuration > Device Management > Users/AAA > AAA Access > Authorization**
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。
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 1-12 页
- 防火墙模式概述，第 1-13 页
- 状态检测概述，第 1-14 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。

- 通过访问规则允许或拒绝流量，第 1-12 页
- 应用 NAT，第 1-12 页
- 保护 IP 分片，第 1-12 页
- 应用 HTTP、 HTTPS 或 FTP 过滤，第 1-12 页
- 应用应用检测，第 1-12 页
- 向受支持的硬件或软件模块发送流量，第 1-13 页
- 应用 QoS 策略，第 1-13 页
- 应用连接限制和 TCP 规范化，第 1-13 页
- 启用威胁检测，第 1-13 页

通过访问规则允许或拒绝流量

可以应用访问规则，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、弃用和传统服务

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

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。

弃用的服务

有关弃用的功能，请参阅相应 ASA 版本的配置指南。同样，对于重新设计的功能 （例如，版本 8.2 与版本 8.3 之间 NAT，或版本 8.3 与版本 8.4 版之间的透明模式接口），请参阅相应版本的配置指南。虽然 ASDM 向后兼容之前的 ASA 版本，但配置指南和在线帮助仅涵盖有关最新版本的内容。

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。

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

在某些情况下，可能需要使用 CLI 为 ASDM 访问配置基本设置。

对于初始配置，请从控制台端口直接访问 CLI。之后可根据第 34 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

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 18-1 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。ASASM 不包括出厂默认配置，因此必须先在 CLI 执行某些配置，然后才能使用 ASDM 访问该配置。本节介绍如何访问 ASASM CLI。

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 34-1 页
- 设置主机名、域名及启用密码和 Telnet 密码，第 18-1 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）

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 2-15 页
- 启用或禁用多情景模式，第 8-14 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 2-15 页
- 设置防火墙模式 （单模式），第 6-7 页
- 访问设备控制台，第 2-2 页
- 启动 ASDM，第 2-12 页
- 第 8 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 8 章 “多情景模式”
- 设置防火墙模式 （单模式），第 6-7 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。

自定义 ASDM 操作

可以安装身份证书来成功启动 ASDM 并增加 ASDM 堆内存，以便 ASDM 可以处理更大的配置。

- 为 ASDM 安装身份证书，第 2-13 页
- 增加 ASDM 配置内存，第 2-13 页

为 ASDM 安装身份证书

使用 Java 7 update 51 及更高版本时，ASDM 启动程序需要可信证书。满足证书要求的一个简单方法就是安装自签名身份证书。可使用 Java Web Start 启动 ASDM，直到安装证书。

请参阅以下文档，以便在 ASA 上安装用于 ASDM 的自签身份证书，并向 Java 注册证书。

http://www.cisco.com/go/asdm-certificate

增加 ASDM 配置内存

ASDM 最多支持 512 KB 的配置。如果超出此数量，可能会遇到性能问题。例如加载配置时，状态对话框显示已完成配置的百分比，但如果有大型配置，它将停止递增并显示为暂停操作，即使 ASDM 仍可能在处理配置。如果发生此情况，我们建议考虑增加 ASDM 系统堆内存。

- 增加 Windows 中的 ASDM 配置内存，第 2-13 页
- 增加 Mac 操作系统中的 ASDM 配置内存，第 2-14 页

增加 Windows 中的 ASDM 配置内存

要增加 ASDM 堆内存大小，请通过执行以下程序编辑 **run.bat** 文件。

操作步骤

1. 转到 ASDM 安装目录，例如 C:\Program Files (x86)\Cisco Systems\ASDM。
2. 使用任意文本编辑器编辑 **run.bat** 文件。

3. 在以 “start javaw.exe” 开头的行中，更改前缀为 “-Xmx” 的参数以指定所需堆大小。例如，如需 768 MB 内存，请将参数更改为 -Xmx768M；如需 1 GB 内存，请将参数更改为 -Xmx1G。
4. 保存 **run.bat** 文件。

增加 Mac 操作系统中的 ASDM 配置内存

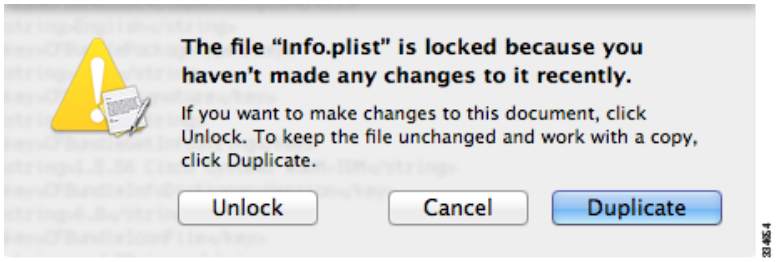
要增加 ASDM 堆内存大小，请通过执行以下程序编辑 **Info.plist** 文件。

操作步骤

1. 右键点击 **Cisco ASDM-IDM** 图标，然后选择 **Show Package Contents**。
2. 在 **Contents** 文件夹中，双击 **Info.plist** 文件。如果已安装开发人员工具，该文件会在 **Property List Editor** 中打开。否则，它将在 **TextEdit** 中打开。
3. 在 **Java > VMOptions** 下方，更改前缀为 “-Xmx” 的字符串以指定所需堆大小。例如，如需 768 MB 内存，请将参数更改为 -Xmx768M；如需 1 GB 内存，请将参数更改为 -Xmx1G。

```
<key>CFBundleIconFile</key>
<string>asdm32.icns</string>

<key>VMOptions</key>
<string>-Xms64m -Xmx512m</string>


<key>CFBundleDocumentTypes</key>
  <array>
```

4. 如果该文件已锁定，则将看到如下错误：



5. 点击 **Unlock** 并保存文件。

   如果未看到 **Unlock** 对话框，请退出编辑器，右键点击 **Cisco ASDM-IDM** 图标，选择 **Copy Cisco ASDM-IDM**，并将其粘贴到您拥有写入权限的位置，例如桌面。然后从该副本更改堆大小。

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 2-15 页
- 恢复 ASAv 部署配置，第 2-16 页
- ASA 5506-X、 5508-X 和 5516-X 默认配置，第 2-17 页
- ASA 5512-X、 5515-X、 5525-X 及更高型号默认配置，第 2-18 页
- ASAv 部署配置，第 2-18 页

恢复出厂默认配置

本节介绍如何恢复出厂默认配置。已提供 CLI 和 ASDM 程序。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。

步骤 1　在主 ASDM 应用窗口中，依次选择 **File > Reset Device to the Factory Default Configuration**。

系统将显示 **Reset Device to the Default Configuration** 对话框。

步骤 2　（可选）在 **Management IP address** 中输入管理接口的管理 IP 地址，而不是使用默认地址 192.168.1.1。

步骤 3　（可选）从下拉列表中选择 **Management Subnet Mask**。

步骤 4　点击 **OK**。

随即显示确认对话框。

注意　该操作还可清除启动映像位置 （如果存在）以及其他配置。在 **Configuration > Device Management > System Image/Configuration > Boot Image/Configuration** 窗格中，可从特定映像启动，包括外部内存上的映像。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 5　点击 **Yes**。

步骤 6　恢复默认配置后，将该配置保存到内部闪存。依次选择 **File > Save Running Configuration to Flash**。

选择该选项可将运行配置保存到启动配置的默认位置，即使之前已配置了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
```

开始配置

要配置和监控 ASA，请执行以下步骤：

备注 ASDM 最多支持 512 KB 的配置。如果超出此量，可能会遇到性能问题。请参阅增加 ASDM 配置内存，第 2-13 页。

操作步骤

步骤 1 要使用启动向导进行初始配置，请依次选择 **Wizards > Startup Wizard**。

步骤 2 要使用 IPsec VPN 向导配置 IPSec VPN 连接，请依次选择 **Wizards > IPsec VPN Wizards**，然后完成系统显示的每个屏幕。

步骤 3 要使用 SSL VPN 向导配置 SSL VPN 连接，请依次选择 **Wizards > SSL VPN Wizards**，然后完成系统显示的每个屏幕。

步骤 4 要配置高可用性和可扩展性设置，请依次选择 **Wizards > High Availability and Scalability Wizard**。

步骤 5 要使用数据包捕获向导配置数据包捕获，请依次选择 **Wizards > Packet Capture Wizard**。

步骤 6 要显示 ASDM GUI 中可用的不同颜色和样式，请依次选择 **View > Office Look and Feel**。

步骤 7 要配置功能，请点击工具栏上的 **Configuration** 按钮，然后点击其中一个功能按钮以显示相关联的配置窗格。

备注 如果 Configuration 屏幕为空，请点击工具栏上的 **Refresh** 以显示屏幕内容。

步骤 8 要监控 ASA，请点击工具栏上的 **Monitoring** 按钮，然后点击功能按钮以显示相关联的监控窗格。

使用 ASDM 中的命令行界面工具

本节介绍如何使用 ASDM 输入命令以及如何处理 CLI。

使用命令行界面工具

该功能可提供基于文本的工具，用于向 ASA 发送命令并查看结果。

可通过 CLI 工具输入的命令取决于用户权限。在主 ASDM 应用窗口底部的状态栏中查看权限级别，以确保拥有执行特权级别 CLI 命令所需的权限。

准备工作

- 通过 ASDM CLI 工具输入的命令与通过 ASA 终端连接输入的命令可能以不同方式运行。
- 命令错误 - 如果由于输入错误命令而出现错误，则会跳过错误命令，并处理剩余命令。Response 区域将显示消息，提醒您是否出现错误，并且显示其他相关信息。
- 交互式命令 - CLI 工具不支持交互式命令。要在 ASDM 中使用这些命令，请使用 **noconfirm** 关键字 （如果可用），如以下命令所示：

  ```
  crypto key generate rsa modulus 1024 noconfirm
  ```

- 避免与其他管理员冲突 - 多个管理用户可更新 ASA 的运行配置。使用 ASDM CLI 工具对配置进行更改之前，检查是否存在其他活动管理会话。如果多个用户同时配置 ASA，则最近的更改生效。

  要查看当前在同一 ASA 上的其他活动管理会话，请依次选择 **Monitoring > Properties > Device Access**。

操作步骤

步骤 1　在主 ASDM 应用窗口中，依次选择 **Tools > Command Line Interface**。

系统将显示 **Command Line Interface** 对话框。

步骤 2　选择需要的命令类型 （单行或多行），然后从下拉列表中选择命令，或在提供的字段中键入命令。

步骤 3　点击 **Send** 以执行命令。

步骤 4　要输入新命令，请点击 **Clear Response**，然后选择 （或键入）要执行的其他命令。

步骤 5　选中 **Enable context-sensitive help (?)** 复选框，为该功能提供情景相关帮助。取消选中该复选框以禁用情景相关帮助。

步骤 6　关闭 Command Line Interface 对话框后，如果已更改配置，请点击 **Refresh** 以查看 ASDM 中的更改。

在设备上显示 ASDM 忽略的命令

该功能可显示 ASDM 不支持的命令列表。通常， ASDM 忽略这些命令。ASDM 不从运行配置更改或删除这些命令。有关详细信息，请参阅不受支持的命令，第 3-29 页。

操作步骤

步骤 1　在主 ASDM 应用窗口中，依次选择 **Tools > Show Commands Ignored by ASDM on Device**。

步骤 2　完成后点击 **OK**。

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。

ASDM 图形用户界面

本章介绍如何使用 ASDM 用户界面。

关于 ASDM 用于界面

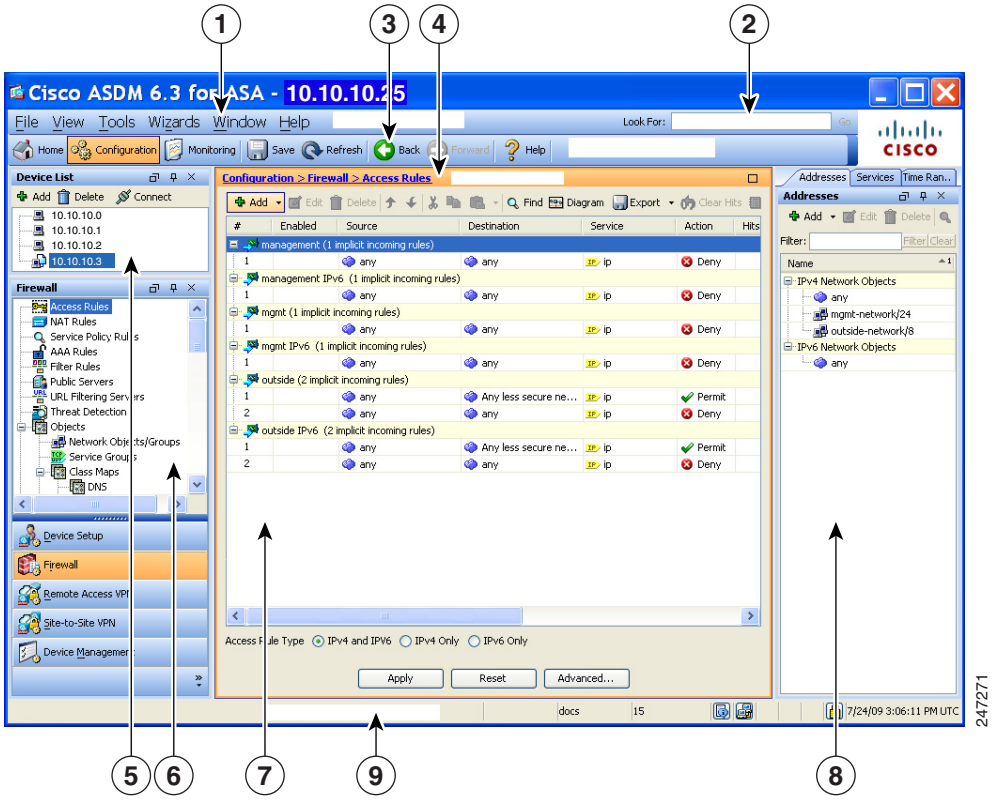
ASDM 用户界面专门用于提供对 ASA 支持的许多功能的轻松方法。ASDM 用户界面包含以下元素：

- 菜单栏，提供对文件、工具、向导和帮助的快速访问。许多菜单项还具有键盘快捷键。
- 工具栏，让您可以导航 ASDM。从工具栏中，您可以访问 **Home**、 **Configuration** 和 **Monitoring** 窗格，还可以获取帮助并在窗格之间导航。

- 可停靠左侧 **Navigation** 窗格，用于浏览 **Configuration** 和 **Monitoring** 窗格。您可以点击标题中的三个按钮之一以最大化或还原此窗格，使其成为可以移动、隐藏或关闭的浮动窗格。要访问 **Configuration** 和 **Monitoring** 窗格，可以执行以下操作之一：
  - 点击左侧 **Navigation** 窗格中应用窗口左侧的链接。**Content** 窗格之后会在所选窗格的标题栏中显示路径（例如， **Configuration > Device Setup > Startup Wizard**）。
  - 如果知道确切的路径，可以将其直接键入到应用窗口右侧 **Content** 窗格的标题栏中，而不点击左侧 **Navigation** 窗格中的任何链接。
- **Content** 窗格右上角的最大化和还原按钮，用于隐藏和显示左侧 **Navigation** 窗格。
- 包含设备列表的可停靠 **Device List** 窗格，可以通过 ASDM 进行访问。您可以点击标题中的三个按钮之一以最大化或还原此窗格，使其成为可以移动、隐藏或关闭的浮动窗格。
- 状态栏，在应用窗口底部显示时间、连接状态、用户、内存状态、运行配置状态、权限级别和 SSL 状态。
- 左侧 **Navigation** 窗格，显示创建访问规则、 NAT 规则、 AAA 规则、筛选规则和服务规则时可在规则表中使用的各种对象。窗格中的选项卡标题根据您查看的功能而更改。此外，在该窗格中还会显示 **ASDM Assistant**。

下图显示 ASDM 用户界面元素的元素。

图 3-1　　ASDM 用户界面



图例

GUI 元素	说明
1	菜单栏
2	搜索字段
3	工具栏
4	导航路径
5	设备列表窗格
6	左侧导航窗格
7	内容窗格
8	右侧导航窗格
9	状态栏

备注　已为 GUI 的各个部分添加工具提示，包括 **Wizards**、**Configuration** 和 **Monitoring** 窗格以及**状态栏**。要查看工具提示，请将鼠标悬停在特定用户界面元素 （如状态栏中的图标）上方。

导航 ASDM 用户界面

要高效地浏览 ASDM 用户界面，可以使用上一节中介绍的菜单、工具栏、可停靠窗格和左右 **Navigation** 窗格的组合。可用功能显示在 **Device List** 窗格下方的按钮列表中。示例列表可以包含以下功能按钮：

- **Device Setup**
- **Firewall**
- **Botnet Traffic Filter**
- **Remote Access VPN**
- **Site to Site VPN**
- **Device Management**

显示的功能按钮列表基于已购买的许可功能。点击每个按钮以访问 Configuration 视图或 Monitoring 视图的所选功能中的第一个窗格。功能按钮在 Home 视图中不可用。

要更改功能按钮的显示，请执行以下步骤：

步骤 1　选择最后一个功能按钮下方的下拉列表以显示情景菜单。

步骤 2　选择以下选项之一：

- 点击 **Show More Buttons** 以显示更多按钮。
- 点击 **Show Fewer Buttons** 以显示更少按钮。
- 点击 **Add or Remove Buttons** 以添加或删除按钮，然后点击要从显示的列表中添加或删除的按钮。

- 选择 **Option** 以显示 **Option** 对话框，其中会按按钮的当前顺序显示其列表。然后，选择以下之一：
  - 点击 **Move Up** 以将列表中的按钮上移。
  - 点击 **Move Down** 以将列表中的按钮下移。
  - 点击 **Reset** 以将列表中各项的顺序还原为默认设置。

步骤 3　点击 **OK** 以保存设置并关闭此对话框。

菜单

您可以使用鼠标或键盘访问 ASDM 菜单。有关从键盘访问菜单栏的信息，请参阅键盘快捷键，第 3-10 页。

ASDM 具有以下菜单：

File 菜单

通过 **File** 菜单，可以管理 ASA 配置。

File 菜单项	说明
Refresh ASDM with the Running Configuration on the Device	将运行配置的副本加载到 ASDM 中。
Reset Device to the Factory Default Configuration	将配置恢复为出厂默认值。
Show Running Configuration in New Window	在新窗口中显示当前运行配置。
Save Running Configuration to Flash	将运行配置的副本写入到闪存。
Save Running Configuration to TFTP Server	将当前运行配置文件的副本存储在 TFTP 服务器上。
Save Running Configuration to Standby Unit	将主单元上的运行配置文件的副本发送到故障切换备用单元的运行配置。
Save Internal Log Buffer to Flash	将内部日志缓冲区保存到闪存。
Print	打印当前页面。打印规则时，建议按照横向页面方向进行打印。如果使用 Internet Explorer，则在最初接受已签名的小程序时便已授予打印权限。

File 菜单项	说明
Clear ASDM Cache	删除本地 ASDM 映像。ASDM 在您连接到 ASDM 时以本地方式下载映像。
Clear ASDM Password Cache	在您已定义新密码并仍然具有不同于新密码的现有密码的情况下删除密码缓存。
Clear Internal Log Buffer	清空系统日志消息缓冲区。
Exit	关闭 ASDM。

View 菜单

通过 **View** 菜单，可以显示 ASDM 用户界面的各个部分。某些项取决于当前视图。不能选择无法在当前视图中显示的项。

View 菜单项	描述
Home	显示 Home 视图。
Configuration	显示 Configuration 视图。
Monitoring	显示 Monitoring 视图。
Device List	在可停靠窗格中显示设备列表。有关详情，请参见设备列表，第 3-9 页。
Navigation	在 Configuration 和 Monitoring 视图中显示和隐藏 **Navigation** 窗格的显示。
ASDM Assistant	搜索和查找关于某些任务的实用 ASDM 操作步骤帮助。有关详情，请参见 ASDM Assistant，第 3-8 页。
Latest ASDM Syslog Messages	在 Home 视图中显示和隐藏 **Latest ASDM Syslog Messages** 窗格的显示。此窗格仅在 Home 视图中可用。如果没有足够的内存升级到最新版本，则会生成系统日志消息 %ASA-1-211004，指示已安装的内存量和所需的内存量。此消息每隔 24 小时重新显示，直到内存升级为止。
Addresses	显示和隐藏 **Addresses** 窗格的显示。**Addresses** 窗格仅适用于 Configuration 视图中的 **Access Rules**、 **NAT Rules**、 **Service Policy Rules**、 **AAA Rules** 和 **Filter Rules** 窗格。
Services	显示和隐藏 **Services** 窗格的显示。**Services** 窗格仅适用于 Configuration 视图中的 **Access Rules**、**NAT Rules**、**Service Policy Rules**、**AAA Rules** 和 **Filter Rules** 窗格。
Time Ranges	显示和隐藏 **Time Ranges** 窗格的显示。**Time Ranges** 窗格仅适用于 Configuration 视图中的 **Access Rules**、**Service Policy Rules**、**AAA Rules** 和 **Filter Rules** 窗格。
Select Next Pane	在多窗格显示中突出显示下一个窗格，例如，从 Service Policies Rules 窗格转至它旁边的 Address 窗格。
Select Previous Pane	在多窗格显示中突出显示上一个窗格。
Back	返回到上一个窗格。
Forward	转至以前访问的下一个窗格。
Find in ASDM	查找您搜索的项，如功能或 **ASDM Assistant**。
Reset Layout	将布局还原为默认配置。
Office Look and Feel	将屏幕字体和颜色更改为 Microsoft Office 设置。

Tools 菜单

Tools 菜单提供要在 ASDM 中使用的以下系列的工具。

Tools 菜单项	描述
Command Line Interface	将命令发送到 ASA 并查看结果。
Show Commands Ignored by ASDM on Device	显示 ASDM 已忽略的不受支持的命令。
Packet Tracer	跟踪从指定源地址和接口到目标源地址和接口的数据包。您可以指定任何类型的数据的协议和端口，并使用有关对数据包采取的操作的详细信息查看该数据包的生命期。有关详情，请参阅防火墙配置指南。
Ping	验证 ASA 和周围通信链路的配置与操作，以及执行对其他网络设备的基本测试。有关详情，请参阅防火墙配置指南。
Traceroute	确定数据包到其目标将采用的路由。有关详情，请参阅防火墙配置指南。
File Management	查看、移动、复制和删除闪存中存储的文件。您还可以在闪存中创建目录。此外，也可以在各种文件系统 （包括 TFTP、闪存和本地 PC）之间传输文件。
Check for ASA/ASDM Updates	通过向导升级 ASA 软件和 ASDM 软件。
Upgrade Software from Local Computer	将 PC 上的 ASA 映像、 ASDM 映像或其他映像上载到闪存。
Downgrade Software	加载比您当前运行的 ASA 映像更旧的映像。
Backup Configurations	备份 ASA 配置、Cisco Secure Desktop 映像以及 SSL VPN 客户端映像和配置文件。
Restore Configurations	恢复 ASA 配置、Cisco Secure Desktop 映像以及 SSL VPN 客户端映像和配置文件。
System Reload	重新启动 ASDM 并将保存的配置重新加载到内存中。
Administrator's Alert to Clientless SSL VPN Users	使管理员能够向无客户端 SSL VPN 用户发送告警消息。有关详情，请参阅VPN 配置指南。
Migrate Network Object Group Members	如果迁移到 8.3 或更高版本， ASA 会创建命名网络对象来替换某些功能中的内联 IP 地址。除命名对象以外， ASDM 还会为配置中使用的任何 IP 地址自动创建非命名对象。这些自动创建的对象仅通过 *IP 地址*进行识别，不具有名称，并且在平台配置中不是作为命名对象存在。 当 ASA 在迁移过程中创建命名对象时，匹配的非命名纯 ASDM 对象会替换为命名对象。唯一的例外是网络对象组中的非命名对象。当 ASA 为网络对象组中包含的 IP 地址创建命名对象时， ASDM 还会保留非命名对象，从而在 ASDM 中创建重复对象。依次选择 **Tools > Migrate Network Object Group Members** 以合并这些对象。 有关详细信息，请参阅 《*思科 ASA 5500 到 8.3 版本及更高版本的迁移*》。
Preferences	在会话之间更改指定的 ASDM 功能的行为。有关详细信息，请参阅定义 ASDM 首选项，第 3-27 页。
ASDM Java Console	显示 Java 控制台。

Wizards 菜单

通过 **Wizards** 菜单，可以运行向导来配置多个功能。

Wizards 菜单项	说明
Startup Wizard	指导您分步完成 ASA 的初始配置。
VPN Wizards	各种 VPN 配置具有单独的向导。有关详情，请参阅VPN 配置指南。
High Availability and Scalability Wizard	允许配置故障切换：VPN 集群负载均衡或 ASA 上的 ASA 集群。
Unified Communication Wizard	支持在 ASA 上配置统一通信功能，如 IP 电话。有关详情，请参阅防火墙配置指南。
ASDM Identity Certificate Wizard	使用 Java 7 update 51 及更高版本时， ASDM 启动程序需要可信证书。满足证书要求的一个简单方法就是安装自签名身份证书。您可以使用 Java Web Start 启动 ASDM，直到使用此向导安装证书为止。有关详细信息，请参阅 http://www.cisco.com/go/asdm-certificate。
Packet Capture Wizard	允许在 ASA 上配置数据包捕获。该向导在入口接口和出口接口各运行一次数据包捕获。运行捕获后，可以将其保存在计算机上，然后使用数据包分析器检查并分析捕获。

Window 菜单

通过 **Window** 菜单，可以在 ASDM 窗口之间移动。活动窗口显示为所选窗口。

Help 菜单

Help 菜单提供指向联机帮助的链接，以及有关 ASDM 和 ASA 的信息。

Help 菜单项	说明
Help Topics	打开新的浏览器窗口可显示 ASDM 联机帮助。如果您在 ASDM 中管理 ASA FirePOWER 模块，此项目会显示为 **ASDM Help Topics**。
ASA FirePOWER Help Topics	打开新的浏览器窗口可显示 ASA FirePOWER 模块的联机帮助。此项目仅在您安装了模块并在 ASDM 中进行管理时可用。
Help for Current Screen	打开有关正查看的屏幕的上下文相关帮助。或者，也可以点击工具栏中的 **? Help** 按钮。
Release Notes	打开 Cisco.com 上最新版本的 *ASDM 版本说明*。版本说明包含有关 ASDM 软件和硬件要求的最新信息，以及有关软件中的更改的最新信息。
Cisco ASA Series Documentation	打开 Cisco.com 上包含指向所有可用产品文档的链接的文档。
ASDM Assistant	打开 **ASDM Assistant**，通过它可以使用有关执行某些任务的详细信息从 Cisco.com 搜索可下载的内容。
About Cisco Adaptive Security Appliance (ASA)	显示有关 ASA 的信息，包括软件版本、硬件集、启动时加载的配置文件和启动时加载的软件映像。此信息有助于疑难解答。
About Cisco ASDM	显示有关 ASDM 的信息，如软件版本、主机名、特权级别、操作系统、设备类型和 Java 版本。

工具栏

菜单下方的**工具栏**提供对 Home 视图、Configuration 视图和 Monitoring 视图的访问。通过它还可以在多情景文模式中选择系统情景或安全情景，并提供导航和其他常用功能。

工具栏按钮	描述
Home	显示 **Home** 窗格，通过它可以查看有关 ASA 的重要信息，如接口的状态、运行的版本、许可信息和性能。有关详情，请参见 Home 窗格 （单模式和情景），第 3-13 页。在多模式中，系统没有 **Home** 窗格。
Configuration	配置 ASA。点击左侧 **Navigation** 窗格中的功能按钮以配置该功能。
Monitoring	监控 ASA。点击左侧 **Navigation** 窗格中的功能按钮以配置该功能。
Save **Save ASA Changes**	仅对于可写访问的情景将运行配置保存到启动配置。如果您在设备上安装了 ASA FirePOWER 模块并且正在通过 ASDM 配置该模块，则按钮会显示为 Save ASA Changes。
Refresh	使用当前运行配置刷新 ASDM，但是任何 Monitoring 窗格中的图形都除外。
Back	返回到已访问的 ASDM 的最后一个窗格。
Forward	前进到已访问的 ASDM 的最后一个窗格。
Help	显示当前打开的屏幕的情景相关帮助。
Search	在 ASDM 中搜索功能部件。Search 功能会浏览每个窗格的标题并呈现匹配项列表，而且提供直接指向该窗格的超链接。点击 **Back** 或 **Forward** 以在找到的两个不同窗格之间快速切换。有关详情，请参见 ASDM Assistant，第 3-8 页。

ASDM Assistant

通过 **ASDM Assistant**，可以搜索并查看有关某些任务的实用 ASDM 操作步骤帮助。此功能在路由模式和透明模式中以及在单情景和系统情景中可用。

依次选择 **View > ASDM Assistant > How Do I?** 或者，从菜单栏中的 **Look For** 字段输入搜索请求以访问信息。从 **Find** 下拉列表中 选择 **How Do I?** 以开始搜索。

要使用 ASDM Assistant，请执行以下步骤：

步骤 1　依次选择 **View > ASDM Assistant**。

系统将显示 **ASDM Assistant** 窗格。

步骤 2　在 **Search** 字段中输入要查找的信息，然后点击 **Go**。

所请求的信息显示在 **Search Results** 窗格中。

步骤 3　点击 **Search Results and Features** 区域中显示的任何链接以获取更多详细信息。

状态栏

状态栏显示在 ASDM 窗口底部。下表列出从左到右显示的区域。

区域	说明
Status	配置的状态 （例如，“Device configuration loaded successfully.”）
Failover	故障切换单元的状态 （主用或备用）
User Name	ASDM 用户的用户名。如果您已登录而没有用户名，则用户名为“admin”。
User Privilege	ASDM 用户的权限。
Commands Ignored by ASDM	点击图标以显示配置中 ASDM 未处理的命令列表。系统将不会从配置中删除这些命令。
Connection to Device	ASDM 到 ASA 的连接状态。有关详细信息，请参阅与设备的连接，第 3-9 页。
Syslog Connection	系统日志连接已启动，并且 ASA 处于受监控状态。
SSL Secure	与 ASDM 的连接安全，因为它使用 SSL。
Time	在 ASA 上设置的时间。

与设备的连接

ASDM 保持与 ASA 的持续连接以维护最新的 **Monitoring** 和 **Home** 窗格数据。此对话框显示连接的状态。进行配置更改时， ASDM 会在配置过程中打开另一个连接，然后将其关闭；但是，此对话框并不表示第二个连接。

设备列表

Device List 是一个可停靠窗格。您可以点击标题中的三个按钮之一以最大化或还原此窗格，使其成为可以移动、隐藏或关闭的浮动窗格。此窗格在 Home、 Configuration、 Monitoring 和 System 视图中可用。您可以使用此窗格切换到其他设备，或在 System 与情景之间切换；但是，该设备必须运行您当前运行的同一版本的 ASDM。要完全显示窗格，必须列出至少两台设备。此功能在路由模式和透明模式中以及在单情景、多情景和系统情景中可用。

要使用此窗格连接到其他设备，请执行以下步骤：

步骤 1　点击 **Add** 以向列表中添加其他设备。

系统将显示 **Add Device** 对话框。

步骤 2　输入设备的设备名称或 IP 地址，然后点击 **OK**。

步骤 3　点击 **Delete** 以从列表中删除所选设备。

步骤 4　点击 **Connect** 以连接到其他设备。

系统将显示 **Enter Network Password** 对话框。

步骤 5　在适用字段中输入用户名和密码，然后点击 **Login**。

常用按钮

许多 ASDM 窗格都包含下表中列出的按钮。点击适用按钮以完成所需任务。

按钮	说明
Apply	将在 ASDM 中进行的更改发送到 ASA 并将其应用于运行配置。
Save	将运行配置的副本写入到闪存。
Reset	丢弃更改并还原为在进行更改之前或上次点击 Refresh 或 Apply 时显示的信息。点击 **Reset** 之后，点击 **Refresh** 以确保显示当前运行配置中的信息。
Restore Default	清除所选设置并返回到默认设置。
Cancel	丢弃更改并返回到上一个窗格。
Enable	显示功能的只读统计信息。
Close	关闭打开的对话框。
Clear	从字段中删除信息，或者取消选中复选框。
Back	返回到上一个窗格。
Forward	转至下一个窗格。
Help	显示所选窗格或对话框的帮助。

键盘快捷键

您可以使用键盘来导航 ASDM 用户界面。

下表列出可用于跨 ASDM 用户界面的三个主要区域移动的键盘快捷键。

表 3-1　　主窗口中的键盘快捷键

要显示	Windows/Linux	MacOS
Home 窗格	Ctrl+H	Shift+Command+H
Configuration 窗格	Ctrl+G	Shift+Command+G
Monitoring 窗格	Ctrl+M	Shift+Command+M
Help	F1	Command+?
Back	Alt+向左箭头	Command+[
Forward	Alt+向右箭头	Command+]
刷新显示	F5	Command+R
Cut	Ctrl+X	Command+X
Copy	Ctrl+C	Command+C
Paste	Ctrl+V	Command+V
保存配置	Ctrl+S	Command+S
弹出菜单	Shift+F10	-
关闭辅助窗口	Alt+F4	Command+W

表 3-1　主窗口中的键盘快捷键 （续）

要显示	Windows/Linux	MacOS
Find	Ctrl+F	Command+F
Exit	Alt+F4	Command+Q
退出表或文本区域	Ctrl_Shift 或 Ctrl+Shift+Tab	Ctril+Shift 或 Ctrl+Shift+Tab

下表列出可用于在窗格内导航的键盘快捷键。

表 3-2　窗格中的键盘快捷键

要将焦点移至	媒体
下一个字段	选项卡
上一个字段	Shift+Tab
下一个字段 （当焦点在表中时）	Ctrl+Tab
上一个字段 （当焦点在表中时）	Shift+Ctrl+Tab
Next 选项卡 （当焦点在选项卡上时）	向右箭头
Previous 选项卡 （当焦点在选项卡上时）	向左箭头
表中的下一个单元格	选项卡
表中的上一个单元格	Shift+Tab
下一个窗格 （当显示多个窗格时）	F6
上一个窗格 （当显示多个窗格时）	Shift+F6

下表列出可与日志查看器配合使用的键盘快捷键。

表 3-3　日志查看器的键盘快捷键

目标	Windows/Linux	MacOS
暂停和恢复实时日志查看器	Ctrl+U	Command+
刷新日志缓冲区窗格	F5	Command+R
清除内部日志缓冲区	Ctrl+Delete	Command+Delete
复制所选日志条目	Ctrl+C	Command+C
保存日志	Ctrl+S	Command+S
打印	Ctrl+P	Command+P
关闭辅助窗口	Alt+F4	Command+W

下表列出可用于访问菜单项的键盘快捷键。

表 3-4　　用于访问菜单项的键盘快捷键

要访问	Windows/Linux
菜单栏	纬度
下一个菜单	向右箭头
上一个菜单	向左箭头
下一个菜单选项	向下箭头
上一个菜单选项	向上箭头
所选菜单选项	输入

ASDM 窗格中的查找功能

一些 ASDM 窗格包含具有许多元素的表。为更轻松地搜索、突出显示，然后编辑特定条目，有些 ASDM 窗格具有查找功能，通过其可以对这些窗格中的对象进行搜索。

要执行搜索，您可以向 Find 字段中键入短语以搜索任何给定窗口内的所有列。该短语可以包含通配符 “*” 和 “?”。* 匹配一个或多个字符，而 ? 匹配一个字符。**Find** 字段右侧的向上和向下箭头定位下一处 （向上）或上一处 （向下）出现的该短语。选中 **Match Case** 复选框以查找具有所输入的精确大写和小写字符的条目。

例如，输入 B*ton-L* 可能会返回以下匹配项：

```
Boston-LA、Boston-Lisbon、Boston-London
```

输入 Bo?ton 可能会返回以下匹配项：

```
Boston, Bolton
```

ACL Manager 窗格中的查找功能

由于 ACL 和 ACE 包含许多不同类型的元素，因此相比于其他窗格中的查找功能，**ACL Manager** 窗格中的查找功能允许进行更有针对性的搜索。

要查找 **ACL Manager** 窗格中的元素，请执行以下步骤：

步骤 1　点击 **ACL Manager** 窗格中的 **Find**。

步骤 2　从下拉列表中的 **Filter** 字段选择以下选项之一：

- **Source** - 搜索包括网络对象组的源 IP 地址、接口 IP 或者根据其允许或拒绝流量的任何地址。您在步骤 4 中指定此地址。
- **Destination** - 搜索包括允许或拒绝将流量发送到 **Source** 部分中列出的 IP 地址的目标 IP 地址（主机或网络）。您在步骤 4 中指定此地址。
- **Source or Destination** - 搜索包括您在步骤 4 中指定的源地址或目标地址。
- **Service** - 搜索包括您在步骤 4 中指定的服务组或预定义服务策略。
- **Query** - 当从下拉列表中选择 **Query** 时，点击 **Query** 以按全部四个先前选项指定详细搜索：**Source**、 **Destination**、 **Source or Destination** 和 **Service**。

步骤 3　在第二个字段中，从下拉列表中选择以下选项之一：

- **is** - 指定在步骤 4 中输入的详细信息的精确匹配。
- **contains** - 指定搜索包含但不限于在步骤 4 中输入的详细信息的 ACL 或 ACE。

步骤 4　在第三个字段中，输入有关要查找的 ACL 或 ACE 的特定条件，或者点击 **Browse** 以搜索 ACL/ACE 配置中的关键元素。

步骤 5　点击 **Filter** 以执行搜索。

ASDM 查找功能返回包含指定条件的 ACL 和 ACE 的列表。

步骤 6　点击 **Clear** 以清除找到的 ACL 和 ACE 的列表。

步骤 7　点击红色 **x** 以关闭查找功能对话框。

启用扩展屏幕阅读器支持

默认情况下，按 **Tab** 键来导航窗格时，未按选项卡顺序包含标签和说明。某些屏幕阅读器 （如 JAWS）仅阅读具有焦点的屏幕对象。您可以通过启用扩展屏幕阅读器支持来按选项卡顺序包含标签和说明。

要启用扩展屏幕阅读器支持，请执行以下步骤：

步骤 1　依次选择 **Tools > Preferences**。

系统将显示 **Preferences** 对话框。

步骤 2　选中 **General** 选项卡上的 **Enable screen reader support** 复选框。

步骤 3　点击 **OK**。

步骤 4　重新启动 ASDM 以激活屏幕阅读器支持。

组织文件夹

配置视图和监控视图的导航窗格中的某些文件夹没有关联的配置窗格或监控窗格。这些文件夹用于组织相关的配置和监控任务。点击这些文件夹会在右侧 **Navigation** 窗格中显示子项的列表。您可以点击子项的名称以转至该项。

Home 窗格 （单模式和情景）

通过 ASDM **Home** 窗格，可以查看有关 ASA 的重要信息。**Home** 窗格中的状态信息每隔 10 秒进行更新。此窗格通常有两个选项卡：**Device Dashboard** 和 **Firewall Dashboard**。

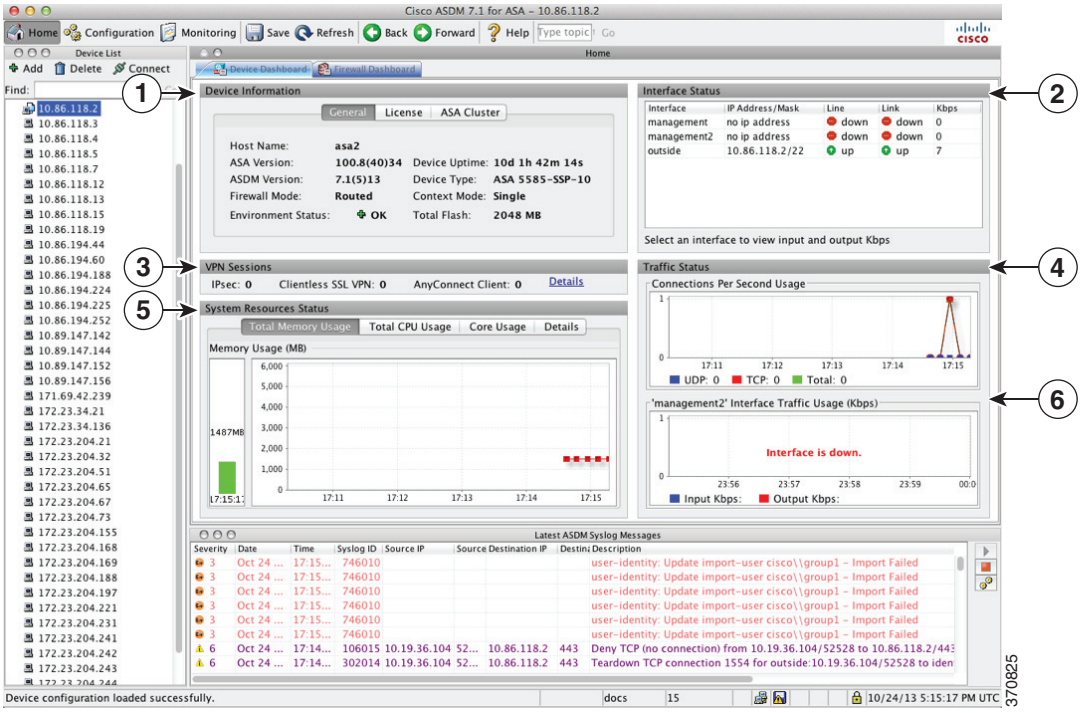
如果您在设备上安装了硬件或软件模块（如 IPS、CX 或 ASA FirePOWER 模块），则这些模块具有单独的选项卡。

Device Dashboard 选项卡

通过 **Device Dashboard** 选项卡，可以概览有关 ASA 的重要信息，如接口的状态、运行的版本、许可信息和性能。

下图显示 **Device Dashboard** 选项卡的元素。

图 3-2　　Device Dashboard 选项卡



图例

GUI 元素	说明
1	Device Information 窗格，第 3-15 页
2	Interface Status 窗格，第 3-16 页
3	VPN Sessions 窗格，第 3-16 页
4	Traffic Status 窗格，第 3-16 页
5	System Resources Status 窗格，第 3-16 页
6	Traffic Status 窗格，第 3-16 页
-	设备列表，第 3-9 页
-	Latest ASDM Syslog Messages 窗格，第 3-17 页

Device Information 窗格

Device Information 窗格包含两个显示设备信息的选项卡：**General** 选项卡和 **License** 选项卡。在 **General** 选项卡下，您有权访问 **Environment Status** 按钮，该按钮提供系统运行状况的概览视图：

General 选项卡

此选项卡显示有关 ASA 的基本信息：

- **Host name** - 显示设备的主机名。
- **ASA version** - 列出在设备上运行的 ASA 软件的版本。
- **ASDM version** - 列出在设备上运行的 ASDM 软件的版本。
- **Firewall mode** - 显示设备运行时所处的防火墙模式。
- **Total flash** - 显示当前使用的总 RAM。
- **ASA Cluster Role** - 启用集群时，显示此单元的角色 （Master 或 Slave）。
- **Device uptime** - 显示设备自从最新软件上载以来运行的时间。
- **Context mode** - 显示设备运行时所处的情景模式。
- **Total Memory** - 显示 ASA 上安装的 DRAM。
- **Environment status** - 显示系统运行状况。通过点击 **General** 选项卡中 **Environment Status** 标签右侧的加号 (+) 来查看硬件统计信息。您可以查看安装的电源数，跟踪风扇和电源模块的运行状态，并且跟踪 CPU 的温度和系统的环境温度。

  一般来说， **Environment Status** 按钮提供系统运行状况的概览视图。如果系统内的所有受监控硬件组件都是在正常范围内运行，则加号 (+) 按钮以绿色显示 OK。相反，如果硬件系统内的任何一个组件是在正常范围外运行，则加号 (+) 按钮会变成红色圆形以显示 Critical 状态并表明硬件组件需要立即注意。

  有关特定硬件统计信息的详细信息，请参阅特定设备的 《硬件指南》。

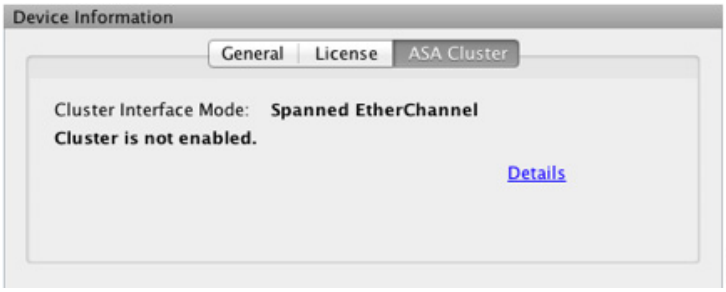
备注 如果没有足够的内存升级到 ASA 的最新版本，则系统将显示 **Memory Insufficient Warning** 对话框。请按照此对话框中显示的指导以受支持的方式继续使用 ASA 和 ASDM。点击 **OK** 以关闭此对话框。

License 选项卡

此选项卡显示许可功能的子集。点击 **More Licenses** 以查看详细许可证信息，或者输入新激活密钥，系统将显示 **Configuration > Device Management > Licensing > Activation Key** 窗格。

Cluster 选项卡

此选项卡显示集群接口模式以及集群状态。



Virtual Resources 选项卡 (ASAv)

此选项卡显示 ASAv 使用的虚拟资源，包括 vCPU 的数量、RAM 以及 ASAv 是配置过量还是配置不足。

Interface Status 窗格

此窗格显示每个接口的状态。如果选择接口行，则表下方会显示输入和输出吞吐量 （以 Kbps 为单位）。

VPN Sessions 窗格

此窗格显示 VPN 隧道状态。点击 **Details** 以依次转至 **Monitoring > VPN > VPN Statistics > Sessions** 窗格。

Failover Status 窗格

此窗格显示故障切换状态。

点击 **Configure** 以启动 High Availability and Scalability Wizard。完成向导后，系统将显示故障切换配置状态 （Active/Active 或 Active/Standby）。

如果配置了故障切换，请点击 **Details** 以依次打开 **Monitoring > Properties > Failover > Status** 窗格。

System Resources Status 窗格

此窗格显示 CPU 和内存使用情况统计信息。

Traffic Status 窗格

此窗格显示所有接口的每秒连接数图形和最低安全性接口的流量吞吐量图形。

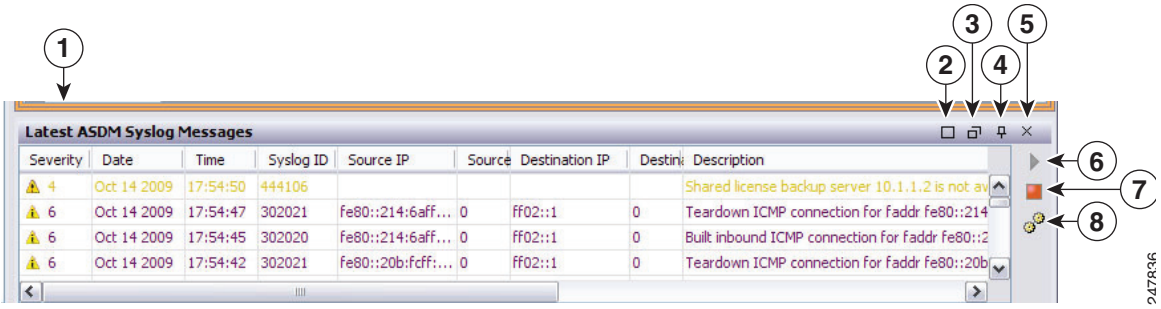
当配置包含多个最低安全级别接口，并且其中任何一个接口命名为 “outside” 时，该接口将用于流量吞吐量图形。否则， ASDM 从最低安全级别接口的字母顺序列表中选取第一个接口。

Latest ASDM Syslog Messages 窗格

此窗格显示 ASA 生成的最新系统消息，最多显示 100 条消息。如果已禁用日志记录，请点击 **Enable Logging** 将其启用。

图 3-3 显示 **Latest ASDM Syslog Messages** 窗格的元素。

图 3-3　　Latest ASDM Syslog Messages 窗格



图例

GUI 元素	说明
1	上下拖动**分隔线**以重新调整窗格大小。
2	展开窗格。点击**双正方形**图标以将窗格还原为默认大小。
3	使窗格浮动。点击**停靠窗格**图标以停靠窗格。
4	启用或禁用自动隐藏。启用自动隐藏时，将光标移至左下角的 **Latest ASDM Syslog Messages** 按钮上方，然后将显示该窗格。将光标从窗格移开，然后该窗格将消失。
5	关闭窗格。选择 **View Latest ASDM Syslog Messages** 以显示窗格。
6	点击右侧的**绿色**图标以继续更新系统日志消息的显示。
7	点击右侧的**红色**图标以停止更新系统日志消息的显示。
8	点击右侧的**过滤器**图标以打开 **Logging Filters** 窗格。

- 右键点击事件，然后选择 **Clear Content** 以清除当前消息。
- 右键点击事件，然后选择 **Save Content** 以将当前消息保存到 PC 上的文件。
- 右键点击事件，然后选择 **Copy** 以复制当前内容。
- 右键点击事件，然后选择 **Color Settings** 以根据系统日志消息的严重性更改其背景色和前景色。

Firewall Dashboard 选项卡

通过 **Firewall Dashboard** 选项卡，可以查看有关通过 ASA 的流量的重要信息。此控制面板根据您处于单情景模式还是多情景模式而异。在多情景模式下，可在每个情景内查看 **Firewall Dashboard**。

图 3-4 显示 **Firewall Dashboard** 选项卡的某些元素。

图 3-4　　Firewall Dashboard 选项卡

图例

GUI 元素	说明
1	Traffic Overview 窗格，第 3-19 页
2	Top 10 Access Rules 窗格，第 3-19 页
3	Top Usage Status 窗格，第 3-19 页
（未显示）	Top Ten Protected Servers Under SYN Attack 窗格，第 3-20 页
（未显示）	Top 200 Hosts 窗格，第 3-20 页
（未显示）	Top Botnet Traffic Filter Hits 窗格，第 3-20 页

Traffic Overview 窗格

默认情况下已启用。如果禁用基本威胁检测 （请参阅 《防火墙配置指南》），则此区域包含可启用基本威胁检测的 **Enable** 按钮。运行时统计信息包含以下*仅作显示用途*信息：

- 连接和 NAT 转换的数量。
- 因访问列表拒绝和应用检查而导致的每秒丢弃数据包的速率。
- 每秒丢弃在扫描攻击过程中标识的数据包或是检测到不完整会话的数据包 （如检测到 TCP SYN 攻击或未检测到数据 UDP 会话攻击）的速率。

Top 10 Access Rules 窗格

默认情况下已启用。如果禁用访问规则的威胁检测统计信息 （请参阅 《防火墙配置指南》），则此区域包含可启用访问规则统计信息的 **Enable** 按钮。

在 Table 视图中，可以在列表中选择规则，然后右键点击该规则以显示弹出菜单项 **Show Rule**。选择此项以转至 Access Rules 表，然后在此表中选择该规则。

Top Usage Status 窗格

默认情况下已禁用。此窗格包含以下四个选项卡：

- **Top 10 Services** - 威胁检测服务
- **Top 10 Sources** - 威胁检测服务
- **Top 10 Destinations** - 威胁检测服务
- **Top 10 Users** - 身份防火墙服务

前三个选项卡 **Top 10 Services**、 **Top 10 Sources** 和 **Top 10 Destinations** 提供威胁检测服务统计信息。每个选项卡包含可启用各威胁检测服务的 **Enable** 按钮。您可以根据 《防火墙配置指南》将其启用。

Top 10 Services Enable 按钮可同时启用端口和协议统计信息 （必须启用两者才会进行显示）。**Top 10 Sources** 和 **Top 10 Destinations Enable** 按钮可启用主机统计信息。系统将显示主机（源和目标）及端口和协议的排名靠前的使用状态统计信息。

第四个选项卡 **Top 10 Users** 提供身份防火墙服务统计信息。身份防火墙服务基于用户的身份提供访问控制。您可以基于用户名和用户组名而不是通过源 IP 地址来配置访问规则和安全策略。ASA 通过访问 IP - 用户映射数据库来提供此服务。

仅当已在 ASA 中配置身份防火墙服务 （其中包括配置以下附加组件：Microsoft Active Directory 和 Cisco Active Directory (AD) 代理）时， **Top 10 Users** 选项卡才会显示数据。

根据选择的选项， **Top 10 Users** 选项卡显示有关前 10 个用户的接收的 EPS 数据包数量、发送的 EPS 数据包数量和发送的攻击数的统计信息。对于每个用户 （显示为 *domain\user_name*），此选项卡显示该用户的平均 EPS 数据包数量、当前 EPS 数据包数量、触发器和总事件数。

注意　启用统计信息可能会影响 ASA 性能，具体取决于所启用统计信息的类型。启用主机统计信息对性能有重大影响，因此如果流量负载较高，您可能会考虑暂时启用此类型的统计信息。不过，启用端口统计信息影响不大。

Top Ten Protected Servers Under SYN Attack 窗格

默认情况下已禁用。此区域包含可启用功能的 **Enable** 按钮，也可以根据 《防火墙配置指南》将其启用。系统将显示遭受攻击的 10 大受保护服务器的统计信息。

对于平均攻击速率， ASA 在速率间隔 （默认情况下为 30 分钟）期间每 30 秒对数据进行采样。

如果有多个攻击者，则系统会显示 “<various>”，后跟最后一个攻击者的 IP 地址。

点击 **Detail** 以查看所有服务器（最多 1000 台）而不是仅 10 台服务器的统计信息。您还可以查看历史记录采样数据。ASA 在速率间隔期间对攻击数进行 60 次采样，因此对于默认的 30 分钟时间段，每 60 秒便会收集统计信息。

Top 200 Hosts 窗格

默认情况下已禁用。显示通过 ASA 连接的前 200 台主机。主机的每个条目都包含主机的 IP 地址和由主机启动的连接数，并且每 120 秒进行更新。输入 **hpm topnenable** 命令以启用此显示。

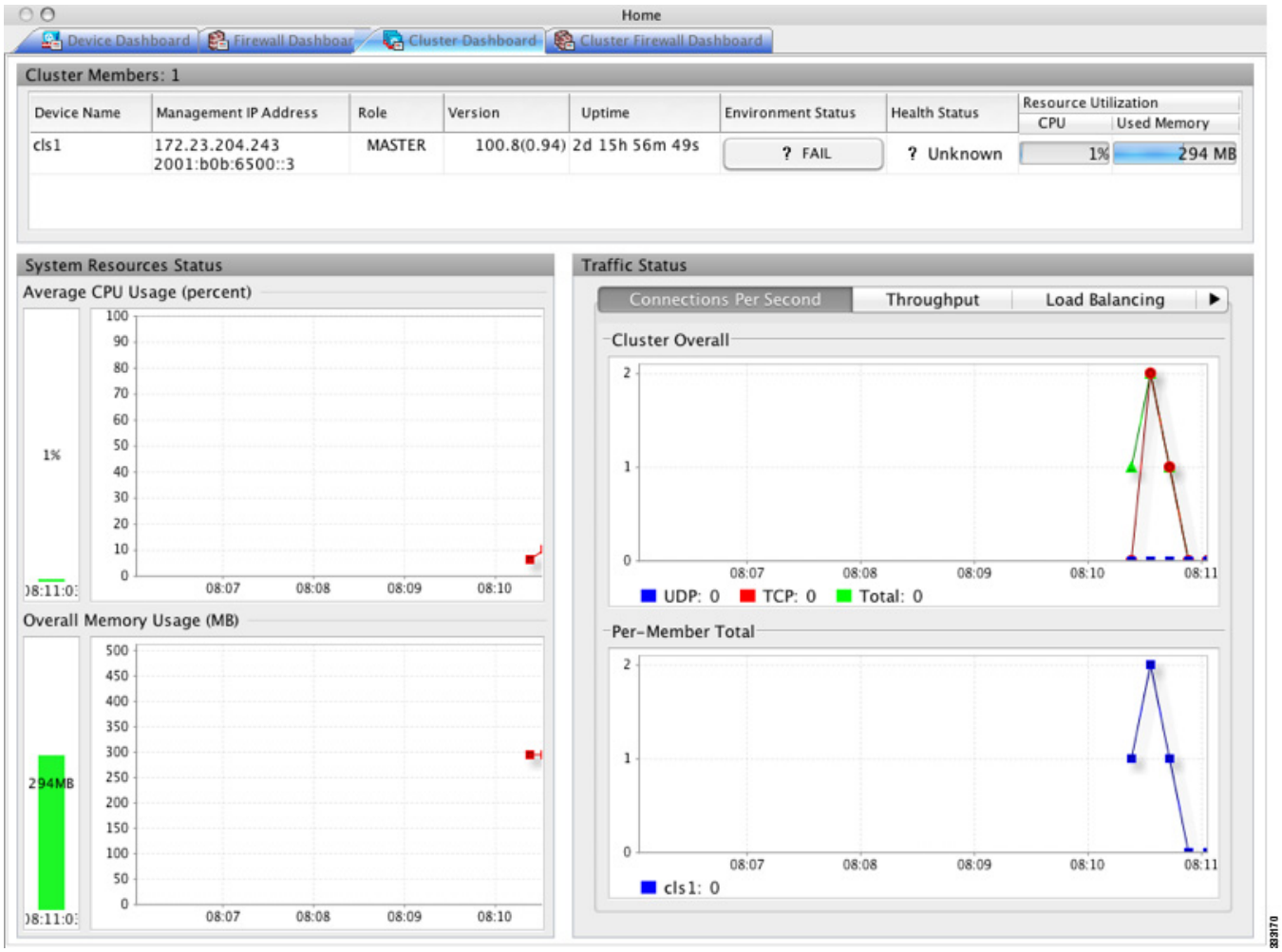
Top Botnet Traffic Filter Hits 窗格

默认情况下已禁用。此区域包含用于配置 Botnet Traffic Filter 的链接。10 大僵尸网络站点、端口和受感染主机的报告提供数据的快照，并且可能与自从开始收集统计信息以来起算的前 10 项不匹配。如果右键点击 IP 地址，则可以调用 whois 工具来了解有关僵尸网络站点的详细信息。

有关详情，请参阅防火墙配置指南。

Cluster Dashboard 选项卡

当启用 ASA 集群并连接到主设备时， **Cluster Dashboard** 选项卡会显示集群成员身份和资源利用率的摘要。



- **Cluster Members** - 显示有关构成集群的成员的名称和基本信息 （其管理 IP 地址、版本、在集群中的角色等）及其运行状况 （环境状态、运行状况和资源利用率）。

  注意　在多情景模式下，如果将 ASDM 连接到管理情景，然后更改为其他情景，则列出的管理 IP 地址不会更改为显示当前情景管理 IP 地址；它会继续显示管理情景管理 IP 地址，包括 ASDM 当前连接到的主集群 IP 地址。

- **System Resource Status** - 按集群范围和逐台设备显示跨集群和流量图形的资源利用率 （CPU 和内存）。
- **Traffic Status** - 每个选项卡具有以下图形。
  - **Connections Per Second** 选项卡：

    Cluster Overall - 显示整个集群内的每秒连接数。

    Per-Member Total - 显示每个成员的每秒平均连接数。

– **Throughput** 选项卡：

  Cluster Overall - 显示整个集群内的汇总出口吞吐量。

  Per-Member Throughput - 每个成员一行显示成员吞吐量。

– **Load Balancing** 选项卡：

  Per-Member Percentage of Total Traffic - 对于每个成员，显示成员接收的总集群流量的百分比。

  Per-Member Locally Processed Traffic - 对于每个成员，显示本地处理的流量的百分比。

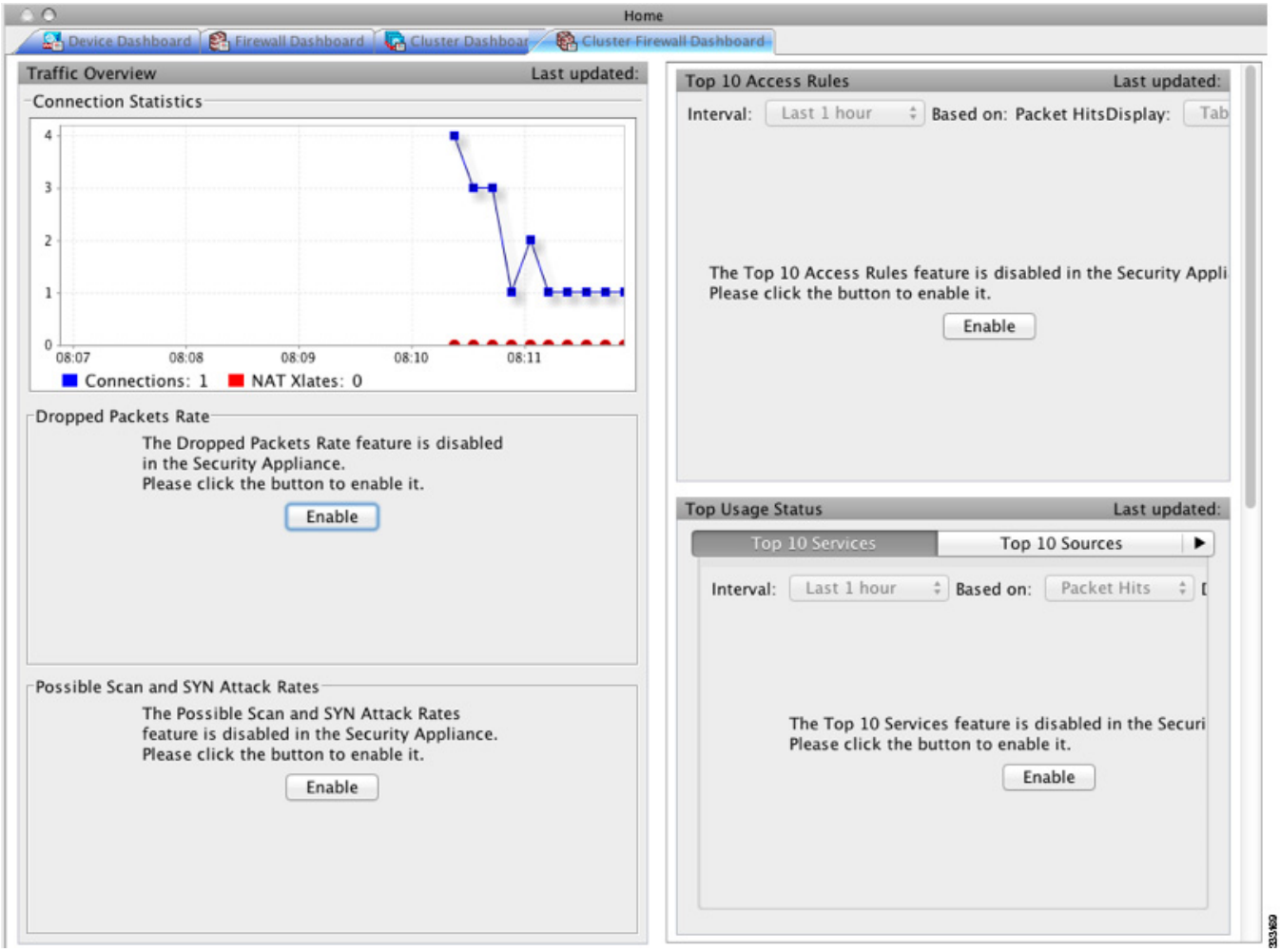
– **Control Link Usage** 选项卡：

  Per-Member Receival Capacity Utilization - 对于每个成员，显示接收容量的使用情况。

  Per-Member Transmittal Capacity Utilization - 对于每个成员，显示传输容量的使用情况。

Cluster Firewall Dashboard 选项卡

Cluster Firewall Dashboard 选项卡显示流量概况和 “前 N 大”统计信息，类似于 **Firewall Dashboard** 中显示的此类信息，但是跨整个集群进行了汇总。



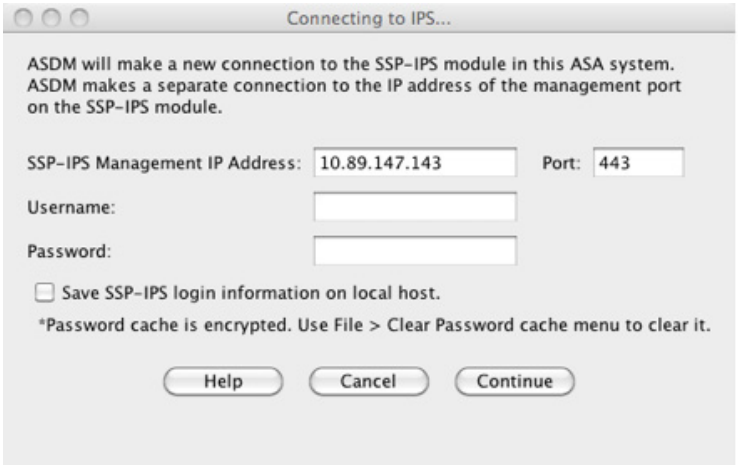
Intrusion Prevention 选项卡

通过 **Intrusion Prevention** 选项卡，可以查看有关 IPS 的重要信息。仅当您在 ASA 上安装有 IPS 模块时，才会显示此选项卡。

要连接到 IPS 模块，请执行以下步骤：

步骤 1　点击 **Intrusion Prevention** 选项卡。

系统将显示 **Connecting to IPS** 对话框。



步骤 2　输入 IP 地址、端口、用户名和密码。默认 IP 地址和端口为 192.168.1.2:443。默认用户名和密码为 **cisco** 和 **cisco**。

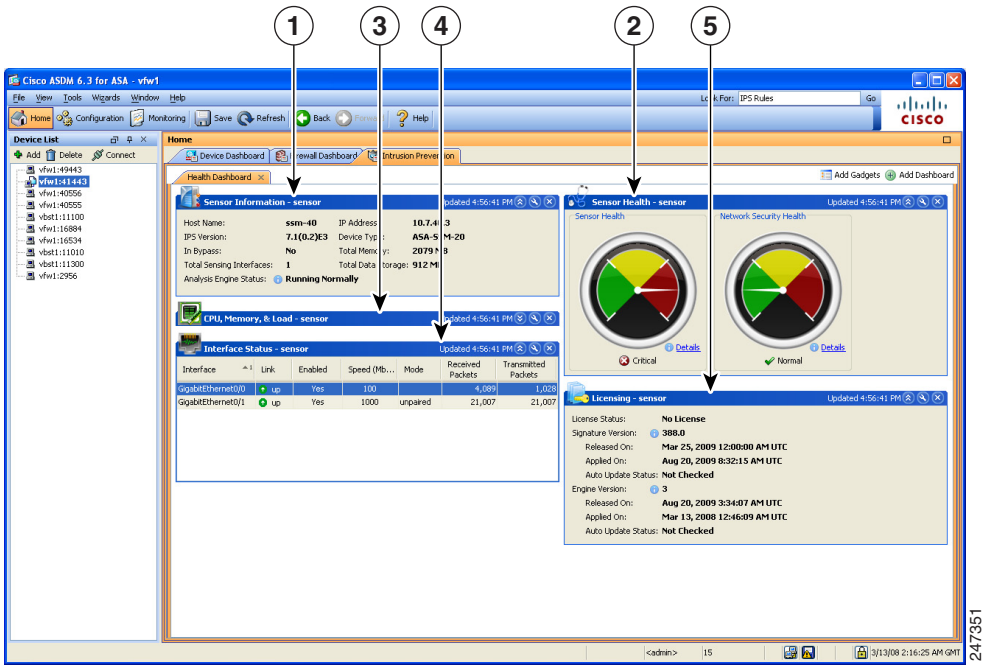
步骤 3　选中 **Save IPS login information on local host** 复选框以将登录信息保存在本地 PC 上。

步骤 4　点击 **Continue**。

有关入侵防护的详细信息，请参阅 《防火墙配置指南》。

下图显示位于 **Intrusion Prevention** 选项卡上的 **Health Dashboard** 选项卡的元素。

图 3-5　　Intrusion Prevention 选项卡 (Health Dashboard)

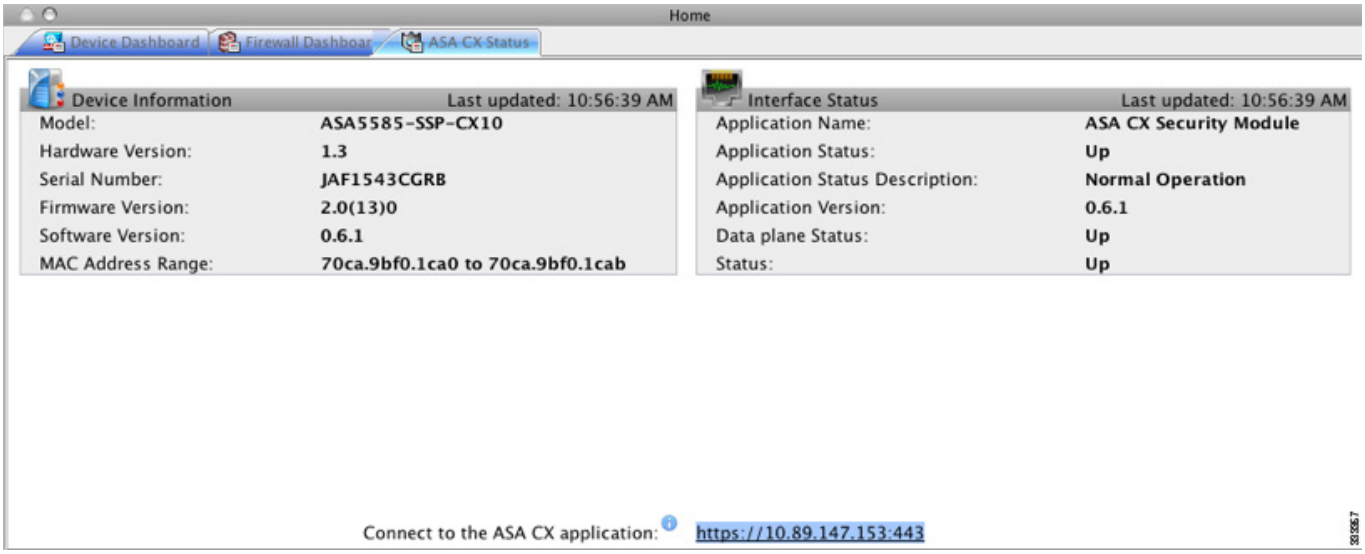


图例

GUI 元素	说明
1	**Sensor Information** 窗格。
2	**Sensor Health** 窗格。
3	**CPU**、 **Memory** 和 **Load** 窗格。
4	**Interface Status** 窗格。
5	**Licensing** 窗格。

ASA CX Status 选项卡

通过 **ASA CX Status** 选项卡，可以查看有关 ASA CX 模块的重要信息。仅当您在 ASA 上安装有 ASA CX 模块时，才会显示此选项卡。



ASA FirePOWER选项卡

通过 **ASA FirePOWER Status** 选项卡，可以查看有关模块的重要信息。这包括模块信息 （如型号、序列号、软件版本）和模块状态 （如应用名称和状态、数据平面状态和总体状态）。如果已向 FireSIGHT 管理中心注册模块，则您可以点击链接以打开应用并执行进一步分析和模块配置。

仅当您在设备中安装有 ASA FirePOWER 模块时，才会显示此选项卡。

如果使用 ASDM （而不是 FireSIGHT 管理中心）管理 ASA FirePOWER 模块，还有其他选项：

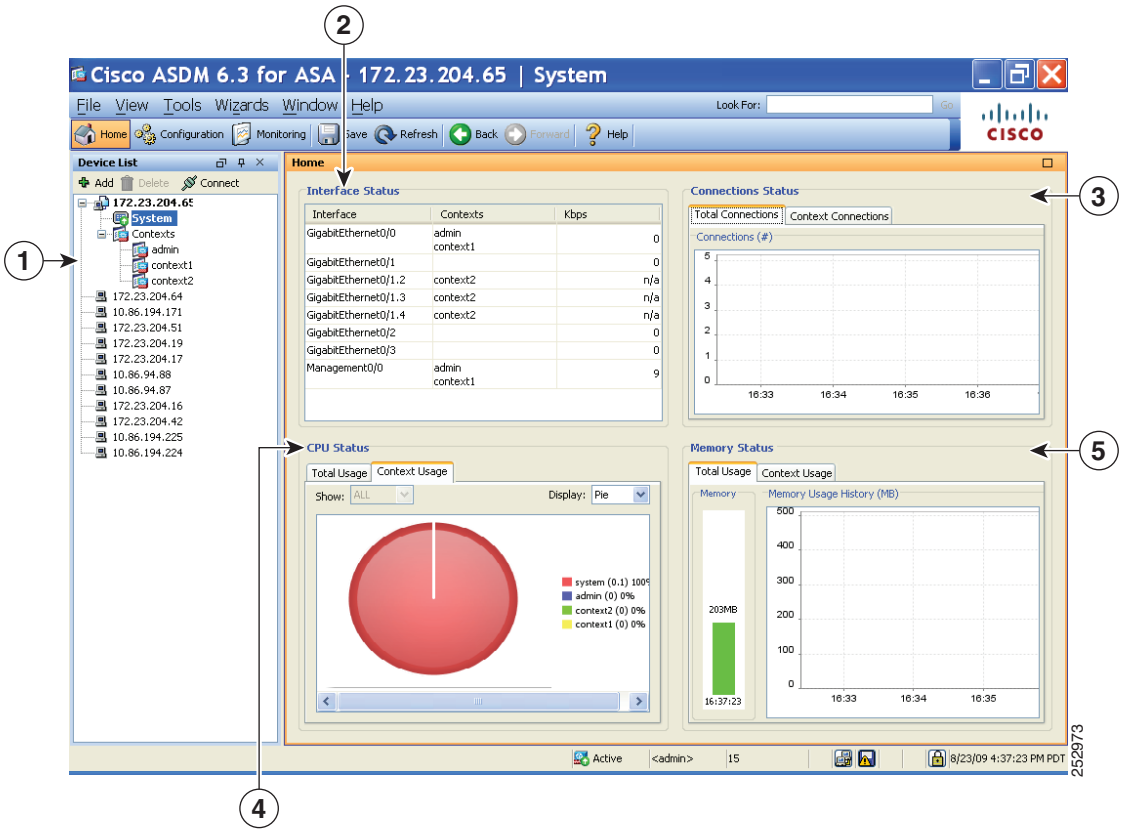
- **ASA FirePOWER Dashboard** - 控制面板提供关于模块上运行的软件、产品更新、许可、系统负载、磁盘使用、系统时间和接口状态的摘要信息。
- **ASA FirePOWER Reporting** - 报告页面提供各种模块统计信息的前 10 个控制面板，例如通过模块的流量的 Web 类别、用户、来源和目标。

Home 窗格 (System)

通过 ASDM System **Home** 窗格，可以查看有关 ASA 的重要状态信息。ASDM System **Home** 窗格中提供的许多详细信息在 ASDM 中的其他位置都可用，但是此窗格仅概要显示 ASA 的运行方式。System **Home** 窗格中的状态信息每 10 秒进行更新。

下图显示 System **Home** 窗格的元素。

图 3-6　　System Home 窗格



图例

GUI 元素	说明
1	系统与情景选择。
2	**Interface Status** 窗格。选择接口以查看通过该接口的总流量。
3	**Connection Status** 窗格。
4	**CPU Status** 窗格。
5	**Memory Status** 窗格。

定义 ASDM 首选项

您可以定义某些 ASDM 设置的行为。

要更改 ASDM 中的各种设置，请执行以下步骤：

步骤 1　依次选择 **Tools > Preferences**。

系统将显示 **Preferences** 对话框，其中含有三个选项卡：**General**、 **Rules Table** 和 **Syslog**。

步骤 2　要定义设置，请点击这些选项卡之一：**General** 选项卡可指定常规首选项， **Rules Table** 选项卡可指定 Rules 表的首选项，**Syslog** 选项卡可指定 **Home** 窗格中显示的系统日志消息的外观并支持为 NetFlow 相关系统日志消息显示警告消息。

步骤 3　在 **General** 选项卡上，请指定以下内容：

- 选中 **Warn that configuration in ASDM is out of sync with the configuration in ASA** 复选框以在启动配置与运行配置不再相互同步时获取通知。
- 选中 **Show configuration restriction message to read-only user** 复选框以在启动时向只读用户显示以下消息。默认情况下，会选中此选项。

  ```
  "You are not allowed to modify the ASA configuration, because you do not have
  sufficient privileges."
  ```

- 选中 **Show configuration restriction message on a slave unit in an ASA cluster** 复选框以向连接到从属单元的用户显示配置限制消息。
- 选中 **Confirm before exiting ASDM** 复选框以在尝试关闭 ASDM 时显示提示来确认要退出。默认情况下，会选中此选项。
- 选中 **Enable screen reader support (requires ASDM restart)** 复选框以使屏幕阅读器能够工作。您必须重新启动 ASDM 才能启用此选项。
- 选中 **Warn of insufficient ASA memory when ASDM loads** 复选框以在最小 ASA 内存量不足而无法运行 ASDM 应用中的完整功能时接收通知。ASDM 在启动时以文本横幅消息形式显示内存，在 ASDM 的标题栏文本中显示消息，并且每 24 小时发送一次系统日志告警。
- 在 **Communications** 区域中：
  - 选中 **Preview commands before sending them to the device** 复选框以查看由 ASDM 生成的 CLI 命令。
  - 选中 **Enable cumulative (batch) CLI delivery** 复选框以将单个组中的多个命令发送到 ASA。
  - 输入为使配置发送超时消息的最小时间量 （以秒为单位）。默认值为 60 秒。
- 在 **Logging** 区域中：
  - 选中 **Enable logging to the ASDM Java console** 复选框以配置 Java 日志记录。
  - 通过从下拉列表中选择 **Logging Level** 来设置严重级别。
- 在 **Packet Capture Wizard** 区域中，要显示捕获的数据包，请输入 **Network Sniffer Application** 的名称，或者点击 **Browse** 以在文件系统中进行查找。

步骤 4　在 **Rules Table** 选项卡上，指定以下内容：

- 通过显示设置，可以更改规则在 Rules 表中的显示方式。
  - 选中 **Auto-expand network and service object groups with specified prefix** 复选框以显示根据 Auto-Expand Prefix 设置自动展开的网络组和服务对象组。
  - 输入网络组和服务对象组的前缀，以在 **Auto-Expand Prefix** 字段中显示时自动展开。
  - 选中 **Show members of network and service object groups** 复选框以在 Rules 表中显示网络组和服务对象组的成员及组名。如果未选中该复选框，仅会显示组名。

  - 在 **Limit Members To** 字段中输入要显示的网络组和服务对象组的编号。显示对象组成员时，仅会显示前 *n* 个成员。
  - 选中 **Show all actions for service policy rules** 复选框以在 Rules 表中显示所有操作。未选中时，系统将显示摘要。
- 通过部署设置，可以在将更改部署到 Rules 表时配置 ASA 的行为。
  - 选中 **Issue “clear xlate” command when deploying access lists** 复选框以在部署新访问列表时清除 NAT 表。此设置确保在 ASA 上配置的访问列表应用于所有已转换地址。
- 通过 Access Rule Hit Count Settings，可以配置命中计数在 Access Rules 表中的更新频率。命中计数仅适用于显式规则。对于 Access Rules 表中的隐式规则将不显示任何命中计数。
  - 选中 **Update access rule hit counts automatically** 复选框以使命中计数在 Access Rules 表中自动更新。
  - 指定命中计数列在 Access Rules 表中的更新频率 （以秒为单位）。有效值为 10 到 86400 秒。

步骤 5　在 **Syslog** 选项卡上，指定以下内容：

- 在 **Syslog Colors** 区域中，可以通过配置处于各严重性级别的消息的背景色或前景色来定制消息显示。**Severity** 列按名称和编号列出各严重性级别。要更改处于指定严重性级别的消息的背景色或前景色，请点击对应的列。系统将显示 **Pick a Color** 对话框。点击以下选项卡之一：
  - 从 **Swatches** 选项卡上的调色板中选择颜色，然后点击 **OK**。
  - 在 **HSB** 选项卡上指定 H、 S 和 B 设置，然后点击 **OK**。
  - 在 **RGB** 选项卡上指定 Red、 Green 和 Blue 设置，然后点击 **OK**。
- 选中 **NetFlow** 区域中的 **Warn to disable redundant syslog messages when NetFlow action is first applied to the global service policy rule** 复选框以支持显示表明要禁用冗余系统日志消息的警告消息。

步骤 6　在这三个选项卡上指定设置后，点击 **OK** 以保存设置并关闭 **Preferences** 对话框。

注意　每次选中或取消选中首选项设置时，更改会保存到 .conf 文件，并且可供此时在工作站上运行的所有其他 ASDM 会话使用。必须重新启动 ASDM 以使所有更改生效。

使用 ASDM Assistant 进行搜索

通过 ASDM Assistant 工具，可以搜索并查看有关某些任务的实用 ASDM 操作步骤帮助。

依次选择 **View > ASDM Assistant > How Do I?** 以访问信息，或者在菜单栏中输入来自 **Look For** 字段的搜索请求。从 **Find** 下拉列表中 选择 **How Do I?** 以开始搜索。

要查看 ASDM Assistant，请执行以下步骤：

步骤 1　依次选择 **View > ASDM Assistant**。

系统将显示 **ASDM Assistant** 窗格。

步骤 2　在 **Search** 字段中输入要查找的信息，然后点击 **Go**。

所请求的信息显示在 **Search Results** 窗格中。

步骤 3　点击 **Search Results and Features** 部分中显示的任何链接以获取更多详细信息。

启用历史记录度量值

通过 **Configuration > Device Management > Advanced > History Metrics** 窗格，可以将 ASA 配置为保留各种统计信息的历史记录，ASDM 可以在任何图形/表上将其显示。如果不启用历史记录度量值，则只能实时查看监控统计信息。通过启用历史记录度量值，可以查看过去 10 分钟、 60 分钟、 12 小时或 5 天的统计信息图形。

要配置历史记录度量值，请执行以下步骤：

步骤 1　依次选择 **Configuration > Device Management > Advanced > History Metrics**。

系统将显示 **History Metrics** 窗格。

步骤 2　选中 **ASDM History Metrics** 复选框以启用历史记录度量值，然后点击 **Apply**。

不受支持的命令

ASDM 支持几乎所有可用于 ASA 的命令，但是， ASDM 在现有配置中会忽略一些命令。其中大多数命令可以保留在配置中；有关详细信息，请参阅 **Tools > Show Commands Ignored by ASDM on Device**。

已忽略和仅供查看的命令

下表列出通过 CLI 添加时 ASDM 在配置中支持但无法在 ASDM 中添加或编辑的命令。如果 ASDM 忽略命令，则在 ASDM GUI 中根本不显示该命令。如果该命令仅供查看，则其会显示在 GUI 中，但是无法对其进行编辑。

表 3-5　不受支持命令的列表

不受支持的命令	ASDM 行为
capture	已忽略。
coredump	已忽略。只能使用 CLI 对此进行配置。
crypto engine large-mod-accel	已忽略。
dhcp-server (tunnel-group name general-attributes)	ASDM 对于所有 DHCP 服务器仅允许一种设置。
eject	不受支持。
established	已忽略。
failover timeout	已忽略。
fips	已忽略。
nat-assigned-to-public-ip	已忽略。
pager	已忽略。
pim accept-register route-map	已忽略。您只能使用 ASDM 配置 **list** 选项。

表 3-5　　不受支持命令的列表（续）

不受支持的命令	ASDM 行为

service-policy global	如果它使用 **match access-list** 类，则会进行忽略。例如：
	`access-list myacl extended permit ip any any`
	`class-map mycm`
	`  match access-list myacl`
	`policy-map mypm`
	`  class mycm`
	`  inspect ftp`
	`service-policy mypm global`

set metric	已忽略。
sysopt nodnsalias	已忽略。
sysopt uauth allow-http-cache	已忽略。
terminal	已忽略。
threat-detection rate	已忽略。

不受支持命令的影响

如果 ASDM 加载现有运行配置并查找其他不受支持命令，则 ASDM 操作不受影响。依次选择 **Tools > Show Commands Ignored by ASDM on Device** 以查看不受支持命令。

不支持不连续子网掩码

ASDM 不支持不连续子网掩码，如 255.255.0.255。例如，不能使用以下子网掩码：

```
ip address inside 192.168.2.1 255.255.0.255
```

ASDM CLI 工具不支持交互式用户命令

ASDM CLI 工具不支持交互式用户命令。如果输入需要交互确认的 CLI 命令，则 ASDM 会提示输入 “[yes/no]”，但是无法识别输入。然后， ASDM 超时等待响应。

例如：

1. 依次选择 **Tools > Command Line Interface**。
2. 输入 **crypto key generate rsa** 命令。

   ASDM 生成默认的 1024 位 RSA 密钥。
3. 再次输入 **crypto key generate rsa** 命令。

   ASDM 会显示以下错误，而不是通过覆盖以前的 RSA 密钥来重新生成 RSA 密钥：

```
Do you really want to replace them? [yes/no]:WARNING: You already have RSA
ke0000000000000$A key
Input line must be less than 16 characters in length.

%Please answer 'yes' or 'no'.
Do you really want to replace them [yes/no]:

%ERROR: Timed out waiting for a response.
ERROR: Failed to create new RSA keys names <Default-RSA-key>
```

解决方法：

- 可以通过 ASDM 窗格来配置需要用户交互的大多数命令。
- 对于带有 **noconfirm** 选项的 CLI 命令，请在输入 CLI 命令时使用此选项。例如：

```
crypto key generate rsa noconfirm
```

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 5 章 “适用于 ASAv 的智能软件许可”。

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

本节列出了适用于每个型号的功能许可证：

- 带 SSP-40 和 SSP-60 的 ASA 5585-X，第 4-11 页
- ASA 服务模块，第 4-12 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 4-23 页。

有关许可证的详细信息，请参阅许可证说明，第 4-13 页。

ASA 5506-X、 ASA 5506W-X 和 ASA 5506H-X

表 4-1　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)*
故障转移	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 4-2　　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 4-3　　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*

表 4-3　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					
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*
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 4-4　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*

表 4-4　　ASA 5515-X 许可证功能 （续）

许可证	基础许可证	
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	
	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）	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 4-5　　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	

表 4-5　　ASA 5516-X 许可证功能 （续）

许可证	基础许可证	
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）	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 4-6　　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							

表 4-6　　ASA 5525-X 许可证功能 （续）

许可证	基础许可证				
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	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 4-7　　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*			

表 4-7　　ASA 5545-X 许可证功能 （续）

许可证	基础许可证	
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 4-8　　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 4-9　　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 4-10　　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 4-11　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 4-12　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 4-13　　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 4-13　　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**均根据此限制进行计数。

表 4-13　　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 4-13　　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。
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 4-17 页
- 永久许可证，第 4-17 页
- 基于时间的许可证，第 4-17 页

- 共享型 AnyConnect 高级版许可证 （AnyConnect 3 和更早版本），第 4-20 页
- 故障切换或 ASA 集群许可证，第 4-20 页
- 无负载加密型号，第 4-23 页
- 许可证常见问题解答，第 4-23 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 4-32 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 4-18 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 4-17 页
- 基于时间的许可证计时器工作方式，第 4-18 页
- 如何合并永久许可证和基于时间的许可证，第 4-18 页
- 堆叠基于时间的许可证，第 4-19 页
- 基于时间的许可证到期，第 4-19 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 4-14　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 4-32 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 4-26 页
- 基于时间的许可证到期，第 4-19 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 4-26 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

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 到 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 4-32 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 4-15，第 4-26 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 4-32 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 4-20 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 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials** 窗格在配置中禁用 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 4-25 页
- 激活或停用密钥，第 4-26 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，方法是依次选择 **Configuration > Device Management > Licensing > Activation Key**（在多情景模式下，查看系统执行空间中的序列号）。

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 4-15　永久许可证重新加载要求

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

操作步骤

步骤 1　依次选择 **Configuration > Device Management**，然后根据您的型号选择 **Licensing > Activation Key** 或 **Licensing Activation Key** 窗格。

步骤 2　要输入新的永久激活密钥或基于时间的激活密钥，请在 **New Activation Key** 字段中输入新的激活密钥。

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。例如：

```
ASA0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

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。如果输入新的基于时间的密钥，则该密钥将默认处于活动状态，并会显示在 Time-based License Keys Installed 表中。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。

步骤 3　要激活或停用某个已安装的基于时间的密钥，请在 **Time-based License Keys Installed** 表中选择该密钥，然后点击 **Activate** 或 **Deactivate**。

对于每个功能，您只能有一个基于时间的密钥处于活动状态。

步骤 4　点击 **Update Activation Key**。

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。如果需要，系统会提示您重新加载。

相关主题

- 基于时间的许可证，第 4-17 页
- 表 4-15，第 4-26 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

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

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

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。

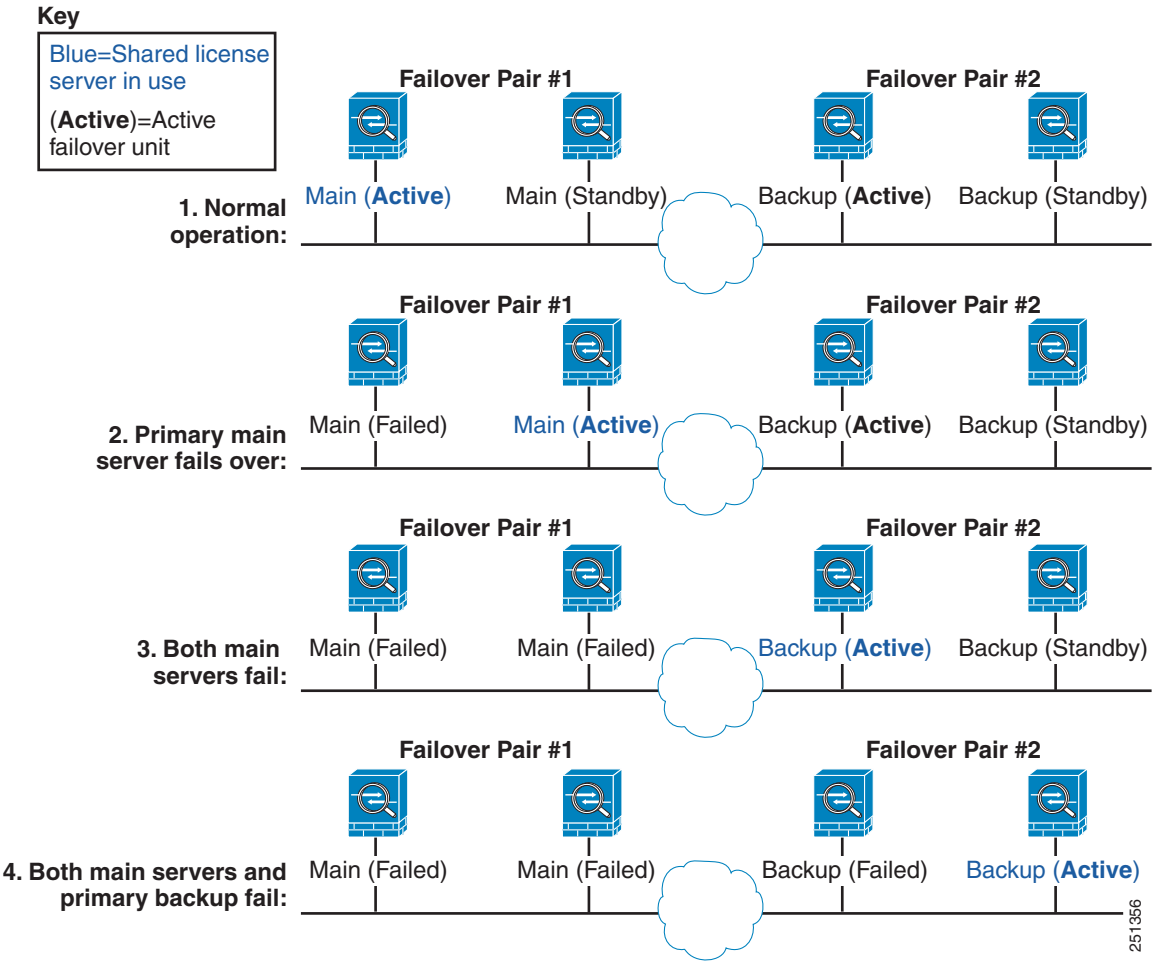
备注　备用服务器机制独立于故障切换，但与其兼容。

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 4-1）。

图 4-1　　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 4-28 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　依次选择 **Configuration > Device Management > Licenses > Shared SSL VPN Licenses** 窗格。

步骤 2　在 **Shared Secret** 字段中，输入由 4 至 128 个 ASCII 字符组成的字符串，作为共享密钥。

拥有此密钥的任何参与者都可以使用许可证服务器。

步骤 3　（可选）在 **TCP IP Port** 字段中，输入服务器用于侦听来自参与者的 SSL 连接的端口，该端口号介于 1 和 65535 之间。

默认值为 TCP 端口 50554。

步骤 4　（可选）在 **Refresh interval** 字段中，输入介于 10 和 300 秒之间的刷新间隔。

该值会提供给参与者，用于设置它们应与服务器通信的频率。默认值为 30 秒。

步骤 5　在 **Interfaces that serve shared licenses** 区域中，对于参与者在其上与服务器进行连接的任何接口选中 **Shares Licenses** 复选框。

步骤 6　（可选）要确定备用服务器，请在 **Optional backup shared SSL VPN license server** 区域中执行以下操作：

a. 在 **Backup server IP address** 字段中，输入备用服务器 IP 地址。

b. 在 **Primary backup server serial number** 字段中，输入备用服务器序列号。

c. 如果备用服务器是故障切换对的一部分，请在 **Secondary backup server serial number** 字段中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 7　点击 **Apply**。

配置共享许可参与者和可选备用服务器

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，以及如何才能选择将参与者配置为备用服务器。

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　依次选择 **Configuration > Device Management > Licenses > Shared SSL VPN Licenses** 窗格。

步骤 2　在 Shared Secret 字段中，输入由 4 至 128 个 ASCII 字符组成的字符串，作为共享密钥。

步骤 3　（可选）在 TCP IP Port 字段中，输入在其上使用 SSL 与服务器进行通信的端口，该端口号介于 1 和 65535 之间。

默认值为 TCP 端口 50554。

步骤 4　（可选）要将参与者确定为备用服务器，请在 Select backup role of participant 区域中执行以下操作：

a. 点击 **Backup Server** 单选按钮。

b. 对于参与者在其上与备用服务器进行连接的任何接口选中 **Shares Licenses** 复选框。

步骤 5　点击 **Apply**。

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 4-32 页
- 监控共享许可证，第 4-33 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 4-23 页。

操作步骤

步骤 1　要查看运行许可证（包括永久许可证和所有活动的基于时间的许可证），请依次选择 **Configuration > Device Management > Licensing > Activation Key** 窗格并查看 Running Licenses 区域。

在多情景模式下，通过依次选择 **Configuration > Device Management > Activation Key** 窗格在系统执行空间中查看激活密钥。

对于故障切换对，所显示的运行许可证是主设备和辅助设备的合并许可证。有关详情，请参见如何合并故障切换或 ASA 集群许可证，第 4-21 页。对于具有数字值的基于时间的许可证（未合并持续时间），License Duration 列会显示主设备或辅助设备中基于最短时间的许可证；当该许可证到期时，将会显示另一台设备的许可证的持续时间。

步骤 2　（可选）要查看基于时间的许可证的详细信息（例如许可证中包含的功能和持续时间），请在 Time-Based License Keys Installed 区域中，选择许可证密钥，然后点击 **Show License Details**。

步骤 3　（可选）对于故障切换设备，要查看该设备上安装的许可证（而不是主设备和辅助设备的合并许可证），请在 Running Licenses 区域中，点击 **Show information of license specifically purchased for this device alone**。

监控共享许可证

要监控共享许可证，请依次选择 **Monitoring > VPN > Clientless SSL VPN > Shared Licenses**。

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。

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。

功能名称	平台版本	说明
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 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials 窗格将其禁用以使用其他许可证。
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。 修改了以下屏幕：Configuration > Device Management > Licensing > Activation Key。
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。

功能名称	平台版本	说明
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。 修改了以下屏幕：Configuration > Device Management > Licensing > Activation Key。
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。 修改了以下屏幕：Configuration > Device Management > Licensing > Activation Key。
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。
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。

功能名称	平台版本	说明
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。
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

本节列出可用于 ASAv 的许可证授权。

ASAv5 和 ASAv10

表 5-1　　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 5-2　　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 5-3　　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**均根据此限制进行计数。
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。

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

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 18-10 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。
- 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。
- 此外，在配置过程中，您还可以选择配置 HTTP 代理。

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 5-7 页。

步骤 2　设置智能许可证授权，第 5-7 页。

步骤 3　向许可证颁发机构注册 ASAv，第 5-8 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　依次选择 **Configuration > Device Management > Smart Call-Home**。

步骤 2　选中 **Enable HTTP Proxy**。

步骤 3　在 **Proxy server** 和 **Proxy port** 字段中输入代理 IP 地址和端口。例如，为 HTTPS 服务器输入端口 443。

步骤 4　点击 **Apply**。

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　依次选择 **Configuration > Device Management > Licensing > Smart Licensing**。

步骤 2　选中 **Enable Smart license configuration**。

步骤 3　从 **Feature Tier** 下拉菜单中，选择 **Standard**。

仅标准层可用。

步骤 4　从 **Throughput Level** 下拉菜单中，选择 **100M**、 **1G** 或 **2G**。

步骤 5　点击 **Apply**。

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　依次选择 **Configuration > Device Management > Licensing > Smart Licensing**。

步骤 3　点击 **Register**。

步骤 4　在 **ID Token** 字段中输入注册令牌。

步骤 5　（可选）点击 **Force registration** 复选框，可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 registration**。

步骤 6　点击 **Register**。

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 5-8 页
- 更新 ID 证书或许可证授权，第 5-9 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　依次选择 **Configuration > Device Management > Licensing > Smart Licensing**。

步骤 2　点击 **Unregister**。

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　依次选择 **Configuration > Device Management > Licensing > Smart Licensing**。

步骤 2　要更新 ID 证书，请点击 **Renew ID Certificate**。

步骤 3　要更新许可证授权，请点击 **Renew Authorization**。

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 5-9 页
- 查看智能许可证状态，第 5-9 页

查看当前许可证

请参阅以下屏幕以查看许可证：

- **Configuration > Device Management > Licensing > Smart Licensing** 窗格并查看 **Effective Running Licenses** 区域。

查看智能许可证状态

请参阅以下屏幕以查看许可证状态：

- **Monitoring > Properties > Smart License**

  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。

- **Configuration > Device Management > Licensing > Smart Licensing > Registration Status**

  显示当前智能许可证注册状态。

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。 引入或修改了以下屏幕： **Configuration > Device Management > Licensing > Smart License** **Configuration > Device Management > Smart Call-Home Monitoring > Properties > Smart License**

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

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

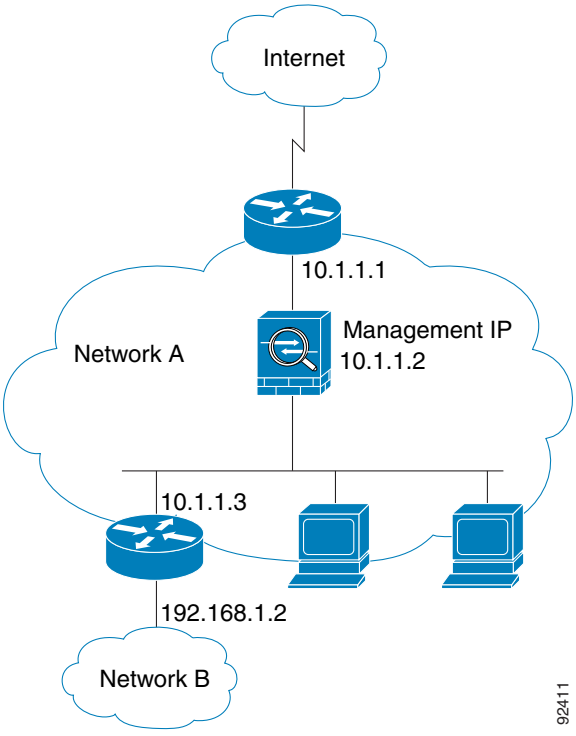
通常情况下，防火墙是一个路由跃点，并充当与其中一个被屏蔽子网连接的主机的默认网关。另一方面，透明防火墙是第 2 层防火墙，充当 “嵌入式防火墙” 或 “隐藏防火墙”，而不被视为已连接设备的路由器跃点。

在网络中使用透明防火墙

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 6-1 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 6-1　　透明防火墙网络

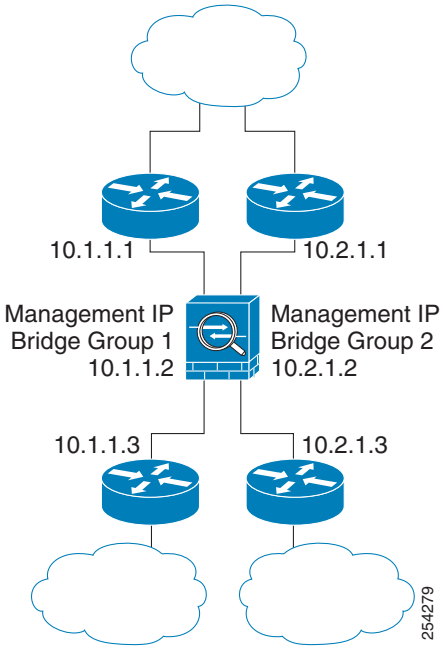


网桥组

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 6-2 显示连接到 ASA 的两个网络，后者具有两个网桥组。

图 6-2　　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 6-3 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 11-2 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 9-14 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 15-4 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（单模式），第 6-7 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。

透明模式下不支持的功能

表 6-1 列出透明模式下不支持的功能。

表 6-1　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 （单模式）

本节介绍如何使用 CLI 更改防火墙模式。对于单模式和对于多模式下当前连接的情景 （通常为管理员情景），无法在 ASDM 中更改模式。对于其他多模式情景，可以在 ASDM 中为每个情景设置模式；请参阅配置安全情景，第 8-17 页。

备注　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 6-6 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。
- 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 6-8 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 6-9 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　依次选择 **Configuration > Device Management > Advanced > ARP > ARP Static Table** 窗格。

步骤 2　（可选）在 **ARP Timeout** 字段中输入一个值，以设置*动态* ARP 条目的 ARP 超时。

该字段在 ASA 重建 ARP 表之前设置介于 60 和 4294967 秒之间的时间。默认值为 14400 秒。重建 ARP 表会自动更新新的主机信息并删除旧的主机信息。由于主机信息频繁更改，因此可能要减少超时。

步骤 3　（可选；仅限 8.4(5)），要允许未连接的子网，请选中 **Allow non-connected subnets** 复选框。默认情况下， ASA ARP 缓存仅包含来自直连子网的条目。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。

步骤 4　点击**Add**。

系统将显示 **Add ARP Static Configuration** 对话框。

步骤 5　从 **Interface** 下拉列表中选择连接到主机网络的接口。

步骤 6　在 **IP Address** 字段中输入主机的 IP 地址。

步骤 7　在 **MAC Address** 字段中输入主机的 MAC 地址，例如 00e0.1e4e.3d8b。

步骤 8　选中 **Proxy ARP** 复选框，以对此地址执行代理 ARP。

如果 ASA 收到面向指定 IP 地址的 ARP 请求，则会使用指定的 MAC 地址作出响应。

步骤 9　点击 **OK**，然后点击 **Apply**。

启用 ARP 检测

本节介绍如何启用 ARP 检测。

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Advanced > ARP > ARP Inspection** 窗格。

步骤 2　选择要启用 ARP 检测的接口行，然后点击 **Edit**。

系统将显示 **Edit ARP Inspection** 对话框。

步骤 3　选中 **Enable ARP Inspection** 对话框，以启用 ARP 检测。

步骤 4　（可选）选中 **Flood ARP Packets** 复选框，以通过泛洪方式传输不匹配的 ARP 数据包。

默认情况下，会以泛洪方式将不匹配的静态 ARP 条目的任何元素传输出除源接口以外的所有接口。如果 MAC 地址、 IP 地址或接口之间不匹配，则 ASA 会丢弃数据包。

如果取消选中此复选框，则会丢弃所有不匹配的数据包，这样会将通过 ASA 的 ARP 仅限于静态条目。

注意　管理 0/0 或 0/1 接口或子接口 （如果有）绝不会以泛洪方式传输数据包，即使此参数设置为 flood 也如此。

步骤 5　点击 **OK**，然后点击 **Apply**。

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

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 6-8 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　依次选择 **Configuration > Device Setup > Bridging > MAC Address Table** 窗格。

步骤 2　（可选）在 **Dynamic Entry Timeout** 字段中输入一个值，以设置 MAC 地址条目在超时前保留在 MAC 地址表中的时间。

该值介于 5 到 720 分钟 （12 小时）之间。默认值为 5 分钟。

步骤 3　点击**添加**。

系统将显示 **Add MAC Address Entry** 对话框。

步骤 4　从 **Interface Name** 下拉列表中选择与 MAC 地址关联的源接口。

步骤 5　在 **MAC Address** 字段中输入 MAC 地址。

步骤 6　点击 **OK**，然后点击 **Apply**。

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　依次选择 **Configuration > Device Setup > Bridging > MAC Learning** 窗格。

步骤 2　要禁用 MAC 地址获悉，请选择一个接口行，然后点击 **Disable**。

步骤 3　要重新启用 MAC 地址获悉，请点击 **Enable**。

步骤 4　点击 **Apply**。

防火墙模式示例

本节包括说明流量如何通过 ASA 的示例。

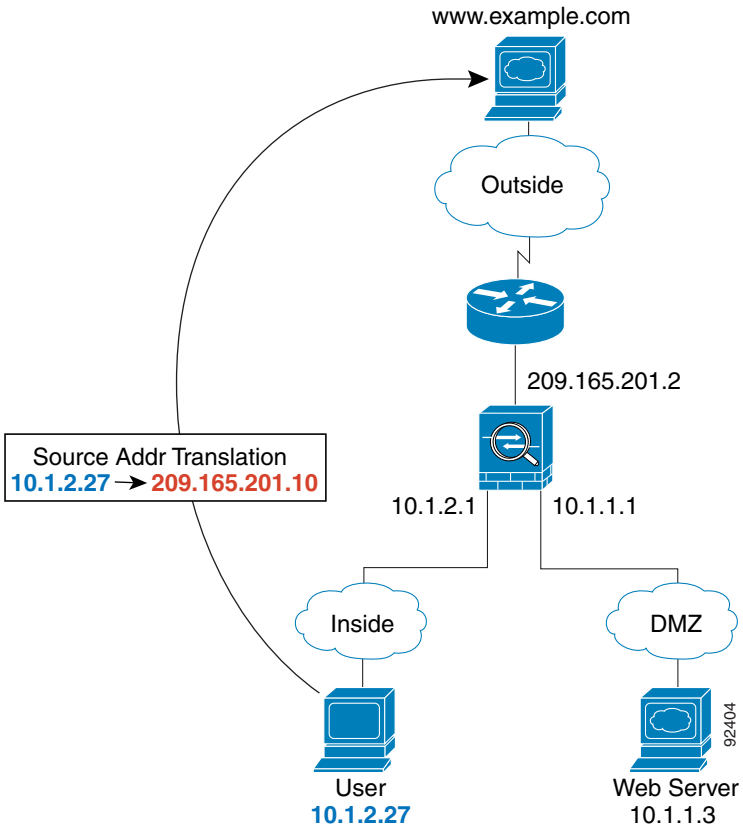
路由防火墙模式下数据通过 ASA 的方式

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

图 6-3 显示内部用户访问外部 Web 服务器。

图 6-3　　从内部到外部



以下步骤介绍数据如何通过 ASA （请参阅图 6-3）：

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。

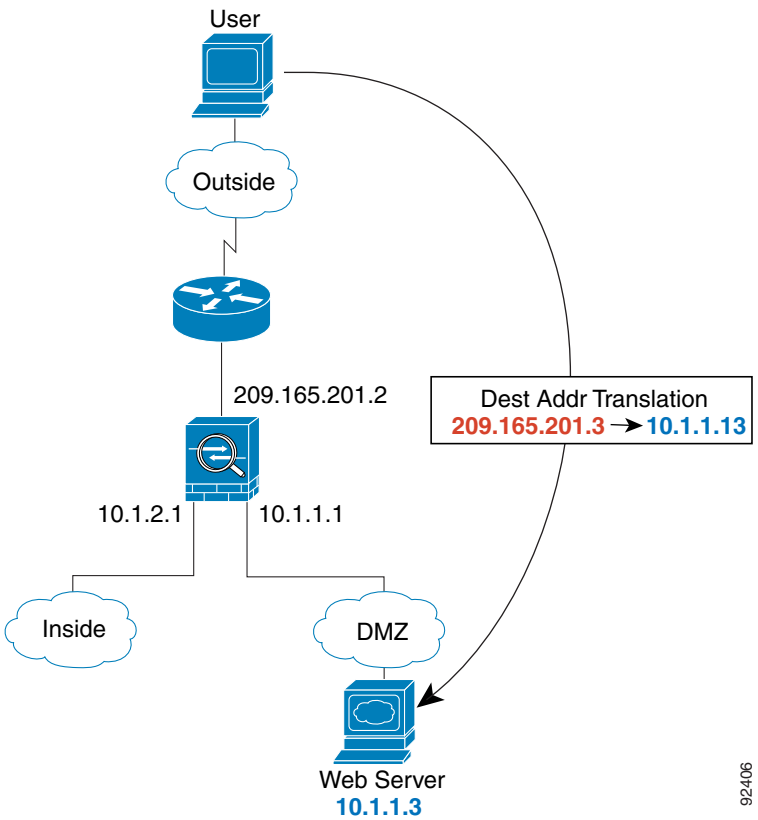
   对于多情景模式， ASA 会首先将数据包分类到一个情景中。
3. ASA 将本地源地址 (10.1.2.27) 转换为位于外部接口子网上的全局地址 209.165.201.10。

   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 6-4 显示访问 DMZ Web 服务器的外部用户。

图 6-4　　从外部到 DMZ



以下步骤介绍数据如何通过 ASA （请参阅图 6-4）：

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。

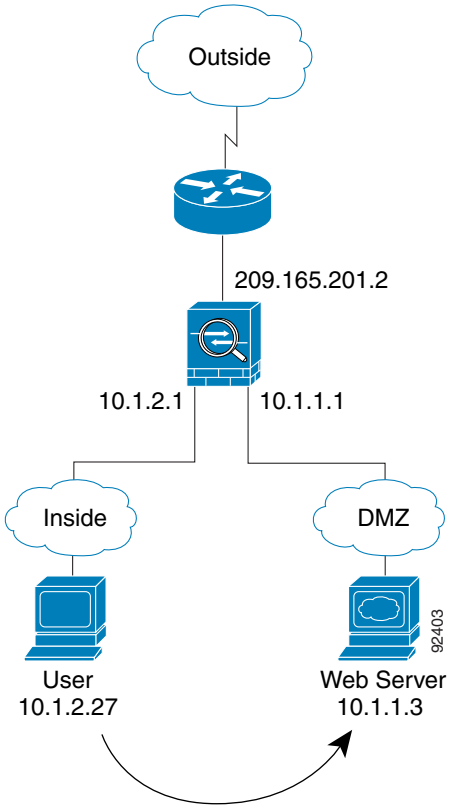
2. ASA 接收数据包并将目标地址逆向转换为本地地址 10.1.1.3。
3. 由于它是新会话，因此 ASA 会根据安全策略条款（访问列表、过滤器、 AAA）验证数据包是否获得允许。

   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 6-5 显示访问 DMZ Web 服务器的内部用户。

图 6-5　从内部到 DMZ



以下步骤介绍数据如何通过 ASA （请参阅图 6-5）：

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。

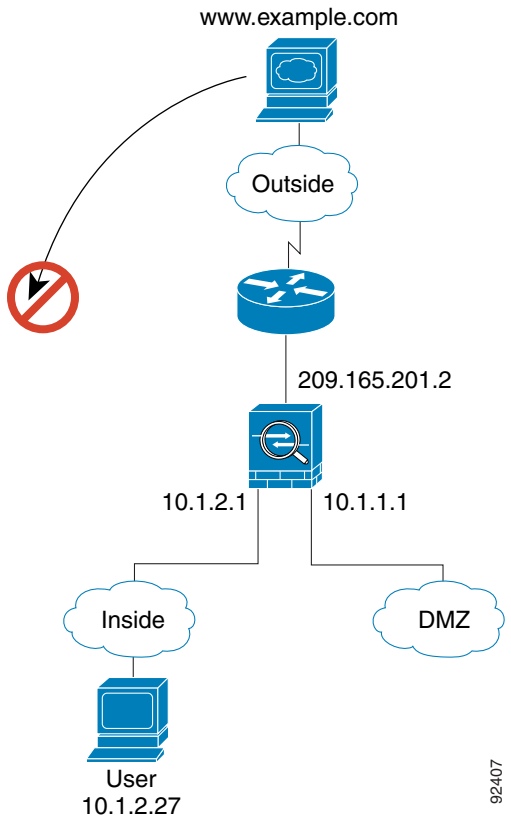
   对于多情景模式， ASA 会首先将数据包分类到一个情景中。
3. 然后， ASA 会记录有关会话已建立的信息，并从 DMZ 接口将数据包转发出去。

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 6-6 显示外部用户尝试访问内部网络。

图 6-6　从外部到内部



以下步骤介绍数据如何通过 ASA （请参阅图 6-6）：

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）。

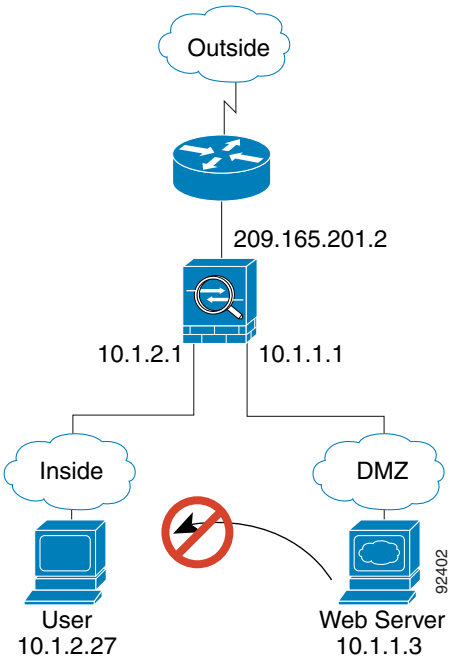
   如果内部网络使用专用地址，则外部用户在没有执行 NAT 的情况下无法访问内部网络。外部用户可能会通过使用现有 NAT 会话尝试访问内部用户。
2. ASA 接收数据包，由于是新会话，因此 ASA 会根据安全策略 （访问列表、过滤器、 AAA）验证数据包是否获得允许。
3. 系统会拒绝数据包，而 ASA 则丢弃数据包并记录连接尝试情况。

   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 6-7 显示 DMZ 中的用户尝试访问内部网络。

图 6-7　　从 DMZ 到内部



以下步骤介绍数据如何通过 ASA （请参阅图 6-7）：

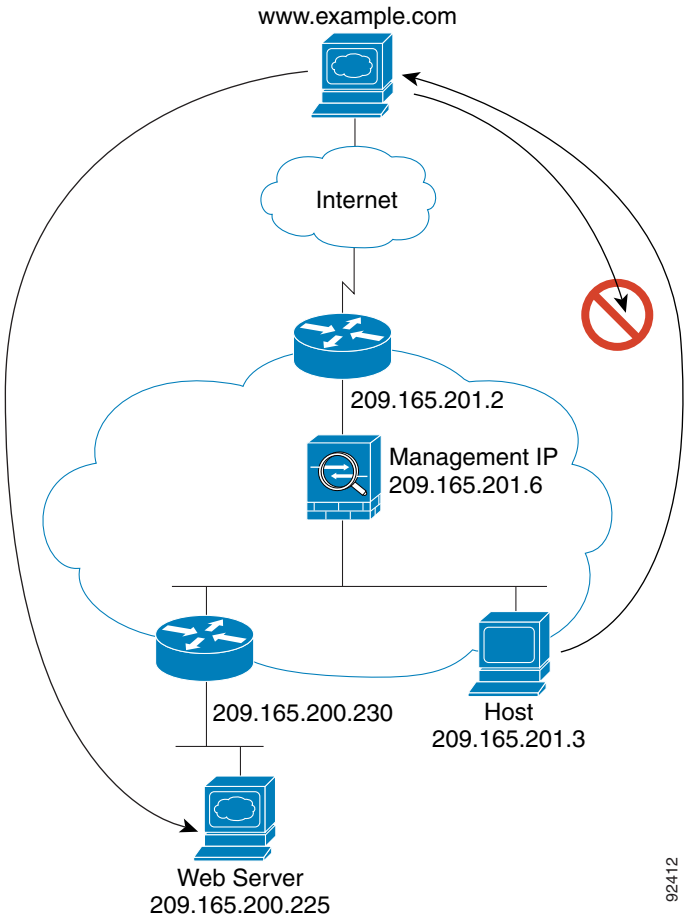
1. DMZ 网络上的用户尝试访问内部主机。由于 DMZ 不必路由互联网上的流量，因此专用寻址方案不会防止路由。
2. ASA 接收数据包，由于是新会话，因此 ASA 会根据安全策略 （访问列表、过滤器、 AAA）验证数据包是否获得允许。

   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 6-8 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 6-8　　典型透明防火墙数据路径



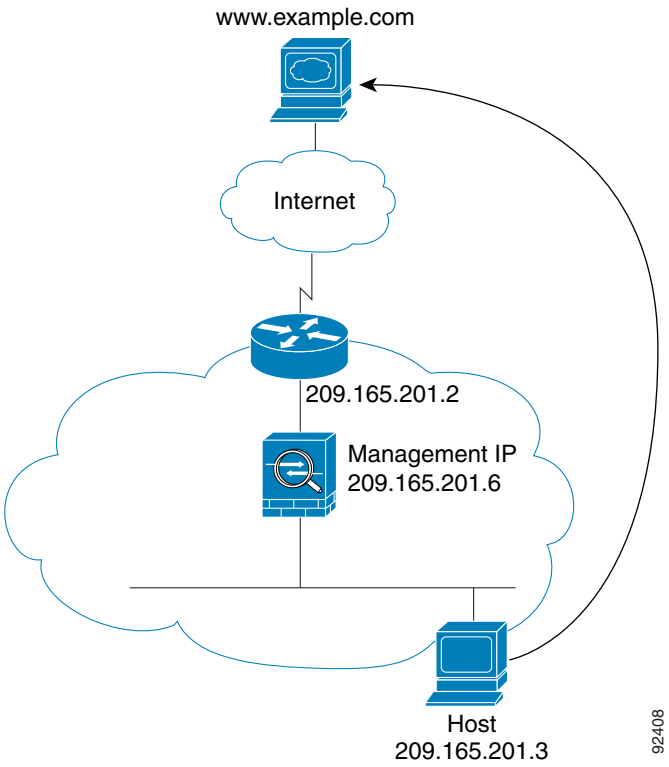
本节介绍数据如何通过 ASA。

- 内部用户访问 Web 服务器，第 6-17 页
- 内部用户使用 NAT 访问 Web 服务器，第 6-18 页
- 外部用户访问内部网络上的 Web 服务器，第 6-19 页
- 外部用户尝试访问内部主机，第 6-20 页

内部用户访问 Web 服务器

图 6-9 显示内部用户访问外部 Web 服务器。

图 6-9　　从内部到外部



以下步骤介绍数据如何通过 ASA （请参阅图 6-9）：

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。

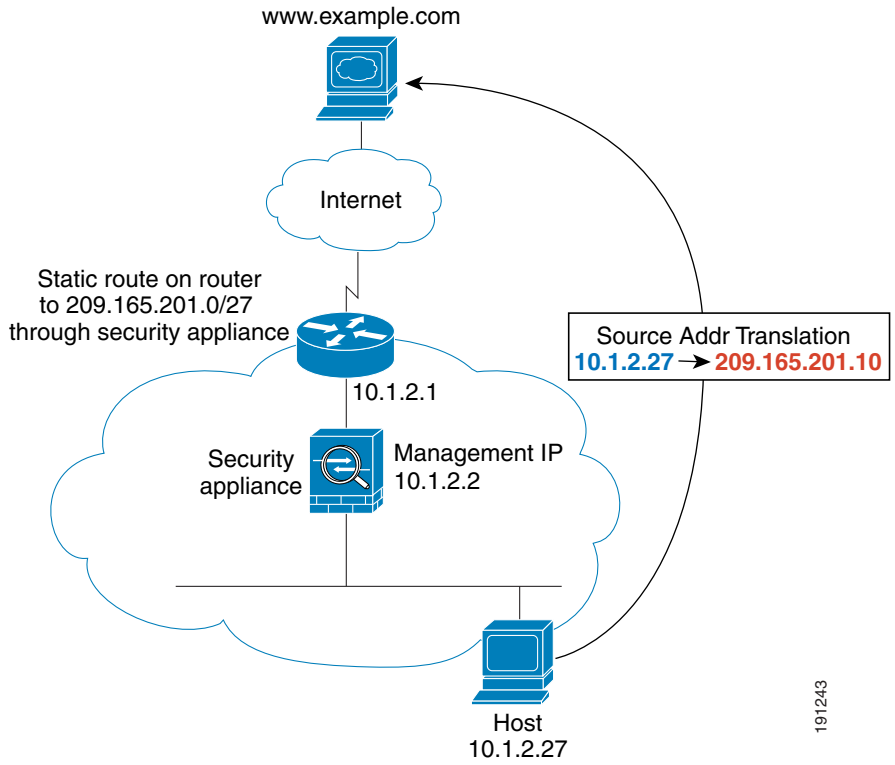
   对于多情景模式， ASA 会首先将数据包分类到一个情景中。
3. ASA 记录有关会话已建立的信息。
4. 如果目标 MAC 地址在其表中，则 ASA 会将数据包从外部接口转发出去。目标 MAC 地址是上游路由器的地址 (209.165.201.2)。

   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 6-10 显示内部用户访问外部 Web 服务器。

图 6-10　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 6-10）：

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。

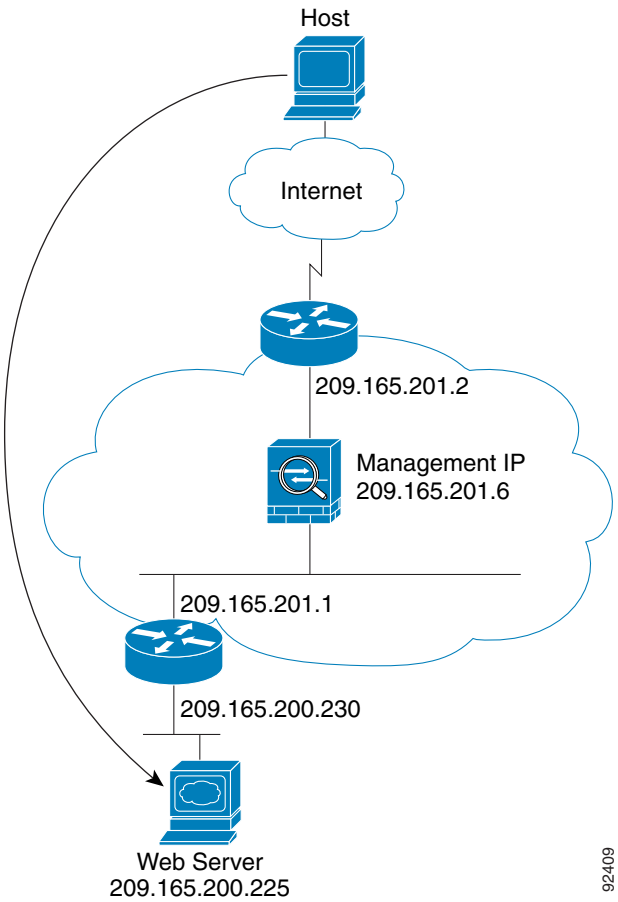
   由于映射地址与外部接口不在同一网络上，因此请确保上游路由器具有至映射网络 （指向 ASA）的静态路由。
4. 然后， ASA 会记录有关会话已建立的信息，并从外部接口转发数据包。
5. 如果目标 MAC 地址在其表中，则 ASA 会将数据包从外部接口转发出去。目标 MAC 地址是上游路由器的地址 (10.1.2.1)。

   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 6-11 显示访问内部 Web 服务器的外部用户。

图 6-11　　从外部到内部



以下步骤介绍数据如何通过 ASA （请参阅图 6-11）：

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。

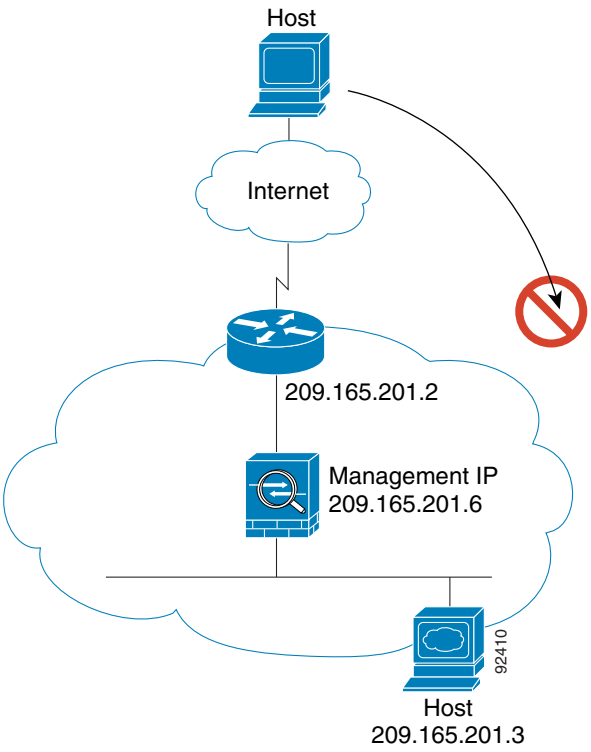
   对于多情景模式， ASA 会首先将数据包分类到一个情景中。
3. ASA 记录有关会话已建立的信息。
4. 如果目标 MAC 地址在其表中，则 ASA 会将数据包从内部接口转发出去。目标 MAC 地址是下游路由器的地址 (209.165.201.1)。

   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 6-12 显示外部用户尝试访问内部网络上的主机。

图 6-12　　从外部到内部



以下步骤介绍数据如何通过 ASA （请参阅图 6-12）：

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 6-2　　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**。 不能在 ASDM 中设置防火墙模式；必须使用命令行界面进行设置。
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。 修改或引入了以下屏幕： Configuration > Device Setup > Interface Settings > Interfaces Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface
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。 修改了以下屏幕：Configuration > Device Management > Advanced > ARP > ARP Static Table。

表 6-2　　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**。 对于单模式，不能在 ASDM 中设置防火墙模式；必须使用命令行界面进行设置。 对于多模式，修改了以下屏幕：Configuration > Context Management > Security Contexts。
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。 修改了以下屏幕： Configuration > Device Setup > Interface Settings > Interfaces Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface

启动向导

本章介绍了 ASDM 启动向导，它将引导您完成思科 ASA 的初始配置并帮助您定义基本设置。

访问启动向导

要访问启动向导，请选择以下任一选项：

- **Wizards > Startup Wizard**。
- **Configuration > Device Setup > Startup Wizard**，然后点击 **Launch Startup Wizard**。

启动向导准则

情景模式准则

系统情景中不支持启动向导。

启动向导屏幕

屏幕的实际顺序由您指定的配置选择决定。除非另有说明，否则每个屏幕均可供所有模式或型号使用。

起点或欢迎页面

- 点击 **Modify existing configuration** 单选按钮以更改现有配置。
- 点击 **Reset configuration to factory defaults** 单选按钮以将配置设置为出厂默认值。
  - 选中 **Configure the IP address of the management interface** 复选框以将管理 0/0 接口的 IP 地址和子网掩码配置为不同于默认值 (192.168.1.1) 的值。

注意　如果将配置重置为出厂默认值，则无法通过点击 **Cancel** 或关闭此屏幕来撤消这些更改。

在多情景模式中，此屏幕不包含任何参数。

基本配置

在此屏幕中设置主机名、域名和启用密码。

相关主题

设置主机名、域名及启用密码和 Telnet 密码，第 18-1 页

接口屏幕

接口屏幕取决于选择的型号和模式。

外部接口配置 （路由模式）

- 配置外部接口 （安全级别最低的接口）的 IP 地址。
- 配置 IPv6 地址。

相关主题

- 配置常规路由模式接口参数，第 15-5 页
- 配置 IPv6 寻址，第 15-11 页

外部接口配置 - PPPoE （路由模式、单模式）

为外部接口配置 PPoE 设置。

相关主题

配置管理接口，第 15-10 页

管理 IP 地址配置 （透明模式）

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。此屏幕可为 BVI 1 设置 IP 地址。

相关主题

配置网桥组，第 15-8 页

其他接口配置

为其他接口配置参数。

相关主题

- 配置常规路由模式接口参数，第 15-5 页
- 允许相同安全级别通信，第 16-6 页

静态路由

配置静态路由。

相关主题

配置静态路由，第 22-4 页

DHCP 服务器

配置 DHCP 服务器。

相关主题

配置 DHCP 服务器，第 19-4 页

地址转换 (NAT/PAT)

访问外部地址 （安全级别最低的接口）时，请为内部地址 （安全级别最高的接口）配置 NAT 或 PAT。有关详情，请参阅防火墙配置指南。

管理访问权限

- 配置 ASDM、 Telnet 或 SSH 访问权限。
- 选中 **Enable HTTP server for HTTPS/ASDM access** 复选框以启用与 HTTP 服务器的安全连接以访问 ASDM。
- 选中 **Enable ASDM history metrics** 复选框。

相关主题

- 配置 ASDM、 Telnet 或 SSH 的 ASA 访问，第 34-4 页
- 启用历史记录度量值，第 3-29 页

IPS 基本配置

在单情景模式下，使用 ASDM 中的启动向导配置基本 IPS 网络配置。这些设置将保存到 IPS 配置中，而非 ASA 配置中。有关详情，请参阅防火墙配置指南。

ASA CX 基本配置 (ASA 5585-X)

您可以使用 ASDM 中的启动向导配置 ASA CX 管理地址和身份验证代理端口。这些设置将保存到 ASA CX 配置中，而非 ASA 配置中。您还需要在 ASA CX CLI 上设置其他网络设置。有关此屏幕的信息，请参阅 《防火墙配置指南》。

ASA FirePOWER 基本配置

您可以使用 ASDM 中的启动向导配置 ASA FirePOWER 管理地址信息并接受用户软件授权协议 (EULA)。这些设置将保存到 ASA FirePOWER 配置中，而非 ASA 配置中。您还需要在 ASA FirePOWER CLI 上配置某些设置。有关详细信息，请参阅 《防火墙配置指南》中有关 ASA FirePOWER 模块的章节。

时区和时钟配置

配置时钟参数。

相关主题

设置日期和时间，第 18-6 页

自动更新服务器 （单模式）

- 通过选中 **Enable Auto Update Server for ASA** 复选框配置自动更新服务器。
- 如果有 IPS 模块，请选中 **Enable Signature and Engine Updates from Cisco.com** 复选框。设置以下额外参数：
  - 输入 Cisco.com 用户名和密码，然后确认密码。
  - 以 hh:mm:ss 的格式用 24 小时制时钟输入开始时间。

相关主题

配置自动更新，第 35-25 页

启动向导摘要

此屏幕汇总了您为 ASA 所做的所有配置设置。

- 点击 **Back** 以返回之前的屏幕更改任意设置。
- 选择如下选项之一：
  - 如果您直接从浏览器运行启动向导，则点击 **Finish** 时，通过向导创建的配置设置将发送到 ASA 并将自动保存在闪存中。
  - 如果从 ASDM 内部运行启动向导，则必须通过依次选择 **File > Save Running Configuration to Flash** 来将配置显式保存在闪存中。

启动向导历史记录

表 7-1　　启动向导历史记录

功能名称	平台版本	说明
Startup Wizard	7.0(1)	引入了此向导。 引入了 **Wizards > Startup Wizard** 屏幕。
ASA IPS 配置	8.4(1)	对于 ASA IPS 模块，启动向导中添加了 **IPS Basic Configuration** 屏幕。IPS 模块的签名更新也已添加到 **Auto Update** 屏幕上。添加了 **Time Zone and Clock Configuration** 屏幕以确保 ASA 上设置了时钟；IPS 模块可从 ASA 获取其时钟。 引入或修改了以下屏幕： **Wizards > Startup Wizard > IPS Basic Configuration** **Wizards > Startup Wizard > Auto Update** **Wizards > Startup Wizard > Time Zone and Clock Configuration**
ASA CX 配置	9.1(1)	对于 ASA IPS 模块，启动向导中添加了 **ASA CX Basic Configuration** 屏幕。 引入了以下屏幕： **Wizards > Startup Wizard > ASA CX Basic Configuration**
ASA FirePOWER 配置	9.2 （2.4 ）	对于 ASA FirePOWER 模块，启动向导中添加了 **ASA FirePOWER Basic Configuration** 屏幕。 引入了以下屏幕： **Wizards > Startup Wizard > ASA FirePOWER Basic Configuration**

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

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 8-13 页。

本节提供安全情景的概述。

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 8-2 页
- 系统配置，第 8-2 页
- 管理情景配置，第 8-2 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 8-3 页
- 分类示例，第 8-4 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 8-3 页
- 唯一 MAC 地址，第 8-3 页
- NAT 配置，第 8-3 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。

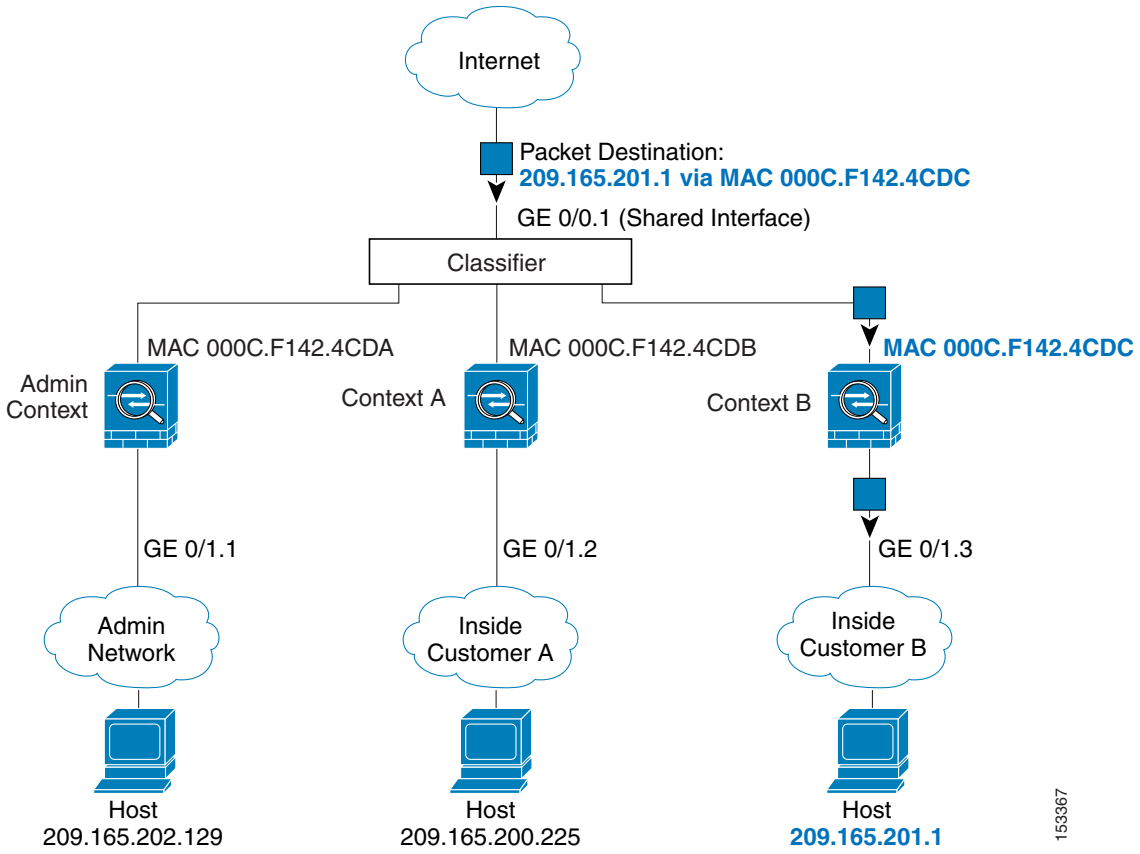
NAT 配置

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

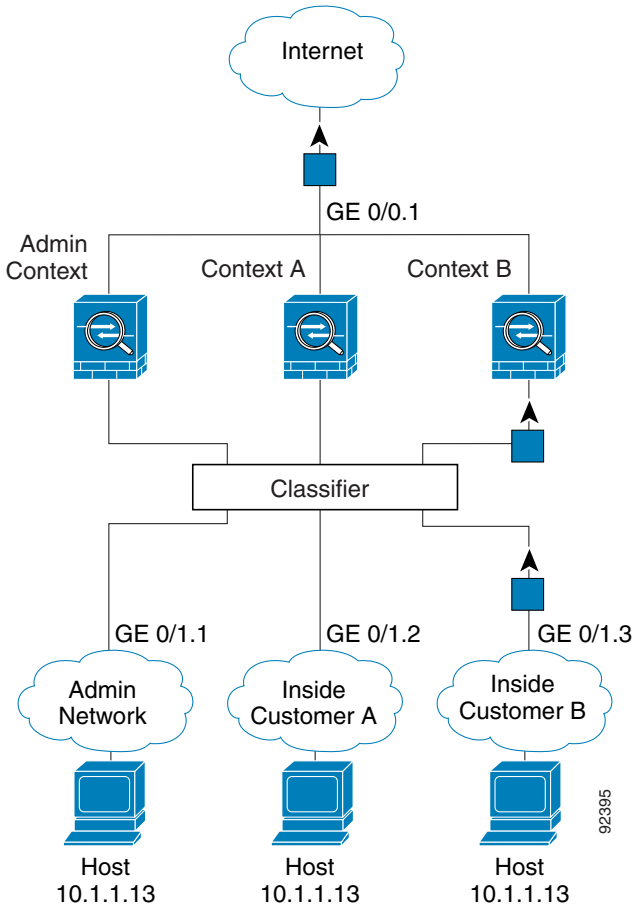
图 8-1 展示了多情景共享一个外部接口。因为情景 B 包含路由器将数据包发送到的 MAC 地址，因此分类器会将该数据包分配至情景 B。

图 8-1　使用 MAC 地址通过共享接口进行数据包分类



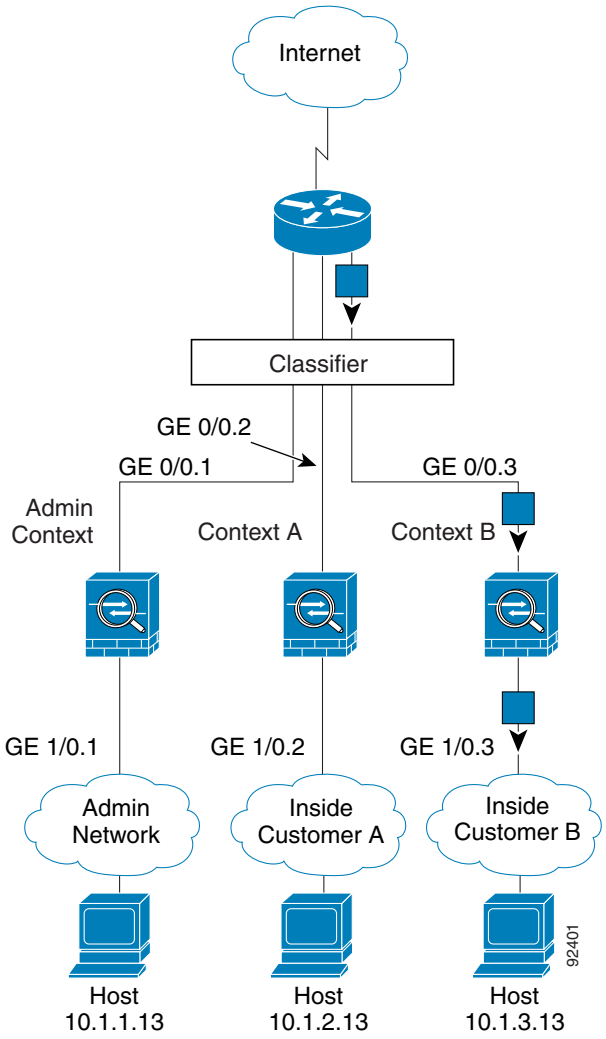
请注意，必须对所有新的传入流量加以分类，即使其来自内部网络。图 8-2 展示了情景 B 内部网络上的主机访问互联网。由于传入接口是分配至情景 B 的千兆以太网 0/1.3，因此分类器会将数据包分配至情景 B。

图 8-2　　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 8-3 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 8-3　　透明防火墙情景



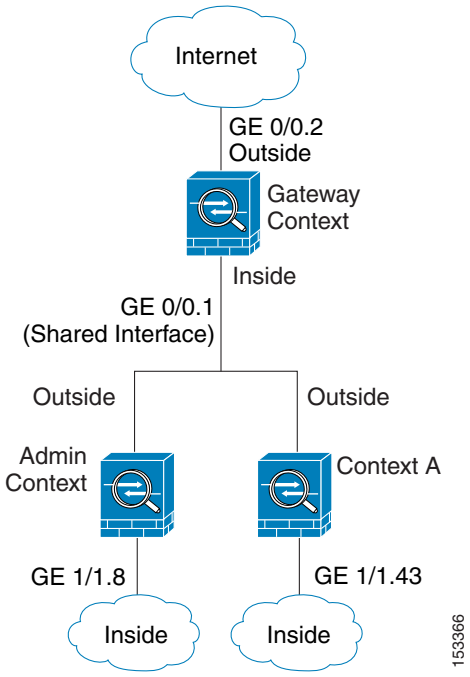
级联安全情景

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 8-4 展示了在网关后有两个情景的网关情景。

图 8-4　　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 8-7 页
- 情景管理员访问，第 8-8 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 34 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 34 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

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。

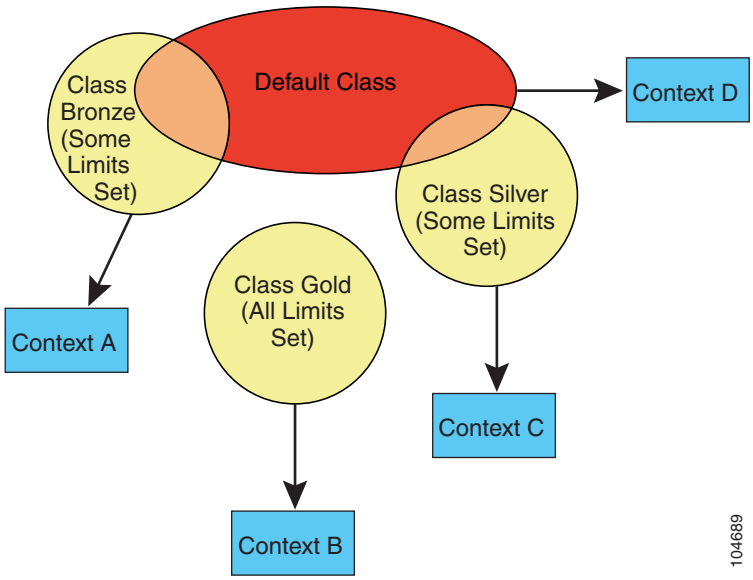
如果某个情景属于除默认类以外的类，则其类设置始终覆盖默认类设置。但是，如果另一个类具有任何未定义的设置，则成员情景为这些限制使用默认类。例如，如果创建的类对所有并发连接具有 2% 的限制，但没有任何其他限制，则所有其他限制都继承自默认类。相反地，如果创建对所有资源都有限制的类，则该类不使用默认类中的任何设置。

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 8-5 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。

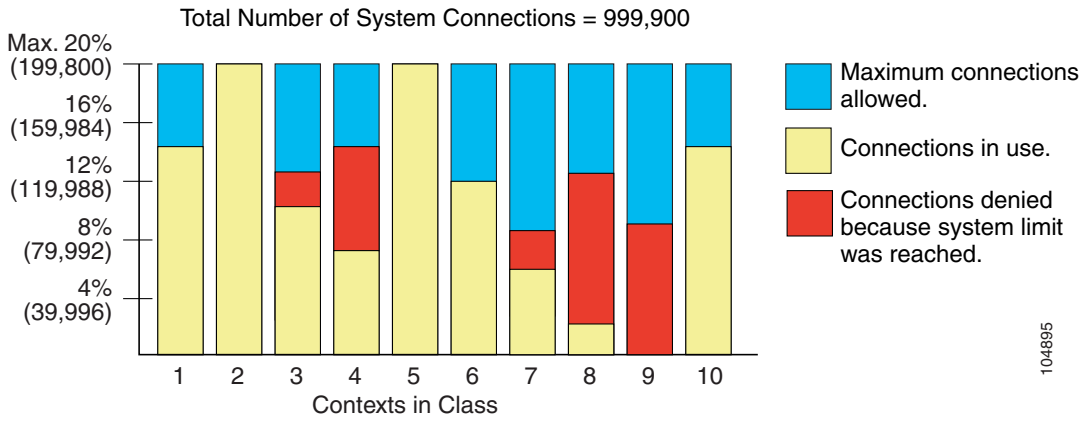
图 8-5　　资源类



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 8-6。）

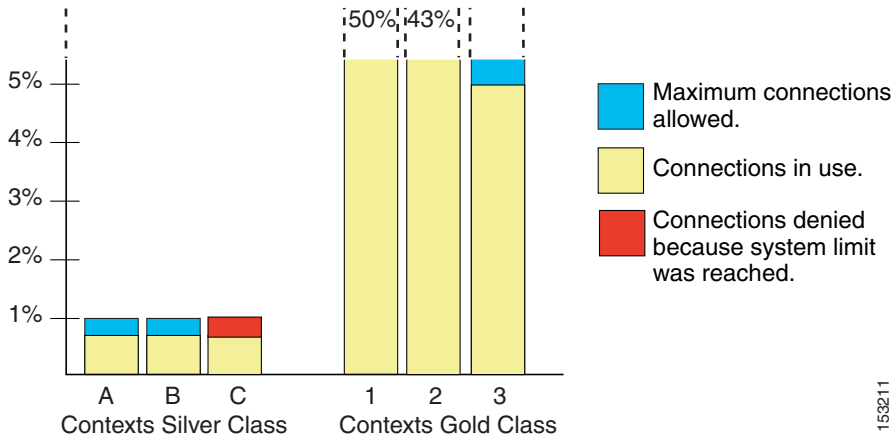
图 8-6　资源超订用



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 8-7。）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 8-7　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 8-20 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 8-2 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 MAC 地址、MTU 和 TCP MSS，第 16-5 页。

- 默认 MAC 地址，第 8-11 页
- 与手动 MAC 地址的交互，第 8-11 页
- 故障切换 MAC 地址，第 8-11 页
- MAC 地址格式，第 8-11 页

默认 MAC 地址

（8.5(1.7) 及更高版本）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 8-11 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 8-11 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。*
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 8-9 页。
- 请参阅默认 MAC 地址，第 8-11 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 8-14 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 8-15 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 11 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 8-17 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 8-20 页。

步骤 6　完成情景中的接口配置。请参阅第 15 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。

ASDM 支持从单模式切换到多模式 （如果使用高可用性和可扩展性向导，并且启用主用/主用故障切换）。有关详情，请参见第 9 章 “通过故障切换实现高可用性”。如果您不想使用主用/主用故障切换，或者希望切换回单模式，则必须使用 CLI 更改模式；因为更改模式要求确认，不能使用命令行界面工具。本节介绍如何在 CLI 中更改模式。

启用多情景模式

当您从单模式转换为多模式时，ASA 会将运行配置转换为两个文件：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 管理文件，第 35-8 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 8-1 列出资源类型和限制。

表 8-1　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 会话数	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。
连接 连接数/秒[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 4-1 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。
主机	并发	N/A	N/A	可以通过 ASA 连接的主机数。
检测数/秒	速率	N/A	N/A	每秒应用检测数。
MAC 条目	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。
路由	并发	N/A	N/A	动态路由数。
站点间 VPN 突发	并发	N/A	您的型号的其他 VPN 会话数量减去分配给站点间 VPN 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站点间 VPN 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，而您为具有站点间 VPN 的所有情景分配了 4000 个会话，则其余 1000 个会话可用于站点间 VPN 突发。与站点间 VPN （保证会话可分配给相应的情景）不同的是，站点间 VPN 突发 可以超订用；突发池按照先到先得的原则供所有情景使用。
站点间 VPN	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 4-1 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。
系统日志数/秒	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　如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2　依次选择 **Configuration > Context Management > Resource Class**，然后点击 **Add**。

系统将显示 **Add Resource Class** 对话框。

步骤 3　在 **Resource Class** 字段中输入最大长度为 20 个字符的类名。

步骤 4　在 **Count Limited Resources** 区域中，设置资源的并发限制。

有关各个资源类型的说明，请参阅表 8-1，第 8-16 页。

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。如果不设置限制，则会从默认类继承限制。如果默认类不设置限制，则表示资源不受限制，或使用系统限制 （如果适用）。对于大多数资源， 0 表示将限制设置为不受限制。对于 VPN 类型， 0 表示将限制设置为无。

步骤 5　在 **Rate Limited Resources** 区域中，设置资源的速率限制。

有关各个资源类型的说明，请参阅表 8-1，第 8-16 页。

如果不设置限制，则会从默认类继承限制。如果默认类不设置限制，则其在默认情况下不受限制。0 表示将限制设置为不受限制。

步骤 6　点击 **OK**。

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 11 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。

操作步骤

步骤 1　如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2　依次选择 **Configuration > Context Management > Security Contexts**，然后点击 **Add**。

系统将显示 **Add Context** 对话框。

步骤 3　在 **Security Context** 字段中，输入最大长度为 32 个字符的情景名称。

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。“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 4　在 **Interface Allocation** 区域中，点击 **Add** 按钮以向情景分配接口。

a.　从 **Interfaces > Physical Interface** 下拉列表中，选择接口。

您可以分配主接口 （在这种情况下，请将子接口 ID 留空），也可以分配与此接口关联的一个子接口或一系列子接口。在透明防火墙模式下，仅会显示尚未分配给其他情景的接口。如果主接口已分配给其他情景，则必须选择子接口。

b. （可选）在 **Interfaces > Subinterface Range** （可选）下拉列表中，选择子接口 ID。

对于子接口 ID 范围，请在第二个下拉列表中选择结束 ID （如果适用）。

在透明防火墙模式下，仅会显示尚未分配给其他情景的子接口。

c. （可选）在 **Aliased Names** 区域中，选中 **Use Aliased Name in Context** 以设置此接口的别名，从而在情景配置中用于替代接口 ID。

– 在 **Name** 字段中，设置别名。

别名必须以字母开头，以字母结尾，并且内部字符只能是字母、数字或下划线。此字段允许您指定以字母或下划线结尾的名称；要在名称后面添加可选数字，请在 Range 字段中设置数字。

– （可选）在 **Range** 字段中，设置别名的数字后缀。

如果您有一系列子接口，则可以输入要添加到名称之后的数字的范围。

d. （可选）要使情景用户能够查看物理接口属性 （即使设置了别名），请选中 **Show Hardware Properties in Context**。

e. 点击 **OK** 返回到 Add Context 对话框。

步骤 5　（可选）如果使用 IPS 虚拟传感器，请在 IPS Sensor Allocation 区域中向情景分配传感器。

有关 IPS 和虚拟传感器的详细信息，请参阅 《防火墙配置指南》。

步骤 6　（可选）要将此情景分配给资源类，请从 **Resource Assignment > Resource Class** 下拉列表中选择类名。

可以直接从此区域中添加或编辑资源类。有关详情，请参见配置用于资源管理的类，第 8-15 页。

步骤 7　通过在 **Config URL** 下拉列表中选择文件系统类型并在字段中输入路径，可以确定 URL，从而设置情景配置位置。

例如， FTP 的组合 URL 格式如下：

ftp://server.example.com/configs/admin.cfg

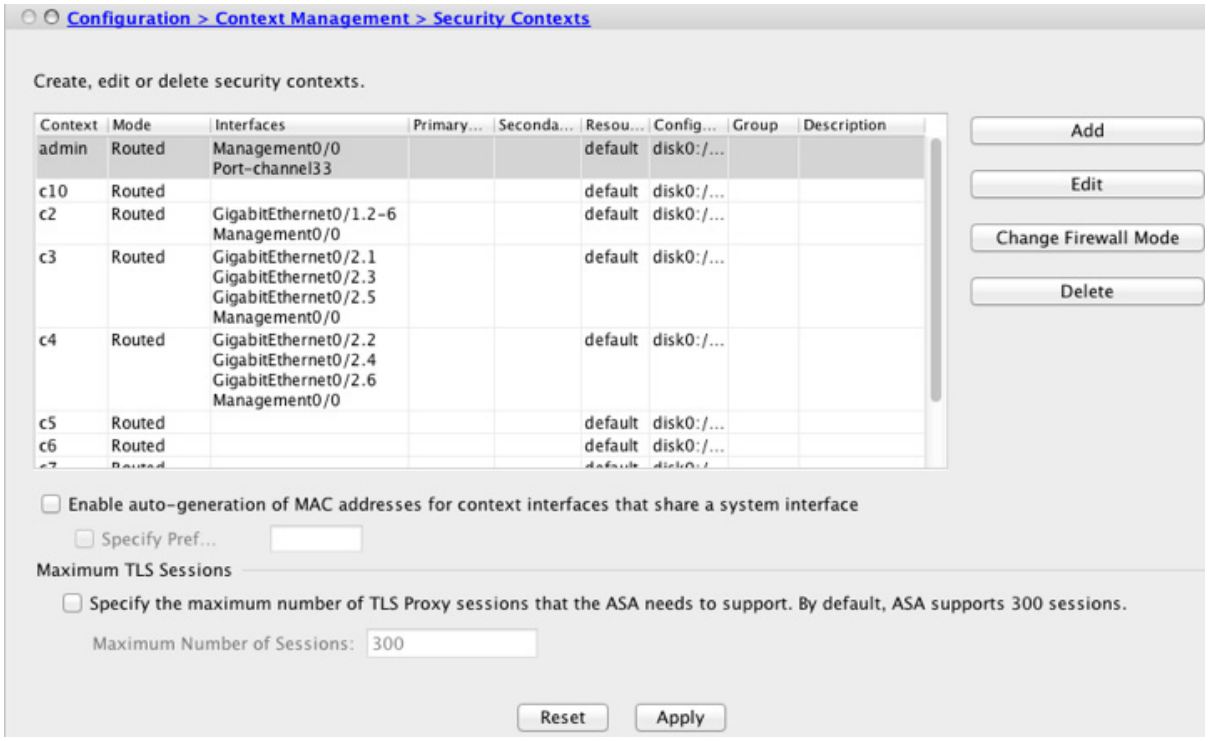
a. （可选）对于外部文件系统，请通过点击 **Login** 设置用户名和密码。

步骤 8　（可选）要设置主用/主用故障切换的故障切换组，请在 **Failover Group** 下拉列表中选择组名。

步骤 9　（可选）要在此情景中启用 ScanSafe 检测，请点击 **Enable**。要覆盖在系统配置中设置的许可证，请在 **License** 字段中输入许可证。

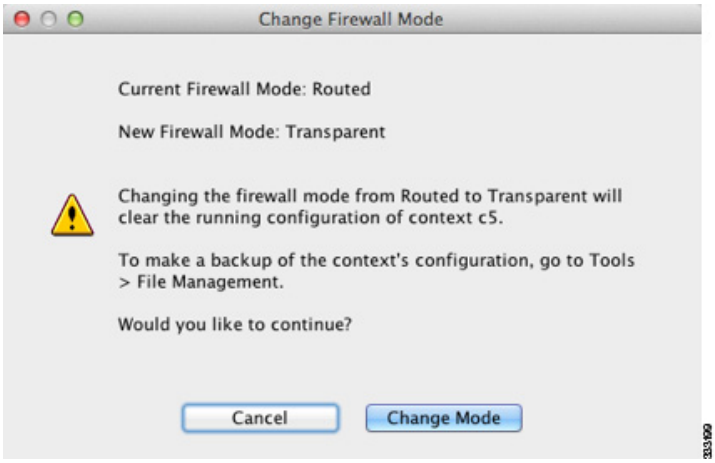
步骤 10　（可选）在 **Description** 字段中，添加说明。

步骤 11　点击 **OK** 返回到 **Security Contexts** 窗格。



步骤 12　（可选）要将防火墙模式设置为透明，请选择情景并点击 **Change Firewall Mode**。

您将会看到以下确认对话框：



如果是新的情景，则没有要擦除的配置。点击 **Change Mode** 切换到透明防火墙模式。

如果是现有情景，则在更改模式之前，请务必备份配置。

注意　不能在 ASDM 中更改当前连接的情景（通常为管理情景）的模式；请参阅设置防火墙模式（单模式），第 6-7 页以在命令行中设置模式。

步骤 13　要自定义 MAC 地址的自动生成，请参阅自动将 MAC 地址分配给情景接口，第 8-20 页。

步骤 14　选中 **Specify the maximum number of TLS Proxy sessions that the ASA needs to support** 复选框，以指定设备的最大 TLS 代理会话数。有关 TLS 代理的详细信息，请参阅 《防火墙配置指南》。

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 8-10 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 8-25 页。

准备工作

- 当在情景中为接口配置名称时，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 MAC 地址、MTU 和 TCP MSS，第 16-5 页。

操作步骤

步骤 1　如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2　依次选择 **Configuration > Context Management > Security Contexts**，然后选中 **Mac-Address auto**。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。

步骤 3　（可选）选中 **Prefix** 复选框，并在字段中输入介于 0 和 65535 之间的一个十进制值。

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 8-11 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。

操作步骤

步骤 1　在 Device List 窗格中，双击主用设备 IP 地址下的 **System** 可配置系统。

步骤 2　在 Device List 窗格中，双击主用设备 IP 地址下的情景名称可配置情景。

管理安全情景

本节介绍如何管理安全情景。

删除安全情景

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。

准备工作

在系统执行空间中执行此程序。

操作步骤

步骤 1　如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2　依次选择 **Configuration > Context Management > Security Contexts**。

步骤 3　选择要删除的情景，然后点击 **Delete**。

系统将显示 Delete Context 对话框。

步骤 4　如果要以后重新添加此情景，并要保留配置文件以供将来使用，请取消选中 **Also delete config URL file from the disk** 复选框。

如果要删除配置文件，请保持选中该复选框。

步骤 5　点击 **Yes**。

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。

备注　对于 ASDM，不能在 ASDM 中更改管理情景，因为 ASDM 会话会断开连接。您可以使用命令行界面工具执行此程序，但请注意，必须重新连接到新的管理情景。

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　如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2　依次选择 **Tools > Command Line Interface**。

系统将显示 Command Line Interface 对话框。

步骤 3　请输入以下命令：

```
admin-context context_name
```

步骤 4　点击 **Send**。

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

注意　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　如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2　依次选择 **Configuration > Context Management > Security Contexts**。

步骤 3　选择要编辑的情景，点击 **Edit**。

系统将显示 Edit Context 对话框。

步骤 4　在 Config URL 字段中输入新 URL，然后点击 **OK**。

系统会立即加载情景，以便其正常运行。

重新加载安全情景

您可以通过两种方式重新加载情景：

- 清除运行配置，然后导入启动配置。

  此操作会清除与情景关联的大多数属性，例如，连接和 NAT 表。
- 从系统配置中删除情景。

  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 8-23 页
- 通过删除并重新添加情景重新加载，第 8-24 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　在 Device List 窗格中，双击主用设备 IP 地址下的情景名称。

步骤 2　依次选择 **Tools > Command Line Interface**。

系统将显示 Command Line Interface 对话框。

步骤 3　请输入以下命令：

```
clear configure all
```

步骤 4　点击 **Send**。

系统会清除情景配置。

步骤 5　再次选择 **Tools > Command Line Interface**。

系统将显示 Command Line Interface 对话框。

步骤 6　请输入以下命令：

```
copy startup-config running-config
```

步骤 7　点击 **Send**。

ASA 会重新加载配置。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 8-21 页确保取消选中 **Also delete config URL file from the disk** 复选框。
2. 配置安全情景，第 8-17 页

监控安全情景

本节介绍如何查看和监控情景信息。

- 监控情景资源使用情况，第 8-24 页
- 查看分配的 MAC 地址，第 8-25 页

监控情景资源使用情况

要从系统执行空间监控所有情景的资源使用情况，请执行以下步骤：

步骤 1　如果您尚未处于系统模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2　点击工具栏上的 **Monitoring** 按钮。

步骤 3　点击 **Context Resource Usage**。

点击每种资源类型以查看所有情景的资源使用情况：

- **ASDM/Telnet/SSH** - 显示 ASDM、 Telnet 和 SSH 连接的使用情况。
  - Context - 显示每个情景的名称。

  对于每种访问方法，请参阅以下使用情况统计信息：
  - Existing Connections (#) - 显示现有连接的数量。
  - Existing Connections (%) - 显示此情景使用的连接数占所有情景使用的连接总数的百分比。
  - Peak Connections (#) - 显示从上次清除统计信息 （使用 **clear resource usage** 命令或因为设备重启）以来，连接数的峰值。
- **Routes** - 显示动态路由的使用情况。
  - Context - 显示每个情景的名称。
  - Existing Connections (#) - 显示现有连接的数量。
  - Existing Connections (%) - 显示此情景使用的连接数占所有情景使用的连接总数的百分比。
  - Peak Connections (#) - 显示从上次清除统计信息 （使用 **clear resource usage** 命令或因为设备重启）以来，连接数的峰值。
- **Xlates** - 显示网络地址转换的使用情况。
  - Context - 显示每个情景的名称。
  - Xlates (#) - 显示当前网络地址转换数量。
  - Xlates (%) - 显示此情景使用的网络地址转换数占所有情景使用的网络地址转换总数的百分比。
  - Peak (#) - 显示从上次清除统计信息 （使用 **clear resource usage** 命令或因为设备重启）以来，网络地址转换数的峰值。

- **NATs** - 显示 NAT 规则数。
  - Context - 显示每个情景的名称。
  - NATs (#) - 显示当前 NAT 规则数。
  - NATs (%) - 显示此情景使用的 NAT 规则数占所有情景使用的 NAT 规则总数的百分比。
  - Peak NATs (#) - 显示从上次清除统计信息 （使用 **clear resource usage** 命令或因为设备重启）以来， NAT 规则数的峰值。
- **Syslogs** - 显示系统日志消息的速率。
  - Context - 显示每个情景的名称。
  - Syslog Rate (#/sec) - 显示系统日志消息的当前速率。
  - Syslog Rate (%) - 显示此情景生成的系统日志消息数占所有情景生成的系统日志消息总数的百分比。
  - Peak Syslog Rate (#/sec) - 显示从上次清除统计信息 （使用 **clear resource usage** 命令或因为设备重启）以来，系统日志消息的峰值速率。
- VPN - 显示 VPN 站点间隧道的使用情况。
  - Context - 显示每个情景的名称。
  - VPN Connections - 显示有保证的 VPN 会话的使用情况。
  - VPN Burst Connections - 显示突发 VPN 会话的使用情况。

    Existing (#) - 显示现有隧道的数量。

    Peak (#) - 显示从上次清除统计信息（使用 **clear resource usage** 命令或因为设备重启）以来，现有隧道数的峰值。

步骤 4　点击 **Refresh** 刷新视图。

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 8-25 页
- 查看情景中的 MAC 地址，第 8-26 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　如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2　依次选择 **Configuration > Context Management > Security Contexts**，然后查看 Primary MAC 和 Secondary MAC 列。

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　如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2　依次选择 **Configuration > Interfaces**，然后查看 MAC Address 地址列。

此表显示正在使用的 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。

多情景模式的历史记录

表 8-2　　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。 引入了以下屏幕：Configuration > Context Management。
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。 修改了以下屏幕：Configuration > Context Management > Security Contexts。
资源管理	7.2(1)	引入了资源管理。 引入了以下屏幕：Configuration > Context Management > Resource Management。
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。 修改了以下屏幕：Configuration > Context Management > Security Contexts。

表 8-2　　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 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。 修改了以下屏幕：Configuration > Context Management > Security Contexts。
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。 修改了以下屏幕：Configuration > Context Management > Security Contexts。
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。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。 修改了以下屏幕：Configuration > Context Management > Security Contexts
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。 修改了以下屏幕：Configuration > Context Management > Resource Class > Add Resource Class
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。

表 8-2　　多情景模式的历史记录 （续）

功能名称	平台版本	功能信息
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。 修改了以下屏幕：Configuration > Context Management > Resource Class > Add Resource Class

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

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

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 9-2 页
- 软件要求，第 9-2 页
- 许可证要求，第 9-3 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 35-4 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 4-20 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。

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

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 9-4 页
- 共享故障切换链路，第 9-5 页
- 共享常规数据接口 （不推荐），第 9-5 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 9-1　使用单台交换机进行连接 - 不推荐

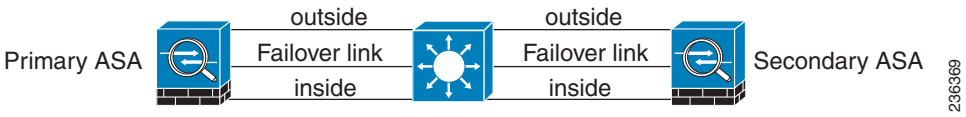
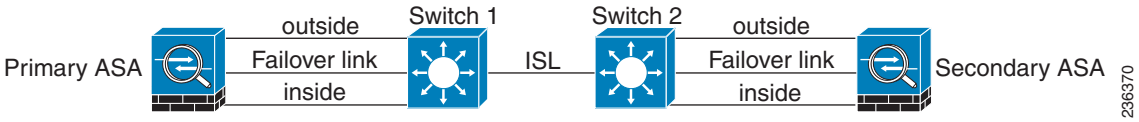


图 9-2　使用两台交换机进行连接 - 不推荐



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 9-3　使用不同的交换机进行连接

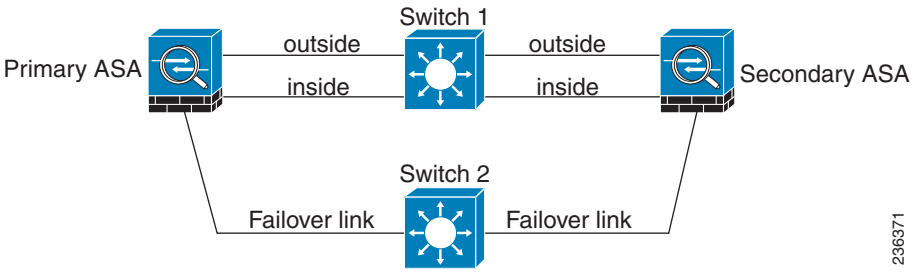
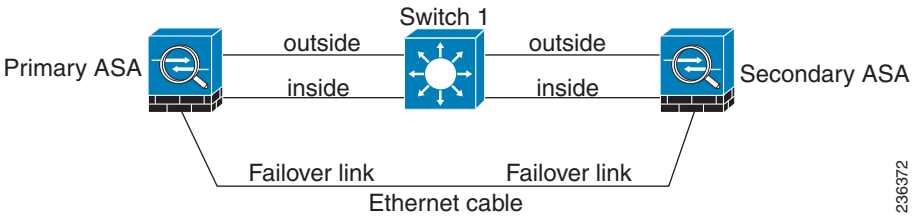


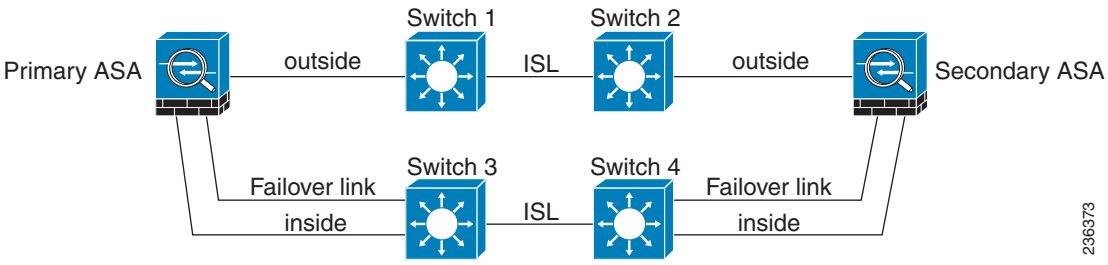
图 9-4　使用电缆进行连接



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 9-5　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 9-6　使用冗余接口进行连接

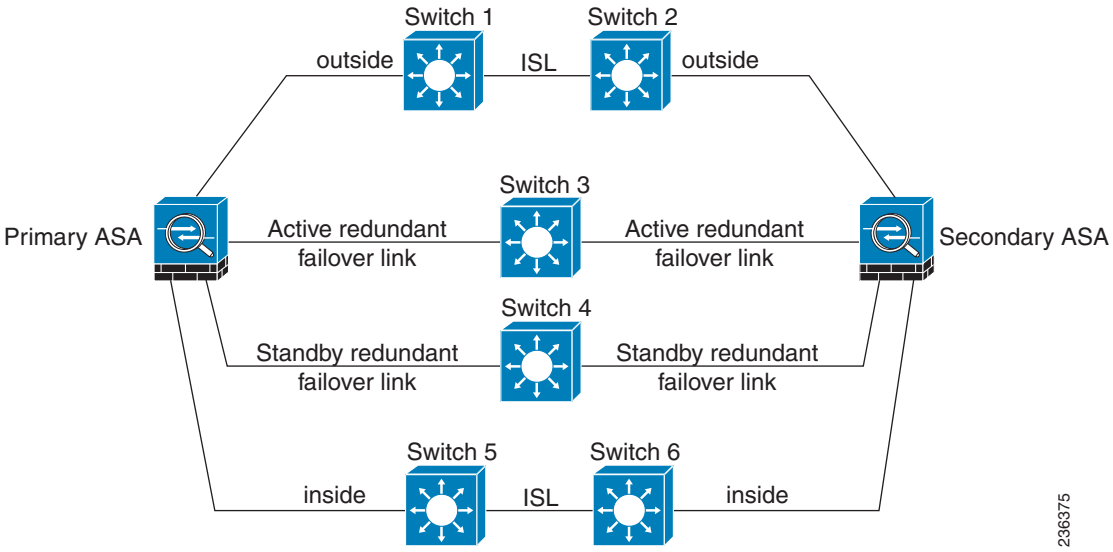
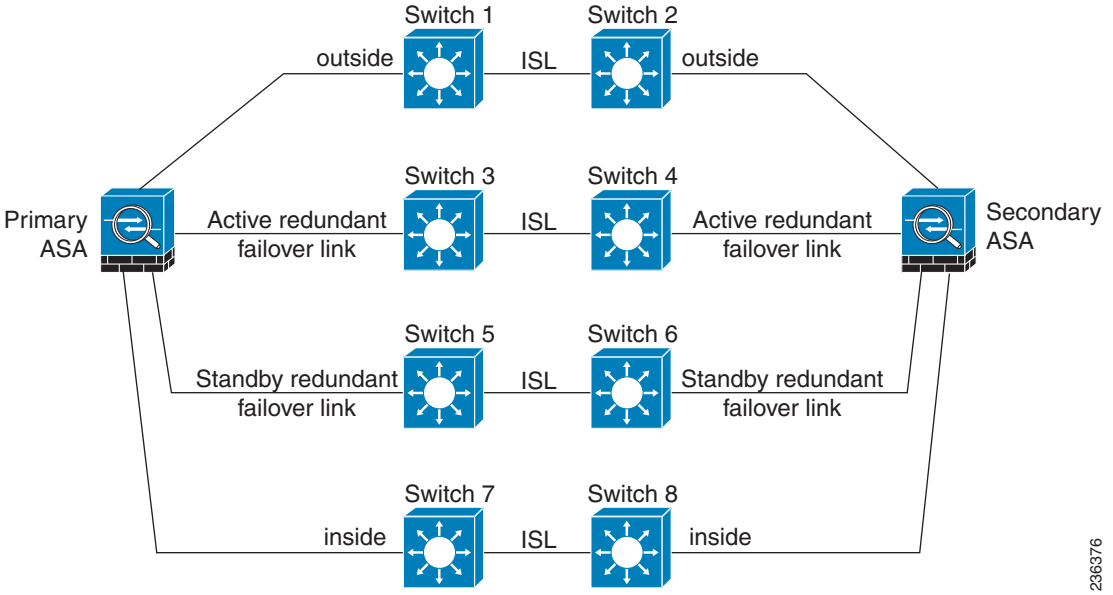


图 9-7　使用交换机间链路进行连接



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 8-10 页
- 配置主用/主用故障切换，第 9-25 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 9-8 页
- 机箱间故障切换，第 9-9 页

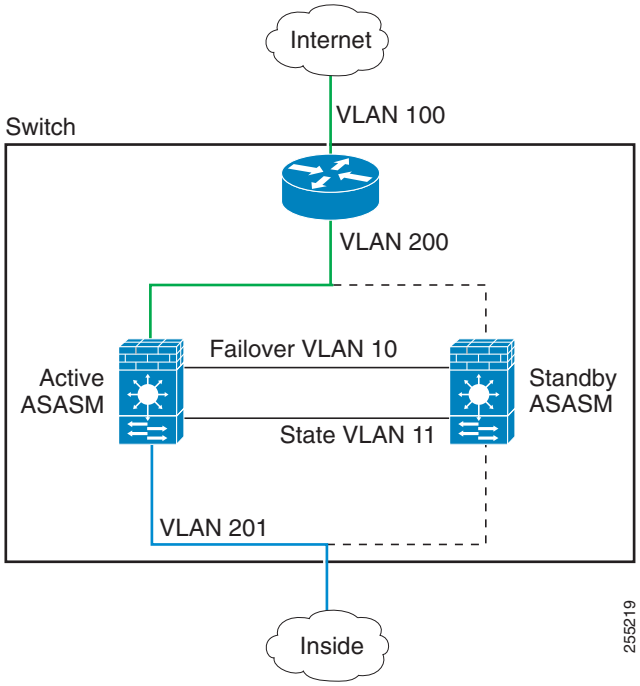
机箱内故障切换

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 9-8　　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。

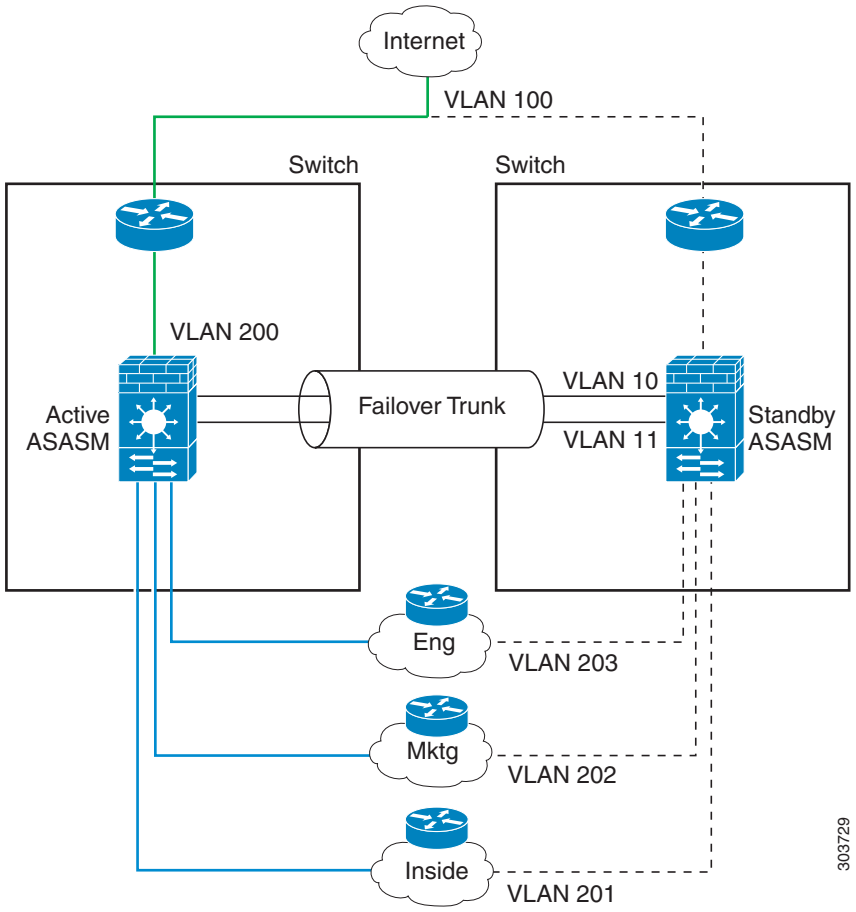
要在 ASASM 之间实现最佳的故障切换通信可靠性，我们建议您在两台交换机之间配置 EtherChannel Trunk 端口，以便承载故障切换和状态 VLAN。

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）。

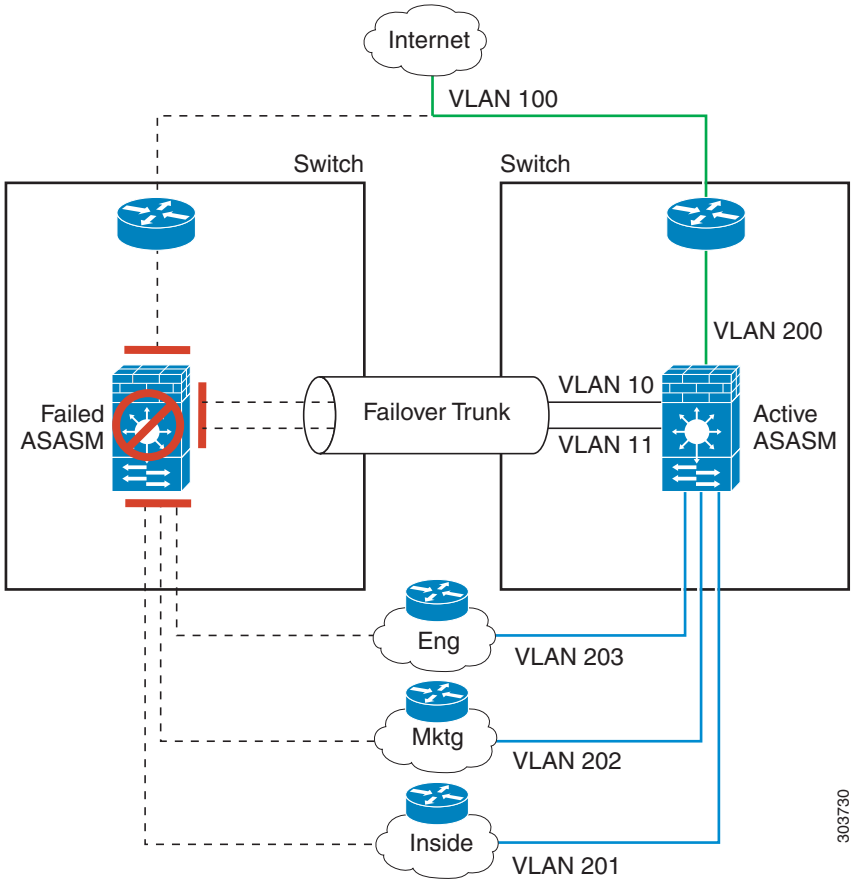
备注　ASASM 故障切换与交换机故障切换操作无关；但是，ASASM 可在任何一种交换机故障切换情景下工作。

图 9-9　　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

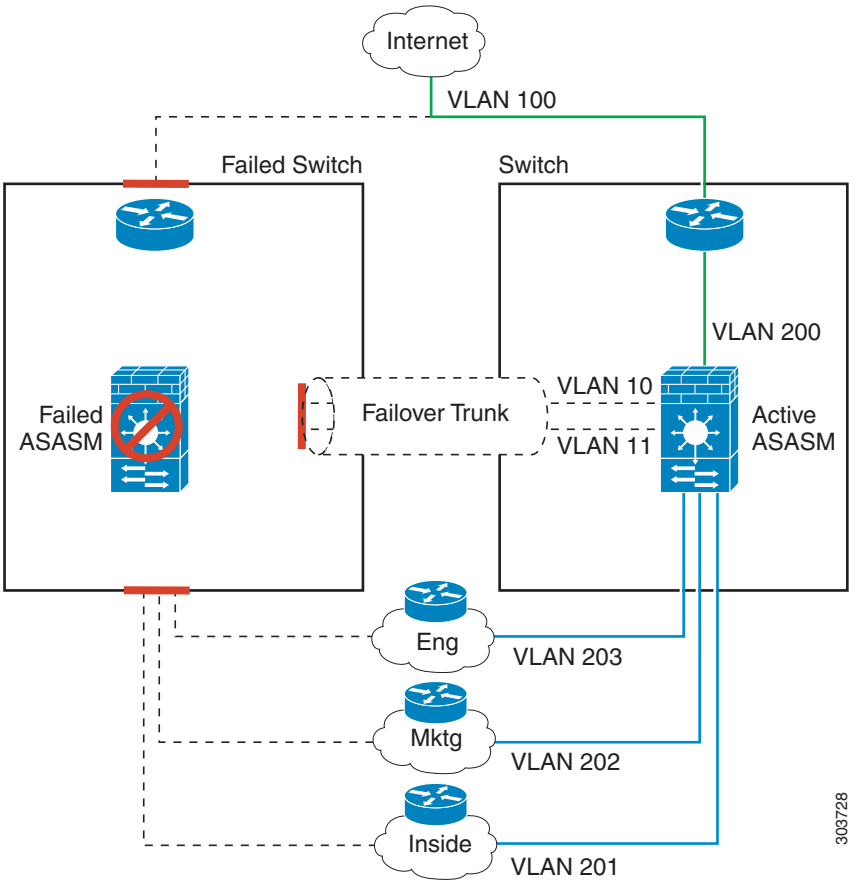
如果主 ASASM 发生故障，则辅助 ASASM 会变为主用状态，并成功穿过防火墙 VLAN。

图 9-10　　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 9-11　　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 9-13 页
- 状态故障切换，第 9-13 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 9-13 页
- 不支持的功能，第 9-14 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 9-14 页
- ASA 服务模块 的透明模式要求，第 9-15 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。

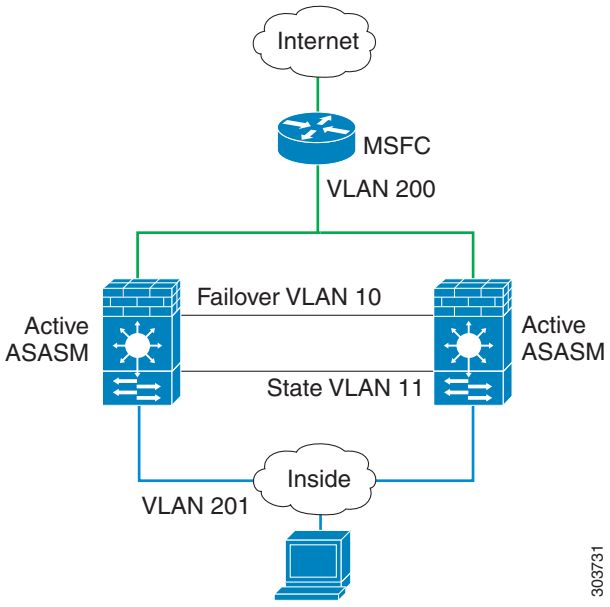
- 禁用接口监控。
- 将接口保持时间增大到一个高值，这将允许 STP 在 ASA 进行故障切换之前融合。
- 降低 STP 计时器的值，以 STP 在接口保持时间之内融合。

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 9-12）。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 9-12　　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

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 9-1　　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 9-18 页
- 文件复制，第 9-18 页
- 命令复制，第 9-18 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更改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更改会导致配置不同步。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 9-19 页
- 启动时的主用设备确定，第 9-19 页
- 故障切换事件，第 9-20 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 9-2　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 9-21 页
- 故障切换组的主/辅助角色和主用/备用状态，第 9-21 页
- 故障切换事件，第 9-22 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 9-3　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。
ASA 5512-X 到 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 35-25 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

High Availability and Scalability Wizard 可以分步骤指导您创建主用/备用故障切换配置。

操作步骤

步骤 1　依次选择 **Wizards > High Availability and Scalability**。请参阅以下步骤中有关选择向导的指引。

步骤 2　在 **Failover Peer Connectivity and Compatibility** 屏幕上，输入对等设备的 IP 地址。此地址必须是已启用 ASDM 访问的接口。

默认情况下，对等体地址会被指定为 ASDM 管理接口的备用地址。

步骤 3　在 **LAN Link Configuration** 屏幕上：

- **Active IP Address** - 此 IP 地址应处于未使用的子网上。
- **Standby IP Address** - 此 IP 地址必须与主用 IP 地址处于相同网络。
- （可选） **Communications Encryption** - 加密故障切换链路上的通信。**注意**：我们建议使用 IPsec 预共享密钥而不是密钥，您可以在退出向导后配置该预共享密钥 （请参阅修改故障切换设置，第 9-31 页）。

步骤 4　在 **State Link Configuration** 屏幕上，如果您选择将另一个接口用于状态故障切换：

- **Active IP Address** - 此 IP 地址应处于不同于故障切换链路的未使用的子网上。
- **Standby IP Address** - 此 IP 地址必须与主用 IP 地址处于相同网络。

步骤 5　在点击 **Finish**后，向导会显示 **Waiting for Config Sync** 屏幕。

指定时段过后，向导将故障切换配置发送到辅助设备，您将看到信息屏幕，该屏幕显示故障切换配置完成。

- 如果您不知道在辅助设备是否已启用故障切换，请在指定时段内进行等待。
- 如果知道故障切换已启用，请点击 **Skip configuring peer**。
- 如果知道辅助设备尚未启用故障切换，请点击 **Stop waiting *xx* more seconds**，故障切换启动配置将立即发送到备用设备。

配置主用/主用故障切换

High Availability and Scalability Wizard 可以分步骤指导您创建主用/主用故障切换配置。

操作步骤

步骤 1　依次选择 **Wizards > High Availability and Scalability**。请参阅以下步骤中有关选择向导的指引。

步骤 2　在 **Failover Peer Connectivity and Compatibility Check** 屏幕中，对等体 IP 地址必须是已启用 ASDM 访问的接口。

默认情况下，对等体地址会被指定为 ASDM 连接到的接口的备用地址。

步骤 3　在 **Security Context Configuration** 屏幕中，如果您在运行向导的过程中已转换到多情景模式，则仅会看到管理情景。退出向导后，可以添加其他情景。

步骤 4　在 **LAN Link Configuration** 屏幕上：

- **Active IP Address** - 此 IP 地址应处于未使用的子网上。
- **Standby IP Address** - 此 IP 地址必须与主用 IP 地址处于相同网络。
- （可选） **Communications Encryption** - 加密故障切换链路上的通信。**注意**：我们建议使用 IPsec 预共享密钥而不是密钥，您可以在退出向导后配置该预共享密钥 （请参阅修改故障切换设置，第 9-31 页）。

步骤 5　在 **State Link Configuration** 屏幕上，如果您选择将另一个接口用于状态故障切换：

- **Active IP Address** - 此 IP 地址应处于不同于故障切换链路的未使用的子网上。
- **Standby IP Address** - 此 IP 地址必须与主用 IP 地址处于相同网络。

步骤 6　在点击 **Finish**后，向导会显示 **Waiting for Config Sync** 屏幕。

指定时段过后，向导将故障切换配置发送到辅助设备，您将看到信息屏幕，该屏幕显示故障切换配置完成。

- 如果您不知道在辅助设备是否已启用故障切换，请在指定时段内进行等待。
- 如果知道故障切换已启用，请点击 **Skip configuring peer**。
- 如果知道辅助设备尚未启用故障切换，请点击 **Stop waiting *xx* more seconds**，故障切换启动配置将立即发送到备用设备。

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

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 9-24 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。本节包括为主用/主用模式下的每个故障切换组启用 HTTP 复制；要为主用/备用模式配置 HTTP 复制，请参阅修改故障切换设置，第 9-31 页。

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　依次选择 **Configuration > Device Management > High Availability and Scalability > Failover**。

步骤 2　禁用在备用设备或情景中直接进行任何配置更改的功能：在 **Setup** 选项卡上，选中 **Disable configuration changes on the standby unit** 复选框。

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。

步骤 3　点击 **Criteria** 选项卡。

步骤 4　配置设备轮询时间：

在 **Failover Poll Times** 区域：

- **Unit Failover** - 设备之间的 Hello 消息所间隔的时长。取值范围介于 1 和 15 秒之间，或者 200 和 999 毫秒之间。
- **Unit Hold Time** - 设置设备在此期间，必须在故障切换链路上收到 Hello 消息，否则设备会开始对等体故障测试过程的时长。取值范围介于 1 和 45 秒之间，或者 800 和 999 毫秒之间。输入的值不得短于轮询时间的 3 倍。

注意　此窗格中的其他设置仅适用于主用/备用模式。在主用/主用模式下，您必须为每个故障切换组配置其余参数。

步骤 5　（仅主用/主用模式）点击 **Active/Active** 选项卡，然后选择故障切换组，并点击 **Edit**。

步骤 6　（仅主用/主用模式）更改故障切换组的首选角色：点击 **Primary** 或 **Secondary**。

如果使用了向导，则故障切换组 1 会分配到主设备，故障切换组 2 会分配到辅助设备。如果需要非标准配置，则可以根据需要指定不同的设备首选项。

步骤 7　（仅主用/主用模式）配置故障切换组抢占：选中 **Preempt after booting with optional delay of** 复选框。

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，此选项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。

注意　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 8　配置 **Interface Policy**：

- **Number of failed interfaces that triggers failover** - 定义要触发故障切换，必须达到的特定故障接口数，范围介于 1 到 250 之间。发生故障的受监控接口数超过您指定的值时， ASA 将会进行故障切换。
- **Percentage of failed interfaces that triggers failover** - 定义要触发故障切换，必须达到的发生故障的已配置接口的百分比。发生故障的受监控接口数超过您设置的百分比时， ASA 将会进行故障切换。

注意　请勿使用 **Use system failover interface policy** 选项。此时您仅可以设置每个组的策略。

步骤 9　（主用/备用模式）配置接口轮询时间：

在 **Failover Poll Time** 区域：

- **Monitored Interfaces** - 接口之间的轮询间隔的时长。取值范围介于 1 和 15 秒之间，或者 500 和 999 毫秒之间。
- **Unit Hold Time** - 设置在此期间，数据接口必须收到 Hello 消息的时长，该时长过后，对等体会被宣布为发送故障。有效值范围为 5 至 75 秒。

对于主用/主用模式，请在 **Add/Edit Failover Group** 对话框中配置接口轮询时间。

步骤 10　（仅主用/主用模式）启用 HTTP 复制：选中 **Enable HTTP replication** 复选框。

有关主用/备用模式，请参阅修改故障切换设置，第 9-31 页。有关这两种模式的 HTTP 复制速率，请参阅修改故障切换设置，第 9-31 页一节。

步骤 11　配置虚拟 MAC 地址：

- 主用/备用模式 - 点击 **MAC Addresses** 选项卡，然后点击 **Add**。

  系统将显示 **Add/Edit Interface MAC Address** 对话框。
- 主用/主用模式 - 转至 **Active/Active** 选项卡底部。

您也可以使用其他方法设置 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。

a. 从 **Physical Interface** 下拉列表中选择接口。

b. 在 **Active MAC Address** 字段中，键入主用接口的新 MAC 地址。

c. 在 **Standby MAC Address** 字段中，键入备用接口的新 MAC 地址。

d. 点击 **OK**。（仅主用/主用模式）再次点击 **OK**。

步骤 12　点击 **Apply**。

配置接口监控和备用地址

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。

如果未在向导中配置备用 IP 地址，可以手动配置这些 IP 地址。

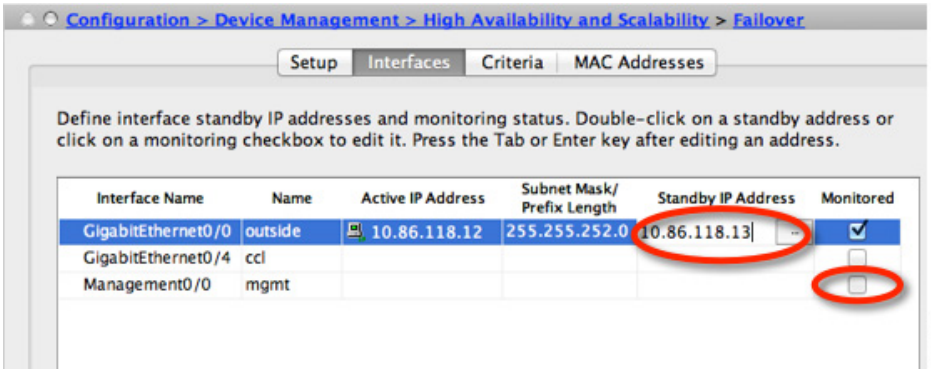
准备工作

- 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　在单模式下，请依次选择 **Configuration > Device Management > High Availability > Failover > Interfaces**。

在多情景模式下，在一个情景中依次选择 **Configuration > Device Management > Failover > Interfaces**



系统将显示配置的接口，以及所有安装的硬件模块 （如 ASA FirePOWER 模块）的列表。**Monitored** 列显示是否将监控某个接口作为故障切换条件的一部分。如果接口受监控，**Monitored** 复选框中会显示复选标记。

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。

每个接口的 IP 地址会显示在 **Active IP Address** 列中。如果已配置，接口的备用 IP 地址会显示在 **Standby IP Address** 列中。故障切换链路和状态链路不会显示 IP 地址；您无法从此选项卡更改这些地址。

步骤 2　要禁用对所列接口的监控，请取消选中相应接口的 **Monitored** 复选框。

步骤 3　要启用对所列接口的监控，请取消选中相应接口的 **Monitored** 复选框。

步骤 4　对于每个没有备用 IP 地址的接口，请双击 **Standby IP Address** 字段，并在该字段中输入 IP 地址。

步骤 5　点击 **Apply**。

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。

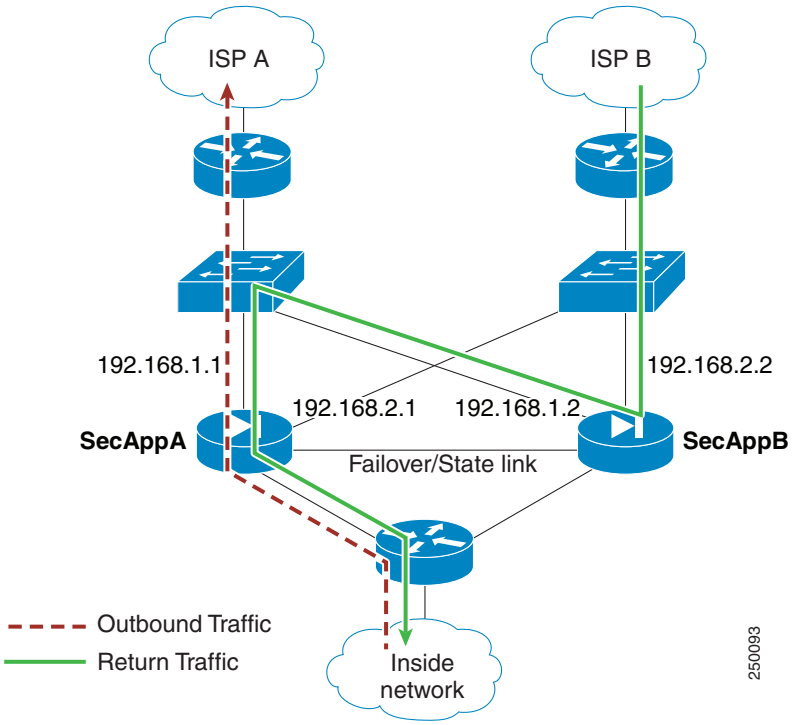
您可以通过允许非对称路由数据包来防止返回数据包。为此，您需要将每台 ASA 上的相似接口分配到同一个 ASR 组。例如，两台 ASA 的内部接口连接到内部网络，但外部接口连接到不同的 ISP。在主设备上，将主用情景外部接口分配给 ASR 组 1；在辅助设备上，将主用情景外部接口分配给相同 ASR 组 1。当主设备外部接口收到没有其会话信息的数据包时，它会检查相同组中处于备用情景中的另一接口的会话信息；在此示例中，即 ASR 组 1。如果没有找到匹配项，数据包会被丢弃。如果找到匹配项，则会进行以下的操作：

- 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 9-13　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　在主设备主用情景上，请依次选择 **Configuration > Device Setup > Routing > ASR Groups**。

步骤 2　对于接收非对称路由数据包的接口，请从下拉列表中选择 **ASR Group ID**。

步骤 3　点击 **Apply** 以保存对运行配置所做的更改。

步骤 4　将 ASDM 连接到辅助设备，然后选择类似于主设备情景的主用情景。

步骤 5　依次选择 **Configuration > Device Setup > Routing > ASR Groups**。

步骤 6　对于此设备上的类似接口，请选择同一 **ASR Group ID**。

步骤 7　点击 **Apply** 以保存对运行配置所做的更改。

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。

修改故障切换设置

如果不使用向导，或者要更改设置，您可以手动配置故障切换设置。本节还包括向导中未包括的以下选项，因此您必须手动配置这些选项：

- 用于加密故障切换流量的 IPsec 预共享密钥
- HTTP 复制速率
- HTTP 复制 （主用/备用模式）

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　在单模式下，请依次选择 **Configuration > Device Management > High Availability and Scalability > Failover > Setup**。

在多情景模式下，请在系统执行空间中依次选择 **Configuration > Device Management > Failover > Setup**。

步骤 2　选中 **Enable Failover** 复选框。

注意　故障切换实际上并未启用，直到您将更改应用到设备。

步骤 3　要加密故障切换和状态链路上的通信，请使用以下其中一个选项：

- **IPsec Preshared Key** （首选） - 此预共享密钥由 IKEv2 用于在故障切换设备之间的故障切换链路上，建立 IPsec LAN 到 LAN 隧道。注意：故障切换 LAN 到 LAN 隧道不计入 IPsec （其他 VPN）许可证。
- **Secret Key** - 输入用于加密故障切换通信的密钥。如果将此字段留空，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和密钥）将采用明文形式。

  Use 32 hexadecimal character key - 要将 32 个十六进制字符的密钥用作密钥，请选中此复选框。

步骤 4　在 **LAN Failover** 区域中，为故障切换链路设置以下参数：

- **Interface** - 选择用于故障切换链路的接口。故障切换需要专用接口，但是，您可以与状态故障切换共享接口。

  仅未配置的接口或子接口会显示在此列表中，并且可以被选择用作故障切换链路。一旦将接口指定为故障切换链路，您将无法在 Configuration > Interfaces 窗格中编辑该接口。
- **Logical Name** - 指定用于故障切换通信的接口逻辑名称，如 “failover”。此名称仅供参考。
- **Active IP** - 指定接口的主用 IP 地址。该 IP 地址可以是 IPv4 或 IPv6 地址。此 IP 地址应处于未使用的子网上。
- **Standby IP** - 指定接口的备用 IP 地址，该地址与主用 IP 地址位于同一子网。
- **Subnet Mask** - 指定子网掩码。
- **Preferred Role** - 选择 **Primary** 或 **Secondary** 以指定此 ASA 的首选角色是主设备还是辅助设备。

步骤 5　（可选）通过执行以下操作配置状态链路：

- **Interface** - 选择用于状态链路的接口。您可以选择一个未配置的接口或子接口、故障切换链路或 **--Use Named--** 选项。

注意　我们建议您，将两个独立的专用接口用于故障切换链路和状态链路。

如果选择一个未配置的接口或子接口，必须提供该接口的 **Active IP**、**Subnet Mask**、**Logical Name** 和 **Standby IP**。

如果选择故障切换链路，则不需要指定 **Active IP**、**Subnet Mask**、**Logical Name** 和 **Standby IP** 值；系统将使用为故障切换链路指定的值。

如果选择 **--Use Named--** 选项，Logical Name 字段将成为已命名接口的下拉列表。从此列表中选择接口。不需要指定 **Active IP**、 **Subnet Mask/Prefix Length** 和 **Standby IP** 值。系统将使用为接口指定的值。

- **Logical Name** - 指定用于状态通信的接口的逻辑名称，如 “state”。此名称仅供参考。
- **Active IP** - 指定接口的主用 IP 地址。该 IP 地址可以是 IPv4 或 IPv6 地址。此 IP 地址应处于不同于故障切换链路的未使用子网上。
- **Standby IP** - 指定接口的备用 IP 地址，该地址与主用 IP 地址位于同一子网。
- **Subnet Mask** - 指定子网掩码。
- （可选，仅主用/备用模式) **Enable HTTP Replication** - 此选项允许状态故障切换将主用 HTTP 会话复制到备用防火墙。如果您不允许 HTTP 复制，则在发生故障切换时， HTTP 连接将会断开。在主用/主用模式下，为每个故障切换组设置 HTTP 复制。

步骤 6　在 **Replication** 区域中，将 HTTP 复制速率设置为每秒 8341 到 50000 次连接。默认值为 50000。要使用默认值，请选中 **Use Default check** 复选框。

步骤 7　点击 **Apply**。

配置将会保存到设备。

步骤 8　如果您启用故障切换，您将会看到用于配置故障切换对等体的对话框。

- 如果要以后连接到故障切换对等体，并手动配置匹配的设置，请点击 **No**。
- 要让 ASDM 自动配置故障切换对等体上的相关故障切换设置，请点击 **Yes**。在 **Peer IP Address** 字段中提供对等体 IP 地址。

相关主题

配置故障切换条件和其他设置，第 9-26 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　要在设备级别强制进行故障切换，请执行以下操作：

a.　根据您的情景模式选择屏幕：

- 在单情景模式下，请依次选择 **Monitoring > Properties > Failover > Status**。

- 在多情景模式下，在 System 中依次选择 **Monitoring > Failover > System**。

b. 点击以下其中一个按钮：

- 点击 **Make Active** 使此设备成为主用设备。
- 点击 **Make Standby** 使另一设备成为主用设备。

步骤 2　（仅主用/主用模式）要强制在故障切换组级别进行故障切换，请执行以下操作：

a. 在 System 中，依次选择 **Monitoring > Failover > Failover Group #**，其中 # 是要控制的故障切换组的编号。

b. 点击以下其中一个按钮：

- 点击 **Make Active**，使故障切换组成为此设备上的主用故障切换组。
- 点击 **Make Standby**，使故障切换组成为另一设备上的主用故障切换组。

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　在单模式下，请依次选择 **Configuration > Device Management > High Availability and Scalability > Failover > Setup**。

在多情景模式下，请在系统执行空间中依次选择 **Configuration > Device Management > Failover > Setup**。

步骤 2　取消选中 **Enable Failover** 复选框。

步骤 3　点击 **Apply**。

步骤 4　要完全禁用故障切换，请保存配置并重新加载：

a. 单击 **Save** 按钮。

b. 依次选择 **Tools > System Reload**，然后重新加载 ASA。

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　要在设备级别恢复故障切换，请执行以下步骤：

a. 根据您的情景模式选择屏幕：

- 在单情景模式下，请依次选择 **Monitoring > Properties > Failover > Status**。
- 在多情景模式下，在 System 中依次选择 **Monitoring > Failover > System**。

b. 点击 **Reset Failover**。

步骤 2　（仅主用/主用模式）要在故障切换组级别重置故障切换，请执行以下步骤：

a. 在 System 中，依次选择 **Monitoring > Failover > Failover Group #**，其中 # 是要控制的故障切换组的编号。

b. 点击 **Reset Failover**。

重新同步配置

复制命令会存储在运行配置中。要将复制的命令保存到备用设备上的闪存，请依次选择 **File > Save Running Configuration to Flash**。

监控故障切换

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

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 38 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 39 章 “SNMP”。

监控故障切换状态

备注　在故障切换事件后，您应重新启动 ASDM 或切换到 Devices 窗格中的另一台设备，以返回原始 ASA 并继续监控设备。此操作是必须的，因为当 ASDM 从设备断开然后重新连接设备时，不会重新建立监控连接。

依次选择 **Monitoring > Properties > Failover** 以监控主用/备用故障切换。

使用 Monitoring > Properties > Failover 区域中的以下屏幕监控主用/主用故障切换：

- 系统，第 9-35 页
- 故障切换组 1 和故障切换组 2，第 9-36 页

系统

System 窗格显示系统的故障切换状态。您还可以通过执行以下操作，控制系统的故障切换状态：

- 切换设备的主用/备用状态。
- 重置故障设备。
- 重新加载备用设备。

字段

Failover state of the system - *仅显示*。显示 ASA 的故障切换状态。显示的信息与从 **show failover** 命令收到的输出相同。有关显示的输出的详细信息，请参阅 《命令参考》。

在 System 窗格上可执行以下操作：

- Make Active - 点击此按钮使 ASA 成为主用/备用配置中的主用设备。在主用/主用配置中，点击此按钮使两个故障切换组在 ASA 上都变为主用状态。
- Make Standby - 点击此按钮使 ASA 成为主用/备用对中的备用设备。在主用/主用配置中，点击此按钮使两个故障切换组在 ASA 上都变为备用状态。

- Reset Failover - 点击此按钮将系统从故障状态重置到备用状态。您无法将系统重置到主用状态。点击主用设备的此按钮可重置备用设备。
- Reload Standby - 点击此按钮可强制重新加载备用设备。
- Refresh - 点击此按钮可刷新 Failover state of the system 字段中的状态信息。

故障切换组 1 和故障切换组 2

Failover Group 1 和 Failover Group 2 窗格显示选定组的故障切换状态。您还可以通过切换组的主用/备用状态或通过重置故障组来控制该组的故障切换状态。

字段

Failover state of Group[*x*] - *仅显示*。显示选定故障切换组的故障切换状态。显示的信息与从 **show failover group** 命令收到的输出相同。

您可从此窗格执行以下操作：

- Make Active - 点击此按钮使故障切换组在 ASA 上变为主用状态。
- Make Standby - 点击此按钮使故障切换组在 ASA 上变为备用状态。
- Reset Failover - 点击此按钮将系统从故障状态重置到备用状态。您无法将系统重置到主用状态。点击主用设备的此按钮可重置备用设备。
- Refresh - 点击此按钮可刷新 Failover state of the system 字段中的状态信息。

故障切换历史记录

表 9-4　　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。 修改了以下屏幕：Configuration > Device Management > High Availability > Failover > Setup。
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。 无 ASDM 更改。
添加了故障切换的 IPv6 支持。	8.2(2)	修改了以下屏幕： Configuration > Device Management > High Availability > Failover > Setup Configuration > Device Management > High Availability > Failover > Interfaces

表 9-4　　故障切换历史记录

功能名称	版本	功能信息
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。 **备注**　故障切换 LAN 到 LAN 隧道不计入 IPsec （其他 VPN）许可证。 修改了以下屏幕：Configuration > Device Management > High Availability > Failover > Setup。
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。 修改了以下屏幕：**Configuration > Device Management > High Availability and Scalability > Failover > Interfaces**
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。 修改了 以下屏幕：**Configuration > Device Management > High Availability and Scalability > Failover > Setup**

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 10-23 页。

关于 ASA 集群

本节介绍集群架构及其工作原理。

- ASA 集群如何管理连接，第 10-20 页
- ASA 功能和集群，第 10-22 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 10-29 页
- 集群控制链路，第 10-5 页
- ASA 集群管理，第 10-10 页
- 跨网络 EtherChannel （推荐），第 10-11 页
- 基于策略的路由 （仅适用于路由防火墙模式），第 10-15 页
- 等价多路径路由 （仅适用于路由防火墙模式），第 10-16 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 10-3 页
- 主设备和从属设备角色，第 10-3 页
- 主设备选举，第 10-3 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 10-23 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

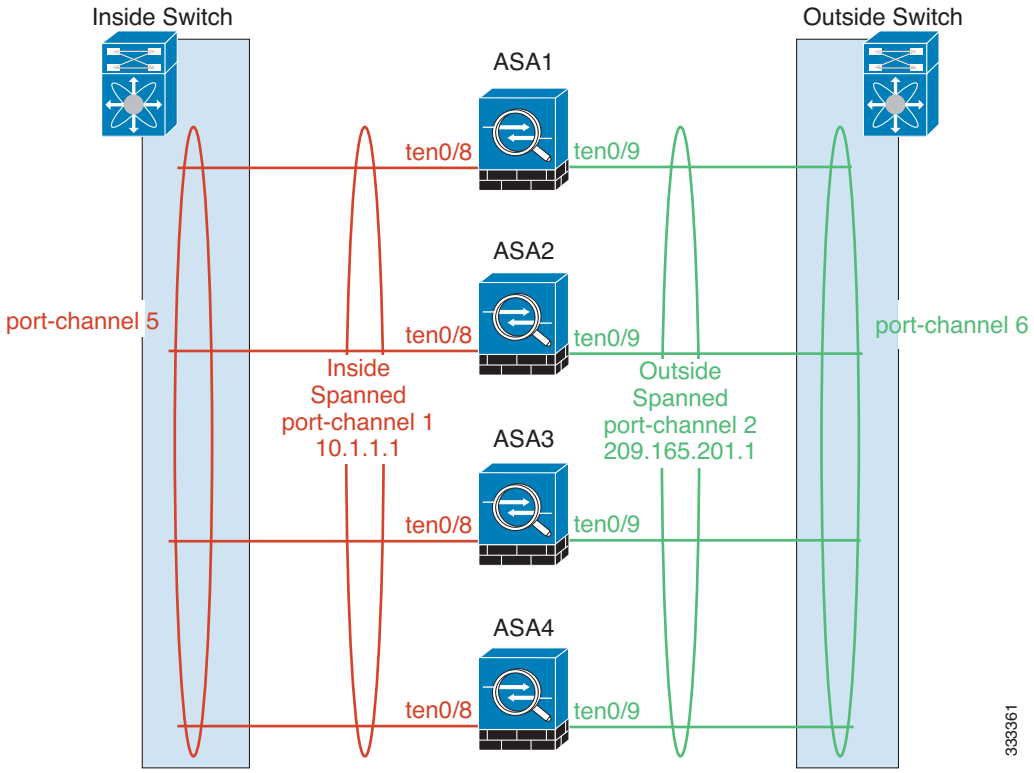
- 集群的集中功能，第 10-23 页

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）

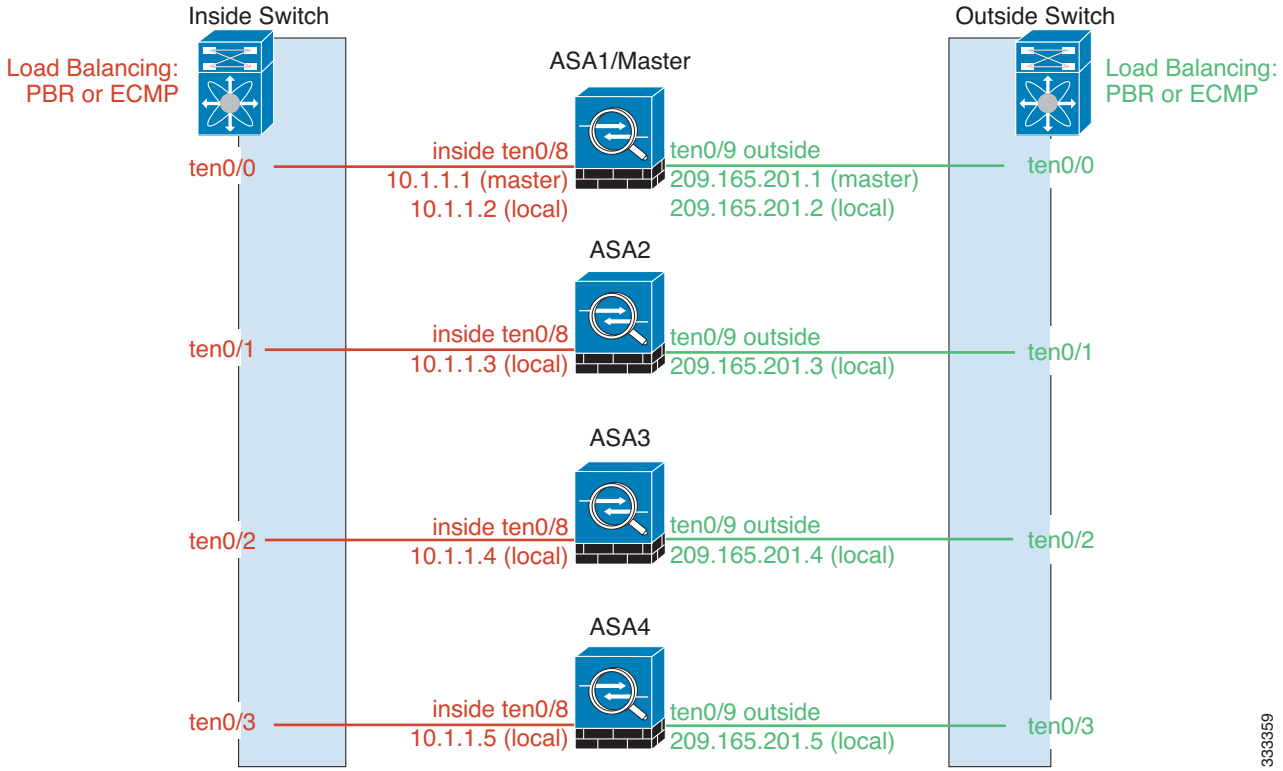
您可以将每台设备的一个或多个接口分组为跨集群中所有设备的 EtherChannel。EtherChannel 汇聚通道中所有可用活动接口上的流量。在路由模式和透明防火墙模式下都可以配置跨网络 EtherChannel。在路由模式下， EtherChannel 被配置为只有一个 IP 地址的路由接口。在透明模式下， IP 地址被分配到网桥组而非接口。负载均衡属于 EtherChannel 固有的基本操作。



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 10-11 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 10-5 页
- 集群控制链路接口和网络，第 10-6 页
- 调整集群控制链路的吞吐量大小，第 10-6 页
- 集群控制链路冗余，第 10-7 页
- 集群控制链路可靠性，第 10-7 页
- 集群控制链路故障，第 10-7 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 10-2 页
- 配置复制，第 10-9 页
- 设备运行状况监控，第 10-8 页
- 数据路径连接状态复制，第 10-9 页
- 在集群中再均衡新的 TCP 连接，第 10-22 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 10-7 页
- 调整集群控制链路的吞吐量大小，第 10-6 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。

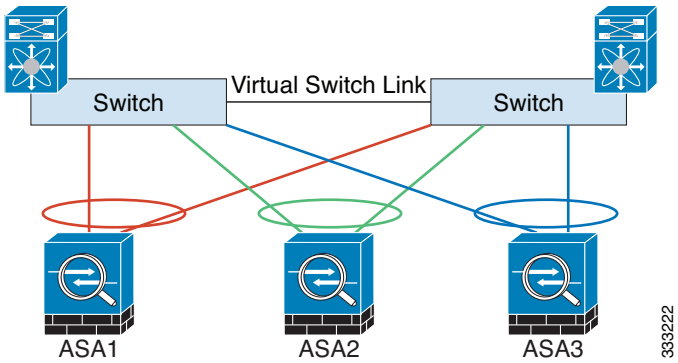
相关主题

- 站点间集群，第 10-16 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 10-9 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

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 10-9 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 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 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启用集群。

相关主题

- 配置 ASA 集群参数，第 10-46 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 10-1　　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

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 20 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 10-11 页
- 基于策略的路由 （仅适用于路由防火墙模式），第 10-15 页
- 等价多路径路由 （仅适用于路由防火墙模式），第 10-16 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 10-11 页
- 最大吞吐量准则，第 10-12 页
- 负载均衡，第 10-12 页
- EtherChannel 冗余，第 10-12 页
- 连接到 VSS 或 vPC，第 10-12 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 12-2 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 12-10 页
- 负载均衡，第 12-4 页
- NAT 和集群，第 10-27 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

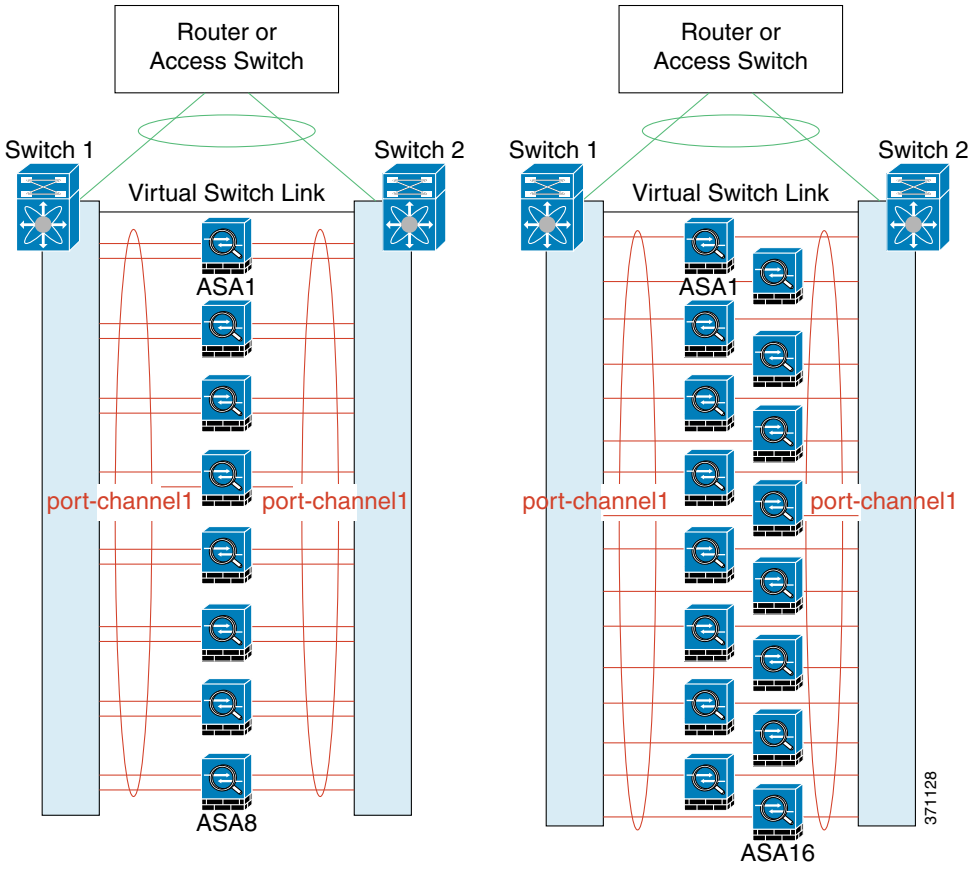
您可以在跨网络 EtherChannel 中包含每台 ASA 的多个接口。每台 ASA 有多个接口，对于连接到 VSS 或 vPC 中两台交换机的情况特别有用。

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）。

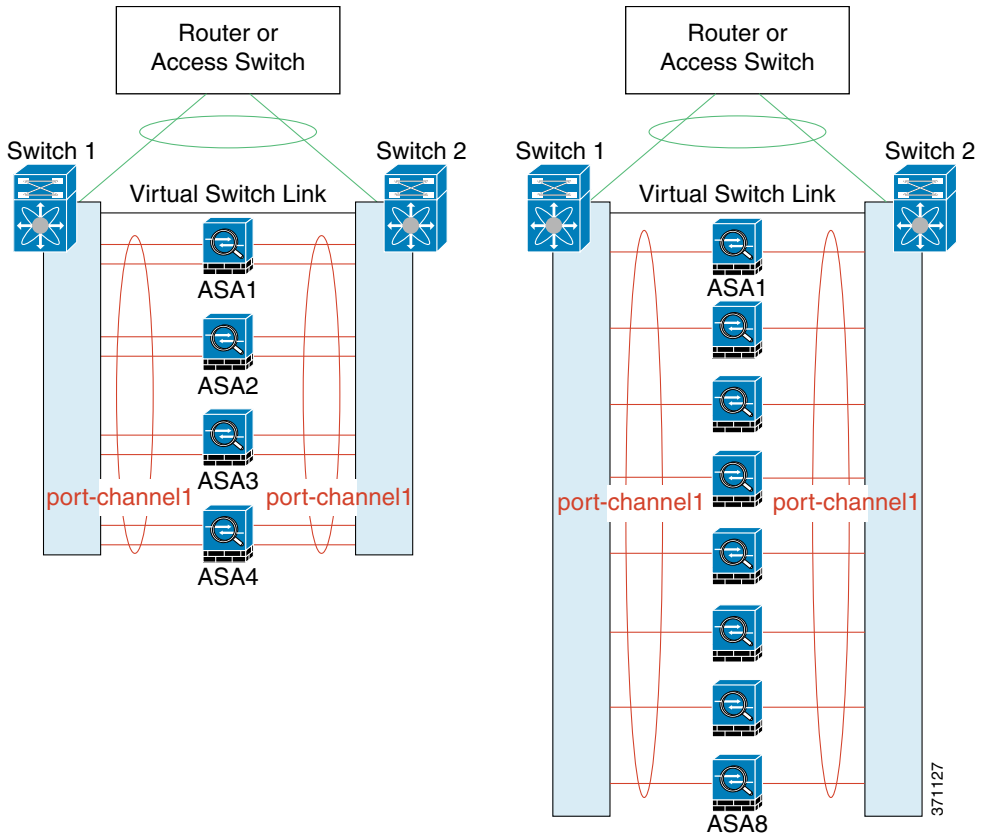
对于支持 EtherChannel 中有 8 条活动链路的交换机，在连接到 VSS/vPC 中的两台交换机时，最多可在跨网络 EtherChannel 中配置 16 条活动链路。

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。

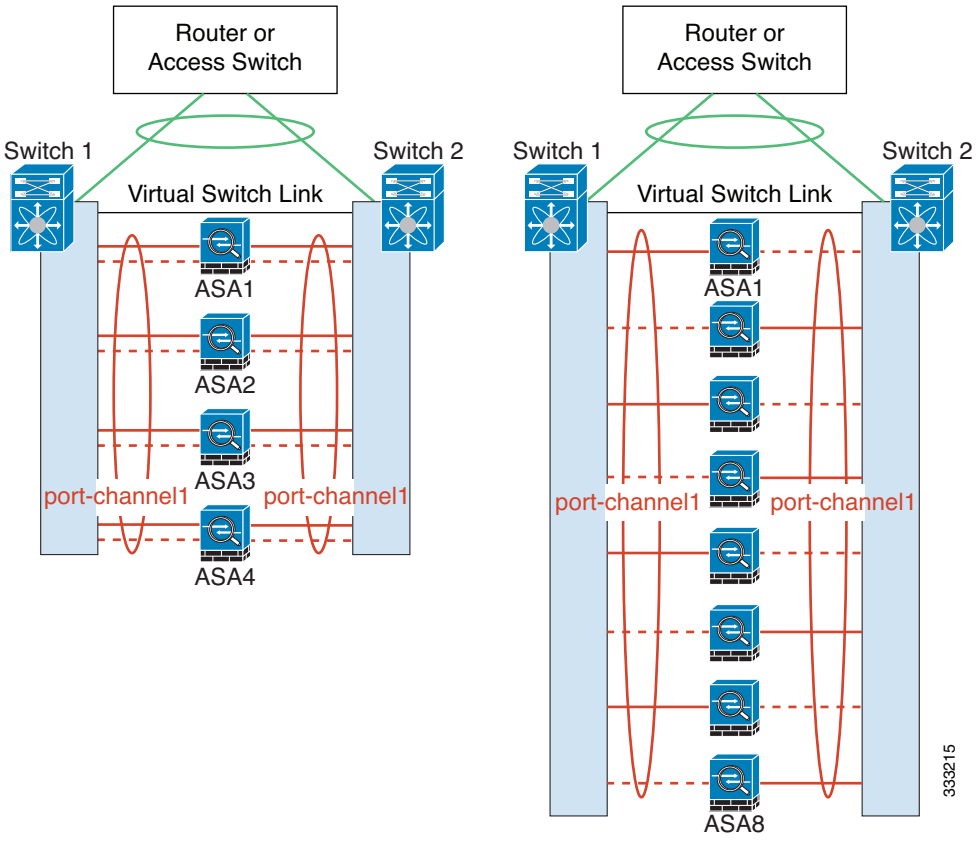
下图所示为 8-ASA 集群和 16-ASA 集群中有 32 条活动链路的跨网络 EtherChannel。



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 10-16 页
- 确定数据中心互联的规格，第 10-17 页
- 站点间集群示例，第 10-18 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 10-22 页
- 连接角色，第 10-21 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)）。

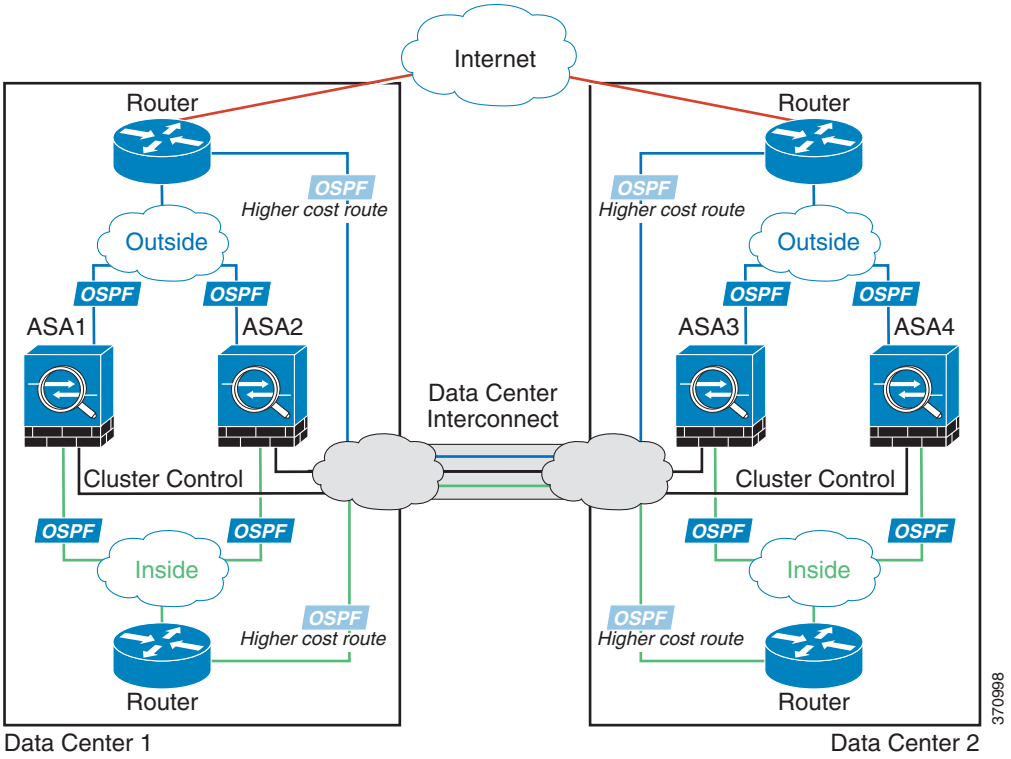
站点间集群示例

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 10-18 页
- 跨网络 EtherChannel 透明模式南北站点间集群示例，第 10-19 页
- 跨网络 EtherChannel 透明模式东西站点间集群示例，第 10-20 页

独立接口路由模式南北站点间集群示例

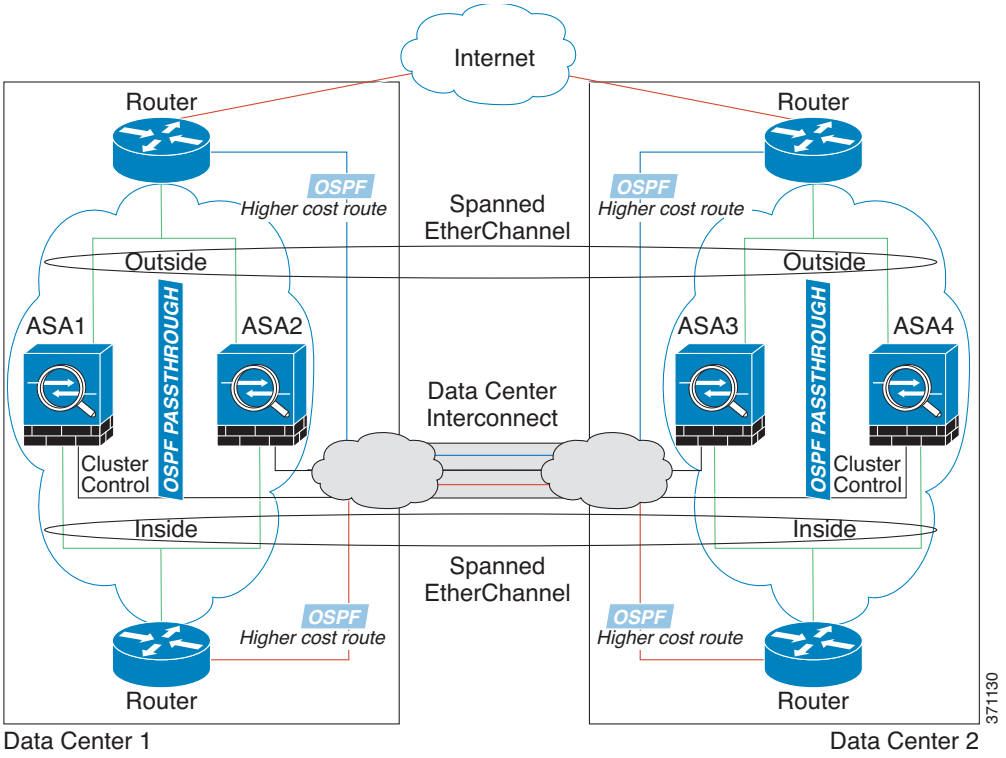
以下示例显示了分别位于 2 个布置于内部和外部路由器（南北插入）之间的数据中心的 2 个 ASA 集群成员。集群成员由集群控制链路通过 DCI 连接。位于每个数据中心的内部和外部路由器使用 OSPF 和 PBR 或 ECMP 在集群成员之间对流量执行负载均衡。通过指定 DCI 中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有 ASA 集群成员都中断连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的 ASA 集群成员。



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。



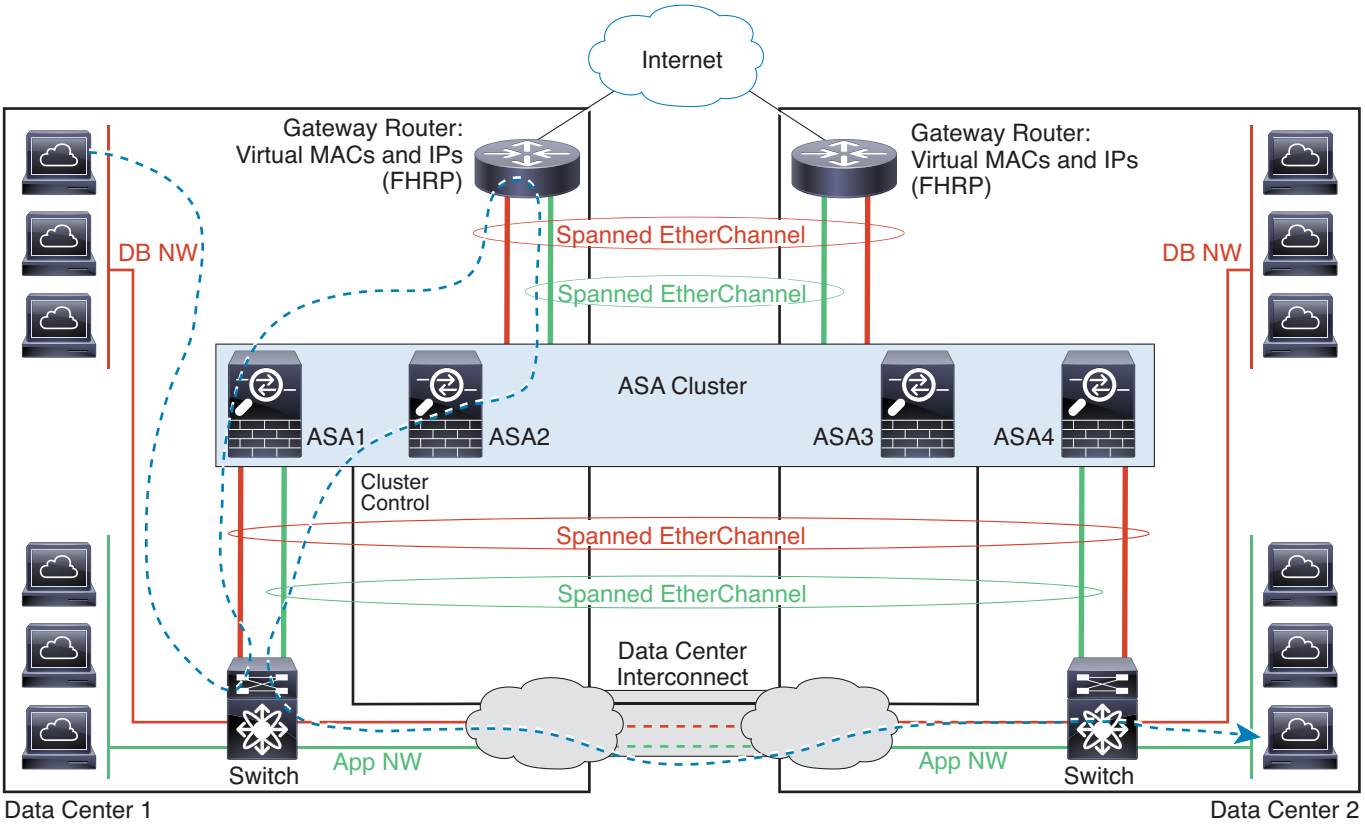
位于每个站点的交换机的实施可包括：

- 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 10-19 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

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

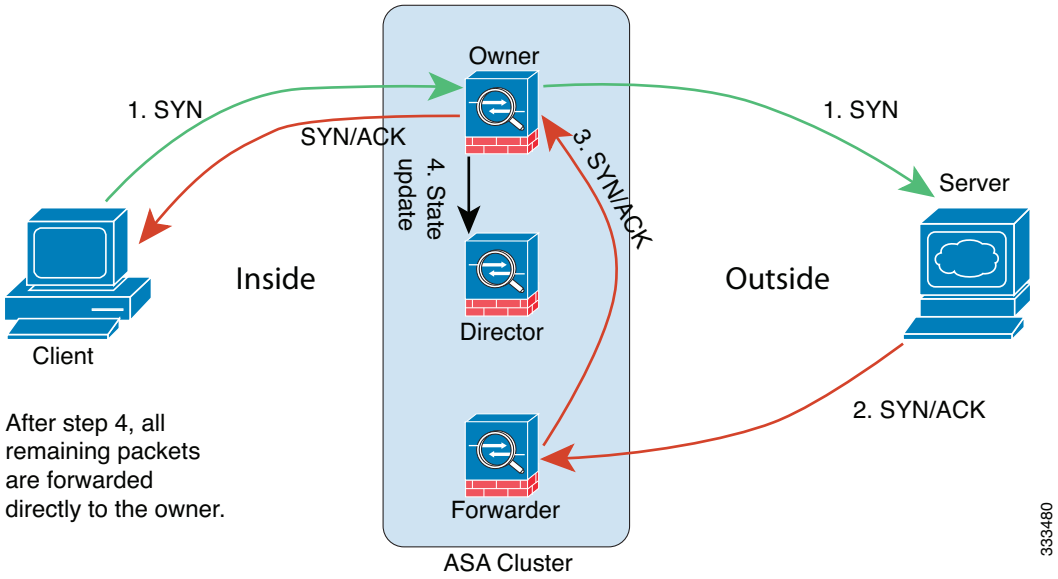
通过负载均衡将新连接定向到集群成员时，该连接的两个方向都由此设备所有。如果该连接有任何数据包到达其他设备，这些数据包都会通过集群控制链路被转发到所有者设备。为了获得最佳性能，对于要到达同一台设备的流量的两个方向以及要在设备之间均摊的流量，都需要执行适当的外部负载均衡。如果反向流量到达其他设备，会被重定向回原始设备。

相关主题

- 负载均衡方法，第 10-11 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 10-23 页
- 集群的集中功能，第 10-23 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 10-6 页
- 在集群中再均衡新的 TCP 连接，第 10-22 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。

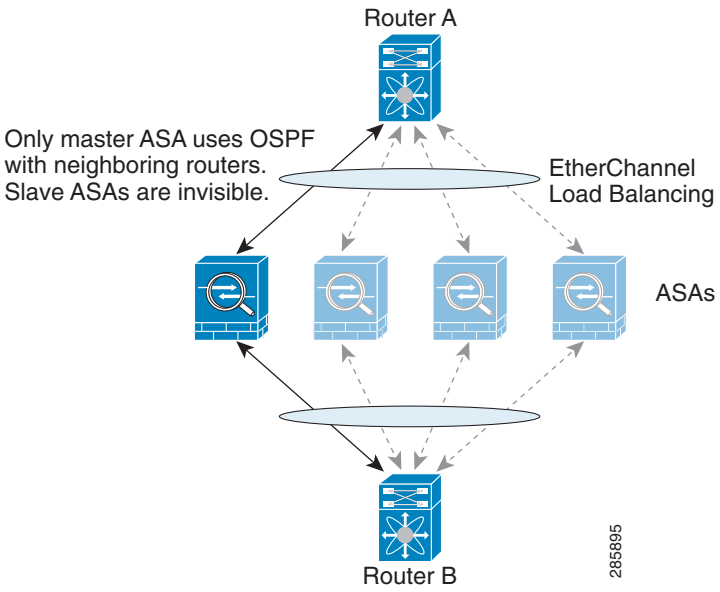
- ASA FirePOWER 模块 - ASA FirePOWER 模块之间不存在配置同步或状态共享。您负责使用 FireSIGHT 管理中心将集群中 ASA FirePOWER 模块上的策略保持一致。请勿对集群内的设备使用不同的基于 ASA 接口的区域定义。
- ASA IPS 模块 - IPS 模块之间不存在配置同步或状态共享。有些 IPS 签名需要 IPS 跨多个连接保存状态信息。例如，当 IPS 模块检测到有人打开多个连接到同一台服务器的连接但端口不同时，将使用端口扫描签名。在集群中，这些连接将在多台 ASA 设备之间进行均衡，其中每台设备都有自己的 IPS 模块。由于这些 IPS 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

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 10-1　跨网络 EtherChannel 模式下的动态路由



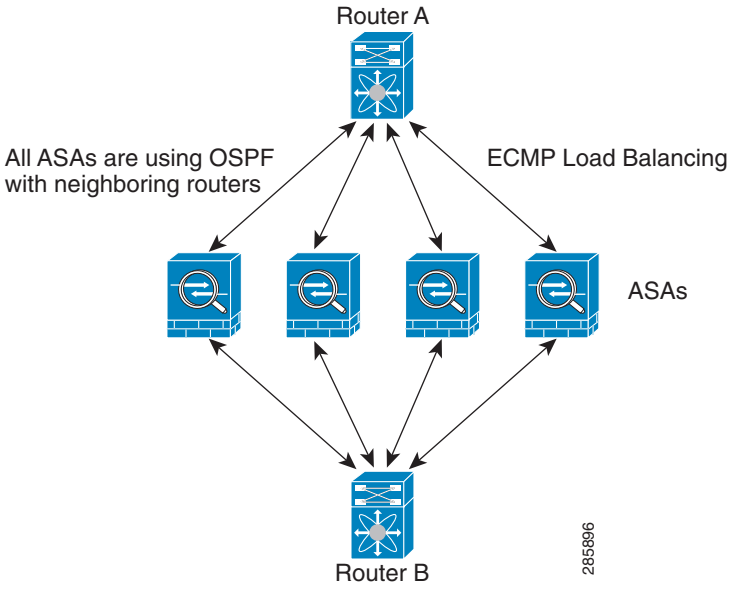
当从属设备成员从主设备获知路由后，每台设备将独立作出转发决定。

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 10-2　　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 10-26 页
- 独立接口模式下的组播路由，第 10-26 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 38-19 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 10-30 页
- 启用巨帧支持，第 11-7 页
- 引导程序配置，第 10-3 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。
- 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。

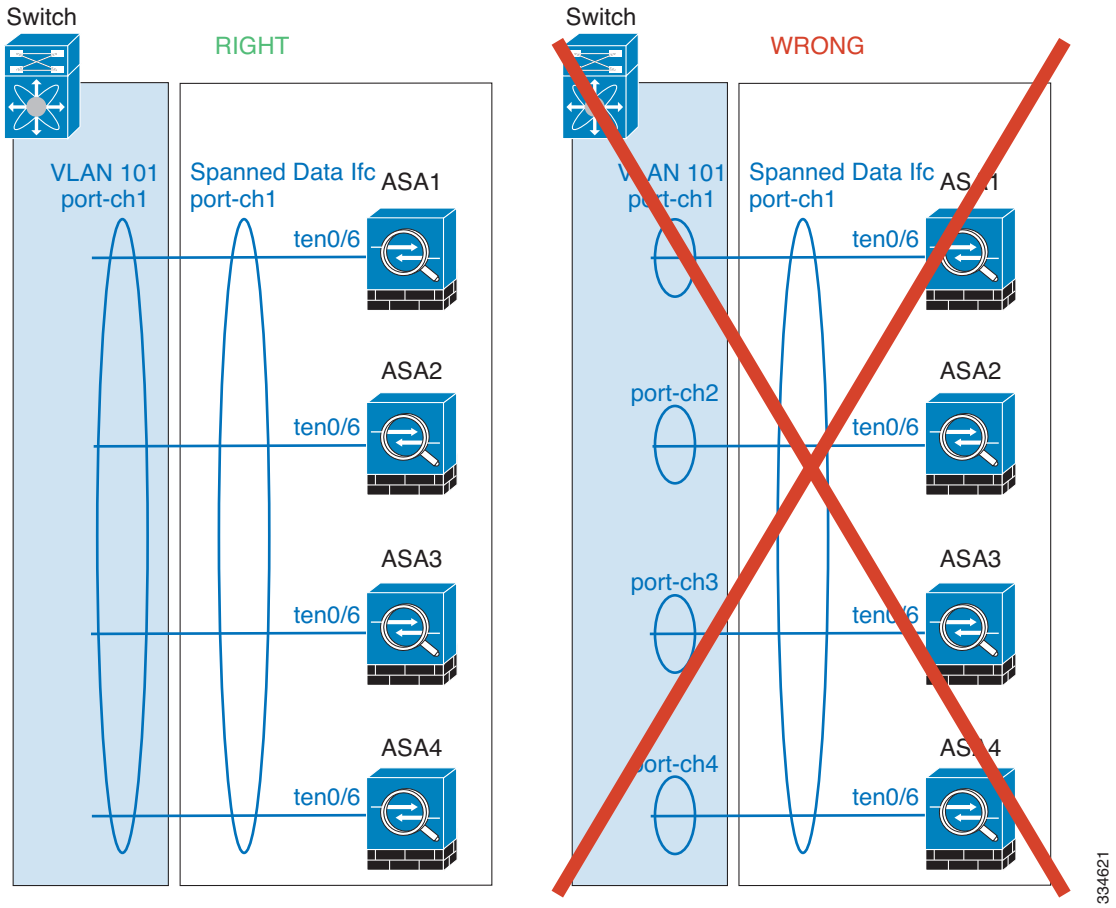
- 有些交换机不支持 LACP 动态端口优先级 （活动链路和备用链路）。您可以禁用动态端口优先级，使跨网络 EtherChannel 具有更高兼容性。
- 集群控制链路路径上的网络要素不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。
- 端口通道绑定中断时间不得超过配置的 keepalive 间隔。
- 在 Supervisor 2T EtherChannel 上，默认的散列值分配算法是自适应算法。为了避免在 VSS 设计中出现非对称流量，请将连接到 ASA 的端口通道上的散列算法更改为固定算法：

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

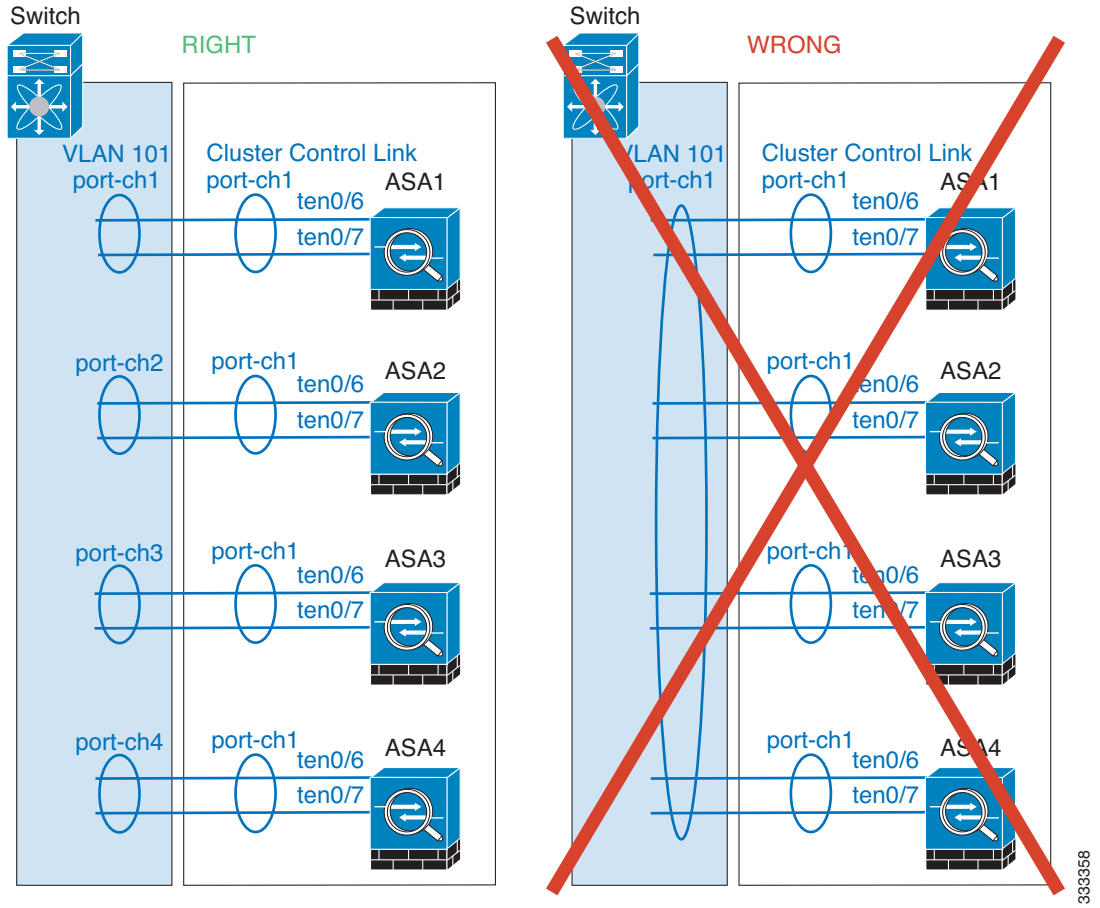
  请勿全局更改算法；您可能需要对 VSS 对等链路使用自适应算法。

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 10-6 页
- 引导程序配置，第 10-3 页

- 集群不支持的功能，第 10-23 页
- 配置 EtherChannel，第 12-8 页
- EtherChannel 接口和冗余接口准则，第 12-4 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 10-29 页和 ASA 集群准则，第 10-30 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 10-33 页。

步骤 3　备份配置 （推荐），第 10-35 页。

步骤 4　在配置主设备集群接口模式，第 10-35 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 5　（推荐；在多情景模式下为必需）在主设备上配置接口，第 10-38 页。如果接口未准备好加入集群，则您无法启用集群。在单情景模式下，您可以选择在 High Availability and Scalability 向导中配置多项接口设置，但并非所有接口选项都在该向导中可用，而且您不能在该向导中配置多情景模式下的接口。

步骤 6　创建或加入 ASA 集群，第 10-43 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。

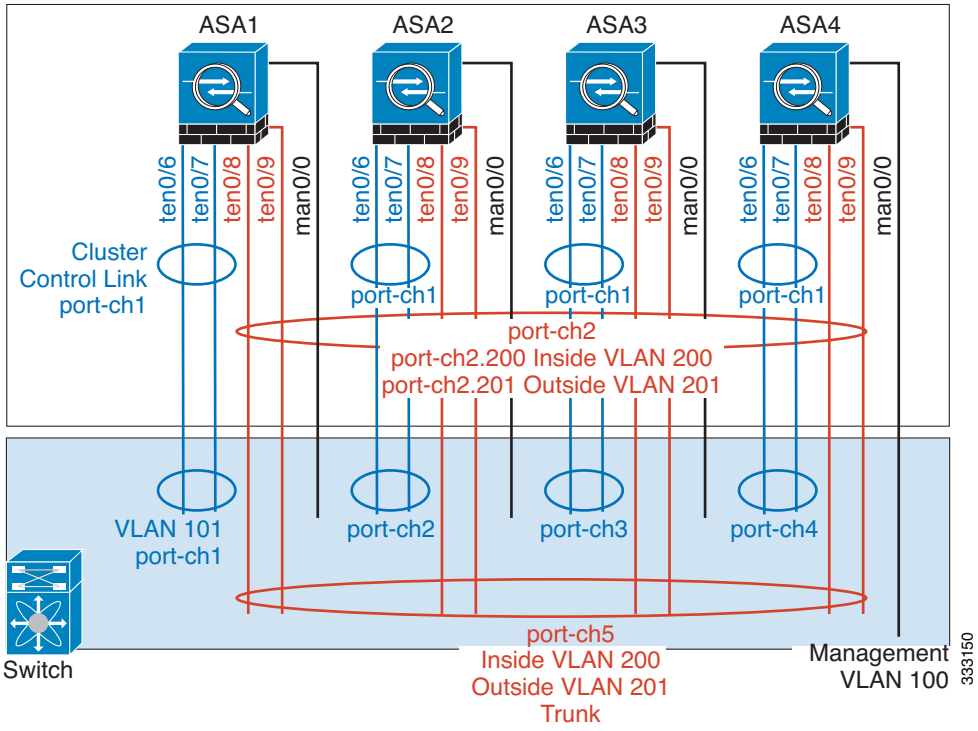
示例

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。
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。

备份配置 （推荐）

在从属设备上启用集群时，当前配置将替换为从主设备同步的配置。如果您要完全退出集群，保留一份含有可用管理接口配置的备份配置可能非常有用。

准备工作

在每台设备上执行备份。

操作步骤

步骤 1　依次选择 **Tools > Backup Configurations**。

步骤 2　至少备份正在运行的配置。有关详细程序，请参阅备份本地 CA 服务器，第 35-21 页。

相关主题

- 退出集群，第 10-51 页

在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。

备注　如果您不从主设备添加从属设备，则必须按照本节中的步骤在所有设备上手动设置接口模式，而不仅仅是在主设备上设置；如果从主设备添加从属设备， ASDM 将在从属设备上自动设置接口模式。

准备工作

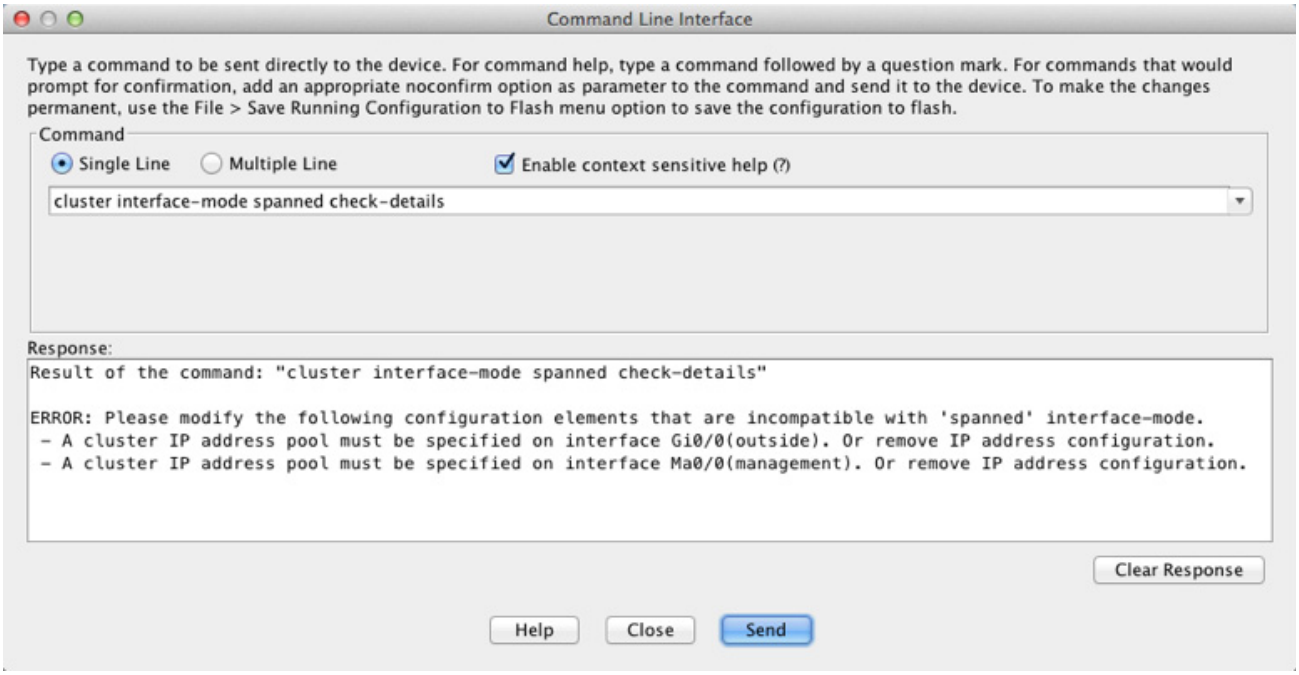
- 您始终可以将管理专用接口配置为独立接口 （推荐），即使是在跨网络 EtherChannel 模式下亦如此。即使是在透明防火墙模式下，管理接口也可以是独立接口。
- 在跨网络 EtherChannel 模式下，如果将管理接口配置为独立接口，您将无法为管理接口启用动态路由。您必须使用静态路由。
- 在多情景模式下，您必须为所有情景选择一种接口类型。例如，如果使用透明和路由模式的混合情景，则必须将跨网络 EtherChannel 模式用于所有情景，因为这是透明模式允许的唯一接口类型。

操作步骤

步骤 1　在主设备的 ASDM 中，依次选择 **Tools > Command Line Interface**。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：

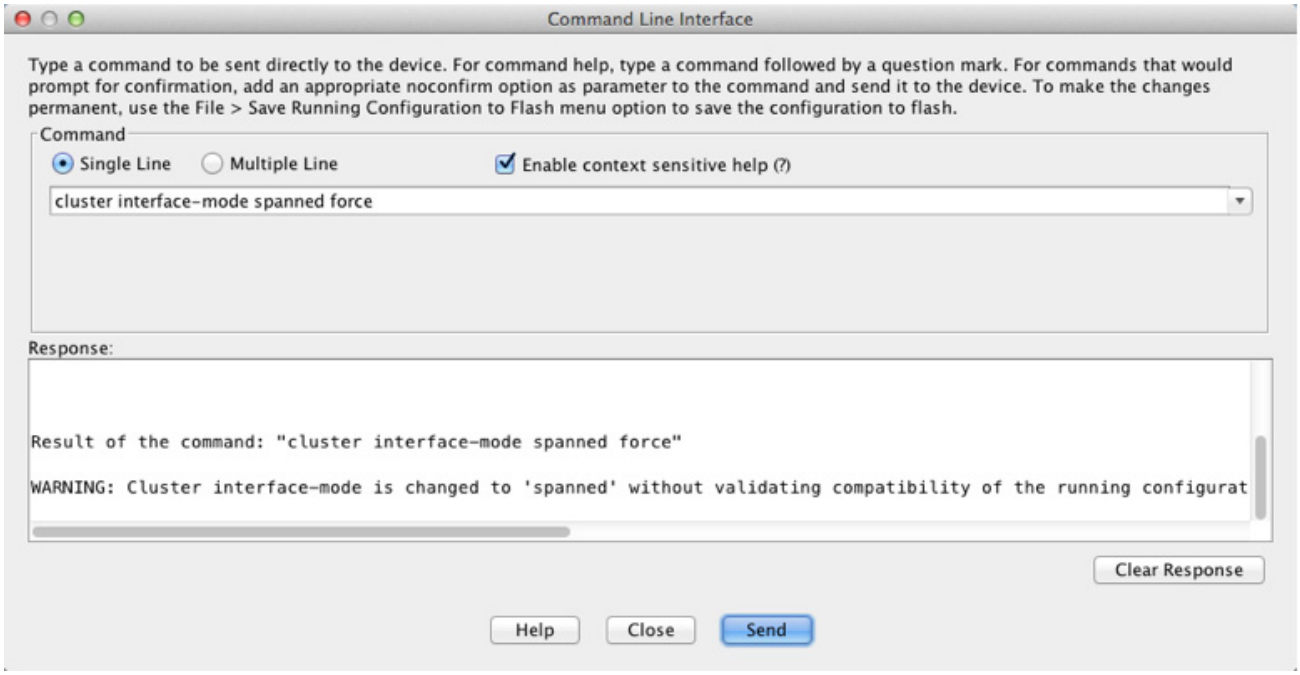


注意　设置接口模式之后，您可以继续连接到接口；但是，如果您在配置管理接口使其符合集群要求（例如添加集群 IP 池）之前重新加载 ASA，则将无法重新连接，因为与集群不兼容的接口配置已删除。在此情况下，您必须连接到控制台端口来修复接口配置。

步骤 2　为集群设置接口模式：

```
cluster interface-mode {individual | spanned} force
```

示例：



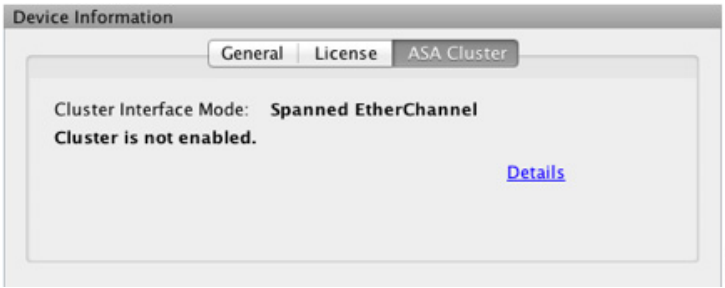
不存在默认设置；您必须明确选择模式。如果尚未设置模式，则无法启用集群。

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。

步骤 3　退出 ASDM 并重新加载。ASDM 需要重新启动才能正确解释集群接口模式。重新加载后，主页上将显示 ASA Cluster 选项卡：



相关主题

- （推荐；在多情景模式下为必需）在主设备上配置接口，第 10-38 页

（推荐；在多情景模式下为必需）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。至少，您必须修改 ASDM 当前连接到的管理接口。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。在多情景模式下，您必须使用本节中的程序修复现有接口或配置新的接口。但是在单情景模式下，您可以跳过本节，在 High Availability and Scalability 向导中配置通用接口参数（请参阅创建或加入 ASA 集群，第 10-43 页）。请注意，诸如为独立接口创建 EtherChannel 之类的高级接口设置在此向导中不可用。

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 10-38 页
- 配置跨网络 EtherChannel，第 10-40 页

相关主题

- 集群接口，第 10-4 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，在 Configuration > Device List 窗格中双击主用设备 IP 地址下的情景名称。
- 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。
- 如果使用 ASDM 远程连接到管理接口，则未来从属设备的当前 IP 地址仅供临时使用。
  - 每个成员都将从主设备上定义的集群 IP 池中分配到一个 IP 地址。
  - 集群 IP 池不能包含网络中已在使用的地址，包括未来从属设备的 IP 地址。

    例如：

  a. 将主设备配置为使用 10.1.1.1。
  b. 其他设备使用 10.1.1.2、 10.1.1.3 和 10.1.1.4。
  c. 在主设备上配置集群 IP 池时，不能在地址池中包含地址 .2、 .3 或 .4，因其已在使用中。
  d. 反之，您需要使用该网络中的其他 IP 地址，如 .5、 .6、 .7 和 .8。

     注意　地址池需要的地址数量与包括主设备在内的集群成员数相等；原始 .1 地址是属于当前主设备的主集群 IP 地址。

  e. 加入集群之后，临时使用的旧地址将被弃用并可用于它处。

操作步骤

步骤 1　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格。

步骤 2　选择接口行，然后点击 **Edit**。设置接口参数。请参阅以下准则：

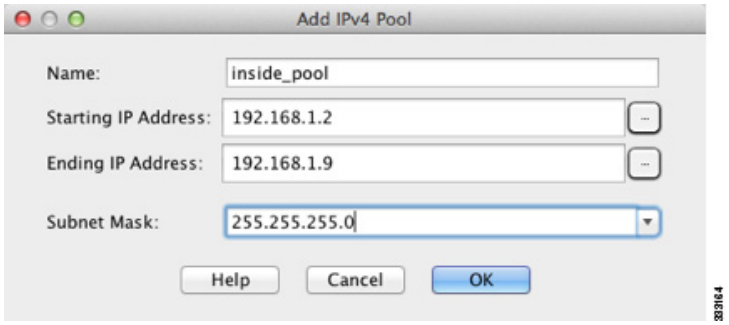
- （对跨网络 EtherChannel 模式下的管理接口为必需项）**Dedicate this interface to management only** - 将一个接口设置为管理专用模式，确保不会有流量流经该接口。默认情况下，管理类型的接口被配置为管理专用。在透明模式下，此命令对管理类型的接口始终启用。
- **Use Static IP** - 不支持 DHCP 和 PPPoE。

步骤 3　要添加 IPv4 集群 IP 池或者 MAC 地址池，请点击 **Advanced** 选项卡。

a. 在 **ASA Cluster** 区域，通过点击 **IP Address Pool** 字段旁的 **...** 按钮来创建集群 IP 池。系统显示的有效范围取决于您在 General 选项卡中设置的主 IP 地址。

b. 点击**添加**。

c. 配置一个地址范围，不含主集群 IP 地址，也不含网络中当前在使用的任何地址。此地址范围应对集群的大小而言足够大，例如有 8 个地址。



d. 点击 **OK** 以创建新的地址池。

e. 选择创建的新地址池并点击 **Assign**，然后点击 **OK**。

地址池名称将显示于 **IP Address Pool** 字段中。

步骤 4　要配置 IPv6 地址，请点击 **IPv6** 选项卡。

a. 选中 **Enable IPv6** 复选框。

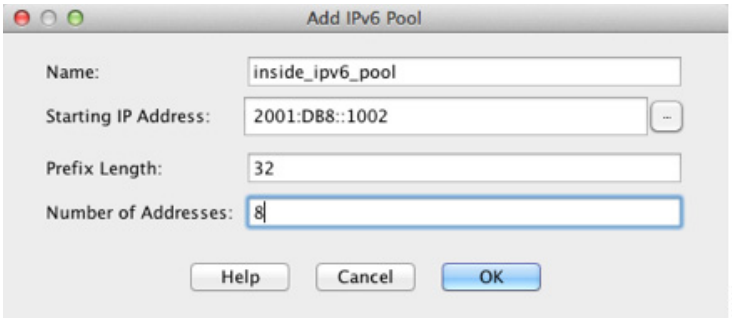
b. 在 **Interface IPv6 Addresses** 区域，点击 **Add**。

不支持 **Enable address autoconfiguration** 选项。

系统将显示 **Add IPv6 Address for Interface** 对话框。

c. 在 **Address/Prefix Length** 字段中，输入全局 IPv6 地址和 IPv6 前缀长度。例如，2001:0DB8::BA98:0:3210/48。点击 **...** 按钮配置集群 IP 池。

d. 点击**添加**。



e. 配置起始 IP 地址 （网络前缀）、前缀长度和地址池中的地址数量。

f. 点击 **OK** 以创建新的地址池。

g. 选择创建的新地址池并点击 **Assign**，然后点击 **OK**。

地址池将显示于 **IP Cluster IP Pool** 字段中。

h. 点击 **OK**。

步骤 5　点击 **OK** 以返回到 Interfaces 窗格。

步骤 6　点击 **Apply**。

相关主题

- 管理接口，第 10-10 页
- 在配置主设备集群接口模式，第 10-35 页
- 负载均衡方法，第 10-11 页
- 配置 EtherChannel，第 12-8 页
- 启用巨帧支持，第 11-7 页
- 配置 VLAN 子接口和 802.1Q 中继，第 13-3 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，在 Configuration > Device List 窗格中双击主用设备 IP 地址下的 **System**。
- 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。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。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。
- 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　视情景模式而定：

- 对于单情景模式，请依次选择 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中依次选择 **Configuration > Context Management > Interfaces** 窗格。

步骤 2　依次选择 **Add > EtherChannel Interface**。

系统将显示 **Add EtherChannel Interface** 对话框。

步骤 3　启用以下项目：

- **Port Channel ID**
- **Span EtherChannel across the ASA cluster**
- **Enable Interface** （默认选中）
- **Members in Group** - 在 **Members in Group** 列表中，至少需要添加一个接口。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。

  确保所有接口的类型和速度相同。添加的第一个接口决定了 EtherChannel 的类型和速度。您添加的任何不匹配接口都将被置于暂停状态。ASDM 不会阻止您添加不匹配的接口。

本程序稍后将介绍此屏幕上的其余字段。

步骤 4　（可选）要覆盖所有成员接口的介质类型、双工、速度以及流量控制暂停帧，请点击 **Configure Hardware Properties**。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。

点击 **OK** 接受 **Hardware Properties** 更改。

步骤 5　要配置 MAC 地址和可选参数，请点击 **Advanced** 选项卡。

- 在 **MAC Address Cloning** 区域，为 EtherChannel 设置手动 MAC 地址。请勿设置备用 MAC 地址；它会被忽略。您必须为跨网络 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；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。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。
- （可选）如果将 ASA 连接到 VSS 或 vPC 中的两台交换机，则应选中 **Enable load balancing between switch pairs in VSS or vPC** 模式复选框来启用 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。

然后，您必须在 **Member Interface Configuration** 区域确定要将给定接口连接到的交换机，**1** 还是 **2**。

注意　我们建议*不要*设置 **Minimum Active Members** 和 **Maximum Active Members**。

步骤 6　（可选）在此 EtherChannel 上配置 VLAN 子接口。本程序的其余部分适用于子接口。

步骤 7　（多情景模式）完成本程序之前，您需要将接口分配到情景。

a. 点击 **OK** 接受更改。

b. 分配接口。

c. 更改为要配置的情景：在 **Device List** 窗格中双击主用设备 IP 地址下的情景名称。

d. 依次选择 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格，选择要自定义的端口通道接口，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框。

步骤 8　点击 **General** 选项卡。

步骤 9　（透明模式）从 **Bridge Group** 下拉列表中选择要将此接口分配到的网桥组。

步骤 10　在 **Interface Name** 字段中，输入长度最大为 48 个字符的名称。

步骤 11　在 **Security level** 字段中，输入介于 0 （最低）和 100 （最高）之间的级别。

步骤 12　（路由模式）对于 IPv4 地址，请点击 **Use Static IP** 单选按钮，然后输入 IP 地址和掩码。不支持 DHCP 和 PPPoE。对于透明模式，您应为网桥组接口而非 EtherChannel 接口配置 IP 地址。

步骤 13　（路由模式）要配置 IPv6 地址，请点击 **IPv6** 选项卡。

对于透明模式，您应为网桥组接口而非 EtherChannel 接口配置 IP 地址。

a. 选中 **Enable IPv6** 复选框。

b. 在 **Interface IPv6 Addresses** 区域，点击 **Add**。

系统将显示 **Add IPv6 Address for Interface** 对话框。

注意：不支持 **Enable address autoconfiguration** 选项。

c. 在 **Address/Prefix Length** 字段中，输入全局 IPv6 地址和 IPv6 前缀长度。例如，2001:DB8::BA98:0:3210/64。

d. （可选）要使用经过修改的 EUI-64 接口 ID 作为主机地址，请选中 **EUI - 64** 复选框。在此情况下，只需在 **Address/Prefix Length** 字段中输入前缀。

e. 点击 **OK**。

步骤 14　点击 **OK** 以返回到 **Interfaces** 屏幕。

步骤 15　点击 **Apply**。

相关主题

- 在配置主设备集群接口模式，第 10-35 页
- 配置网桥组，第 15-8 页
- 创建或加入 ASA 集群，第 10-43 页
- 配置 EtherChannel，第 12-8 页
- EtherChannel 接口和冗余接口准则，第 12-4 页

- 连接到 VSS 或 vPC，第 10-12 页
- 启用物理接口和配置以太网参数，第 11-6 页
- 配置 VLAN 子接口和 802.1Q 中继，第 13-3 页
- 配置安全情景，第 8-17 页
- 安全级别，第 15-1 页
- 配置 ASA 集群参数，第 10-46 页
- ASA 集群准则，第 10-30 页

创建或加入 ASA 集群

集群中的每台设备都需要有引导程序配置才能加入集群。在 （将要成为主设备的）一台设备上运行 High Availability and Scalability 向导来创建集群，然后将从属设备添加到该集群。

备注　对于主设备，如果您要更改 cLACP 系统 ID 和优先级的默认值，则不能使用此向导；必须手动配置集群。

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。如果您尚未进入系统配置模式，请在 Configuration > Device List 窗格中双击主用设备 IP 地址下的 **System**。
- 我们建议将集群控制链路 MTU 设置为 1600 字节或更大值，这需要*在每台设备上*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。
- 在连接的交换机上，意图用于集群控制链路接口的接口必须处于运行状态。
- 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　依次选择 **Wizards > High Availability and Scalability Wizard**。请参阅以下步骤中有关选择向导的指引。

步骤 2　在 **Interfaces** 屏幕中，您无法从此屏幕创建新的 EtherChannel （集群控制链路除外）。

步骤 3　在 ASA Cluster Configuration 屏幕中，配置引导程序设置，包括：

- **Member Priority** - 设置此设备用于主设备选举的优先级，其值为 1 到 100，其中 1 为最高优先级。
- （可选）**Shared Key** - 设置加密密钥以便控制集群控制链路上的流量。共享密钥是长度为 1 到 63 个字符的 ASCII 字符串。共享密钥用于生成加密密钥。此参数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。如果您还启用了密码加密服务，则必须配置此参数。
- （可选）**Enable connection rebalancing for TCP traffic across all the ASAs in the cluster** - 启用连接再均衡。默认情况下，此参数处于禁用状态。如果已启用，集群中的 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。此参数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。

注意　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。

- （可选）**Enable health monitoring of this device within the cluster** - 启用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。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。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。如果设备在保持时间内没有收到接口状态消息，则 ASA 从集群中删除成员之前所经过的时间取决于接口类型以及设备是已建立的成员还是正在加入集群。默认情况下，为所有接口启用运行状况检查。您可以选择稍后按接口禁用。

注意　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），您必须禁用运行状况检查。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。

  - **Time to Wait Before Device Considered Failed** - 此值用于确定设备 keepalive 状态消息的间隔时间，可设置为 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）。
  - （可选） **Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support** - 如果将集群控制链路配置为 EtherChannel （推荐），而且链路连接到 VSS 或 vPC 对，则您可能需要启用此选项。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。当您启用此选项时， 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。

- （可选） **Replicate console output to the master’ s console** - 启用从属设备到主设备的控制台复制。默认情况下，此功能处于禁用状态。对于特定的重要事件， ASA 可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。此参数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。
- **Cluster Control Link** - 指定集群控制链路接口。
  - （可选）**MTU** - 为集群控制链路接口指定最大传输单位，其值为 64 到 65,535 字节。大于 MTU 值的数据将分片后再发送。默认 MTU 为 1500 字节。如果已启用巨型帧保留，我们建议将 MTU 设置为 1600 字节或更大值。如果您要使用巨型帧又没有预先启用巨型帧保留，则应先退出向导，启用巨型帧后再重新开始本程序。

步骤 4　单击 **Finish**。

步骤 5　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。点击 **OK** 删除不兼容的命令。如果点击 **Cancel**，则不会启用集群。

步骤 6　经过一段时间后，当 ASDM 启用集群并重新连接到 ASA 时，系统将显示 Information 屏幕，确认 ASA 已添加到集群。

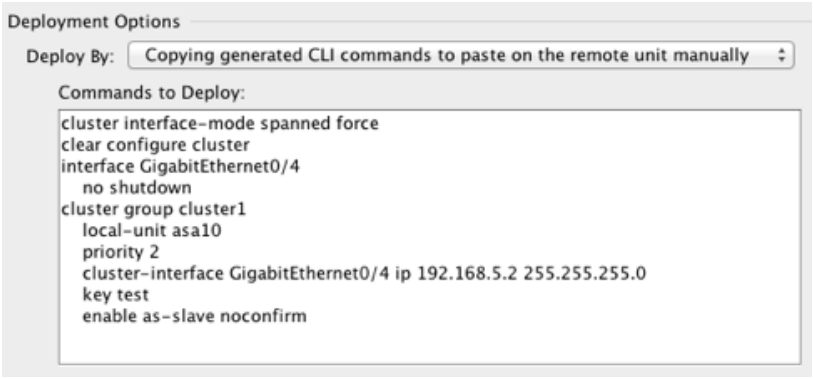
注意　在某些情况下，完成向导后加入集群时可能会出现错误。如果 ASDM 断开连接， ASDM 不会收到来自 ASA 的任何后续错误。如果重新连接 ASDM 后集群仍被禁用，应连接到 ASA 控制台端口来确定禁用集群的具体错误情况；例如，集群控制链路可能关闭。

步骤 7　要添加从属设备，请点击 **Yes**。

如果您从主设备重新运行向导，可以在首次启动向导时选择 **Add another member to the cluster** 选项来添加从属设备。

步骤 8　在 **Deployment Options** 区域，从以下 **Deploy By** 选项中选择一个选项：

- **Sending CLI commands to the remote unit now** - 将引导程序配置发送到从属设备的 （临时）管理 IP 地址。输入从属设备管理 IP 地址、用户名和密码。
- **Copying generated CLI commands to paste on the remote unit manually** - 生成命令，以便剪切并粘贴到从属设备 CLI 中或在 ASDM 中使用 CLI 工具。在 Commands to Deploy 复选框中，选择并复制生成的命令供稍后使用。



相关主题

- 配置 ASA 集群参数，第 10-46 页
- 启用巨帧支持，第 11-7 页
- 配置跨网络 EtherChannel，第 10-40 页
- 配置独立接口 （管理接口的推荐配置），第 10-38 页
- 接口监控，第 10-8 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。

- 配置 ASA 集群参数，第 10-46 页
- 从主设备添加新的从属设备，第 10-48 页
- 成为非活动成员，第 10-49 页
- 从主设备停用从属设备成员，第 10-50 页
- 退出集群，第 10-51 页

- 更改主设备，第 10-52 页
- 在集群范围内执行命令，第 10-52 页

配置 ASA 集群参数

如果您不使用向导来将设备添加到集群，可以手动配置集群参数。如果已启用集群，则可以编辑某些集群参数；启用集群时无法编辑的其他参数将灰显。本程序还包括向导中没有的高级参数。

准备工作

- 加入集群之前，在每台设备上预配置集群控制链路接口。如果是单个接口，您必须将其启用；不要配置其他设置。如果是 EtherChannel 接口，请启用该接口并将 EtherChannel 模式设置为 On。
- 对于多情景模式，请在系统执行空间中执行本程序。如果您尚未进入系统配置模式，请在 **Configuration > Device List** 窗格中双击主用设备 IP 地址下的 **System**。

操作步骤

步骤 1　依次选择 **Configuration > Device Management > High Availability and Scalability > ASA Cluster**。

如果设备已经在集群中并且是主设备，则此窗格位于 Cluster Configuration 选项卡中。

步骤 2　选中 **Configure ASA cluster settings** 复选框。

如果取消选中此复选框，设置将被擦除。在设置完所有参数之前，请勿选中 **Participate in ASA cluster**。

注意　启用集群后，请勿在不了解后果的情况下取消选中 **Configure ASA cluster settings** 复选框。此操作会清除所有集群配置并关闭所有接口，包括 ASDM 连接到的管理接口。在此情况下，要恢复连接，您需要在控制台端口上访问 CLI。

步骤 3　配置以下引导程序参数：

- **Cluster Name** - 为集群命名。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。集群的所有成员必须使用同一名称。
- **Member Name** - 使用唯一的 ASCII 字符串为此集群成员命名，长度必须为 1 到 38 个字符。
- **Member Priority** - 设置此设备用于主设备选举的优先级，其值为 1 到 100，其中 1 为最高优先级。
- （可选）**Shared Key** - 设置加密密钥以便控制集群控制链路上的流量。共享密钥是长度为 1 到 63 个字符的 ASCII 字符串。共享密钥用于生成加密密钥。此参数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。如果您还启用了密码加密服务，则必须配置此参数。
- （可选）**Enable connection rebalancing for TCP traffic across all the ASAs in the cluster** - 启用连接再均衡。默认情况下，此参数处于禁用状态。如果已启用，集群中的 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。此参数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。
- （可选）**Enable health monitoring of this device within the cluster** - 启用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。**注意**：将新设备添加到集群并在 ASA 或交换机上进行拓扑结构更改时，您应临时禁用此功能，直到集群完成。您可以在集群

和拓扑更改完成之后重新启用此功能。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。接口状态消息将检测链路故障。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。如果设备在保持时间内没有收到接口状态消息，则 ASA 从集群中删除成员之前所经过的时间取决于接口类型以及设备是已建立的成员还是正在加入集群。默认情况下，为所有接口启用运行状况检查。您可以在 **Cluster Interface Health Monitoring** 选项卡上选择按接口禁用此功能。

注意　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），您必须禁用运行状况检查。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。

  - （可选） **Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support** - 如果将集群控制链路配置为 EtherChannel （推荐），而且链路连接到 VSS 或 vPC 对，则您可能需要启用此选项。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。当您启用此选项时， 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。

- （可选） **Replicate console output to the master’ s console** - 启用从属设备到主设备的控制台复制。默认情况下，此功能处于禁用状态。对于特定的重要事件， ASA 可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。此参数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。
- **Cluster Control Link** - 指定集群控制链路接口。此接口不能配置名称；可用接口显示于下拉列表中。
  - **Interface** - 指定接口 ID，最好是 EtherChannel。不允许指定子接口和管理类型的接口。
  - **IP Address** - 指定 IPv4 地址作为 IP 地址；此接口不支持 IPv6。
  - **Subnet Mask** - 指定子网掩码。
  - （可选）**MTU** - 为集群控制链路接口指定最大传输单位，其值为 64 到 65,535 字节。大于 MTU 值的数据将分片后再发送。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。
- （可选） **Cluster LACP** - 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。
  - **Enable static port priority** - 禁用 LACP 中的动态端口优先级。某些交换机不支持动态端口优先级，所以此参数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。如果不使用此参数，则只能支持 8 个活动成员和 8 个备用成员。如果启用此参数，则无法使用任何备用成员；所有成员都是活动成员。此参数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。
  - **Virtual System MAC Address** - 设置 MAC 地址格式的 cLACP 系统 ID。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 00-0C-F1-42-4C-DE 以 000C.F142.4CDE 的形式输入。此参数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。

– **System Priority** - 设置系统优先级，其值为 1 到 65535。优先级用于决定哪台设备负责做出捆绑决策。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。此参数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 4　选中 **Participate in ASA cluster** 复选框加入集群。

步骤 5　（可选）点击 **Cluster Interface Health Monitoring** 选项卡，在一个或多个接口上禁用运行状况监控。在 **Monitored Interfaces** 对话框中选择一个接口，然后点击 **Add**，将其移动到 **Unmonitored Interfaces** 对话框中。

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。您可以监控任何端口通道 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 6　点击 **Apply**。

相关主题

- 接口监控，第 10-8 页
- 启用巨帧支持，第 11-7 页

从主设备添加新的从属设备

您可以从主设备将更多从属设备添加到集群，也可以使用 High Availability and Scalability 向导添加从属设备。从主设备添加从属设备的优势在于，您可以配置集群控制链路并设置要添加的每台从属设备上的集群接口模式。

或者，您也可以选择登录到从属设备并直接在该设备上配置集群。但是在启用集群后， ASDM 会话将断开连接，您必须重新连接。

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。如果您尚未进入系统配置模式，请在 Configuration > Device List 窗格中双击主用设备 IP 地址下的 **System**。
- 如果您要通过管理网络发送引导程序配置，请确保从属设备具有可访问的 IP 地址。

操作步骤

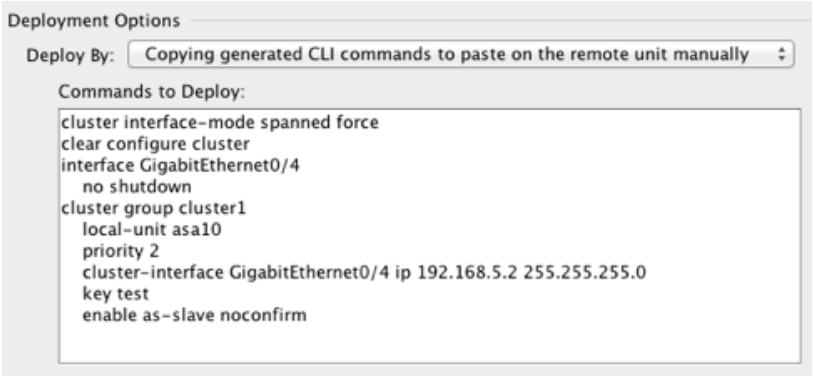
步骤 1　依次选择 **Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Members**。

步骤 2　点击**添加**。

步骤 3　配置以下参数：

- **Member Name** - 使用唯一的 ASCII 字符串为此集群成员命名，长度必须为 1 到 38 个字符。
- **Member Priority** - 设置此设备用于主设备选举的优先级，其值为 1 到 100，其中 1 为最高优先级。
- **Cluster Control Link > IP Address** - 为此成员指定唯一的集群控制链路 IP 地址，其必须与主设备集群控制链路位于同一个网络中。

- 在 **Deployment Options** 区域，从以下 **Deploy By** 选项中选择一个选项：
  - **Sending CLI commands to the remote unit now** - 将引导程序配置发送到从属设备的 （临时）管理 IP 地址。输入从属设备管理 IP 地址、用户名和密码。
  - **Copying generated CLI commands to paste on the remote unit manually** - 生成命令，以便剪切并粘贴到从属设备 CLI 中或在 ASDM 中使用 CLI 工具。在 Commands to Deploy 复选框中，选择并复制生成的命令供稍后使用。



步骤 4　点击 **OK**，然后点击 **Apply**。

相关主题

- 配置 ASA 集群参数，第 10-46 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

- 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，在 Configuration > Device List 窗格中双击主用设备 IP 地址下的 **System**。

操作步骤

步骤 1　依次选择 **Configuration > Device Management > High Availability and Scalability > ASA Cluster**。

如果设备已经在集群中并且是主设备，则此窗格位于 Cluster Configuration 选项卡中。

步骤 2　取消选中 **Participate in ASA cluster** 复选框。

注意　请勿取消选中 **Configure ASA cluster settings** 复选框，此操作会清除所有集群配置并关闭所有接口，包括 ASDM 连接到的管理接口。在此情况下，要恢复连接，您需要在控制台端口上访问 CLI。

步骤 3　点击 **Apply**。

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 10-51 页

从主设备停用从属设备成员

要停用从属设备成员，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，在 Configuration > Device List 窗格中双击主用设备 IP 地址下的 **System**。

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。

步骤 1　依次选择 **Configuration > Device Management > High Availability and Scalability > ASA Cluster**。

步骤 2　选择要删除的从属设备，然后点击 **Delete**。

从属设备的引导程序配置保持不变，因此您可于稍后重新添加该从属设备而不会丢失配置。

步骤 3　点击 **Apply**。

相关主题

- 退出集群，第 10-51 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。

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，在 Configuration > Device List 窗格中双击主用设备 IP 地址下的 **System**。

操作步骤

步骤 1　依次选择 **Monitoring > ASA Cluster > Cluster Summary**。

步骤 2　从 **Change Master To** 下拉列表中，选择要成为主设备的从属设备，然后点击 **Make Master**。

步骤 3　系统将提示您确认主设备更改。点击 **Yes**。

步骤 4　退出 ASDM，然后使用主集群 IP 地址重新连接。

相关主题

- 成为非活动成员，第 10-49 页
- 集群的集中功能，第 10-23 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。

准备工作

在命令行界面工具中执行本程序：依次选择 **Tools > Command Line Interface**。

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：

```
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：

```
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：

```
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

请参阅以下用于监控集群状态的屏幕：

- **Monitoring > ASA Cluster > Cluster Summary**

  此窗格显示有关要连接的设备以及集群中其他设备的集群信息。您还可以在此窗格中更改主设备。

- **集群控制面板**

  在主设备的主页上，您可以使用集群控制面板和集群防火墙控制面板监控集群。

相关主题

- Cluster Dashboard 选项卡，第 3-21 页
- Cluster Firewall Dashboard 选项卡，第 3-22 页

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屏幕：

Wizards > Packet Capture Wizard

要支持集群范围的故障排除，您可以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

- 使用 Packet Capture Wizard 配置和运行捕获，第 37-1 页

监控集群资源

请参阅以下用于监控集群资源的屏幕：

- **Monitoring > ASA Cluster > System Resources Graphs > CPU**

  此窗格可用于创建显示所有集群成员 CPU 使用率的图或表。

- **Monitoring > ASA Cluster > System Resources Graphs > Memory**。此窗格可用于创建显示所有集群成员可用内存和已用内存的图或表。

监控集群流量

请参阅以下用于监控集群流量的屏幕：

- **Monitoring > ASA Cluster > Traffic Graphs > Connections**。

  此窗格可用于创建显示所有集群成员连接的图或表。

- **Monitoring > ASA Cluster > Traffic Graphs > Throughput**。

  此窗格可用于创建显示所有集群成员流量吞吐量的图或表。

监控集群控制链路

请参阅以下用于监控集群状态的屏幕：

Monitoring > Properties > System Resources Graphs > Cluster Control Link。

此窗格可用于创建显示集群控制链路接收和传送容量使用率的图或表。

配置集群日志记录

请参阅以下用于配置集群日志记录的屏幕：

Configuration > Device Management > Logging > Syslog Setup

集群中的每台设备将独立生成系统日志消息。您可以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 38-19 页

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 10-55 页
- 单臂防火墙，第 10-58 页
- 流量分离，第 10-60 页
- 包含备用链路 （传统的 8 主用/8 备用）的跨网络 EtherChannel，第 10-62 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 10-55 页
- 思科 IOS 交换机配置，第 10-57 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

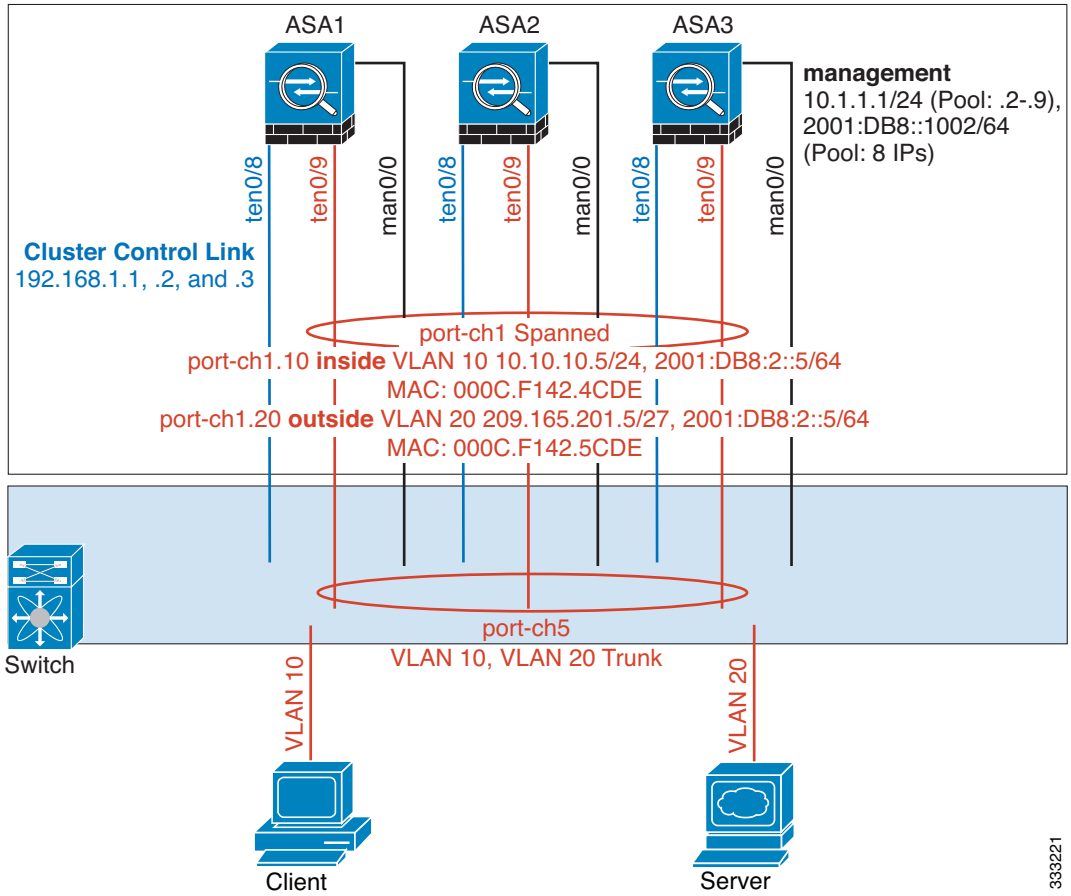
```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

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
```

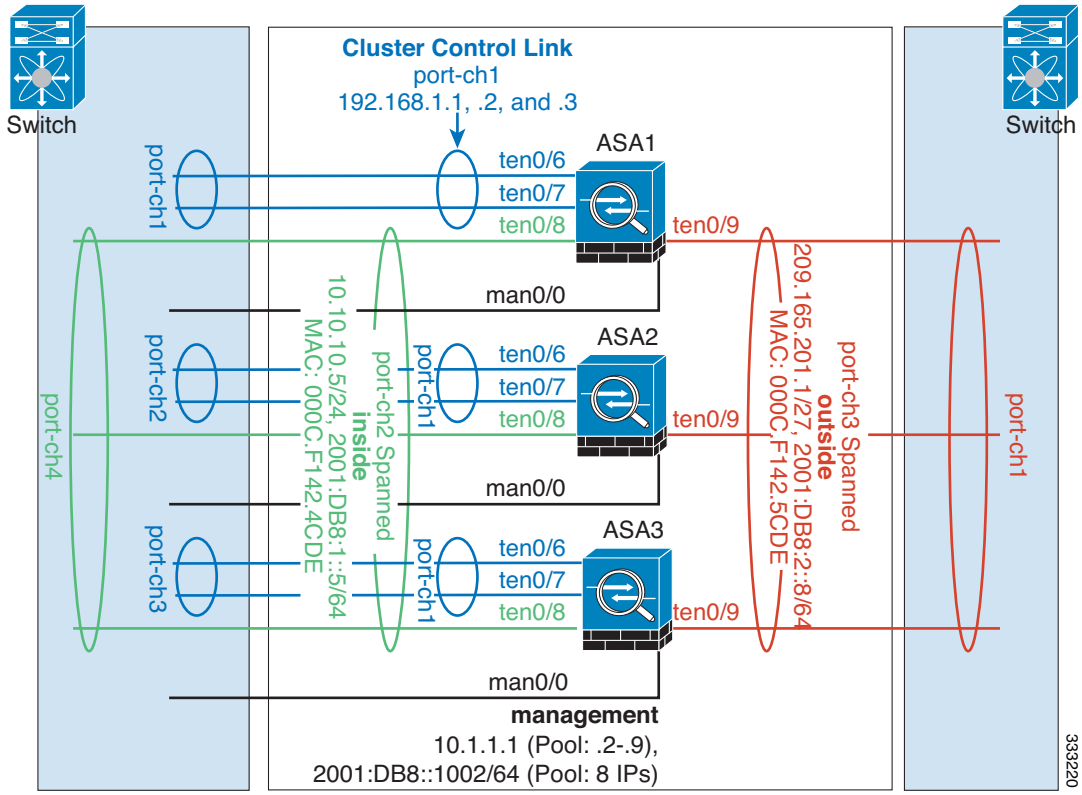
ASA3 从属设备引导程序配置

```
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
```

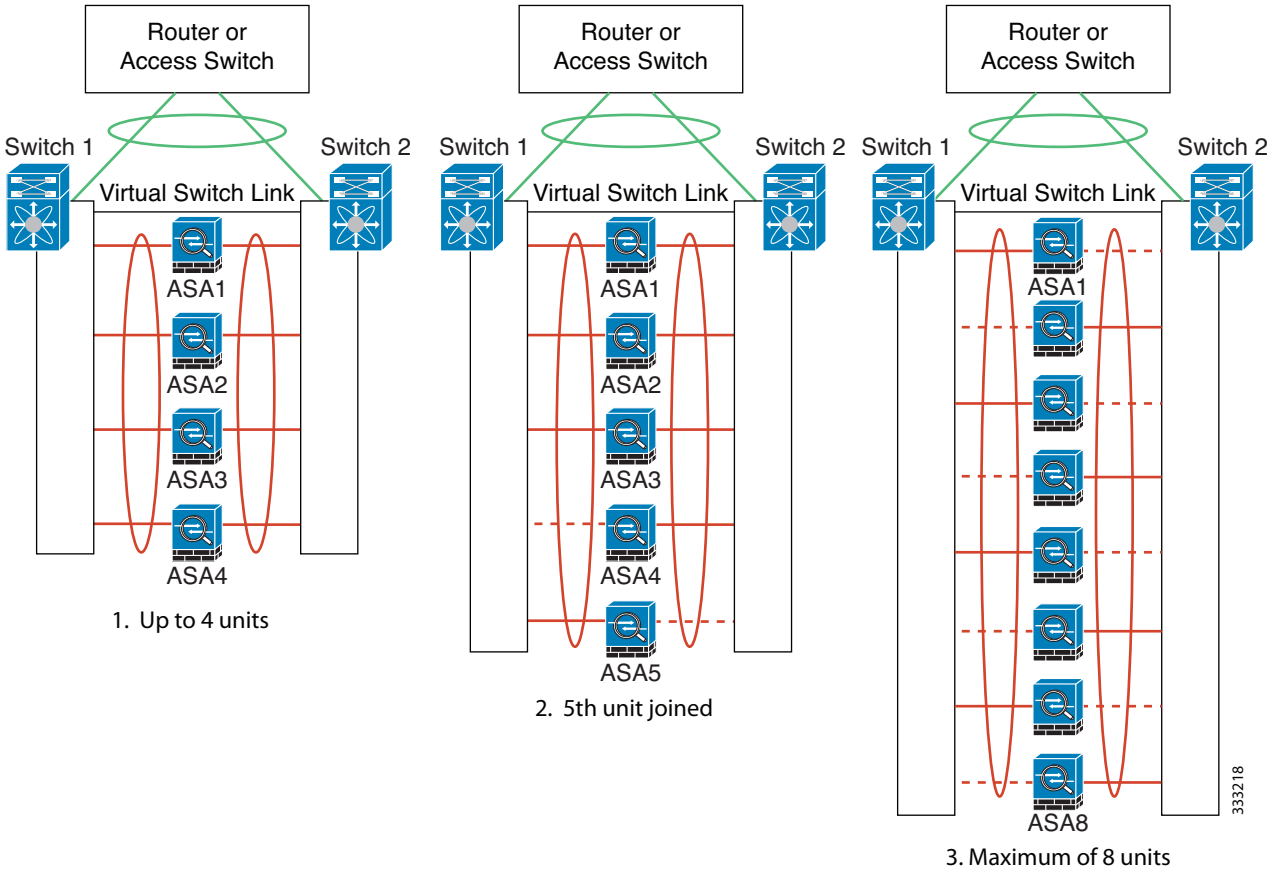
主设备接口配置

```
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
```

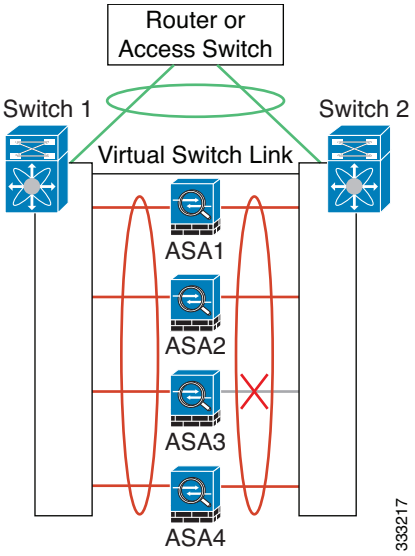
包含备用链路 （传统的 8 主用/8 备用）的跨网络 EtherChannel

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：

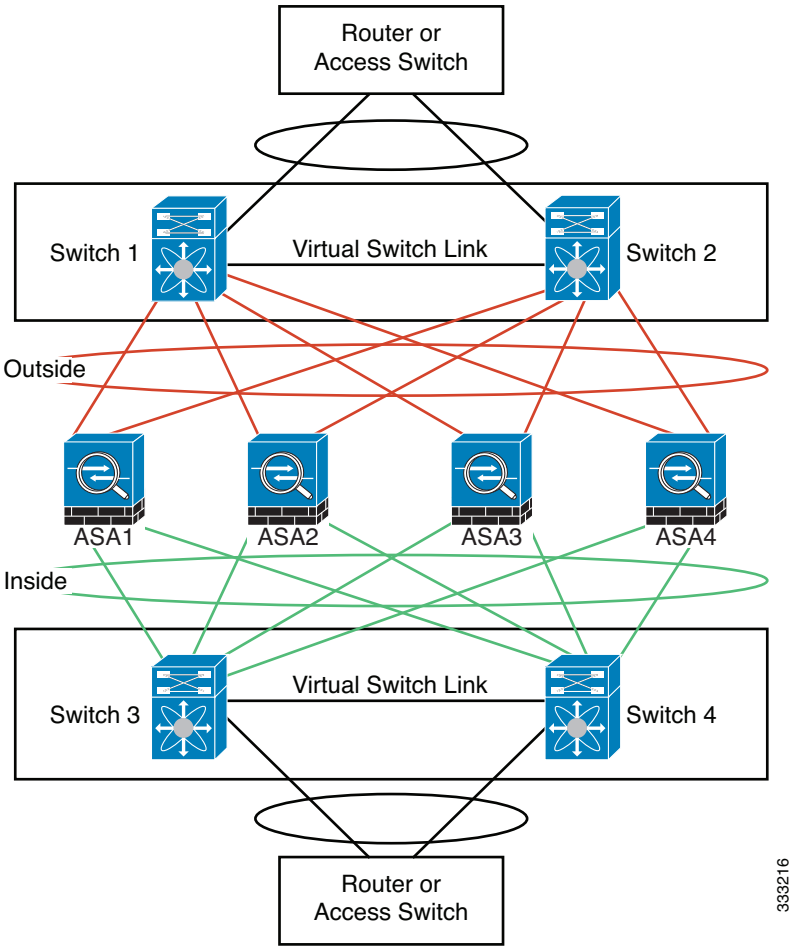


此时的处理原则是，首先将通道中的活动端口数增加到最大值，其次是保持活动的主端口数与活动的辅助端口数之间的均衡。请注意，当第 5 台设备加入集群时，流量并未在所有设备之间达到均衡。

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。 引入或修改了以下屏幕： Home > Device Dashboard Home > Cluster Dashboard Home > Cluster Firewall Dashboard Configuration > Device Management > Advanced > Address Pools > MAC Address Pools Configuration > Device Management > High Availability and Scalability > ASA Cluster Configuration > Device Management > Logging > Syslog Setup > Advanced Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface > Advanced Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface > IPv6 Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit EtherChannel Interface > Advanced Configuration > Firewall > Advanced > Per-Session NAT Rules Monitoring > ASA Cluster Monitoring > Properties > System Resources Graphs > Cluster Control Link Tools > Preferences > General Tools > System Reload Tools > Upgrade Software from Local Computer Wizards > High Availability and Scalability Wizard Wizards > Packet Capture Wizard Wizards > Startup Wizard
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 ASDM 屏幕。
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。 修改了以下屏幕：**Configuration > Device Management > High Availability and Scalability > ASA Cluster**

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 ASDM 屏幕。
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 ASDM 屏幕。
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。 修改了以下屏幕：**Configuration > Device Management > High Availability and Scalability > ASA Cluster**
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。 修改了以下屏幕：**Configuration > Device Management > High Availability and Scalability > ASA Cluster**
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。 未修改任何屏幕。
BGP 对 ASA 集群的支持	9.3(1)	增加了对 BGP 用于 ASA 集群的支持。 修改了以下屏幕：**Configuration > Device Setup > Routing > BGP > IPv4 Family > General**
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。 引入了以下屏幕：**Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Interface Health Monitoring**
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。 未修改任何屏幕。
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。 未修改任何屏幕。

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。如果您尚未处于系统执行空间中，请在 Configuration > Device List 窗格中双击主用设备 IP 地址下的 **System**。

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

本节介绍接口功能与特殊接口。

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

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 34 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 11-1　　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。

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**均根据此限制进行计数。

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。如果您尚未处于系统配置模式下，请在 Configuration > Device List 窗格中双击主用设备 IP 地址下的 **System**。

操作步骤

步骤 1　视情景模式而定：

- 对于单情景模式，请依次选择 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中依次选择 **Configuration > Context Management > Interfaces** 窗格。

默认情况下，所有物理接口均已列出。

步骤 2　点击要配置的物理接口，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框。

注意　在单模式下，此程序仅涉及 **Edit Interface** 对话框中的一部分参数。请注意，在多情景模式下，完成接口配置之前，您需要将接口分配到情景。

步骤 3　要启用接口，请选中 **Enable Interface** 复选框。

步骤 4　要添加说明，请在 Description 字段中输入文本。

一行说明最多可包含 240 个字符 （不包括回车符）。例如，对于故障切换或状态链路，说明固定为“LAN Failover Interface”、“STATE Failover Interface”或“LAN/STATE Failover Interface”。您无法编辑此说明。如果将此接口设为故障切换或状态链路，则固定说明将覆盖在此处输入的任何说明。

步骤 5　（可选）要设置媒体类型、双工、速度并为流量控制启用暂停帧，请点击 **Configure Hardware Properties**。

a. 您可以从 **Media Type** 下拉列表中选择 **RJ-45** 或 **SFP** （具体取决于接口类型）。

   RJ-45 是默认接口。

b. 要设置 RJ-45 接口的双工，请从 **Duplex** 下拉列表中选择 **Full**、 **Half** 或 **Auto** （具体取决于接口类型）。

   注意　EtherChannel 接口的双工设置必须为 **Full** 或 **Auto**。

c. 要设置速度，请从 **Speed** 下拉列表中选择一个值。

   可用速度因接口类型而异。对于 SFP 接口，您可以将速度设置为 **Negotiate** 或 **Nonegotiate**。**Negotiate**（默认设置）启用链路协商，从而交换流量控制参数和远程故障信息。**Nonegotiate** 不会协商链路参数。对于 RJ-45 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。

d. 要在千兆以太网接口和 10 千兆以太网接口上启用暂停 (XOFF) 帧，请选中 **Enable Pause Frame** 复选框。

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。

要更改 Low Watermark、 High Watermark 和 Pause Time 的默认值，请取消选中 **Use Default Values** 复选框。

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。

e. 点击 **OK** 接受 **Hardware Properties** 更改。

步骤 6　点击 **OK** 接受 **Interface** 更改。

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，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，或者根据 MTU 增加 TCP MSS 的值。

操作步骤

步骤 1　视情景模式而定：

- 多模式 - 要启用巨帧支持，请依次选择 **Configuration > Context Management > Interfaces**，然后点击 **Enable jumbo frame support** 复选框。
- 单模式 - 将 MTU 设置为大于 1500 字节将会自动启用巨帧。要手动启用或禁用此设置，请依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**，然后点击 **Enable jumbo frame support** 复选框。

相关主题

- 关于高级接口配置，第 16-1 页
- 配置 MAC 地址、MTU 和 TCP MSS，第 16-5 页

基本接口示例

请参阅以下配置示例。

- 物理接口参数示例，第 11-8 页
- 多情景模式示例，第 11-8 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 11-2　　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。

表 11-2　　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。 修改了以下屏幕：Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface > Advanced。
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。 修改了以下屏幕： （单情景模式） Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface > General （多情景模式，系统） Configuration > Interfaces > Add/Edit Interface。
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。 修改了以下屏幕： （单情景模式） Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface > General （多情景模式，系统） Configuration > Interfaces > Add/Edit Interface。

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。如果您尚未处于系统执行空间中，请在 Configuration > Device List 窗格中双击主用设备 IP 地址下的 **System**。

备注 有关具有特殊要求的 ASA 集群接口，请参阅第 10 章 “ASA 集群”。

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

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 MAC 地址、MTU 和 TCP MSS，第 16-5 页
- 配置多情景，第 8-14 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 12-2 页
- 连接到另一台设备上的 EtherChannel，第 12-2 页
- 链路汇聚控制协议，第 12-3 页
- 负载均衡，第 12-4 页
- EtherChannel MAC 地址，第 12-4 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。

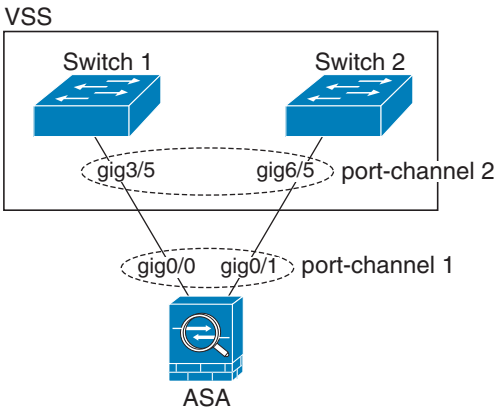
EtherChannel 汇聚通道中所有可用活动接口上的流量。系统根据源或目标 MAC 地址、 IP 地址、 TCP 端口号、 UDP 端口号和 VLAN 编号使用专有散列算法来选择接口。

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。

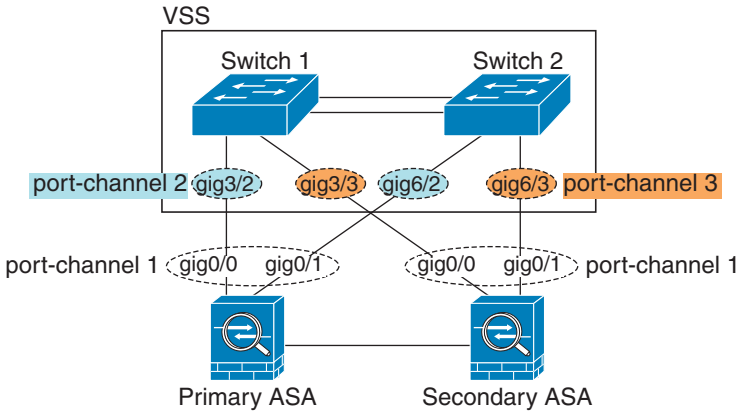
如果交换机属于虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 的一部分，则可以将同一 EtherChannel 内的 ASA 接口连接到 VSS/vPC 中的单独交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台单独的交换机的行为就像一台交换机一样。

图 12-1　　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 12-2　　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 12-10 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。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

- 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 12-6 页
- 更改主用接口，第 12-8 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** 窗格中删除该名称。
- 对于多情景模式，请在系统执行空间中完成本程序。如果您尚未处于系统配置模式下，请在 **Configuration > Device List** 窗格中双击主用设备 IP 地址下的 **System**。

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　视情景模式而定：

- 对于单情景模式，请依次选择 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中依次选择 **Configuration > Context Management > Interfaces** 窗格。

步骤 2　依次选择 **Add > Redundant Interface**。

系统将显示 **Add Redundant Interface** 对话框。

注意　在单情景模式下，此程序仅涉及 Edit Redundant Interface 对话框中的一部分参数；要配置其他参数，请参阅第 15 章 “路由模式和透明模式接口”。请注意，在多情景模式下，您需要在完成接口配置之前将接口分配给情景。请参阅配置多情景，第 8-14 页。

步骤 3　在 **Redundant ID** 字段中，请输入一个介于 1 和 8 之间的整数。

步骤 4　从 **Primary Interface** 下拉列表中，选择要设置为主接口的物理接口。

请务必选择没有子接口且尚未分配给情景的接口。冗余接口不支持管理*插槽/端口*接口作为成员。

步骤 5　从 **Secondary Interface** 下拉列表中，选择要设置为辅助接口的物理接口。

步骤 6　如果该接口尚未启用，请选中 **Enable Interface** 复选框。

默认情况下，该接口已启用。

步骤 7　要添加说明，请在 **Description** 字段中输入文本。

一行说明最多可包含 240 个字符 （不包括回车符）。对于多情景模式，系统说明与情景说明无关。例如，对于故障切换或状态链路，说明固定为 “LAN Failover Interface”、“STATE Failover Interface”或 “LAN/STATE Failover Interface”。您无法编辑此说明。如果将此接口设为故障切换或状态链路，则固定说明将覆盖在此处输入的任何说明。

步骤 8　点击 **OK**。

系统将返回到 **Interfaces** 窗格。现在，成员接口在接口 ID 左侧显示锁形图标，表明只能为其配置基本参数。冗余接口已添加到该表中。

GigabitEthernet0/2	Enabled	No	Redundant8	Hardware	native
GigabitEthernet0/3	Enabled	No		Hardware	native
GigabitEthernet0/3.10	Enabled	No		Logical	vlan100
GigabitEthernet0/3.11	Enabled	No		Logical	vlan11
Management0/0	Enabled	No		Hardware	native
Redundant8	Enabled	Yes		Logical	native

254710

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，请在 **Tools > Command Line Interface** 工具中输入以下命令：

```
show interface redundantnumber detail | grep Member
```

示例：

```
show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

步骤 2　更改主用接口：

```
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 12-8 页
- 自定义 EtherChannel，第 12-10 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** 窗格中删除该名称。
- 对于多情景模式，请在系统执行空间中完成本程序。如果您尚未处于系统配置模式下，请在 **Configuration > Device List** 窗格中双击主用设备 IP 地址下的 **System**。

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　视情景模式而定：

- 对于单情景模式，请依次选择 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中依次选择 **Configuration > Context Management > Interfaces** 窗格。

步骤 2　依次选择 **Add > EtherChannel Interface**。

系统将显示 **Add EtherChannel Interface** 对话框。

注意　在单情景模式下，此程序仅涉及 Edit Interface 对话框中的一部分参数；要配置其他参数，请参阅第 15 章 “路由模式和透明模式接口”。请注意，在多情景模式下，您需要在完成接口配置之前将接口分配给情景。请参阅配置多情景，第 8-14 页。

步骤 3　在 **Port Channel ID** 字段中，输入介于 1 和 48 之间的数字。

步骤 4　在 *Available Physical Interface* 区域中，点击一个接口，然后点击 **Add >>** 以将其移至 **Members in Group** 区域。

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。

注意　如果要将 EtherChannel 模式设置为 On，则最初必须仅包含一个接口。完成此程序后，编辑成员接口，并将模式设置为 **On**。应用更改，然后编辑 EtherChannel 以添加更多成员接口。

步骤 5　为要添加到通道组中的每个接口重复上述步骤。

确保所有接口的类型和速度相同。添加的第一个接口决定了 EtherChannel 的类型和速度。您添加的任何不匹配接口都将被置于暂停状态。ASDM 不会阻止您添加不匹配的接口。

步骤 6　点击 **OK**。

系统将返回到 **Interfaces** 窗格。现在，成员接口在接口 ID 左侧显示锁形图标，表明只能为其配置基本参数。EtherChannel 接口已添加到该表中。

步骤 7　点击 **Apply**。所有成员接口都自动启用。

相关主题

- 链路汇聚控制协议，第 12-3 页
- 自定义 EtherChannel，第 12-10 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　视情景模式而定：

- 对于单情景模式，请依次选择 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中依次选择 **Configuration > Context Management > Interfaces** 窗格。

步骤 2　点击要自定义的端口通道接口，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框。

步骤 3　要覆盖媒体类型、双工、速度和暂停帧以对所有成员接口进行流量控制，请点击 **Configure Hardware Properties**。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 4　要自定义 EtherChannel，请点击 **Advanced** 选项卡。

a. 在 **EtherChannel** 区域中，从 **Minimum** 下拉列表中选择使 EtherChannel 成为主用接口所需的最小主用接口数 （介于 1 和 16 之间）。默认值为 1。

b. 从 **Maximum** 下拉列表中，选择 EtherChannel 中允许的最大主用接口数 （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。

c. 从 **Load Balance** 下拉列表中，选择在组通道接口之间对数据包进行负载均衡所用的标准。默认情况下， ASA 根据数据包的源 IP 地址和目标 IP 地址来均衡接口上的数据包负载。如果要更改分类数据包所依据的属性，请选择另一组条件。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。有关负载均衡的详细信息，请参阅负载均衡，第 12-4 页。

步骤 5　点击 **OK**。

系统将返回到 **Interfaces** 窗格。

步骤 6　要在通道组中设置物理接口的模式和优先级，请执行以下操作：

a. 点击 **Interfaces** 表中的物理接口，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框。

b. 点击 **Advanced** 选项卡。

c. 在 **EtherChannel** 区域中，从 **Mode** 下拉列表中选择 **Active**、 **Passive** 或 **On**。我们建议使用 Active 模式 （默认）。

d. 在 **LACP Port Priority** 字段中，设置介于 1 和 65535 之间的端口优先级。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 接口上将优先级值设置为 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。要设置系统优先级，请参阅步骤 9。

步骤 7　点击 **OK**。

系统将返回到 **Interfaces** 窗格。

步骤 8　点击 **Apply**。

步骤 9　要设置 LACP 系统优先级，请执行以下步骤。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。有关详细信息，请参阅步骤 6d。

a. 视情景模式而定：

- 对于单情景模式，请依次选择 **Configuration > Device Setup > EtherChannel** 窗格。
- 对于多情景模式，请在系统执行空间中依次选择 **Configuration > Context Management > EtherChannel** 窗格。

b. 在 **LACP System Priority** 字段中，输入介于 1 和 65535 之间的优先级值。

默认值为 32768。

相关主题

- 负载均衡，第 12-4 页
- 将接口添加到 EtherChannel，第 12-8 页

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 12-1　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。 修改或引入了以下屏幕： Configuration > Device Setup > Interface Settings > Interfaces Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit EtherChannel Interface Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface Configuration > Device Setup > EtherChannel **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。 修改了以下屏幕：Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit EtherChannel Interface > Advanced。

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。如果您尚未处于系统执行空间中，请在 Configuration > Device List 窗格中双击主用设备 IP 地址下的 **System**。

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
ASA 5512-X	基础许可证：50 增强型安全许可证：100

型号	许可证要求
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。

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，请通过不为接口配置名称来确保物理接口、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 name。
- （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。如果您尚未处于系统配置模式下，请在 **Configuration > Device List** 窗格中双击主用设备 IP 地址下的 **System**。

操作步骤

步骤 1　视情景模式而定：

- 对于单情景模式，请依次选择 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中依次选择 **Configuration > Context Management > Interfaces** 窗格。

步骤 2　依次选择 **Add > Interface**。

系统将显示 **Add Interface** 对话框。

注意　在单模式下，此程序仅涉及 Edit Interface 对话框中的一部分参数；要配置其他参数，请参阅第 15 章 “路由模式和透明模式接口”。请注意，在多情景模式下，您需要在完成接口配置之前将接口分配给情景。请参阅配置多情景，第 8-14 页。

步骤 3　从 **Hardware Port** 下拉列表中，选择要添加子接口的物理接口、冗余接口或端口通道接口。

步骤 4　如果该接口尚未启用，请选中 **Enable Interface** 复选框。

默认情况下，该接口已启用。

步骤 5　在 **VLAN ID** 字段中，输入介于 1 和 4095 之间的 VLAN ID。

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。对于多情景模式，您只能在系统配置中设置 VLAN。

步骤 6　在 **Subinterface ID** 字段中，输入子接口 ID （介于 1 和 4294967293 之间的整数）。

允许的子接口数因平台而异。此 ID 一旦设置便不可更改。

步骤 7　（可选）在 **Description** 字段中，输入此接口的说明。

一行说明最多可包含 240 个字符 （不包括回车符）。对于多情景模式，系统说明与情景说明无关。例如，对于故障切换或状态链路，说明固定为 “LAN Failover Interface”、“STATE Failover Interface”或 “LAN/STATE Failover Interface”。您无法编辑此说明。如果将此接口设为故障切换或状态链路，则固定说明将覆盖在此处输入的任何说明。

步骤 8　点击 **OK**。

系统将返回到 **Interfaces** 窗格。

相关主题

- VLAN 接口许可，第 13-1 页

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 13-1　　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

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。

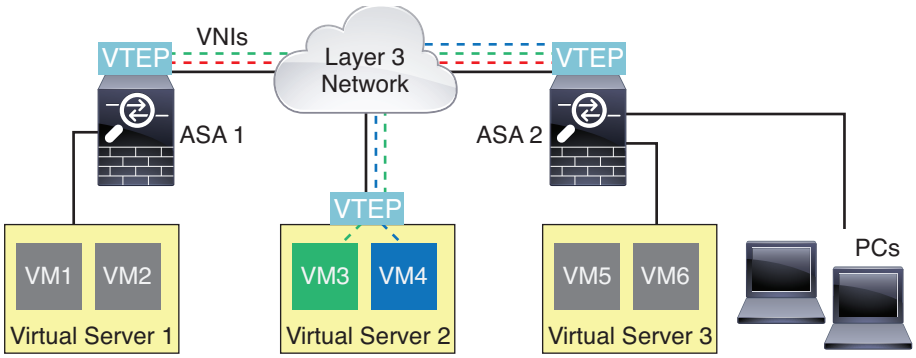
VXLAN 封装

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

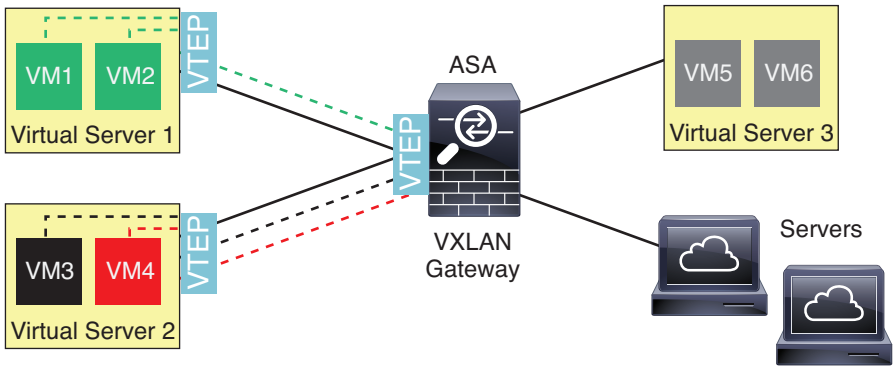
本节介绍在 ASA 上实施 VXLAN 的使用案例。

- VXLAN 网桥或网关概述，第 14-3 页
- VXLAN 网桥 （透明模式），第 14-4 页
- VXLAN 网关 （路由模式），第 14-4 页
- VXLAN 域之间的路由器，第 14-5 页

VXLAN 网桥或网关概述

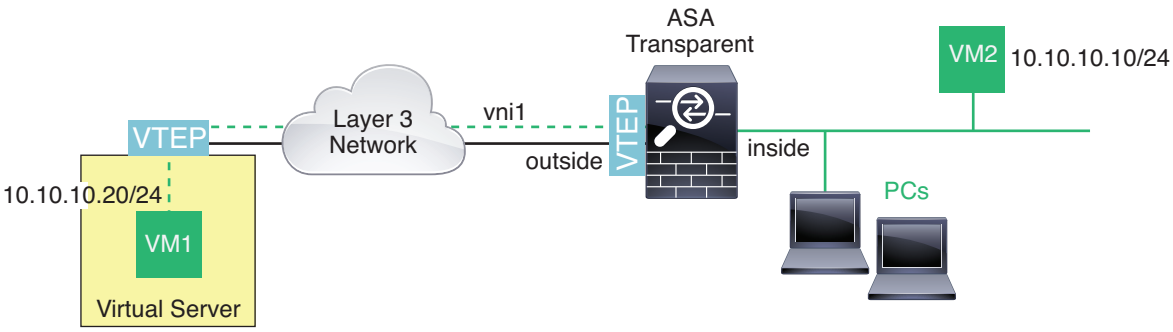
每个 ASA VTEP 都可作为终端节点 （例如 VM、服务器和 PC）和 VXLAN 重叠网络之间的网桥或网关。对于通过 VTEP 源接口借助 VXLAN 封装接收的传入帧，ASA 去掉 VXLAN 报头，并基于内部以太网帧的目标 MAC 地址，将传入帧转发到连接非 VXLAN 网络的物理接口。

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。



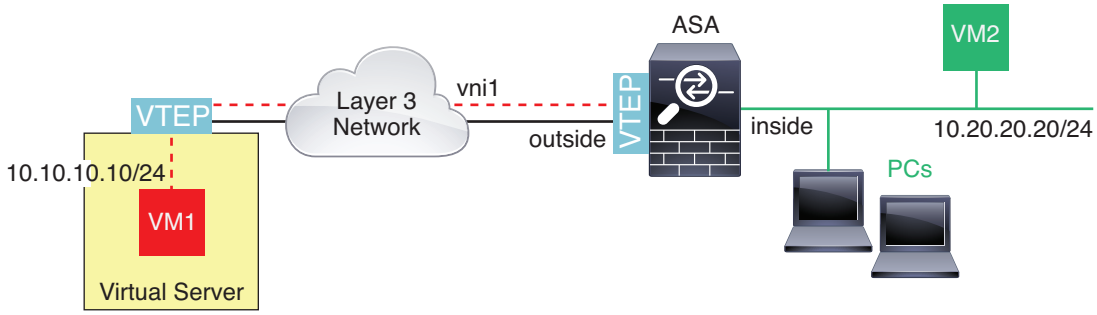
VXLAN 网桥 （透明模式）

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。



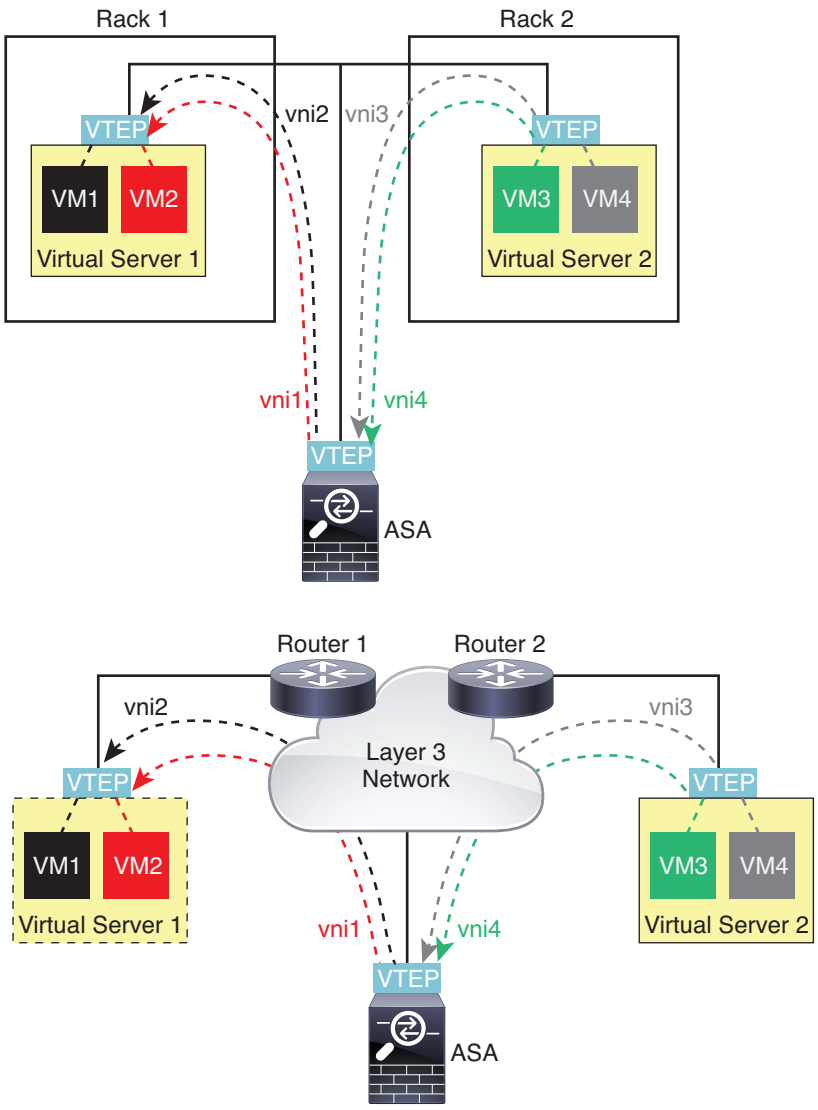
VXLAN 网关 （路由模式）

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 14-6 页。

步骤 2　配置 VNI 接口，第 14-7 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。在 Configuration > Device List 窗格中双击主用设备 IP 地址下的情景名称。

操作步骤

步骤 1　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**，然后编辑要用于 VTEP 源接口的接口。

步骤 2　（透明模式）选中 **VTEP Source Interface** 复选框。

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，此设置仅限制到此接口上的 VXLAN 的流量。

步骤 3　配置源接口名称和 IPv4 地址，然后点击 **OK**。

步骤 4　依次选择 **Configuration > Device Setup > Interface Settings > VXLAN**。

步骤 5　（可选）如果要更改默认值 4789，请输入 **VXLAN Destination Port** 值。

在多情景模式下，请在系统执行空间中配置此设置。

步骤 6　选中 **Enable Network Virtualization Endpoint encapsulation using VXLAN** 复选框。

步骤 7　从下拉列表中选择 **VTEP Tunnel Interface**。

步骤 8　（可选）选中 **Configure Packet Recipient** 复选框。

- （多情景模式；对于单情景模式为可选）输入 **Specify Peer VTEP IP Address** 以手动指定对等体 VTEP IP 地址

  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。

- （仅限单情景模式）输入 **Multicast traffic to default multicast address**，以指定所有相关 VNI 接口的默认组播组。

  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。

步骤 9　点击 **Apply**。

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。

步骤 1　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**，然后点击 **Add > VNI Interface**。

步骤 2　输入介于 1 和 10000 之间的 **VNI ID**。

此 ID 仅为内部接口标识符。

步骤 3　输入介于 1 和 16777215 之间的 **VNI Segment ID**。

网段 ID 用于 VXLAN 标记。

步骤 4　（透明模式）选择要向其分配此接口的 **Bridge Group**。

请参阅配置透明模式接口，第 15-8 页，以配置 BVI 接口并将常规接口关联到此网桥组。

步骤 5　输入 **Interface Name**。

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 6　输入介于 0（最低）和 100（最高）之间的 **Security Level**。请参阅安全级别，第 15-1 页。

步骤 7　（单情景模式）输入 **Multicast Group IP Address**。

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。

步骤 8　选中 **NVE Mapped to VTEP Interface** 复选框。

此设置将 VNI 接口与 VTEP 源接口相关联。

步骤 9　选中 **Enable Interface** 复选框。此设置已默认启用。

步骤 10　（路由模式）在 **IP Address** 区域中，配置 IPv4 地址。要配置 IPv6，请点击 **IPv6** 选项卡。

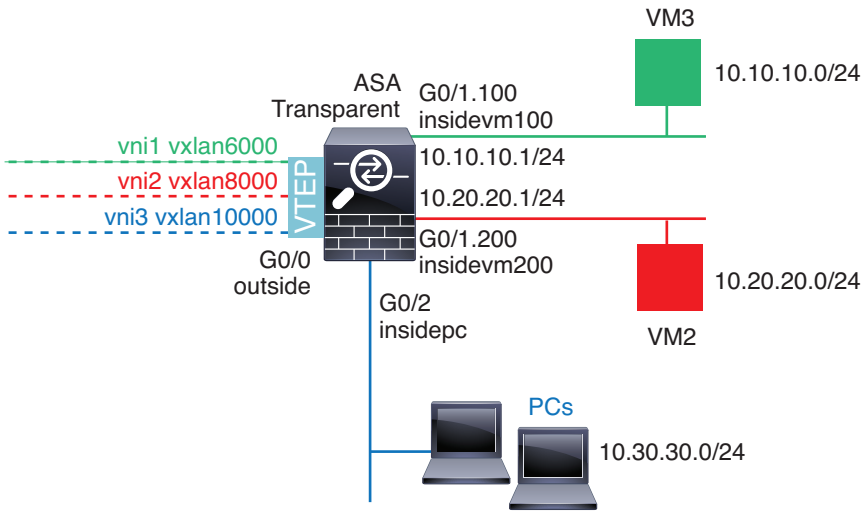
步骤 11　点击 **OK**，然后点击 **Apply**。

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 14-8 页
- VXLAN 路由示例，第 14-10 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

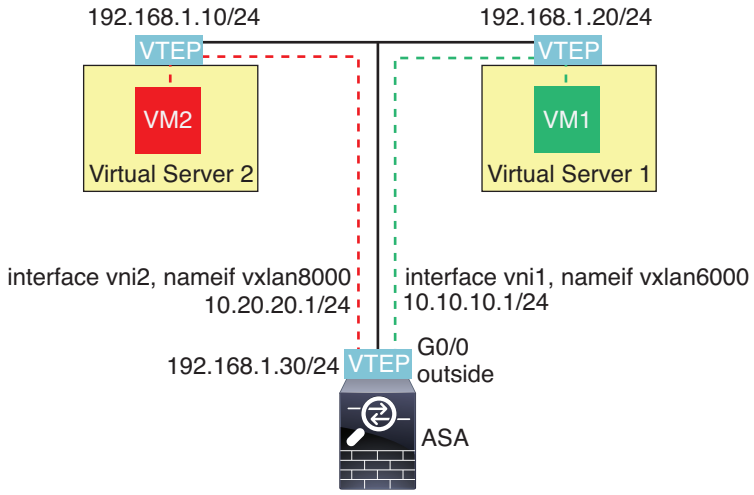
```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  bridge-group 1
  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 14-1　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。 引入了以下屏幕： **Configuration > Device Setup > Interface Settings > Interfaces > Add > VNI Interface** **Configuration > Device Setup > Interface Settings > VXLAN**

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。

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。在 Configuration > Device List 窗格中双击主用设备 IP 地址下的情景名称。

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

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 16-6 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 11-2 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

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。

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 8-14 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 9 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 15-5 页。

步骤 2　配置 PPPoE，第 15-7 页。

步骤 3　配置 IPv6 寻址，第 15-11 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，然后在 Configuration > Device List 窗格中双击主用设备 IP 地址下的情景名称。

操作步骤

步骤 1　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择接口行，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框，其中 **General** 选项卡已选定。

步骤 3　在 **Interface Name** 字段中，输入长度最大为 48 个字符的名称。

步骤 4　在 **Security level** 字段中，输入介于 0 （最低）和 100 （最高）之间的级别。

步骤 5　（可选；不支持用于冗余接口）要将此接口设置为管理专属接口，请选中 **Dedicate this interface to management-only** 复选框。

在管理专属接口上不接受通过流量。

（除 ASA 5585-X 以外的所有 ASA）无法在管理接口上禁用此选项。

注意　Channel Group 字段为只读字段，指示此接口是否为 EtherChannel 的一部分。

步骤 6　如果该接口尚未启用，请选中 **Enable Interface** 复选框。

步骤 7　要设置 IP 地址，请使用以下其中一个选项。

注意　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 和 PPPoE。在 **Configuration > Device Management > High Availability > Failover > Interfaces** 选项卡上设置备用 IP 地址。

- 要手动设置 IP 地址，请点击 **Use Static IP** 单选按钮并输入 IP 地址和掩码。
- 要从 DHCP 服务器获取 IP 地址，请点击 **Obtain Address via DHCP** 单选按钮。
  a. 要强制将 MAC 地址存储在选项 61 的 DHCP 请求数据包内，请点击 **Use MAC Address** 单选按钮。

     某些 ISP 期望选项 61 成为接口 MAC 地址。如果 MAC 地址未包含在 DHCP 请求数据包中，则不会分配 IP 地址。
  b. 要将生成的字符串用于选项 61 ，请点击 **Use “Cisco-<MAC>-<interface_name>-<host>”**。
  c. （可选）要从 DHCP 服务器获取默认路由，请选中 **Obtain Default Route Using DHCP**。
  d. （可选）要分配已获悉的路由的管理距离，请在 **DHCP Learned Route Metric** 字段中输入介于 1 和 255 之间的值。如果将此字段留空，则已获悉的路由的管理距离为 1。
  e. （可选）要启用对通过 DHCP 获悉的路由的跟踪，请选中 **Enable Tracking for DHCP Learned Routes**。设置以下值：

     Track ID - 路由跟踪进程的唯一标识符。有效值范围为 1 至 500。

     Track IP Address - 输入被跟踪目标的 IP 地址。通常，这会是路由的下一跳网关的 IP 地址，但也可能是该接口外可用的任何网络对象。

     注意　路由跟踪仅在单一路由模式下可用。

     SLA ID - SLA 监控进程的唯一标识符。有效值范围为 1 至 2147483647。

     Monitor Options - 点击此按钮可打开 **Route Monitoring Options** 对话框。在 **Route Monitoring Options** 对话框中，您可以配置被跟踪对象监控进程的参数。
  f. （可选）要在 DHCP 客户端发送发现以请求 IP 地址时在 DHCP 数据包报头中将广播标记设置为 1，请选中 **Enable DHCP Broadcast flag for DHCP request and discover messages**。

     DHCP 服务器侦听此广播标志，并在标志设置为 1 时广播应答数据包。
  g. （可选）要续租，请点击 **Renew DHCP Lease**。
- （仅限单情景模式）要使用 PPPoE 来获取 IP 地址，请选中 **Use PPPoE**。
  a. 在 **Group Name** 字段中，指定组名。
  b. 在 **PPPoE Username** 字段中，指定 ISP 提供的用户名。
  c. 在 **PPPoE Password** 字段中，指定 ISP 提供的密码。
  d. 在 **Confirm Password** 字段中，重新键入密码。
  e. 对于 PPP 身份验证，请点击 **PAP**、 **CHAP** 或 **MSCHAP** 单选按钮。

PAP 在身份验证过程中传递明文用户名和密码，这样并不安全。使用 CHAP 时，客户端可返回加密的 [challenge plus password] 和明文用户名来响应服务器质询。CHAP 比 PAP 更安全，但其不会加密数据。MSCHAP 与 CHAP 类似但更安全，因为服务器只对加密密码进行存储和比较，而不是像 CHAP 一样存储和比较明文密码。MSCHAP 还可生成密钥，以便 MPPE 进行数据加密。

f. （可选）要将用户名和密码存储在闪存中，请选中 **Store Username and Password in Local Flash** 复选框。

ASA 将用户名和密码存储在 NVRAM 中的专用位置。如果某自动更新服务器将 **clear configure** 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。

g. （可选）要显示 **PPPoE IP Address and Route Settings** 对话框，请点击 **IP Address and Route Settings**，您可以在该对话框中选择寻址和跟踪选项。

步骤 8　（可选）在 **Description** 字段中，输入此接口的说明。

一行说明最多可包含 240 个字符 （不包括回车符）。例如，对于故障切换或状态链路，说明固定为“LAN Failover Interface”、“STATE Failover Interface”或“LAN/STATE Failover Interface”。您无法编辑此说明。如果将此接口设为故障切换或状态链路，则固定说明将覆盖在此处输入的任何说明。

步骤 9　点击 **OK**。

相关主题

- 配置 MAC 地址、MTU 和 TCP MSS，第 16-5 页
- 配置 IPv6 寻址，第 15-11 页
- 启用物理接口和配置以太网参数，第 11-6 页
- 配置 PPPoE，第 15-7 页

配置 PPPoE

如果使用 PPPoE 进行 IP 寻址，则可以手动配置 IP 地址并配置路由设置。

操作步骤

步骤 1　依次选择 **Configuration > Interfaces > Add/Edit Interface > General**，然后点击 **PPPoE IP Address and Route Settings**。

步骤 2　在 **IP Address** 区域中，选择以下其中一个选项：

- **Obtain IP Address using PPP** - 动态配置 IP 地址。
- **Specify an IP Address** - 手动配置 IP 地址。

步骤 3　在 **Route Settings** 区域中，配置以下选项：

- **Obtain default route using PPPoE** - 在 PPPoE 客户端尚未建立连接时设置默认路由。使用此选项时，配置中不能有静态定义的路由。
- **PPPoE learned route metric** - 向获悉的路由分配管理距离。有效值范围为 1 至 255。如果将此字段留空，则已获悉的路由的管理距离为 1。
- **Enable tracking** - 对 PPPoE 获悉的路由启用路由跟踪。路由跟踪仅在单一路由模式下可用。

- **Primary Track** - 配置主 PPPoE 路由跟踪。
- **Track ID** - 路由跟踪进程的唯一标识符。有效值范围为 1 至 500。
- **Track IP Address** - 输入被跟踪目标的 IP 地址。通常，这会是路由的下一跳网关的 IP 地址，但也可能是该接口外可用的任何网络对象。
- **SLA ID** - SLA 监控进程的唯一标识符。有效值范围为 1 至 2147483647。
- **Monitor Options** - 点击此按钮可打开 **Route Monitoring Options** 对话框。在 **Route Monitoring Options** 对话框中，您可以配置被跟踪对象监控进程的参数。
- **Secondary Track** - 配置辅助 PPPoE 路由跟踪。
- **Secondary Track ID** - 路由跟踪进程的唯一标识符。有效值范围为 1 至 500。

步骤 4　点击 **OK**。

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 15-8 页。
步骤 2　配置常规透明模式接口参数，第 15-9 页。
步骤 3　配置管理接口，第 15-10 页。
步骤 4　配置 IPv6 寻址，第 15-11 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　依次选择 **Configuration > Interfaces**，然后选择 **Add > Bridge Group Interface**。
步骤 2　在 **Bridge Group ID** 字段中，输入介于 1 和 250 之间的网桥组 ID。
步骤 3　在 **IP Address** 字段中，输入管理 IPv4 地址。
步骤 4　在 Subnet Mask 字段中，输入子网掩码或从菜单中选择子网掩码。

请勿将主机地址 （/32 或 255.255.255.255）分配给透明防火墙。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。例如，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。

步骤 5　（可选）在 **Description** 字段中，输入此网桥组的说明。

步骤 6　点击 **OK**。

步骤 7　系统会将网桥组虚拟接口 (BVI) 连同物理接口和子接口添加至接口表。

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，然后在 Configuration > Device List 窗格中双击主用设备 IP 地址下的情景名称。
- 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 15-10 页。

操作步骤

步骤 1　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

BVI 显示在表中物理接口、子接口、冗余接口和 EtherChannel 端口通道接口旁边。在多情景模式中，表中只显示已分配给情景执行空间中情景的接口。

步骤 2　选择与非 BVI 接口对应的行，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框，其中 **General** 选项卡已选定。

步骤 3　在 **Bridge Group** 下拉菜单中，选择要向其分配此接口的网桥组。

步骤 4　在 **Interface Name** 字段中，输入长度最大为 48 个字符的名称。

步骤 5　在 **Security level** 字段中，输入介于 0 （最低）和 100 （最高）之间的级别。

步骤 6　如果该接口尚未启用，请选中 **Enable Interface** 复选框。

注意　**Channel Group** 字段为只读字段，指示此接口是否为 EtherChannel 的一部分。

步骤 7　（可选）如果安装模块，并要在非生产 ASA 上演示该模块功能，请选中 **Forward traffic to the ASA module for inspection and reporting** 复选框。有关详细信息，请参阅模块相关章节或《快速入门指南》。

步骤 8　（可选）在 **Description** 字段中，输入此接口的说明。

一行说明最多可包含 240 个字符 （不包括回车符）。例如，对于故障切换或状态链路，说明固定为“LAN Failover Interface”、“STATE Failover Interface”或“LAN/STATE Failover Interface”。您无法编辑此说明。如果将此接口设为故障切换或状态链路，则固定说明将覆盖在此处输入的任何说明。

步骤 9　点击 **OK**。

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，然后在 Configuration > Device List 窗格中双击主用设备 IP 地址下的情景名称。

操作步骤

步骤 1　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　为管理接口、子接口或组成管理接口的 EtherChannel 端口通道接口选择对应的行，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框，其中 **General** 选项卡已选定。

步骤 3　在 **Bridge Group** 下拉菜单中，保留默认值 **--None--**。您不能将管理接口分配给网桥组。

步骤 4　在 **Interface Name** 字段中，输入长度最大为 48 个字符的名称。

步骤 5　在 **Security level** 字段中，输入介于 0 （最低）和 100 （最高）之间的级别。

注意　**Dedicate this interface to management only** 复选框已默认启用且不可配置。

步骤 6　如果该接口尚未启用，请选中 **Enable Interface** 复选框。

步骤 7　要设置 IP 地址，请使用以下其中一个选项。

注意　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。在 **Configuration > Device Management > High Availability > Failover > Interfaces** 选项卡上设置备用 IP 地址。

- 要手动设置 IP 地址，请点击 **Use Static IP** 单选按钮并输入 IP 地址和掩码。
- 要从 DHCP 服务器获取 IP 地址，请点击 **Obtain Address via DHCP** 单选按钮。
  a. 要强制将 MAC 地址存储在选项 61 的 DHCP 请求数据包内，请点击 **Use MAC Address** 单选按钮。

     某些 ISP 期望选项 61 成为接口 MAC 地址。如果 MAC 地址未包含在 DHCP 请求数据包中，则不会分配 IP 地址。
  b. 要将生成的字符串用于选项 61 ，请点击 **Use “Cisco-<MAC>-<interface_name>-<host>”**。
  c. （可选）要从 DHCP 服务器获取默认路由，请选中 **Obtain Default Route Using DHCP**。
  d. （可选）要在 DHCP 客户端发送发现以请求 IP 地址时在 DHCP 数据包报头中将广播标记设置为 1，请选中 **Enable DHCP Broadcast flag for DHCP request and discover messages**。

     DHCP 服务器侦听此广播标志，并在标志设置为 1 时广播应答数据包。
  e. （可选）要续租，请点击 **Renew DHCP Lease**。

步骤 8　（可选）在 **Description** 字段中，输入此接口的说明。

一行说明最多可包含 240 个字符 （不包括回车符）。

步骤 9　点击 **OK**。

相关主题

管理接口，第 11-2 页

配置 IPv6 寻址

本节介绍如何在路由模式和透明模式下配置 IPv6 寻址。

配置全局 IPv6 地址

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 29 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，然后在 Configuration > Device List 窗格中双击主用设备 IP 地址下的情景名称。

操作步骤

步骤 1　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择接口，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框，其中 **General** 选项卡已选定。

在透明模式下，仅选择网桥组接口或管理接口。

步骤 3　点击 **IPv6** 选项卡。

步骤 4　选中 **Enable IPv6** 复选框。

步骤 5　（可选）要在本地链路上的 IPv6 地址中强制使用修改的 EUI-64 格式的接口标识符，请选中 **Enforce EUI-64** 复选框。

步骤 6　使用以下其中一种方法配置全局 IPv6 地址。

- （仅限路由模式）无状态自动配置 - 在 **Interface IPv6 Addresses** 区域中，选中 **Enable address autoconfiguration** 复选框。

在接口上启用无状态自动配置时，将基于路由器通告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。请选中 **Suppress RA** 复选框来抑制消息。

- 手动配置 - 要手动配置全局 IPv6 地址，请执行以下操作：
  a. 在 **Interface IPv6 Addresses** 区域，点击 **Add**。

     系统将显示 **Add IPv6 Address for Interface** 对话框。
  b. 在 **Address/Prefix Length** 字段中，输入完整全局 IPv6 地址 （包括接口 ID），或输入 IPv6 前缀以及 IPv6 前缀长度。 （仅限路由模式）如果仅输入前缀，请务必选中 **EUI 64** 复选框，以使用修改的 EUI-64 格式生成接口 ID。例如， 2001:0DB8::BA98:0:3210/48 （完整地址）或 2001:0DB8::/48 （前缀，且选中 EUI 64）。
  c. 点击 **OK**。

步骤 7　（可选）要配置在 IPv6 路由器通告中包含哪些 IPv6 前缀，请参阅配置路由器通告中的 IPv6 前缀，第 29-9 页。

步骤 8　点击 **OK**。

系统将返回到 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格。

（可选）自动配置链路本地地址

如果您不想配置全局地址，且只需配置链路本地地址，则可以选择根据接口 MAC 地址生成链路本地地址 （修改的 EUI-64 格式。由于 MAC 地址的长度为 48 位，因此必须插入额外的位，以填充接口 ID 所需的 64 位。）

要自动配置接口的链路本地地址，请执行以下步骤。

操作步骤

步骤 1　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择接口，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框，其中 **General** 选项卡已选定。

在透明模式下，选择任何非网桥组接口。

步骤 3　点击 **IPv6** 选项卡。

步骤 4　在 **IPv6 configuration** 区域中，选中 **Enable IPv6** 复选框。

此选项启用 IPv6，并且根据接口 MAC 地址使用修改的 EUI-64 格式自动生成链路本地地址。

步骤 5　点击 **OK**。

（可选）手动配置链路本地地址

如果您不想配置全局地址，且只需配置链路本地地址，则可以选择手动定义链路本地地址。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

要向接口分配链路本地地址，请执行以下步骤。

操作步骤

步骤 1　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择接口，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框，其中 **General** 选项卡已选定。

在透明模式下，选择任何非网桥组接口。

步骤 3　点击 **IPv6** 选项卡。

步骤 4　要设置链路本地地址，请在 **Link-local address** 字段中输入地址。

链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。 有关 IPv6 寻址的详细信息，请参阅 IPv6 地址，第 41-4 页。

步骤 5　点击 **OK**。

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 等。

接口统计信息

- **Monitoring > Interfaces > Interface Graphs**

  以图形或表格形式查看接口统计信息。如果某个接口在情景之间共享，则 ASA 仅显示当前情景的统计信息。为子接口显示的统计信息数是为物理接口显示的统计信息数的子集。

- **Monitoring > Interfaces > Interface Graphs > Graph/Table**

  显示选定统计信息的图形。Graph 窗口一次最多可以显示四个图形和表格。默认情况下，图形或表格显示实时统计信息。如果您启用 History Metrics，则可以查看过去时间段的统计信息。

静态路由跟踪

- **Monitoring > Interfaces > interface connection > Track Status**

  显示有关被跟踪对象的信息。
- **Monitoring > Interfaces > interface connection > Monitoring Statistics**

  显示 SLA 监控进程的统计信息。

PPPoE

- **Monitoring > Interfaces > PPPoE Client > PPPoE Client Lease Information**

  显示有关当前 PPPoE 连接的信息。

DHCP

- **Monitoring > Interfaces > DHCP > DHCP Server Table**

  列出分配给 DHCP 客户端的 IP 地址。
- **Monitoring > Interfaces > DHCP > DHCP Server Table > DHCP Client Lease Information**

  显示有关 DHCP 租用的信息。
- **Monitoring > Interfaces > DHCP > DHCP Statistics**

  显示 DHCP 服务器功能的统计信息。

动态 ACL

Monitoring > Interfaces > Dynamic ACLs

显示动态 ACL 表，这些动态 ACL 与用户配置的 ACL 功能相同，不同之处在于它们是由 ASA 自动创建、激活和删除的。这些 ACL 不会显示在配置中，仅在此表中可见。它们通过 ACL 报头中的 “(dynamic)”关键字进行识别。

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 15-1　　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。 修改或引入了以下屏幕： Configuration > Device Setup > Interface Settings > Interfaces Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface

表 15-1　　透明模式下的接口历史记录 （续）

功能名称	平台版本	功能信息
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。 修改了以下屏幕： Configuration > Device Setup > Interface Settings > Interfaces Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface

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。

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。在 Configuration > Device List 窗格中双击主用设备 IP 地址下的情景名称。

关于高级接口配置

本节介绍高级接口设置。

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 8-2 页
- 自动将 MAC 地址分配给情景接口，第 8-20 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 16-2 页
- 路径 MTU 发现，第 16-2 页
- MTU 和巨帧，第 16-3 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 16-3 页
- VPN 和非 VPN 流量的 TCP MSS，第 16-3 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。

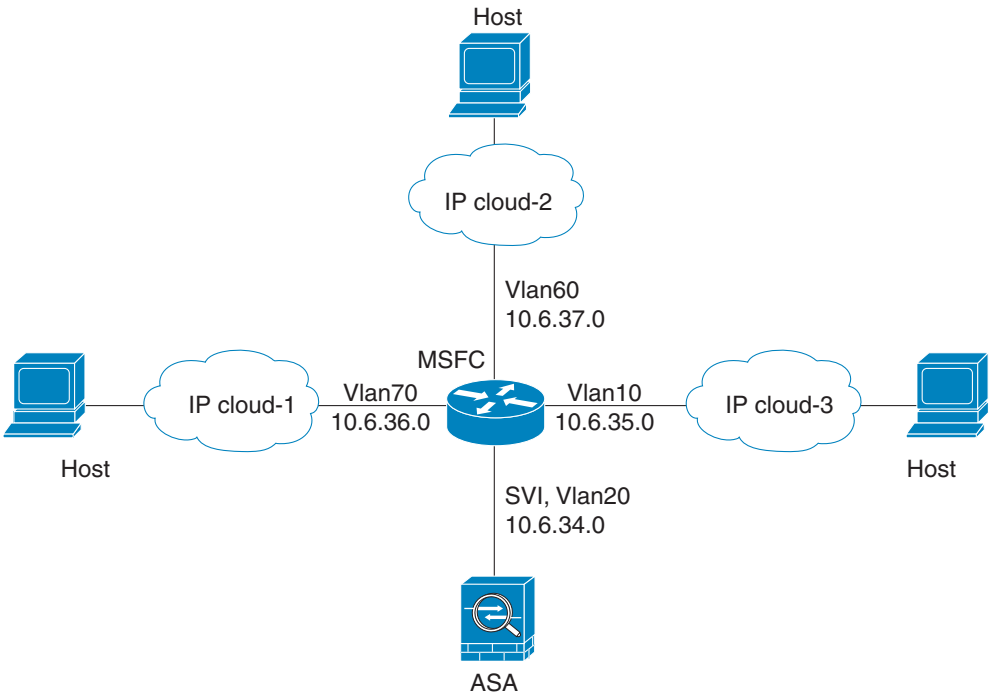
如果启用同一安全级别接口通信，则仍可以照常配置不同安全级别的接口。

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、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，然后在 Configuration > Device List 窗格中双击主用设备 IP 地址下的情景名称。

操作步骤

步骤 1　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择接口行，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框，其中 **General** 选项卡已选定。

步骤 3　点击 **Advanced** 选项卡。

步骤 4　要设置 MTU 或启用巨帧支持 （仅限支持的型号），请在 **MTU** 字段输入 300 至 9198 字节之间的数值 （对于 ASAv，为 9000）。

默认值为 1500 字节。

注意　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。

- 对于在单情景模式下支持句型帧的型号 - 如果为任何接口输入的值大于 1500，则您将自动为所有接口启用巨帧支持。如将所有接口的 MTU 值均设置回小于 1500 的值，则将禁用巨帧支持。
- 对于在多情景模式下支持句型帧的型号 - 如果为任何接口输入的值大于 1500，则务必在系统配置中启用巨帧支持。请参阅启用巨帧支持，第 11-7 页。

注意　启用或禁用巨帧支持需要重新加载 ASA。

步骤 5　要手动向该接口分配 MAC 地址，请在 **Active Mac Address** 字段中以 H.H.H 格式输入 MAC 地址，其中， H 是 16 位的十六进制数字。

例如，MAC 地址 00-0C-F1-42-4C-DE 将需要输入 000C.F142.4CDE。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。

步骤 6　如果使用故障切换，请在 **Standby Mac Address** 字段输入备用 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。

步骤 7　要设置 TCP MSS，请依次选择 **Configuration > Firewall > Advanced > TCP Options**。设置以下选项：

- Force Maximum Segment Size for TCP - 将最大 TCP 分片大小设置为介于 48 和任何最大数值之间的字节数。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。
- Force Minimum Segment Size for TCP **-** 覆盖最大分片大小，使其不小于已设置的字节数，介于 48 和任何最大数值之间。默认情况下，此功能已禁用 （设置为 0）。

步骤 8　对于 **Secure Group Tagging**，请参阅 《防火墙配置指南》中的 TrustSec 章节。

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　要启用相同安全级别的接口之间的通信，请在 **Configuration > Interfaces** 窗格中选中 **Enable traffic between two or more interfaces which are configured with same security level**。

步骤 2　要启用连接到同一接口的主机之间的通信，请选中 **Enable traffic between two or more hosts connected to the same interface**。

监控 ARP 和 MAC 地址表

- **Monitoring > Interfaces > ARP Table**

  显示 ARP 表，包括静态和动态条目。ARP 表包含将给定接口的 MAC 地址映射到 IP 地址的条目。

- **Monitoring > Interfaces > MAC Address Table**

  显示静态和动态 MAC 地址条目。

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

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

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 1-14 页

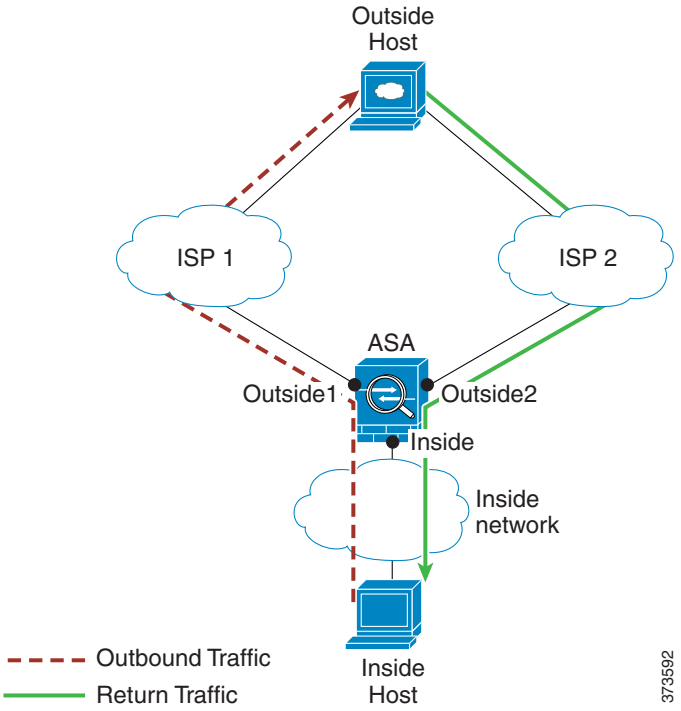
为什么使用区域？

您可以使用区域来支持几种路由情景。

- 非对称路由，第 17-2 页
- 丢失的路由，第 17-3 页
- 负载均衡，第 17-4 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。

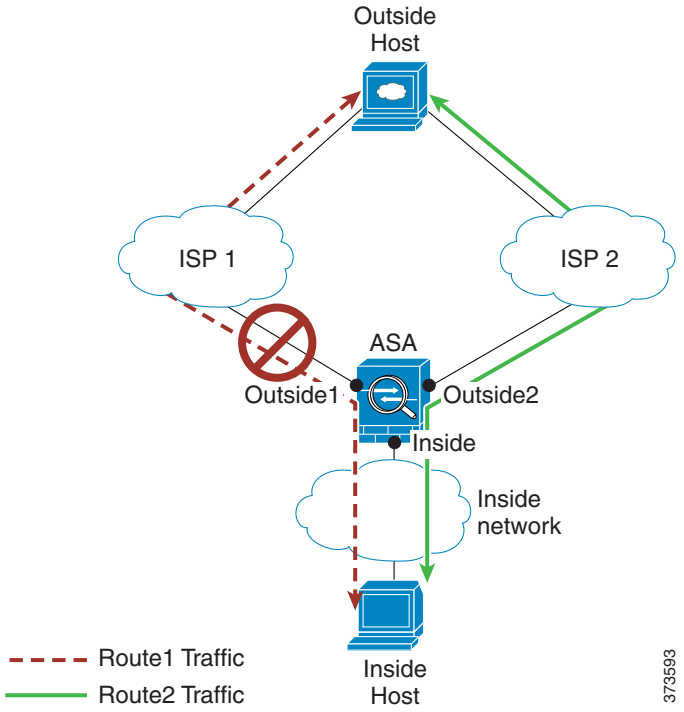


因未划分区域出现的问题：ASA 针对每个接口维护连接表。返回到达 Outside2 的流量时，它不会匹配连接表，并且将被丢弃。

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。

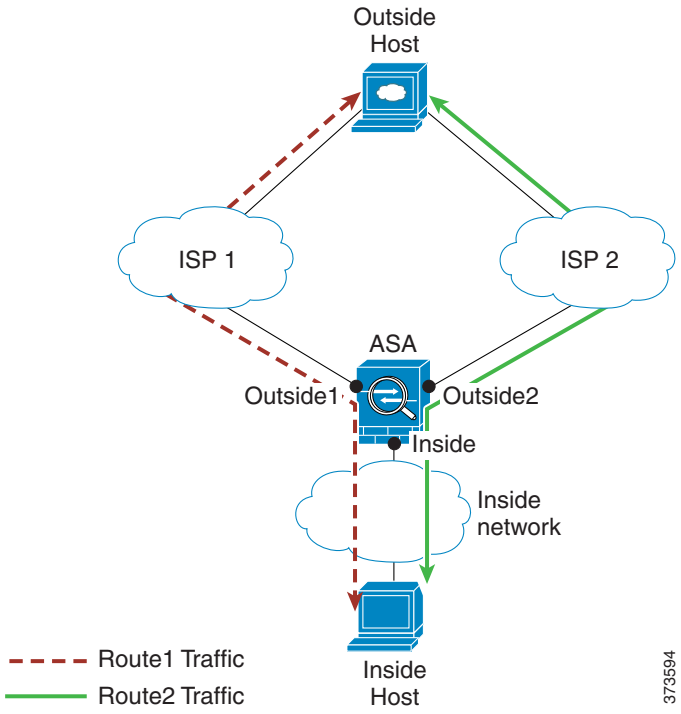


因未划分区域出现的问题：内部主机和外部主机之间的连接将被删除；您必须使用新的次优路由建立新连接。对于 UDP，新路由将在单次丢包之后使用；但对于 TCP，需要重新建立新连接。

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 17-5 页
- 划分区域的 ECMP 支持，第 17-5 页
- 如何对连接进行负载均衡，第 17-5 页
- 回退到另一区域中的路由，第 17-5 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 17-7 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 17-7 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 17-7 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 **Configuration > Device Setup > Interface Settings > Interfaces > Enable traffic between two or more hosts connected to the same interface**，此命令允许流量流入和流出同一接口，并启用 **Configuration > Device Setup > Interface Settings > Interfaces > Enable traffic between two or more interfaces which are configured with same security level**，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 9-29 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　依次选择 **Configuration > Device Setup > Interface Settings > Zones**，点击 **Add**。

您也可以从 **Configuration > Device Setup > Interface Settings > Interfaces > Add Interface** 对话框向区域分配接口。

步骤 2　使用最多 48 个字符的名称为区域命名。

步骤 3　将一个或多个接口添加到 **Member** 区域。确保所有接口都有相同的安全级别。

步骤 4　点击 **Apply**。

监控流量区域

本节介绍如何监控流量区域。

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**

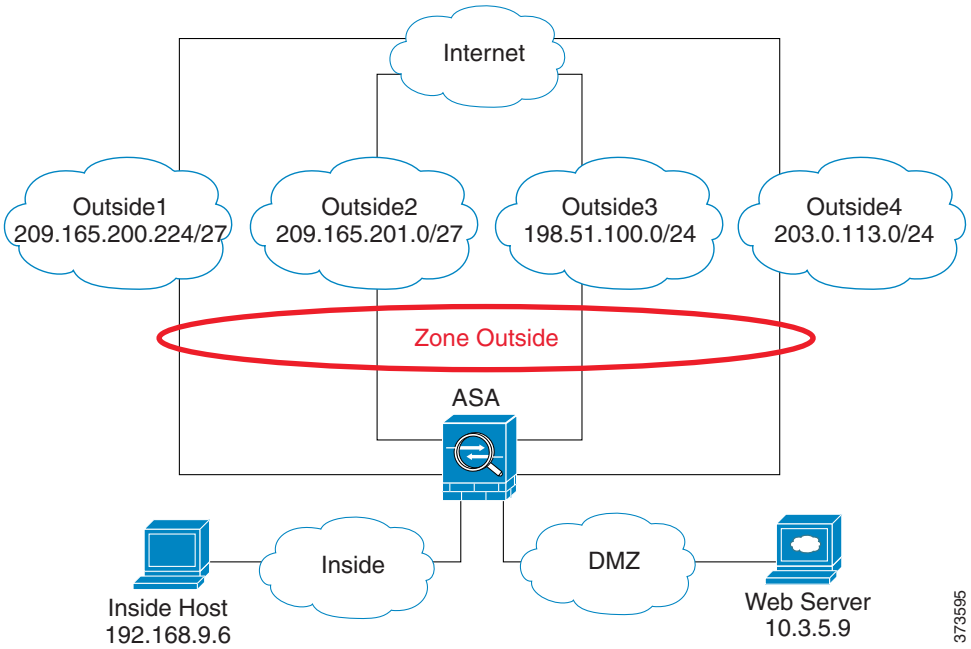
  显示用于调试的加速安全路径表，并显示与每个路由关联的区域。

  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。 引入或修改了以下屏幕： **Configuration > Device Setup > Interface Parameters > Zones** **Configuration > Device Setup > Interface Parameters > Interfaces**

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

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。
- 要从系统更改为情景配置，请在 **Configuration > Device List** 窗格中双击主用设备 IP 地址下的情景名称。

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 依次选择 **Configuration > Device Setup > Device Name/Password**。

步骤 2 输入主机名。默认主机名为 “ciscoasa”。

该主机名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。该主机名同时用于系统日志消息。

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。在情景中选择性设置的主机名将不会显示在命令行中；但可用于标题。

步骤 3　输入域名。默认域名为 default.domain.invalid。

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 4　更改特权模式 （启用）密码。默认密码为空。

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。

a. 选中 **Change the privileged mode password** 复选框。

b. 输入原密码 （默认密码为空）和新密码，然后确认新密码。

步骤 5　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。

a. 选中 **Change the password to access the console of the security appliance** 复选框。

b. 输入原密码 （对于新 ASA，请将此字段留空）和新密码，然后确认新密码。

步骤 6　点击 **Apply** 保存更改。

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。

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　依次选择 **Configuration > Device Setup > System Time > NTP**。

步骤 2　点击 **Add** 以显示 **Add NTP Server Configuration** 对话框。

步骤 3　输入 NTP 服务器 IP 地址。

步骤 4　选中 **Preferred** 复选框，将该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，则使用首选服务器。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。

步骤 5　从下拉列表中选择接口。该设置指定 NTP 数据包的传出接口。如果接口为空，则 ASA 根据路由表使用默认管理情景接口。要确保稳定性，请选择 **None**（默认接口），以更改管理情景（和可用接口）。

步骤 6　从下拉列表中选择密钥编号。该设置指定此身份验证密钥的密钥 ID，可供您使用 MD5 身份验证与 NTP 服务器进行通信。NTP 服务器数据包必须也使用此密钥 ID。如果以前已为其他服务器配置密钥 ID，则可从列表中选择该 ID；否则，请输入一个介于 1 和 4294967295 之间的数字。

步骤 7　选中 **Trusted** 复选框，以将该身份验证密钥设置为受信任密钥，要使身份验证成功，必须执行此操作。

步骤 8　输入密钥值，设置身份验证密钥，密钥字符串最多为 32 个字符。

步骤 9　重新输入密钥值，确保两次输入正确。

步骤 10　点击 **OK**。

步骤 11　选中 **Enable NTP authentication** 复选框，以启动 NTP 身份验证。

步骤 12　点击 **Apply** 保存更改。

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　依次选择 **Configuration > Device Setup > System Time > Clock**。

步骤 2　从下拉列表中选择时区。该设置将时区指定为 GMT 加上或减去适当的小时数。如果选择东部时间、中部时间、山地时间或太平洋时间时区，则时间将自动调整为夏令时，时间范围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。

注意　更改 ASA 上的时区可能会丢弃与智能 SSM 的连接。

步骤 3　点击 **Date** 下拉列表以显示日历。然后，使用以下方法查找正确的日期：

- 点击月份名称以显示月份列表，然后点击所需的月份。日历将更新至该月。
- 点击年份进行更改。使用向上和向下箭头滚动浏览年份，或在输入字段中输入年份。
- 点击月份和年份右侧和左侧的箭头，向前向后滚动日历，每次一个月。
- 点击日历上的一个日期，设置日期。

步骤 4　以小时、分钟和秒的形式手动输入时间。

步骤 5　点击 **Update Display Time**，更新 ASDM 窗格右下角显示的时间。当前时间每十秒钟自动更新一次。

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。

依次选择 **Configuration > Device Management > High Availability > Failover**，在 Shared Key 字段中输入任意字符，或如果已选择故障切换十六进制密钥，则请输入 32 个十六进制数字 (0-9A-Fa-f)，但退格符号除外。然后点击 **Apply**。

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　选择以下选项之一：

- 在单一情景模式下，依次选择 **Configuration > Device Management > Advanced > Master Passphrase**。

- 在多情景模式下，依次选择 **Configuration > Device Management > Device Administration > Master Passphrase**。

步骤 2　选中 **Advanced Encryption Standard (AES) password encryption** 复选框。

如果没有有效主密码，则在点击 **Apply** 时将显示警告消息。可点击 **OK** 或 **Cancel** 继续操作。

如果稍后禁用密码加密，所有现有加密密码将保持不变，并且只要主密码存在，加密密码就会根据应用要求被解密。

步骤 3　选中 **Change the encryption master passphrase** 复选框，以便能够输入并确认新的主密码。其已默认禁用。

新的主密码长度必须介于 8 和 128 个字符之间。

如果更改现有密码，则必须在输入新密码之前输入原密码。

将 **New** 和 **Confirm master passphrase** 字段留空，以删除主密码。

步骤 4　点击 **Apply**。

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。
- 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　选择以下选项之一：

- 在单一情景模式下，依次选择 **Configuration > Device Management > Advanced > Master Passphrase**。
- 在多情景模式下，依次选择 **Configuration > Device Management > Device Administration > Master Passphrase**。

步骤 2　选中 **Advanced Encryption Standard (AES) password encryption** 复选框。

如果没有有效主密码，则在点击 **Apply** 时将显示警告语句。可点击 **OK** 或 **Cancel** 继续操作。

步骤 3　选中 **Change the encryption master passphrase** 复选框。

步骤 4　在 **Old master passphrase** 字段中输入原主密码。只有提供原主密码才能禁用该主密码。

步骤 5　将 **New master passphrase** 和 **Confirm master passphrase** 字段留空。

步骤 6　点击 **Apply**。

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。

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　依次选择 **Configuration > Device Management > DNS > DNS Client**。

步骤 2　确保至少在一个接口上已启用 DNS 查找。在 DNS 服务器组表下方的 **DNS Lookup** 接口列表中，点击 DNS Enabled 列，然后选择 **True** 以在该接口上启用查找。

步骤 3　在 **DNS Setup** 区域中，选择以下选项之一：

- **Configure one DNS server group**.
- **Configure multiple DNS server groups**.

步骤 4　执行以下操作之一：

- 选择 DNS 组，然后点击 **Edit**。
- 如果已选择配置多个 DNS 组，请点击 **Add** 以添加新组。输入组名称。

步骤 5　配置 DNS 服务器组。

a. 输入已配置服务器的 IP 地址，然后点击 **Add**。

   最多可添加六台 DNS 服务器。ASA 按顺序尝试每台 DNS 服务器，直至收到响应。使用 **Move Up**/**Move Down** 按钮按优先级顺序放置服务器。

b. 在 **Other Setting** 区域的列表中，输入尝试下一台 DNS 服务器之前等待的秒数（介于 1 和 30 之间）。默认值为 2 秒。每当 ASA 重新尝试查找服务器列表时，超时时间就会加倍。

c. 为已配置服务器组输入 DNS 域名。

d. 点击 **OK**。

步骤 6　如果有多个服务器组，请选择要使用的一个组，然后点击 **Set Active**。该服务器组将用于 DNS 请求。

步骤 7　选中 **Enable DNS Guard on all interfaces** 复选框，对每个查询执行一次 DNS 响应。

配置 DNS 检查时，还可设置 DNS Guard。对于给定接口，已在 DNS 检查中配置的 DNS Guard 设置优先于该全局设置。默认情况下，在启用 DNS Guard 的情况下，在所有接口上均已启用 DNS 检查。

步骤 8　点击 **Apply** 保存更改。

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

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，请依次选择 **Configuration > Device Management > Advanced > Rule Engine**，然后选择所需选项：

- **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。

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。

在有多个核心的 ASA 模型上，如果发现许多数据包丢弃，同时 CPU 使用率显著低于 100%，则应启用负载均衡选项。

依次选择 **Configuration > Device Management > Advanced > ASP Load Balancing**，然后选中 **Enable ASP load balancing** 复选框。

选中 **Dynamically enable or disable ASP load balancing based on traffic monitoring** 复选框，自动启用 ASP 负载均衡。

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。 引入了以下屏幕：Configuration > Device Management > Advanced > Master Passphrase。 Configuration > Device Management > Device Administration > Master Passphrase。
密码加密可见性	8.4(1)	已修改了 **show password encryption** 命令。
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。 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。 未修改任何 ASDM 屏幕。

功能名称	平台版本	说明
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。 引入了以下屏幕：Configuration > Device Management > Advanced > ASP Load Balancing。

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

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 19-4 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 19-4 页。

步骤 2　配置高级 DHCP 选项。请参阅配置高级 DHCP 选项，第 19-6 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 19-7 页或配置 DHCPv6 中继代理，第 19-7 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　依次选择 **Configuration > Device Management > DHCP > DHCP Server**。

步骤 2　选择接口，然后点击 **Edit**。

a. 选中 **Enable DHCP Server** 复选框以启用选定接口上的 DHCP 服务器。

b. 在 **DHCP Address Pool** 字段中，输入 DHCP 服务器使用的从最低到最高的 IP 地址范围。IP 地址范围必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。

c. 在 **Optional Parameters** 区域内设置以下参数：
   - 为接口配置的 DNS 服务器 （1 和 2）。
   - 为接口配置的 WINS 服务器 （主服务器和次要服务器）。
   - 接口的域名
   - ASA 等待接口上的 ICMP ping 响应的时间 （以毫秒为单位）。
   - 接口上配置的 DHCP 服务器允许 DHCP 客户端使用所分配的 IP 地址的持续时间。
   - 当 ASA 充当指定接口（通常为外部接口）上的 DHCP 客户端时，DHCP 客户端上为自动配置提供 DNS、 WINS 和域名信息的接口。
   - 点击 **Advanced** 以显示 **Advanced DHCP Options** 对话框，从而配置多个 DHCP 选项。有关详情，请参见配置高级 DHCP 选项，第 19-6 页。

d. 选中 **Dynamic Settings for DHCP Server** 区域内的 **Update DNS Clients** 复选框，以指定除了更新客户端 PTR 资源记录这一默认操作外，选定 DHCP 服务器还应执行以下更新操作：
   - 选中 **Update Both Records** 复选框，以指定 DHCP 服务器应同时更新 A RR 和 PTR RR。
   - 选中 **Override Client Settings** 复选框，以指定 DHCP 服务器操作应覆盖 DHCP 客户端请求的任何更新操作。

e. 点击 **OK** 以关闭 **Edit DHCP Server** 对话框。

步骤 3　选中 DHCP 服务器表下方 **Global DHCP Options** 区域中的 **Enable Auto-configuration from interface** 复选框，以便在只有 ASA 充当指定接口 （通常为外部接口）上的 DHCP 客户端时才启用 DHCP 自动配置。

DHCP 自动配置使 DHCP 服务器能为 DHCP 客户端提供从运行于指定接口上的 DHCP 客户端获得的 DNS 服务器、域名和 WINS 服务器信息。如果在 **Global DHCP Options** 区域内还手动指定通过自动配置获取的信息，则手动指定的信息优先于发现的信息。

步骤 4　从下拉列表中选择接口。

步骤 5　选中 **Allow VPN Override** 复选框，以使用 VPN 客户端参数覆盖 DHCP 或 PPPoE 客户端参数。

步骤 6　在 **DNS Server 1** 字段中，为 DHCP 客户端输入 DNS 主服务器的 IP 地址。

步骤 7　在 **DNS Server 2** 字段中，为 DHCP 客户端输入 DNS 备选服务器的 IP 地址。

步骤 8　在 **Domain Name** 字段中，输入 DHCP 客户端的 DNS 域名 （例如， example.com）。

步骤 9　在 **Lease Length** 字段中，输入在租赁到期之前客户端可使用向其分配的 IP 地址的时间 （以秒为单位）。有效值的范围为 300 到 1048575 秒。默认值为 3600 秒 （1 小时）。

步骤 10　在 **Primary WINS Server** 字段中，为 DHCP 客户端输入 WINS 主服务器的 IP 地址。

步骤 11　在 **Secondary WINS Server** 字段中，为 DHCP 客户端输入 WINS 备选服务器的 IP 地址。

步骤 12　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。在 **Ping Timeout** 字段中输入 ASA 等待 DHCP ping 尝试超时的时间 （以毫秒为单位）。有效值的范围为 10 到 10000 秒。默认值为 50 毫秒。

步骤 13　点击 **Advanced** 选项卡，以显示 **Configuring Advanced DHCP Options** 对话框，从而在其中指定其他 DHCP 选项及其参数。有关详细信息，请参阅配置高级 DHCP 选项，第 19-6 页。

步骤 14　为 **Dynamic DNS Settings for DHCP Server** 区域内的 DHCP 服务器配置 DDNS 更新设置。选中 **Update DNS Clients** 复选框，以指定除了更新客户端 PTR 资源记录这一默认操作外，选定 DHCP 服务器还应执行以下更新操作：

- 选中 **Update Both Records** 复选框，以指定 DHCP 服务器应同时更新 A RR 和 PTR RR。
- 选中 **Override Client Settings** 复选框，以指定 DHCP 服务器操作应覆盖 DHCP 客户端请求的任何更新操作。

步骤 15　点击 **Apply** 保存更改。

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。

操作步骤

步骤 1　依次选择 **Configuration > Device Management > DHCP > DHCP Server**，然后点击 **Advanced**。

步骤 2　从下拉列表中选择选项代码。所有 DHCP 选项 (1-255) 均受支持，但 1、12、50–54、58–59、61、67 和 82 除外。

步骤 3　选择要配置的选项。某些选项属于标准选项。对于标准选项，选项名称显示在选项编号之后并用括号括起来，选项参数限定于那些受该选项支持的参数。对于所有其他选项，仅显示选项编号，您必须选择要随该选项提供的适当参数。例如，如果选择 DHCP 选项 2 （时间偏移量），则只能输入该选项的十六进制值。对于所有其他 DHCP 选项，所有选项值类型均可用，必须选择适当的一个。

步骤 4　指定选项向 **Option Data** 区域内 DHCP 客户端返回的信息的类型。对于标准 DHCP 选项，仅支持的选项值类型可用。对于所有其他 DHCP 选项，所有选项值类型均可用。点击 **Add** 以将选项添加到 DHCP 选项列表。点击 **Delete** 以将选项从 DHCP 选项列表中删除。

- 点击 **IP Address** 以表明已向 DHCP 客户端返回一个 IP 地址。最多可以指定两个 IP 地址。IP 地址 1 和 IP 地址 2 以点分十进制表示法显示 IP 地址。

  注意　关联 IP 地址字段的名称可能随选择的 DHCP 选项改变。例如，如果选择 DHCP 选项 3（路由器），则字段名将更改为 Router 1 和 Router 2。

- 点击 **ASCII** 以指定已向 DHCP 客户端返回一个 ASCII 值。在 **Data** 字段中，输入一个 ASCII 字符串。字符串不能包含空格。

  注意　关联 Data 字段的名称可能随选择的 DHCP 选项改变。例如，如果选择 DHCP 选项 14（Merit Dump File），则关联 Data 字段将更改为 File Name。

- 点击 **Hex** 以指定已向 DHCP 客户端返回一个十六进制值。在 **Data** 字段中，输入一个偶数位数且无空格的十六进制字符串。您无需使用 0x 前缀。

  注意　关联 Data 字段的名称可能随选择的 DHCP 选项改变。例如，如果选择 DHCP 选项 2（时间偏移量），则关联 Data 字段变为 Offset 字段。

步骤 5　点击 **OK** 以关闭 **Advanced DHCP Options** 对话框。

步骤 6　点击 **Apply** 保存更改。

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。

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　依次选择 **Configuration > Device Management > DHCP > DHCP Relay**。

步骤 2　在 **DHCP Relay Agent** 区域选中，为每个接口所需服务选择对应的复选框。

- **IPv4 > DHCP Relay Enabled**。
- **IPv4 > Set Route** - 将来自服务器的 DHCP 消息中默认网关地址更改为最接近 DHCP 客户端的 ASA 接口的地址，该客户端中继原始 DHCP 请求。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。
- **IPv6 > DHCP Relay Enabled**。
- **Trusted Interface** - 指定要信任的 DHCP 客户端接口。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。另外，可通过选中 **Set dhcp relay information as trusted on all interfaces** 复选框信任所有接口 （请参阅步骤 7）。

步骤 3　在 **Global DHCP Relay Servers** 区域中，添加一个或多个要将 DHCP 请求中继到的 DHCP 服务器。

a. 点击**添加**。系统将显示 **Add Global DHCP Relay Server** 对话框。
b. 在 **DHCP Server** 字段中，输入 DHCP 服务器的 IPv4 或 IPv6 地址。
c. 从 **Interface** 下拉列表中，选择指定 DHCP 服务器要连接的接口。
d. 点击 **OK**。

Global DHCP Relay Servers 列表中将显示新添加的全局 DHCP 中继服务器。

步骤 4　（可选）在 **IPv4 Timeout** 字段中，输入为 DHCP 地址处理预留的时间量 （以秒为单位）。有效值的范围为 1 到 3600 秒。默认值为 60 秒。

步骤 5　（可选）在 **IPv6 Timeout** 字段中，输入为 DHCP 地址处理预留的时间量 （以秒为单位）。有效值的范围为 1 到 3600 秒。默认值为 60 秒。

步骤 6　在 **DHCP Relay Interface Servers** 区域中，添加要将给定接口上 DHCP 请求中继到的一个或多个接口专用 DHCP 服务器。

a. 点击**添加**。系统将显示 **Add DHCP Relay Server** 对话框。

b. 从 **Interface** 下拉列表中，选择连接到 DHCP 客户端的接口。请注意，如同在全局 DHCP 服务器中，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。

c. 在 **Server to**... 字段中，输入 DHCP 服务器的 IPv4 地址，然后点击 **Add>>**。服务器已成功添加到右侧列表。添加多达 4 台服务器 （如未超过服务器总数上限）。接口专用服务器不支持 IPv6。

d. 点击 **OK**。

新添加的接口 DHCP 中继服务器将显示在 **DHCP Relay Interface Servers** 列表中。

步骤 7　要将所有接口配置为受信任接口，请选中 **Set dhcp relay information as trusted on all interfaces** 复选框。或者，可以信任单个接口 （请参阅步骤 2）。

步骤 8　点击 **Apply** 保存设置。

配置 DDNS

本节介绍如何配置 DDNS。

要配置动态 DNS 及更新 DNS 服务器，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Device Management > DNS > Dynamic DNS**。

步骤 2　点击 **Add** 以显示 **Add Dynamic DNS Update Method** 对话框。

步骤 3　输入 DDNS 更新方法的名称。

步骤 4　以日、小时、分钟和秒为单位指定为更新方法配置的 DNS 更新尝试之间的更新间隔。

- 从 0 到 364 中选择更新尝试间隔的天数。
- 从 0 到 23 中选择更新尝试间隔的小时数 （取整数）。
- 从 0 到 59 中选择更新尝试间隔的分钟数 （取整数）。
- 从 0 到 59 中选择更新尝试间隔的秒数 （取整数）。

这些单位是累加的。即，如果输入 0 天 0 小时 5 分钟 15 秒，则只要更新方法有效，其就会每隔 5 分钟 15 秒尝试更新一次。

步骤 5　选择下列其中一个选项存储 DNS 客户端更新的服务器资源记录更新：

- A 资源记录和 PTR 资源记录。
- 仅 A 资源记录。

步骤 6　点击 **OK** 以关闭 **Add Dynamic DNS Update Method** 对话框。

系统将显示新的动态 DNS 客户端设置。

注意　编辑现有方法时， Name 字段为 *display-only* 并显示所选编辑方法的名称。

步骤 7　点击 **Add** 以显示 **Add Dynamic DNS Interface Settings** 对话框，在其中为每个已配置的接口添加 DDNS 设置。

步骤 8　从下拉列表中选择接口。

步骤 9　从下拉列表中选择分配给接口的更新方法。

步骤 10　输入 DDNS 客户端的主机名。

步骤 11　选择以下其中一个选项存储资源记录更新：

- Default (PTR Records)，指定客户端请求由服务器更新 PTR 记录。
- Both (PTR Records and A Records)，指定客户端请求由服务器更新 A 和 PTR DNS 资源记录。
- None，指定客户端请求服务器不执行更新。

注意　只有在选定接口上启用 DHCP，此操作才能生效。

步骤 12　点击 **OK** 以关闭 **Add Dynamic DNS Interface Settings** 对话框。

系统将显示新的动态 DNS 接口设置。

步骤 13　点击 **Apply** 以保存您的更改，或点击 **Reset** 以丢弃更改并输入新设置。

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 服务的屏幕：

- **Monitoring > Interfaces > DHCP > DHCP Client Lease Information**。

  此窗格显示已配置的 DHCP 客户端 IP 地址。
- **Monitoring > Interfaces > DHCP > DHCP Server Table**

  此窗格显示已配置的动态 DHCP 客户端 IP 地址。
- **Monitoring > Interfaces > DHCP > DHCP Statistics**

  此窗格显示 DHCPv4 消息类型、计数器、值、方向、接收的消息和发送的消息。
- **Monitoring > Interfaces > DHCP > IPV6 DHCP Statistics**

  此窗格显示 DHCPv6 消息类型、计数器、值、方向、接收的消息和发送的消息。
- **Monitoring > Interfaces > DHCP > IPV6 DHCP Binding**

  此窗格显示 DHCPv6 绑定。
- **Tools > Command Line Interface**

  此窗格将非交互式命令发送到 ASA 并列出结果。

监控 DDNS 状态

请参阅以下用于监控 DDNS 状态的屏幕：

- **Tools > Command Line Interface**

  此窗格将非交互式命令发送到 ASA 并列出结果。

DHCP 和 DDNS 服务历史记录

表 19-1　　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。 引入了以下屏幕： Configuration > Device Management > DHCP > DHCP Relay。 Configuration > Device Management > DHCP > DHCP Server。
DDNS	7.0(1)	引入了此功能。 引入了以下屏幕： Configuration > Device Management> DNS > DNS Client。 Configuration > Device Management > DNS > Dynamic DNS。
DHCP for IPv6 (DHCPv6)	9.0(1)	增加了对 IPv6 的支持。 修改了以下屏幕：Configuration > Device Management > DHCP > DHCP Relay。
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。 修改了以下屏幕：Configuration > Device Management > DHCP > DHCP Relay。
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。 修改了以下屏幕：Configuration > Device Management > DHCP > DHCP Relay。
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。 未修改任何 ASDM 屏幕。
IPv6 的 DHCP 监控	9.4(1)	现在可监控 IPv6 的 DHCP。 引入了以下屏幕： Monitoring > Interfaces > DHCP > IPV6 DHCP Statistics Monitoring > Interfaces > DHCP > IPV6 DHCP Binding。

数字证书

本章介绍如何配置数字证书。

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。

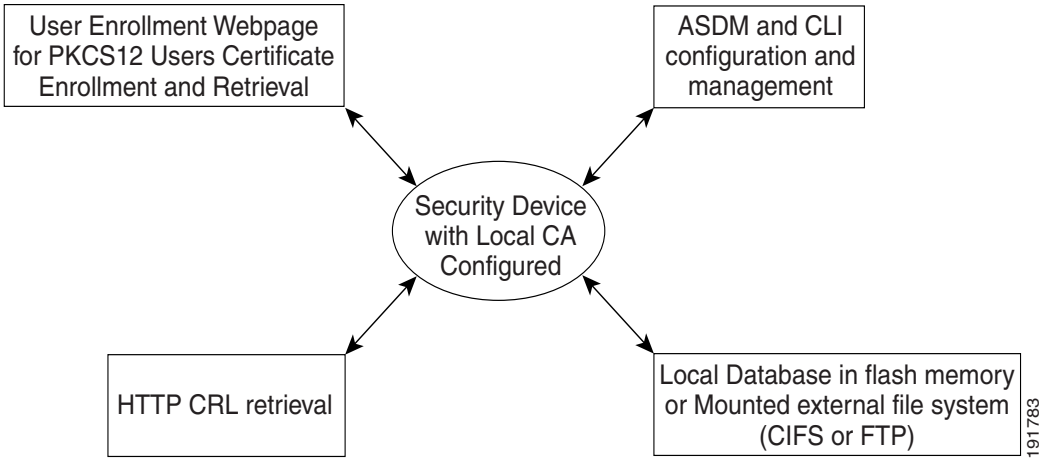
可存储在本地 CA 用户数据库中的用户数不受限制；但是，如果出现闪存存储问题，将生成系统日志以提示管理员采取行动，并且本地 CA 可能会禁用，直到存储问题得到解决。闪存可存储不超过 3500 个用户的数据库；但如果数据库的用户数超过 3500，则需要外部存储器。

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 20-1　　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+QG5vG515Hi5imwtYfaWwPEdPQxaWZ
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
```

添加或安装 CA 证书

要添加或安装 CA 证书，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Remote Access VPN > Certificate Management > CA Certificates**。

步骤 2　点击**添加**。

系统将显示 **Install Certificate** 对话框。

步骤 3　点击 **Install from a file** 单选按钮以从现有文件添加证书配置 （这是默认设置）。

步骤 4　输入路径和文件名，或点击 **Browse** 以搜索文件。然后，点击 **Install Certificate**。

步骤 5　系统将显示 **Certificate Installation** 对话框，其中包含一条指示证书已安装成功的消息。点击 **OK** 以关闭此对话框。

步骤 6　点击 **Paste certificate in PEM format** 单选按钮以手动注册。

步骤 7　将 PEM 格式 （base64 或十六进制）证书复制并粘贴到提供的区域中，然后点击 **Install Certificate**。

步骤 8　系统将显示 **Certificate Installation** 对话框，其中包含一条指示证书已安装成功的消息。点击 **OK** 以关闭此对话框。

步骤 9　点击 **Use SCEP** 单选按钮以自动注册。ASA 使用 SCEP 联系 CA，获取证书并在设备上安装这些证书。要使用 SCEP，您必须向支持 SCEP 的 CA 注册，并且必须通过互联网注册。使用 SCEP 自动注册要求提供以下信息：

- 要自动安装的证书的路径和文件名。
- 重试证书安装的最大分钟数。默认值为一分钟。
- 安装证书的重试次数。默认值为零，表示在重试期间重试次数无限制。

步骤 10　点击 **More Options** 以显示新证书和现有证书的其他配置选项。

系统将显示 **Configuration Options for CA Certificates** 窗格。

步骤 11　要更改现有 CA 证书配置，请选择该配置，然后点击 **Edit**。

步骤 12　要删除 CA 证书配置，请选择该配置，然后点击 **Delete**。

注意　删除证书配置后，无法将其恢复。要重新创建已删除的证书，请点击 **Add** 以重新输入所有证书配置信息。

步骤 13　点击 **Show Details** 以显示 **Certificate Details** 对话框，其中包含以下三个仅作显示用途的选项卡：

- **General** 选项卡显示类型、序列号、状态、用法、公钥类型、 CRL 分发点、证书有效期和关联信任点等值。这些值同时适用于可用和暂停状态。
- **Issued to** 选项卡显示使用者 DN 或证书所有者的 X.500 字段及其值。这些值仅适用于可用状态。
- **Issued by** 选项卡显示授予证书的实体的 X.500 字段。这些值仅适用于可用状态。

配置 CA 证书吊销检查

要配置 CA 证书吊销检查，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add** 以显示 **Install Certificates** 对话框。然后，点击 **More Options**。

步骤 2　点击 **Revocation Check** 选项卡。

步骤 3　点击 **Do not check certificates for revocation** 单选按钮以禁用证书的吊销检查。

步骤 4　点击 **Check certificates for revocation** 单选按钮以选择一个或多个吊销检查方法 （CRL 或 OCSP）。

步骤 5　点击 **Add** 可将某个吊销方法移至右侧，将其变为可用。点击 **Move Up** 或 **Move Down** 可更改方法顺序。

您选择的方法按照其添加顺序进行执行。如果某个方法返回错误，则会激活下一个吊销检查方法。

步骤 6　选中 **Consider certificate valid if revocation checking returns errors** 复选框以在证书验证过程中忽略吊销检查错误。

步骤 7　点击 **OK** 以关闭 **Revocation Check** 选项卡。

配置 CRL 检索策略

要配置 CRL 检索策略，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add** 以显示 **Install Certificates** 对话框。然后，点击 **More Options**。

步骤 2　选中 **Use CRL Distribution Point from the certificate** 复选框以将吊销检查从正在检查的证书定向至 CRL 分发点。

步骤 3　选中 **Use Static URLs configured below** 复选框以列出要用于 CRL 检索的特定 URL。您选择的 URL 按照其添加顺序进行实施。如果指定的 URL 发生错误，则顺序采用下一个 URL。

步骤 4　点击 Static Configuration 区域中的 **Add** 。

系统将显示 **Add Static URL** 对话框。

步骤 5　输入用于分发 CRL 的静态 URL，然后点击 **OK**。

输入的 URL 将显示在 Static URL 列表中。

步骤 6　点击 **OK** 以关闭此对话框。

配置 CRL 检索方法

要配置 CRL 检索方法，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add** 以显示 **Install Certificates** 对话框。然后，点击 **More Options**。

步骤 2　点击 **Configuration Options for CA Certificates** 窗格中的 **CRL Retrieval Methods** 选项卡。

步骤 3　选择以下三种检索方法的其中一种：

- 要启用 LDAP 进行 CRL 检索，请选中 **Enable Lightweight Directory Access Protocol (LDAP)** 复选框。通过 LDAP，CRL 检索通过连接到使用密码进行访问的已命名 LDAP 服务器来启动 LDAP 会话。默认情况下，连接位于 TCP 端口 389 上。输入以下必需参数：
  - **Name**
  - **Password**
  - **Confirm Password**
  - **Default Server**（服务器名称）
  - **Default Port** (389)
- 要启用 HTTP 以进行 CRL 检索，请选中 **Enable HTTP** 复选框。

步骤 4　点击 **OK** 以关闭此选项卡。

配置 OCSP 规则

本节介绍如何配置 OSCP 规则。

准备工作

确保您已在尝试添加 OCSP 规则之前配置证书映射。如果尚未配置证书映射，系统将显示错误消息。

要配置 OCSP 规则以获取 X.509 数字证书的吊销状态，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add** 以显示 **Install Certificates** 对话框。然后，点击 **More Options**。

步骤 2　点击 **Configuration Options for CA Certificates** 窗格中的 **OCSP Rules** 选项卡。

步骤 3　选择要匹配此 OCSP 规则的证书映射。证书映射会将用户权限与证书中的特定字段进行匹配。ASA 用于验证响应方证书的 CA 的名称显示在 **Certificate** 字段中。规则的优先级编号显示在 **Index** 字段中。此证书的 OCSP 服务器的 URL 显示在 **URL** 字段中。

步骤 4　点击**添加**。

系统将显示 **Add OCSP Rule** 对话框。

步骤 5　从下拉列表中选择要使用的证书映射。

步骤 6　从下拉列表中选择要使用的证书。

步骤 7　输入规则的优先级编号。

步骤 8　输入此证书的 OCSP 服务器的 URL。

步骤 9　完成后，点击 **OK** 以关闭此对话框。

新添加的 OCSP 规则将显示在列表中。

步骤 10　点击 **OK** 以关闭此选项卡。

配置高级 CRL 和 OCSP 设置

要配置其他 CRL 和 OCSP 设置，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add** 以显示 **Install Certificates** 对话框。然后，点击 **More Options**。

步骤 2　点击 **Configuration Options for CA Certificates** 窗格中的 **Advanced** 选项卡。

步骤 3　在 **CRL Options** 区域中输入缓存刷新间隔的分钟数。默认值为 60 分钟。范围为 1 至 1440 分钟。为避免必须从 CA 重复检索相同的 CRL， ASA 可将检索到的 CRL 存储在本地，这称为 CRL 缓存。CRL 缓存容量根据平台而异，并且是跨所有情景的累积容量。如果尝试缓存新检索的 CRL 会超出其容量限制，则 ASA 将删除最近最少使用的 CRL，直到更多空间可供使用。

步骤 4　选中 **Enforce next CRL update** 复选框可要求有效的 CRL 具有未到期的 Next Update 值。取消选中 **Enforce next CRL update** 复选框可允许有效的 CRL 没有 Next Update 值或具有已到期的 Next Update 值。

步骤 5　在 **OCSP Options** 区域中输入 OCSP 服务器的 URL。ASA 根据以下顺序使用 OCSP 服务器：

1. 匹配证书覆盖规则中的 OCSP URL
2. 选定 OCSP Options 属性中配置的 OCSP URL
3. 用户证书的 AIA 字段

步骤 6　默认情况下， **Disable nonce extension** 复选框处于选中状态，从而以加密方式将请求与响应绑定来避免重放攻击。此过程适用是由于通过将请求中的扩展与响应中的扩展进行匹配，从而确保其相同。如果您所使用的 OCSP 服务器发送的是不包含此匹配随机数扩展的预生成响应，请取消选中 **Disable nonce extension** 复选框。

步骤 7　在 **Other Options** 域中，选择以下其中一个选项：

- 选中 **Accept certificates issued by this CA** 复选框以指示 ASA 应接受来自指定 CA 的证书。
- 选中 **Accept certificates issued by the subordinate CAs of this CA** 复选框以指示 ASA 应接受来自从属 CA 的证书。

步骤 8　点击 **OK** 以关闭此选项卡，然后点击 **Apply** 以保存配置更改。

添加或导入身份证书

要添加或导入新的身份证书配置，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Remote Access VPN > Certificate Management > Identity Certificates**。

步骤 2　点击**添加**。

系统将显示 **Add Identity Certificate** 对话框，其中选定信任点名称显示在顶部。

步骤 3　点击 **Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)** 单选按钮以从现有文件导入身份证书。

步骤 4　输入用于解密 PKCS12 文件的密码。

步骤 5　输入文件的路径名称，或点击 **Browse** 以显示 **Import ID Certificate File** 对话框。查找证书文件，然后点击 **Import ID Certificate File**。

步骤 6　点击 **Add a new identity certificate** 单选按钮以添加新的身份证书。

步骤 7　点击 **New** 以显示 **Add Key Pair** 对话框。

步骤 8　选择 **RSA** 或 **ECDSA** 密钥类型。

步骤 9　点击 **Use default keypair name** 单选按钮以使用默认密钥对名称。

步骤 10　点击 **Enter a new key pair name** 单选按钮，然后输入新名称。ASA 支持多个密钥对。

步骤 11　从下拉列表中选择模数长度。如果不确定模数长度，请向 Entrust 查询。

步骤 12　通过点击 **General purpose** 单选按钮 （默认）或 **Special** 单选按钮选择密钥对用法。选中 **Special** 单选按钮时， ASA 将生成两个密钥对，一个用于签名，一个用于加密。此选择表示对应的身份需要两个证书。

步骤 13　点击 **Generate Now** 以创建新密钥对，然后点击 **Show** 以显示 **Key Pair Details** 对话框，其中包含以下仅作显示用途的信息：

- 要认证其公钥的密钥对的名称。
- 生成密钥对的时间和日期。
- RSA 密钥对的用法。
- 密钥对的模数长度 （位）：512、 768、 1024 和 2048。默认值为 1024。
- 密钥数据，其中包含文本格式的特定密钥数据。

步骤 14　完成后点击 **OK**。

步骤 15　选择证书使用者 DN 以生成身份证书中的 DN，然后点击 **Select** 以显示 **Certificate Subject DN** 对话框。

步骤 16　从下拉列表中选择一个或多个要添加的 DN 属性，输入一个值，然后点击 **Add**。Certificate Subject DN 的可用 X.500 属性如下：

- **Common Name (CN)**
- **Department (OU)**
- **Company Name (O)**
- **Country (C)**
- **State/Province (ST)**
- **Location (L)**
- **E-mail Address (EA)**

步骤 17　完成后点击 **OK**。

步骤 18　选中 **Generate self-signed certificate** 复选框以创建自签名证书。

步骤 19　选中 **Act as local certificate authority and issue dynamic certificates to TLS proxy** 复选框以将身份证书作为本地 CA。

步骤 20　点击 **Advanced** 以建立其他身份证书设置。

系统将显示 **Advanced Options** 对话框，其中包含以下三个选项卡：**Certificate Parameters**、**Enrollment Mode** 和 **SCEP Challenge Password**。

注意　注册模式设置和 SCEP 质询密码对于自签名证书不可用。

步骤 21　点击 **Certificate Parameters** 选项卡，然后输入以下信息：

- FQDN，一个明确的域名，用于指示 DNS 树状层次结构中的节点位置。
- 与身份证书关联的邮件地址。
- 网络中的 ASA IP 地址，采用由四部分组成的点分十进制表示法。
- 选中 **Include serial number of the device** 复选框以将 ASA 序列号添加到证书参数。

步骤 22　点击 **Enrollment Mode** 选项卡，然后输入以下信息：

- 通过点击 **Request by manual enrollment** 单选按钮或 **Request from a CA** 单选按钮选择注册方法。
- 要通过 SCEP 自动安装的证书的注册 URL。
- 允许重试安装身份证书的最大分钟数。默认值为一分钟。
- 允许安装身份证书的最大重试次数。默认值为零，表示在重试期间重试次数无限制。

步骤 23　点击 **SCEP Challenge Password** 选项卡，然后输入以下信息：

- SCEP 密码
- SCEP 密码确认

步骤 24　完成后点击 **OK**。

步骤 25　点击 **Add Identity Certificate** 对话框中的 **Add Certificate**。

新身份证书将显示在 Identity Certificates 列表中。

步骤 26　点击 **Apply** 以保存新身份证书配置。

步骤 27　点击 **Show Details** 以显示 **Certificate Details** 对话框，其中包含以下三个仅作显示用途的选项卡：

- **General** 选项卡显示类型、序列号、状态、用法、公钥类型、 CRL 分发点、证书有效期和关联信任点等值。这些值同时适用于可用和暂停状态。
- **Issued to** 选项卡显示使用者 DN 或证书所有者的 X.500 字段及其值。这些值仅适用于可用状态。
- **Issued by** 选项卡显示授予证书的实体的 X.500 字段。这些值仅适用于可用状态。

步骤 28　要删除身份证书配置，请选择该配置，然后点击 **Delete**。

注意　删除证书配置后，无法将其恢复。要重新创建已删除的证书，请点击 **Add** 以重新输入所有证书配置信息。

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。

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。

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。

操作步骤

步骤 1　依次浏览至 **Configuration > Device Management > Certificate Management > Identity Certificate/CA Certificate**。

步骤 2　选中 **Enable Certificate Expiration Alert** 复选框。

步骤 3　填写所需的天数：

- Send the first alert before - 配置将发出第一个提醒时的到期前天数 （1 至 90）。
- Repeat the alert for - 配置未续签证书时的提醒频率 （1 至 14 天）。默认情况下，在到期前 60 天发送第一个提醒，此后每周发送一次提醒，直至续签并删除证书。此外，系统会在到期当日发送提醒，此后每天发送一次提醒，并且无论提醒如何配置，都会在到期前的最后一周内每天发送提醒。

导出身份证书

要导出身份证书，请执行以下步骤：

操作步骤

步骤 1　点击 **Export** 以显示 **Export Certificate** 对话框。

步骤 2　输入要用于导出证书配置的 PKCS12 格式文件的名称。或者，点击 **Browse** 以显示 **Export ID Certificate File** 对话框，以便查找要向其导出证书配置的文件。

步骤 3　通过点击 **PKCS12 Format** 单选按钮或 **PEM Format** 单选按钮选择证书格式。

步骤 4　输入用于加密要导出的 PKCS12 文件的密码。

步骤 5　确认加密密码。

步骤 6　点击 **Export Certificate** 以导出证书配置。

系统将显示一个信息对话框，通知您证书配置文件已成功导出到指定的位置。

生成证书签名请求

要生成将发送到 Entrust 的证书签名请求，请执行以下步骤：

操作步骤

步骤 1　点击 **Enroll ASA SSL VPN with Entrust** 以显示 **Generate Certificate Signing Request** 对话框。

步骤 2　在 **Key Pair** 区域中执行以下步骤：

a. 从下拉列表中选择其中一个配置的密钥对。

b. 点击 **Show** 以显示 **Key Details** 对话框，其中提供有关选定密钥对的信息，包括生成日期和时间、用法 （通用或特殊用法）、模数长度和密钥数据。

c. 完成后点击 **OK**。

d. 点击 **New** 以显示 **Add Key Pair** 对话框。生成密钥对后，您可以将其发送到 ASA 或将其保存到文件中。

步骤 3　在 **Certificate Subject DN** 区域中输入以下信息：

a. ASA 的 FQDN 或 IP 地址。

b. 公司名称。

c. 两个字母的国家/地区代码。

步骤 4　在 **Optional Parameters** 区域中执行以下步骤：

a. 点击 **Select** 以显示 **Additional DN Attributes** 对话框。

b. 从下拉列表中选择要添加的属性，然后输入值。

c. 点击 **Add** 以将每个属性添加到属性表中。

d. 点击 **Delete** 以从属性表中删除属性。

e. 完成后点击 **OK**。

添加的属性将显示在 **Additional DN Attributes** 字段中。

步骤 5　如果 CA 需要，请输入其他完全限定域名信息。

步骤 6　点击 **Generate Request** 以生成证书签名请求，之后可将其发送到 Entrust，或保存到文件中稍后发送。

系统将显示 **Enroll with Entrust** 对话框，其中显示了 CSR。

步骤 7　通过点击 **request a certificate from Entrust** 链接完成注册过程。然后，复制并粘贴所提供的 CSR 且通过 http://www.entrust.net/cisco/ 上提供的 Entrust Web 表单将其提交。或者，如果要稍后注册，请将生成的 CSR 保存到文件中，然后点击 **Identity Certificates** 窗格上的 **enroll with Entrust** 链接。

步骤 8　Entrust 将在验证请求的真实性后颁发证书，这可能需要几天时间。然后，您需要通过在 **Identity Certificate** 窗格中选择待处理的请求并点击 **Install** 来安装证书。

步骤 9　点击 **Close** 以关闭 **Enroll with Entrust** 对话框。

安装身份证书

要安装新的身份证书，请执行以下步骤：

操作步骤

步骤 1　在 **Identity Certificates** 窗格中点击 **Add** 以显示 **Add Identity Certificate** 对话框。

步骤 2　点击 **Add a new identity certificate** 单选按钮。

步骤 3　更改密钥对或创建新的密钥对。密钥对是必需的。

步骤 4　输入证书使用者 DN 信息，然后点击 **Select** 以显示 **Certificate Subject DN** 对话框。

步骤 5　指定相关 CA 所需的所有使用者 DN 属性，然后点击 **OK** 以关闭 **Certificate Subject DN** 对话框。

步骤 6　在 **Add Identity Certificate** 对话框中，点击 **Advanced** 以显示 **Advanced Options** 对话框。

步骤 7　要继续，请参阅添加或导入身份证书，第 20-14 页中的第 17 至 23 步。

步骤 8　在 **Add Identity Certificate** 对话框中，点击 **Add Certificate**。

系统将显示 **Identity Certificate Request** 对话框。

步骤 9　输入 CSR 文本文件的文件名，例如 c:\verisign-csr.txt，然后点击 **OK**。

步骤 10　将 CSR 文本文件发送到 CA。或者，您也可以将该文本文件粘贴到 CA 网站上的 CSR 注册页面中。

步骤 11　当 CA 将身份证书返回给您时，请转至 **Identity Certificates** 窗格，选择待处理的证书条目，然后点击 **Install**。

系统将显示 **Install Identity Certificate** 对话框。

步骤 12　通过点击适用的单选按钮，选择以下其中一个选项：

- **Install from a file**。

  或者，点击 **Browse** 以搜索文件。

- **Paste the certificate data in base-64 format**。

  将复制的证书数据粘贴到提供的区域中。

步骤 13　点击 **Install Certificate**。

步骤 14　点击 **Apply** 以使用 ASA 配置保存新安装的证书。

步骤 15　要显示有关选定身份证书的详细信息，请点击 **Show Details** 以显示 **Certificate Details** 对话框，其中包含以下三个仅作显示用途的选项卡：

- **General** 选项卡显示类型、序列号、状态、用法、公钥类型、 CRL 分发点、证书有效期和关联信任点等值。这些值同时适用于可用和暂停状态。
- **Issued to** 选项卡显示使用者 DN 或证书所有者的 X.500 字段及其值。这些值仅适用于可用状态。
- **Issued by** 选项卡显示授予证书的实体的 X.500 字段。这些值仅适用于可用状态。

步骤 16　要删除代码签名者证书配置，请选择该配置，然后点击 **Delete**。

注意　删除证书配置后，无法将其恢复。要重新创建已删除的证书，请点击 **Import** 以重新输入所有证书配置信息。

导入代码签名者证书

要导入代码签名者证书，请执行以下步骤：

操作步骤

步骤 1　在 **Code Signer** 窗格中，点击 **Import** 以显示 **Import Certificate** 对话框。

步骤 2　输入用于解密 PKCS12 格式文件的密码。

步骤 3　输入要导入的文件的名称，或点击 **Browse** 以显示 **Import ID Certificate File** 对话框并搜索文件。

步骤 4　选择要导入的文件并点击 **Import ID Certificate File**。

选定证书文件将显示在 **Import Certificate** 对话框中。

步骤 5　点击 **Import Certificate**。

导入的证书将显示在 **Code Signer** 窗格中。

步骤 6　点击 **Apply** 以保存新导入的代码签名者证书配置。

导出代码签名者证书

要导出代码签名者证书，请执行以下步骤：

操作步骤

步骤 1　在 **Code Signer** 窗格中，点击 **Export** 以显示 **EXport Certificate** 对话框。

步骤 2　输入要用于导出证书配置的 PKCS12 格式文件的名称。

步骤 3　在 **Certificate Format** 区域中，要使用公钥加密标准 （可以是 base64 编码或十六进制格式），请点击 **PKCS12 format** 单选按钮。否则，请点击 **PEM format** 单选按钮。

步骤 4　点击 **Browse** 以显示 **Export ID Certificate File** 对话框，以便查找要向其导出证书配置的文件。

步骤 5　选择文件并点击 **Export ID Certificate File**。

选定证书文件将显示在 **Export Certificate** 对话框中。

步骤 6　输入用于解密要导出的 PKCS12 格式文件的密码。

步骤 7　确认解密密码。

步骤 8　点击 **Export Certificate** 以导出证书配置。

配置本地 CA 服务器

要在 ASA 上配置本地 CA 服务器，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server**。

步骤 2　要激活本地 CA 服务器，请选中 **Enable Certificate Authority Server** 复选框。默认设置处于禁用状态 （未选中）。启用本地 CA 服务器后， ASA 将生成本地 CA 服务器证书、密钥对和必要的数据库文件，然后将本地 CA 服务器证书和密钥对存档在 PKCS12 文件中。

注意　启用配置的本地 CA 之前，请务必仔细检查所有可选设置。启用后，证书颁发者名称和密钥长度等服务器值不能更改。

自签名证书密钥用法扩展可启用密钥加密、密钥签名、 CRL 签名和证书签名功能。

步骤 3　第一次启用本地 CA 时，您必须输入并确认字母数字启用密码，该密码必须具有至少七个字母数字字符。该密码可保护存档在存储器中的本地 CA 证书和本地 CA 证书密钥对，并防止擅自关闭或意外关闭本地 CA 服务器。如果本地 CA 证书或密钥对丢失且必须恢复，则必需该密码才能解锁 PKCS12 存档。

注意　必需此启用密码才能启用本地 CA 服务器。请务必将启用密码保存在安全位置。

步骤 4　点击 **Apply** 以保存本地 CA 证书和密钥对，使得配置在重新启动 ASA 时不会丢失。

步骤 5　要在第一次配置本地 CA 后更改或重新配置本地 CA，您必须通过取消选中 **Enable Certificate Authority Server** 复选框来关闭 ASA 上的本地 CA 服务器。在此状态下，配置和所有关联文件保留在存储器中，并且注册处于禁用状态。

启用已配置的本地 CA 后，以下两项设置仅作显示用途：

- **Issuer Name** 字段，用于列出颁发者名称和使用者名称以及域名，并且是将 username 和 subject-name-default DN 设置用作 cn=FQDN 生成的。本地 CA 服务器是授予证书的实体。默认证书名称以 cn=hostname.domainname 格式提供。
- **CA Server Key Size** 设置，用于为本地 CA 服务器生成的服务器证书。密钥长度可以是每个密钥 512、768、1024 或 2048 位。默认值为每个密钥 1024 位。我们建议您使用至少为 2048 位的密钥长度。

步骤 6　从下拉列表中，选择要为每个由本地 CA 服务器颁发的用户证书生成的密钥对的客户端密钥长度。密钥长度可以是每个密钥 512、768、1024 或 2048 位。默认值为每个密钥 1024 位。我们建议您使用至少为 2048 位的密钥长度。

步骤 7　输入 CA 证书有效期值，该值指定 CA 服务器证书有效的天数。默认值为 3650 天（10 年）。确保将证书的有效期限制为不超过建议的结束日期， 2038 年 1 月 19 日凌晨 3:14:08 (UTC)。

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，以在证书过期后对由本地 CA 颁发的用户证书进行本地 CA 证书验证。

要通知用户即将到期，在 **Latest ASDM Syslog Messages** 窗格中会显示以下系统日志消息：

```
%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，管理员必须采取行动以确保新的本地 CA 证书在到期前已导入到所有必要的设备上。

步骤 8　输入客户端证书有效期值，该值指定由 CA 服务器颁发的用户证书有效的天数。默认值为 365 天（一年）。确保将证书的有效期限制为不超过建议的结束日期， 2038 年 1 月 19 日凌晨 3:14:08 (UTC)。

步骤 9　通过在 **SMTP Server & Email Settings** 区域中指定以下设置，为本地 CA 服务器设置邮件访问：

a. 输入 SMTP 邮件服务器名称或 IP 地址。或者，点击省略号 (...) 以显示 **Browse Server Name/IP Address** 对话框，您可在其中选择服务器名称或 IP 地址。完成后点击 **OK**。

b. 输入 “adminname@hostname.com”格式的发件人地址，从该地址将邮件发送到本地 CA 用户。自动邮件可将一次性密码发送给新注册的用户，并在需要续签或更新证书时发出邮件。

c. 输入主题，它指定由本地 CA 服务器发送给用户的所有邮件中的主题行。如果未指定主题，则默认为 “Certificate Enrollment Invitation”。

步骤 10　点击 **More Options** 下拉箭头以配置其他选项。

步骤 11　输入 CRL 分发点，它是 ASA 上的 CRL 位置。默认位置为 http://hostname.domain/+CSCOCA+/asa_ca.crl。

步骤 12　要使 CRL 可供在给定接口或端口上进行 HTTP 下载，请从下拉列表中选择 publish-CRL 接口，然后，输入端口号，可以是 1 至 65535 之间的任意端口号。默认端口号为 TCP 端口 80。

注意　无法重命名 CRL；其名称始终为 LOCAL-CA-SERVER.crl。

例如，输入 URL，http://10.10.10.100/user8/my_crl_file。 在这种情况下，只有带指定 IP 地址的接口才有效，当请求传入时， ASA 会将路径 /user8/my_crl_file 与配置的 URL 进行匹配。如果路径匹配， ASA 将返回存储的 CRL 文件。

步骤 13　以小时为单位输入 CRL 的有效期。CA 证书的默认有效期为六小时。

本地 CA 将在每次吊销或取消吊销用户证书时更新和重新发出 CRL，但如果未发生吊销变更，则会在每个 CRL 有效期到期后重新发出一次 CRL。您可以通过点击 **CA Certificates** 窗格中的 **Request CRL** 强制立即更新和重新生成 CRL。

步骤 14　输入数据库存储位置，以指定本地 CA 配置和数据文件的存储区域。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。或者，要指定外部文件，请输入外部文件的路径名称或点击 **Browse** 以显示 **Database Storage Location** 对话框。

步骤 15　从显示的文件夹列表中选择存储位置，然后点击 **OK**。

注意　闪存可存储不超过 3500 个用户的数据库；如果数据库的用户数超过 3500，则需要外部存储器。

步骤 16　输入默认使用者 （DN 字符串）以附加到已颁发证书上的用户名中。以下列表中提供了允许的 DN 属性：

- **CN （公用名）**
- **SN （姓氏）**
- **O （组织名称）**
- **L （地区）**
- **C （国家/地区）**

- **OU （组织单位）**
- **EA （邮件地址）**
- **ST （省/自治区/直辖市）**
- **T （职务）**

步骤 17　以小时为单位输入已注册的用户可以检索 PKCS12 注册文件以注册和检索用户证书的时间长度。注册期与一次性密码 (OTP) 有效期无关。默认值为 24 小时。

注意　只有无客户端 SSL VPN 连接支持本地 CA 的证书注册。对于此类型的连接，客户端与 ASA 之间的通信通过使用标准 HTML 的 Web 浏览器进行。

步骤 18　输入以邮件形式发送给注册用户的一次性密码有效的时间长度。默认值为 72 小时，然后点击 **Email OTP**。

系统将显示 **Information** 对话框，指示 OTP 已发送给新用户。

请点击 **Replace OTP**，以自动重新颁发新的 OTP，并将包含新密码的邮件通知发送给现有用户或新用户。

要查看或重新生成 OTP，请从列表中选择一个用户，然后点击 **View/Regenerate OTP** 以显示 **View & Regenerate OTP** 对话框。

系统将显示当前 OTP。

点击 **Regenerate OTP**。

系统将显示重新生成的 OTP。

步骤 19　点击 **OK**。

步骤 20　输入向用户发送提醒邮件时距到期的天数。默认时间为 14 天。

步骤 21　点击 **Apply** 以保存新的或已修改的 CA 证书配置。

要从 ASA 中删除本地 CA 服务器，请点击 **Delete Certificate Authority Server** 以显示 **Delete Certificate Authority** 对话框。点击 **OK**。

注意　删除本地 CA 服务器后，将无法恢复或还原。要重新创建已删除的 CA 服务器配置，您必须重新输入所有 CA 服务器配置信息。

添加本地 CA 用户

要添加本地 CA 用户，请执行以下步骤：

操作步骤

步骤 1　要将新用户输入到本地 CA 数据库，请点击 **Add** 以显示 **Add User** 对话框。

步骤 2　输入有效的用户名。

步骤 3　输入现有有效邮件地址。

步骤 4　输入使用者 （DN 字符串）。或者，点击 **Select** 以显示 **Certificate Subject DN** 对话框。

步骤 5　从下拉列表中选择一个或多个要添加的 DN 属性，输入一个值，然后点击 **Add**。Certificate Subject DN 的可用 X.500 属性如下：

- **Common Name (CN)**
- **Department (OU)**
- **Company Name (O)**
- **Country (C)**
- **State/Province (ST)**
- **Location (L)**
- **E-mail Address (EA)**

步骤 6　完成后点击 **OK**。

步骤 7　选中 **Allow enrollment** 复选框以注册用户，然后点击 **Add User**。

新用户将显示在 **Manage User Database** 窗格中。

编辑本地 CA 用户

要修改有关数据库中现有本地 CA 用户的信息，请执行以下步骤：

步骤 1　选择特定用户并点击 **Edit** 以显示 **Edit User** 对话框。

步骤 2　输入有效的用户名。

步骤 3　输入现有有效邮件地址。

步骤 4　输入使用者 （DN 字符串）。或者，点击 **Select** 以显示 **Certificate Subject DN** 对话框。

步骤 5　从下拉列表中选择一个或多个要更改的 DN 属性，输入一个值，然后点击 **Add** 或 **Delete**。

步骤 6　完成后点击 **OK**。

要从数据库中删除用户并从本地 CA 数据库中删除颁发给该用户的任何证书，请选择该用户，然后点击 **Delete**。

注意　无法恢复已删除的用户。要重新创建已删除的用户记录，请点击 **Add** 以重新输入所有用户信息。

步骤 7　选中 **Allow enrollment** 复选框以重新注册用户，然后点击 **Edit User**。

注意　如果用户已注册，系统会显示一条错误消息。

已更新的用户详细信息将显示在 **Manage User Database** 窗格中。

管理用户证书

要更改证书状态，请执行以下步骤：

操作步骤

步骤 1　在 **Manage User Certificates** 窗格中按用户名或按证书序列号选择特定证书。

步骤 2　选择以下选项之一：

- 如果用户证书有效期到期，请点击 **Revoke** 以删除用户访问。本地 CA 还会在证书数据库中将证书标记为已吊销，自动更新信息并重新发出 CRL。
- 选择已吊销证书并点击 **Unrevoke** 以恢复访问。本地 CA 还会在证书数据库中将证书标记为未吊销，自动更新证书信息并重新发出已更新的 CRL。

步骤 3　完成后点击 **Apply** 以保存更改。

监控数字证书

请参阅以下用于监控数字证书状态的屏幕：

- **Monitoring > Properties > CRL**

  此窗格显示 CRL 详细信息。

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

证书管理历史记录

表 20-1　　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。 引入了以下屏幕： Configuration > Remote Access VPN > Certificate Management Configuration > Site-to-Site VPN > Certificate Management。 引入或修改了以下屏幕： Configuration > Firewall > Advanced > Certificate Management > CA Certificates Configuration > Device Management > Certificate Management > CA Certificates。
证书管理	7.2(1)	
证书管理	8.0(2)	
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。

第 5 部分

IP 路由

路由概述

本章介绍有关路由如何在思科 ASA 内部运行的基本概念以及支持的路由协议。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

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

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 21-3 页
- 下一跳选择过程，第 21-3 页
- ECMP 路由，第 21-4 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 27-3 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 26-5 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 25-3 页。

路由表

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 21-1 显示 ASA 支持的路由协议的默认管理距离值。

表 21-1　　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　依次选择 **Configuration > Device Setup > Routing > Proxy ARP/Neighbor Discovery**。

Interface 字段会列出接口名称。**Enabled** 字段显示对于 NAT 全局地址是启用 (Yes) 还是禁用 (No) 代理 ARP/邻居发现。

步骤 2　要为选定接口启用代理 ARP/邻居发现，请点击 **Enable**。默认情况下，将为所有接口启用代理 ARP/邻居发现。

步骤 3　要为选定接口上禁用代理 ARP/邻居发现，请点击 **Disable**。

步骤 4　点击 **Apply** 以将设置保存到运行配置。

显示路由表

操作步骤

步骤 1　要在 ASDM 中显示路由表中的所有路由，请依次选择 **Monitoring > Routing > Routes**。

在此窗格中，每一行代表一条路由。

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

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

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 21-4 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 21-4 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 22-3 页
- 配置静态路由，第 22-4 页
- 跟踪静态路由，第 22-5 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，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　依次选择 **Configuration > Device Setup > Routing > Static Routes**，然后点击 **Add**。

步骤 2　选择 **IP Address Type**、 **IPv4** 或 **IPv6**。

步骤 3　选择要通过其发送流量的 **Interface**。

步骤 4　对于 **Network**，输入 **any4** 或 **any6**，具体取决于类型。

步骤 5　输入发送流量所在的 **Gateway IP**。

步骤 6　设置 **Metric** 以设置路由的管理距离。

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。

步骤 7　（可选）在 **Options** 区域中，设置以下选项：

- **Tunneled** - 您可以为隧道流量定义单独的默认路由以及标准默认路由。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。
- **Tracked** - （仅限 IPv4）有关跟踪路由的信息，请参阅跟踪静态路由，第 22-5 页。

步骤 8　点击 **OK**。

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　依次选择 **Configuration > Device Setup > Routing > Static Routes**，然后点击 **Add**。

步骤 2　选择 **IP Address Type**、 **IPv4** 或 **IPv6**。

步骤 3　选择要通过其发送流量的 **Interface**。要将不必要的流量转发到 “黑洞”，请选择 **Null0** 接口。

步骤 4　对于 **Network**，输入要为其路由流量的目标网络。

步骤 5　输入发送流量所在的 **Gateway IP**。

步骤 6　设置 **Metric** 以设置路由的管理距离。

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。

步骤 7　（可选）在 **Options** 区域中，设置以下选项：

- **Tunneled** - 您可以为隧道流量定义单独的默认路由以及标准默认路由。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。
- **Tracked** - （仅限 IPv4）有关跟踪路由的信息，请参阅跟踪静态路由，第 22-5 页。

步骤 8　点击 **OK**。

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

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 依次选择 **Configuration > Device Setup > Routing > Static Routes** 并根据配置静态路由，第 22-4 页添加或编辑静态路由。

步骤 2 点击 **Options** 区域中的 **Tracked** 单选按钮。

步骤 3 在 **Track ID** 字段中，为路由跟踪进程输入唯一标识符。

步骤 4 在 **Track IP Address/DNS Name** 字段中，输入被跟踪目标的 IP 地址或主机名。通常，这将是路由的下一跳网关的 IP 地址，但也可能是可以从该接口使用的任何网络对象。

步骤 5 在 **SLA ID** 字段中，为 SLA 监控进程输入唯一标识符。

步骤 6 （可选）点击 **Monitoring Options**。

系统将显示 **Route Monitoring Options** 对话框。从此处更改以下跟踪对象监控属性：

- **Frequency** - 设置 ASA 应测试跟踪目标是否存在的频率 （以秒为单位）。有效值的范围为 1 到 604800 秒。默认值为 60 秒。
- **Threshold** - 设置指示超过阈值事件的时间 （以毫秒为单位）。该值不能大于超时值。
- **Timeout** - 设置路由监控操作应等待来自请求数据包的响应的时间 （以毫秒为单位）。有效值的范围为 0 到 604800000 秒。默认值为 5000 毫秒。
- **Data Size** - 设置要在回应请求数据包中使用的数据负载的大小。默认值为 28。有效值范围为 0 到 16384。

  注意　此设置仅指定负载的大小；不指定整个数据包的大小。

- **ToS** - 设置回应请求的 IP 报头中服务类型字节的值。有效值范围为 0 至 255。默认值为 0。
- **Number of Packets** - 设置要为每个测试发送的回应请求数。有效值范围为 1 到 100。默认值为 1。

点击 **OK**。

步骤 7　点击 **OK** 以保存路由，然后点击 **Apply**。

一旦应用路由跟踪，监控进程随即开始。

步骤 8　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

- **Monitoring > Routing > Routes**。

  在 **Routes** 窗格中，每一行代表一个路由。您可以按 IPv4 连接和/或 IPv6 连接进行过滤。路由信息包括协议、路由类型、目标 IP 地址、子网掩码或前缀长度、网关 IP 地址、路由连接所通过的接口和管理距离。

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

ASDM 可向后兼容多个平台版本，因此此处未列出新增支持的具体 ASDM 版本。

表 22-1　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。 引入或修改了以下屏幕： **Configuration > Device Setup > Routing > Static Routes > Add Static Route** **Configuration > Device Setup > Routing > Static Routes > Add Static Route > Route Monitoring Options**
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)。 修改了以下屏幕： **Configuration > Device Setup > Routing > Static Routes > Add Static 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

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？

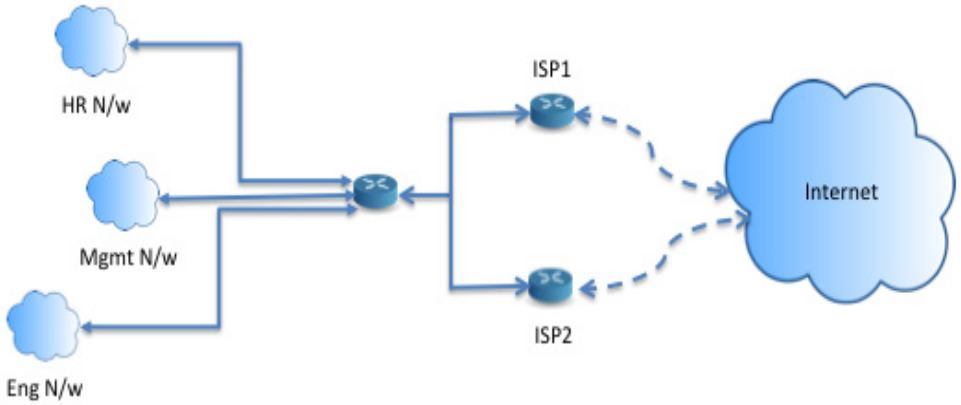
假设某公司在不同位置之间具有两个链路，一个是高带宽低延迟的昂贵链路，另一个是低带宽而延迟较高的价格更低廉链路。在使用传统路由协议时，依据带宽和/或延迟 （使用 EIGRP 或 OSPF）特征获取的节约指标，较高带宽链路会通过其发送的大部分流量。PBR 允许您通过高带宽/低延迟链路路由更高优先级的流量，并通过低带宽/高延迟链路发送所有其他流量。

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

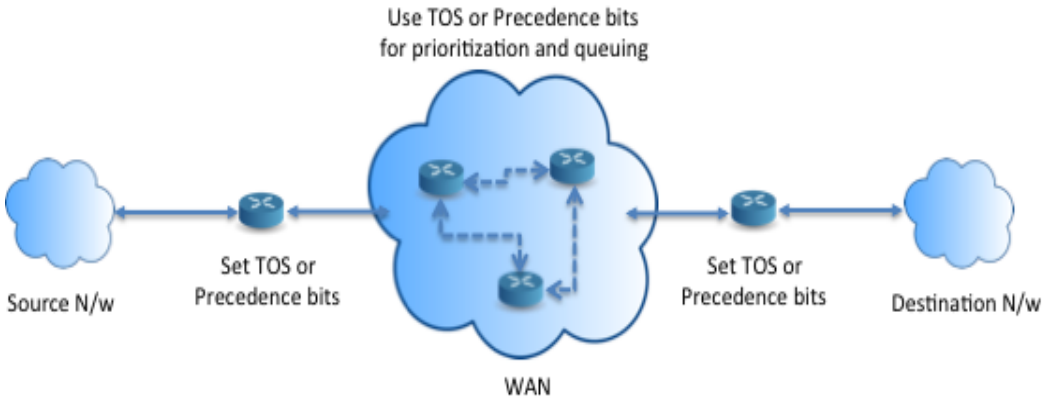
同等访问和基于源的路由

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。



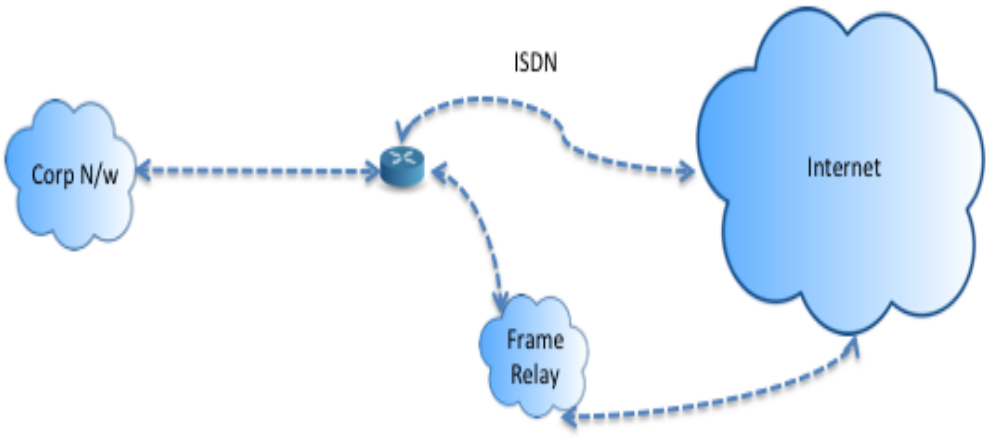
服务质量

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

不支持集群。

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > Route Maps**。

步骤 2　点击**添加**。

系统将显示 Add Route Map 或 Edit Route Map 对话框。

步骤 3　输入路由映射名称和序列号。路由映射名称是分配给特定路由的名称。序列号是在 ASA 中添加或删除路由映射条目的顺序。

注意　如果编辑一个现有路由映射，则已填写 Route Map Name 和 Sequence Number 字段。

步骤 4　要拒绝路由匹配重新分发，请点击 **Deny**。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。要允许重新分发路由匹配，请点击 **Permit**。如果在路由映射 permit 子句中使用 ACL，则会重新分发 ACL 允许的路由。

此外，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。

步骤 5　点击 **Match Clause** 选项卡以选择应将此子句应用到的路由，并设置以下参数：

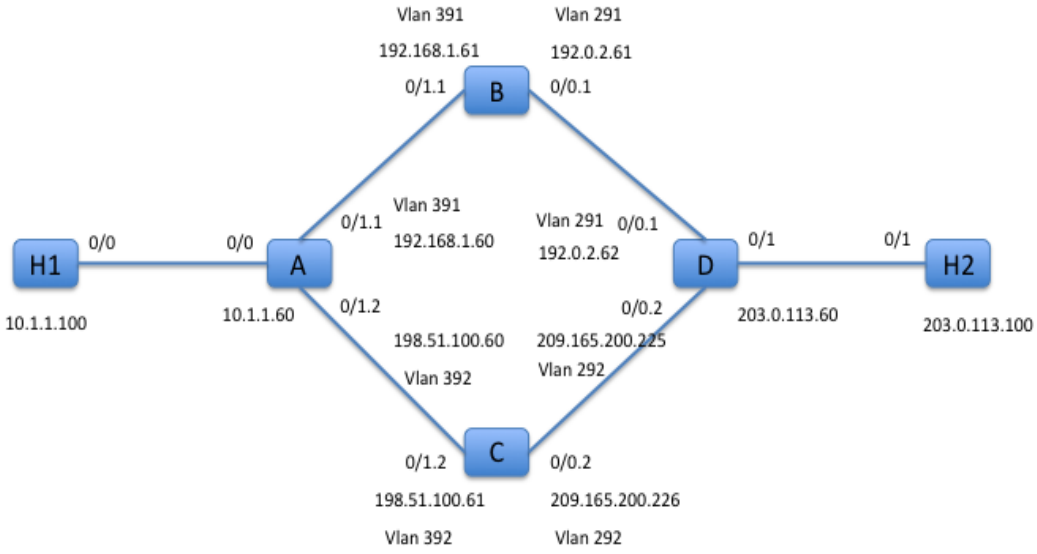
- 在 IPv4 和 IPv6 部分中，执行以下一个或多个操作，选择所需的 ACL 或前缀列表。

步骤 6　点击 **Policy Based Routing** 选项卡以定义流量的策略，并减少对派生自路由协议的路由的依赖。PBR 通过扩展和补充路由协议提供的现有机制来增强对路由的控制。PBR 允许您设置 IP 优先。它还允许为某些流量指定路径，例如高成本链路上的优先级流量。

- 选中 **Set default next-hop IP address** 复选框以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：在 **IPv4 Address** 中，输入目标地址。
- 选中 **Recursively find and set next-hop IP address** 复选框并在 **IPv4 Address** 字段中指定 IP 地址。在这种情况下，下一跳 IP 地址不需要位于直连子网上。
- 选中 **Verify the availability of the next hop IPv4 address** 复选框以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。此处创建了一个跟踪对象，以使用 ICMP 回显/回复来跟踪下一跳的可达性，并在下一跳不回复 ICMP 回显请求时将其标记为不可达。
  - 在 **IPv4 Address** 字段中，输入下一跳 IP 地址。
  - 在 **Sequence number** 字段和 **Track** 字段中，输入用于验证受跟踪对象的可达性的有效值。
- 选中 **Set interfaces** 复选框并从下拉列表中选择目标接口。

- 如果需要将流量完全转发到黑洞或丢弃，请选中 **Set null0 interface as the default interface** 复选框。
- 选中 **Set do-not-fragment bit to either 1or 0**，然后选择相应的单选按钮。
- 选中 **Set differential service code point (DSCP) value in QoS bits for IPv4 packets** 复选框，然后从 **IPv4 DSCP value** 下拉列表中选择值。

步骤 7　点击 **OK**。



基于策略的路由的历史记录

表 23-1　　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。 更新了以下屏幕：Configuration > Device Setup > Routing > Route Maps >Policy Based Routing，Configuration > Device Setup > Routing > Interface Settings > Interfaces。
IPv6 支持前缀规则	9.3.2	引入了此功能。 更新了以下屏幕：Configuration > Device Setup > Routing > Prefix Rules > Add prefix Rule
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。 更新了以下屏幕：Configuration > Device Setup > Routing > Route Maps >Policy Based Routing，Configuration > Device Setup > Routing > Interface Settings > Interfaces。

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

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 24-4 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

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。在 ASDM 中，可以通过添加、编辑或删除路由映射名称、序列号或重新分发来定义路由映射。

操作步骤

步骤 1　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > Route Maps**。

步骤 2　点击**添加**。

系统将显示 Add Route Map 或 Edit Route Map 对话框。

步骤 3　输入路由映射名称和序列号。路由映射名称是分配给特定路由的名称。序列号是在 ASA 中添加或删除路由映射条目的顺序。

注意　如果编辑一个现有路由映射，则已填写 Route Map Name 和 Sequence Number 字段。

步骤 4　要拒绝路由匹配重新分发，请点击 **Deny**。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。要允许重新分发路由匹配，请点击 **Permit**。如果在路由映射 permit 子句中使用 ACL，则会重新分发 ACL 允许的路由。

此外，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。

步骤 5　点击 **Match Clause** 选项卡以选择应将此子句应用到的路由，并设置以下参数：

- 选中 **Match first hop interface of route** 复选框以启用或禁用匹配路由的第一跳接口或将任何路由与指定的下一跳接口相匹配。如果指定多个接口，则路由可以匹配任一接口。
  - 在 Interface 字段中输入接口名称，或点击省略号以显示 Browse Interface 对话框。
  - 选择一个或多个接口，点击 **Interface**，然后点击 **OK**。
- 在 IPv4 和 IPv6 部分中，执行以下一项或多项操作：
  - 选中 **Match Address** 复选框以启用或禁用匹配路由或匹配数据包的地址。
  - 选中 **Match Next Hop** 复选框以启用或禁用匹配路由的下一跳地址。
  - 选中 **Match Route Source** 复选框以启用或禁用匹配路由的通告源地址。
  - 从下拉列表中选择 Access List to Prefix List 以匹配 IP 地址。
  - 根据先前的选择，点击省略号以显示 Browse Access List 或 Browse Prefix List 对话框。
  - 选择所需的 ACL 或前缀列表。
- 选中 **Match metric of route** 复选框以启用或禁用匹配路由的指标。
  - 在 Metric Value 字段中，键入指标值。可以输入多个以逗号分隔的值。通过此设置可匹配具有指定指标的任何路由。指标值范围在 0 到 4294967295 之间。
- 选中 **Match Route Type** 复选框以启用或禁用路由类型匹配。有效路由类型为 External1、External2、 Internal、 Local、 NSSA-External1 和 NSSA-External2。启用后，即可从列表中选择多个路由类型。

步骤 6　点击 **Set Clause** 选项卡以修改以下信息，该信息将重新分发到目标协议：

- 选中 **Set Metric Clause** 复选框以启用或禁用目标路由协议的指标值，并在 Value 字段中键入值。
- 选中 **Set Metric Type** 复选框以启用或禁用目标路由协议的指标类型，并从下拉列表中选择指标类型。

步骤 7　点击 **BGP Match Clause** 选项卡以选择应将此子句应用到的路由，并设置以下参数：

- 选中 **Match AS path access lists** 复选框以启用将 BGP 自治系统路径访问列表与指定的路径访问列表相匹配。如果指定多个路径访问列表，则路由可以匹配任一路径访问列表。
- 选中 **Match Community** 复选框以启用将 BGP 社区与指定的社区相匹配。如果指定多个社区，则路由可以匹配任一社区。未与任何社区匹配的路由将不作为出站路由映射进行通告。
  - 选中 **Match the specified community exactly** 复选框以启用将 BGP 社区与指定的社区完全匹配。
- 选中 **Match Policy list** 复选框以配置路由映射，从而评估和处理 BGP 策略。如果指定多个策略列表，则路由可以处理任一策略列表。

步骤 8　点击 **BGP Set Clause** 选项卡以修改以下信息，该信息将重新分发到 BGP 协议：

- 选中 **Set AS Path** 复选框以修改 BGP 路由的自治系统路径。
  - 选中 **Prepend AS path** 复选框以向 BGP 路由预置任意自治系统路径字符串。通常本地 AS 编号预置多次，从而增加自治系统路径长度。如果指定多个 AS 路径编号，则路径可以预置任一 AS 编号。
  - 选中 **Prepend Last AS to the AS Path** 复选框以向 AS 路径预置最后一个 AS 编号。为 AS 编号输入 1 到 10 之间的值。
  - 选中 **Convert route tag into AS Path** 复选框以将路由的标记转换为自治系统路径。
- 选中 **Set Community** 复选框以设置 BGP 社区属性。
  - 点击 **Specify Community** 以输入社区编号 （如果适用）。有效值的范围为 1 到 4294967200、 internet、 no-advertise 和 no-export。
  - 选中 **Add to the existing communities** 以将社区添加到已现有的社区。
  - 点击 **None** 以从用于传递路由映射的前缀删除社区属性。
- 选中 **Set local preference** 复选框以便为自治系统路径指定首选项值。
- 选中 **Set weight** 复选框以便为路由表指定 BGP 权重。输入 0 到 65535 之间的值。
- 选中 **Set origin** 复选框以指定 BGP 源代码。有效值为 Local IGP 和 Incomplete。
- 选中 **Set next hop** 复选框以指定实现路由映射的 match 子句的数据包输出地址。
  - 点击 **Specify IP address** 以输入将数据包输出到的下一跳的 IP 地址。它不需要是相邻路由器。如果指定多个 IP 地址，则数据包可以在任一 IP 地址输出。
  - 点击 **Use peer address** 以将下一跳设置为 BGP 对等体地址。

步骤 9　点击 **OK**。

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 24-6 页
- 配置前缀规则，第 24-6 页

定义路由以匹配特定目标地址

操作步骤

步骤 1　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > Route Maps**。

步骤 2　点击**添加**。

系统将显示 Add Route Map 对话框。从该对话框中，可以分配或选择路由映射名称、序列号及其重新分发访问 （即，允许或拒绝）。路由映射条目按顺序读取。您可以使用序列号标识顺序，否则 ASA 会使用您添加条目的顺序。

步骤 3　点击 **Match Clause** 选项卡以选择应将此子句应用到的路由，并设置以下参数：

- 选中 **Match first hop interface of route** 复选框以启用或禁用匹配路由的第一跳接口或将任何路由与指定的下一跳接口相匹配。如果指定多个接口，则路由可以匹配任一接口。
  - 在 Interface 字段中输入接口名称，或点击省略号以显示 Browse Interface 对话框。
  - 选择接口类型 （**inside** 或 **outside**），点击 **Selected Interface**，然后点击 **OK**。
  - 选中 **Match IP Address** 复选框以启用或禁用匹配路由或匹配数据包的地址。
  - 选中 **Match Next Hop** 复选框以启用或禁用匹配路由的下一跳地址。
  - 选中 **Match Route Source** 复选框以启用或禁用匹配路由的通告源地址。
  - 从下拉列表中选择 Access List to Prefix List 以匹配 IP 地址。
  - 根据先前的选择，点击省略号以显示 Browse Access List 或 Browse Prefix List 对话框。
  - 选择所需的 ACL 或前缀列表。
- 选中 **Match metric of route** 复选框以启用或禁用匹配路由的指标。
  - 在 Metric Value 字段中，键入指标值。可以输入多个以逗号分隔的值。通过此设置可匹配具有指定指标的任何路由。指标值范围在 0 到 4294967295 之间。
- 选中 **Match Route Type** 复选框以启用或禁用路由类型匹配。有效路由类型为 External1、External2、 Internal、 Local、 NSSA-External1 和 NSSA-External2。启用后，即可从列表中选择多个路由类型。

配置前缀规则

备注　配置前缀规则之前，必须先配置前缀列表。

要配置前缀规则，请执行以下步骤：

步骤 1　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > Prefix Rules**。

步骤 2　点击 **Add** 并选择 **Add Prefix Rule**。

系统将显示 Add Prefix Rule 对话框。从该对话框中，可以添加序列号、选择 IP 版本 （IPv4 或 IPv6）、指定网络的前缀、其重新分发访问 （即，允许或拒绝）及最小和最大前缀长度。

步骤 3　输入可选序列号或接受默认值。

步骤 4　以 IP 地址/掩码长度格式指定前缀数字。

步骤 5　点击 **Permit** 或 **Deny** 单选按钮以指示重新分发访问。

步骤 6　输入可选的最小和最大前缀长度。

步骤 7　完成后点击 **OK**。

列表中将显示新前缀规则或修改后的前缀规则。

步骤 8　如果要使用自动生成的序列号，请选中 **Enable Prefix list sequence numbering** 复选框。

步骤 9　点击 **Apply** 保存更改。

配置前缀列表

ABR 类型 3 LSA 过滤扩展了 ABR 的功能，即在不同 OSPF 区域之间运行 OSPF 过滤类型 3 LSA。配置前缀列表后，便会仅将指定的前缀从一个 OSPF 区域发送到另一个 OSPF 区域。所有其他前缀都限用于各自的 OSPF 区域。可以向传入或传出 OSPF 区域的流量或者同时为该区域的传入和传出流量应用此类型的区域过滤。

当前缀列表的多个条目与给定前缀相匹配时，将使用具有最低序列号的条目。为提高效率，可能需要手动为最常用的匹配或拒绝项分配较低的序列号来将其置于列表顶部附近。默认情况下，序列号从 5 开始并以 5 为增量自动生成。

要添加前缀列表，请执行以下步骤：

步骤 1　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > Prefix Rules**。

步骤 2　点击 **Add** 并选择 **Add Prefix List**。

系统将显示 Add Prefix List 对话框。

步骤 3　输入前缀名称和说明，然后点击 **OK**。

为路由操作配置指标值

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > Route Maps**。

步骤 2　点击**添加**。

系统将显示 Add Route Map 或 Edit Route Map 对话框。从该对话框中，可以分配或选择路由映射名称、序列号及其重新分发访问 （即，允许或拒绝）。路由映射条目按顺序读取。您可以使用序列号标识顺序，否则 ASA 会使用您添加路由映射的顺序。

步骤 3　点击 **Set Clause** 选项卡以修改以下信息，该信息将重新分发到目标协议：

- 选中 **Set Metric Clause** 复选框以启用或禁用目标路由协议的指标值，并在 Value 字段中输入值。
- 选中 **Set Metric Type** 复选框以启用或禁用目标路由协议的指标类型，并从下拉列表中选择指标类型。

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。

步骤 1　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > Route Maps**。

步骤 2　点击**添加**。

步骤 3　在 Route Map Name 字段中输入 **1-to-2**。

步骤 4　在 Sequence Number 字段中输入路由序列号。

步骤 5　点击 **Permit** 单选按钮。

默认情况下，该选项卡位于顶部。

步骤 6　点击 **Match Clause** 选项卡。

步骤 7　选中 **Match Metric of Route** 复选框，并键入 **1** 作为指标值。

步骤 8　点击 **Set Clause** 选项卡。

步骤 9　选中 **Set Metric Value** 复选框，并键入 **5** 作为指标值。

步骤 10　选中 **Set Metric-Type** 复选框并选择 **Type-1**。

路由映射的功能历史记录

表 24-1　　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。 引入了以下屏幕：Configuration > Device Setup > Routing > Route Maps。
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。
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。

表 24-1　　路由映射的功能历史记录 （续）

功能名称	平台版本	功能信息
支持 BGP	9.2(1)	引入了此功能。 更新了以下屏幕：Configuration > Device Setup > Routing > Route Maps，增加了 2 个选项卡：BGP match clause 和 BGP set clause。
IPv6 支持前缀规则	9.3.2	引入了此功能。 更新了以下屏幕：Configuration > Device Setup > Routing > Prefix Rules > Add prefix Rule

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

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

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 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP**。

步骤 2　通过选中 **General** 选项卡上的 **Enable BGP routing** 复选框，启用 BGP 路由进程。请参阅启用 BGP，第 25-4 页。

步骤 3　在 **BGP > Best Path** 选项卡上，定义与 BGP 路由最佳路径选择过程有关的配置。请参阅定义 BGP 路由进程的最佳路径，第 25-5 页。

步骤 4　在 **BGP > Policy Lists** 选项卡上，为 BGP 路由配置策略列表。请参阅配置策略列表，第 25-5 页。

步骤 5　在 **BGP > AS Path Filters** 选项卡上，为 BGP 路由配置 AS 路径过滤器。请参阅配置 AS 路径过滤器，第 25-7 页。

步骤 6　在 **BGP > Community Rules** 选项卡上为 BGP 路由配置社区规则。请参阅配置社区规则，第 25-7 页。

步骤 7　在 **BGP > IPv4 Family** 选项卡上，配置 IPv4 地址系列设置。请参阅配置 IPv4 地址系列设置，第 25-8 页。

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　对于单模式，在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > General**。

注意　对于多模式，在 ASDM 中，依次选择 **Configuration > Context Management > BGP**。启用 BGP 后，通过依次选择 **Configuration > Device Setup > Routing > BGP > General** 切换到安全情景并启用 BGP。

系统将显示 **General** 窗格。

步骤 2　选中 **Enable BGP Routing** 复选框。

步骤 3　在 **AS Number** 字段中，输入 BGP 进程的自治系统 (AS) 编号。AS 编号内部包含多个自主编号。AS 编号范围为 1 至 4294967295 或 1.0 至 XX.YY。

步骤 4　（可选）选中 **Limit the number of AS numbers in the AS_PATH attribute of received routes** 复选框，将 AS_PATH 属性中的 AS 编号数量限制为特定数量。有效值范围为 1 至 254。

步骤 5　（可选）选中 **Log neighbor changes** 复选框，以启用 BGP 邻居更改（上或下）和重置日志记录。这有助于解决网络连接问题并衡量网络稳定性。

步骤 6　（可选）选中 **Use TCP path MTU discovery** 复选框，使用 Path MTU Discovery 方法确定两个 IP 主机之间网络路径上的最大传输单位 (MTU) 大小。这可以避免 IP 分片。

步骤 7　（可选）选中 **Enable fast external failover** 复选框，在发生链路故障时立即重置外部 BGP 会话。

步骤 8　（可选）选中 **Enforce that first AS is peer’s AS for EBGP routes** 复选框，放弃从未在 AS_PATH 属性中将其 AS 编号列为首个分段的外部 BGP 对等体接收的传入更新。这可以防止错误配置或未经授权的对等体通过通告路由（如同其源自另一个自治系统）来错误定向流量。

步骤 9　（可选）选中 **Use dot notation for AS numbers** 复选框，将完整的二进制 4 字节 AS 编号拆分为两个单词，每个单词 16 位，以点分隔。0-65553 的 AS 编号以十进制数字表示，大于 65535 的 AS 编号使用点分表示法来表示。

步骤 10　在 **Neighbor timers** 区域中指定计时器信息：

a. 在 **Keepalive interval** 字段中，输入 BGP 邻居在不发送 keepalive 消息后保持活动的时间间隔。在此 keepalive 时间间隔结束时，如果未发送消息，则声明 BGP 对等体处于失效状态。默认值为 60 秒。

b. （可选）在 **Hold Time** 字段中，输入 BGP 邻居在发起并配置 BGP 连接时保持活动的时间间隔。

c. （可选）在 **Min. Hold Time** 字段中，输入 BGP 邻居在发起并配置 BGP 连接时保持活动的最小时间间隔。指定一个从 0 至 65535 的值。

步骤 11　（可选）在 **Non Stop Forwarding** 部分中，执行以下操作：

a. 选中 **Enable Graceful Restart** 复选框，使 ASA 对等体避免在切换之后出现路由抖动。

b. 在 **Restart Time** 字段中，输入 ASA 对等体在接收 BGP 打开消息之前等待删除过时路由的持续时间。默认值为 120 秒。有效值介于 1 至 3600 秒之间。

c. 在 **Stale Path Time** 字段中，输入 ASA 在从重新启动的 ASA 接收记录终止 (EOR) 消息之后，删除过时路由之前等待的持续时间。默认值为 360 秒。有效值介于 1 至 3600 秒之间。

步骤 12　点击 **OK**。

步骤 13　点击 **Apply**。

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 25-2 页。

操作步骤

步骤 1　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > Best Path**。

系统将显示 **Best Path configuration** 窗格。

步骤 2　在 **Default Local Preference** 字段中，指定介于 0 与 4294967295 之间的值。默认值为 100。值越大，表示优先级越高。此首选项会发送到本地自治系统中的所有路由器和接入服务器。

步骤 3　选中 **Allow comparing MED from different neighbors** 复选框，允许比较来自不同自治系统中不同邻居的路径的多出口鉴别器 (MED)。

步骤 4　选中 **Compare router-id for identical EBGP paths** 复选框，在最佳路径选择过程中，比较从外部 BGP 对等体接收的类似路径，并将最佳路径切换到路由器 ID 最低的路由。

步骤 5　选中 **Pick the best MED path among paths advertised from the neighboring AS** 复选框，启用从联盟对等体获悉的路径之间的 MED 比较，以添加新的网络条目。仅当路径中没有外部自治系统时，才会比较 MED。

步骤 6　选中 **Treat missing MED as the least preferred one** 复选框，将缺失的 MED 属性视为具有无穷值，从而使此路径成为最不需要使用的路径；因此，缺少 MED 的路径最不优先考虑。

步骤 7　点击 **OK**。

步骤 8　点击 **Apply**。

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > Policy Lists**。

步骤 2　点击**添加**。

系统将显示 **Add Policy List** 对话框。在此对话框中，您可以添加策略列表名称、重新分发访问（即，允许或拒绝）、匹配接口、指定 IP 地址、匹配 AS 路径、匹配社区名称列表、匹配指标以及匹配标签号。

步骤 3　在 **Policy List Name** 字段中，输入策略列表的名称。

步骤 4　点击 **Permit** 或 **Deny** 单选按钮以指示重新分发访问。

步骤 5　选中 **Match Interfaces** 复选框，以分发使其下一跳脱离指定接口之一的路由，并执行以下操作之一：

- 在 **Interface** 字段中，输入接口名称。
- 在 **Interface** 字段中，点击省略号以手动浏览并查找接口。选择一个或多个接口，点击 **Interface**，然后点击 **OK**。

步骤 6　在 **Specify IP** 区域中，配置以下内容：

a. 选中 **Match Address** 复选框，重新分发任何具有标准访问列表或前缀列表许可的目标网络编号地址的路由，并对数据包执行策略路由。

   指定访问列表/前缀列表，或者点击省略号以手动浏览并查找访问列表。选择一个或多个访问列表，点击 **Access List**，然后点击 **OK**。

b. 选中 **Match Next Hop** 复选框，重新分发任何具有指定访问列表或前缀列表之一传递的下一跳路由器地址的路由。

   指定访问列表/前缀列表，或者点击省略号以手动浏览并查找访问列表。选择一个或多个访问列表，点击 **Access List**，然后点击 **OK**。

c. 选中 **Match Route Source** 复选框，重新分发在访问列表或前缀列表指定的地址由路由器和接入服务器通告的路由。

   指定访问列表/前缀列表，或者点击省略号以手动浏览并查找访问列表。选择一个或多个访问列表，点击 **Access List**，然后点击 **OK**。

步骤 7　选中 **Match AS Path** 复选框以匹配 BGP 自治系统路径。

指定 AS 路径过滤器，或者点击省略号以手动浏览并查找 AS 路径过滤器。选择一个或多个 AS 路径过滤器，点击 **AS Path Filter**，然后点击 **OK**。

步骤 8　选中 **Match Community Names List** 复选框以匹配 BGP 社区。

a. 指定社区规则，或者点击省略号以手动浏览并查找社区规则。选择一个或多个社区规则，点击 **Community Rules**，然后点击 **OK**。

b. 选中 **Match the specified community exactly** 复选框以匹配特定 BGP 社区。

步骤 9　选中 **Match Metrices** 复选框以重新分发具有指定指标的路由。如果指定多个指标，则路由可以通过任一指标进行匹配。

步骤 10　选中 **Match Tag Numbers** 复选框以重新分发路由表中与指定标签相匹配的路由。如果指定多个标签号，则路由可以通过任一指标进行匹配。

步骤 11　点击 **OK**。

步骤 12　点击 **Apply**。

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 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > AS Path Filters**。

步骤 2　点击**添加**。

系统将显示 **Add Filter** 对话框。从此对话框中，您可以添加过滤器名称、其重新分发访问 （即，允许或拒绝）和正则表达式。

步骤 3　在 **Name** 字段中，输入 AS 路径过滤器的名称。

步骤 4　点击 **Permit** 或 **Deny** 单选按钮以指示重新分发访问。

步骤 5　指定正则表达式。点击 **Build** 以构建正则表达式。

步骤 6　点击 **Test** 以测试正则表达式是否与选择的字符串相匹配。

步骤 7　点击 **OK**。

步骤 8　点击 **Apply**。

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > Community Rules**。

步骤 2　点击**添加**。

系统将显示 **Add Community Rule** 对话框。从该对话框中，您可以添加规则名称、规则类型、其重新分发访问 （即，允许或拒绝）以及特定社区。

步骤 3　在 **Rule Name** 字段中，输入社区规则的名称。

步骤 4　点击 **Standard** 或 **Expanded** 单选按钮以指示社区规则类型。

步骤 5　点击 **Permit** 或 **Deny** 单选按钮以指示重新分发访问。

步骤 6　要添加标准社区规则，请执行以下操作：

a. 在 **Communities** 字段中，指定社区号。有效值范围为 1 至 4294967200。

b. （可选）选中 **Internet** （公认社区）复选框以指定互联网社区。系统向所有对等体 （内部和外部）通告具有此社区的路由。

c. （可选）选中 **Do not advertise to any peers**（公认社区）复选框以指定无通告社区。系统不向任何对等体 （内部或外部）通告具有此社区的路由。

d. （可选）选中 **Do not export to next AS** （公认社区）复选框以指定无导出社区。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。

步骤 7　要添加扩展社区规则，请执行以下操作：

a. 在 **Regular Expression** 字段中，输入正则表达式。或者，点击 **Build** 以构建正则表达式。

b. 点击 **Test** 以检查所构建的正则表达式是否与选择的字符串相匹配。

步骤 8　点击 **OK**。

步骤 9　点击 **Apply**。

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 25-8 页
- 配置 IPv4 系列聚合地址设置，第 25-9 页
- 配置 IPv4 系列过滤设置，第 25-10 页
- 配置 IPv4 系列 BGP 邻居设置，第 25-10 页
- 配置 IPv4 网络设置，第 25-13 页
- 配置重新分发设置，第 25-13 页
- 配置路由注入设置，第 25-14 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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv4 Family**。

步骤 2　点击 **General**。

系统将显示 **General IPv4 family BGP parameters** 配置窗格。

步骤 3　在 **Administrative Distances** 区域中，指定 **External**、 **Internal** 和 **Local** 距离。

步骤 4　从 **Learned Routes Map** 下拉列表中选择路由映射名称。点击 **Manage** 以添加并配置路由映射。

步骤 5　（可选）选中 **Generate Default Route** 复选框，以将 BGP 路由进程配置为分发默认路由 （网络 0.0.0.0）。

步骤 6　（可选）选中 **Summarize subnet routes into network-level routes** 复选框，以将子网路由配置为自动汇总到网络级路由中。

步骤 7　（可选）选中 **Advertise inactive routes** 复选框，以通告未装载至路由信息库 (RIB) 中的路由。

步骤 8　（可选）选中 **Redistribute iBGP into an IGP** 复选框，以将 iBGP 配置为重新分发到内部网关协议 (IGP) 中，例如 IS-IS 或 OSPF。

步骤 9　（可选）在 Scanning Interval 字段中，为下一跳验证输入 BGP 路由器的扫描间隔 （以秒为单位）。有效值范围为 5 至 60 秒。

步骤 10　（可选）选中 **Enable address tracking** 复选框，以启用 BGP 下一跳地址跟踪。在 **Delay Interval** 字段中，指定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。

步骤 11　（可选）在 **Number of paths** 字段中，指定可以安置在路由表中的并行内部边界网关协议 (iBGP) 路由的最大数量，并选中 **iBGP multipaths** 复选框。

步骤 12　点击 **Apply**。

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv4 Family**。

步骤 2　点击 **Aggregate Address**。

系统将显示 Aggregate Address 参数配置窗格。

步骤 3　点击**添加**。

系统将显示 Add Aggregate Address 窗格。

步骤 4　在 **Network** 字段中指定网络对象。

步骤 5　选中 **Generate autonomous system set path information** 复选框，以生成自治系统集路径信息。

步骤 6　选中 **Filters all more- specific routes from the updates** 复选框，以过滤来自更新的所有更具体的路由。

步骤 7　从 **Attribute Map** 下拉列表中选择路由映射。点击 **Manage** 以添加或配置路由映射。

步骤 8　从 **Advertise Map** 下拉列表中选择路由映射。点击 **Manage** 以添加或配置路由。

步骤 9　从 **Suppress Map** 下拉列表中选择路由映射。点击 **Manage** 以添加或配置路由。

步骤 10　点击 **OK**。

步骤 11　在 Aggregate Timer 字段中，为聚合计时器指定一个值（以秒为单位）。有效值为 0 或介于 6 与 60 之间的任意值。

步骤 12　点击 **Apply**。

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv4 Family**。

步骤 2　点击 **Filtering**。

系统将显示 Define filters for BGP updates 窗格。

步骤 3　点击**添加**。

系统将显示 Add Filter 窗格。

步骤 4　从 **Direction** 下拉列表中选择方向。此方向将指定过滤器应用于入站更新还是出站更新。

步骤 5　从 **Access List** 下拉列表中选择访问列表。点击 **Manage** 以添加新的 ACL。

步骤 6　从 Protocol 下拉列表中选择协议。这仅在选择出站方向的情况下适用。

步骤 7　从 Process ID 下拉列表中为指定协议选择进程 ID。

步骤 8　点击 **OK**。

步骤 9　点击 **Apply**。

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv4 Family**。

步骤 2　点击 **Neighbor**。

步骤 3　点击**添加**。

步骤 4　点击左窗格中的 **General**。

步骤 5　在 **IP Address** 字段中，输入 BGP 邻居 IP 地址。此 IP 地址会添加到 BGP 邻居表。

步骤 6　在 **Remote AS** 字段中，输入 BGP 邻居所属的自治系统。

步骤 7　（可选）在 **Description** 字段中，输入 BGP 邻居描述。

步骤 8　（可选）选中 Shutdown neighbor administratively 复选框，以禁用邻居或对等组。

步骤 9　（可选）选中 Enable address family 复选框，以启用与 BGP 邻居的通信。

步骤 10　（可选）选中 **Global Restart Functionality for this peer** 复选框，以启用或禁用 ASA 邻居或对等组的边界网关协议 (BGP) 平稳重启功能。

步骤 11　点击左窗格中的 **Filtering**。

步骤 12　（可选）在 Filter routes using an access list 区域中，选择相应的传入或传出访问控制列表，以分发 BGP 邻居信息。点击 **Manage**，以根据需要添加 ACL 和 ACE。

步骤 13　（可选）在 Filter routes using a route map 区域，选择相应的传入或传出路由映射，以将路由映射应用于传入或传出路由。点击 **Manage** 以配置路由映射。

步骤 14　（可选）在 Filter routes using a prefix list 区域中，选择相应的传入或传出前缀列表，以分发 BGP 邻居信息。点击 **Manage** 以配置前缀列表。

步骤 15　（可选）在 Filter routes using AS path filter 区域中，选择相应的传入或传出 AS 路径过滤器，以分发 BGP 邻居信息。点击 **Manage** 以配置 AS 路径过滤器。

步骤 16　（可选）选中 **Limit the number of prefixes allowed from the neighbor** 复选框，以控制可以从邻居接收的前缀的数量。

- 在 Maximum prefixes 字段中，输入允许从特定邻居接收的前缀的最大数量。
- 在 Threshold level 字段中，输入路由器开始生成警告消息时所处的 （最大值的）百分比。有效值为 1 至 100 的整数。默认值为 75。
- （可选）选中 **Control prefixes received from a peer** 复选框，以指定对从对等体接收的前缀的额外控制。执行以下操作之一：
  - 点击 **Terminate peering when prefix limit is exceeded**，以在达到前缀限制时停止 BGP 邻居。在 Restart interval 字段中，指定 BGP 邻居重新启动前的间隔。
  - 点击 **Give only warning message when prefix limit is exceeded**，以在达到最大前缀限制时生成日志消息。此时将不会终止 BGP 邻居。

步骤 17　点击左窗格中的 **Routes**。

步骤 18　在 Advertisement Interval 字段中，输入前后两次发送 BGP 路由更新的最小间隔 （以秒为单位）。

步骤 19　（可选）选中 **Generate Default route** 复选框，以允许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。

- 从 Route map 下拉列表中选择允许有条件地注入路由 0.0.0.0 的路由映射。点击 **Manage** 以添加并配置路由映射。

步骤 20　（可选）要添加有条件地通告的路由，请执行以下操作：

a. 在 Conditionally Advertised Routes 部分中，点击 **Add**。

b. 从 Advertise Map 下拉列表中选择在达到存在映射或非存在映射的条件时将通告的路由映射。

c. 执行以下操作之一：
   - 点击 **Exist Map** 并选择路由映射。此路由映射将与 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。
   - 点击 **Non-exist Map** 并选择路由映射。此路由映射将与 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。

d. 点击 **OK**。

步骤 21　（可选）选中 **Remove private autonomous system (AS) numbers from outbound routing updates** 复选框，以阻止在出站路由上通告专用 AS 号。

步骤 22　点击左窗格中的 **Timers**。

步骤 23　（可选）选中 **Set timers for the BGP peer** 复选框，以设置 keepalive 频率、抑制时间和最小抑制时间。

- 在 Keepalive frequency 字段中输入 ASA 向邻居发送 keepalive 消息的频率（以秒为单位）。有效值介于 0 和 65535 之间。默认值为 60 秒。
- 在 Hold time 字段中，输入 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。
- 在 Min Hold time 字段中，输入 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 24　点击左窗格中的 **Advanced**。

步骤 25　（可选）选中 **Enable Authentication** 复选框，以在两个 BGP 对等体之间的 TCP 连接上启用 MD5 身份验证。

- 从 Encryption Type 下拉列表中选择加密类型。
- 在 Password 字段中输入密码。在 Confirm Password 字段中重新输入密码。

注意　密码区分大小写，当启用 **service password-encryption** 命令时，长度最大为 25 个字符；未启用 **service password-encryption** 命令时，长度最大为 81 个字符。第一个字符不能为数字。此字符串可以包含任意字母数字字符，包括空格。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 26　（可选）选中 **Send Community Attribute to this neighbor** 复选框。

步骤 27　（可选）选中 **Use ASA as next hop for neighbor** 复选框，以将路由器配置为 BGP 发言邻居或对等组的下一跳。

步骤 28　执行以下操作之一：

- 点击 **Allow connections with neighbor that is not directly connected**，以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。
  - （可选）在 TTL hops 字段中输入生存时间。有效值介于 1 和 255 之间。
  - （可选）选中 **Disable connection verification** 复选框，以禁用连接验证，从而与使用环回接口的单跳对等体建立 eBGP 对等会话。
- 点击 **Limit number of TTL hops to neighbor**，使您能够确保 BGP 对等会话安全。
  - 在 TTL hops 字段中，输入用于分隔 eBGP 对等体的最大跳数。有效值介于 1 和 254 之间。

步骤 29　（可选）在 Weight 字段中，输入 BGP 邻居连接权重。

步骤 30　从 BGP version 下拉列表中选择 ASA 将接受的 BGP 版本。

注意　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 31　（可选）选中 **TCP Path MTU Discovery** 复选框以对 BGP 会话启用 TCP 传输会话。

步骤 32　从 TCP transport mode 下拉列表中选择 TCP 连接模式。

步骤 33　点击左窗格中的 **Migration**。

步骤 34　（可选）选中 **Customize the AS number for routes received from the neighbor** 复选框，为从 eBGP 邻居接收的路由自定义 AS_PATH 属性。

- 在 Local AS Number 字段中输入本地自治系统号。有效值介于 1 和 65535 之间。
- （可选）选中 **Do not prepend local AS number for routes received from neighbor** 复选框。系统不会从 eBGP 对等体接收的任何路由预置本地 AS 号。
- （可选）选中 **Replace real AS number with local AS number in routes received from neighbor** 复选框。系统不会预置从本地路由进程接收的 AS 号。
- （可选）选中 **Accept either real AS number or local AS number in routes received from neighbor** 复选框。

步骤 35　点击 **OK**。

步骤 36　点击 **Apply**。

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv4 Family**。

步骤 2　点击 **Networks**。

系统将显示 Define networks to be advertised by the BGP routing process configuration 窗格。

步骤 3　点击**添加**。

系统将显示 Add Network 窗格。

步骤 4　在 Address 字段中指定 BGP 将通告的网络。

步骤 5　（可选）从 Netmask 下拉列表中选择网络或子网掩码。

步骤 6　从 **Route Map** 下拉列表中选择为过滤要通告的网络而应检查的路由映射。点击 **Manage** 以配置或添加路由映射。

步骤 7　点击 **OK**。

步骤 8　点击 **Apply**。

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv4 Family**。

步骤 2　点击 **Redistribution**。

系统将显示 Redistribution 窗格。

步骤 3　点击**添加**。

系统将显示 Add Redistribution 窗格。

步骤 4　从 Source Protocol 下拉列表中选择要将路由重新分发到 BGP 域所使用的协议。

步骤 5　从 **Process ID** 下拉列表中为源协议选择进程 ID。

步骤 6　（可选）在 Metric 字段输入已重新分发的路由的指标。

步骤 7　从 **Route Map** 下拉列表中选择为过滤要重新分发的网络而应检查的路由映射。点击 **Manage** 以配置或添加路由映射。

步骤 8　选中 Internal、 External 和 NSSA External Match 复选框中的一个或多个，以从 OSPF 网络重新分发路由。

注意　此步骤仅适用于从 OSPF 网络进行的重新分发。

步骤 9　点击 **OK**。

步骤 10　点击 **Apply**。

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv4 Family**。

步骤 2　点击 **Route Injection**。

系统将显示 Route Injection 窗格。

步骤 3　点击**添加**。

系统将显示 Add Conditionally injected route 窗格。

步骤 4　从 Inject Map 下拉列表中选择用于指定要注入本地 BGP 路由表的前缀的路由映射。

步骤 5　从 **Exist Map** 下拉列表中选择包含 BGP 发言者将跟踪的前缀的路由映射。

步骤 6　选中 **Injected routes will inherit the attributes of the aggregate route** 复选框，以将已注入的路由配置为继承聚合路由的属性。

步骤 7　点击 **OK**。

步骤 8　点击 **Apply**。

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 25-14 页
- 配置 IPv6 系列聚合地址设置，第 25-15 页
- 配置 IPv6 系列 BGP 邻居设置，第 25-16 页
- 配置 IPv6 网络设置，第 25-18 页
- 配置重新分发设置，第 25-13 页
- 配置路由注入设置，第 25-14 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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv6 Family**。

步骤 2　点击 **General**。

系统将显示 General IPv6 family BGP parameters 配置窗格。

步骤 3　在 **Administrative Route Distances** 区域中指定外部、内部和本地距离。

步骤 4　（可选）选中 **Generate Default Route** 复选框，以将 BGP 路由进程配置为分发默认路由 （网络 0.0.0.0）。

步骤 5　（可选）选中 **Advertise inactive routes** 复选框，以通告未装载至路由信息库 (RIB) 中的路由。

步骤 6　（可选）选中 **Redistribute iBGP into an IGP** 复选框，以将 iBGP 配置为重新分发到内部网关协议 (IGP) 中，例如 IS-IS 或 OSPF。

步骤 7　（可选）在 Scanning Interval 字段中，为下一跳验证输入 BGP 路由器的扫描间隔 （以秒为单位）。有效值范围为 5 至 60 秒。

步骤 8　（可选）在 **Number of paths** 字段中，指定可以安置在路由表中的边界网关协议路由的最大数量。

步骤 9　（可选）选中 **IBGP multipaths** 复选框，并在 **Number of paths** 字段中指定可以安置在路由表中的并行内部边界网关协议 (iBGP) 路由的最大数量。

步骤 10　点击 **Apply**。

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv6 Family**。

步骤 2　点击 **Aggregate Address**。

系统将显示 Aggregate Address 参数配置窗格。

步骤 3　点击**添加**。

系统将显示 Add Aggregate Address 窗格。

步骤 4　在 IPv6/Address Mask 字段中指定 IPv6 地址。或者，浏览添加网络对象。

步骤 5　选中 **Generate autonomous system set path information** 复选框，以生成自治系统集路径信息。为此路由通告的路径将是 AS_SET，由包含在所有正在汇总的路径中的元素组成。

备注　聚合多个路径时，请勿使用这种形式的聚合地址命令，因为已汇总路由的自治系统路径可达性信息会发生更改，必须不断撤回并更新此路由。

步骤 6　选中 **Filters all more- specific routes from the updates** 复选框，以过滤来自更新的所有更具体的路由。这不仅会创建聚合路由，还将抑制向所有邻居通告更具体的路由。

步骤 7　从 **Attribute Map** 下拉列表中选择路由映射。点击 **Manage** 以添加或配置路由映射。这允许更改聚合路由的属性。

步骤 8　从 **Advertise Map** 下拉列表中选择路由映射。点击 **Manage** 以添加或配置路由。这将选择用于构建聚合路由不同组件的特定路由。

步骤 9　从 **Suppress Map** 下拉列表中选择路由映射。点击 **Manage** 以添加或配置路由。这将创建聚合路由，但会抑制通告指定的路由。

步骤 10　点击 **OK**。

步骤 11　在 Aggregate Timer 字段中，为聚合计时器指定一个值（以秒为单位）。有效值为 0 或介于 6 与 60 之间的任意值。这将指定路由的聚合时间间隔。默认值为 30 秒。

步骤 12　点击 **Apply**。

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 在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv6 Family**。

步骤 2 点击 **Neighbor**。

步骤 3 点击**添加**。

步骤 4 点击左窗格中的 **General**。

步骤 5 在 **IPv6 Address** 字段中，输入 BGP 邻居 IPv6 地址。此 IPv6 地址会添加到 BGP 邻居表。

步骤 6 在 **Remote AS** 字段中，输入 BGP 邻居所属的自治系统。

步骤 7 （可选）在 **Description** 字段中，输入 BGP 邻居描述。

步骤 8 （可选）选中 Shutdown neighbor administratively 复选框，以禁用邻居或对等组。

步骤 9 （可选）选中 Enable address family 复选框，以启用与 BGP 邻居的通信。

步骤 10 点击左窗格中的 **Filtering**。

步骤 11 （可选）在 Filter routes using a route map 区域，选择相应的传入或传出路由映射，以将路由映射应用于传入或传出路由。点击 **Manage** 以配置路由映射。

步骤 12 （可选）在 Filter routes using a prefix list 区域中，选择相应的传入或传出前缀列表，以分发 BGP 邻居信息。点击 **Manage** 以配置前缀列表。

步骤 13 （可选）在 Filter routes using AS path filter 区域中，选择相应的传入或传出 AS 路径过滤器，以分发 BGP 邻居信息。点击 **Manage** 以配置 AS 路径过滤器。

步骤 14 （可选）选中 **Limit the number of prefixes allowed from the neighbor** 复选框，以控制可以从邻居接收的前缀的数量。

- 在 Maximum prefixes 字段中，输入允许从特定邻居接收的前缀的最大数量。
- 在 Threshold level 字段中，输入路由器开始生成警告消息时所处的 （最大值的）百分比。有效值为 1 至 100 的整数。默认值为 75。
- （可选）选中 **Control prefixes received from a peer** 复选框，以指定对从对等体接收的前缀的额外控制。执行以下操作之一：
  - 点击 **Terminate peering when prefix limit is exceeded**，以在达到前缀限制时停止 BGP 邻居。在 Restart interval 字段中，指定 BGP 邻居重新启动前的间隔。
  - 点击 **Give only warning message when prefix limit is exceeded**，以在达到最大前缀限制时生成日志消息。此时将不会终止 BGP 邻居。

步骤 15 点击左窗格中的 **Routes**。

步骤 16 在 **Advertisement Interval** 字段中，输入前后两次发送 BGP 路由更新的最小间隔 （以秒为单位）。

步骤 17 （可选）选中 **Generate Default route** 复选框，以允许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。

- 从 Route map 下拉列表中选择允许有条件地注入路由 0.0.0.0 的路由映射。点击 **Manage** 以添加并配置路由映射。

步骤 18 （可选）要添加有条件地通告的路由，请执行以下操作：

a. 在 Conditionally Advertised Routes 部分中，点击 **Add**。

b. 从 Advertise Map 下拉列表中选择在达到存在映射或非存在映射的条件时将通告的路由映射。

c. 执行以下操作之一：

- 点击 **Exist Map** 并选择路由映射。此路由映射将与 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。
- 点击 **Non-exist Map** 并选择路由映射。此路由映射将与 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。

d. 点击 **OK**。

步骤 19　（可选）选中 **Remove private autonomous system (AS) numbers from outbound routing updates** 复选框，以阻止在出站路由上通告专用 AS 号。

步骤 20　点击左窗格中的 **Timers**。

步骤 21　（可选）选中 **Set timers for the BGP peer** 复选框，以设置 keepalive 频率、抑制时间和最小抑制时间。

- 在 Keepalive frequency 字段中输入 ASA 向邻居发送 keepalive 消息的频率（以秒为单位）。有效值介于 0 和 65535 之间。默认值为 60 秒。
- 在 Hold time 字段中，输入 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。
- 在 Min Hold time 字段中，输入 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 22　点击左窗格中的 **Advanced**。

步骤 23　（可选）选中 **Enable Authentication** 复选框，以在两个 BGP 对等体之间的 TCP 连接上启用 MD5 身份验证。

- 从 Encryption Type 下拉列表中选择加密类型。
- 在 Password 字段中输入密码。在 Confirm Password 字段中重新输入密码。

注意　密码区分大小写，当启用 **service password-encryption** 命令时，长度最大为 25 个字符；未启用 **service password-encryption** 命令时，长度最大为 81 个字符。第一个字符不能为数字。此字符串可以包含任意字母数字字符，包括空格。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 24　（可选）选中 **Send Community Attribute to this neighbor** 复选框。

步骤 25　（可选）选中 **Use ASA as next hop for neighbor** 复选框，以将路由器配置为 BGP 发言邻居或对等组的下一跳。

步骤 26　执行以下操作之一：

- 点击 **Allow connections with neighbor that is not directly connected**，以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。
  - （可选）在 TTL hops 字段中输入生存时间。有效值介于 1 和 255 之间。
  - （可选）选中 **Disable connection verification** 复选框，以禁用连接验证，从而与使用环回接口的单跳对等体建立 eBGP 对等会话。
- 点击 **Limit number of TTL hops to neighbor**，使您能够确保 BGP 对等会话安全。
  - 在 TTL hops 字段中，输入用于分隔 eBGP 对等体的最大跳数。有效值介于 1 和 254 之间。

步骤 27　（可选）在 Weight 字段中，输入 BGP 邻居连接权重。

步骤 28　从 BGP version 下拉列表中选择 ASA 将接受的 BGP 版本。

注意 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 29 （可选）选中 **TCP Path MTU Discovery** 复选框以对 BGP 会话启用 TCP 传输会话。

步骤 30 从 TCP transport mode 下拉列表中选择 TCP 连接模式。

步骤 31 点击左窗格中的 **Migration**。

步骤 32 （可选）选中 **Customize the AS number for routes received from the neighbor** 复选框，为从 eBGP 邻居接收的路由自定义 AS_PATH 属性。

- 在 Local AS Number 字段中输入本地自治系统号。有效值介于 1 和 65535 之间。
- （可选）选中 **Do not prepend local AS number for routes received from neighbor** 复选框。系统不会从 eBGP 对等体接收的任何路由预置本地 AS 号。
- （可选）选中 **Replace real AS number with local AS number in routes received from neighbor** 复选框。系统不会预置从本地路由进程接收的 AS 号。
- （可选）选中 **Accept either real AS number or local AS number in routes received from neighbor** 复选框。

步骤 33 点击 **OK**。

步骤 34 点击 **Apply**。

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 在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv6 Family**。

步骤 2 点击 **Networks**。

系统将显示 **Define the networks to be advertised by the BGP routing process configuration** 窗格。

步骤 3 点击**添加**。

系统将显示 **Add Network** 窗格。

步骤 4 在 **IPv6 Address/mask** 字段中，指定 BGP 将通告的网络。

步骤 5 从 **Route Map** 下拉列表中选择为过滤要通告的网络而应检查的路由映射。或者，点击 **Manage** 以配置或添加路由映射。

步骤 6 点击 **OK**。

步骤 7 点击 **Apply**。

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv6 Family**。

步骤 2　点击 **Redistribution**。

步骤 3　点击**添加**。

系统将显示 **Add Redistribution** 窗格。

步骤 4　在 **Source Protocol** 下拉列表中，选择要将路由重新分发到 BGP 域所使用的协议。

步骤 5　在 **Process ID** 下拉列表中，选择源协议的进程 ID。这仅适用于 OSPF 源协议。

步骤 6　（可选）在 **Metric** 字段中，输入已重新分发的路由的指标。

步骤 7　在 **Route Map** 下拉列表中，选择为过滤要重新分发的网络而应检查的路由映射。点击 **Manage** 以配置或添加路由映射。

步骤 8　选中以下 Match 复选框中的一个或多个 - **Internal**、**External 1**、**External 2**、**NSSA External 1** 和 **NSSA External 2** 复选框，以从 OSPF 网络重新分发路由。

注意　此步骤仅适用于从 OSPF 网络进行的重新分发。

步骤 9　点击 **OK**。

步骤 10　点击 **Apply**。

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　在 ASDM 中，依次选择 **Configuration > Device Setup > Routing > BGP > IPv4 Family**。

步骤 2　点击 **Route Injection**。

步骤 3　点击**添加**。

系统将显示 **Add Conditionally injected route** 窗格。

步骤 4　在 **Inject Map** 下拉列表中，选择用于指定要注入本地 BGP 路由表中的前缀的路由映射。

步骤 5　在 **Exist Map** 下拉列表中，选择包含 BGP 发言者将跟踪的前缀的路由映射。

步骤 6　选中 **Injected routes will inherit the attributes of the aggregate route** 复选框，以将已注入的路由配置为继承聚合路由的属性。

步骤 7　点击 **OK**。

步骤 8　点击 **Apply**。

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，并执行以下步骤：

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。

- **Monitoring > Routing > BGP Neighbors**

  每行代表一个 BGP 邻居。对于每个邻居，此列表包括 IP 地址、 AS 号、路由器 ID、状态（活动或空闲等）、正常运行时间、平稳重启功能、重启时间和过时路径时间。

- **Monitoring > Routing > BGP Routes**

  每行代表一个 BGP 路由。对于每个路由，此列表包括状态代码、IP 地址、下一跳地址、路由指标、本地优先值、权重和路径。

BGP 历史记录

表 25-1 列出各种功能变更以及实施相应功能变更的平台版本。ASDM 可向后兼容多个平台版本，因此此处未列出新增支持的具体 ASDM 版本。

表 25-1　　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。 引入了以下屏幕： Configuration > Device Setup > Routing > BGP Monitoring > Routing > BGP Neighbors, Monitoring > Routing > BGP Routes 修改了以下屏幕： Configuration > Device Setup > Routing > Static Routes> Add > Add Static Route Configuration > Device Setup > Routing > Route Maps> Add > Add Route Map
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。 修改了以下屏幕：Configuration > Device Setup > Routing > BGP > IPv4 Family > General
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。 修改了以下屏幕：Configuration > Device Setup > Routing > BGP > General, Configuration > Device Setup > Routing > BGP > IPv4 Family > Neighbor, Monitoring > Routing > BGP Neighbors

表 25-1 BGP 的功能历史记录

功能名称	平台版本	功能信息
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。 修改了以下屏幕：Configuration > Device Setup > Routing > BGP > IPv4 Family > Neighbor > Add BGP Neighbor > Routes
IPv6 的 BGP 支持	9.3(2)	我们添加了对 IPv6 的支持。 引入了以下屏幕：Configuration > Device Setup > Routing > BGP > IPv6 Family

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

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 26-3 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 24-4 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 22-4 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 26-6 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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

在 OSPF Setup 窗格中，您可以启用 OSPF 进程，配置 OSPF 区域和网络，以及定义 OSPF 路由汇总。

步骤 2　ASDM 中用于启用 OSPF 的三个选项卡如下：

- 通过 **Process Instances** 选项卡，您最多可以为每个情景启用两个 OSPF 进程实例。单情景模式和多情景模式均受支持。选中 **Enable Each OSPF Process** 复选框后，可以为该 OSPF 进程输入唯一数字标识符。此进程 ID 在内部使用，并且无需与任何其他 OSPF 设备上的 OSPF 进程 ID 匹配；有效值范围为 1 至 65535。每个 OSPF 进程具有其自己的关联区域和网络。

如果点击 **Advanced**，系统将显示 Edit OSPF Process Advanced Properties 对话框。从此处，您可以配置每个 OSPF 进程的 Router ID、Spanned EtherChannel 或 Individual Interface 集群中的集群 IP 地址池、 Adjacency Changes、 Administrative Route Distances、 Timers 和 Default Information Originate 设置。

- 通过 **Area/Networks** 选项卡，您可以显示其为 ASA 上的各 OSPF 进程包含的区域和网络。从此选项卡可以显示区域 ID、区域类型和为区域设置的身份验证类型。要添加或编辑 OSPF 区域或网络，请参阅配置 OSPFv2 区域参数，第 26-12 页以获取详细信息。
- 通过 **Route Summarization 选项卡**，您可以配置 ABR。在 OSPF 中，ABR 会将一个区域中的网络通告到另一个区域中。如果您以某种方式分配区域中的网络号来使其连续，则可以将 ABR 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。有关详情，请参见配置 OSPFv2 区域之间的路由汇总，第 26-9 页。

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。

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

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 22-4 页，然后根据定义路由映射，第 24-4 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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Redistribution**。

Redistribution 窗格显示用于将路由从一个路由进程重新分发到 OSPF 路由进程中的规则。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。如果静态路由或已连接路由属于已通过 Setup > Networks 选项卡配置的网络范围，则无需重新分发这些路由。

步骤 2　点击 **Add** 或 **Edit**。

或者，双击 Redistribution 窗格中的表条目 （如有）将为所选条目打开 Add/Edit OSPF Redistribution Entry 复选框。

注意　后面所有步骤都是可选的。

通过 Add/Edit OSPF Redistribution Entry 对话框，您可以在 Redistribution 表中添加新的重新分发规则或编辑现有重新分发规则。编辑现有重新分发规则时，无法更改某些重新分发规则信息。

步骤 3　选择与路由重新分发条目关联的 OSPF 进程。如果编辑的是现有重新分发规则，则无法更改此设置。

步骤 4　选择根据其重新分发路由的源协议。您可以选择以下其中一个选项：

- Static - 将静态路由重新分发到 OSPF 路由进程。
- Connected - 将已连接路由（通过在接口上启用 IP 地址自动建立的路由）重新分发到 OSPF 路由进程。已连接路由重新分发为 AS 的外部路由。
- OSPF - 从另一个 OSPF 路由进程重新分发路由。从列表中选择 OSPF 进程 ID。如果选择此协议，则此对话框中的 Match 选项变为可见。当重新分发静态、已连接、 RIP 或 EIGRP 路由时，这些选项不可用。请跳至步骤 5。
- RIP - 从 RIP 路由进程重新分发路由。
- BGP - 从 BGP 路由进程重新分发路由。
- EIGRP - 从 EIGRP 路由进程重新分发路由。从列表中选择 EIGRP 路由进程的自治系统编号。

步骤 5　如果已为源协议选择 OSPF，请选择用于将路由从另一个 OSPF 路由进程重新分配到所选 OSPF 路由进程中的条件。当重新分发静态、已连接、RIP 或 EIGRP 路由时，这些选项不可用。路由必须与要重新分发的所选条件相匹配。您可以选择以下一个或多个匹配条件：

- Internal - 该路由必须是特定 AS 的内部路由。
- External 1 - 对于自治系统而言属于外部的路由，但是会作为 1 类外部路由导入 OSPF。
- External 2 - 对于自治系统而言属于外部的路由，但是会作为 2 类外部路由导入 OSPF。
- NSSA External 1 - 对于自治系统而言属于外部的路由，但是会作为 2 类 NSSA 路由导入 OSPF。
- NSSA External 2 - 对于自治系统而言属于外部的路由，但是会作为 2 类 NSSA 路由导入 OSPF。

步骤 6　在 Metric Value 字段中，输入进行重新分发的路由的指标值。有效值范围为 1 到 16777214。

在同一设备上从一个 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 OSPF 进程时，如果未指定指标值，则默认指标为 20。

步骤 7　为 Metric Type 选择以下其中一个选项。

- 如果指标是 1 类外部路由，请选择 **1**。
- 如果指标是 2 类外部路由，请选择 **2**。

步骤 8　在 Tag Value 字段中输入标签值。

标签值是附加到 OSPF 本身未使用但可用于在 ASBR 之间传达信息的各外部路由的 32 位十进制值。有效值范围为 0 到 4294967295。

步骤 9　选中 **Use Subnets** 复选框以启用子网路由的重新分发。取消选中此复选框会导致仅重新分发未划分子网的路由。

步骤 10　从 Route Map 下拉列表中选择要应用于重新分发条目的路由映射的名称。

步骤 11　如果需要添加或配置路由映射，请点击 **Manage**。

系统将显示 Configure Route Map 对话框。

步骤 12　点击 **Add** 或 **Edit** 以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。有关详细信息，请参阅定义路由映射，第 24-4 页。

步骤 13　点击 **OK**。

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 26-8 页
- 添加或编辑 OSPF 汇总地址，第 26-9 页

添加路由汇总地址

Summary Address 窗格显示有关为每个 OSPF 路由进程配置的汇总地址的信息。

可以汇总从其他路由协议获知的路由。用于通告汇总的指标是所有较为具体路由的最小指标。汇总路由帮助减小路由表的大小。

对 OSPF 使用汇总路由会导致 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。只能汇总重新分发到 OSPF 中的来自其他路由协议的路由。

注意　OSPF 不支持汇总地址 0.0.0.0 0.0.0.0。

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　在 ASDM 主页中，依次选择 **Configuration > Device Setup > Routing > OSPF > Summary Address**。

步骤 2　点击**添加**。

系统将显示 Add OSPF Summary Address Entry 对话框。您可以向 Summary Address 表中的现有条目添加新条目。编辑现有条目时，无法更改某些汇总地址信息。

步骤 3　从 OSPF Process 下拉列表中选择与汇总地址关联的指定 OSPF 进程 ID。编辑现有条目时，无法更改此信息。

步骤 4　在 **IP Address** 字段中输入汇总地址的 IP 地址。编辑现有条目时，无法更改此信息。

步骤 5　从 Netmask 下拉列表中选择汇总地址的网络掩码。编辑现有条目时，无法更改此信息。

步骤 6　选中 **Advertise** 复选框以通告汇总路由。取消选中此复选框以抑制属于汇总地址的路由。默认情况下，此复选框为选中状态。

标签值显示附加到各外部路由的 32 位十进制值。OSPF 本身未使用此值，但是其可能用于在 ASBR 之间传达信息。

步骤 7　点击 **OK**。

添加或编辑 OSPF 汇总地址

操作步骤

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

步骤 2　点击 **Route Summarization** 选项卡。

系统将显示 Add/Edit a Route Summarization Entry 对话框。

通过 Add/Edit a Route Summarization Entry 对话框，您可以在 Summary Address 表中添加新条目或修改现有条目。编辑现有条目时，无法更改某些汇总地址信息。

步骤 3　从 OSPF Process 下拉列表中选择与汇总地址关联的指定 OSPF 进程 ID。编辑现有条目时，无法更改此信息。

步骤 4　在 IP Address 字段中输入汇总地址的 IP 地址。编辑现有条目时，无法更改此信息。

步骤 5　从 Netmask 下拉列表中输入汇总地址的网络掩码。编辑现有条目时，无法更改此信息。

步骤 6　选中 **Advertise** 复选框以通告汇总路由。取消选中此复选框以抑制属于汇总地址的路由。默认情况下，此复选框为选中状态。

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 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

步骤 2 点击 **Route Summarization** 选项卡。

系统将显示 Add/Edit a Route Summarization Entry 对话框。

通过 Add/Edit a Route Summarization Entry 对话框，您可以在 Summary Address 表中添加新条目或修改现有条目。编辑现有条目时，无法更改某些汇总地址信息。

步骤 3 在 Area ID 字段中输入 OSPF 区域 ID。编辑现有条目时，无法更改此信息。

步骤 4 在 IP Address 字段中输入汇总地址的 IP 地址。编辑现有条目时，无法更改此信息。

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：（即呼叫间隔、停顿间隔和身份验证密钥）。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

在 ASDM 中，通过 Interface 窗格可以配置特定于接口的 OSPF 路由属性，例如 OSPF 消息验证和属性。有两个选项卡可帮助配置 OSPF 中的接口：

- Authentication 选项卡显示 ASA 接口的 OSPF 身份验证信息。
- Properties 选项卡以表格式显示为每个接口定义的 OSPF 属性。

步骤 1 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Interface**。

步骤 2 点击 **Authentication** 选项卡以显示 ASA 接口的身份验证信息。双击表中的行以打开所选接口的 Edit OSPF Authentication Interface 对话框。

步骤 3 点击 **Edit**。

系统将显示 Edit OSPF Authentication Interface 对话框。通过 Edit OSPF Authentication Interface 对话框，您可以配置所选接口的 OSPF 身份验证类型和参数。

步骤 4 根据以下选项从 Authentication 下拉列表中选择身份验证类型：

- **None**，表示禁用 OSPF 身份验证。
- **Authentication Password**，表示使用明文密码身份验证 （在有安全问题的情况下不建议使用）。
- **MD5**，表示使用 MD5 身份验证 （建议）。
- **Area** （默认），表示使用为区域指定的身份验证类型。有关配置区域身份验证的信息，请参阅配置 OSPFv2 区域参数，第 26-12 页。默认情况下，区域身份验证已禁用。因此，除非先前已指定区域身份验证类型，否则设置为使用区域身份验证的接口会禁用身份验证，直到配置此设置为止。

步骤 5　点击 Authentication Password 区域中的单选按钮，该区域包含对于在启用密码身份验证时输入密码的设置。

a. 在 Enter Password 字段中，键入最多八个字符的文本字符串。

b. 在 Re-enter Password 字段中，再次键入密码。

步骤 6　在 ID 字段中输入 MD5 ID 和密钥的设置，其中包括对于在启用 MD5 身份验证时输入 MD5 密钥和参数的设置。接口上所有使用 OSPF 身份验证的设备都必须使用同一 MD5 密钥和 ID。

a. 在 Key ID 字段中，输入数字密钥标识符。有效值范围为 1 到 255。系统将显示所选接口的密钥 ID。

b. 在 Key 字段中，输入最多 16 字节的字母数字字符串。系统将显示所选接口的密钥。

c. 点击 **Add** 或 **Delete** 以在 MD5 ID 和 Key 表中添加或删除指定的 MD5 密钥。

步骤 7　点击 **OK**。

步骤 8　点击 **Properties** 选项卡。

步骤 9　选择要编辑的接口。双击表中的行以打开所选接口的 Properties 选项卡对话框。

步骤 10　点击 **Edit**。

系统将显示 Edit OSPF Interface Properties 对话框。Interface 字段显示正在为其配置 OSPF 属性的接口的名称。您无法编辑此字段。

步骤 11　选中或取消选中 **Broadcast** 复选框以指定接口是广播接口。

默认情况下，对于以太网接口会选中此复选框。取消选中此复选框以将接口指定为点对点非广播接口。将接口指定为点对点非广播可以通过 VPN 隧道传输 OSPF 路由。

当接口配置为点对点非广播时，以下限制适用：

- 只能为接口定义一个邻居。
- 需要手动配置邻居。有关详情，请参见定义静态 OSPFv2 邻居，第 26-16 页。
- 您无需定义指向加密终端的静态路由。有关详情，请参见配置静态路由，第 22-4 页。
- 如果通过隧道执行的 OSPF 是在接口上运行，则上游路由器的常规 OSPF 不能在同一接口上运行。
- 在指定 OSPF 邻居之前应将加密映射绑定到接口，以确保通过 VPN 隧道传递 OSPF 更新。如果在指定 OSPF 邻居之后将加密映射绑定到接口，请使用 **clear local-host all** 命令清除 OSPF 连接，以便可以通过 VPN 隧道建立 OSPF 邻接。

步骤 12　配置以下选项：

- 在 Cost 字段中输入值，该值确定通过接口发送数据包的开销。默认值为 10。
- 在 Priority 字段中，输入 OSPF 路由器优先级值。

  当两个路由器连接到网络时，两者均尝试成为指定路由器。具有更高路由器优先级的设备成为指定路由器。如果有绑定，则具有更高路由器 ID 的路由器成为指定路由器。

  此设置的有效值范围为 0 至 255。默认值为 1。为此设置输入 0 将使路由器不符合成为指定路由器或备用指定路由器的条件。此设置不适用于配置为点对点非广播接口的接口。
- 选中或取消选中 **MTU Ignore** 复选框。

  OSPF 检查邻居在公用接口上是否使用的是同一 MTU。在邻居交换 DBD 数据包时会执行此检查。如果 DBD 数据包中的接收 MTU 高于传入接口上配置的 IP MTU，将不建立 OSPF 邻接。
- 选中或取消选中 **Database filter** 复选框。

  使用此设置在同步和泛洪过程中筛选传出 LSA 接口。默认情况下， OSPF 会在同一区域中的所有接口上泛洪新 LSA，但 LSA 到达的接口除外。在全网状拓扑中，此泛洪可能会浪费带宽并产生过多的链路和 CPU 使用情况。选中此复选框可防止 OSPF 在所选接口上进行 LSA 泛洪。

步骤 13 （可选）点击 **Advanced** 以显示 Edit OSPF Advanced Interface Properties 对话框，通过其可以更改 OSPF 呼叫间隔、重新传输间隔、传输延迟和停顿间隔的值。

通常，仅在网络上遇到 OSPF 问题的情况下才需要根据默认值更改这些值。

步骤 14 在 Intervals 部分中，输入以下各项的值：

- Hello Interval，它指定在接口上发送的呼叫数据包之间的间隔 （以秒为单位）。呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。此值对于特定接口上的所有路由器和接入服务器都必须相同。有效值的范围为 1 到 8192 秒。默认值为 10 秒。
- Retransmit Interval，它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）。当路由器向其邻居发送 LSA 时，它会保留 LSA，直到其接收到确认消息为止。如果路由器没有接收到确认，则将重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。有效值的范围为 1 到 8192 秒。默认值为 5 秒。
- Transmit Delay，它指定在接口上发送 LSA 数据包所需的估计时间（以秒为单位）。更新数据包中的 LSA 在传输之前会按此字段指定的量增大其年龄。如果在通过链路进行传输之前未添加延迟，则不考虑 LSA 通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。有效值的范围为 1 到 8192 秒。默认值为 1 秒。

步骤 15 在 Detecting Lost Neighbors 部分中，执行以下其中一项操作：

- 点击 **Configure interval within which hello packets are not received before the router declares the neighbor to be down**。在 Dead Interval 字段中，指定在其期间未接收到呼叫数据包而导致邻居声明路由器关闭的时间间隔 （以秒为单位）。有效值的范围为 1 到 8192 秒。此设置的默认值是 Hello Interval 字段中设置的间隔的四倍。
- 点击 **Send fast hello packets within 1 seconds dead interval**。在 Hello multiplier 字段中，指定每秒要发送的呼叫数据包的数量。有效值介于 3 和 20 之间。

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。

操作步骤

步骤 1 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

步骤 2 点击 **Area/Networks** 选项卡。

系统将显示 Add OSPF Area 对话框。

步骤 3 选择以下其中一个 Area Type 选项：

- **Normal**，用于使该区域成为标准 OSPF 区域。首次创建区域时，默认情况下会选择此选项。
- **Stub**，用于使该区域成为末节区域。末节区域外没有任何路由器或区域。末节区域防止 AS 外部 LSA（5 类 LSA）泛洪至末节区域中。创建末节区域时，可以通过取消选中 Summary 复选框来选择防止汇总 LSA （3 类和 4 类）泛洪至该区域中。
- **Summary**，用于防止将 LSA 发送到末节区域中，当所定义的区域是末节区域时，请取消选中此复选框。默认情况下，对于末节区域会选中此复选框。

- **NSSA**，用于使区域成为次末节区域。NSSA 接受 7 类 LSA。创建 NSSA 时，可以通过取消选中 Summary 复选框来选择防止汇总 LSA 泛洪至该区域中。您也可以通过取消选中 Redistribute 复选框并选中 Default Information Originate 复选框来禁用路由重新分发。

步骤 4　在 IP Address 字段中输入要添加到区域中的网络或主机的 IP 地址。将 **0.0.0.0** 与子网掩码 **0.0.0.0** 配合使用以创建默认区域。您只能在一个区域中输入 **0.0.0.0**。

步骤 5　在 Network Mask 字段中输入要添加到区域中的 IP 地址或主机的网络掩码。如果添加的是主机，请选择 **255.255.255.255** 掩码。

步骤 6　从以下选项中选择 OSPF 身份验证类型：

- **None**，表示禁用 OSPF 区域身份验证。这是默认设置。
- **Password**，表示提供明文密码进行区域身份验证，在有安全问题的情况下不建议使用。
- **MD5**，表示允许 MD5 身份验证。

步骤 7　在 Default Cost 字段中输入值以指定 OSPF 区域的默认开销。

有效值范围为 0 到 65535。默认值为 1。

步骤 8　点击 **OK**。

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　从 ASDM 主页中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

步骤 2　点击 **Area/Networks** 选项卡。

步骤 3　点击**添加**。

系统将显示 Add OSPF Area 对话框。

步骤 4　点击 Area Type 区域中的 **NSSA** 单选按钮。

选择此选项以使该区域成为次末节区域。NSSA 接受 7 类 LSA。创建 NSSA 时，可以通过取消选中 Summary 复选框来选择防止汇总 LSA 泛洪至该区域中。您也可以通过取消选中 Redistribute 复选框并选中 Default Information Originate 复选框来禁用路由重新分发。

步骤 5 在 IP Address 字段中输入要添加到区域中的网络或主机的 IP 地址。将 **0.0.0.0** 与子网掩码 **0.0.0.0** 配合使用以创建默认区域。您只能在一个区域中输入 **0.0.0.0**。

步骤 6 在 Network Mask 字段中输入要添加到区域中的 IP 地址或主机的网络掩码。如果添加的是主机，请选择 **255.255.255.255** 掩码。

步骤 7 在 Authentication 区域中，点击 **None** 单选按钮以禁用 OSPF 区域身份验证。

步骤 8 在 Default Cost 字段中输入值以指定 OSPF 区域的默认开销。

有效值范围为 0 到 65535。默认值为 1。

步骤 9 点击 **OK**。

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 的单个接口中的路由器 ID 集群池分配 IPv4 地址范围，请执行以下步骤：

步骤 1 从 ASDM 主页中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

步骤 2 点击 **Process Instances** 选项卡。

步骤 3 选择要编辑的 OSPF 进程，然后点击 **Advanced**。

系统将显示 Edit OSPF Process Advanced Properties 对话框。

步骤 4 点击 **Cluster Pool** 单选按钮。如果使用的是集群，则无需指定路由器 ID 的 IP 地址池 （即，将字段留空）。如果不输入 IP 地址池，则 ASA 使用自动生成的路由器 ID。

步骤 5 输入 IP 地址池的名称，或者点击省略号以显示 Select IP Address Pool 对话框。

步骤 6 双击现有 IP 地址池名称以将其添加到 Assign 字段中。或者，点击 **Add** 以创建新 IP 地址池。

系统将显示 Add IPv4 Pool 对话框。

步骤 7 在 Name 字段中输入新 IP 地址池名称。

步骤 8 输入开始 IP 地址，或者点击或省略号以显示 Browse Starting IP Address 对话框。

步骤 9 双击某个条目以将其添加到 Starting IP Address 字段中，然后点击 **OK**。

步骤 10 输入结束 IP 地址，或者点击或省略号以显示 Browse Ending IP Address 对话框。

步骤 11 双击某个条目以将其添加到 Ending IP Address 字段中，然后点击 **OK**。

步骤 12 从下拉列表中选择子网掩码，然后点击 **OK**。

在 Select IP Address Pool 列表中将显示新 IP 地址池。

步骤 13 双击新 IP 地址池名称以将其添加到 Assign 字段中，然后点击 **OK**。

在 Edit OSPF Process Advanced Properties 对话框的 Cluster Pool 字段中将显示新 IP 地址池名称。

步骤 14 点击 **OK**。

步骤 15 如果要更改新添加的 IP 地址池设置，请点击 **Edit**。

系统将显示 Edit IPv4 Pool 对话框。

步骤 16　重复步骤 4 至步骤 14。

注意　无法编辑或删除已分配和已经在由一个或多个连接配置文件使用的现有 IP 地址池。

步骤 17　点击 **OK**。

要为 OSPFv3 的单个接口中的路由器 ID 集群池分配 IPv4 地址范围，请执行以下步骤：

步骤 1　从 ASDM 主页中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup**。

步骤 2　点击 **Process Instances** 选项卡。

步骤 3　选择要编辑的 OSPF 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

步骤 4　从 Router ID 下拉列表选择 Cluster Pool 选项。如果无需指定路由器 ID 的 IP 地址池，请选择 Automatic 选项。如果不配置 IP 地址池，则 ASA 使用自动生成的路由器 ID。

步骤 5　输入 IP 地址池名称。或者，点击省略号以显示 Select IP Address Pool 对话框。

步骤 6　双击现有 IP 地址池名称以将其添加到 Assign 字段中。或者，点击 **Add** 以创建新 IP 地址池。

系统将显示 Add IPv4 Pool 对话框。

步骤 7　在 Name 字段中输入新 IP 地址池名称。

步骤 8　输入开始 IP 地址，或者点击或省略号以显示 Browse Starting IP Address 对话框。

步骤 9　双击某个条目以将其添加到 Starting IP Address 字段中，然后点击 **OK**。

步骤 10　输入结束 IP 地址，或者点击或省略号以显示 Browse Ending IP Address 对话框。

步骤 11　双击某个条目以将其添加到 Ending IP Address 字段中，然后点击 **OK**。

步骤 12　从下拉列表中选择子网掩码，然后点击 **OK**。

在 Select IP Address Pool 列表中将显示新 IP 地址池。

步骤 13　双击新 IP 地址池名称以将其添加到 Assign 字段中，然后点击 **OK**。

在 Edit OSPF Process Advanced Properties 对话框的 Cluster Pool 字段中将显示新 IP 地址池名称。

步骤 14　点击 **OK**。

步骤 15　如果要更改新添加的集群池设置，请点击 **Edit**。

系统将显示 Edit IPv4 Pool 对话框。

步骤 16　重复步骤 4 至步骤 14。

注意　无法编辑或删除已分配和已经在由其他 OSPFv3 进程使用的现有 IP 地址池。

步骤 17　点击 **OK**。

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 22 章“静态路由和默认路由”。

操作步骤

步骤 1 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Static Neighbor**。

步骤 2 点击 **Add** 或 **Edit**。

系统将显示 Add/Edit OSPF Neighbor Entry 对话框。通过此对话框，您可以定义新静态邻居或更改现有静态邻居的信息。您必须为每个点对点非广播接口定义静态邻居。请注意以下限制：

- 不能为两个不同的 OSPF 进程定义同一静态邻居。
- 需要为每个静态邻居定义静态路由。

步骤 3 从 OSPF Process 下拉列表中，选择与静态邻居关联的 OSPF 进程。如果编辑的是现有静态邻居，则无法更改该值。

步骤 4 在 Neighbor 字段中，输入静态邻居的 IP 地址。

步骤 5 在 Interface 字段中，选择与静态邻居关联的接口。如果编辑的是现有静态邻居，则无法更改该值。

步骤 6 点击 **OK**。

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 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

步骤 2 点击 **Process Instances** 选项卡。

步骤 3 选择要编辑的 OSPF 进程，然后点击 **Advanced**。

系统将显示 Edit OSPF Process Advanced Properties 对话框。

步骤 4 通过 Timers 区域，您可以修改用于配置 LSA 步调计时器和 SPF 计算计时器的设置。在 Timers 区域中，输入以下值：

- Initial SPF Delay，指定 OSPF 接收拓扑更改时和 SPF 计算启动时间隔的时间 （以毫秒为单位）。有效值的范围为 0 到 600000 秒。
- Minimum SPF Hold Time，指定连续 SPF 计算之间的保持时间（以毫秒为单位）。有效值范围为 0 至 600000 毫秒。
- Maximum SPF Wait Time，指定两次连续 SPF 计算间隔的最长等待时间。有效值的范围为 0 到 600000 秒。

步骤 5 点击 **OK**。

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。

操作步骤

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

步骤 2　点击 **Process Instances** 选项卡。

步骤 3　点击 **Advanced**。

系统将显示 Edit OSPF Process Advanced Properties 对话框。

步骤 4　Adjacency Changes 区域包含用于定义导致发送系统日志消息的邻接更改的设置。在 Adjacency Changes 区域中，输入以下值：

- 选中 **Log Adjacency Changes** 复选框以使 ASA 只要 OSPFv2 邻居启动或关闭便发送系统日志消息。默认情况下，此设置处于选中状态。
- 选中 **Log Adjacency Changes Detail** 复选框以使 ASA 只要发生任何状态更改便发送系统日志消息，而不只是在邻居启动或关闭时发送系统日志消息。默认情况下，此设置处于未选中状态。

步骤 5　点击 **OK**。

注意　必须启用日志记录才能发送邻居启动或关闭消息。

在 OSPF 中配置筛选

Filtering 窗格显示已为每个 OSPF 进程配置的 ABR 3 类 LSA 过滤器。

ABR 3 类 LSA 过滤器仅允许将指定的前缀从一个区域发送到另一个区域，并会限制其他所有前缀。此类型的区域筛选可以应用在特定 OSPF 区域外、应用到特定 OSPF 区域中，或者同时在相同 OSPF 区域的内外进行应用。

OSPF ABR 3 类 LSA 筛选可提高对 OSPF 区域之间路由重新分发的控制。

备注　系统仅筛选源于 ABR 的 3 类 LSA。

要在 OSPF 中配置筛选，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Filtering**。

步骤 2　点击 **Add** 或 **Edit**。

通过 Add/Edit OSPF Filtering Entry 对话框，您可以向过滤器表中添加新过滤器或修改现有过滤器。编辑现有过滤器时，某些筛选信息无法更改。

步骤 3　从 OSPF Process 下拉列表中选择与过滤器条目关联的 OSPF 进程。

步骤 4　从 Area ID 下拉列表中选择与过滤器条目关联的区域 ID。如果编辑的是现有过滤器条目，则无法修改此设置。

步骤 5　从 Prefix List 下拉列表中选择前缀列表。

步骤 6 从 Traffic Direction 下拉列表中选择筛选的流量方向。

选择 Inbound 以筛选传入 OSPF 区域的 LSA，或者选择 Outbound 以筛选传出 OSPF 区域的 LSA。如果编辑的是现有过滤器条目，则无法修改此设置。

步骤 7 点击 **Manage** 以显示 Configure Prefix Lists 对话框，您可以从中添加、编辑或删除前缀列表和规则前缀。有关详细信息，请参阅配置前缀列表，第 24-7 页和为路由操作配置指标值，第 24-7 页。

步骤 8 点击 **OK**。

在 OSPF 中配置虚拟链路

如果将区域添加到 OSPF 网络，并且无法将该区域直接连接到主干区域，则需要创建虚拟链路。虚拟链路连接具有公共区域 （称为中转区域）的两台 OSPF 设备。其中一台 OSPF 设备必须连接到主干区域。

要定义新虚拟链路或更改现有虚拟链路的属性，请执行以下步骤：

步骤 1 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Virtual Link**。

步骤 2 点击 **Add** 或 **Edit**。

系统将显示 Add/Edit OSPF Virtual Link 对话框，通过其可以定义新虚拟链路或更改现有虚拟链路的属性。

步骤 3 从 OSPF Process 下拉列表中选择与虚拟链路关联的 OSPF 进程 ID。如果编辑的是现有虚拟链路条目，则无法修改此设置。

步骤 4 从 Area ID 下拉列表中选择与虚拟链路关联的区域 ID。

选择 OSPF 邻居设备共享的区域。所选区域不能是 NSSA 区域或末节区域。如果编辑的是现有虚拟链路条目，则无法修改此设置。

步骤 5 在 Peer Router ID 字段中，输入虚拟链路邻居的路由器 ID。

如果编辑的是现有虚拟链路条目，则无法修改此设置。

步骤 6 点击 **Advanced** 以编辑高级虚拟链路属性。

系统将显示 Advanced OSPF Virtual Link Properties 对话框。您可以在此区域中配置虚拟链路的 OSPF 属性。这些属性包括身份验证和数据包间隔设置。

步骤 7 在 Authentication 区域中，通过点击以下其中一个选项旁边的单选按钮来选择身份验证类型：

- **None**，表示禁用 OSPF 身份验证。
- **Authentication Password**，表示使用明文密码身份验证。在有安全问题的情况下不推荐此选项。
- **MD5**，表示使用 MD5 身份验证 （建议）。
- **Area** （默认），表示使用为区域指定的身份验证类型。有关配置区域身份验证的信息，请参阅配置 OSPFv2 区域参数，第 26-12 页。默认情况下，区域身份验证已禁用。因此，除非先前已指定区域身份验证类型，否则设置为使用区域身份验证的接口会禁用身份验证，直到配置此设置为止。

步骤 8 在 Authentication Password 区域中，启用密码身份验证后输入并重新输入密码。密码必须是最多 8 个字符的文本字符串。

步骤 9　在 MD5 IDs and Key 区域中，启用 MD5 身份验证后输入 MD5 密钥和参数。接口上所有使用 OSPF 身份验证的设备都必须使用同一 MD5 密钥和 ID。指定以下设置：

a. 在 Key ID 字段中，输入数字密钥标识符。有效值范围为 1 到 255。系统将显示所选接口的密钥 ID。

b. 在 Key 字段中，输入最多 16 字节的字母数字字符串。系统将显示所选接口的密钥 ID。

c. 点击 **Add** 或 **Delete** 以在 MD5 ID 和 Key 表中添加或删除指定的 MD5 密钥。

步骤 10　在 Interval 区域中，通过从以下选项中选择来指定数据包的间隔时间：

- **Hello Interval**，用于指定在接口上发送的呼叫数据包之间的间隔 （以秒为单位）。呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。此值对于特定接口上的所有路由器和接入服务器都必须相同。有效值的范围为 1 到 65535 秒。默认值为 10 秒。
- **Retransmit Interval**，用于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）。当路由器向其邻居发送 LSA 时，它会保留 LSA，直到其接收到确认消息为止。如果路由器没有接收到确认，则将重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。有效值的范围为 1 到 65535 秒。默认值为 5 秒。
- **Transmit Delay**，用于指定在接口上发送 LSA 数据包所需的估计时间 （以秒为单位）。更新数据包中的 LSA 在传输之前会按此字段指定的量增大其年龄。如果在通过链路进行传输之前未添加延迟，则不考虑 LSA 通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。有效值的范围为 1 到 65535 秒。默认值为 1 秒。
- **Dead Interval**，用于指定在其期间未接收到呼叫数据包而导致邻居声明路由器关闭的间隔（以秒为单位）。有效值范围为 1 到 65535。此字段的默认值是 Hello Interval 字段设置的间隔的四倍。

步骤 11　点击 **OK**。

配置 OSPFv3

本节介绍如何配置 OSPFv3 路由进程。

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 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup**。

步骤 2 在 Process Instances 选项卡上，选中 **Enable OSPFv3 Process** 复选框。您最多可以启用两个 OSPF 进程实例。仅支持单情景模式。

步骤 3 在 Process ID 字段中输入进程 ID。ID 可以是任何正整数。

步骤 4 点击 **Apply** 保存更改。

步骤 5 要继续，请参阅配置 OSPFv3 区域参数，第 26-21 页。

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：（即呼叫间隔和停顿间隔）。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 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Interfaces**。

步骤 2 点击 **Authentication** 选项卡。

步骤 3 要指定接口的身份验证参数，请选择该接口并点击 **Edit**。

系统将显示 Edit OSPFv3 Interface Authentication 对话框。

步骤 4 从 Authentication Type 下拉列表中选择身份验证类型。可用选项为 Area、Interface 和 None。None 选项表示未使用身份验证。

步骤 5 从 Authentication Algorithm 下拉列表中选择身份验证算法。支持的值为 SHA-1 和 MD5。

步骤 6 在 Authentication Key 字段中输入身份验证密钥。使用 MD5 身份验证时，密钥长度必须为 32 位十六进制数字（16 字节）。使用 SHA-1 身份验证时，密钥长度必须为 40 位十六进制数字（20 字节）。

步骤 7 从 Encryption Algorithm 下拉列表中选择加密算法。支持的值为 AES-CDC、3DES 和 DES。NULL 条目表示不加密。

步骤 8 在 Encryption Key 字段中输入加密密钥。

步骤 9 点击 **OK**。

步骤 10 点击 **Properties** 选项卡。

步骤 11 选择要修改其属性的接口，然后点击 **Edit**。

系统将显示 Edit OSPFv3 Interface Properties 对话框。

步骤 12 选中 **Enable OSPFv3 on this interface** 复选框。

步骤 13 从下拉列表中选择进程 ID。

步骤 14 从下拉列表中选择区域 ID。

步骤 15　（可选）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 16　从下拉列表中选择网络类型。支持的选项为 Default、 Broadcast 和 Point-to-Point。

步骤 17　在 Cost 字段中输入在接口上发送数据包的开销。

步骤 18　在 Priority 字段中输入用于帮助确定网络的指定路由器的路由器优先级。有效值范围为 0 到 255。

步骤 19　收到 DBD 数据包后，选中 **Disable MTU mismatch detection** 复选框以禁用 OSPF MTU 不匹配检测。默认情况下， OSPF MTU 不匹配检测已启用。

步骤 20　选中 **Filter outgoing link state advertisements** 复选框以筛选到 OSPFv3 接口的传出 LSA。默认情况下，所有传出 LSA 都泛洪至该接口。

步骤 21　在 Timers 区域中的 Dead Interval 字段内，输入在邻居表明路由器关闭之前不得查看呼叫数据包的时间段 （以秒为单位）。该值必须对于同一网络上的所有节点都相同，并且范围可以是 1 至 65535。

步骤 22　在 Hello Interval 字段中，输入接口上发送的呼叫数据包之间的间隔 （以秒为单位）。该值必须对于特定网络上的所有节点都相同，并且范围可以是 1 至 65535。默认间隔对于以太网接口为 10 秒，对于非广播接口为 30 秒。

步骤 23　在 Retransmit Interval 字段中，输入属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）。该时间必须大于连接的网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。默认值为 5 秒。

步骤 24　在 Transmit Delay 字段中，输入在接口上发送链路状态更新数据包所需的估计时间 （以秒为单位）。有效值的范围为 1 到 65535 秒。默认值为 1 秒。

步骤 25　点击 **OK**。

步骤 26　点击 **Apply** 保存更改。

配置 OSPFv3 区域参数

操作步骤

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup**。

步骤 2　点击 **Areas** 选项卡。

步骤 3　要添加新区域，请点击 **Add**。要修改现有区域，请点击 **Edit**。要删除所选区域，请点击 **Delete**。

系统将显示 Add OSPFv3 Area 对话框或 Edit OSPFv3 Area 对话框。

步骤 4　从 OSPFv3 Process ID 下拉列表中，选择进程 ID。

步骤 5　在 Area ID 字段中输入区域 ID，它指定要为其汇总路由的区域。

步骤 6　从 Area Type 下拉列表中选择区域类型。可用选项为 Normal、 NSSA 和 Stub。

步骤 7　要允许将汇总 LSA 发送到区域中，请选中 **Allow sending of summary LSAs into the area** 复选框。

步骤 8　要允许重新分发以将路由导入到普通区域和次末节区域，请选中 **Redistribution imports routes to normal and NSSA areas** 复选框。

步骤 9　要生成到 OSPFv3 路由域中的默认外部路由，请选中 **Default information originate** 复选框。

步骤 10　在 Metric 字段中输入用于生成默认路由的指标。默认值为 10。有效十进制值范围为 0 到 16777214。

步骤 11 从 Metric Type 下拉列表中选择指标类型。指标类型是与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。可用选项为 1 （表示 1 类外部路由）或 2 （表示 2 类外部路由）。

步骤 12 在 Default Cost 字段中输入开销。

步骤 13 点击 **OK**。

步骤 14 点击 **Route Summarization** 选项卡。

步骤 15 要指定整合与汇总路由的新范围，请点击 **Add**。要修改整合与汇总路由的现有范围，请点击 **Edit**。

系统将显示 Add Route Summarization 对话框或 Edit Route Summarization 对话框。

步骤 16 从 Process ID 下拉列表中选择进程 ID。

步骤 17 从 Area ID 下拉列表中选择区域 ID。

步骤 18 在 IPv6 Prefix/Prefix Length 字段中输入 IPv6 前缀和前缀长度。

步骤 19 （可选）输入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 20 选中 **Advertised** 复选框以将地址范围状态设置为已通告并生成 3 类汇总 LSA。

步骤 21 点击 **OK**。

步骤 22 要继续，请参阅配置虚拟链路邻居，第 26-22 页。

配置虚拟链路邻居

要配置虚拟链路邻居，请执行以下步骤：

步骤 1 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Virtual Link**。

步骤 2 要添加新虚拟链路邻居，请点击 **Add**。要修改现有虚拟链路邻居，请点击 **Edit**。要删除所选虚拟链路邻居，请点击 **Delete**。

系统将显示 Add Virtual Link 对话框或 Edit Virtual Link 对话框。

步骤 3 从 Process ID 下拉列表中选择进程 ID。

步骤 4 从 Area ID 下拉列表中选择区域 ID。

步骤 5 在 Peer Router ID 字段中输入对等路由器 ID （即 IP 地址）。

步骤 6 （可选）在 TTL Security 字段中输入虚拟链路上的生存时间 (TTL) 安全跃点计数。跃点计数值范围可以为 1 至 254。

步骤 7 在 Timers 区域中的 Dead Interval 字段内输入在邻居表明路由器关闭之前看不到呼叫数据包的时间（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。

步骤 8 在 Hello Interval 字段中输入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。

步骤 9 在 Retransmit Interval 字段中输入属于接口的邻接的 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。

步骤 10　在 Transmit Delay 字段中输入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。

步骤 11　在 Authentication 区域中，选中 **Enable Authentication** 复选框以启用身份验证。

步骤 12　在 Security Policy Index 字段中输入安全策略索引，它必须是从 256 至 4294967295 的数字。

步骤 13　从 Authentication Algorithm 下拉列表中选择身份验证算法。支持的值为 SHA-1 和 MD5。使用 MD5 身份验证时，密钥长度必须为 32 位十六进制数字（16 字节）。使用 SHA-1 身份验证时，密钥长度必须为 40 位十六进制数字 （20 字节）。

步骤 14　在 Authentication Key 字段中输入身份验证密钥。密钥必须包含 32 个十六进制字符。

步骤 15　从 Encryption Algorithm 下拉列表中选择加密算法。支持的值为 AES-CDC、3DES 和 DES。NULL 条目表示不加密。

步骤 16　在 Encryption Key 字段中输入加密密钥。

步骤 17　点击 **OK**。

步骤 18　点击 **Apply** 保存更改。

配置 OSPFv3 被动接口

操作步骤

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup**。

步骤 2　点击 **Process Instances** 选项卡。

步骤 3　选择要编辑的 OSPFv3 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

步骤 4　通过 Passive Interfaces 区域，您可以在接口上启用备用 OSPFv3 路由。备用路由帮助控制 OSPFv3 路由信息的通告并禁用在接口上发送和接收 OSPFv3 路由更新。在 Passive Interfaces 区域中，选择以下设置：

- 选中 **Global passive** 复选框以使表中列出的所有接口都成为被动接口。取消选中单个接口以使其成为非被动接口。
- 取消选中 **Global passive** 复选框以使所有接口都成为非被动接口。选中单个接口以使其成为被动接口。

步骤 5　点击 **OK**。

步骤 6　点击 **Apply** 保存更改。

配置 OSPFv3 管理距离

操作步骤

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup**。

步骤 2　点击 **Process Instances** 选项卡。

步骤 3 选择要编辑的 OSPF 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

通过 Administrative Route Distances 区域，您可以修改用于配置管理路由距离的设置。管理路由距离是从 10 至 254 的整数。在 Administrative Route Distances 区域中，输入以下值：

- Inter Area，用于指定 OSPV 的区域间路由作为 IPv6 路由。
- Intra Area，用于指定 OSPF 的区域内路由作为 IPv6 路由。
- External，用于指定 OSPF 的外部 5 类和 7 类路由作为 IP6 路由。

步骤 4 点击 **OK**。

步骤 5 点击 **Apply** 保存更改。

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 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup**。

步骤 2 点击 **Process Instances** 选项卡。

步骤 3 选择要编辑的 OSPFv3 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

步骤 4 通过 Timers 区域，您可以修改用于配置 LSA 到达时间、 LSA 步调设置时间、 LSA 重新传输时间、 LSA 调速时间和 SPF 调速时间的设置。在 Timers 区域中，输入以下值：

- LSA Arrival，用于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 6000,000 毫秒。默认值为 1000 毫秒。
- LSA Flood Pacing，用于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。
- LSA Group Pacing，用于指定将 LSA 收集到组中并刷新、校验和或老化的间隔 （以秒为单位）。有效值范围为 10 到 1800。默认值为 240。
- LSA Retransmission Pacing，用于指定重新传输队列中 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。
- LSA Throttle Initial，用于指定生成 LSA 的第一次出现所需的延迟 （以毫秒为单位）。默认值为 0 毫秒。
- LSA Throttle Min Hold，用于指定发起同一 LSA 所需的最小延迟 （以毫秒为单位）。默认值为 5000 毫秒。
- LSA Throttle Max Wait，用于指定发起同一 LSA 所需的最大延迟 （以毫秒为单位）。默认值为 5000 毫秒。

注意 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。

- SPF Throttle Initial，用于指定接收对 SPF 计算的更改所需的延迟 （以毫秒为单位）。默认值为 5000 毫秒。
- SPF Throttle Min Hold，用于指定第一次和第二次 SPF 计算之间的延迟 （以毫秒为单位）。默认值为 10000 毫秒。
- SPF Throttle Max Wait，用于指定 SPF 计算最长等待时间 （以毫秒为单位）。默认值为 10000 毫秒。

注意　对于 SPF 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。

步骤 5　点击 **OK**。

步骤 6　点击 **Apply** 保存更改。

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 22 章“静态路由和默认路由”。

操作步骤

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Static Neighbor**。

步骤 2　点击 **Add** 或 **Edit**。

系统将显示 Add/Edit Static Neighbor 对话框。通过此对话框，您可以定义新静态邻居或更改现有静态邻居的信息。您必须为每个点对点非广播接口定义静态邻居。请注意以下限制：

- 不能为两个不同的 OSPFv3 进程定义同一静态邻居。
- 需要为每个静态邻居定义静态路由。

步骤 3　从 Interface 下拉列表中，选择与静态邻居关联的接口。如果编辑的是现有静态邻居，则无法更改该值。

步骤 4　在 Link-local Address 字段中，输入静态邻居的 IPv6 地址。

步骤 5　（可选）在 Priority 字段中，输入优先级。

步骤 6　（可选）在 Poll Interval 字段中，输入轮询间隔 （以秒为单位）。

步骤 7　点击 **OK**。

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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup**。

步骤 2　点击 **Process Instances** 选项卡。

步骤 3　选择要编辑的 OSPF 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

通过 Adjacency Changes 区域，您可以修改在 OSPFv3 邻居启动或关闭时发送系统日志消息的设置。在 Adjacency Changes 区域中，执行以下操作：

- 要在 OSPFv3 邻居启动或关闭时发送系统日志消息，请选中 **Log Adjacency Changes** 复选框。
- 要为每个状态发送系统日志消息，而不只是在 OSPFv3 邻居启动或关闭时才发送系统日志消息，请选中 **Include Details** 复选框。

步骤 4　点击 **OK**。

步骤 5　点击 **Apply** 保存更改。

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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup**。

步骤 2　点击 **Process Instances** 选项卡。

步骤 3　选择要编辑的 OSPFv3 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

步骤 4　选中 **Ignore LSA MOSPF** 复选框，然后点击 **OK**。

计算汇总路由开销

操作步骤

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup**。

步骤 2　点击 **Process Instances** 选项卡。

步骤 3　选择要编辑的 OSPF 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

步骤 4　选中 **RFC1583 Compatible** 复选框，然后点击 **OK**。

生成到 OSPFv3 路由域中的默认外部路由

操作步骤

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup**。

步骤 2　点击 **Process Instances** 选项卡。

步骤 3　选择要编辑的 OSPFv3 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

步骤 4　在 Default Information Originate Area 中，执行以下操作：

a. 选中 **Enable** 复选框以启用 OSPFv3 路由进程。

b. 选中 **Always advertise** 复选框以始终通告默认路由 （无论其是否存在）。

c. 在 Metric 字段中输入用于生成默认路由的指标。有效十进制值范围为 0 到 16777214。默认值为 10。

d. 从 Metric Type 下拉列表中，选择与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。有效值包括以下值：

- 1 - 1 类外部路由
- 2 - 2 类外部路由

默认为 2 类外部路由。

e. 从 Route Map 下拉列表中，选择在满足路由的情况下生成默认路由的路由进程。

步骤 5　点击 **OK**。

步骤 6　点击 **Apply** 保存更改。

配置 IPv6 汇总前缀

操作步骤

步骤 1　在 ASDM 主窗口中，选择 **Configuration > Device Setup > Routing > OSPFv3 > Summary Prefix**。

步骤 2　要添加新汇总前缀，请点击 **Add**。要修改现有汇总前缀，请点击 **Edit**。要删除汇总前缀，请点击 **Delete**。

系统将显示 Add Summary Prefix 对话框或 Edit Summary Prefix 对话框。

步骤 3　从 Process ID 下拉列表中选择进程 ID。

步骤 4　在 IPv6 Prefix/Prefix Length 字段中输入 IPv6 前缀和前缀长度。

步骤 5　选中 **Advertise** 复选框以通告与指定前缀/掩码对匹配的路由。取消选中此复选框以抑制与指定前缀/掩码对匹配的路由。

步骤 6　在 Tag 字段中输入可用作通过路由映射控制重新分发的匹配值的标签值。

步骤 7　点击 **OK**。

步骤 8　点击 **Apply** 保存更改。

重新分发 IPv6 路由

操作步骤

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Redistribution**。

步骤 2　要添加用于将已连接路由重新分发到 OSPFv3 进程中的新参数，请点击 **Add**。要修改用于将已连接路由重新分发到 OSPFv3 进程中的现有参数，请点击 **Edit**。要删除所选参数集，请点击 **Delete**。

系统将显示 Add Redistribution 对话框或 Edit Redistribution 对话框。

步骤 3　从 Process ID 下拉列表中选择进程 ID。

步骤 4　从 Source Protocol 下拉列表中选择从其重新分发路由的源协议。支持的协议为 connected、 static 和 OSPF。

步骤 5　在 Metric 字段中输入指标值。在同一路由器上将路由从一个 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 OSPF 进程时，如果未指定指标值，则默认指标为 20。

步骤 6　从 Metric Type 下拉列表中选择指标类型。可用选项为 None、 1 和 2。

步骤 7　（可选）在 Tag 字段中输入标签值。此参数指定连接到每个外部路由的 32 位十进制值，该值可用于在 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。有效值为 0 到 4294967295。

步骤 8　从 Route Map 下拉列表中选择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。如果未指定此参数，则会重新分发所有路由。如果已指定此参数，但未列出路由映射标签，则不会导入任何路由。

步骤 9　要在重新分发中包含已连接路由，请选中 **Include connected** 复选框。

步骤 10　选中 **Match** 复选框以将路由重新分发到其他路由域中，然后选中以下其中一个复选框：

- **Internal**，表示特定自治系统的内部路由
- **External 1**，表示自治系统的外部路由，但会作为 1 类外部路由导入 OSPFv3
- **External 2**，表示自治系统的外部路由，但会作为 2 类外部路由导入 OSPFv3
- **NSSA External 1**，表示自治系统的外部路由，但会在 IPv6 的 NSSA 中作为 1 类外部路由导入到 OSPFv3 中
- **NSSA External 2**，表示自治系统的外部路由，但会在 IPv6 的 NSSA 中作为 2 类外部路由导入到 OSPFv3 中

步骤 11　点击 **OK**。

步骤 12　点击 **Apply** 保存更改。

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。

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 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup > Advanced > Add NSF Properties**。

步骤 2　在 Configuring Cisco NSF 下，选中 **Enable Cisco nonstop forwarding (NSF)** 复选框。

步骤 3　（可选）如果需要，请选中 **Cancels NSF restart when non-NSF-aware neighboring networking devices are detected** 复选框。

步骤 4　（可选）在 Configuring Cisco NSF 助手下，取消选中 **Enable Cisco nonstop forwarding (NSF) for helper mode** 复选框。

备注 默认情况下，此复选框处于选中状态。取消选中此复选框将在支持 NSF 感知的设备上禁用思科 NSF 助手模式。

步骤 5 点击 **OK**。

步骤 6 点击 **Apply** 保存更改。

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 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup > Advanced > Add NSF Properties**。

步骤 2 在 Configuring IETF NSF 下，选中 **Enable IETF nonstop forwarding (NSF)** 复选框。

步骤 3 （可选）在 Length of graceful restart interval 字段中输入重启间隔。

备注 默认值为 120 秒。对于低于 30 秒的重启间隔，将终止平稳重启。

步骤 4 （可选）在 Configuring IETF NSF 助手下，取消选中 **Enable IETF nonstop forwarding (NSF) for helper mode** 复选框。

备注 默认情况下，此复选框处于选中状态。取消选中此复选框将在支持 NSF 感知的设备上禁用 IETF NSF 助手模式。

步骤 5 点击 **OK**。

步骤 6 点击 **Apply** 保存更改。

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 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup > Advanced > Add NSF Properties**。

步骤 2 在 Configuring Graceful Restart 下，选中 **Enable Graceful Restart** 复选框。

步骤 3 （可选）在 Restart Interval 字段中输入重启间隔值。

备注　默认值为 120 秒。对于低于 30 秒的重启间隔，将终止平稳重启。

步骤 4　在 Configuring Graceful Restart Helper 下，选中 **Enable Graceful Restart Helper** 复选框。

备注　默认情况下，此复选框处于选中状态。取消选中此复选框将在支持 NSF 感知的设备上禁用平稳重启助手模式。

步骤 5　（可选）选中 **Enable LSA checking** 复选框以启用严格链路状态通告检查。

备注　启用后，它指示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 LSA 发生会泛洪至重新启动的路由器的更改，或者在发起平稳重启过程时重新启动的路由器的重新传输列表上有已更改的 LSA。

步骤 6　点击 **OK**。

步骤 7　点击 **Apply** 保存更改。

删除 OSPF 配置

删除 OSPFv2 配置。

操作步骤

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

步骤 2　取消选中 **Enable this OSPF Process** 复选框。

步骤 3　点击 **Apply**。

删除 OSPFv3 配置。

操作步骤

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup**。

步骤 2　取消选中 **Enable OSPFv3 Process** 复选框。

步骤 3　点击 **Apply**。

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 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

步骤 2 点击 **Process Instances** 选项卡，并在 OSPF Process 1 字段中键入 **2**。

步骤 3 点击 **Area/Networks** 选项卡，然后点击 **Add**。

步骤 4 在 Area ID 字段中输入 **0**。

步骤 5 在 Area Networks 区域中的 IP Address 字段内输入 **10.0.0.0**。

步骤 6 从 Netmask 下拉列表中选择 255.0.0.0。

步骤 7 点击 **OK**。

步骤 8 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Redistribution**。

步骤 9 点击**添加**。

系统将显示 Add/Edit OSPF Redistribution Entry 对话框。

步骤 10 在 Protocol 区域中，点击 **OSPF** 单选按钮以选择从其重新分发路由的源协议。选择 OSPF 将从其他 OSPF 路由进程重新分发路由。

步骤 11 从 OSPF Process 下拉列表中选择 OSPF 进程 ID。

步骤 12 在 Match 区域中，选中 **Internal** 复选框。

步骤 13 在 Metric Value 字段中，输入 **5** 作为进行重新分发的路由的指标值。

步骤 14 从 Metric Type 下拉列表中，选择 1 作为 Metric Type 值。

步骤 15 从 Route Map 下拉列表中，选择 1。

步骤 16 点击 **OK**。

步骤 17 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Interface**。

步骤 18 从 Properties 选项卡中，选择 **inside** 接口，然后点击 **Edit**。

系统将显示 Edit OSPF Properties 对话框。

步骤 19 在 Cost 字段中，输入 **20**。

步骤 20 点击 **Advanced**。

步骤 21 在 Retransmit Interval 字段中，输入 **15**。

步骤 22 在 Transmit Delay 字段中，输入 **20**。

步骤 23 在 Hello Interval 字段中，输入 **10**。

步骤 24 在 Dead Interval 字段中，输入 **40**。

步骤 25 点击 **OK**。

步骤 26 在 Edit OSPF Properties 对话框中的 Priorities 字段内输入 **20**，然后点击 **OK**。

步骤 27 点击 **Authentication** 选项卡。

系统将显示 Edit OSPF Authentication 对话框。

步骤 28 在 Authentication 区域中，点击 **MD5** 单选按钮。

步骤 29 在 MD5 and Key ID 区域中，在 MD5 Key 字段内输入 **cisco**，在 MD5 Key ID 字段内输入 **1**。

步骤 30 点击 **OK**。

步骤 31　依次选择 **Configuration > Device Setup > Routing > OSPF > Setup**，然后点击 **Area/Networks** 选项卡。

步骤 32　选择 **OSPF 2** 进程，然后点击 **Edit**。

系统将显示 Edit OSPF Area 对话框。

步骤 33　在 Area Type 区域中，选择 **Stub**。

步骤 34　在 Authentication 区域中，选择 **None**，然后在 Default Cost 字段中输入 **20**。

步骤 35　点击 **OK**。

步骤 36　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

步骤 37　点击 **Process Instances** 选项卡，然后选中 **OSPF process 2** 复选框。

步骤 38　点击 **Advanced**。

系统将显示 Edit OSPF Area 对话框。

步骤 39　在 Timers 区域中，在 SPF Delay Time 字段内输入 **10**，在 SPF Hold Time 字段内输入 **20**。

步骤 40　在 Adjacency Changes 区域中，选中 **Log Adjacency Change Details** 复选框。

步骤 41　点击 **OK**。

步骤 42　点击 **Reset**。

OSPFv3 示

以下示例显示如何在 ASDM 中配置 OSPFv3 路由：

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup**。

步骤 2　在 Process Instances 选项卡上，执行以下操作：

a. 选中 **Enable OSPFv3 Process** 复选框。

b. 在 Process ID 字段中输入 **1**。

步骤 3　点击 **Areas** 选项卡，然后点击 **Add** 以显示 Add OSPFv3 Area 对话框。

步骤 4　从 OSPFv3 Process ID 下拉列表中，选择 **1**。

步骤 5　在 Area ID 字段中输入 **22**。

步骤 6　从 Area Type 下拉列表中选择 **Normal**。

步骤 7　在 Default Cost 字段中输入 **10**。

步骤 8　选中 **Redistribution imports routes to normal and NSSA areas** 复选框。

步骤 9　在 Metric 字段中输入 **20**。

步骤 10　从 Metric Type 下拉列表中选择 **1**。

步骤 11　选中 **inside** 复选框作为使用的指定接口。

步骤 12　选中 **Enable Authentication** 复选框。

步骤 13　在 Security Policy Index 字段中输入 **300**。

步骤 14　从 Authentication Algorithm 下拉列表中选择 **SHA-1**。

步骤 15　在 Authentication Key 字段中输入 **12345ABCDE**。

步骤 16　从 Encryption Algorithm 下拉列表中选择 **DES**。

步骤 17　在 Encryption Key 字段中输入 **1122334455aabbccddee**。

步骤 18　点击 **OK**。

步骤 19　点击 **Route Summarization** 选项卡，然后点击 **Add** 以显示 Add Route Summarization 对话框。

步骤 20　从 Process ID 下拉列表中选择 **1**。

步骤 21　从 Area ID 下拉列表中选择 **22**。

步骤 22　在 IPv6 Prefix/Prefix Length 字段中输入 **2000:122::/64**。

步骤 23　（可选）在 Cost 字段中输入 **100**。

步骤 24　选中 **Advertised** 复选框。

步骤 25　点击 **OK**。

步骤 26　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Interface**。

步骤 27　点击 **Properties** 选项卡。

步骤 28　选中 **inside** 复选框，然后点击 **Edit** 以显示 Edit OSPF Properties 对话框。

步骤 29　在 Cost 字段中，输入 **20**。

步骤 30　在 Priority 字段中输入 **1**。

步骤 31　选中 **point-to-point** 复选框。

步骤 32　在 Dead Interval 字段中，输入 **40**。

步骤 33　在 Hello Interval 字段中，输入 **10**。

步骤 34　在 Retransmit Interval 字段中，输入 **15**。

步骤 35　在 Transmit Delay 字段中，输入 **20**。

步骤 36　点击 **OK**。

步骤 37　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > Redistribution**。

步骤 38　从 Process ID 下拉列表中选择 **1**。

步骤 39　从 Source Protocol 下拉列表中选择 **OSPF**。

步骤 40　在 Metric 字段中输入 **50**。

步骤 41　从 Metric Type 下拉列表中选择 **1**。

步骤 42　点击 **OK**。

步骤 43　点击 **Apply** 保存更改。

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。

要在 ASDM 中监控或显示各种 OSPFv2 路由统计，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，依次选择 **Monitoring > Routing > OSPF LSAs**。

步骤 2　您可以选择并监控 OSPF LSA， 1 类至 5 类和 7 类。每个窗格显示一种 LSA 类型，如下所示：

- 1 类 LSA 表示进程下区域中的路由。
- 2 类 LSA 显示通告路由器的指定路由器的 IP 地址。
- 3 类 LSA 显示目标网络的 IP 地址。
- 4 类 LSA 显示 AS 边界路由器的 IP 地址。
- 5 类 LSA 和 7 类 LSA 显示 AS 外部网络的 IP 地址。

步骤 3　点击 **Refresh** 以更新每个 LSA 类型窗格。

步骤 4　在 ASDM 主窗口中，依次选择 **Monitoring > Routing > OSPF Neighbors**。

在 OSPF Neighbors 窗格中，每行表示一个 OSPF 邻居。此外，OSPF Neighbors 窗格还会显示邻居运行所在的网络、优先级、状态、停顿时间量 （以秒为单位）、邻居的 IP 地址及其运行所在的接口。有关 OSPF 邻居的可能状态的列表，请参阅 RFC 2328。

步骤 5　点击 **Refresh** 以更新 OSPF Neighbors 窗格。

要在 ASDM 中监控或显示各种 OSPFv3 路由统计，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，依次选择 **Monitoring > Routing > OSPFv3 LSAs**。

步骤 2　您可以选择并监控 OSPFv3 LSA。从 Link State type 下拉列表中选择链路状态类型，以根据指定的参数显示其状态。支持的链路状态类型为 router、 network、 inter-area prefix、 inter-area router、 AS external、 NSSA、 link 和 intra-area prefix。

步骤 3　点击 **Refresh** 以更新每种链路状态类型。

步骤 4　在 ASDM 主窗口中，依次选择 **Monitoring > Routing > OSPFv3 Neighbors**。

在 OSPFv3 Neighbors 窗格中，每行表示一个 OSPFv3 邻居。此外，OSPFv3 Neighbors 窗格还会显示邻居的 IP 地址、优先级、状态、停顿时间量 （以秒为单位）及其运行所在的接口。有关 OSPFv3 邻居的可能状态的列表，请参阅 RFC 5340。

步骤 5　点击 **Refresh** 以更新 OSPFv3 Neighbors 窗格。

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 26-1 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。 引入了以下屏幕：Configuration > Device Setup > Routing > OSPF。
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。 修改了以下屏幕：Configuration > Device Setup > Routing > OSPF > Setup
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。
OSPFv3 支持 IPv6		IPv6 支持 OSPFv3 路由。 引入了以下屏幕：Configuration > Device Setup > Routing > OSPFv3 > Setup、Configuration > Device Setup > Routing > OSPFv3 > Interface、Configuration > Device Setup > Routing > OSPFv3 > Redistribution、 Configuration > Device Setup > Routing > OSPFv3 > Summary Prefix、 Configuration > Device Setup > Routing > OSPFv3 > Virtual Link, Monitoring > Routing > OSPFv3 LSAs、Monitoring > Routing > OSPFv3 Neighbors。

表 26-1　　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。 修改了以下屏幕：Configuration > Device Setup > Routing > OSPF > Interface > Edit OSPF Interface Advanced Properties
计时器		添加了新 OSPF 计时器；弃用了旧 OSPF 计时器。 修改了以下屏幕：Configuration > Device Setup > Routing > OSPF > Setup > Edit OSPF Process Advanced Properties
使用访问列表筛选路由		现在支持使用 ACL 筛选路由。 引入了以下屏幕：Configuration > Device Setup > Routing > OSPF > Filtering Rules > Add Filter Rules
OSPF 监控增强功能		添加了其他 OSPF 监控信息。
OSPF 重新分发 BGP		添加了 OSPF 重新分发功能。 添加了以下屏幕：Configuration > Device Setup > Routing > OSPF > Redistribution
OSPF 支持不间断转发 (NSF)	9.3(1)	添加了对 NSF 的 OSPFv2 和 OSPFv3 支持。 添加了以下屏幕：Configuration > Device Setup > Routing > OSPF > Setup > NSF Properties、 Configuration > Device Setup > Routing > OSPFv3 > Setup > NSF Properties

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

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 进程

要在 ASA 中配置 EIGRP 路由，请执行以下步骤：

步骤 1 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP**。

步骤 2 通过选中 Process Instances 选项卡中的 **Enable this EIGRP process** 复选框，启用 EIGRP 路由进程。请参阅启用 EIGRP，第 27-3 页或启用 EIGRP 末节路由，第 27-4 页。

步骤 3 在 Setup > Networks 选项卡中定义将参与 EIGRP 路由的网络和接口。有关详情，请参见为 EIGRP 路由进程定义网络，第 27-6 页。

步骤 4　（可选）在 **Filter Rules** 窗格中定义路由过滤器。路由过滤对允许在 EIGRP 更新中发送或接收的路由加强控制。有关详情，请参见在 EIGRP 中过滤网络，第 27-12 页。

步骤 5　（可选）在 Redistribution 窗格中定义路由重新分发。

可以将 RIP 和 OSPF 发现的路由重新分发给 EIGRP 路由进程。还可以将静态路由和已连接路由重新分发给 EIGRP 路由进程。有关详情，请参见将路由重新分发到 EIGRP 中，第 27-11 页。

步骤 6　（可选）在 Static Neighbor 窗格中定义静态 EIGRP 邻居。

有关详情，请参见定义 EIGRP 邻居，第 27-10 页。

步骤 7　（可选）在 Summary Address 窗格中定义汇总地址。

有关定义汇总地址的详细信息，请参阅在接口上配置汇总汇聚地址，第 27-8 页。

步骤 8　（可选）在 Interfaces 窗格中定义特定于接口的 EIGRP 参数。这些参数包括 EIGRP 消息身份验证、保持时间、呼叫间隔、延迟指标和使用水平分割。有关详情，请参见为 EIGRP 配置接口，第 27-6 页。

步骤 9　（可选）在 Default Information 窗格中控制 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。有关详情，请参见在 EIGRP 中配置默认信息，第 27-14 页。

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

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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

EIGRP Setup 主窗格中三个可用于启用 EIGRP 的选项卡如下所示：

- Process Instances 选项卡，通过它可为每个情景启用 EIGRP 路由进程。单情景模式和多情景模式均受支持。有关详细信息，请参阅启用 EIGRP，第 27-3 页和启用 EIGRP 末节路由，第 27-4 页。
- Networks 选项卡，通过它可指定 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。有关详情，请参见为 EIGRP 路由进程定义网络，第 27-6 页。
- Passive Interfaces 选项卡，通过它可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。Passive Interfaces 表列出了每一个配置为被动接口的接口。

步骤 2 选中 **Enable this EIGRP process** 复选框。

只能在设备中启用一个 EIGRP 路由进程。必须在 EIGRP Process 字段中为路由进程输入自治系统编号 (AS)，然后才能保存更改。

步骤 3 在 EIGRP Process 字段中，为 EIGRP 进程输入自治系统 (AS) 编号。AS 编号可在 1 到 65535 之间。

步骤 4 （可选）点击 **Advanced** 以配置 EIGRP 进程设置，例如路由器 ID、默认指标、末节路由、邻居更改和 EIGRP 路由的管理距离。

步骤 5 点击 **Networks** 选项卡。

步骤 6 要添加新的网络条目，请点击 **Add**。

系统将显示 Add EIGRP Network 对话框。要删除网络条目，请选择表中的某个条目并点击 **Delete**。

步骤 7 从下拉列表中选择 EIGRP 路由进程的 AS 编号。

步骤 8 在 IP Address 字段中，输入要参与 EIGRP 路由进程的网络的 IP 地址。

注意 要更改某个网络条目，必须首先删除该条目，然后再添加新条目。无法编辑现有条目。

步骤 9 在 Network Mask 字段中，输入要应用于 IP 地址的网络掩码。

步骤 10 点击 **OK**。

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 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

步骤 2 选中 **Enable EIGRP routing** 复选框。

步骤 3 在 EIGRP Process 字段中，为 EIGRP 进程输入自治系统 (AS) 编号。AS 编号可在 1 到 65535 之间。

步骤 4 点击 **Advanced** 以配置 EIGRP 末节路由进程。

系统将显示 Edit EIGRP Process Advanced Properties 对话框。

步骤 5　在 Edit EIGRP Process Advanced Properties 对话框的 Stub 区域中，选择以下一个或多个 EIGRP 末节路由进程：

- Stub Receive only - 将 EIGRP 末节路由进程配置为接收来自相邻路由器的路由信息，但不向邻居发送路由信息。如果选中此选项，则不能选择任何其他末节路由选项。
- Stub Connected - 通告已连接路由。
- Stub Static - 通告静态路由。
- Stub Redistributed - 通告重新分发的路由。
- Stub Summary - 通告汇总路由。

步骤 6　点击 **OK**。

步骤 7　点击 **Networks** 选项卡。

步骤 8　点击 **Add** 以添加新网络条目。

系统将显示 Add EIGRP Network 对话框。要删除网络条目，请在表中选择该条目并点击 **Delete**。

步骤 9　从下拉列表中选择 EIGRP 路由进程的 AS 编号。

步骤 10　在 IP Address 字段中，输入要参与 EIGRP 路由进程的网络的 IP 地址。

注意　要更改某个网络条目，必须首先删除该条目，然后再添加新条目。无法编辑现有条目。

步骤 11　在 Network Mask 字段中，输入要应用于 IP 地址的网络掩码。

步骤 12　点击 **OK**。

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

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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

步骤 2　选中 **Enable EIGRP routing** 复选框。

步骤 3　在 EIGRP Process 字段中，为 EIGRP 进程输入自治系统 (AS) 编号。AS 编号可在 1 到 65535 之间。

步骤 4　点击 **Networks** 选项卡。

步骤 5　点击 **Add** 以添加新网络条目。

系统将显示 Add EIGRP Network 对话框。要删除网络条目，请在表中选择该条目并点击 **Delete**。

步骤 6　从下拉列表中选择 EIGRP 路由进程的 AS 编号。

步骤 7　在 IP Address 字段中，输入要参与 EIGRP 路由进程的网络的 IP 地址。

注意　要更改某个网络条目，必须首先删除该条目，然后再添加新条目。无法编辑现有条目。

步骤 8　在 Network Mask 字段中，输入要应用于 IP 地址的网络掩码。

步骤 9　点击 **OK**。

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 ASA，并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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

步骤 2　选中 **Enable EIGRP routing** 复选框。

步骤 3　点击 **OK**。

步骤 4　依次选择 **Configuration > Device Setup > Routing > EIGRP > Interfaces**。

系统将显示 Interface 窗格，并且其中会显示 EIGRP 接口配置。Interface Parameters 表显示 ASA 中的所有接口，通过该表可逐个接口修改以下设置：

- 身份验证密钥和模式。
- EIGRP 呼叫间隔和保持时间。
- EIGRP 指标计算中所使用的接口延迟指标。
- 接口上水平分割的使用。

步骤 5　通过双击接口条目将其选定，或者选择该接口条目并点击 **Edit**。

系统将显示 Edit EIGRP Interface Entry 对话框。

步骤 6　在 EIGRP Process 字段中，为 EIGRP 进程输入 AS 编号。AS 编号范围可在 1 到 65535 之间。

步骤 7　在 Hello Interval 字段中，输入在接口上发送 EIGRP Hello 数据包的间隔。

有效值的范围为 1 到 65535 秒。默认值为 5 秒。

步骤 8　在 Hold Time 字段中，以秒为单位输入保持时间。有效值的范围为 1 到 65535 秒。默认值为 15 秒。

步骤 9　选中与 Split Horizon 对应的 **Enable** 复选框。

步骤 10　在 Delay 字段中，输入延迟值。延迟时间以 10 倍微秒数为单位。有效值范围为 1 到 16777215。

步骤 11　选中 **Enable MD5 Authentication** 复选框以对 EIGRP 进程消息启用 MD5 身份验证。

步骤 12　输入 Key 或 Key ID 值。

- 在 Key 字段中，输入用于对 EIGRP 更新进行身份验证的密钥。密钥可包含最多 16 个字符。
- 在 Key ID 字段中，输入密钥标识值。有效值范围为 1 到 255。

步骤 13　点击 **OK**。

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。在 ASDM 中， Passive Interface 表列出了每一个配置为被动接口的接口。

要配置被动接口，请执行以下步骤：

操作步骤

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

步骤 2　选中 **Enable EIGRP routing** 复选框。

步骤 3　点击 **OK**。

步骤 4　点击 **Passive Interfaces** 选项卡。

步骤 5　从下拉列表中选择要配置的接口。

步骤 6　选中 **Suppress routing updates on all interfaces** 复选框以将所有接口都指定为被动接口。即使一个接口未显示在 Passive Interface 表中，选中该复选框后，该接口也会配置为被动接口。

步骤 7 点击 **Add** 以添加被动接口条目。

系统将显示 Add EIGRP Passive Interface 对话框。选择要设置为被动的接口并点击 **Add**。要删除被动接口，请在表中选择该接口并点击 **Delete**。

步骤 8 点击 **OK**。

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 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Interfaces**。

Interface 窗格将显示 EIGRP 接口配置。Interface Parameters 表显示 ASA 中的所有接口，通过该表可逐个接口修改设置：有关这些设置的详细信息，请参阅为 EIGRP 配置接口，第 27-6 页。

步骤 2 要为接口配置 EIGRP 参数，请双击某个接口条目，或者选择该条目并点击 **Edit**。

步骤 3 点击 **OK**。

步骤 4 依次选择 **Configuration > Device Setup > Routing > EIGRP > Summary Address**。

Summary Address 窗格将显示静态定义的 EIGRP 汇总地址表。默认情况下，EIGRP 会将子网路由汇总到网络级别。可以从 Summary Address 窗格创建汇总至子网级别的静态定义的 EIGRP 汇总地址。

步骤 5 点击 **Add** 以添加新的 EIGRP 汇总地址，或者点击 **Edit** 以编辑表中的现有 EIGRP 汇总地址。

系统将显示 Add Summary Address 或 Edit Summary Address 对话框。还可以双击表中的某个条目来编辑该条目。

步骤 6 在 EIGRP Process 字段中，为 EIGRP 进程输入自治系统 (AS) 编号。AS 编号可在 1 到 65535 之间。

步骤 7 在 Interface 下拉列表中，选择要从其中通告汇总地址的接口。

步骤 8 在 IP Address 字段中，输入汇总路由的 IP 地址。

步骤 9 在 Netmask 字段中，选择或输入要应用于 IP 地址的网络掩码。

步骤 10 在 Administrative Distance 字段中，输入路由的管理距离。如果保留为空，则路由的默认管理距离为 5。

步骤 11 点击 **OK**。

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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Interfaces**。

Interface 窗格将显示 EIGRP 接口配置。Interface Parameters 表显示 ASA 中的所有接口，通过该表可逐个接口修改设置：有关这些设置的详细信息，请参阅为 EIGRP 配置接口，第 27-6 页。

步骤 2　双击某个接口条目，或者选择该接口条目并点击 **Edit**，以在接口的 EIGRP 参数中配置延迟值。

系统将显示 Edit EIGRP Interface Entry 对话框。

步骤 3　在 Delay 字段中，输入延迟时间，以 10 倍微秒数为单位。有效值范围为 1 至 16777215。

步骤 4　点击 **OK**。

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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

步骤 2　选中 **Enable EIGRP routing** 复选框。

步骤 3　在 **EIGRP Process** 字段中，为 EIGRP 进程输入自治系统 (AS) 编号。AS 编号范围可在 1 到 65535 之间。

步骤 4　点击 **Networks** 选项卡。

步骤 5　点击 **Add** 以添加新网络条目。

系统将显示 Add EIGRP Network 对话框。要删除网络条目，请在表中选择该条目并点击 **Delete**。

步骤 6　从下拉列表中选择 EIGRP 路由进程的 AS 编号。

步骤 7　在 IP Address 字段中，输入要参与 EIGRP 路由进程的网络的 IP 地址。

注意　要更改某个网络条目，必须首先删除该条目，然后再添加新条目。无法编辑现有条目。

步骤 8 在 Network Mask 字段中，选择或输入要应用于 IP 地址的网络掩码。

步骤 9 点击 **OK**。

步骤 10 依次选择 **Configuration > Device Setup > Routing > EIGRP > Interfaces**。

Interface 窗格显示 EIGRP 接口配置。Interface Parameters 表显示 ASA 中的所有接口，通过该表可逐个接口修改设置：有关这些设置的详细信息，请参阅为 EIGRP 配置接口，第 27-6 页。

步骤 11 选中 **Enable MD5 Authentication** 复选框以对 EIGRP 进程消息启用 MD5 身份验证。选中此复选框后，请提供下列内容中一项：

- 在 Key 字段中，输入用于对 EIGRP 更新进行身份验证的密钥。密钥可包含最多 16 个字符。
- 在 Key ID 字段中，输入密钥标识值。有效值范围为 1 到 255。

步骤 12 点击 **OK**。

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 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

步骤 2 选中 **Enable EIGRP routing** 复选框。

步骤 3 在 EIGRP Process 字段中，为 EIGRP 进程输入 AS 编号。AS 编号范围可在 1 到 65535 之间。

步骤 4 依次选择 **Configuration > Device Setup > Routing > EIGRP > Static Neighbor**。

系统将显示 Static Neighbor 窗格，并且其中会显示静态定义的 EIGRP 邻居。EIGRP 邻居向 ASA 发送 EIGRP 路由信息并从其接收 EIGRP 路由信息。通常，通过邻居发现过程来动态发现邻居。但是，在点对点非广播网络中，必须静态定义邻居。

Static Neighbor 表的每一行显示邻居的 EIGRP 自治系统编号、邻居 IP 地址以及用于访问邻居的接口。

从 Static Neighbor 窗格中，可以添加或编辑静态邻居。

步骤 5 点击 **Add** 或 **Edit** 以添加或编辑 EIGRP 静态邻居。

系统将显示 Add or Edit EIGRP Neighbor Entry 对话框。

步骤 6 对于正在为其配置邻居的 EIGRP 进程，从下拉列表中选择 EIGRP AS 编号。

步骤 7 从 Interface Name 下拉列表中选择接口名称，通过该接口访问邻居。

步骤 8 在 Neighbor IP Address 字段中输入邻居的 IP 地址。

步骤 9 点击 **OK**。

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 24 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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

步骤 2　选中 **Enable EIGRP routing** 复选框。

步骤 3　在 EIGRP Process 字段中，为 EIGRP 进程输入 AS 编号。AS 编号范围可在 1 到 65535 之间。

步骤 4　依次选择 **Configuration > Device Setup > Routing > EIGRP > Redistribution**。

Redistribution 窗格将显示用于将来自其他路由协议的路由重新分发到 EIGRP 路由进程的规则。当将静态路由和已连接路由重新分发到 EIGRP 路由进程时，无需配置指标，但建议进行配置。Redistribution 窗格表的每一行均包括一个路由重新分发条目。

步骤 5　点击 **Add** 以添加新的重新分发规则。如果编辑的是现有重新分发规则，请转至步骤 6。

系统将显示 Add EIGRP Redistribution Entry 对话框。

步骤 6　选择表中的地址并点击 **Edit** 以编辑现有 EIGRP 静态邻居，还可以双击表中的条目以编辑该条目。

系统将显示 Edit EIGRP Redistribution Entry 对话框。

步骤 7　从下拉列表中选择要向其应用条目的 EIGRP 路由进程的 AS 编号。

步骤 8　在 Protocol 区域中，点击某一个协议旁边的单选按钮，下述协议用于路由进程：

- **Static**，用于将静态路由重新分发到 EIGRP 路由进程。位于 network 语句范围内的静态路由会自动重新分发到 EIGRP；不需要为其定义重新分发规则。
- **Connected**，用于将已连接路由重新分发到 EIGRP 路由进程。位于 network 语句范围内的已连接路由会自动重新分发到 EIGRP；不需要为其定义重新分发规则。
- **RIP**，用于将由 RIP 路由进程发现的路由重新分发到 EIGRP。
- **OSPF**，用于将由 OSPF 路由进程发现的路由重新分发到 EIGRP。

步骤 9　在 **Optional Metrics** 区域中，选择用于已重新分发路由的以下指标之一：

- **Bandwidth**， EIGRP 带宽指标，以千位/秒为单位。有效值范围为 1 到 4294967295。
- **Delay**， EIGRP 延迟指标，以 10 倍微秒数为单位。有效值范围为 0 到 4294967295。
- **Reliability**， EIGRP 可靠性指标。有效值范围为 0 到 255；255 表示可靠性为 100%。
- **Loading**， EIGRP 有效带宽 （正在加载）指标。有效值范围为 1 到 255；255 表示已 100% 加载。
- **MTU**，路径的 MTU。有效值范围为 1 到 65535。

步骤 10　从 Route Map 下拉列表中选择路由映射，以定义将哪些路由重新分发到 EIGRP 路由进程。有关如何配置路由映射的详细信息，请参阅第 24 章 “路由映射”

步骤 11　在 Optional OSPF Redistribution 区域中，点击以下 OSPF 单选按钮之一，以进一步指定将哪些 OSPF 路由重新分发到 EIGRP 路由进程：

- **Match Internal**，用于匹配指定的 OSPF 进程的内部路由。
- **Match External 1**，用于匹配指定的 OSPF 进程的外部 1 类路由。
- **Match External 2**，用于匹配指定的 OSPF 进程的外部 2 类路由。
- **Match NSSA-External 1**，用于匹配指定的 OSPF NSSA 进程的外部 1 类路由。
- **Match NSSA-External 2**，用于匹配指定的 OSPF NSSA 进程的外部 2 类路由。

步骤 12　点击 **OK**。

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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

步骤 2　选中 **Enable EIGRP routing** 复选框。

步骤 3　在 EIGRP Process 字段中，为 EIGRP 进程输入 AS 编号。AS 编号范围可在 1 到 65535 之间。

步骤 4　依次选择 **Configuration > Device Setup > Routing > EIGRP > Filter Rules**。

系统将显示 Filter Rule 窗格出现，并且其中会显示为 EIGRP 路由进程配置的路由过滤规则。利用过滤规则，可以控制 EIGRP 路由进程接受或通告哪些路由。

Filter Rule 表的每一行均描述特定接口或路由协议的过滤规则。例如，外部接口上传入方向的过滤规则会将过滤应用于外部接口上收到的所有 EIGRP 更新。传出方向且指定 OSPF 10 作为路由协议的过滤规则会将过滤规则应用于重新分发到出站 EIGRP 更新中 EIGRP 路由进程的路由。

步骤 5　点击 **Add** 以添加过滤规则。如果编辑的是已现有的过滤规则，请跳至步骤 6。

系统将显示 Add Filter Rules 对话框。

步骤 6　要编辑过滤规则，请在表中选择该过滤规则并点击 **Edit**。

系统将显示 Edit Filter Rules 对话框。也可双击过滤规则以编辑该规则。要删除过滤规则，请在表中选择该过滤规则并点击 **Delete**。

步骤 7　从下拉列表中选择要向其应用条目的 EIGRP 路由进程的 AS 编号。

步骤 8　从下拉列表中选择过滤路由的方向。

对于过滤来自传入 EIGRP 路由更新的路由的规则，请选择 **in**。选择 **out** 可过滤来自由 ASA 发送的 EIGRP 进程更新的路由。

如果选择 **out**，则 Routing Process 字段将激活。选择要过滤的路由类型。可以过滤从静态、已连接、 RIP 和 OSPF 路由进程重新分发的路由。指定路由进程的过滤器可过滤来自所有接口上发送的更新的路由。

步骤 9　在 ID 字段中，输入 OSPF 进程 ID。

步骤 10　点击 **Interface** 单选按钮并选择过滤器所应用的接口。

步骤 11　点击 **Add** 或 **Edit** 以定义过滤规则的 ACL。点击 **Edit** 以打开选定网络规则的 Network Rule 对话框。

系统将显示 Network Rule 对话框。

步骤 12　在 Action 下拉列表中，选择 Permit 以允许向指定的网络进行通告；选择 Deny 以阻止向指定的网络进行通告。

步骤 13　在 IP Address 字段中，键入要允许或拒绝的网络的 IP 地址。要允许或拒绝所有地址，请使用网络掩码为 **0.0.0.0** 的 IP 地址 **0.0.0.0**。

步骤 14　从 Netmask 下拉列表中，选择应用于网络 IP 地址的网络掩码。可以在此字段中键入网络掩码，或从列表中选择一个常用掩码。

步骤 15　点击 **OK**。

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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

步骤 2　选中 **Enable EIGRP routing** 复选框。

步骤 3　点击 **OK**。

步骤 4　依次选择 **Configuration > Device Setup > Routing > EIGRP > Interfaces**。

系统将显示 Interface 窗格，并且其中会显示所有 EIGRP 接口配置。

步骤 5　双击接口条目，或选择该接口条目并点击 **Edit**。

系统将显示 Edit EIGRP Interface Entry 对话框。

步骤 6　从下拉列表中选择 EIGRP AS 编号，该编号根据启用 EIGRP 路由进程时设置的系统编号进行填充。

步骤 7　在 Hello Interval 字段中，输入在接口上发送 EIGRP Hello 数据包的间隔。

有效值的范围为 1 到 65535 秒。默认值为 5 秒。

步骤 8　在 Hold Time 字段中，以秒为单位指定保持时间。

有效值的范围为 1 到 65535 秒。默认值为 15 秒。

步骤 9　点击 **OK**。

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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

步骤 2　选中 **Enable EIGRP routing** 复选框。

步骤 3　点击 **Process Instance** 选项卡。

步骤 4　点击 **Advanced**。

步骤 5　在 Summary 区域中，取消选中 **Auto-Summary** 复选框。

注意　此设置已默认启用。

步骤 6　点击 **OK**。

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

在 ASDM 中，Default Information 窗格显示用于控制 EIGRP 更新中默认路由信息发送和接收的规则表。可以为每个 EIGRP 路由进程实施一个传入规则和一个传出规则 （当前仅支持一个进程）。

默认情况下，将发送并接受默认路由。要限制或禁用默认路由信息的发送和接收，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 主窗格。

步骤 2　选中 **Enable EIGRP routing** 复选框。

步骤 3　点击 **OK**。

步骤 4　执行以下操作之一：

- 点击 **Add** 以创建新条目。
- 要编辑条目，请在表中双击该条目，或在表中选择条目并点击 **Edit**。

系统会为该条目显示 Add Default Information 或 Edit Default Information 对话框。EIGRP AS 编号会在 EIGRP 字段中自动选定。

步骤 5　在 Direction 字段中，从以下选项中为规则选择方向：

- **in** - 规则过滤来自传入 EIGRP 更新的默认路由信息。
- **out** - 规则过滤来自传出 EIGRP 更新的默认路由信息。

可为每个 EIGRP 进程使用一个传入规则和一个传出规则。

步骤 6　将网络规则添加到网络规则表。网络规则用于定义接收或发送默认路由信息时允许哪些网络以及不允许哪些网络。针对要添加到默认信息过滤规则的每条网络规则重复执行以下步骤。

a. 点击 **Add** 以添加网络规则。双击现有网络规则以编辑该规则。

b. 在 Action 区域中，点击 **Permit** 以允许网络，或者点击 **Deny** 以阻止网络。

c. 在 IP Address 和 Network Mask 字段中，输入规则允许或拒绝的网络的 IP 地址和网络掩码。

要拒绝接受或发送所有默认路由信息，请输入 **0.0.0.0** 作为网络地址并选择 **0.0.0.0** 作为网络掩码。

d. 点击 **OK** 以将指定的网络规则添加到默认信息过滤规则。

步骤 7　点击 **OK** 以接受默认信息过滤规则。

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　在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Interfaces**。

系统将显示 Interface 窗格，并且其中会显示 EIGRP 接口配置。

步骤 2　双击接口条目，或选择该接口条目并点击 **Edit**。

系统将显示 Edit EIGRP Interface Entry 对话框。

步骤 3　从下拉列表中选择 EIGRP 自治系统 (AS) 编号，该编号根据启用 EIGRP 路由进程时设置的系统编号进行填充。

步骤 4　取消选中 **Split Horizo** 复选框。

步骤 5　点击 **OK**。

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 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

步骤 2 点击 **Reset**。

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，请并执行以下步骤：

步骤 1 在 ASDM 主窗口中，依次选择 **Monitoring > Routing > EIGRP Neighbor**。

每行代表一个 EIGRP 邻居。对于每个邻居，列表包括邻居的 IP 地址、邻居连接到的接口、保持时间、正常运行时间、队列长度、序列号、平滑到达往返时间和重新传输超时。可能的状态更改列表如下：

- NEW ADJACENCY - 已建立新邻居。
- PEER RESTARTED - 另一个邻居发起邻居关系重置。获取消息的路由器不是重置邻居的路由器。
- HOLD TIME EXPIRED - 在保持时间限制内，路由器尚未收到来自邻居的任何 EIGRP 数据包。
- RETRY LIMIT EXCEEDED - EIGRP 未收到来自邻居的对 EIGRP 可靠数据包的确认，且 EIGRP 已尝试重新传输可靠数据包 16 次，无一次成功。
- ROUTE FILTER CHANGED - 由于路由过滤器发生更改， EIGRP 邻居正在重置。
- INTERFACE DELAY CHANGED - 由于接口上的延迟参数发生手动配置更改， EIGRP 邻居正在重置。
- INTERFACE BANDWIDTH CHANGED - 由于接口上的接口带宽发生手动配置更改， EIGRP 邻居正在重置。
- STUCK IN ACTIVE - 由于 EIGRP 陷入主动状态， EIGRP 邻居正在重置。陷入主动状态导致邻居发生重置。

步骤 2 点击要监控的 EIGRP 邻居。

步骤 3 要删除当前邻居列表，请点击 **Clear Neighbors**。

步骤 4 要刷新当前邻居列表，请点击 **Refresh**。

备注 默认情况下，会记录邻居变更消息和邻居警告消息。

EIGRP 历史记录

表 27-1 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。 引入了以下屏幕：Configuration > Device Setup > Routing > 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。 修改了以下屏幕：Configuration > Device Setup > Routing > EIGRP > Setup。
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。
EIGRP 自动汇总	9.2(1)	默认情况下，现已针对 EIGRP 禁用 Auto-Summary 字段。 修改了以下屏幕：Configuration > Device Setup > Routing > EIGRP > Setup > Edit EIGRP Process Advanced Properties

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

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

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。有关如何配置组播组的信息，请参阅配置组播组，第 28-13 页。

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 10 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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast**。

步骤 2　在 Multicast 窗格中，选中 **Enable Multicast routing** 复选框。

选中此复选框可在 ASA 上启用 IP 组播路由。取消选中此复选框将禁用 IP 组播路由。默认情况下，组播已禁用。启用组播路由可在所有接口上启用组播。您可以逐个接口禁用组播。

表 28-1 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 28-1　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 28-4 页
- 配置静态组播路由，第 28-4 页
- 配置 IGMP 功能，第 28-5 页
- 配置 PIM 功能，第 28-9 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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast**。

步骤 2　在 Multicast 窗格中，选中 **Enable Multicast routing** 复选框。

步骤 3　点击 **Apply** 保存更改。

步骤 4　依次选择 **Configuration > Device Setup > Routing > Multicast > IGMP > Protocol**。

步骤 5　要修改要从其中转发 IGMP 消息的特定接口，请选择该接口并点击 **Edit**。

系统将显示 Configure IGMP Parameters 对话框。

步骤 6　从 **Forward Interface** 下拉列表中，选择要从其中转发 IGMP 消息的特定接口。

步骤 7　点击 **OK** 关闭此对话框，然后点击 **Apply** 保存更改。

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > MRoute**。

步骤 2　选择 **Add** 或 **Edit**。

系统将显示 Add Multicast Route 或 Edit Multicast Route 对话框。

使用 Add Multicast Route 对话框可将新静态组播路由添加到 ASA。使用 Edit Multicast Route 对话框可更改现有的静态组播路由。

步骤 3　在 Source Address 字段中，输入组播源的 IP 地址。编辑现有的静态组播路由时，不能更改此值。

步骤 4　从 Source Mask 下拉列表中选择组播源 IP 地址的网络掩码。

步骤 5　在 Incoming Interface 区域中，点击 **RPF Interface** 单选按钮以选择用于转发路由的 RPF，或者点击 **Interface Name** 单选按钮，然后输入以下内容：

- 在 Source Interface 字段中，从下拉列表中选择组播路由的传入接口。
- 在 Destination Interface 字段中，从下拉列表中选择路由转发要通过的目标接口。

注意　您可以指定接口或 RPF 邻居，但不能同时指定这两者。

步骤 6　在 Administrative Distance 字段中，选择静态组播路由的管理距离。如果静态组播路由的管理距离与单播路由相同，则静态组播路由优先。

步骤 7　点击 **OK**。

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

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > IGMP > Protocol**。

Protocol 窗格将显示 ASA 上的每个接口的 IGMP 参数。

步骤 2　选择要禁用的接口，然后点击 **Edit**。

步骤 3　要禁用指定接口，请取消选中 **Enable IGMP** 复选框。

步骤 4　点击 **OK**。

如果 IGMP 在接口上已启用， Protocol 窗格将显示 Yes；如果 IGMP 在接口上已禁用，将显示 No。

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 28-7 页。

操作步骤

步骤 1　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > IGMP > Join Group**。

步骤 2　点击 **Join Group** 窗格中的 **Add** 或 **Edit** 。

Add IGMP Join Group 对话框可用于将接口配置为组播组的成员。**Edit IGMP Join Group** 对话框可用于更改现有的成员身份信息。

步骤 3　在 **Interface Name** 字段中，从下拉列表中选择接口名称。如果编辑的是现有条目，则无法更改此值。

步骤 4　在 **Multicast Group Address** 字段中，输入接口所在组播组的地址。有效的组地址范围是 224.0.0.0 到 239.255.255.255。

步骤 5　点击 **OK**。

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。

在主 ASDM 窗口中，依次选择 **Configuration > Routing > Multicast > IGMP > Static Group**，以将 ASA 配置为组的静态连接成员。使用此方法时， ASA 不会接受数据包本身，只会转发它们。因此，此方法可用于快速切换。传出接口显示在 IGMP 缓存中，但此接口不是组播组的成员。

操作步骤

步骤 1　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > IGMP > Static Group**。

步骤 2　点击 **Static Group** 窗格中的 **Add** 和 **Edit**。

使用 **Add IGMP Static Group** 对话框可以将组播组静态分配给接口。使用 **Edit IGMP Static Group** 对话框可以更改现有的静态组分配。

步骤 3　在 **Interface Name** 字段中，从下拉列表中选择接口名称。如果编辑的是现有条目，则无法更改此值。

步骤 4　在 **Multicast Group Address** 字段中，输入接口所在组播组的地址。有效的组地址范围是 224.0.0.0 到 239.255.255.255。

步骤 5　点击 **OK**。

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > IGMP > Access Group**。

系统将显示 **Access Group** 窗格。Access Group 窗格中的表条目按自上而下的顺序处理。越具体的条目越靠近表格顶部，越宽泛的条目越位于底部。例如，将允许特定组播组的访问组条目放在靠近表顶部的位置，并将拒绝多个组播组（包括允许规则中的组）的访问组条目放在下方。由于允许规则在拒绝规则前执行，因此该组获允许。

双击表中的一个条目会打开选定条目的 Add Access Group 或 Edit Access Group 对话框。

步骤 2　点击 **Add** 或 **Edit**。

系统将显示 **Add Access Group 或 Edit Access Group** 对话框。**Add Access Group** 对话框可用于向 Access Group Table 中添加新的访问组。**Edit Access Group** 对话框可用于更改现有访问组条目的信息。编辑现有条目时，有些字段可能会灰显。

步骤 3　从 **Interface** 下拉列表中选择与访问组关联的接口名称。编辑现有访问组时，不能更改相关的接口。

步骤 4　从 **Action** 下拉列表中选择 **permit**，以允许选定接口上的组播组。从 **Action** 下拉列表中选择 **deny**，以从选定接口筛选组播组。

步骤 5　在 **Multicast Group Address** 字段中，输入要应用访问组的组播组。

步骤 6　输入组播组地址的网络掩码，或者从 **Netmask** 下拉列表中选择一个常用的网络掩码。

步骤 7　点击 **OK**。

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > IGMP > Protocol**。

步骤 2　在 **Protocol** 窗格的表中选择要限制的接口，然后点击 **Edit**。

系统将显示 **Configure IGMP Parameters** 对话框。

步骤 3　在 **Group Limit** 字段中输入可以在接口上加入的主机的最大数量。

默认值为 500。有效值范围介于 0 到 500 之间。

注意　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。

步骤 4　点击 **OK**。

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。

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > IGMP > Protocol**。

步骤 2　在 **Protocol** 窗格的表中选择要限制的接口，然后点击 **Edit**。

系统将显示 **Configure IGMP Parameters** 对话框。

步骤 3　在 **Query Interval** 字段中输入指定路由器发送 IGMP 主机查询消息的时间间隔 （以秒为单位）。

有效值的范围为 1 到 3600 秒。默认值为 125 秒。

注意　如果 ASA 不能在指定超时值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 4　在 **Query Timeout** 字段中输入接口上的上一个请求方停止工作后到 ASA 接替该请求方之间相隔的时间 （以秒为单位）。

有效值的范围为 60 到 300 秒。默认值为 255 秒。

步骤 5　点击 **OK**。

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，。

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > IGMP > Protocol**。

步骤 2　在 **Protocol** 窗格的表中选择要更改其 IGMP 版本的接口，然后点击 **Edit**。

系统将显示 **Configure IGMP Interface** 对话框。

步骤 3　从 **Version** 下拉列表中选择版本号。

步骤 4　点击 **OK**。

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 28-10 页
- 配置静态交汇点地址，第 28-10 页
- 配置指定路由器优先级，第 28-11 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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > PIM > Protocol**。

步骤 2　在 **Protocol** 窗格的表中选择要启用 PIM 的接口，然后点击 **Edit**。

系统将显示 **Edit PIM Protocol** 对话框。

步骤 3　选中 **Enable PIM** 复选框。要禁用 PIM，请取消选中此复选框。

步骤 4　点击 **OK**。

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > PIM > Rendezvous Points**。

步骤 2　点击 **Add** 或 **Edit**。

系统将显示 **Add Rendezvous Point or Edit Rendezvous Point** 对话框。**Add Rendezvous Point** 对话框可用于向 Rendezvous Point 表添加新条目。**Edit Rendezvous Point** 对话框可用于更改现有的 RP 条目。此外，还可以点击 **Delete** 以从表中删除选定的组播组条目。

以下限制适用于 RP：

- 一个 RP 地址不能用两次。
- 不能为多个 RP 指定所有组。

步骤 3　在 **Rendezvous Point Address** 字段中，输入 RP 的 IP 地址。

编辑现有的 RP 条目时，不能更改此值。

步骤 4　如果指定的组播组要在双向模式下运行，请选中 **Use bi-directional forwarding** 复选框。如果指定的组播组要在双向模式下运行，Rendezvous Point 窗格将显示 Yes；如果指定的组播组要在稀疏模式下运行，该窗格将显示 No。在双向模式下，如果 ASA 接收组播数据包，且没有直连成员或 PIM 邻居，则会将删除消息发送回源。

步骤 5　点击 **Use this RP for All Multicast Groups** 单选按钮，以将指定 RP 用于接口上的所有组播组；或者点击 **Use this RP for the Multicast Groups as specified below** 单选按钮，以将组播组指定为要与指定 RP 配合使用。

有关组播组的详细信息，请参阅配置组播组，第 28-13 页。

步骤 6　点击 **OK**。

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > PIM > Protocol**。

步骤 2　在 **Protocol** 窗格的表中选择要启用 PIM 的接口，然后点击 **Edit**。

系统将显示 **Edit PIM Protocol** 对话框。

步骤 3　在 **DR Priority** 字段中，键入选定接口的指定路由器优先级值。子网上具有最高 DR 优先级的路由器将成为指定路由器。有效值范围为 0 到 4294967294。默认 DR 优先级为 1。将此值设置为 0 会使 ASA 接口没有资格成为默认路由器。

步骤 4　点击 **OK**。

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > PIM > Request Filter**。

步骤 2　点击**添加**。

Request Filter Entry 对话框可用于定义当 ASA 用作 RP 时可注册到 ASA 的组播源。您可根据源 IP 地址和目标组播地址创建筛选规则。

步骤 3　从 **Action** 下拉列表中，选择 **Permit** 以创建允许特定组播流量的特定源注册到 ASA 的规则，或者选择 **Deny** 以创建防止特定组播流量的特定源注册到 ASA 的规则。

步骤 4　在 **Source IP Address** 字段中键入注册消息源的 IP 地址。

步骤 5　在 **Source Netmask** 字段中键入或从下拉列表中选择注册消息源的网络掩码。

步骤 6　在 **Destination IP Address** 字段中键入组播目标地址。

步骤 7　在 **Destination Netmask** 字段中键入或从下拉列表中选择组播目标地址的网络掩码。

步骤 8　点击 **OK**。

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > PIM > Protocol**。

步骤 2　在 **Protocol** 窗格的表中选择要启用 PIM 的接口，然后点击 **Edit**。

系统将显示 **Edit PIM Protocol** 对话框。

步骤 3　在 **Hello Interval** 字段中键入接口发送 PIM Hello 消息的频率 （以秒为单位）。

步骤 4　在 **Prune Interval** 字段中键入接口发送 PIM 加入通告和删除通告的频率 （以秒为单位）。

步骤 5　点击 **OK**。

配置路由树

默认情况下， PIM 枝叶路由器在第一个数据包从新源到达后会立即加入到最短路径树。此方法可降低延迟，但需要的内存比共享树多。您可以将 ASA 配置为对于所有组播组或仅对于特定组播地址加入到最短路径树或者使用共享树。

要配置 PIM 枝叶路由器树，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > PIM > Route Tree**。

步骤 2　点击以下单选按钮之一：

- **Use Shortest Path Tree for All Groups** - 选择此选项会将最短路径树用于所有的组播组。
- **Use Shared Tree for All Groups** - 选择此选项会将共享树用于所有的组播组。

- **Use Shared Tree for the Groups specified below** - 选择此选项会将共享树用于 Multicast Groups 表中指定的组。最短路径树用于未在 Multicast Groups 表中指定的任何组。

  Multicast Groups 表显示与共享树配合使用的组播组。

  表条目按自上而下的顺序进行处理。您可以通过以下方法来创建包含一系列组播组但不包含该系列中特定组的条目：将特定组的拒绝规则放置在表的顶部，并将该系列组播组的允许规则放置在拒绝语句下面。

  要编辑组播组，请参阅配置组播组，第 28-13 页。

配置组播组

组播组是访问规则列表，用于定义哪些组播地址属于组的一部分。一个组播组可以包含一个组播地址或多个组播地址。使用 Add Multicast Group 对话框可创建新的组播组规则。使用 Edit Multicast Group 对话框可修改现有的组播组规则。

要配置组播组，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > PIM > Rendezvous Points**。

步骤 2　系统将显示 **Rendezvous Point** 窗格。点击要配置的组。

系统将显示 **Edit Rendezvous Point** 对话框。

步骤 3　点击 **Use this RP for the Multicast Groups as specified below** 单选按钮，以指定要与指定 RP 配合使用的组播组。

步骤 4　点击 **Add** 或 **Edit**。

系统将显示 **Add Multicast Group or Edit Multicast Group** 对话框。

步骤 5　从 **Action** 下拉列表中，选择 **Permit** 以创建允许指定组播地址的组规则，或选择 **Deny** 以创建筛选指定组播地址的组规则。

步骤 6　在 Multicast Group Address 字段中，键入与所选组相关的组播地址。

步骤 7　从 Netmask 下拉列表中，选择组播组地址的网络掩码。

步骤 8　点击 **OK**。

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > PIM > Neighbor Filter**。

步骤 2　点击 **Add/Edit/Insert**，以从表中选择要配置的 PIM 邻居。

系统将显示 **Add/Edit/Insert Neighbor Filter** Entry 对话框。通过此对话框，您可以为组播边界 ACL 创建 ACL 条目，还可以删除选定的 PIM 邻居条目。

步骤 3　从 **Interface Name** 下拉列表中选择接口名称。

步骤 4　从 **Action** 下拉列表中，为邻居过滤器 ACL 条目选择 **Permit** 或 **Deny**。

选择 **Permit** 将会允许组播组通告通过接口。选择 **Deny** 将会禁止指定的组播组通告通过接口。在接口上配置组播边界时，会阻止所有的组播流量通过接口，除非使用邻居过滤器条目允许通过。

步骤 5　在 **IP Address** 字段中输入被允许或拒绝的组播 PIM 组的 IP 地址。有效的组地址范围是 224.0.0.0 到 239.255.255.255。

步骤 6　从 **Netmask** 下拉列表中，选择组播组地址的网络掩码。

步骤 7　点击 **OK**。

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > PIM > Bidirectional Neighbor Filter**。

步骤 2　双击 **PIM Bidirectional Neighbor Filter** 表中的一个条目，以打开该条目的 **Edit Bidirectional Neighbor Filter Entry** 对话框。

步骤 3　点击 **Add/Edit/Insert**，以从表中选择要配置的 PIM 邻居。

系统将显示 **Add/Edit/Insert Bidirectional Neighbor Filter Entry** 对话框，您可以在其中为 PIM 双向邻居过滤器 ACL 创建 ACL 条目。

步骤 4　从 **Interface** Name 下拉列表中选择接口名称。选择要为其配置 PIM 双向邻居过滤器 ACL 条目的接口。

步骤 5　从 **Action** 下拉列表中，为邻居过滤器 ACL 条目选择 **Permit** 或 **Deny**。

选择 **Permit** 可允许指定设备参与 DF 选举过程。选择 **Deny** 可阻止指定设备参与 DF 选举过程。

步骤 6　输入被允许或拒绝的组播 PIM 组的 IP 地址。在 **IP Address** 字段中输入有效的组地址，范围为 224.0.0.0 到 239.255.255.255.255。

步骤 7　从 **Netmask** 下拉列表中，选择组播组地址的网络掩码。

步骤 8　点击 **OK**。

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：在 ASDM 中依次选择 **Configuration > Routing > Multicast > MBoundary**，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　在主 ASDM 窗口中，依次选择 **Configuration > Routing > Multicast > MBoundary**。

MBoundary 窗格可用于配置使用管理性界定的组播地址的组播边界。组播边界限制组播数据包流，并允许在不同的管理域中重复使用相同的组播组地址。在接口上定义了组播边界后，只有过滤器 ACL 允许的组播流量可通过接口。

步骤 2　点击 **Edit**。

系统将显示 **Edit Boundary Filter** 对话框，并显示组播边界过滤器 ACL。您可以使用此对话框添加和删除过滤器 ACL 条目。

如果边界过滤器配置应用于 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）。

步骤 3　从 **Interface** 下拉列表中选择要为其配置组播边界过滤器 ACL 的接口。

步骤 4　选中 **Remove any Auto-RP group range** 复选框，以从边界 ACL 拒绝的源中筛选 Auto-RP 消息。如果取消选中 **Remove any Auto-RP group range** 复选框，将会允许所有 Auto-RP 消息通过。

步骤 5　点击 **OK**。

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　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast**。

步骤 2　在 Multicast 窗格中，选中 **Enable Multicast routing** 复选框并点击 **Apply**。

步骤 3　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > MRoute**。

步骤 4　点击 **Add** 或 **Edit**。

系统将显示 **Add Multicast Route 或 Edit Multicast Route** 对话框。

使用 **Add Multicast Route** 对话框可将新静态组播路由添加到 ASA。使用 **Edit Multicast Route** 对话框可更改现有的静态组播路由。

步骤 5　在 **Source Address** 字段中，输入组播源的 IP 地址。编辑现有的静态组播路由时，不能更改此值。

步骤 6　从 **Source Mask** 下拉列表中选择组播源 IP 地址的网络掩码。

步骤 7　在 **Incoming Interface** 区域中，点击 **RPF Interface** 单选按钮以选择用于转发路由的 RPF，或者点击 **Interface Name** 单选按钮，然后输入以下内容：

- 在 **Source Interface** 字段中，从下拉列表中选择组播路由的传入接口。
- 在 **Destination Interface** 字段中，从下拉列表中选择要通过选定接口向其转发路由的目标接口。

注意　您可以指定接口或 RPF 邻居，但不能同时指定这两者。

步骤 8　在 **Administrative Distance** 字段中，选择静态组播路由的管理距离。如果静态组播路由的管理距离与单播路由相同，则静态组播路由优先。

步骤 9　点击 **OK**。

步骤 10　在主 ASDM 窗口中，依次选择 **Configuration > Device Setup > Routing > Multicast > IGMP > Join Group**。

系统将显示 **Join Group** 窗格。

步骤 11　点击 **Add** 或 **Edit**。

Add IGMP Join Group 对话框可用于将接口配置为组播组的成员。**Edit IGMP Join Group** 对话框可用于更改现有的成员身份信息。

步骤 12　在 **Interface Name** 字段中，从下拉列表中选择接口名称。如果编辑的是现有条目，则无法更改此值。

步骤 13　在 **Multicast Group Address** 字段中，输入接口所在组播组的地址。有效的组地址范围是 224.0.0.0 到 239.255.255.255。

步骤 14　点击 **OK**。

组播路由历史记录

表 28-2　　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。 引入了以下屏幕：Configuration > Device Setup > Routing > Multicast。
支持群集功能	9.0(1)	增加了集群支持。

IPv6 邻居发现

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。

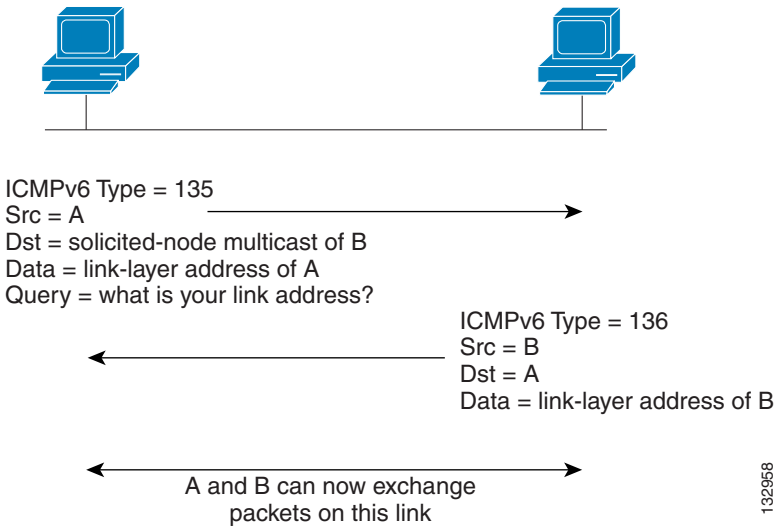
邻居请求消息

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。图 29-1 显示邻居请求和响应流程。

图 29-1　　IPv6 邻居发现 - 邻居请求消息



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。

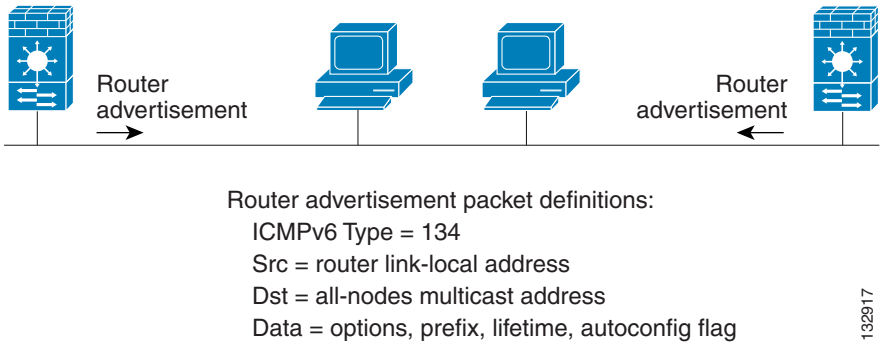
如果接口的链路本地地址发生变化，则会将新的链路本地地址执行重复地址检测，并将重新生成与接口关联的所有其他 IPv6 地址（重复地址检测仅在新的链路本地地址上执行）。

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。图 29-2 显示了如何在 IPv6 配置接口上发送路由器通告消息的示例。

图 29-2　IPv6 邻居发现 - 路由器通告消息



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 15-11 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 29-1 列出 IPv6 邻居发现的默认设置。

表 29-1　　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。
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

- 配置邻居请求消息间隔，第 29-6 页
- 配置邻居可访问时间，第 29-6 页

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，请执行以下步骤。

操作步骤

步骤 1　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择要在其上配置邻居请求时间间隔的接口。必须已使用 IPv6 地址对接口进行配置。有关详情，请参见配置 IPv6 寻址，第 15-11 页。

步骤 3　点击 **Edit**。系统将显示 **Edit Interface** 对话框。

步骤 4　点击 **IPv6** 选项卡。

步骤 5　在 **NS Interval** 字段中输入时间间隔。

步骤 6　点击 **OK**。

步骤 7　点击 **Apply** 以保存运行配置。

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　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择要为其配置时间的接口。必须已使用 IPv6 地址对接口进行配置。有关详细信息，请参阅配置 IPv6 寻址，第 15-11 页。

步骤 3　点击 **Edit**。系统将显示 **Edit Interface** 对话框。

步骤 4　点击 **IPv6** 选项卡。

步骤 5　在 **Reachable Time** 字段中输入有效值。

步骤 6　点击 **OK**。

步骤 7　点击 **Apply** 以保存运行配置。

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　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择要为其配置时间的接口。

必须已使用 IPv6 地址对接口进行配置。有关详细信息，请参阅配置 IPv6 寻址，第 15-11 页。

步骤 3　点击 **Edit**。系统将显示 **Edit Interface** 对话框。

步骤 4　点击 **IPv6** 选项卡。

步骤 5　在 **RA Interval** 字段中输入有效的传输时间间隔值。

注意　（可选）要以毫秒为单位添加路由器通告传输时间间隔值，请选中 **RA Interval in Milliseconds** 复选框，并输入 500 到 1800000 范围之间的值。

步骤 6　点击 **OK**。

步骤 7　点击 **Apply** 以保存运行配置。

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　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择要配置的接口。

必须已使用 IPv6 地址对接口进行配置。有关详细信息，请参阅配置 IPv6 寻址，第 15-11 页。

步骤 3　点击 **Edit**。

系统将显示 **Edit Interface** 对话框。

步骤 4　点击 **IPv6** 选项卡。

步骤 5　在 **RA Lifetime** 字段中输入有效的有效期值。

步骤 6　点击 **OK**。

步骤 7　点击 **Apply** 以保存运行配置。

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　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择要配置的接口。

必须已使用 IPv6 地址对接口进行配置。有关详细信息，请参阅配置 IPv6 寻址，第 15-11 页。

步骤 3　点击 **Edit**。

系统将显示 **Edit Interface** 对话框。

步骤 4　点击 **IPv6** 选项卡。

步骤 5　输入允许的 DAD 尝试次数。

此设置可配置当对 IPv6 地址执行 DAD 时，接口上发送的连续邻居请求消息的数量。

- 有效值范围为 0 到 600。
- 零值可在指定的接口上禁用 DAD 处理。默认值为一条消息。

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　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择要抑制路由器通告传输的接口。必须已使用 IPv6 地址对接口进行配置。

步骤 3　点击 **Edit**。

系统将显示 **Edit Interface** 对话框。

步骤 4　点击 **IPv6** 选项卡。

步骤 5　选中 **Suppress RA** 复选框。

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　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择要配置的接口。

步骤 3　点击 **Edit**。

系统将显示 **Edit Interface** 对话框。

步骤 4　点击 **IPv6** 选项卡。

步骤 5　选中 **Hosts should use DHCP for address config** 复选框以在 IPv6 路由器通告数据包中设置托管地址配置标志。

此标志通知 IPv6 自动配置客户端应使用 DHCPv6 来获取相关地址以及派生的无状态自动配置地址。

步骤 6　选中 **Hosts should use DHCP for address config** 复选框以在 IPv6 路由器通告数据包中设置其他地址配置标志。

此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。

配置路由器通告中的 IPv6 前缀

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　依次选择 **Configuration > Device Setup > Interface Settings > Interfaces**。

步骤 2　选择要抑制路由器通告传输的接口。必须已使用 IPv6 地址对接口进行配置。

步骤 3　点击 **Edit**。

系统将显示 **Edit Interface** 对话框。

步骤 4　点击 **IPv6** 选项卡。

步骤 5　在 **Interface IPv6 Prefixes** 区域中，点击 **Add**。

系统将显示 **Add IPv6 Prefix for Interface** 对话框。

步骤 6　使用前缀长度输入 IPv6 地址。

步骤 7　（可选）要手动配置 IPv6 地址，请选中 **No Auto-Configuration** 复选框。此设置向本地链路上的主机指示指定的前缀无法用于 IPv6 自动配置。

步骤 8　（可选）要指示不通告 IPv6 前缀，请选中 **No Advertisements** 复选框。

步骤 9　（可选） **Off Link** 复选框指示指定的前缀已分配给链路。向包含指定前缀的地址发送流量的节点会将目标视为在链路上本地可访问。此前缀不得用于链路上确定。

步骤 10　在 **Prefix Lifetime** 区域中，点击 **Lifetime Duration** 单选按钮，指定以下各项：

a. 从下拉列表中选择前缀的有效有效期 （以秒为单位）。此设置是将指定的 IPv6 前缀通告为有效的时间。最大值代表无穷大。有效值为 0 到 4294967295。默认值为 2592000 秒 （30 天）。

b. 从下拉列表中选择前缀的首选有效期。此设置是将指定的 IPv6 前缀通告为首选时间。最大值代表无穷大。有效值为 0 到 4294967295。默认设置为 604800 秒 （七天）。

步骤 11　要定义前缀有效期到期日期，请点击 **Lifetime Expiration Date** 单选按钮，并指定以下各项：

a. 从下拉列表中选择有效的月份和日期，然后以 hh:mm 格式输入时间。

b. 从下拉列表中选择首选月份和日期，然后以 hh:mm 格式输入时间。

步骤 12　点击 **OK** 保存设置。

系统将显示 **Interface IPv6 Prefixes Address** 字段，其中包括首选日期和有效日期。

配置静态 IPv6 邻居

尝试添加邻居之前，请确保在至少一个接口上启用了 IPv6，否则 ASDM 会返回错误消息，指示配置失败。

有关配置 IPv6 地址的信息，请参阅配置 IPv6 寻址，第 15-11 页。

要添加 IPv6 静态邻居，请执行以下步骤。

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Advanced > IPv6 Neighbor Discovery Cache**。

步骤 2　点击**添加**。

系统将显示 Add IPv6 Static Neighbor 对话框。

步骤 3　从 Interface Name 下拉列表中，选择要在其上面添加邻居的接口。

步骤 4　在 IP Address 字段中，输入对应于本地数据链路地址的 IPv6 地址，或点击省略号 (...) 浏览查找地址。

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。

步骤 5　在 MAC address 字段中，输入本地数据线路 （硬件） MAC 地址。

步骤 6　点击 **OK**。

注意　在应用更改并保存配置之前，点击 **Reset** 可取消任何更改并恢复原始值。

步骤 7　点击 **Apply** 以保存运行配置。

查看和清除动态发现的邻居

当主机或节点与邻居通信时，会将邻居添加到邻居发现缓存。当不再与邻居存在任何通信时，会将该邻居从缓存中删除。

要查看动态发现的邻居并从 IPv6 邻居发现缓存清除这些邻居，请执行以下步骤：

步骤 1　依次选择 **Monitoring > Interfaces > IPv6 Neighbor Discovery Cache**。

您可以从 IPv6 Neighbor Discovery Cache 窗格查看所有静态和动态发现的邻居。

步骤 2　要从缓存清除所有动态发现的邻居，请点击 **Clear Dynamic Neighbor Entries**。

动态发现的邻居将从缓存中删除。

注意　本程序仅从缓存清除动态发现的邻居；将不清除静态邻居。

IPv6 邻居发现历史记录

表 29-2　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。 引入了以下屏幕： Monitoring > Interfaces > IPv6 Neighbor Discovery Cache。 Configuration > Device Management > Advanced > IPv6 Neighbor Discovery Cache。 Configuration > Device Setup > Interface Settings > Interfaces > IPv6。
IPv6 DHCP 中继的地址配置标志	9.0(1)	修改了以下屏幕：Configuration > Device Device Setup > Interfaces > IPv6。

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

本节介绍 AAA 和本地数据库。

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。ASDM 允许您启用三个预定义的权限级别，各个命令将分配到级别 15 （管理员）、级别 5 （只读）和级别 3 （仅监控）。如果您使用预定义的级别，请将用户分配到这三个权限级别的其中一个。
- 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 34-21 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　依次选择 **Configuration > Device Management > Users/AAA > User Accounts**，然后点击 **Add**。

系统将显示 **Add User Account-Identity** 对话框。

步骤 2　输入长度为 4 到 64 个字符的用户名。

步骤 3　输入长度为 3 到 32 个字符的密码。密码区分大小写。此字段仅显示星号。为了确保安全，我们建议密码长度至少为 8 个字符。

注意　要从 User Accounts 窗格中配置启用密码，请更改 enable_15 用户的密码。enable_15 用户始终显示在 User Accounts 窗格中，它代表默认用户名。这种配置启用密码的方法是在 ASDM 中进行系统配置的唯一可用方法。如果您在 CLI 中配置了其他启用级别的密码（例如，启用密码 10），则那些用户将列出为 enable_10，依次类推。

步骤 4　请重新输入密码。

为安全起见，密码字段仅显示星号。

步骤 5　如果使用 MSCHAP 进行身份验证，请选中 **User authenticated using MSCHAP** 复选框。

步骤 6　在 **Access Restriction** 区域中设置用户的管理访问级别。您必须先在 **Configuration > Device Management > Users/AAA > AAA Access > Authorization** 选项卡上点击 **Perform authorization for exec shell access** 选项，才能启用管理授权。

选择以下选项之一：

- **Full Access (ASDM, Telnet, SSH and console)** - 如果配置了使用本地数据库对管理访问进行身份验证，则此选项使用户能够使用 ASDM、 SSH、 Telnet 和控制台端口。如果还启用了身份验证，则用户可以访问全局配置模式。
  - **Privilege Level** - 为 ASDM 和本地命令授权设置权限级别。范围为 0 （最低）到 15 （最高）。要授予无限制的管理员访问权限，请指定值 15。预定义的 ASDM 角色将 15 用于表示管理员访问权限，5 用于表示只读访问权限，3 用于表示仅监控访问权限（用户仅限于访问 Home 窗格和 Monitoring 窗格）。
- **CLI login prompt for SSH, Telnet and console (no ASDM access)** - 如果配置了使用本地数据库对管理访问进行身份验证，则此选项使用户能够使用 SSH、 Telnet 和控制台端口。如果配置了 HTTP 身份验证，则用户无法使用 ASDM 进行配置。允许进行 ASDM 监控。如果还配置了启用身份验证，则用户无法访问全局配置模式。
- **No ASDM, SSH, Telnet, or console access** - 如果配置了使用本地数据库对管理访问进行身份验证，则此选项禁止用户访问任何配置了身份验证的管理访问方法 （不包括 Serial 选项；允许进行串行访问）。

步骤 7　（可选）对于与 ASA 的 SSH 连接，要按每个用户启用公钥身份验证，请点击 **Navigation** 窗格中的下列选项之一：

- **Public Key Authentication** - 粘贴 Base64 编码的公钥。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。您查看现有密钥时，该密钥会使用 SHA-256 散列算法进行加密。如果需要复制并粘贴经过散列处理的密钥，请选择 **Key is hashed** 复选框。

  要删除身份验证密钥，请点击 **Delete Key** 以显示确认对话框。点击 **Yes** 删除身份验证密钥，或者点击 **No** 保留该密钥。
- **Public Key Using PKF** - 选中 **Specify a new PKF key** 复选框，然后粘贴或导入公钥文件 (PKF) 格式的密钥（其长度可达 4096 位）。此格式用于由于过长而无法以 Base64 格式粘贴的密钥。例如，可以使用 ssh keygen 生成 4096 位的密钥，然后将其转换为 PKF 格式，并在此窗格中导入。您查看现有密钥时，该密钥会使用 SHA-256 散列算法进行加密。如果需要复制并粘贴经过散列处理的密钥，请从 **Public Key Authentication** 窗格中复制该密钥，然后在新 ASA 上的该窗格中，在 **Key is hashed** 复选框选中的情况下粘贴该密钥。

  要删除身份验证密钥，请点击 **Delete Key** 以显示确认对话框。点击 **Yes** 删除身份验证密钥，或者点击 **No** 保留该密钥。

步骤 8　点击 **VPN Policy**，以便为此用户配置 VPN 策略属性。请参阅VPN 配置指南。

步骤 9　点击 **Apply**。

用户将添加到本地数据库中，并且更改将保存到运行配置。

提示　您可以在 **Configuration > Device Management > Users/AAA > User Accounts** 窗格的每一列中搜索特定文本。请在 **Find** 框中输入要查找的特定文本，然后点击 **Up** 或 **Down** 箭头。在文本搜索中，还可以使用星号 (“*”) 和问号 (“?”) 作为通配符。

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：

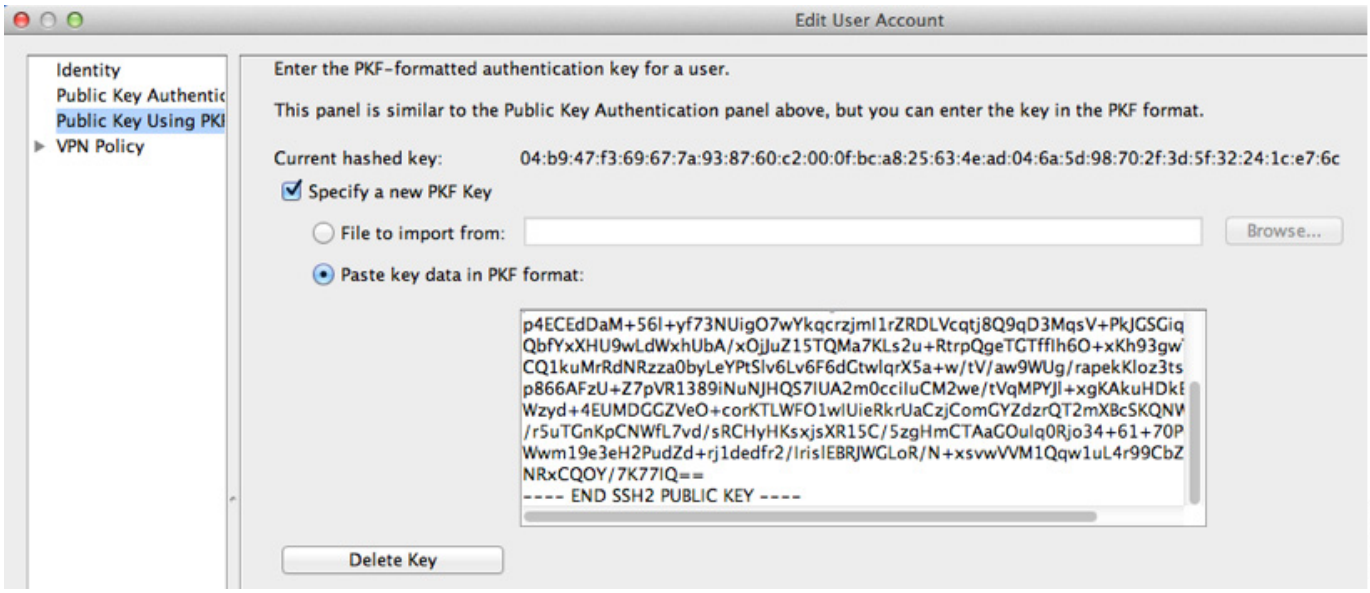
```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
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+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

步骤 3　将密钥复制到剪贴板。

步骤 4　在 ASDM 中，依次选择 **Configuration > Device Management > Users/AAA > User Accounts**，选择用户名，然后点击 **Edit**。点击 **Public Key Using PKF** 并将密钥粘贴到窗口中：



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>
```

测试本地数据库身份验证和授权

要确定 ASA 是否能够联系本地数据库并对用户进行身份验证或授权，请执行下列步骤：

操作步骤

步骤 1　在 **Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups** 表中，点击服务器所在的服务器组。

步骤 2　在 **Servers in the Selected Group** 表中点击要测试的服务器。

步骤 3　点击 **Test**。

系统将针对所选服务器显示 **Test AAA Server** 对话框。

步骤 4　点击要执行的测试的类型 - **Authentication** 或 **Authorization**。

步骤 5　输入用户名。

步骤 6　如果要测试身份验证，请输入该用户名的密码。

步骤 7　点击 **OK**。

ASA 将向服务器发送身份验证或授权测试消息。如果测试失败， ASDM 将显示错误消息。

监控本地数据库

请查看以下用于监控本地数据库的屏幕：

- **Monitoring > Properties > AAA Servers**

  此窗格显示 AAA 服务器统计信息。

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

本地数据库历史记录

表 30-1　　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。 引入了以下屏幕： Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > User Accounts。

表 30-1　　本地数据库历史记录

功能名称	平台版本	说明
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。 引入了以下屏幕： Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Authentication Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Using PKF *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

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 31-1 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 31-1　　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。

表 31-1　　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
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
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

表 31-1　　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-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
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

表 31-1　　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-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
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。

表 31-1　　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-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
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。

表 31-1　　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
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
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”

表 31-1　　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
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
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

表 31-1　　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-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
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）

表 31-1　　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-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
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 31-2　　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
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

连接断开原因代码 （续）
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 30-3 页
- 组中存在多个服务器时的回退方式，第 30-4 页
- 从锁定中恢复，第 34-21 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 31-14 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 31-15 页。

步骤 4　（可选）指定在 AAA 身份验证质询过程中要向用户显示的文本。请参阅添加身份验证提示，第 31-16 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　依次选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**。

步骤 2　点击 **AAA Server Groups** 区域中的 **Add**。

系统将显示 **Add AAA Server Group** 对话框。

步骤 3　在 **Server Group** 字段中输入组的名称。

步骤 4　从 **Protocol** 下拉列表中选择 RADIUS 服务器类型。

步骤 5　点击 **Accounting Mode** 字段中的 **Simultaneous** 或 **Single**。

在 Single 模式下， ASA 将记帐数据仅发送到一个服务器。

在 Simultaneous 模式下， ASA 将记帐数据发送到组中的所有服务器。

步骤 6　点击 **Reactivation Mode** 字段中的 **Depletion** 或 **Timed**。

在 Depletion 模式下，只有在组中所有服务器都处于非活动状态后，故障服务器才重新激活。

在 Timed 模式下，故障服务器在 30 秒停机时间后重新激活。

步骤 7　如果选择 Depletion 重新激活模式，请在 **Dead Time** 字段中输入时间间隔。

Dead Time 是从禁用组中的最后一个服务器到随后重新启用所有服务器所经过的时间，以分钟为单位。

步骤 8　在 **Max Failed Attempts** 字段中添加允许的失败尝试次数。

此选项设置在宣布无响应服务器为非活动状态之前允许的失败连接尝试次数。

步骤 9　（可选）如果添加的是 RADIUS 服务器类型，请执行以下操作：

a. 如果要为无客户端 SSL VPN 和 AnyConnect 会话启用多会话记帐，请选中 **Enable interim accounting update** 复选框。

b. 选中 **Enable Active Directory Agent Mode** 复选框，以指定 ASA 和 AD 代理之间的共享密钥并指出 RADIUS 服务器组包含并非全功能 RADIUS 服务器的 AD 代理。只能将使用此选项配置的 RADIUS 服务器组与用户身份关联。

c. 选中 **Enable dynamic authorization** 复选框，以使 ISE 能够发送授权变更 (CoA) RADIUS 数据包。这样使得在 ISE 上做出的策略更改可以在 VPN 连接的有效期期间执行。

d. 输入 **Dynamic Authorization Port**。这是用于 RADIUS CoA 请求的侦听端口。通常为 1700。有效范围为 1 至 65535。

e. 选中 **Use authorization only mode (no common password configuration required)** 复选框以对 RADIUS 服务器组启用仅授权模式。如果选中此复选框，则为单个 AAA 服务器配置的公用密码不是必需的，而且也不需要进行配置。

f. 点击 **VPN3K Compatibility Option** 向下箭头将列表展开，然后点击以下其中一个选项来指定是否应将从 RADIUS 数据包收到的可下载 ACL 与思科 AV 对 ACL 合并。

- **Do not merge**
- **Place the downloadable ACL after Cisco AV-pair ACL**
- **Place the downloadable ACL before Cisco AV-pair ACL**

步骤 10　点击 **OK**。

系统将关闭 **Add AAA Server Group** 对话框，并将新服务器组添加到 **AAA Server Groups** 表。

步骤 11　在 **AAA Server Groups** 对话框中，点击 **Apply** 以将更改保存到运行配置。

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　依次选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**，然后在 **AAA Server Groups** 区域中，点击要向其添加服务器的服务器组。

步骤 2　点击 **Servers in the Selected Group** 区域 （下窗格）中的 **Add**。

系统将为该服务器组显示 **Add AAA Server Group** 对话框。

步骤 3　选择身份验证服务器所在接口的名称。

步骤 4　为正添加到组中的服务器添加名称或 IP 地址。

步骤 5　添加超时值或保留默认值。超时是指在将请求发送到备用服务器之前，ASA 等待来自主用服务器的响应的时间 （以秒为单位）。

步骤 6　指定希望 ASA 处理在可下载 ACL 中收到的网络掩码的方法。从以下选项中选择：

- **Detect automatically** - ASA 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 ASA 会将其转换为标准网络掩码表达式。

  注意　由于难以明确检测这些通配符表达式，此设置可能会误将通配符网络掩码表达式当作标准网络掩码表达式。

- **Standard** - ASA 假定从 RADIUS 服务器收到的可下载 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。
- **Wildcard** - 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 7　指定通过此 ASA 访问该 RADIUS 授权服务器的用户的公用密码 （区分大小写）。请务必将此信息提供给 RADIUS 服务器管理员。

注意　对于身份验证 RADIUS 服务器 （而非授权服务器），请勿配置公用密码。

如果将此字段留空，则用户名即是用于访问此 RADIUS 授权服务器的密码。

请勿使用 RADIUS 授权服务器进行身份验证。公用密码或使用用户名作为密码不如指定唯一的用户密码安全。

虽然 RADIUS 协议和 RADIUS 服务器要求密码，但用户并不需要知道该密码。

步骤 8　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，则可以通过取消选中此复选框，将该服务器配置为发送非 MS-CHAPv2 的身份验证请求。

步骤 9　指定 ASA 前后两次尝试与服务器进行通信中间所等待的时长 （1 到 10 秒）。

注意　无论您输入了哪种 retry-interval 设置，随后的重试间隔时间都将始终为 50 或 100 毫秒。这是预期行为。

步骤 10　点击 **Simultaneous** 或 **Single**。

在 Single 模式下， ASA 将记帐数据仅发送到一个服务器。

在 Simultaneous 模式下， ASA 将记帐数据发送到组中的所有服务器。

步骤 11　指定用于用户记帐的服务器端口。默认端口为 1646。

步骤 12　指定用于用户身份验证的服务器端口。默认端口为 1645。

步骤 13　指定用于向 ASA 对 RADIUS 服务器进行身份验证的共享密钥。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，请询问 RADIUS 服务器管理员。最大字段长度为 64 个字符。

步骤 14　点击 **OK**。

系统将关闭 **Add AAA Server Group** 对话框，并会将 AAA 服务器添加到 AAA 服务器组。

步骤 15　在 **AAA Server Groups** 窗格中，点击 **Apply** 以将更改保存到运行配置。

添加身份验证提示

当要求通过 RADIUS 服务器进行用户身份验证时，您可以通过 ASA 为 HTTP、FTP 和 Telnet 访问指定质询文本。此文本是主要用于修饰目的，并且显示在用户登录时看到的用户名和密码提示符上方。如果不指定身份验证提示，则用户在使用 RADIUS 服务器进行身份验证时会看到以下信息：

连接类型	默认提示
FTP	FTP 身份验证
HTTP	HTTP 身份验证
Telnet	无

要添加身份验证提示，请执行以下操作：

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Users/AAA > Authentication Prompt**。

步骤 2　在 **Prompt** 字段中输入文本，以将其添加为用户登录时看到的用户名和密码提示符上方显示的消息。

下表显示身份验证提示的允许字符数限制：

应用层	字符限制
Microsoft Internet Explorer	37
Telnet	235
FTP	235

步骤 3　在 **User accepted message** 和 **User rejected message** 字段中添加消息。

如果通过 Telnet 进行用户身份验证，则可以使用 **User accepted message** 和 **User rejected message** 选项来显示不同的状态提示，以表明 RADIUS 服务器接受还是拒绝身份验证尝试。

如果 RADIUS 服务器对用户进行身份验证，则 ASA 会向用户显示 **User accepted message** 文本（如果指定）；否则， ASA 显示 **User rejected message** 文本（如果指定）。HTTP 和 FTP 会话的身份验证仅在提示时才会显示质询文本。系统不会显示 **User accepted message** 和 **User rejected message** 文本。

步骤 4　点击 **Apply** 以将更改保存到运行配置。

测试 RADIUS 服务器身份验证和授权

要确认 ASA 是否能够联系 RADIUS 服务器并对用户进行身份验证或授权，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**。

步骤 2　在 **AAA Server Groups** 表中点击服务器所在的服务器组。

步骤 3　在 **Servers in the Selected Group** 表中点击要测试的服务器。

步骤 4　点击 **Test**。

系统将针对所选服务器显示 **Test AAA Server** 对话框。

步骤 5　点击要执行的测试的类型 - **Authentication** 或 **Authorization**。

步骤 6　输入用户名。

步骤 7　如果测试的是身份验证，请输入与用户名对应的密码。

步骤 8　点击 **OK**。

ASA 将向服务器发送身份验证或授权测试消息。如果测试失败，系统会显示错误消息。

监控用于 AAA 的 RADIUS 服务器

请参阅以下屏幕以监控用于 AAA 的 RADIUS 服务器的状态：

- **Monitoring > Properties > AAA Servers**

  此窗格显示 RADIUS 服务器运行配置。

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

用于 AAA 的 RADIUS 服务器历史记录

表 31-3　　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。 引入了以下屏幕： Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > Authentication Prompt.
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

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 32-1 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 32-2　　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。
指定所使用的服务	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 30-3 页
- 组中存在多个服务器时的回退方式，第 30-4 页
- 从锁定中恢复，第 34-21 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 32-3 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 32-4 页。

步骤 3　（可选）指定在 AAA 身份验证质询过程中要向用户显示的文本。请参阅添加身份验证提示，第 32-4 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　依次选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**。

步骤 2　点击 **AAA Server Groups** 区域中的 **Add**。

系统将显示 **Add AAA Server Group** 对话框。

步骤 3　在 **Server Group** 字段中输入组的名称。

步骤 4　从 **Protocol** 下拉列表中选择 **TACACS+** 服务器类型：

步骤 5　点击 **Accounting Mode** 字段中的 **Simultaneous** 或 **Single**。

在 Single 模式下， ASA 将记帐数据仅发送到一个服务器。

在 Simultaneous 模式下， ASA 将记帐数据发送到组中的所有服务器。

步骤 6　点击 **Reactivation Mode** 字段中的 **Depletion** 或 **Timed**。

在 Depletion 模式下，只有在组中所有服务器都处于非活动状态后，故障服务器才重新激活。

在 Timed 模式下，故障服务器在 30 秒停机时间后重新激活。

步骤 7　如果选择 Depletion 重新激活模式，请在 **Dead Time** 字段中输入时间间隔。

Dead Time 是从禁用组中的最后一个服务器到随后重新启用所有服务器所经过的时间，以分钟为单位。

步骤 8　添加允许的最大失败尝试次数。

此选项设置在宣布无响应服务器为非活动状态之前允许的失败连接尝试次数。

步骤 9　点击 **OK**。

系统将关闭 **Add AAA Server Group** 对话框，并将新服务器组添加到 **AAA Server Groups** 表。

步骤 10　点击 **Apply** 以将更改保存到运行配置。

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　依次选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**。

步骤 2　点击要向其添加服务器的服务器组。

步骤 3　在 **Servers in the Selected Group** 区域点击 **Add**。

系统将为该服务器组显示 **Add AAA Server Group** 对话框。

步骤 4　选择身份验证服务器所在接口的名称。

步骤 5　为正添加到组中的服务器添加名称或 IP 地址。

步骤 6　添加超时值或保留默认值。超时时间是指在将请求发送到备用服务器之前，ASA 等待来自主用服务器的响应的时间 （以秒为单位）。

步骤 7　指定服务器端口。该服务器端口是端口号 139，或者是 ASA 用于与 TACACS+ 服务器通信的 TCP 端口号。

步骤 8　指定服务器密钥。该共享密钥用于面向 ASA 对 TACACS+ 服务器进行身份验证。您在此处配置的服务器密钥，应与在 TACACS+ 服务器上配置的密钥匹配。如果您不知道服务器密钥，请询问 TACACS+ 服务器管理员。最大字段长度为 64 个字符。

步骤 9　点击 **OK**。

系统将关闭 **Add AAA Server Group** 对话框，并会将 AAA 服务器添加到 AAA 服务器组。

步骤 10　点击 **Apply** 以将更改保存到运行配置。

添加身份验证提示

您可以指定在 AAA 身份验证质询过程中，将会向用户显示的文本。要求通过 TACACS+ 服务器进行用户身份验证时，您可以通过 ASA 为 HTTP、 FTP 和 Telnet 访问指定 AAA 质询文本。此文本是主要用于修饰目的，并且显示在用户登录时看到的用户名和密码提示上方。

如果不指定身份验证提示，则用户在使用 RADIUS 服务器进行身份验证时会看到以下信息：

连接类型	默认提示
FTP	FTP 身份验证
HTTP	HTTP 身份验证
Telnet	无

要添加身份验证提示，请执行以下操作：

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Users/AAA > Authentication Prompt**。

步骤 2　添加用户登录时在用户名和密码提示上方看到的文本。

下表显示身份验证提示的允许字符数限制：

应用层	身份验证提示的字符数限制
Microsoft Internet Explorer	37
Telnet	235
FTP	235

步骤 3　在 **User accepted message** 和 **User rejected message** 字段中添加消息。

如果是通过 Telnet 进行用户身份验证，则可以使用 **User accepted message** 和 **User rejected message** 选项来显示不同的状态提示，以表明 AAA 服务器是接受，还是拒绝身份验证尝试。

如果 AAA 服务器对用户进行身份验证，则 ASA 会向用户显示 **User accepted message** 文本（如已指定）；否则， ASA 会显示 **User rejected message** 文本 （如已指定）。HTTP 和 FTP 会话的身份验证仅在提示时才会显示质询文本。系统不会显示 User accepted message 和 User rejected message 文本。

步骤 4　点击 **Apply** 以将更改保存到运行配置。

测试 TACACS+ 服务器身份验证和授权

要确定 ASA 是否能够联系 TACACS+ 服务器并对用户进行身份验证或授权，请执行下列步骤：

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**。

步骤 2　点击服务器所在的服务器组。

步骤 3　点击要测试的服务器。

步骤 4　点击 **Test**。

系统将针对所选服务器显示 **Test AAA Server** 对话框。

步骤 5　点击要执行的测试的类型 - **Authentication** 或 **Authorization**。

步骤 6　输入用户名。

步骤 7　如果要测试身份验证，请输入该用户名的密码。

步骤 8　点击 **OK**。

ASA 将向服务器发送身份验证或授权测试消息。如果测试失败，系统会显示错误消息。

监控用于 AAA 的 TACACS+ 服务器

请参阅以下用于监控用于 AAA 的 TACACS+ 服务器的屏幕：

- **Monitoring > Properties > AAA Servers**

  此窗格显示已配置的 TACACS+ 服务器统计信息。

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

用于 AAA 的 TACACS+ 服务器历史记录

表 32-3　　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。 引入了以下屏幕： Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > Authentication Prompt.

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

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。

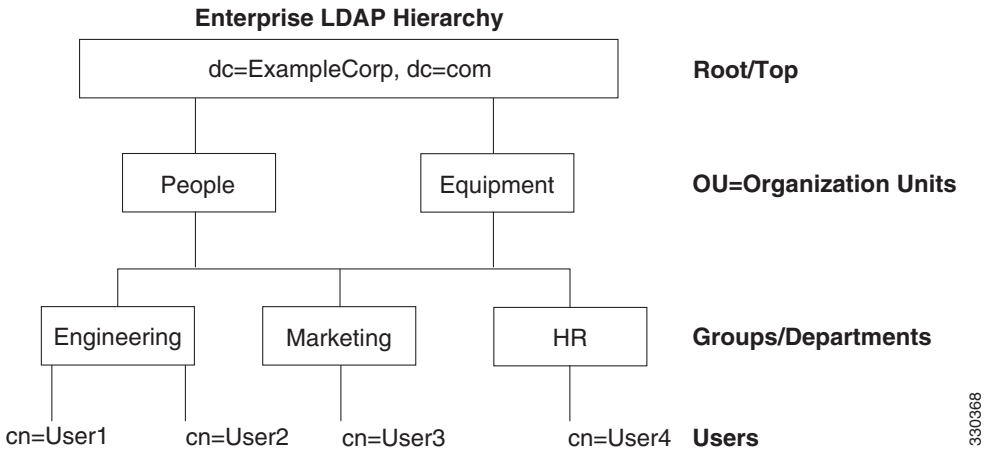
备注　有关 LDAP 协议的详细信息，请参阅 RFC 1777、 2251 和 2849。

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 33-1　　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 33-1　　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 33-5 页。

步骤 2　添加 LDAP 服务器组。请参阅配置 LDAP 服务器组，第 33-6 页。

步骤 3　向组中添加服务器，然后配置服务器参数。请参阅向服务器组中添加 LDAP 服务器，第 33-6 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　依次选择 **Configuration > Remote Access VPN > AAA Local Users > LDAP Attribute Map**（对于本地用户），或者依次选择 **Configuration > Device Management > Users/AAA > LDAP Attribute Map**（对于其他所有用户），然后点击 **Add**。

系统将显示 **Add LDAP Attribute Map** 对话框，其中 **Mapping of Attribute Name** 选项卡处于活动状态。

步骤 2　创建此属性映射的名称。

步骤 3　添加要映射的其中一个 LDAP 属性的名称。

步骤 4　选择思科属性。

步骤 5　点击 **Add**。

步骤 6　要映射更多属性，请重复步骤 1 至 5。

步骤 7　点击 **Mapping of Attribute Value** 选项卡以将任何 LDAP 属性的值映射到已映射的思科属性中的新值。

步骤 8　点击 **Add**。

系统将显示 **Add Mapping of Attribute Value** 对话框。

步骤 9　输入您希望从 LDAP 服务器返回的此 LDAP 属性的值。

步骤 10　当此 LDAP 属性包含以前的 LDAP 属性值时，输入要在思科属性中使用的值。

步骤 11　点击 **Add**。

步骤 12　要映射更多属性值，请重复步骤 8 至 11。

步骤 13　点击两下 **OK** 以关闭每个对话框。

步骤 14　点击 **Apply** 以将设置保存到运行配置。

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　为 VPN 用户依次选择 **Configuration > Device Management > Users/AAA > AAA Server Groups** 或 **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**。

步骤 2　点击**添加**。

系统将显示 **Add AAA Server Group** 对话框。

步骤 3　输入 AAA 服务器组的名称。

步骤 4　从 **Protocol** 下拉列表中选择 LDAP 服务器类型。

步骤 5　点击要使用的重新激活模式的对应单选按钮 （**Depletion** 或 **Timed**）。

在 Depletion 模式下，只有在组中所有服务器都处于非活动状态后，故障服务器才重新激活。

在 Timed 模式下，故障服务器在 30 秒停机时间后重新激活。

a. 如果选择 Depletion 重新激活模式，请在 **Dead Time** 字段中输入时间间隔。

Dead Time 是从禁用组中的最后一个服务器到随后重新启用所有服务器所经过的时间，以分钟为单位。

步骤 6　添加为连接到服务器而允许的最大失败尝试数。

此选项设置在宣布无响应服务器为非活动状态之前允许的失败连接尝试次数。

步骤 7　点击 **OK**。

系统将关闭 **Add AAA Server Group** 对话框，并会将新服务器组添加到 AAA 服务器组。

步骤 8　点击 **Apply** 以将更改保存到运行配置。

向服务器组中添加 LDAP 服务器

要向服务器组中添加 LDAP 服务器，请执行以下步骤：

操作步骤

步骤 1　为 VPN 用户依次选择 **Configuration > Device Management > Users/AAA > AAA Server Groups** 或 **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**。

步骤 2　选择要向其添加服务器的服务器组，然后点击 **Add**。

系统将针对选定服务器组显示 **Add AAA Server** 对话框。

步骤 3　选择连接到 LDAP 服务器的接口的名称。

步骤 4　输入 LDAP 服务器的服务器名称或 IP 地址。

步骤 5　添加超时值或保留默认值。超时时间是指在将请求发送到备用服务器之前，ASA 等待来自主用服务器的响应的时间 （以秒为单位）。

步骤 6　在 **LDAP Parameters for authentication/authorization** 区域中，配置以下设置：

- **Enable LDAP over SSL** （也称为安全 LDAP 或 LDAP-S） - 如果要使用 SSL 保护 ASA 与 LDAP 服务器之间的通信，请选中此复选框。

注意　如果未配置 SASL 协议，则强烈建议通过 SSL 来保护 LDAP 通信。

- **Server Port** - 输入 TCP 端口号 389，ASA 使用该端口访问 LDAP 服务器进行简单 （非安全） 身份验证；或输入 TCP 端口 636 以进行安全身份验证 (LDAP-S)。所有 LDAP 服务器都支持身份验证和授权。仅 Microsoft AD 和 Sun LDAP 服务器另行提供 VPN 远程访问密码管理功能，该功能需要 LDAP-S。
- **Server Type** - 从下拉列表中指定 LDAP 服务器类型。可用选项包括：
  - **Detect Automatically/Use Generic Type**
  - **Microsoft**
  - **Novell**
  - **OpenLDAP**
  - **Sun，现在是 Oracle Directory Server Enterprise Edition 的一部分**
- **Base DN** - 在 LDAP 层次结构中输入基础可分辨名称 (DN) 或服务器在收到 LDAP 请求 （例如， OU=people, dc=cisco, dc=com） 时应开始搜索的位置。
- **Scope** - 指定服务器在收到来自下拉列表中的授权请求时应在 LDAP 层次结构中执行搜索的范围。可提供以下选项：
  - **One Level** - 仅搜索 Base DN 以下的一个级别。此选项速度更快。
  - **All Levels** - 搜索 Base DN 以下的所有级别 （即搜索整个子树层次结构）。此选项需要更长的时间。
- **Naming Attribute(s)** - 输入唯一识别 LDAP 服务器上的某个条目的相对可分辨名称属性。常用命名属性为通用名称 (CN)、 sAMAccountName、 userPrincipalName 和用户 ID (uid)。
- **Login DN and Login Password** - ASA 使用登录 DN 和登录密码与 LDAP 服务器建立信任（绑定）。指定登录密码，该密码是登录 DN 用户帐户的密码。
- **LDAP Attribute Map** - 选择所创建的供该 LDAP 服务器使用的属性映射之一。这些属性映射将 LDAP 属性名称映射到思科属性名称和值。
- **SASL MD5 authentication** - 该选项使 SASL 的 MD5 机制能够对 ASA 与 LDAP 服务器之间的通信进行身份验证。
- **SASL Kerberos authentication** - 使 SASL 的 Kerberos 机制能够对 ASA 与 LDAP 服务器之间的通信进行安全身份验证。您必须已定义 Kerberos 服务器，才能启用该选项。
- **LDAP Parameters for Group Search** - 该区域中的字段配置 ASA 向 AD 组提出请求的方式。
  - **Group Base DN** - 指定在 LDAP 层次结构中开始搜索 AD 组（即 memberOf 枚举列表）的位置。如果未配置此字段，ASA 将使用基础 DN 执行 AD 组检索。ASDM 使用检索到的 AD 组列表定义动态访问策略的 AAA 选择条件。有关详细信息，请参阅 **show ad-groups** 命令。
  - **Group Search Timeout** - 指定等待来自 AD 服务器（已查询来获取可用组）的响应的最长时间。

步骤 7　点击 **OK**。

系统将关闭 **Add AAA Server** 对话框，并会将 AAA 服务器添加到 AAA 服务器组。

步骤 8　点击 **Apply** 以将更改保存到运行配置。

测试 LDAP 服务器身份验证和授权

要确定 ASA 是否可以联系 LDAP 服务器并对用户进行身份验证或授权，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**。

步骤 2　选择服务器驻留所在的服务器组。

步骤 3　选择要测试的服务器。

步骤 4　点击 **Test**。

系统将针对所选服务器显示 **Test AAA Server** 对话框。

步骤 5　点击要执行的测试的类型 - **Authentication** 或 **Authorization**。

步骤 6　输入用户名。

步骤 7　如果要测试身份验证，请输入该用户名的密码。

步骤 8　点击 **OK**。

ASA 将向服务器发送身份验证或授权测试消息。如果测试失败，系统会显示错误消息。

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，请参阅以下屏幕：

- **Monitoring > Properties > AAA Servers**

  此窗格显示已配置的 AAA 服务器统计信息。

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

用于 AAA 的 LDAP 服务器的历史记录

表 33-2　　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。 引入了以下屏幕： Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Remote Access VPN > AAA Local Users > LDAP Attribute Map.

第 7 部分

系统管理

管理访问

本章介绍如何通过 Telnet、 SSH 和 HTTPS （使用 ASDM）访问思科 ASA 进行系统管理，如何对用户进行身份验证和授权以及如何创建登录横幅。

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，必须依次选择 **Configuration > Device Management > Users/AAA > AAA Access > Authentication** 配置 AAA 身份验证；然后依次选择 **Configuration > Device Management > Users/AAA > User Accounts** 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 18-1 页
- 向本地数据库添加用户帐户，第 30-4 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）。

步骤 1　依次浏览至 **Configuration > Device Management > Management Access > HTTP Certificate Rule**。

备注　此配置不适用于透明防火墙模式和多情景模式。

步骤 2　点击 **Specify the certificate fields to be used as the username** 输入主要和辅助字段。

步骤 3　从 Primary Field 和 Secondary Field 下拉列表中选择值，指定要用于派生用户名的属性和其他属性。

- C - 国家/地区：符合 ISO 3166 国家/地区缩写的两个字母的国家/地区缩写。
- CN - 公用名称：人员、系统或其他实体的名称。不可用作辅助属性。
- DNQ - 域名限定符。
- EA - 邮件地址。
- GENQ - 世代限定符。
- GN - 名。
- I - 首字母。
- L - 区域：组织所在的城市或城镇。
- N - 名称。
- O - 组织：公司、机构、办事处、协会或其他实体的名称。
- OU - 组织单位：组织 (O) 内的子组。
- SER - 序列号。
- SN - 姓氏。
- SP - 省/自治区/直辖市：组织所在的省/自治区/直辖市。
- T - 职位。
- UID - 用户标识符。
- UPN - 用户主体名称。

步骤 4　（可选并仅适用于主要属性）选择 **Use the entire DN as the username**。

步骤 5　（可选）如要使用 ASDM 生成的脚本，请选择 **Use script to select username**。

步骤 6　选中 **Prefill Username** 复选框可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。如果用户名与用户最初输入的用户名不同，则会显示一个新的弹出窗口，其中包含预填充的用户名，只要求用户输入用于身份验证的密码。

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。

准备工作

在多情景模式下，请在情景执行空间中完成此程序。如要从系统更改为情景配置，请在 **Configuration > Device List** 窗格中双击主用设备 IP 地址下的情景名称。

如要确定允许使用 Telnet、 SSH 或 ASDM 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　依次选择 **Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH**，然后点击 **Add**。

系统将显示 **Add Device Access Configuration** 对话框。

步骤 2　从列出的三个选项中选择会话类型：**ASDM/HTTPS**、 **Telnet** 或 **SSH**。

步骤 3　选择管理接口并设置允许的主机 IP 地址，然后点击 **OK**。

步骤 4　确保选中 **Enable HTTP Server** 复选框。默认情况下，此选项已启用。根据需要设置其他 HTTP 服务器选项。

步骤 5　（可选）配置 Telnet 设置。默认超时值为 5 分钟。

步骤 6　（可选）配置 SSH 设置。对于 **DH Key Exchange**，请点击适用的单选按钮选择 Diffie-Hellman (DH) 密钥交换群 1 或群 14。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。

步骤 7　点击 **Apply**。

步骤 8　（Telnet 必需）设置登录密码，然后才可以使用 Telnet 连接；没有默认密码。

a. 依次选择 **Configuration > Device Setup > Device Name/Password**。

b. 在 **Telnet Password** 区域中，选中 **Change the password to access the console of the security appliance** 复选框。

c. 输入原密码 （对于新 ASA，请将此字段留空）和新密码，然后确认新密码。

d. 点击 **Apply**。

步骤 9　（SSH 必需）配置 SSH 用户身份验证。

a. 依次选择 **Configuration > Device Management > Users/AAA > AAA Access > Authentication**。

b. 选中 **SSH** 复选框。

c. 从 **Server Group** 下拉列表中选择 **LOCAL** 数据库。或者，也可以配置使用 AAA 服务器的身份验证。

d. 点击 **Apply**。

e. 添加本地用户。依次选择 **Configuration > Device Management > Users/AAA > User Accounts**，然后点击 **Add**。

系统将显示 **Add User Account-Identity** 对话框。

f. 输入用户名和密码，然后确认密码。

g. 点击 **OK**，然后点击 **Apply**。

配置 HTTP 重定向

通过 ASDM，您可以使用 HTTPS 连接至 ASA。为了方便起见，可以将到管理接口的 HTTP 连接重定向至 HTTPS。例如，通过重定向 HTTP，用户输入 http://10.1.1.4/admin/ 或 https://10.1.8.4/admin/ 均可到达位于该 HTTPS 地址的 ASDM 启动页面。

提示 管理接口上的访问规则必须既允许 HTTP 连接也允许 HTTPS 连接；这些协议通常分别使用端口 80 和 443。

如要为支持用于 ASDM 访问的每个接口启用重定向，请执行以下步骤：

操作步骤

步骤 1 依次选择 **Configuration > Device Management > HTTP Redirect**。

该表显示当前已配置的接口以及是否已在某个接口上启用重定向。

步骤 2 选择用于 ASDM 的接口，然后点击 **Edit**。

步骤 3 在 **Edit HTTP/HTTPS Settings** 对话框中配置下列选项：

- **Redirect HTTP to HTTPS** - 将 HTTP 请求重定向至 HTTPS。
- **HTTP Port** - 确定接口从其重定向 HTTP 连接的端口。默认值为 80。

步骤 4 点击 **OK**。

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 依次选择 **Configuration > Device Management > Management Access > Command Line (CLI) > Banner**。

步骤 2 将横幅文本添加到为 CLI 创建的横幅类型所对应的字段中：

- 当用户在 CLI 中访问特权 EXEC 模式时，系统将显示会话 (exec) 横幅。

- 当用户登录 CLI 时，系统将显示 login 横幅。
- 当用户首次连接至 CLI 时，系统将显示 message-of-the-day (motd) 横幅。
- 当用户在通过用户身份验证后连接至 ASDM 时，系统将显示 ASDM 横幅。系统为用户提供两个选项解除横幅：
  - **Continue** - 解除横幅并完成登录。
  - **Disconnect** - 解除横幅并终止连接。
- 只允许使用 ASCII 字符，包括换行符 （Enter，计为两个字符）。
- 请勿在横幅中使用制表符，因共并未保留在 CLI 版本中。
- 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。

步骤 3　点击 **Apply**。

新的横幅将保存到运行配置中。

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　依次选择 **Configuration > Device Management > Management Access > Command Line (CLI) > CLI Prompt**。

步骤 2　执行以下任意操作以自定义提示符：

- 点击 **Available Prompts** 列表中的属性，然后点击 **Add**。可以将多个属性添加到提示符中。该属性将从 **Available Prompts** 列表移到 **Selected Prompts** 列表中。
- 点击 **Selected Prompts** 列表中的属性，然后点击 **Delete**。该属性将从 **Selected Prompts** 列表移到 **Available Prompts** 列表中。
- 点击 **Selected Prompts** 列表中的属性，然后点击 **Move Up** 或 **Move Down** 更改属性的显示顺序。

提示符将更改并显示在 **CLI Prompt Preview** 字段中。

步骤 3　点击 **Apply**。

新的提示符将保存到运行配置中。

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　依次选择 **Configuration > Device Management > Management Access > Command Line (CLI) > Console Timeout**。

步骤 2　定义新的超时值 （以分钟为单位）。如要指定无限制时间，请输入 **0**。默认值为 0。

步骤 3　点击 **Apply**。

超时值更改将保存到运行配置中。

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　依次选择 **Configuration > Device Management > Management Access > Management Interface**。

步骤 2　从 **Management Access Interface** 下拉列表中选择具有最高安全级别的接口 （内部接口）。

步骤 3　点击 **Apply**。

管理接口已指定，更改将保存到运行配置中。

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。（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。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， 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、ASDM 和 enable 命令访问的身份验证

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　如要对使用 **enable** 命令的用户进行身份验证，请依次选择 **Configuration > Device Management > Users/AAA > AAA Access > Authentication**，然后配置以下设置：

a. 选中 **Enable** 复选框。

b. 选择服务器组名称或 LOCAL 数据库。

c. （可选）如果选择 AAA 服务器，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。选中 **Use LOCAL when server group fails** 复选框。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。

步骤 2　如要对访问 CLI 或 ASDM 的用户进行身份验证，请依次选择 **Configuration > Device Management > Users/AAA > AAA Access > Authentication**，然后配置以下设置：

a. 选中一个或多个以下复选框：

- **HTTP/ASDM** - 对使用 HTTPS 访问 ASA 的 ASDM 客户端进行身份验证。HTTP 管理身份验证不支持 AAA 服务器组的 SDI 协议。
- **Serial** - 对使用控制台端口访问 ASA 的用户进行身份验证。对于 ASASM，此参数使用 **service-module session** 命令影响从交换机访问的虚拟控制台。
- **SSH** - 对使用 SSH 访问 ASA 的用户进行身份验证。
- **Telnet** - 对使用 Telnet 访问 ASA 的用户进行身份验证。对于 ASASM，此参数还可使用 **session** 命令影响来自交换机的会话。

b. 对于选中的每项服务选择服务器组名称或 LOCAL 数据库。

c. （可选）如果选择 AAA 服务器，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。选中 **Use LOCAL when server group fails** 复选框。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。

步骤 3　点击 **Apply**。

步骤 4　如要配置从证书提取用户名的规则，请依次选择 **Configuration > Device Management > Management Access > HTTP Certificate Rule**，然后执行以下操作之一：

- 点击 **Specify the Certificate Fields to be used** 单选按钮，然后从 **Primary Field** 和 **Secondary Field** 下拉列表中选择值。
- 点击 **Use the entire DN as the username** 单选按钮。
- 点击 **Use script to select username**，然后点击 **Add** 添加脚本内容。

注意　选中 **Prefill Username** 复选框，启用要从证书提取的用于身份验证的用户名。

步骤 5　点击 **Apply**。

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 依次启用 **Authentication > Serial** 选项，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 Telnet 和 SSH 会话的管理授权，请依次选择 **Configuration > Device Management > Users/AAA > AAA Access > Authorization**，然后选中 **Enable Authorization for ASA Command Access** 区域中的 **Enable** 复选框。
- 如要启用对 HTTP 会话的管理授权，请依次选择 **Configuration > Device Management > Users/AAA > AAA Access > Authorization**，然后选中 **Enable Authorization for ASA Command Access** 区域中的 **HTTP** 复选框。

  当配置 **LOCAL** 选项时，本地用户数据库是输入的用户名和已分配的 Service-Type 和 Privilege-Level 属性的源。

  此选项还启用对来自 RADIUS 的管理用户权限级别的支持，这些权限级别可与本地命令权限级别配合用于命令授权。

  当配置 **authentication-server** 选项时，使用同一服务器进行身份验证和授权。您可以设置用于 HTTP 的单独的授权配置，也可以将授权和身份验证设置为独立工作或一起工作。

步骤 2　点击 **Configure Command Privileges** 向个人或组分配命令权限级别。默认情况下会禁用授权，因此必须点击 **Set ASDM Defined User Roles** 将其启用。

步骤 3　在 **Perform authorization for exec shell access** 区域中，选中 **Enable** 执行授权，然后选择 **Remote** 或 **Local** 单选按钮指定要用于执行外壳访问授权的服务器。

步骤 4　如要启用管理授权，请选中 **Allow privileged users to enter into EXEC mode on login** 复选框。

auto-enable 选项使来自登录身份验证服务器的拥有足够权限的用户能够直接进入特权 EXEC 模式。否则，用户将处于用户 EXEC 模式。这些权限由进入每个 EXEC 模式所需的 Service-Type 和 Privilege-Level 属性决定。如要进入特权 EXEC 模式，用户的 Service-Type 属性必须为 Administrative，而且分配给这些用户的 Privilege Level 属性必须大于 1 。

在系统情景中不支持此选项。但是，如果在管理员情景中配置 Telnet 或串行身份验证，则身份验证也适用于从交换机到 ASASM 的会话。

如果单独输入 **aaa authorization exec** 命令，则没有影响。

在管理授权中使用串行身份验证时，不包括 **auto-enable** 选项。

auto-enable 选项不会影响 **aaa authentication http** 命令。

在配置 **auto-enable** 选项之前，建议同时配置协议登录和 enable 身份验证，使所有身份验证请求都转至相同的 AAA 服务器组，如以下示例所示：

```
ciscoasa (config)# aaa authentication ssh console RADIUS
ciscoasa (config)# aaa authentication enable console RADIUS
ciscoasa (config)# aaa authorization exec authentication-server auto-enable
```

建议 *不要* 使用其他类型的配置。

步骤 5　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，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 **Authentication** 选项卡选项指定的任何服务进行完全访问。
  - Service-Type 7 (NAS prompt) - 允许在配置 **Telnet** 或 **SSH** 身份验证选项时访问 CLI，但是如果配置 **HTTP** 选项，则拒绝 ASDM 配置访问。允许 ASDM 监控访问。如果使用 **Enable** 选项配置 **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 **Authentication** 选项卡选项指定的任何服务 （不包括 **Serial** 选项；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。

- 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 - 允许对 **Authentication** 选项卡选项指定的任何服务进行完全访问。
  - PASS, privilege level 2 和更高级别 - 允许在配置 **Telnet** 或 **SSH** 身份验证选项时访问 CLI，但是如果配置 **HTTP** 选项，则拒绝 ASDM 配置访问。允许 ASDM 监控访问。如果使用 **Enable** 选项配置 **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 **Authentication** 选项卡选项指定的任何服务 （不包括 **Serial** 选项；允许串行访问）。

- 本地用户

  为给定用户名配置 **Access Restrictions** 选项。默认情况下，访问限制是 **Full Access**，允许对 **Authentication** 选项卡选项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 **User Accounts** 窗格更改密码时，以及使用 **Change My Password** 窗格更改密码时，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　依次选择 **Configuration > Device Management > Users/AAA > Password Policy**。

步骤 2　配置以下选项的任意组合：

- **Minimum Password Length** - 输入最小密码长度。有效值范围为 3 到 64 个字符。建议的最小密码长度为 8 个字符。
- **Lifetime** - 输入远程用户（SSH、Telnet、HTTP）密码到期前的间隔（以天为单位）；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：

  - 让另一位管理员更改您的密码。
  - 登录到物理控制台端口更改密码。
- **Minimum Number Of** - 指定以下类型的最小字符数：
  - **Numeric Characters** - 输入密码必须具有的最小数字字符数。有效值为 0 到 64 个字符。默认值为 0。
  - **Lower Case Characters** - 输入密码必须具有的最小小写字符数。有效值范围为 0 到 64 个字符。默认值为 0。
  - **Upper Case Characters** - 输入密码必须具有的最小大写字符数。有效值范围为 0 到 64 个字符。默认值为 0。
  - **Special Characters** - 输入密码必须具有的最小特殊字符数。有效值范围为 0 到 64 个字符。特殊字符包括以下字符：!、@、#、$、%、^、&、*、\q(‘和 ‘)’。默认值为 0。
  - **Different Characters from Previous Password** - 输入与旧密码相比，新密码中必须更改的最小字符数。有效值为 0 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）选中 **Authentication Enable** 复选框，要求用户在 **Change My Password** 窗格更改密码，而不是在 **User Accounts** 窗格进行更改。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在 **User Accounts** 窗格中更改密码，系统会生成以下错误消息：

```
ERROR: Changing your own password is prohibited
```

步骤 4　点击 **Apply** 保存配置设置。

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　依次选择 **Configuration > Device Management > Users/AAA > Change Password**。

步骤 2　输入旧密码。

步骤 3　输入新密码。

步骤 4　确认新密码。

步骤 5　点击 **Make Change**。

步骤 6　点击 **Save** 图标将更改保存到运行配置中。

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　依次选择 **Configuration > Device Management > Users/AAA > AAA Access > Authorization**。

步骤 2　选中 **Enable authorization for command access > Enable** 复选框。

步骤 3　从 **Server Group** 下拉列表中选择 **LOCAL**。

步骤 4　当启用本地命令授权时，可以选择手动向单个命令或命令组分配权限级别，也可以启用预定义的用户帐户权限。

- 点击 **Set ASDM Defined User Roles** 使用预定义的用户帐户权限。

  系统将显示 **ASDM Defined User Roles Setup** 对话框。点击 **Yes** 使用预定义的用户帐户权限：**Admin** （15 级权限，可对所有 CLI 命令进行完全访问）；**Read Only** （5 级权限，只读访问）；**Monitor Only** （3 级权限，只能访问 **Monitoring** 部分）。

- 点击 **Configure Command Privileges** 手动配置命令级别。

  系统将显示 **Command Privileges Setup** 对话框。您可以从 **Command Mode** 下拉列表中选择 **All Modes** 以查看所有命令，也可以选择配置模式以查看该模式下可用的命令。例如，如果选择情景，则可以查看该情景配置模式下的所有可用命令。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。

  Variant 列显示 show、 clear 或 cmd。您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。

  如要更改命令级别，请双击此命令或点击 **Edit**。可将级别设置为 0 到 15。只能配置*去*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。

  如要更改显示的所有命令的级别，请点击 **Select All**，然后点击 **Edit**。

  点击 **OK** 接受所作更改。

步骤 5　选中 **Perform authorization for exec shell access > Enable** 复选框，支持来自 RADIUS 的管理用户权限级别。

此选项还启用对本地、 RADIUS、映射的 LDAP 和 TACACS+ 用户的管理授权。

如果没有此选项，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。

步骤 6　点击 **Apply**。

授权设置已指定，更改将保存到运行配置中。

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。

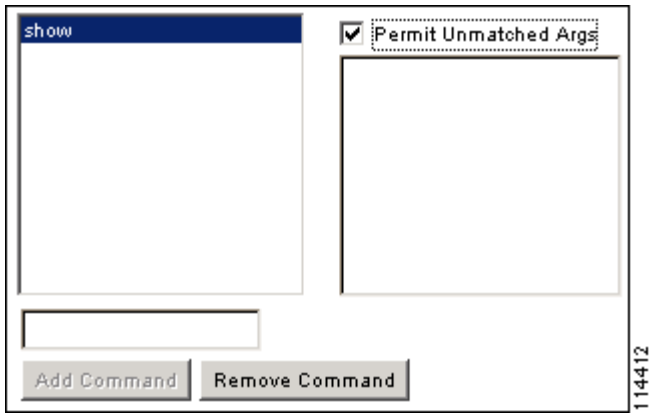
- 命令的第一个词被视为主命令。所有附加的单词都被视为参数，需要在其前面放置 **permit** 或 **deny**。

  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。

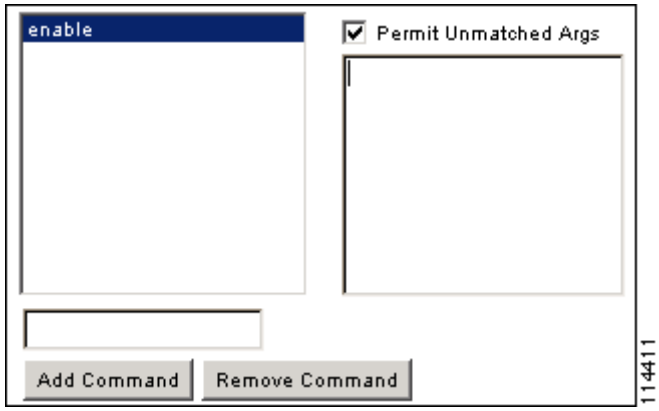
  例如，您可以仅配置 **show** 命令，那么将允许所有 **show** 命令。建议使用此方法，这样您就无需预测命令的每个变体 （包括缩写和问号），其显示 CLI 的使用情况 （请参阅下图）。

图 34-1　　允许所有相关命令



- 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**（请参阅下图）。

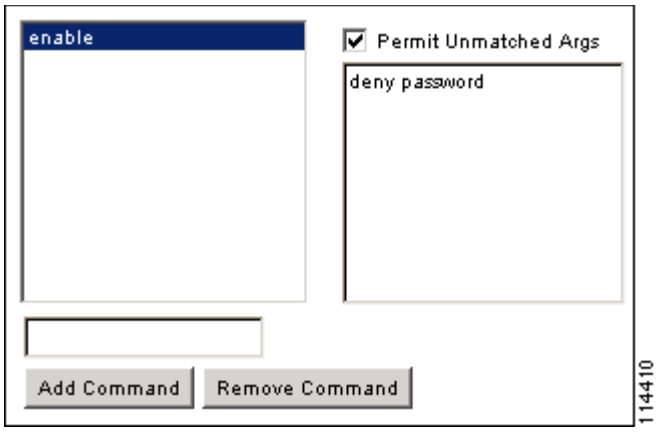
图 34-2　　允许单个单词的命令



- 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**（请参阅下图）。

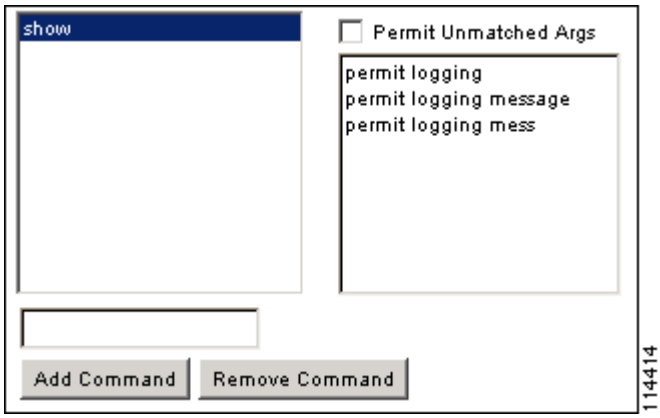
图 34-3　　禁止参数



- 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 （请参阅下图）。

图 34-4　　指定缩写



- 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 34-21 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 34-15 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　依次选择 **Configuration > Device Management > Users/AAA > AAA Access > Authorization**。

步骤 2　选中 **Enable authorization for command access > Enable** 复选框。

步骤 3　从 **Server Group** 下拉列表中选择 AAA 服务器组名称。

步骤 4　（可选）您可以将 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。为此，请选中 **Use LOCAL when server group fails** 复选框。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。请确保在本地数据库和命令权限级别中配置用户。

步骤 5　点击 **Apply**。

命令授权设置已指定，更改将保存到运行配置中。

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　如要在用户输入 **enable** 命令时启用用户记帐，请执行以下步骤：

a. 依次选择 **Configuration > Device Management > Users/AAA > AAA Access > Accounting**，然后选中 **Require accounting to allow accounting of user activity > Enable** 复选框。

b. 选择 RADIUS 或 TACACS+ 服务器组名称。

步骤 2　如要在用户使用 Telnet、 SSH 或串行控制台访问 ASA 时启用用户记帐，请执行以下步骤：

a. 在 **Require accounting for the following types of connections** 区域中，选中 **Serial**、**SSH** 和/或 **Telnet** 复选框。

b. 为每个连接类型选择 RADIUS 或 TACACS+ 服务器组名称。

步骤 3　如要配置命令记帐，请执行以下步骤：

a. 在 **Require accounting for the following types of connections** 区域中，选中 **Enable** 复选框。

b. 选择 TACACS+ 服务器组名称。不支持 RADIUS。

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。

c. 如果使用 **Command Privilege Setup** 对话框自定义命令权限级别，可以通过在 **Privilege level** 下拉列表中指定最低权限级别来限定 ASA 对哪些命令记帐。 ASA 不对低于最低权限级别的命令记帐。

步骤 4　点击 **Apply**。

记账设置已指定，更改将保存到运行配置中。

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　依次选择 **Configuration > Device Management > Management Access > Management Session Quota**。

步骤 2　输入在 ASA 上允许的并发 ASDM、 SSH 和 Telnet 会话的最大数量。有效值范围为 0 到 10000。

注意　如果超过管理配额会话数，系统将显示错误消息， ASDM 将关闭。

步骤 3　点击 **Apply** 保存配置更改。

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 34-1　　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。
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。

监控设备访问

有关监控 SNMP 的信息，请参阅以下屏幕。

- **Monitoring > Properties > Device Access > ASDM/HTTPS/Telnet/SSH Sessions**

  顶部窗格列出通过 ASDM、 HTTPS 和 Telnet 会话连接的用户的连接类型、会话 ID 和 IP 地址。如要断开特定会话，请点击 **Disconnect**。

  底部窗格中列出客户端、用户名、连接状态、软件版本、传入加密类型、传出加密类型，传入 HMAC、传出 HMAC、 SSH 会话 ID、剩余重新生成密钥的数据、剩余重新生成密钥的时间、基于数据重新生成密钥次数、基于时间重新生成密钥次数和上次重新生成密钥的时间。如要断开特定会话，请点击 **Disconnect**。

- **Monitoring > Properties > Device Access > Authenticated Users**

  此窗格列出通过 AAA 服务器进行身份验证的用户的用户名、 IP 地址、动态 ACL、非活动超时 （如果有）和绝对超时。

- **Monitoring > Properties > Device Access > AAA Local Locked Out Users**

  此窗格列出锁定的 AAA 本地用户的用户名、尝试身份验证的失败次数和用户锁定的次数。如要清除锁定的特定用户，请点击 **Clear Selected Lockout**。如要清除锁定的所有用户，请点击 **Clear All Lockouts**。

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

管理访问的历史记录

表 34-2　　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。 引入了以下屏幕： Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH Configuration > Device Management > Management Access > Command Line (CLI) > Banner Configuration > Device Management > Management Access > CLI Prompt Configuration > Device Management > Management Access > ICMP Configuration > Device Management > Management Access > File Access > FTP Client Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server Configuration > Device Management > Management Access > File Access > Mount-Points Configuration > Device Management > Users/AAA > AAA Access > Authentication Configuration > Device Management > Users/AAA > AAA Access > Authorization Configuration > Device Management > Users/AAA > AAA Access > Accounting。
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。

表 34-2　　管理访问的历史记录 （续）

功能名称	平台版本	说明
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。 引入了以下屏幕：Configuration > Device Management > Users/AAA > 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。 引入了以下屏幕： Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Authentication Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Using PKF。 *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。 修改了以下屏幕：Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH。
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。 引入了以下屏幕：Configuration > Device Management > Management Access > Management Session Quota。
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。
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。
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。 修改了以下屏幕：Configuration > Device Management > Users/AAA > AAA Access > Authorization。
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。 添加了以下屏幕：Configuration > Device Management > Management Access > HTTP Certificate Rule。 修改了以下屏幕：Configuration > Device Management > Users/AAA > AAA Access > Authorization。

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

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

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
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

软件版本显示在 ASDM 主页上；请查看主页以验证 ASA 的软件版本。

从 Cisco.com 下载软件

如果您正在使用 ASDM 升级向导，则不必预先下载软件。如果您正在进行手动升级，例如故障转移升级，请将映像下载到本地计算机。

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

升级独立设备

本节介绍如何安装 ASDM 和操作系统 (OS) 映像。

- 从本地计算机升级，第 35-3 页
- 使用 Cisco.com 向导升级，第 35-3 页

从本地计算机升级

Upgrade Software from Local Computer 工具允许您将映像文件从本地计算机上传至闪存文件系统，以便进行升级 ASA。

操作步骤

1. （如果要进行配置迁移）在 ASDM 中，使用 **Tools > Backup Configurations** 工具备份现有配置。
2. 在 ASDM 主应用窗口中，选择 **Tools > Upgrade Software from Local Computer**。

   系统将显示 **Upgrade Software** 对话框。
3. 从 **Image to Upload** 下拉列表中选择 **ASDM**。
4. 在 **Local File Path** 字段中，输入该文件在计算机上的本地路径，或者点击 **Browse Local Files** 在计算机上查找文件。
5. 在 **Flash File System Path** 字段中，输入闪存文件系统的路径，或者点击 **Browse Flash** 在闪存文件系统中查找目录或文件。
6. 点击 **Upload Image**。上传过程可能需要数分钟。
7. 系统会提示您将此映像设置为 ASDM 映像。点击 **Yes**。
8. 系统将提醒您退出 ASDM 并保存配置。点击 **OK**。您会退出 **Upgrade** 工具。**注意：**在升级 ASA 软件*之后*，您将保存配置并重新加载 ASDM。
9. 重复 2. 到 8.，从 **Image to Upload** 下拉列表中选择 **ASA**。您也可以使用此操作步骤上传其他文件类型。
10. 选择 **Tools > System Reload**，重新加载 ASA。

    系统将显示新窗口，要求您确认重新加载的详细信息。

    a. 点击 **Save the running configuration at the time of reload** 单选按钮 （默认）。

    b. 选择重新加载的时间 （例如，默认值 **Now**）。

    c. 点击 **Schedule Reload**。

    重新加载开始后，系统将显示 **Reload Status** 窗口，指示正在执行重新加载。系统还提供了退出 ASDM 的选项。
11. 在 ASA 重新加载后，重新启动 ASDM。

使用 Cisco.com 向导升级

Cisco.com 向导提供的升级软件允许您将 ASDM 和 ASA 自动升级至更加新的版本。

在此向导中，您可以执行以下操作：

- 选择 ASA 映像文件和/或 ASDM 映像文件以执行升级。

  注意：ASDM 会下载最新的映像版本，其版本号包括内部版本号。例如，如果您要下载 9.4(1)，实际下载的可能为 9.4(1.2)。这是预期行为，因此，您可以继续执行计划的升级。
- 查看您所做的升级更改。
- 下载一个或多个映像，并进行安装。
- 查看安装的状态。
- 如果安装成功完成，请重新启动 ASA 以保存配置并完成升级。

操作步骤

1. （如果要进行配置迁移）在 ASDM 中，使用 **Tools > Backup Configurations** 工具备份现有配置。
2. 选择 **Tools > Check for ASA/ASDM Updates**。

   在多情景模式中，从 System 访问此菜单。

   系统将显示 **Cisco.com Authentication** 对话框。
3. 输入 Cisco.com 用户名和密码，然后点击 **Login**。

   系统将显示 **Cisco.com Upgrade Wizard**。

   注意：如果无可用升级，系统将显示一个对话框。点击 **OK** 退出向导。
4. 点击 **Next** 显示 **Select Software** 屏幕。

   系统将显示当前的 ASA 版本和 ASDM 版本。
5. 如要升级 ASA 版本和 ASDM 版本，请执行以下步骤：

a. 在 **ASA** 区域，选中 **Upgrade to** 复选框，然后从下拉列表中选择要升级到的 ASA 版本。

b. 在 **ASDM** 区域，选中 **Upgrade to** 复选框，然后从下拉列表中选择要升级到的 ASDM 版本。

6. 点击 **Next**，显示 **Review Changes** 屏幕。
7. 请验证以下项：
   - 已下载的文件是正确的 ASA 映像文件和/或 ASDM 映像文件。
   - 您想要上传的文件是正确的 ASA 映像文件和/或 ASDM 映像文件。
   - 已选择正确的 ASA 启动映像。
8. 点击 **Next**，开始升级安装。

   然后，您可以在升级安装过程中查看其状态。

   系统将显示 **Results** 屏幕，其中提供详细信息，如升级安装状态 （成功或失败）。
9. 如果升级安装成功，为了使升级版本生效，请选中 **Save configuration and reload device now** 复选框来重新启动 ASA，然后重新启动 ASDM。
10. 点击 **Finish**，退出向导，保存对配置的更改。

    注意：要升级到下一个较高的版本 （如有），您必须重新启动向导。

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 35-5 页
- 升级主用/主用故障转移对，第 35-6 页
- 升级 ASA 集群，第 35-7 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。

操作步骤

1. （如果要进行配置迁移）在 ASDM 中，使用 **Tools > Backup Configurations** 工具备份现有配置。
2. 在主用设备上的 ASDM 主应用窗口中，选择 **Tools > Upgrade Software from Local Computer**。

   系统将显示 **Upgrade Software** 对话框。
3. 从 **Image to Upload** 下拉列表中选择 **ASDM**。
4. 在 **Local File Path** 字段中，输入该文件在计算机上的本地路径，或者点击 **Browse Local Files** 在计算机上查找文件。
5. 在 **Flash File System Path** 字段中，输入闪存文件系统的路径，或者点击 **Browse Flash** 在闪存文件系统中查找目录或文件。
6. 点击 **Upload Image**。上传过程可能需要数分钟。
7. 系统会提示您将此映像设置为 ASDM 映像。点击 **Yes**。
8. 系统将提醒您退出 ASDM 并保存配置。点击 **OK**。您会退出 **Upgrade** 工具。**注意：**在升级 ASA 软件*之后*，您将保存配置并重新加载 ASDM。
9. 重复 2. 到 8.，从 **Image to Upload** 下拉列表中选择 **ASA**。
10. 点击工具栏上的 **Save** 图标，保存配置更改。
11. 将 ASDM 连接到*备用*设备，并根据 2. 到 9.，使用在主用设备上使用的相同位置上传 ASA 和 ASDM 软件。
12. 选择 **Tools > System Reload**，以便重新加载备用 ASA。

    系统将显示新窗口，要求您确认重新加载的详细信息。
    a. 点击 **Save the running configuration at the time of reload** 单选按钮 （默认）。
    b. 选择重新加载的时间 （例如，默认值 **Now**）。
    c. 点击 **Schedule Reload**。

    重新加载开始后，系统将显示 **Reload Status** 窗口，指示正在执行重新加载。系统还提供了退出 ASDM 的选项。
13. 在备用 ASA 重新加载后，请重新启动 ASDM 并连接到备用设备以确保其运行。
14. 再次将 ASDM 连接到*主用*设备。
15. 通过选择 **Monitoring > Properties > Failover > Status**，然后点击 **Make Standby**，强行要求主用设备故障转移至备用设备。
16. 选择 **Tools > System Reload**，以便重新加载 （以前的）主用 ASA。

    系统将显示新窗口，要求您确认重新加载的详细信息。
    a. 点击 **Save the running configuration at the time of reload** 单选按钮 （默认）。
    b. 选择重新加载的时间 （例如，默认值 **Now**）。
    c. 点击 **Schedule Reload**。

    重新加载开始后，系统将显示 **Reload Status** 窗口，指示正在执行重新加载。系统还提供了退出 ASDM 的选项。

    该 ASA 启动后，会立即成为备用设备。

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。

操作步骤

1. （如果要进行配置迁移）在 ASDM 中，使用 **Tools > Backup Configurations** 工具备份现有配置。
2. 在主设备上的 ASDM 主应用窗口中，选择 **Tools > Upgrade Software from Local Computer**。

   系统将显示 **Upgrade Software** 对话框。
3. 从 **Image to Upload** 下拉列表中选择 **ASDM**。
4. 在 **Local File Path** 字段中，输入该文件在计算机上的本地路径，或者点击 **Browse Local Files** 在计算机上查找文件。
5. 在 **Flash File System Path** 字段中，输入闪存文件系统的路径，或者点击 **Browse Flash** 在闪存文件系统中查找目录或文件。
6. 点击 **Upload Image**。上传过程可能需要数分钟。
7. 系统会提示您将此映像设置为 ASDM 映像。点击 **Yes**。
8. 系统将提醒您退出 ASDM 并保存配置。点击 **OK**。您会退出 **Upgrade** 工具。**注意：**在升级 ASA 软件*之后*，您将保存配置并重新加载 ASDM。
9. 重复 2. 到 8.，从 **Image to Upload** 下拉列表中选择 **ASA**。
10. 点击工具栏上的 **Save** 图标，保存配置更改。
11. 选择 **Monitoring > Failover > Failover Group #**（其中的 **#** 是您想要其移动到主设备的故障转移组的编号），然后点击 **Make Active**，从而使两个故障转移组在主设备上均处于活动状态。
12. 将 ASDM 连接到*辅助*设备，并根据 2. 到 9.，使用在主用设备上使用的相同位置上传 ASA 和 ASDM 软件。
13. 选择 **Tools > System Reload**，以便重新加载辅助 ASA。

    系统将显示新窗口，要求您确认重新加载的详细信息。

    a. 点击 **Save the running configuration at the time of reload** 单选按钮 （默认）。

    b. 选择重新加载的时间 （例如，默认值 **Now**）。

    c. 点击 **Schedule Reload**。

    重新加载开始后，系统将显示 **Reload Status** 窗口，指示正在执行重新加载。系统还提供了退出 ASDM 的选项。
14. 将 ASDM 连接至*主*设备，然后选择 **Monitoring > Failover > System**，检查辅助设备重新加载的时间。
15. 在辅助设备重新加载完成后，选择 **Monitoring > Properties > Failover > System**，然后点击 **Make Standby**，从而强行要求主设备故障转移至辅助设备。
16. 选择 **Tools > System Reload**，以便重新加载 （以前的）主用 ASA。

    系统将显示新窗口，要求您确认重新加载的详细信息。

    a. 点击 **Save the running configuration at the time of reload** 单选按钮 （默认）。

    b. 选择重新加载的时间 （例如，默认值 **Now**）。

    c. 点击 **Schedule Reload**。

重新加载开始后，系统将显示 **Reload Status** 窗口，指示正在执行重新加载。系统还提供了退出 ASDM 的选项。

如果故障转移组被配置为 Preempt Enabled，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。如果故障转移组未被配置为 Preempt Enabled，您可以使用 **Monitoring > Failover > Failover Group #** 窗格，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. 在主设备上启动 ASDM。
2. （如果要进行配置迁移）在 ASDM 中，使用 **Tools > Backup Configurations** 工具备份现有配置。
3. 在 ASDM 主应用窗口中，选择 **Tools > Upgrade Software from Local Computer**。

   系统将显示 **Upgrade Software from Local Computer** 对话框。
4. 点击 **All devices in the cluster** 单选按钮。

   系统将显示 **Upgrade Software** 对话框。
5. 从 **Image to Upload** 下拉列表中选择 **ASDM**。
6. 在 **Local File Path** 字段中，输入该文件在计算机上的本地路径，或者点击 **Browse Local Files** 在计算机上查找文件。
7. 在 **Flash File System Path** 字段中，输入闪存文件系统的路径，或者点击 **Browse Flash** 在闪存文件系统中查找目录或文件。
8. 点击 **Upload Image**。上传过程可能需要数分钟。
9. 系统会提示您将此映像设置为 ASDM 映像。点击 **Yes**。
10. 系统将提醒您退出 ASDM 并保存配置。点击 **OK**。您会退出 Upgrade 工具。**注意：**在升级 ASA 软件*之后*，您将保存配置并重新加载 ASDM。
11. 重复 3. 到 10.，从 **Image to Upload** 下拉列表中选择 **ASA**。
12. 点击工具栏上的 **Save** 图标，保存配置更改。
13. 选择 **Tools > System Reload**。

    系统将显示 System Reload 对话框。
14. 通过从 Device 下拉列表中选择从属设备名称，然后点击 **Schedule Reload** 立即重新加载该设备，从而加载每台从属设备 （一次重新加载一台）。

    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）。要查看设备重新加入集群的时间，请查看 **Monitoring > ASA Cluster > Cluster Summary** 窗格。
15. 在所有从属设备均已重新加载后，通过执行以下操作步骤在主设备上禁用集群：选择 **Configuration > Device Management > High Availability and Scalability > ASA Cluster**，取消选中 **Participate in ASA cluster** 复选框，然后点击 **Apply**。

    等待 5 分钟，以便系统选出新的主设备，并且流量变得稳定。当以前的主设备重新加入集群时，它将成为从属设备。

    请勿保存配置；当主设备重新加载时，您可能会想要在其上启用集群。

16. 通过选择 **Tools > System Reload**，并从 Device 下拉列表中选择 **--This Device--**，从而在 System Reload 对话框中重新加载主设备。
17. 退出并重新启动 ASDM；您将重新连接到新的主设备。

管理文件

ASDM 提供一组文件管理工具来帮助您执行基本文件管理任务。通过 File Management 工具可查看、移动、复制和删除存储在闪存中的文件，传输文件和管理远程存储设备 （装载点）上的文件。

备注　在多情景模式下，此工具仅适用于系统安全情景。

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

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　从 Configuration > Device Management > Management Access > File Access > FTP Client 窗格中，选中 **Specify FTP mode as passive** 复选框。

步骤 2　点击 **Apply**。

系统会更改 FTP 客户端配置并将更改保存到运行配置。

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 ASDM、Telnet 或 SSH 的 ASA 访问，第 34-4 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。如果您尚未进入系统配置模式，请在 Configuration > Device List 窗格中双击主用设备 IP 地址下的 **System**。

操作步骤

步骤 1　视情景模式而定：

- 对于单模式，依次选择 **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP)**。
- 对于系统中的多模式，依次选择 **Configuration > Device Management > Device Administration > Secure Copy**。

步骤 2　选中 **Enable secure copy server** 复选框。

步骤 3　（可选）ASA 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如果需要，可以在 ASA 数据库中手动添加或删除服务器及其密钥。

要添加密钥，请执行以下操作：

a. 点击 **Add**（对于新服务器），或者从 Trusted SSH Hosts 表中选择服务器，然后点击 **Edit**。

b. 对于新服务器，在 Host 字段中，输入服务器 IP 地址。

c. 选中 **Add public key for the trusted SSH host** 复选框。

d. 指定以下密钥之一：

  – Fingerprint - 输入已经过散列处理的密钥；例如，您从 **show** 命令输出复制的密钥。

  – Key - 输入 SSH 主机的公钥或经过散列处理的值。密钥字符串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。

要删除密钥，请执行以下操作：

a. 从 Trusted SSH Hosts 表中选择服务器，然后点击 **Delete**。

步骤 4　（可选）要在检测到新主机密钥时收到通知，请选中 **Inform me when a new host key is detected** 复选框。

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 5　点击 **Apply**。

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。

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　依次选择 **Configuration > Device Management > Management Access > File Access > TFTP Client**，然后选中 **Enable** 复选框。

步骤 2　从 Interface Name 下拉列表中，选择要用作 TFTP 客户端的接口。

步骤 3　在 IP Address 字段中，输入将保存配置文件的 TFTP 服务器的 IP 地址。

步骤 4　在 Path 字段中，输入将保存配置文件的 TFTP 服务器的路径。

例如：/tftpboot/asa/config3

步骤 5　点击 **Apply**。

相关主题

传输文件，第 35-12 页

添加装载点

您可以添加 CIFS 或 FTP 装载点。

- 添加 CIFS 装载点，第 35-10 页
- 添加 FTP 装载点，第 35-11 页

添加 CIFS 装载点

要定义通用互联网文件系统 (CIFS) 装载点，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Management Access > File Access > Mount-Points**，然后点击 **Add > CIFS Mount Point**。

系统将显示 Add CIFS Mount Point 对话框。

步骤 2　选中 **Enable mount point** 复选框。

此选项会将 ASA 上的 CIFS 文件系统附加到 UNIX 文件树。

步骤 3　在 Mount Point Name 字段中，输入现有 CIFS 位置的名称。

步骤 4　在 Server Name 或 IP Address 字段中，输入装载点所在服务器的名称或 IP 地址。

步骤 5　在 Share Name 字段中，输入 CIFS 服务器上的文件夹名称。

步骤 6　在 NT Domain Name 字段中，输入服务器所在 NT 域的名称。

步骤 7　在 User Name 字段中，输入已获授权可在服务器上装载文件系统的用户的名称。

步骤 8　在 Password 字段中，输入已获授权可在服务器上装载文件系统的用户的密码。

步骤 9　在 Confirm Password 字段中，重新输入密码。

步骤 10　点击 **OK**。

系统将关闭 Add CIFS Mount Point 对话框。

步骤 11　点击 **Apply**。

添加 FTP 装载点

对于 FTP 安装点， FTP 服务器必须采用 UNIX 目录列表样式。Microsoft FTP 服务器默认采用 MS-DOS 目录列表样式。

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Management Access > File Access > Mount-Points**，然后点击 **Add > FTP Mount Point**。

系统将显示 Add FTP Mount Point 对话框。

步骤 2　选中 **Enable** 复选框。

此选项会将 ASA 上的 FTP 文件系统附加到 UNIX 文件树。

步骤 3　在 Mount Point Name 字段中，输入现有 FTP 位置的名称。

步骤 4　在 Server Name 或 IP Address 字段中，输入装载点所在服务器的名称或 IP 地址。

步骤 5　在 Mode 字段中，点击 FTP 模式对应的单选按钮 （**Active** 或 **Passive**）。当选择 Passive 模式时，客户端会发起 FTP 控制连接和数据连接。服务器会使用其用于此连接的监听端口号进行响应。

步骤 6　在 Path to Mount 字段中，输入 FTP 文件服务器的目录路径名称。

步骤 7　在 User Name 字段中，输入已获授权可在服务器上装载文件系统的用户的名称。

步骤 8　在 Password 字段中，输入已获授权可在服务器上装载文件系统的用户的密码。

步骤 9　在 Confirm Password 字段中，重新输入密码。

步骤 10　点击 **OK**。

系统将关闭 Add FTP Mount Point 对话框。

步骤 11　点击 **Apply**。

访问文件管理工具

要使用文件管理工具，请执行以下步骤：

操作步骤

步骤 1　在 ASDM 主应用程序窗口中，依次选择 **Tools > File Management**。

系统将显示 File Management 对话框。

- Folders 窗格显示磁盘上的可用文件夹。
- Flash Space 显示闪存总量，以及可用的内存量。
- Files 区域显示选定文件夹中的文件的以下有关信息：
  - 路径
  - 文件名
  - Size (bytes)
  - Time Modified
  - Status，表明将所选文件指定为启动配置文件、启动映像文件、ASDM 映像文件、SVC 映像文件、 CSD 映像文件，还是 APCF 映像文件。

步骤 2　点击 **View** 以在浏览器中显示选定文件。

步骤 3　点击 **Cut** 以剪切选定文件，从而将其粘贴到其他目录。

步骤 4　点击 **Copy** 以复制选定文件，从而将其粘贴到其他目录。

步骤 5　点击 **Paste** 以将复制的文件粘贴到选定目标。

步骤 6　点击 **Delete** 以将从选定文件从闪存中删除。

步骤 7　点击 **Rename** 以重命名文件。

步骤 8　点击 **New Directory** 以创建用于存储文件的新目录。

步骤 9　点击 **File Transfer** 以打开 File Transfer 对话框。有关详细信息，请参阅传输文件，第 35-12 页。

步骤 10　点击 **Mount Points** 以打开 Manage Mount Points 对话框。有关详情，请参见添加装载点，第 35-10 页。

传输文件

通过 File Transfer 工具，可以传输来自本地或远程位置的文件。您可以将您计算机或闪存文件系统上的本地文件传输到 ASA，也可以从中传出文件。您可以使用 HTTP、HTTPS、TFTP、FTP 或 SMB 将远程文件传输到 ASA，也可以从中传出文件。

备注　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。

- 在本地 PC 和闪存之间传输文件，第 35-13 页
- 在远程服务器和闪存之间传输文件，第 35-13 页

在本地 PC 和闪存之间传输文件

要在您的本地计算机和闪存文件系统之间传输文件，请执行以下步骤。

操作步骤

步骤 1　在 ASDM 主应用程序窗口中，依次选择 **Tools > File Management**。

系统将显示 File Management 对话框。

步骤 2　点击 **File Transfer** 旁边的向下箭头，然后点击 **Between Local PC and Flash**。

系统将显示 File Transfer 对话框。

步骤 3　从您的本地计算机或闪存文件系统中，选择并*拖动*要上传或下载至所需位置的文件。或者，从您的本地计算机或闪存文件系统中，选择要上传或下载的文件，然后点击向右箭头或向左箭头，以便将文件传输到所需位置。

步骤 4　完成后点击 **Close**。

在远程服务器和闪存之间传输文件

要在远程服务器和闪存文件系统之间传输文件，请执行以下步骤。

操作步骤

步骤 1　在 ASDM 主应用程序窗口中，依次选择 **Tools > File Management**。

系统将显示 File Management 对话框。

步骤 2　点击 File Transfer 下拉列表中的向下箭头，然后点击 **Between Remote Server and Flash**。

系统将显示 File Transfer 对话框。

步骤 3　要从远程服务器传输文件，请点击 **Remote server** 选项。

步骤 4　定义要传输的源文件。

a. 选择文件所在位置的路径，包括服务器的 IP 地址。

注意　文件传输支持 IPv4 和 IPv6 地址。

b. 输入远程服务器的类型 （如果路径是 FTP）或端口号 （如果路径是 HTTP 或 HTTPS）。有效的 FTP 类型如下：

- ap - 被动模式下的 ASCII 文件
- an - 非被动模式下的 ASCII 文件
- ip - 被动模式下的二进制映像文件
- in - 非被动模式下的二进制映像文件

步骤 5　要从闪存文件系统传输文件，请点击 **Flash file system** 选项。

步骤 6　输入文件所在位置的路径，或者点击 **Browse Flash** 以查找文件位置。

步骤 7　此外，可以通过 CLI 从启动配置、运行配置或 SMB 文件系统中复制文件。有关使用 **copy** 命令的说明，请参阅 《CLI 配置指南》。

步骤 8　定义要传输的文件的目标位置。

a. 要将文件传输到闪存文件系统，请选择 **Flash file system** 选项。

b. 输入文件所在位置的路径，或者点击 **Browse Flash** 以查找文件位置。

步骤 9　要将文件传输到远程服务器，请选择 **Remote server** 选项。

a. 输入文件所在位置的路径。

b. 对于 FTP 传输，请输入类型。有效的类型如下：

- ap - 被动模式下的 ASCII 文件
- an - 非被动模式下的 ASCII 文件
- ip - 被动模式下的二进制映像文件
- in - 非被动模式下的二进制映像文件

步骤 10　点击 **Transfer** 以开始文件传输。

系统将显示 Enter Username and Password 对话框。

步骤 11　输入远程服务器的用户名、密码和域 （如果需要）。

步骤 12　点击 **OK** 以继续文件传输。

文件传输过程可能需要几分钟的时间；请确保等待其完成为止。

步骤 13　文件传输完成后，点击 **Close**。

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 ，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　依次选择 **Configuration > Device Management > System Image/Configuration > Boot Image/Configuration**。

您可以指定最多四个用作启动映像的本地二进制映像文件，以及一个位于 TFTP 服务器上用于设备从其启动的映像。如果指定位于 TFTP 服务器上的映像，则该映像必须是列表中的第一个映像。如果设备无法访问 TFTP 服务器以加载映像，则它会尝试加载位于闪存中的列表中的下一个映像文件。

步骤 2　点击 Boot Image/Configuration 窗格中的 **Add**。

步骤 3　浏览至要从其启动的映像。对于 TFTP 映像，请在 File Name 字段中输入 TFTP URL。点击 **OK**。

步骤 4　使用 Move Up 和 Move Down 按钮按顺序排放映像。

步骤 5　（可选）在 Boot Configuration File Path 字段中，通过点击 **Browse Flash** 并选择配置来指定启动配置文件。点击 **OK**。

步骤 6　在 ASDM Image File Path 字段中，通过点击 **Browse Flash** 并选择映像来指定 ASDM 映像。点击 **OK**。

步骤 7　点击 **Apply**。

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 35-15 页
- 使用 ROM 监控加载 ASASM 的映像，第 35-16 页
- 恢复并加载 ASA 5506W-X 无线接入点的映像，第 35-18 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 2-2 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

以下程序介绍如何将配置和映像备份至 zip 文件并将该文件传输到本地计算机。

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。
- ASA 必须处于单情景模式下。
- 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 18-8 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　在计算机上创建用于存储备份文件的文件夹，从而在今后需要恢复时，可以轻松找到这些文件。

步骤 2　依次选择 **Tools > Backup Configurations**。

系统将显示 Backup Configurations 对话框。点击 **SSL VPN Configuration** 区域中的向下箭头，以查看 SSL VPN 配置的备份选项。默认情况下，会选中并备份所有配置文件（如果可用）。如果要备份列表中的所有文件，请转至步骤 5。

步骤 3　如果要选择将备份的配置，请取消选中 **Backup All** 复选框。

步骤 4　选中要备份的选项旁边的复选框。

步骤 5　点击 **Browse Local** 以指定 .zip 备份文件的目录和文件名。

步骤 6　在 Select 对话框中，选择要在其中存储备份文件的目录。

步骤 7　点击 **Select**。在 Backup File 字段中将显示路径。

步骤 8　在目录路径后输入目标备份文件的名称。备份文件名的长度必须介于 3 到 232 个字符之间。

步骤 9　点击 **Backup**。除非备份的是证书或者 ASA 使用的是主口令，否则将立即进行备份。

步骤 10　如果您在 ASA 上配置并启用了主口令，而且您不知道该密码，则在继续备份之前，您会收到一条警告消息，建议您更改主口令。如果您知道主口令，请点击 **Yes** 以继续进行备份。除非备份的是身份证书，否则将立即进行备份。

步骤 11　如果备份的是身份证书，则系统会要求您输入一个单独的口令，该口令将用于对 PKCS12 格式的证书进行编码。您可以输入口令，也可以跳过此步骤。

注意　此过程会备份身份证书，但不会备份证书颁发机构证书。有关备份 CA 证书的说明，请参阅备份本地 CA 服务器，第 35-21 页。

- 要加密证书，请在 Certificate Passphrase 对话框中输入并确认您的证书口令，然后点击 **OK**。恢复证书时，您将需要记得在此对话框中输入的密码。
- 点击 **Cancel** 会跳过此步骤且不对证书进行备份。

点击 OK 或 Cancel 后，备份将会立即开始。

步骤 12　备份完成后，系统将会关闭状态窗口，并显示 Backup Statistics 对话框以提供成功或失败消息。

注意　备份 “失败消息”最有可能是由于缺少指定类型的现有配置所导致。

步骤 13　点击 **OK** 以关闭 Backup Statistics 对话框。

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　依次选择 **Tools > Restore Configurations**。

步骤 2　在 Restore Configurations 对话框中，点击 **Browse Local Directory**，在您的本地计算机上选择包含要恢复的配置的 zip 文件，然后点击 **Select**。路径和 zip 文件名会显示在 **Local File** 字段中。

必须通过依次选择 **Tools > Backup Configurations** 选项创建要恢复的 zip 文件。

步骤 3　点击 **Next**。系统将会显示第二个 Restore Configuration 对话框。选中要恢复的配置旁边的复选框。默认情况下，会选中所有可用的 SSL VPN 配置。

步骤 4　点击 **Restore**。

步骤 5　如果您在创建备份文件时指定了用于加密证书的证书口令，则 ASDM 会提示您输入该口令。

步骤 6　如果您选择恢复运行配置，系统会询问您是希望合并运行配置，替换运行配置，还是跳过恢复过程的这一部分。

- 合并配置会整合当前运行配置和已备份的运行配置。
- 替换运行配置仅使用已备份的运行配置。
- 跳过此步骤将不会恢复备份的运行配置。

ASDM 会显示状态对话框，直至恢复操作完成。

步骤 7　如果您替换或合并了运行配置，请关闭 ASDM，然后将其重新启动。如果未恢复运行配置，请刷新 ASDM 会话以使更改生效。

备份本地 CA 服务器

当执行 ASDM 备份时，备份不包括本地 CA 服务器数据库，因此不会备份存储在该服务器上的 CA 证书。如果要备份本地 CA 服务器，请将此手动过程与 ASA CLI 结合使用。

操作步骤

步骤 1　输入 **show run crypto ca server** 命令。

```
crypto ca server
 keysize server 2048
 subject-name-default OU=aa,O=Cisco,ST=ca,
 issuer-name CN=xxx,OU=yyy,O=Cisco,L=Bxb,St=Mass
 smtp from-address abcd@cisco.com
 publish-crl inside 80
 publish-crl outside 80
```

步骤 2　使用 **crypto ca import** 命令导入本地 CA PKCS12 文件，以创建 LOCAL-CA-SERVER 信任点并恢复密钥对。

```
crypto ca import LOCAL-CA-SERVER pkcs12 <passphrase> (paste the pkcs12
base64 data here)
```

注意　请务必在此步骤中使用确切的名称 “LOCAL-CA-SERVER”。

步骤 3　如果 LOCAL-CA-SERVER 目录不存在，则需要通过输入 **mkdirLOCAL-CA-SERVER** 来创建该目录。

步骤 4　将本地 CA 文件复制到 LOCAL-CA-SERVER 目录。

```
copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.ser
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.cdb
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.udb
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.crl
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.p12
disk0:/LOCAL-CA-SERVER/
```

步骤 5　输入 **crypto ca server** 命令，以启用本地 CA 服务器

```
crypto ca server
 no shutdown
```

步骤 6　输入 **show crypto ca server** 命令，以检查本地 CA 服务器是否正在正常运行。

步骤 7　保存配置。

将运行配置保存到 TFTP 服务器

此功能可在 TFTP 服务器上存储当前运行配置文件的副本。

操作步骤

步骤 1　依次选择 **File > Save Running Configuration to TFTP Server**。

系统将显示 Save Running Configuration to TFTP Server 对话框。

步骤 2　输入 TFTP 服务器的 IP 地址，以及将会在其中保存配置文件的文件路径，然后点击 **Save Configuration**。

注意　要配置默认 TFTP 设置，请依次选择 **Configuration > Device Management > Management Access > File Access > TFTP Client**。在配置此设置后，TFTP 服务器的 IP 地址和 TFTP 服务器上的文件路径会自动显示在此对话框中。

计划系统重新启动

通过 System Reload 工具可计划系统重新启动，或者取消挂起的重新启动。

操作步骤

步骤 1　选择 **Tools > System Reload**。

步骤 2　在 Reload Scheduling 区域中，定义以下设置：

a. 对于 Configuration State，请选择在重新启动时保存或放弃运行配置。

b. 对于 Reload Start Time，请从以下选项中进行选择：

- 点击 **Now** 以立即执行重新启动。
- 点击 **Delay by** 以将重新启动延迟指定的时长。以小时和分钟或仅以分钟为单位，输入开始重新启动之前的时间。
- 点击 **Schedule at** 以计划在特定的时间和日期进行重新启动。输入将要进行重新启动的时间，并选择计划的重新启动的日期。

c. 在 Reload Message 字段中，输入在重新启动时发送到打开的 ASDM 实例的消息。

d. 选中 **On reload failure force immediate reload after** 复选框，从而以小时和分钟或仅以分钟为单位，显示再次尝试重新启动之前的耗用时间。

e. 点击 **Schedule Reload** 以按配置来计划重新启动。

Reload Status 区域显示重新启动的状态。

步骤 3　选择如下选项之一：

- 点击 **Cancel Reload** 以停止计划的重新启动。
- 点击 **Refresh** 以在计划的重新启动完成后刷新 Reload Status 显示。
- 点击 **Details** 以显示计划的重新启动的结果。

降级软件

本节介绍如何降级。

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　依次选择 **Tools > Downgrade Software**。

系统将显示 Downgrade Software 对话框。

步骤 2　对于 ASA 映像，请点击 **Select Image File**。

系统将显示 Browse File Locations 对话框。

步骤 3　点击以下单选按钮之一：

- **Remote Server** - 从下拉列表中选择 **ftp**、 **smb** 或 **http**，然后键入旧映像文件的路径。
- **Flash File System** - 点击 **Browse Flash** 以选择本地闪存文件系统上的旧映像文件。

步骤 4　对于 Configuration，请点击 **Browse Flash** 以选择预迁移配置文件。（默认情况下，此配置文件保存在 disk0 上）。

步骤 5　（可选）在 Activation Key 字段中，输入旧的激活密钥 （如果您需要还原至 8.3 版本之前的激活密钥）。

有关详情，请参见关于激活密钥兼容性，第 35-23 页。

步骤 6　点击 **Downgrade**。

此工具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

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

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 ASA 配置是通过自动更新服务器进行更新，则不会通知 ASDM。您必须选择 **Refresh** 或依次选择 **File > Refresh ASDM with the Running Configuration on the Device** 以获取最新配置，在 ASDM 中进行的任何更改都将丢失。
- 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　依次选择 **Configuration > Device Management > System Image/Configuration > Auto Update**。

Auto Update 窗格包含 Auto Update Servers 表和两个区域：Timeout 区域和 Polling 区域。

通过 Auto Update Servers 表可查看以前配置的自动更新服务器的参数。ASA 会先轮询该表顶部列出的服务器。

步骤 2　要更改服务器在该表中的顺序，请点击 **Move Up** 或 **Move Down**。

Auto Update Servers 表包含以下列：

- Server - 自动更新服务器的名称或 IP 地址。
- User Name - 用于访问自动更新服务器的用户名。
- Interface - 向自动更新服务器发送请求时使用的接口。
- Verify Certificate - 指示 ASA 是否使用 CA 根证书检查自动更新服务器返回的证书。自动更新服务器和 ASA 必须使用相同的 CA。

步骤 3　双击 Auto Update Server 表中的任意行可以打开 Edit Auto Update Server 对话框，在其中可修改自动更新服务器参数。这些更改会立即反映在表中，但必须点击 **Apply** 才能将其保存到配置。

步骤 4　通过 Timeout 区域可设置 ASA 等待自动更新服务器超时的时长。Timeout 区域包含以下字段：

- Enable Timeout Period - 选中该字段会使 ASA 在未接收到来自自动更新服务器的响应时超时。
- Timeout Period (Minutes) - 输入在未收到来自自动更新服务器的响应时，ASA 在超时前将会等待的分钟数。

步骤 5　通过 Polling 区域可配置 ASA 将轮询来自自动更新服务器的信息的频率。Polling 区域包含以下字段：

- Polling Period (Minutes) - ASA 在轮询自动更新服务器以获取新信息前将会等待的分钟数。
- Poll on Specified Days - 允许您指定轮询计划。
- Set Polling Schedule - 显示 Set Polling Schedule 对话框，在其中可配置轮询自动更新服务器的日期和时间。
- Retry Period (minutes) - 在尝试轮询服务器失败时，ASA 在轮询自动更新服务器以获取新信息前将会等待的分钟数。
- Retry Count - ASA 将会尝试重试轮询自动更新服务器以获取新信息的次数。

步骤 6　设置轮询计划

通过 Set Polling Schedule 对话框可配置 ASA 轮询自动更新服务器的日期和时间。

Set Polling Schedule 对话框包含以下字段：

Days of the Week - 选中您希望 ASA 在每个星期的星期几轮询自动更新服务器。

通过 Daily Update 窗格组可配置您希望 ASA 轮询自动更新服务器的时间，该窗格组包含以下字段：

- Start Time - 输入开始自动更新轮询的小时和分钟。
- Enable randomization - 选中该字段以使 ASA 能够随机选择轮询自动更新服务器的时间。

监控自动更新

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。从终端会话运行 **debug** 命令。

```
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
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。

软件和配置的历史记录

表 35-1　　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。 修改了以下屏幕： Tools > File Management > File Transfer > Between Remote Server and Flash **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server**
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 修改了以下屏幕：Configuration > Device Management > System/Image Configuration > Auto Update > Add Auto Update Server。
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。 未修改任何 ASDM 屏幕。

表 35-1　　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。 未修改任何 ASDM 屏幕。
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。 未修改任何 ASDM 屏幕。

第 36 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

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 36-3 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 36-4 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 36-5 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 36-5 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　在 ASDM 中，依次选择 **Configuration > Device Management > Advanced > Embedded Event Manager**。

步骤 2　点击 **Add** 以显示 **Add Event Manager Applet** 对话框。

步骤 3　输入小程序的名称 （不能包含空格）并对其进行说明。说明最多可包含 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 4　在 **Events** 区域中点击 **Add**，以显示 **Add Event Manager Applet Event** 对话框。

步骤 5　从 **Type** 下拉列表中选择要配置的事件类型。可用选项为 **crashinfo**、**None**、**Syslog**、**Once-a-day timer**、 **One-shot timer** 和 **Periodic** 计时器。

- **Syslog**：输入一条或一系列系统日志消息。如果出现与指定的一条或一系列系统日志消息相匹配的系统日志消息，将会触发事件管理器小程序。 （可选）在 **occurrences** 字段中输入调用事件管理器小程序时系统日志消息必须已出现的次数。默认情况为每 0 秒出现 1 次。有效值为 1 到 4294967295。 （可选）在 **period** 字段中输入要调用操作而必须有系统日志消息出现的时间段 （以秒为单位）。此值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。
- **Periodic**：输入时间段 （以秒为单位）。时间范围可以是 1 到 604800 秒。
- **Once-a-day timer**：以 hh:mm:ss 为格式输入时间。时间范围为 00:00:00（午夜）到 23:59:59。
- **One-shot timer**：输入时间段 （以秒为单位）。时间范围可以是 1 到 604800 秒。
- **None**：选择此选项可手动调用事件管理器小程序。
- **crashinfo**：选择此选项可在 ASA 崩溃时调用崩溃事件。

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　点击 **Add** 以显示 **Add Event Manager Applet** 对话框。

步骤 2　输入小程序的名称 （不能包含空格）并对其进行说明。说明最多可包含 256 个字符。

步骤 3　在 **Actions** 区域中点击 **Add**，以显示 **Add Event Manager Applet Action** 对话框。

步骤 4　在 **Sequence #** 字段中输入唯一的序列号。有效序列号的范围为 0 到 4294967295。

步骤 5　在 **CLI Command** 字段中输入 CLI 命令。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。

步骤 6　点击 **OK** 以关闭 **Add Event Manager Applet Action** 对话框。

新添加的操作将显示在 **Actions** 列表中。

步骤 7　点击 **Add** 以打开 **Add Event Manager Applet** 对话框。

步骤 8　选择一个可用的输出目标选项：

- 从 **Output Location** 下拉列表中选择 **None** 选项，以丢弃 **action** 命令的任何输出。这是默认设置。
- 从 **Output Location** 下拉列表中选择 **Console** 选项，以将 **action** 命令的输出发送到控制台。

注意　运行此命令会影响性能。

- 从 **Output Location** 下拉列表中选择 **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。**Create a unique file** 选项自动选择为默认设置。

  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。
- 从 **Output Location** 下拉列表中选择 **File** 选项，然后从下拉列表中选择 **Create a set of files** 选项，以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。最新的文件以 0 表示，最旧的文件以最高编号表示。轮换值的有效值范围为 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。
- 从 **Output Location** 下拉列表中选择 **File** 选项，然后从下拉列表中选择 **Create/overwrite a file** 选项，以将 **action** 命令输出写入到一个文件中，每次写入时都会覆盖原有文件。
- 从 **Output Location** 下拉列表中选择 **File** 选项，然后从下拉列表中选择 **Create/append a file** 选项，以将 **action** 命令输出写入到一个文件，每次写入时都会附加到原有文件。

步骤 9　点击 **OK** 以关闭 **Add Event Manager Applet** 对话框。

指定的输出目标将显示在 **Embedded Event Manager** 窗格中。

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　在 **Embedded Event Manager** 窗格中，从使用 **None** 事件配置的列表中选择事件管理器小程序。

步骤 2　点击 **Run**。

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　依次选择 **Configuration > Device Management > Advanced > Embedded Event Manager**。

步骤 2　点击 **Add** 以显示 **Add Event Manager Applet** 对话框。

步骤 3　再次点击 **Add** 以显示 **Add Event Manager Applet Event** 对话框。

步骤 4　从下拉列表中选择 **memory-logging-wrap**。

步骤 5　点击 **OK** 以将其添加到 **Events** 列表。

步骤 6　再次点击 **OK** 以将其添加到 **Applets** 列表。

监控 EEM

您可使用以下屏幕监控 EEM。

- **Monitoring > Properties > EEM Applets**

  此窗格显示 EEM 小程序列表及其命中次数值。
- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

EEM 历史记录

表 36-1　　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。 引入了以下屏幕：Configuration > Device Management > Advanced > Embedded Event Manager、 Monitoring > Properties > EEM Applets。
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。 修改了以下屏幕：Configuration > Device Management > Advanced > Embedded Event Manager > Add Event Manager Applet > Add Event Manager Applet Event。

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。

使用 Packet Capture Wizard 配置和运行捕获

您可以使用 Packet Capture Wizard 配置和运行捕获以对错误进行故障排除。捕获可以使用 ACL 来限制捕获的流量类型、源地址和目标地址与端口，以及一个或多个接口。该向导在每个入口接口和出口接口上运行一个捕获。您可以在 PC 上保存捕获以在数据包分析器中对它们进行检查。

备注 此工具不支持无客户端 SSL VPN 捕获。

要配置和运行捕获，请执行以下步骤：

操作步骤

步骤 1 依次选择 **Wizards > Packet Capture Wizard**。

系统将显示 **Overview of Packet Capture** 屏幕，其中列出向导将指导您完成的任务。这些任务包括：

- 选择入口接口。
- 选择出口接口。
- 设置缓冲区参数。
- 运行捕获。
- 将捕获保存到 PC （可选）。

步骤 2 点击 **Next**。

在集群环境中，系统将显示 **Cluster Option** 屏幕。转至步骤 3。

在非集群环境中，系统将显示 **Ingress Traffic Selector** 屏幕。转至步骤 4。

步骤 3　在运行捕获的 **Cluster Option** 屏幕中选择以下一个选项：**This device only** 或 **The whole cluster**，然后点击 **Next** 以显示 **Ingress Selector** 屏幕。

步骤 4　点击 **Select Interface** 单选按钮以捕获接口上的数据包。点击 **Use backplane channel** 单选按钮以捕获 ASA CX 数据层面上的数据包。

步骤 5　在 **Packet Match Criteria** 区域执行以下其中一项操作：

- 点击 **Specify access-list** 单选按钮以指定用于匹配数据包的 ACL，然后从 **Select ACL** 下拉列表中选择 ACL。点击 **Manage** 以显示 **ACL Manager** 窗格，以便将之前配置的 ACL 添加到当前下拉列表中。选择一个 ACL，然后点击 **OK**。
- 点击 **Specify Packet Parameters** 单选按钮以指定数据包参数。

步骤 6　要继续，请参阅入口流量选择器，第 37-3 页。

步骤 7　点击 **Next** 以显示 **Egress Traffic Selector** 屏幕。要继续，请参阅出口流量选择器，第 37-3 页。

注意　源端口服务、目标端口服务和 ICMP 类型是只读的且基于您在 **Ingress Traffic Selector** 屏幕中所做的选择。

步骤 8　点击 **Next** 以显示 **Buffers & Captures** 屏幕。要继续，请参阅缓冲区，第 37-4 页。

步骤 9　在 **Capture Parameters** 区域选中 **Get capture every 10 seconds** 复选框以便每隔 10 秒钟自动获取最新捕获。默认情况下，此捕获使用循环缓冲区。

步骤 10　您可在 **Buffer Parameters** 区域指定缓冲区大小和数据包大小。缓冲区大小是捕获可用于存储数据包的最大内存量。数据包大小是捕获可以容纳的最长数据包。我们建议您使用最长的数据包大小以捕获尽可能多的信息。

a. 输入数据包大小。有效的大小范围为 14 - 1522 个字节。
b. 输入缓冲区大小。有效的大小范围为 1534 - 33554432 个字节。
c. 选中 **Use circular buffer** 复选框以存储捕获的数据包。

注意　选择此设置时，如果所有缓冲存储空间都已占用，则捕获将开始覆盖最旧的数据包。

步骤 11　点击 **Next** 以显示 **Summary** 屏幕，该屏幕将显示集群中所有设备的集群选项 （如果使用的是集群）、流量选择器和已输入的缓冲区参数。要继续，请参阅汇总，第 37-4 页。

步骤 12　点击 **Next** 以显示 **Run Captures** 屏幕，然后点击 **Start** 以开始捕获数据包。点击 **Stop** 以结束捕获。要继续，请参阅运行捕获，第 37-4 页。如果使用的是集群，请转至第 14 步。

步骤 13　点击 **Get Capture Buffer** 以确定剩余的缓冲区空间。点击 **Clear Buffer on Device** 以删除当前内容并在缓冲区中腾出空间以捕获更多数据包。

步骤 14　在集群环境中，在 **Run Captures** 屏幕上执行以下一个或多个步骤：

- 点击 **Get Cluster Capture Summary** 以查看集群中所有设备的数据包捕获信息汇总，其后显示每台设备的数据包捕获信息。
- 点击 **Get Capture Buffer** 以确定集群的每台设备中剩余的缓冲区空间。系统将显示 **Capture Buffer from Device** 对话框。
- 点击 **Clear Capture Buffer** 以删除集群中一个或所有设备的当前内容并在缓冲区中腾出空间以捕获更多数据包。

步骤 15　点击 **Save captures** 以显示 **Save Capture** 对话框。您可以选择保存入口捕获、出口捕获，或同时保存两者。要继续，请参阅保存捕获，第 37-5 页。

步骤 16　点击 **Save Ingress Capture** 以显示 **Save capture file** 对话框。指定 PC 上的存储位置，然后点击 **Save**。

步骤 17　点击 **Launch Network Sniffer Application** 以启动在 **Tools > Preferences** 中指定的数据包分析应用，以便分析入口捕获。

步骤 18　点击 **Save Egress Capture** 以显示 **Save capture file** 对话框。指定 PC 上的存储位置，然后点击 **Save**。

步骤 19　点击 **Launch Network Sniffer Application** 以启动在 **Tools > Preferences** 中指定的数据包分析应用，以便分析出口捕获。

步骤 20　点击 **Close**，然后点击 **Finish** 以退出向导。

入口流量选择器

要配置入口接口、源和目标主机或网络，以及数据包捕获协议，请执行以下步骤：

操作步骤

步骤 1　从下拉列表中选择入口接口名称。

步骤 2　输入入口源主机和网络。点击 **Use backplane channel** 单选按钮以捕获 ASA CX 数据层面上的数据包。

步骤 3　输入入口目标主机和网络。

步骤 4　输入要捕获的协议类型。可用的协议包括：ah、 eigrp、 esp、 gre、 icmp、 icmp6、 igmp、 igrp、 ip、 ipinip、 nos、 ospf、 pcp、 pim、 snp、 tcp 或 udp。

a. 仅为 ICMP 输入 ICMP 类型。可用的类型包括：all、 alternate address、 conversion-error、 echo、 echo-reply、 information-reply、 information-request、 mask-reply、 mask-request、 mobile-redirect、 parameter-problem、 redirect、 router-advertisement、 router-solicitation、 source-quench、 time-exceeded、 timestamp-reply、 timestamp-request、 traceroute 或 unreachable。

b. 仅为 TCP 和 UDP 协议指定源和目标端口服务。可用的选项包括：

- 选择 **All Services** 以包含所有服务。
- 选择 **Service Groups** 以包含服务组。

  要包含特定服务，请选择以下其中一项：aol、 bgp、 chargen、 cifx、 citrix-ica、 ctiqbe、 daytime、 discard、 domain、 echo、 exec、 finger、 ftp、 ftp-data、 gopher、 h323、 hostname、 http、 https、 ident、 imap4、 irc、 kerberos、 klogin、 kshell、 ldap、 ldaps、 login、 lotusnotes、 lpd、 netbios-ssn、 nntp、 pcanywhere-data、 pim-auto-rp、 pop2、 pop3、 pptp、 rsh、 rtsp、 sip、 smtp、 sqlnet、 ssh、 sunrpc、 tacacs、 talk、 telnet、 uucp 或 whois。

步骤 5　在 **Security Group Tagging** 区域选中 **SGT number** 复选框并输入安全组标签编号以为思科 TrustSec 服务启用数据包捕获。有效的安全组标签编号范围为 2-65519。

出口流量选择器

要配置出口接口、源和目标主机/网络，以及数据包捕获的源和目标端口服务，请执行以下步骤：

操作步骤

步骤 1　点击 **Select Interface** 单选按钮以捕获接口上的数据包。点击 **Use backplane channel** 单选按钮以捕获 ASA CX 数据层面上的数据包。

步骤 2　从下拉列表中选择出口接口名称。

步骤 3　输入出口源主机和网络。

步骤 4　输入出口目标主机和网络。

在入口配置时选择的协议类型已列出。

缓冲区

要配置数据包大小、缓冲区大小，以及在数据包捕获中使用循环缓冲区，请执行以下步骤：

操作步骤

步骤 1　输入捕获可以容纳的最长数据包。使用可用的最长数据包以捕获尽可能多的信息。

步骤 2　输入捕获可用于存储数据包的最大内存量。

步骤 3　使用循环缓冲区来存储数据包。当循环缓冲区已使用所有缓冲存储空间时，捕获将先覆盖最旧的数据包。

汇总

Summary 屏幕显示了集群选项 （如果使用的是集群）、流量选择器，以及在之前的向导屏幕中选择的数据包捕获的缓冲区参数。

运行捕获

要启动和停止捕获会话、查看捕获缓冲区、启动网络分析器应用、保存数据包捕获和清除缓冲区，请执行以下步骤：

操作步骤

步骤 1　点击 **Start** 以启动选定接口上的数据包捕获会话。

步骤 2　点击 **Stop** 以停止选定接口上的数据包捕获会话。

步骤 3　点击 **Get Capture Buffer** 以获取接口上的捕获数据包快照。

步骤 4　点击 **Ingress** 以显示入口接口上的捕获缓冲区。

步骤 5　点击 **Egress** 以显示出口接口上的捕获缓冲区。

步骤 6　点击 **Clear Buffer on Device** 以清除设备上的缓冲区。

步骤 7　点击 **Launch Network Sniffer Application** 以启动数据包分析应用，以便分析在 **Tools > Preferences** 中指定的入口捕获或出口捕获。

步骤 8　点击 **Save Captures** 以使用 ASCII 或 PCAP 格式保存入口和出口捕获。

保存捕获

要将入口和出口数据包捕获保存到 ASCII 或 PCAP 文件格式以进行进一步的数据包分析，请执行以下步骤：

操作步骤

步骤 1　点击 **ASCII** 以使用 ASCII 格式保存捕获缓冲区。

步骤 2　点击 **PCAP** 以使用 PCAP 格式保存捕获缓冲区。

步骤 3　点击 **Save ingress capture** 以指定要在其中保存入口数据包捕获的文件。

步骤 4　点击 **Save egress capture** 以指定要在其中保存出口数据包捕获的文件。

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 37-7 页
- 跟踪主机路由，第 37-11 页
- 跟踪数据包以测试策略配置，第 37-12 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

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包含允许用于回送消息和回送回复消息的任意地址的规则。在 **Configuration > Device Management > Management Access > ICMP** 页面配置 ICMP 规则。

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。

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。

在 **Configuration > Firewall > Access Rules** 页面配置访问规则。如果仅为测试目的添加规则，则可以在完成测试后删除所添加的规则。

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。

a. 依次选择 **Configuration > Firewall > Service Policy Rules**。

b. 编辑 **inspection_default** 全局规则。

c. 在 **Rule Actions > Protocol Inspection** 选项卡上，选择 ICMP。

d. 点击 **OK**，然后点击 **Apply**。

Ping 主机

要 ping 任何设备，只需依次选择 **Tools > Ping**，然后输入要 ping 的目标的 IP 地址或主机名，然后点击 **Ping**。对于 TCP ping，应选择 **TCP**，并且还应包含目标端口。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 - 您可以选择借以连接目标主机的接口。如果不选择接口，系统会使用路由表确定正确的接口。您可以 ping IPv4 或 IPv6 地址或主机名。
- TCP ping - 您还必须为要 ping 的目标选择 TCP 端口。例如，选择 **www.example.com 80** 来 ping HTTP 端口。您可以 ping IPv4 地址或主机名，但是不可以 ping IPv6 地址。

  您还可以选择指定发送 ping 的源地址和端口。在这种情况下，可以选择源借以发送 ping 的接口 （如果不选择接口，系统将使用路由表）。

  最后，您可以指定重复 ping 的频率 （默认值为 5 次）或每次尝试的超时时间 （默认值为 2 秒）。

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。

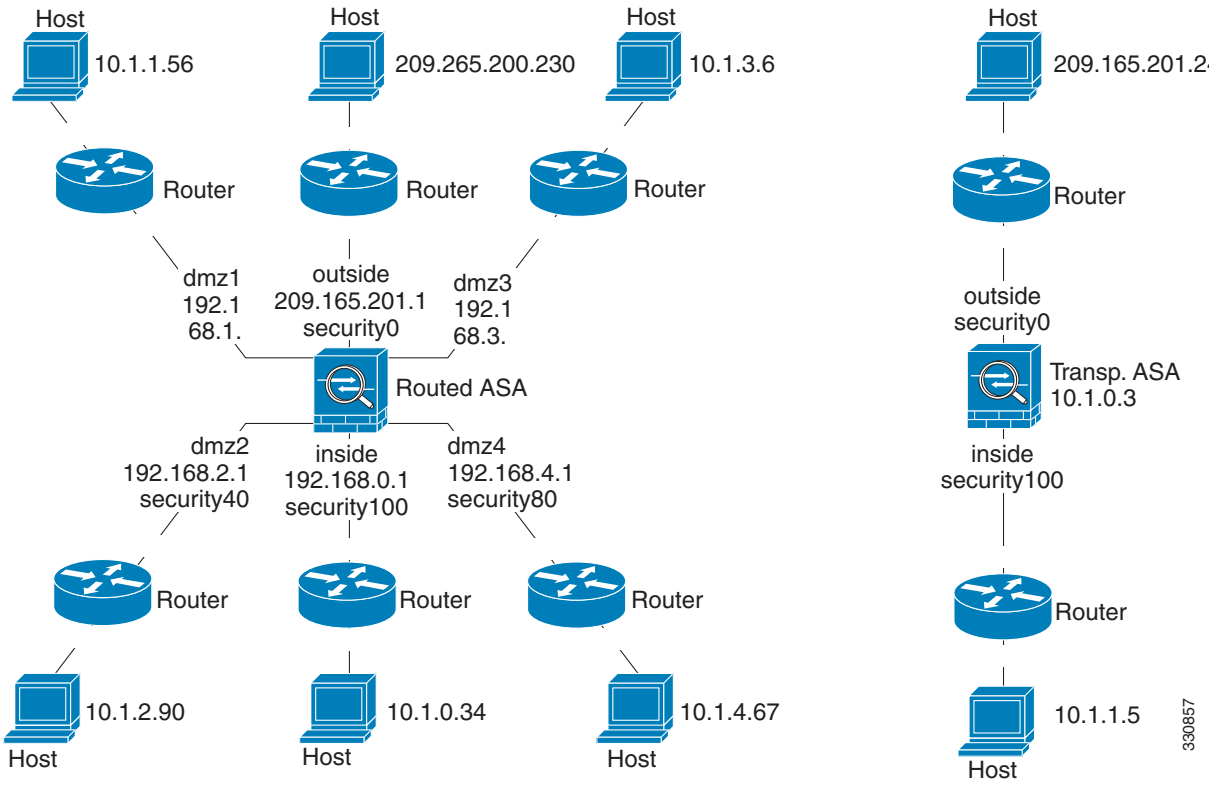
准备工作

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**）。

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。

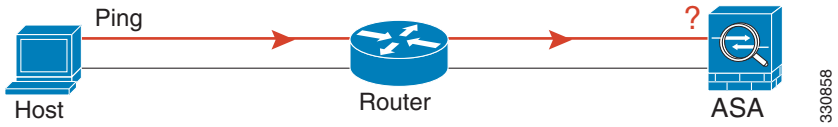
图 37-1　　接口、路由器和主机的网络图



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。

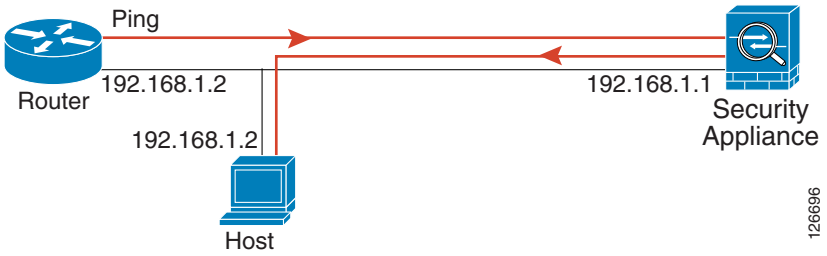
如果 ASA 接口处于非活动状态、接口配置不正确，或 ASA 与路由器之间的交换机关闭 （参阅下图）， ping 操作可能会失败。在这种情况下，数据包不能到达 ASA，因此调试消息或系统日志消息不会显示。

图 37-2　　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 37-3　　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 37-4　　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 37-5　　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 37-11 页。

步骤 2　确定数据包路由，第 37-12 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　使用服务策略减小 TTL。

a. 依次选择 **Configuration > Firewall > Service Policy Rules**。

b. 添加或编辑规则。例如，如果您已具有可以添加减小 TTL 的选项的规则，则不需要创建新规则。

c. 通过向导前进至 Rule Actions 页面，将规则应用于全局或某个接口，并指定流量匹配。例如，您可以创建全局匹配 any 规则。

d. 在 Rule Actions 页面上，点击 **Connection Settings** 选项卡，然后选择 **Decrement time to live for a connection**。

e. 点击 **OK** 或 **Finish**，然后点击 **Apply**。

步骤 2　增加 ICMP 不可达消息的速率限制。

a. 依次选择 **Configuration > Device Management > Management Access > ICMP**。

b. 在页面底部增加 **IPv4 ICMP Unreachable Message Limits > Rate Limit** 值。例如，将此值增至 50。

c. 点击 **Apply**。

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　依次选择 **Tools > Traceroute**。

步骤 2　输入您跟踪路由的目标主机名或 IP 地址。将 DNS 服务器配置为使用主机名。

步骤 3　（可选）配置跟踪的特征。在大多数情况下默认值都适用。

- **Timeout** - 超时之前等待响应的时间。默认值为 3 秒。
- **Port** - 要使用的 UDP 端口。默认值为 33434。
- **Probe** - 在每个 TTL 级别发送多少探测。默认值为 3。
- **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。
- **Specify source interface or IP address** - 要用作跟踪源的接口。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。
- **Reverse Resolve** - 指定如果配置了 DNS 名称解析，是否要求输出显示所遇到的跃点的名称。取消选择此选项将仅显示 IP 地址。
- **Use ICMP** - 是否发送 ICMP 探测数据包，而不发送 UDP 探测数据包。

步骤 4　点击 **Trace Route** 开始跟踪路由。

Traceroute Output 区域会显示有关跟踪路由结果的详细信息。

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　依次选择 **Tools > Packet Tracer**。

步骤 2　选择数据包跟踪的源接口。

步骤 3　指定用于数据包跟踪的协议类型。可用的协议类型包括 ICMP、 IP、 TCP 和 UDP。

步骤 4　（可选。）如果要跟踪将安全组标签值嵌入第 2 层 CMD 报头 (Trustse) 的数据包，请选中 **SGT number**，然后输入安全组标签编号 0-65533。

步骤 5　为数据包指定源和目标。

如果您使用思科 Trustsec，则可以指定 IPv4 或 IPv6 地址、完全限定域名 (FQDN) 或安全组名称或标签。对于源地址，您还可以指定 Domain\username 格式的用户名。

步骤 6　指定协议特征：

- ICMP - 输入 ICMP 类型、 ICMP 代码 (0-255)，并且可以选择键入 ICMP 标识符。
- TCP/UDP - 输入源和目标端口号。
- Raw IP - 输入协议编号， 0-255。

步骤 7　点击 **Start** 开始跟踪数据包。

Information Display 区域会显示数据包跟踪结果的详细消息。

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。

监控性能

您可以用图形或表格的形式查看 ASA 性能信息。

操作步骤

步骤 1　依次选择 **Monitoring > Properties > Connection Graphs > Perfmon**。

步骤 2　您可以在 **Graph Window Title** 中为图形窗口输入标题，也可以选择现有标题。

步骤 3　从 Available Graphs 列表中选择最多四个条目，然后点击 **Add** 将其移至 Selected Graphs 列表。可用的选项如下：

- AAA Perfmon - 身份验证、授权和记帐请求的每秒请求数。
- Inspection Perfmon - HTTP、 FTP 和 TCP 检测的每秒数据包数。
- Web Perfmon - URL 访问和 URL 服务器请求的每秒请求数。
- Connections Perfmon - 所有连接、 UDP 连接、 TCP 连接和 TCP 拦截的每秒连接数。
- Xlate Perfmon - 每秒 NAT 转换数。

步骤 4　点击 **Show Graphs**。

您可以在图形视图与表视图之间切换每个图表。您也可以更改数据刷新的频率以及导出或打印数据。

监控内存块

您可以用图形或表格的形式查看可用和已用内存块信息。

操作步骤

步骤 1　依次选择 **Monitoring > Properties > System Resources Graphs > Blocks**。

步骤 2　您可以在 **Graph Window Title** 中为图形窗口输入标题，也可以选择现有标题。

步骤 3　从 Available Graphs 列表中选择相应条目，然后点击 **Add** 将其移至 Selected Graphs 列表。可用的选项如下：

- Blocks Used - 显示 ASA 的已用内存块。
- Blocks Free - 显示 ASA 的可用内存块。

步骤 4　点击 **Show Graphs**。

您可以在图形视图与表视图之间切换每个图表。您也可以更改数据刷新的频率以及导出或打印数据。

监控 CPU

您可以查看 CPU 利用率。

操作步骤

步骤 1　依次选择 **Monitoring > Properties > System Resources Graphs > CPU**。

步骤 2　您可以在 **Graph Window Title** 中为图形窗口输入标题，也可以选择现有标题。

步骤 3　将 CPU Utilization 添加到 Selected Graphs 列表。

步骤 4　点击 **Show Graphs**。

您可以在图形视图与表视图之间切换图表。您也可以更改数据刷新的频率以及导出或打印数据。

监控内存

您可以用图形或表格的形式查看内存利用率信息。

操作步骤

步骤 1　依次选择 **Monitoring > Properties > System Resources Graphs > Memory**。

步骤 2　您可以在 **Graph Window Title** 中为图形窗口输入标题，也可以选择现有标题。

步骤 3　从 Available Graphs 列表中选择相应条目，然后点击 **Add** 将其移至 Selected Graphs 列表。可用的选项如下：

- Free Memory - 显示 ASA 的可用内存。
- Used Memory - 显示 ASA 的已用内存。

步骤 4　点击 **Show Graphs**。

您可以在图形视图与表视图之间切换每个图表。您也可以更改数据刷新的频率以及导出或打印数据。

监控每个进程的 CPU 使用率

您可以监控 CPU 上运行的进程。您可以获得某个进程的 CPU 使用百分比信息。CPU 使用率统计信息以降序排序显示，占比最高的进程排在顶部。其中也包括有关每个进程的 CPU 负载信息，显示日志时间之前 5 秒、 1 分钟和 5 分钟的数据。此信息每 5 秒自动更新一次，提供实时的统计信息。在 ASDM 中，统计信息每 30 秒更新一次。

要查看每个进程的 CPU 使用率，请依次选择 **Monitoring > Properties > Per-Process CPU Usage**。

您可以停止自动刷新、手动刷新信息，或将其保存到某个文件中。您还可以点击 **Configure CPU Usage Colors** 按钮，根据使用率百分比选择背景和前景颜色，以更方便地扫描高使用率进程。

监控连接

要以表格的形式查看当前连接，请在 ASDM 主窗口中依次选择 **Monitoring > Properties > Connections**。每个连接的信息包括协议、源和目标地址特征、最后一次发送或接收数据包后的空闲时间，以及连接中的流量数量。

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

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 38-1　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。

对日志查看器中的消息进行排序

您可以对 ASDM 日志查看器 （即 Real-Time Log Viewer、 Log Buffer Viewer 和 Latest ASDM Syslog Events Viewer）中的所有消息进行排序。要按多列对表进行排序，请点击要按其排序的第一列的标题，然后按住 **Ctrl** 键，同时点击要包含在排序顺序中的其他列的标题。要按时间顺序对消息进行排序，请同时选中日期和时间列；否则，消息仅按日期 （无论时间）或仅按时间 （无论日期）排序。

在 Real-Time Log Viewer 和 Latest ASDM Syslog Events Viewer 中对消息进行排序时，传入的新消息按照已排序的顺序显示，而不是显示在顶部。也就是说，它们会与其他消息混合。

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。

备注　要监控来自集群中的设备的系统日志消息，必须打开要监控的每台设备的 ASDM 会话。

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，请在 **Syslog Server** 窗格中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 38-6 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 38-6 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　在 ASDM 中，依次选择以下其中一项：

- **Home > Latest ASDM Syslog Messages > Enable Logging**
- **Configuration > Device Management > Logging > Logging Setup**
- **Monitoring > Real-Time Log Viewer > Enable Logging**
- **Monitoring > Log Buffer > Enable Logging**

步骤 2　选中 **Enable logging** 复选框以开启日志记录。

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　依次选择 **Configuration > Device Management > Logging > Logging Setup**。

步骤 2　选中 **Enable logging** 复选框为 ASA 开启日志记录。

步骤 3　选中 **Enable logging on the failover standby unit** 复选框为备用 ASA 开启日志记录（如果适用）。

步骤 4　选中 **Send debug messages as syslogs** 复选框以将所有调试跟踪输出重定向到系统日志。如果启用了此选项，则在控制台上不显示系统日志消息。因此，要查看调试消息，必须在控制台上启用日志记录并将其配置为调试系统日志消息号和严重性级别的目标。要使用的系统日志消息号为 **711001**。此系统日志消息的默认严重性级别为调试。

步骤 5　选中 **Send syslogs in EMBLEM format** 复选框以启用 EMBLEM 格式，以便将其用于所有日志记录目标 （系统日志服务器除外）。

步骤 6　指定在启用了日志记录缓冲区的情况下将系统日志消息保存到的内部日志缓冲区的大小。当缓冲区已满时，除非将日志保存到 FTP 服务器或内部闪存，否则会覆盖消息。默认缓冲区大小为 4096 字节。范围为 4096 到 1048576。

步骤 7　要在覆盖缓冲区内容之前将其保存到 FTP 服务器，请选中 **Save Buffer To FTP Server** 复选框。要允许覆盖缓冲区内容，请取消选中此复选框。

步骤 8　点击 **Configure FTP Settings** 以确定 FTP 服务器并配置用于保存缓冲区内容的 FTP 参数。

步骤 9　选中 **Save Buffer To Flash** 复选框在覆盖缓冲区内容之前将其保存到内部闪存。

注意　此选项仅可用于路由模式或透明单模式。

步骤 10　点击 **Configure Flash Usage** 以指定在用于日志记录的内部闪存中要使用的最大空间和要保留的最小可用空间 （以 KB 为单位）。启用此选项将在存储消息的设备磁盘上创建一个名为 “syslog” 的目录。

注意　此选项仅可用于单一路由模式或透明模式。

步骤 11　指定要在 ASA 或 ASASM 中查看的系统日志的队列大小。

配置 FTP 设置

要指定用于保存日志缓冲区内容的 FTP 服务器的配置，请执行以下步骤：

操作步骤

步骤 1　选中 **Enable FTP client** 复选框以启用 FTP 客户端的配置。

步骤 2　指定 FTP 服务器的 IP 地址。

步骤 3　指定用于存储已保存日志缓冲区内容的 FTP 服务器的目录路径。

步骤 4　指定用于登录到 FTP 服务器的用户名。

步骤 5　指定与用于登录到 FTP 服务器的用户名相关联的密码。

步骤 6　确认密码，然后点击 **OK**。

配置日志记录闪存使用情况

要指定将日志缓冲区内容保存到内部闪存的限制，请执行以下步骤：

操作步骤

步骤 1　指定可用于日志记录的最大内部闪存量 （以 KB 为单位）。

步骤 2　指定保留的内部闪存量 （以 KB 为单位）。当内部闪存接近该限制时，不再保存新日志。

步骤 3　点击 **OK** 以关闭 **Configure Logging Flash Usage** 对话框。

配置系统日志消息传递

要配置系统日志消息传递，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Logging > Syslog Setup**。

步骤 2　为系统日志服务器选择要用作文件消息基础的系统日志设备。默认为大多数 UNIX 系统期望的 LOCAL(4)20。但是，由于网络设备共享八台可用设备，您可能需要为系统日志更改这个值。

步骤 3　选中 **Include timestamp in syslogs** 复选框在发送的各系统日志消息中添加日期和时间。

步骤 4　选择要在 **Syslog ID** 表中显示的信息。可用选项如下：

- 选择 **Show all syslog IDs** 以指定 **Syslog ID** 表应显示整个系统日志消息 ID 列表。
- 选择 **Show disabled syslog IDs** 以指定 **Syslog ID** 表应仅显示已显式禁用的系统日志消息 ID。
- 选择 **Show syslog IDs with changed logging** 以指定 **Syslog ID** 表应仅显示严重性级别默认值已更改的系统日志消息 ID。
- 选择 **Show syslog IDs that are disabled or with a changed logging level** 以指定 **Syslog ID** 表应仅显示严重性级别已修改的系统日志消息 ID 和已显式禁用的系统日志消息 ID。

步骤 5　**Syslog ID Setup Table** 根据 Syslog ID Setup Table 中的设置显示系统日志消息列表。选择要修改的单条消息或消息 ID 范围。可以禁用所选消息 ID 或修改其严重性级别。要选择列表中的多个消息 ID，请点击范围中的第一个 ID，然后按住 Shift 键并点击范围中的最后一个 ID。

步骤 6　点击 **Advanced** 以将系统日志消息配置为包含设备 ID。

编辑系统日志 ID 设置

要更改系统日志消息设置，请执行以下步骤：

备注　**Syslog ID** 字段仅用于显示。此区域中显示的值由在位于 **Syslog Setup** 窗格中的 **Syslog ID** 表内的条目确定。

操作步骤

步骤 1　选中 **Disable Message(s)** 复选框以禁用 **Syslog ID** 列表中显示的系统日志消息 ID 的消息。

步骤 2　选择要为 **Syslog ID** 列表中显示的系统日志消息 ID 发送的消息的日志记录严重性级别。严重性级别定义如下：

- Emergency （级别 0，系统不可用）

  注意　不建议使用严重性级别 0。

- Alert （级别 1，需要立即采取措施）
- Critical （级别 2，严重情况）
- Error （级别 3，错误情况）
- Warning （级别 4，警告情况）
- Notification （级别 5，正常但重大的情况）
- Informational （级别 6，消息仅供参考）
- Debugging （级别 7，消息仅供调试）

步骤 3　点击 **OK** 以关闭 **Edit Syslog ID Settings** 对话框。

在非 EMBLEM 格式化系统日志消息中包含设备 ID

要在非 EMBLEM 格式化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　选中 **Enable syslog device ID** 复选框以指定应在所有非 EMBLEM 格式化系统日志消息中包含的设备 ID。

步骤 2　要指定使用哪一项作为设备 ID，请选择以下其中一个选项：

- ASA 的主机名
- 接口 IP 地址

  从下拉列表中选择与所选 IP 地址对应的接口名称。

  如果正在使用集群，请选中 **In an ASA cluster, always use master’ s IP address for the selected interface** 复选框。

- 字符串

  指定用户定义的字母数字字符串。

- ASA 集群名称

步骤 3　点击 **OK** 以关闭 **Advanced Syslog Configuration** 对话框。

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　选择以下其中一个选项以指定应将哪些系统日志记录消息发送到内部日志缓冲区：

- **Home > Latest ASDM Syslog Messages > Configure ASDM Syslog Filters**
- **Configuration > Device Management > Logging > Logging Filters**

步骤 2　依次选择 **Monitoring > Logging > Log Buffer > View**。然后，选择 **Log Buffer** 窗格中的 **File > Clear Internal Log Buffer** 以清空内部日志缓冲区。

步骤 3　依次选择 **Configuration > Device Management > Logging > Logging Setup** 以更改内部日志缓冲区的大小。默认缓冲区大小为 4 KB。

ASA 和 ASASM 继续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。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）。

步骤 4　要将新消息保存到其他位置，请选择以下其中一个选项：

- 选中 **Flash** 复选框以将新消息发送到内部闪存，然后点击 **Configure Flash Usage**。系统将显示 **Configure Logging Flash Usage** 对话框。
  a. 指定要用于日志记录的最大闪存量（以 KB 为单位）。
  b. 指定日志记录在闪存中将保留的最小可用空间量（以 KB 为单位）。
  c. 点击 **OK** 以关闭此对话框。
- 选中 **FTP Server** 复选框以将新消息发送到 FTP 服务器，然后点击 **Configure FTP Settings**。系统将显示 **Configure FTP Settings** 对话框。
  a. 选中 **Enable FTP Client** 复选框。
  b. 在提供的字段中输入以下信息：FTP 服务器 IP 地址、路径、用户名和密码。
  c. 确认密码，然后点击 **OK** 以关闭此对话框。

将内部日志缓冲区保存到闪存

要将内部日志缓冲区保存到闪存，请执行以下步骤：

操作步骤

步骤 1　依次选择 **File > Save Internal Log Buffer to Flash**。

系统将显示 **Enter Log File Name** 对话框。

步骤 2　选择第一个选项以使用默认用户名 LOG-YYYY-MM-DD-hhmmss.txt 保存日志缓冲区。

步骤 3　选择第二个选项以指定日志缓冲区的文件名。

步骤 4　输入日志缓冲区的文件名，然后点击 **OK**。

使用 ASDM Java 控制台查看和复制已记录的条目

使用 ASDM Java 控制台以文本格式查看并复制已记录的条目，这可能有助于对 ASDM 错误进行疑难解答。

要访问 ASDM Java 控制台，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Tools > ASDM Java Console**。

步骤 2　在控制台中输入 **m** 以显示虚拟机内存统计信息。

步骤 3　在控制台中输入 **g** 以执行垃圾回收。

步骤 4　打开 Windows 任务管理器并双击 **asdm_launcher.exe** 文件以监控内存使用情况。

注意　允许的最大内存分配为 256 MB。

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　依次选择 **Configuration > Device Management > Logging > E-Mail Setup**。

步骤 2　指定用作以邮件形式发送的系统日志消息的源地址的邮件地址。

步骤 3　点击 **Add** 以输入指定的系统日志消息的新邮件地址收件人。

步骤 4　从下拉列表中选择发送给收件人的系统日志消息的严重性级别。用于目标邮件地址的系统日志消息严重性过滤器会导致发送指定严重性级别和更高严重性级别的消息。在 **Logging Filters** 窗格中指定的全局过滤器还会应用于每个邮件收件人。

步骤 5　点击 **Edit** 以修改发送给此收件人的系统日志消息的现有严重性级别。

步骤 6　点击 **OK** 以关闭 **Add E-mail Recipient** 对话框。

添加或编辑邮件收件人

要添加或编辑邮件收件人和严重性级别，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Logging > E-mail Setup**。

步骤 2　点击 **Add** 或 **Edit** 以显示 **Add/Edit E-Mail Recipient** 对话框。

步骤 3　输入目标邮件地址，然后从下拉列表中选择系统日志严重性级别。严重性级别定义如下：

- Emergency （级别 0，系统不可用）

注意　不建议使用严重性级别 0。

- Alert （级别 1，需要立即采取措施）
- Critical （级别 2，严重情况）
- Error （级别 3，错误情况）
- Warning （级别 4，警告情况）
- Notification （级别 5，正常但重大的情况）
- Informational （级别 6，消息仅供参考）
- Debugging （级别 7，消息仅供调试）

注意　用于过滤目标邮件地址的消息的严重性级别是在 **Add/Edit E-Mail Recipient** 对话框中指定的更高的严重性级别，并且是为 **Logging Filters** 窗格中所有邮件收件人设置的全局过滤器。

步骤 4　点击 **OK** 以关闭 **Add/Edit E-Mail Recipient** 对话框。

在 **E-mail Recipients** 窗格中将显示已添加或已修改的条目。

步骤 5　点击 **Apply** 以保存对运行配置所做的更改。

配置远程 SMTP 服务器

要配置为响应特定事件而将邮件提醒和通知发送到的远程 SMTP 服务器，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Device Setup > Logging > SMTP**。

步骤 2　输入主 SMTP 服务器的 IP 地址。

步骤 3　（可选）输入备用 SMTP 服务器的 IP 地址，然后点击 **Apply** 以保存对运行配置所做的更改。

在 ASDM 中查看系统日志消息

要查看已发送到 ASDM 的最新系统日志消息，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Home > Latest ASDM Syslog Messages**。

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。

将消息过滤器应用于日志记录目标

要将消息过滤器应用于日志记录目标，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Logging > Logging Filters**。

步骤 2　选择要对其应用过滤器的日志记录目标的名称。可用的日志记录目标如下：

- ASDM
- 控制台端口
- 电邮
- 内部缓冲区
- SNMP 服务器
- 系统日志服务器
- Telnet 或 SSH 会话

  此选择中包含第二列 Syslogs From All Event Classes 和第三列 Syslogs From Specific Event Classes。第二列列出要用于过滤日志记录目标的消息的严重性或事件类，或者是否为所有事件类禁用了日志记录。第三列列出要用于过滤该日志记录目标的消息的事件类。

步骤 3　点击 **Edit** 以显示 **Edit Logging Filters** 对话框。要应用、编辑或禁用过滤器，请参阅应用日志记录过滤器，第 38-13 页。

应用日志记录过滤器

要应用过滤器，请执行以下步骤：

操作步骤

步骤 1　选择 **Filter on severity** 选项以根据系统日志消息的严重性级别将其过滤。

步骤 2　选择 **Use event list** 选项以根据事件列表过滤系统日志消息。

步骤 3　选择 **Disable logging from all event classes** 选项以禁用到所选目标的所有日志记录。

步骤 4　点击 **New** 以添加新事件列表。要添加新事件列表，请参阅创建自定义事件列表，第 38-15 页。

步骤 5　从下拉列表中选择事件类。可用事件类根据使用的设备模式进行更改。

步骤 6　从下拉列表中选择日志记录消息的级别。严重性级别包括：

- Emergency （级别 0，系统不可用）

注意　不建议使用严重性级别 0。

- Alert （级别 1，需要立即采取措施）
- Critical （级别 2，严重情况）
- Error （级别 3，错误情况）
- Warning （级别 4，警告情况）
- Notification （级别 5，正常但重大的情况）
- Informational （级别 6，消息仅供参考）
- Debugging （级别 7，消息仅供调试）

步骤 7　点击 **Add** 以添加事件类和严重性级别，然后点击 **OK**。

过滤器的所选日志记录目标显示在顶部。

添加或编辑消息类和严重性过滤器

要添加或编辑用于过滤消息的消息类和严重性级别，请执行以下步骤：

操作步骤

步骤 1　从下拉列表中选择事件类。可用事件类根据使用的设备模式进行更改。

步骤 2　从下拉列表中选择日志记录消息的级别。严重性级别包括：

- Emergency （级别 0，系统不可用）

注意　不建议使用严重性级别 0。

- Alert （级别 1，需要立即采取措施）
- Critical （级别 2，严重情况）
- Error （级别 3，错误情况）
- Warning （级别 4，警告情况）
- Notification （级别 5，正常但重大的情况）
- Informational （级别 6，消息仅供参考）
- Debugging （级别 7，消息仅供调试）

步骤 3　进行选择完成后，点击 **OK**。

添加或编辑系统日志消息 ID 过滤器

要添加或编辑系统日志消息 ID 过滤器，请参阅编辑系统日志 ID 设置，第 38-8 页。

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　选择以下选项之一：

- **Home > Latest ASDM Syslog Messages > Configure ASDM Syslog Filters**
- **Configuration > Device Management > Logging > Logging Filters**

步骤 2　在 **Logging Destination** 列中选择控制台，然后点击 **Edit**。

系统将显示 **Edit Logging Filters** 对话框。

步骤 3　选择来自所有事件类的系统日志或来自特定事件类的系统日志，以指定应将哪些系统日志消息发送到控制台端口。

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　选择以下其中一个选项：

- **Home > Latest ASDM Syslog Messages > Configure ASDM Syslog Filters**
- **Configuration > Device Management > Logging > Logging Filters**

步骤 2　在 **Logging Destination** 列中选择 **Telnet** 和 **SSH Sessions**，然后点击 **Edit**。

系统将显示 **Edit Logging Filters** 对话框。

步骤 3　选择来自所有事件类的系统日志或来自特定事件类的系统日志，以指定应将哪些系统日志消息发送到 Telnet 或 SSH 会话。

步骤 4　依次选择 **Configuration > Device Management > Logging > Logging Setup** 以仅为当前会话启用日志记录。

步骤 5　选中 **Enable logging** 复选框，然后点击 **Apply**。

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　依次选择 **Configuration > Device Management > Logging > Event Lists**。

步骤 2　点击 **Add** 以显示 **Add Event List** 对话框。

步骤 3　输入事件列表的名称。不允许使用空格。

步骤 4　点击 **Add** 以显示 **Add Class and Severity Filter** 对话框。

步骤 5　从下拉列表中选择事件类。可用事件类根据使用的设备模式进行更改。

步骤 6　从下拉列表中选择严重性级别。严重性级别包括：

- Emergency （级别 0，系统不可用）

注意　不建议使用严重性级别 0。

- Alert （级别 1，需要立即采取措施）
- Critical （级别 2，严重情况）
- Error （级别 3，错误情况）
- Warning （级别 4，警告情况）
- Notification （级别 5，正常但重大的情况）
- Informational （级别 6，消息仅供参考）
- Debugging （级别 7，消息仅供调试）

步骤 7　点击 **OK** 以关闭 **Add Event List** 对话框。

步骤 8　点击 **Add** 以显示 **Add Syslog Message ID Filter** 对话框。

步骤 9　输入要在过滤器中包含的系统日志消息 ID 或 ID 范围 （例如 101001 至 199012）。

步骤 10　点击 **OK** 以关闭 **Add Event List** 对话框。

列表中将显示相关事件。

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　依次选择 **Configuration > Device Management > Logging > Syslog Server**。

步骤 2　点击 **Add** 以添加新系统日志服务器。

系统将显示 **Add Syslog Server** 对话框。

注意　可以设置每个安全情景最多四个系统日志服务器 （最多 16 个）。

步骤 3　指定当系统日志服务器繁忙时允许在 ASA 或 ASASM 上排队的消息数。零值意味着可以将无限数量的消息进行排队。

步骤 4　选中 **Allow user traffic to pass when TCP syslog server is down** 复选框以指定在任何系统日志服务器关闭的情况下是否限制所有流量。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。

添加或编辑系统日志服务器设置

要添加或编辑系统日志服务器设置，请执行以下步骤：

操作步骤

步骤 1　从下拉列表中选择用于与系统日志服务器进行通信的接口。

步骤 2　输入用于与系统日志服务器进行通信的 IP 地址。

选择供系统日志服务器用于与 ASA 或 ASASM 进行通信的协议（TCP 或 UDP）。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。

步骤 3　输入供系统日志服务器用于与 ASA 或 ASASM 进行通信的端口号。

步骤 4　选中 **Log messages in Cisco EMBLEM format (UDP only)** 复选框以指定是否记录思科 EMBLEM 格式的消息 （仅在选择 UDP 作为协议的情况下才可用）。

步骤 5　选中 **Enable secure logging using SSL/TLS (TCP only)** 复选框以指定通过使用 SSL/TLS over TCP，与系统日志服务器的连接是安全的，并且系统日志消息内容已加密。

步骤 6　点击 **OK** 以完成配置。

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　依次选择 **Configuration > Device Management > Logging > Logging Setup**。

步骤 2　选中 **Send syslogs in EMBLEM format** 复选框。

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　依次选择 **Configuration > Device Management > Logging > Logging Setup**。

步骤 2　选中 **Enable Logging** 复选框。

步骤 3　选中 **Logging to Internal Buffer** 区域中的 **Save Buffer to Flash** 复选框。

步骤 4　点击 **Configure Flash Usage**。

系统将显示 **Configure Logging Flash Usage** 对话框。

步骤 5　输入允许用于日志记录的最大内部闪存量 （以 KB 为单位）。

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 6　输入在闪存中要保留用于日志记录的最小可用空间量 （以 KB 为单位）。

步骤 7　点击 **OK** 以关闭 **Configure Logging Flash Usage** 对话框。

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　依次选择 **Configuration > Device Management > Logging > Logging Setup**。

步骤 2　选中 **Enable Logging** 复选框。

步骤 3　输入在 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。

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。

步骤 4　点击 **Apply** 以保存对运行配置所做的更改。

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　依次选择 **Configuration > Device Management > Logging > Logging Filters**。

步骤 2　要覆盖指定输出目标中的配置，请选择要更改的输出目标，然后点击 **Edit**。

系统将显示 **Edit Logging Filters** 对话框。

步骤 3　修改 **Syslogs from All Event Classes** 或 **Syslogs from Specific Event Classes** 区域中的设置，然后点击 **OK** 以关闭此对话框。

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。

要指定类应转至多个目标，请为每个输出目标选择不同的过滤选项。

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　依次选择 **Configuration > Device Management > Logging > Syslog Server**。

步骤 2　选择要为其启用安全日志记录的系统日志服务器，然后点击 **Edit**。

系统将显示 **Edit Syslog Server** 对话框。

步骤 3　点击 **TCP** 单选按钮。

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。

步骤 4　选中 **Enable secure syslog with SSL/TLS** 复选框，然后点击 **OK**。

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　依次选择 **Configuration > Device Management > Logging > Syslog Setup > Advanced > Advanced Syslog Configuration**。

步骤 2　选中 **Enable syslog device ID** 复选框。

步骤 3　点击 **Device ID** 区域中的 **Hostname**、 **Interface IP Address** 或 **String** 单选按钮。

- 如果选择 **Interface IP Address** 选项，请确保在下拉列表中选择正确的接口。

- 如果选择 **String** 选项，请在 **User-Defined ID** 字段中输入设备 ID。字符串可以包含多达 16 个字符。

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。

步骤 4　点击 **OK** 以关闭 **Advanced Syslog Configuration** 对话框。

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　依次选择 **Configuration > Device Management > Logging > Syslog Setup**。

步骤 2　选中 **Syslog ID Setup** 区域中的 **Include timestamp in syslogs** 复选框。

步骤 3　点击 **Apply** 保存更改。

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　依次选择 **Configuration > Device Management > Logging > Syslog Setup**。

步骤 2　选择要从表中禁用的系统日志，然后点击 **Edit**。

系统将显示 **Edit Syslog ID Settings** 对话框。

步骤 3　选中 **Disable messages** 复选框，然后点击 **OK**。

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　依次选择 **Configuration > Device Management > Logging > Syslog Setup**。

步骤 2　从表中选择要更改其严重性级别的系统日志，然后点击 **Edit**。

系统将显示 **Edit Syslog ID Settings** 对话框。

步骤 3　从 **Logging Level** 下拉列表中选择期望严重性级别，然后点击 **OK**。

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　依次选择 **Configuration > Device Management > Logging > Syslog Settings**。

步骤 2　在表中选择系统日志 ID，然后点击 **Edit**。

系统将显示 **Edit Syslog ID Settings** 对话框。

步骤 3　选中 **Disable messages on standby unit** 复选框以阻止在备用设备上生成系统日志消息。

步骤 4　点击 **OK** 以关闭此对话框。

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　依次选择 **Configuration > Device Management > Logging > Rate Limit**。

步骤 2　选择要向其指定速率限制的日志记录级别 （消息严重性级别）。严重性级别定义如下：

说明	严重级别
应急	0 - 系统不可用
警报	1 - 需要立即采取措施
严重	2 - 严重情况
错误	3 - 错误情况
警告	4 - 警告情况
通知	5 - 正常但重大的情况
参考	6 - 消息仅供参考
除错	7 - 消息仅供调试

步骤 3　No of Messages 字段显示发送的消息数。Interval (Seconds) 字段显示用于限制可发送的此日志记录级别的消息数的间隔 （以秒为单位）。从表中选择日志记录级别，然后点击 **Edit** 以显示 **Edit Rate Limit for Syslog Logging Level** 对话框。

步骤 4　要继续，请参阅指定或更改单独系统日志消息的速率限制，第 38-22 页。

指定或更改单独系统日志消息的速率限制

要指定或更改单独系统日志消息的速率限制，请执行以下步骤：

操作步骤

步骤 1　要指定特定系统日志消息的速率限制，请点击 **Add** 以显示 **Add Rate Limit for Syslog Message** 对话框。

步骤 2　要继续，请参阅添加或编辑系统日志消息的速率限制，第 38-22 页。

步骤 3　要更改特定系统日志消息的速率限制，请点击 **Edit** 以显示 **Edit Rate Limit for Syslog Message** 对话框。

步骤 4　要继续，请参阅编辑系统日志严重性级别的速率限制，第 38-22 页。

添加或编辑系统日志消息的速率限制

要添加或更改特定系统日志消息的速率限制，请执行以下步骤：

操作步骤

步骤 1　要向特定系统日志消息中添加速率限制，请点击 **Add** 以显示 **Add Rate Limit for Syslog Message** 对话框。要更改系统日志消息的速率限制，请点击 **Edit** 以显示 **Edit Rate Limit for Syslog Message** 对话框。

步骤 2　输入要限制的系统日志消息的消息 ID。

步骤 3　输入在指定时间间隔内可以发送的最大消息数。

步骤 4　输入用于限制指定消息的速率的时间量 （以秒为单位），然后点击 **OK**。

注意　要允许无限数量的消息，请将 **Number of Messages** 和 **Time Interval** 字段均留空。

编辑系统日志严重性级别的速率限制

要更改指定系统日志严重性级别的速率限制，请执行以下步骤：

操作步骤

步骤 1　输入可以发送的处于此严重性级别的最大消息数。

步骤 2　输入用于限制处于此严重性级别的消息的速率的时间量 （以秒为单位），然后点击 **OK**。

系统将显示所选消息严重性级别。

注意　要允许无限数量的消息，请将 **Number of Messages** 和 **Time Interval** 字段均留空。

监控日志

有关监控日志记录状态的信息，请参阅以下屏幕。

- **Monitoring > Logging > Log Buffer > View**

  通过此窗格可查看日志缓冲区。

- **Monitoring > Logging > Real-Time Log Viewer > View**

  通过此窗格可查看实时日志。

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

通过日志查看器过滤系统日志消息

可以根据与 Real-Time Log Viewer 和 Log Buffer Viewer 中的任何列对应的一个或多个值过滤系统日志消息。

要通过其中一个日志查看器过滤系统日志消息，请执行以下步骤：

操作步骤

步骤 1　选择以下选项之一：

- **Monitoring > Logging > Real-Time Log Viewer > View**
- **Monitoring > Logging > Log Buffer > View**

步骤 2　在 **Real-Time Log Viewer** 或 **Log Buffer Viewer** 对话框中，点击工具栏上的 **Build Filter**。

步骤 3　在 **Build Filter** 对话框中，指定要应用于系统日志消息的过滤条件。

a. 在 **Date and Time** 区域中选择以下三个选项之一：real-time、特定时间或时间范围。如果选择特定时间，请通过输入数字并从下拉列表中选择小时或分钟来指示时间。如果选择时间范围，请点击 **Start Time** 字段中的下拉箭头以显示日历。从下拉列表中选择开始日期和开始时间，然后点击 **OK**。点击 **End Time** 字段中的下拉箭头以显示日历。从下拉列表中选择结束日期和结束时间，然后点击 **OK**。

b. 在 **Severity** 字段中输入有效的严重性级别。或者，点击 **Severity** 字段右侧的 **Edit** 图标。点击列表中要按其过滤的严重性级别。要包含严重性级别 1 至 7，请点击 **All**。点击 **OK** 以在 **Build Filter** 对话框中显示这些设置。点击 **Severity** 字段右侧的 **Info** 图标以获取有关要使用的正确输入格式的其他信息。

c. 在 **Syslog ID** 字段中输入有效的系统日志 ID。或者，点击 **Syslog ID** 字段右侧的 **Edit** 图标。从下拉列表中选择要按其过滤的条件，然后点击 **Add**。点击 **OK** 以在 **Build Filter** 对话框中显示这些设置。点击 **Syslog ID** 字段右侧的 **Info** 图标以获取有关要使用的正确输入格式的其他信息。

d. 在 **Source IP Address** 字段中输入有效的源 IP 地址，或者点击 **Source IP Address** 字段右侧的 **Edit** 图标。选择单个 IP 地址或指定的 IP 地址范围，然后点击 **Add**。选中 **Do not include (exclude) this address or range** 复选框以排除特定 IP 地址或 IP 地址范围，点击 **OK** 以在 **Build Filter** 对话框中显示这些设置。点击 **Source IP Address** 字段右侧的 **Info** 图标以获取有关要使用的正确输入格式的其他信息。

e. 在 **Source Port** 字段中输入有效的源端口，或者点击 **Source Port** 字段右侧的 **Edit** 图标。从下拉列表中选择要按其过滤的条件，然后点击 **Add**。点击 **OK** 以在 **Build Filter** 对话框中显示这些设置。点击 **Source Port** 字段右侧的 **Info** 图标以获取有关要使用的正确输入格式的其他信息。

f. 在 **Destination IP Address** 字段中输入有效的目标 IP 地址，或者点击 **Destination IP Address** 字段右侧的 **Edit** 图标。选择单个 IP 地址或指定的 IP 地址范围，然后点击 **Add**。选中 **Do not include (exclude) this address or range** 复选框以排除特定 IP 地址或 IP 地址范围。点击 **OK** 以在 **Build Filter** 对话框中显示这些设置。点击 **Destination IP Address** 字段右侧的 **Info** 图标以获取有关要使用的正确输入格式的其他信息。

g. 在 **Destination Port** 字段中输入有效的目标端口，或者点击 **Destination Port** 字段右侧的 **Edit** 图标。从下拉列表中选择要按其过滤的条件，然后点击 **Add**。点击 **OK** 以在 **Build Filter** 对话框中显示这些设置。点击 **Destination Port** 字段右侧的 **Info** 图标以获取有关要使用的正确输入格式的其他信息。

h. 为 **Description** 字段输入过滤文本。文本可能是由一个或多个字符组成的任意字符串，包括正则表达式。但是，分号是无效字符，并且此设置区分大小写。多个条目须以逗号分隔。

i. 点击 **OK** 以将刚指定的过滤器设置添加到日志查看器中的 **Filter By** 下拉列表。过滤器字符串遵循特定格式。前缀 FILTER: 指定在 **Filter By** 下拉列表中显示的所有自定义过滤器。仍然可以在此字段中键入随机文本。

   下表显示所使用的格式的示例。

构建过滤器示例	过滤器字符串格式
Source IP = 192.168.1.1 或 0.0.0.0 Source Port = 67	FILTER: srcIP=192.168.1.1,0.0.0.0;srcPort=67;
Severity = Informational Destination IP = 1.1.1.1 至 1.1.1.10	FILTER: sev=6;dstIP=1.1.1.1-1.1.1.10;
系统日志 ID 不在范围 725001 至 725003 内	FILTER: sysID=!725001-725003;
Source IP = 1.1.1.1 Description = Built outbound	FILTER: srcIP=1.1.1.1;descr=Built outbound

步骤 4　选择 **Filter By** 下拉列表中的设置之一以过滤系统日志消息，然后点击工具栏上的 **Filter**。此设置还适用于所有将来的系统日志消息。点击工具栏上的 **Show All** 以清除所有过滤器。

注意　无法使用 **Build Filter** 对话框保存已指定的过滤器。这些过滤器仅对其创建期间的 ASDM 会话有效。

编辑过滤设置

要使用 **Build Filter** 对话框编辑所创建的过滤器设置，请执行以下步骤：

操作步骤

步骤 1　选择以下选项之一：

- 直接通过在 **Filter By** 下拉列表中执行更改来修改过滤器。
- 在 **Filter By** 下拉列表中选择过滤器，然后点击 **Build Filter** 以显示 **Build Filter** 对话框。点击 **Clear Filter** 以删除当前过滤器设置并输入新设置。否则，请更改显示的设置，然后点击 **OK**。

注意　这些过滤器设置仅适用于 **Build Filter** 对话框中定义的过滤器。

- 点击工具栏上的 **Show All** 以停止过滤并显示所有系统日志消息。

使用日志查看器发出特定命令

可以使用任一日志查看器发出以下命令：**ping**、 **traceroute**、 **whois** 和 **dns lookup**。

要运行其中任何命令，请执行以下步骤：

操作步骤

步骤 1　选择以下选项之一：

- **Monitoring > Logging > Real-Time Log Viewer > View**
- **Monitoring Logging > Log Buffer > View**

步骤 2　从 **Real-Time Log Viewer** 或 **Log Buffer** 窗格中点击 **Tools**，然后选择要执行的命令。或者，可以右键点击所列的特定系统日志消息以显示情景菜单，然后选择要执行的命令。

系统将显示 **Entering command** 对话框，其中所选命令会自动显示在下拉列表中。

步骤 3　在 **Address** 字段中输入所选系统日志消息的源 IP 地址或目标 IP 地址，然后点击 **Go**。

在提供的区域中将显示命令输出。

步骤 4　点击 **Clear** 以删除输出，然后从下拉列表中选择要执行的其他命令。如有必要，请重复第 3 步。完成后点击 **Close**。

日志记录的历史记录

表 38-2　　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。 引入了以下屏幕：Configuration > Device Management > Logging > Logging Setup。
速率限制	7.0(4)	限制生成系统日志消息的速率。 修改了以下屏幕：Configuration > Device Management > 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。 修改了以下屏幕：Configuration > Device Management > Logging > Event Lists。

表 38-2　　日志记录的历史记录 （续）

功能名称	平台版本	说明
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。 修改了以下屏幕：Configuration > Device Management > Logging > Syslog Server。
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。 修改了以下屏幕：Configuration > Device Management > Logging > Logging Filters。
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。 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。 修改了以下屏幕：Configuration > Device Management > Logging > Logging Setup。
密码加密	8.3(1)	添加了对密码加密的支持。
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，请继续选中 Configuration > Device Management > Logging > Syslog Servers 窗格上的 **Allow user traffic to pass when TCP syslog server is down** 复选框。 引入了以下系统日志消息：414005、 414006、 414007 和 414008。 未修改任何 ASDM 屏幕。
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。

表 38-2　　日志记录的历史记录 （续）

功能名称	平台版本	说明
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。 修改了以下屏幕：Configuration > Logging > Syslog Setup > Advanced > Advanced Syslog Configuration。
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。 修改了以下屏幕：Configuration > Device Management > Logging > Syslog Setup。

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

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 39-1 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。

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，配置 SNMP NMS 并确保将 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。
- 如果 NMS 无法成功请求对象或者未在正确处理来自 ASA 的传入陷阱，则执行数据包捕获是确定的问题最实用方法。依次选择 **Wizards > Packet Capture Wizard**，然后遵循屏幕上的说明执行操作。
- 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。

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 39-5 页。

步骤 2　将 SNMP 管理站配置为接收来自 ASA 的请求。请参阅配置 SNMP 管理站，第 39-5 页。

步骤 3　配置 SNMP 陷阱。请参阅配置 SNMP 陷阱，第 39-6 页。

步骤 4　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 39-7 页或配置 SNMP 第 3 版的参数，第 39-7 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

配置 SNMP 管理站

要配置 SNMP 管理站，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Management Access > SNMP**。默认情况下，SNMP 服务器已启用。

步骤 2　点击 **SNMP Management Stations** 窗格中的 **Add**。

系统将显示 **Add SNMP Host Access Entry** 对话框。

步骤 3　选择 SNMP 主机所在的接口。

步骤 4　输入 SNMP 主机 IP 地址。

步骤 5　输入 SNMP 主机 UDP 端口或保留默认值，即端口 162。

步骤 6　添加 SNMP 主机社区字符串。如果没有为管理站指定社区字符串，则会使用 **SNMP Management Stations** 窗格上的 **Community String**（默认）字段中设置的值。

步骤 7　选择 SNMP 主机使用的 SNMP 版本。

步骤 8　如果在上一步中选择 SNMP 第 3 版，请选择已配置的用户的名称。

步骤 9　要指定用于与此 NMS 进行通信的方法，请选中 **Poll** 或 **Trap** 复选框。

步骤 10　点击 **OK**。

系统将关闭 **Add SNMP Host Access Entry** 对话框。

步骤 11　点击 **Apply**。

系统将配置 NMS 并将更改保存到运行配置。有关 SNMP 第 3 版 NMS 工具的详细信息，请参阅以下 URL：

http://www.cisco.com/en/US/docs/security/asa/asa82/snmp/snmpv3_tools.html

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　依次选择 **Configuration > Device Management > Management Access > SNMP**。

步骤 2　点击 **Configure Traps**。

系统将显示 **SNMP Trap Configuration** 对话框。

步骤 3　选中 **SNMP Server Traps Configuration** 复选框。

陷阱分为以下类别：标准、IKEv2、实体 MIB、IPsec、远程访问、资源、NAT、系统、CPU 利用率、 CPU 利用率和监控间隔，以及 SNMP 接口阈值和间隔。为 SNMP 事件选中适用的复选框以通过 SNMP 陷阱进行通知。默认配置已启用所有 SNMP 标准陷阱。如果不指定陷阱类型，则默认为系统日志陷阱。默认 SNMP 陷阱随系统日志陷阱继续启用。默认情况下会禁用所有其他陷阱。要禁用陷阱，请取消选中适用的复选框。要配置系统日志陷阱严重性级别，请依次选择 **Configuration > Device Management > Logging > Logging Filters**。

步骤 4　点击 **OK** 以关闭 **SNMP Trap Configuration** 对话框。

步骤 5　点击 **Apply**。

系统将配置 SNMP 陷阱配置并将更改保存到运行配置。

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　依次选择 **Configuration > Device Management > Management Access > SNMP**。

步骤 2　如果使用的是 SNMP 第 1 版或第 2c 版，请在 **Community String**（默认）字段中输入默认社区字符串。在 SNMP NMS 将请求发送到 ASA 时输入其使用的密码。SNMP 社区字符串是 SNMP NMS 和托管网络节点之间的共享密钥。ASA 使用密码确定传入 SNMP 请求是否有效。密码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。默认值为 public。SNMP 第 2c 版允许为每个 NMS 设置单独的社区字符串。如果没有为任何 NMS 配置社区字符串，则默认情况下使用此处设置的值。

步骤 3　输入 ASA 系统管理员的名称。名称区分大小写，并且最多可以为 127 个字母字符。接受空格，但多个空间缩为一个空格。

步骤 4　输入由 SNMP 管理的 ASA 的位置。文本区分大小写，并且最多可以为 127 个字符。接受空格，但多个空间缩为一个空格。

步骤 5　输入侦听来自 NMS 的 SNMP 请求的 ASA 端口号；或者保留默认值，即端口号 161。

步骤 6　点击 **SNMP Host Access List** 窗格中的 **Add**。

系统将显示 **Add SNMP Host Access Entry** 对话框。

步骤 7　从下拉列表中选择从其发送陷阱的接口名称。

步骤 8　输入可以连接到 ASA 的 NMS 或 SNMP 管理器的 IP 地址。

步骤 9　输入 UDP 端口号。默认值为 162。

步骤 10　从下拉列表中选择您使用的 SNMP 版本。如果选择第 1 版或第 2c 版，则必须输入社区字符串。如果选择第 3 版，则必须从下拉列表中选择用户名。

步骤 11　选中 **Server Poll/Trap Specification** 区域中的 **Poll** 复选框，以将 NMS 限制为仅发送请求（轮询）。选中 **Trap** 复选框以将 NMS 限制为仅接收陷阱。您可以同时选中两个复选框以执行 SNMP 主机的两个功能。

步骤 12　点击 **OK** 以关闭 **Add SNMP Host Access Entry** 对话框。

新主机将显示在 **SNMP Host Access List** 窗格中。

步骤 13　点击 **Apply**。

系统将配置第 1、 2c 或 3 版的 SNMP 参数并将更改保存到运行配置。

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　依次选择 **Configuration > Device Management > Management Access > SNMP**。

步骤 2　依次点击 **SNMPv3 Users** 窗格中 **SNMPv3 User/Group** 选项卡上的 **Add > SNMP User** 来向组中添加已配置的用户或新用户。删除组中的最后一个用户时， ASDM 会删除该组。

注意　创建用户后，不能更改该用户所属的组。

系统将显示 **Add SNMP User Entry** 对话框。

步骤 3　选择 SNMP 用户所属的组。可用的组如下：

- **Auth&Encryption**，其中用户已配置身份验证和加密
- **Authentication_Only**，其中用户仅配置了身份验证
- **No_Authentication**，其中用户未配置身份验证和加密

注意　不能更改组名。

步骤 4　点击 **USM Model** 选项卡以使用用户安全模式 (USM) 组。

步骤 5　点击**添加**。

系统将显示 **Add SNMP USM Entry** 对话框。

步骤 6　输入组名称。

步骤 7　从下拉列表中选择安全级别。此设置允许将已配置的 USM 组作为安全级别分配给 SNMPv3 用户。

步骤 8　输入已配置的用户或新用户的名称。用户名对于所选 SNMP 服务器组必须唯一。

步骤 9　通过点击以下两个单选按钮之一指示要使用的密码类型：**Encrypted** 或 **Clear Text**。

步骤 10　通过点击以下两个单选按钮之一指示要使用的身份验证类型：**MD5** 或 **SHA**。

步骤 11　输入要用于身份验证的密码。

步骤 12　通过点击以下三个单选按钮之一指示要使用的加密类型：**DES**、 **3DES** 或 **AES**。

步骤 13　如果选择 AES 加密，则选择要使用的 AES 加密级别：**128**、 **192** 或 **256**。

步骤 14　输入要用于加密的密码。此密码允许的最大字母数字字符数为 64。

步骤 15　点击 **OK** 以创建组 （如果这是该组中的第一个用户），在 **Group Name** 下拉列表中显示该组，然后为该组创建用户。

系统将关闭 **Add SNMP User Entry** 对话框。

步骤 16　点击 **Apply**。

系统将配置第 3 版的 SNMP 参数并将更改保存到运行配置。

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　依次选择 **Configuration > Device Management > Management Access > SNMP**。

步骤 2　依次点击 **SNMPv3 Users** 窗格中 **SNMPv3 User/Group** 选项卡上的 **Add > SNMP User Group** 来添加已配置的用户组或新用户组。删除组中的最后一个用户时， ASDM 会删除该组。

系统将显示 **Add SNMP User Group** 对话框。

步骤 3　输入用户组名。

步骤 4　点击 **Existing User/User Group** 单选按钮以选择现有用户或用户组。

步骤 5　点击 **Create new user** 单选按钮以创建新用户。

步骤 6　选择 SNMP 用户所属的组。可用的组如下：

- **Auth&Encryption**，其中用户已配置身份验证和加密
- **Authentication_Only**，其中用户仅配置了身份验证
- **No_Authentication**，其中用户未配置身份验证和加密

步骤 7　输入已配置的用户或新用户的名称。用户名对于所选 SNMP 服务器组必须唯一。

步骤 8　通过点击以下两个单选按钮之一指示要使用的密码类型：**Encrypted** 或 **Clear Text**。

步骤 9　通过点击以下两个单选按钮之一指示要使用的身份验证类型：**MD5** 或 **SHA**。

步骤 10　输入要用于身份验证的密码。

步骤 11　确认要用于身份验证的密码。

步骤 12　通过点击以下三个单选按钮之一指示要使用的加密类型：**DES**、 **3DES** 或 **AES**。

步骤 13　输入要用于加密的密码。此密码允许的最大字母数字字符数为 64。

步骤 14　确认要用于加密的密码。

步骤 15　点击 **Add** 以将新用户添加到 **Members in Group** 窗格中的指定用户组。点击 **Remove** 以从 **Members in Group** 窗格中删除现有用户。

步骤 16　点击 **OK** 为指定用户组创建新用户。

系统将关闭 **Add SNMP User Group** 对话框。

步骤 17　点击 **Apply**。

系统将配置第 3 版的 SNMP 参数并将更改保存到运行配置。

监控 SNMP

请参阅以下用于监控 SNMP 的信息的额屏幕：

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

SNMP 历史记录

表 39-2 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。 修改了以下屏幕：Configuration > Device Management > Management Access > SNMP。
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。 修改了以下屏幕：Configuration > Device Management > Management Access > SNMP。
密码加密	8.3(1)	支持密码加密。
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。 修改了以下屏幕：Configuration > Device Management > Management Access > SNMP。
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。
ASA 服务模块 (ASASM)	8.5(1)	ASASM 支持 8.4(1) 中存在的所有 MIB 和陷阱，但以下除外： 8.5(1) 中不受支持的 MIB： • CISCO-ENTITY-SENSOR-EXT-MIB （仅支持 entPhySensorTable 组下的对象）。 • ENTITY-SENSOR-MIB （仅支持 entPhySensorTable 组中的对象）。 • DISMAN-EXPRESSION-MIB （仅支持 expExpressionTable、expObjectTable 和 expValueTable 组中的对象）。 8.5(1) 中不受支持的陷阱： • ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)。此陷阱仅用于电源故障、风扇故障和高 CPU 温度事件。 • InterfacesBandwidthUtilization.

表 39-2 SNMP 历史记录 （续）

功能名称	平台版本	说明
SNMP 陷阱	8.6(1)	支持 ASA 5512-X、 5515-X、 5525-X、 5545-X 和 5555-X 的以下其他关键字：**entity power-supply-presence**、 **entity power-supply-failure**、 **entity chassis-temperature**、 **entity chassis-fan-failure**、 **entity power-supply-temperature**。 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。 修改了以下屏幕：Configuration > Device Management > Management Access > SNMP。
SNMP 消息大小	9.2(1)	SNMP 发送的消息大小限制已增大为 1472 字节。
SNMP OID 和 MIB	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。

表 39-2 SNMP 历史记录 （续）

功能名称	平台版本	说明
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。 修改了以下屏幕：Configuration > Device Management > Management Access > SNMP > Configure Traps > SNMP Trap Configuration。
SNMP MIB 和陷阱	9.4(1)	The ASA 5506W-X, ASA 5506H-X, ASA 5508-X, and ASA 5516-X have been added as a new product to the SNMP sysObjectID OID and entPhysicalVendorType OID tables.
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。 未修改任何 ASDM 屏幕。

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

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。

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 40-2 页
- 配置 DNS 服务器，第 18-10 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。

配置 Anonymous Reporting

要配置 Anonymous Reporting，请执行以下步骤：

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Smart Call Home**。

步骤 2　选中 **Enable Anonymous Reporting** 复选框。

步骤 3　点击 **Test Connection** 以确保系统能够发送消息。

ASDM 将返回一条成功或错误消息，以便向您通知测试结果。

步骤 4　点击 **Apply** 以保存配置并启用 Anonymous Reporting。

配置 Smart Call Home

要配置 Smart Call Home 服务、系统设置和警报订用配置文件，请执行以下步骤。

操作步骤

步骤 1　依次选择 **Configuration > Device Management > Smart Call Home**。

步骤 2　选中 **Enable Registered Smart Call Home** 复选框，以启用 Smart Call Home 并向思科 TAC 注册 ASA。

步骤 3　双击 **Advanced System Setup**。此区域包含三个窗格。双击标题行可以展开或折叠每个窗格。

a. 可以在 **Mail Servers** 窗格中设置邮件服务器，用于将 Smart Call Home 消息传递给邮件用户。

b. 可以在 ASA 的 **Contact Information** 窗格中输入联系人信息，此信息将显示在 Smart Call Home 消息中。此窗格包含以下信息：

- 联系人的姓名。
- 联系人的电话号码。
- 联系人的邮寄地址。
- 联系人的邮件地址。
- Smart Call Home 邮件中的 “发件人”邮件地址。
- Smart Call Home 邮件中的 “回复”邮件地址。
- 客户 ID。
- 站点 ID。
- 合同 ID。

c. 可以在 **Alert Control** 窗格中调整警报控制参数。此窗格包含 **Alert Group Status** 窗格，后者列出以下警报组的状态（已启用或已禁用）：

- 诊断警报组。
- 配置警报组。
- 环境警报组。
- 资产警报组。

- 快照警报组。
- 系统日志警报组。
- 遥测警报组。
- 威胁警报组。
- 每分钟处理的最大 Smart Call Home 消息数。
- Smart Call Home 邮件中的 “发件人” 邮件地址。

步骤 4　双击 **Alert Subscription Profiles**。每个指定的订用配置文件都标识了感兴趣的用户和警报组。

a. 点击 **Add** 或 **Edit** 以显示 **Subscription Profile Editor**，可以在其中创建新的订用配置文件或者编辑现有订用配置文件。

b. 点击 **Delete** 以删除所选配置文件。

c. 选中 **Active** 复选框，以便向用户发送所选订用配置文件的 Smart Call Home 消息。

步骤 5　点击 **Add** 或 **Edit** 以显示 **Add** 或 **Edit Alert Subscription Profile** 对话框。

a. **Name** 字段是只读字段，不可编辑。

b. 选中 **Enable this subscription profile** 复选框以启用或禁用此特定配置文件。

c. 点击 **Alert Delivery Method** 区域中的 **HTTP** 或 **Email** 单选按钮。

d. 在 **Subscribers** 字段中输入邮件地址或 Web 地址。

e. 管理员可以在 **Alert Dispatch** 区域中指定要向用户发送的 Smart Call Home 信息类型以及要在哪些情况下发送这些信息。根据警报触发方式，已选中两种类型的警报，即基于时间的警报和基于事件的警报。下列警报组基于时间：配置、资产、快照和遥测。下列警报组基于事件：诊断、环境、系统日志和威胁。

f. 可以在 **Message Parameters** 区域中调整用于控制向用户发送的消息的参数，包括首选消息格式和最大消息大小。

步骤 6　对于基于时间的警报，请点击 **Alert Dispatch** 区域中的 **Add** 或 **Edit**，以显示 **Add** 或 **Edit Configuration Alert Dispatch Condition** 对话框。

a. 在 **Alert Dispatch Frequency** 区域中指定向用户发送信息的频率：

- 对于每月订用，请指定要在一个月中的哪一天的什么时间发送信息。如果未指定这些信息，则 ASA 将选择适当的值。
- 对于每周订用，请指定要在一周中的哪一天的什么时间发送信息。如果未指定这些信息，则 ASA 将选择适当的值。
- 对于每日订用，请指定要在一天中的什么时间发送信息。如果未指定此信息，则 ASA 将选择适当的值。
- 对于每小时订用，请指定要在一个小时内的第几分钟发送信息。如果未指定此信息，则 ASA 将选择适当的值。每小时订用仅适用于快照和遥测警报组。

b. 点击 **Basic** 或 **Detailed** 单选按钮，以便向用户提供所需级别的信息。

c. 点击 **OK** 以保存配置。

步骤 7　对于基于诊断、环境和威胁事件的警报，请点击 **Alert Dispatch** 区域中的 **Add** 或 **Edit**，以显示 **Create** 或 **Edit Diagnostic Alert Dispatch Condition** 对话框。

步骤 8　在 **Event Severity** 下拉列表中指定将会触发向用户发送警报的事件严重性，然后点击 **OK**。

步骤 9　对于基于资产时间的警报，请点击 **Alert Dispatch** 区域中的 **Add** 或 **Edit**，以显示 **Create** 或 **Edit Inventory Alert Dispatch Condition** 对话框。

步骤 10　在 **Alert Dispatch Frequency** 下拉列表中指定向用户发送警报的频率，然后点击 **OK**。

步骤 11　对于基于快照时间的警报，请点击 **Alert Dispatch** 区域中的 **Add** 或 **Edit**，以显示 **Create** 或 **Edit Snapshot Alert Dispatch Condition** 对话框。

a. 在 **Alert Dispatch Frequency** 区域中指定向用户发送信息的频率：
   - 对于每月订用，请指定要在一个月中的哪一天的什么时间发送信息。如果未指定这些信息，则 ASA 将选择适当的值。
   - 对于每周订用，请指定要在一周中的哪一天的什么时间发送信息。如果未指定这些信息，则 ASA 将选择适当的值。
   - 对于每日订用，请指定要在一天中的什么时间发送信息。如果未指定此信息，则 ASA 将选择适当的值。
   - 对于每小时订用，请指定要在一个小时内的第几分钟发送信息。如果未指定此信息，则 ASA 将选择适当的值。每小时订用仅适用于快照和遥测警报组。
   - 对于时间间隔订用，请指定向用户发送信息的频率 （以分钟为单位）。此要求仅适用于快照警报组。

b. 点击 **OK** 以保存配置。

步骤 12　对于基于系统日志事件的警报，请点击 **Alert Dispatch** 区域中的 **Add** 或 **Edit**，以显示 **Create** 或 **Edit Syslog Alert Dispatch Condition** 对话框。

a. 选中 **Specify the event severity which triggers the dispatch of alert to subscribers** 复选框，然后从下拉列表中选择事件严重性。

b. 选中 **Specify the message IDs of syslogs which trigger the dispatch of alert to subscribers** 复选框。

c. 根据屏幕上的说明，指定将会触发向用户发送警报的系统日志消息 ID。

d. 点击 **OK** 以保存配置。

步骤 13　对于基于遥测事件的警报，请点击 **Alert Dispatch** 区域中的 **Add** 或 **Edit**，以显示 **Create** 或 **Edit Telemetry Alert Dispatch Condition** 对话框。

a. 在 **Alert Dispatch Frequency** 区域中指定向用户发送信息的频率：
   - 对于每月订用，请指定要在一个月中的哪一天的什么时间发送信息。如果未指定这些信息，则 ASA 将选择适当的值。
   - 对于每周订用，请指定要在一周中的哪一天的什么时间发送信息。如果未指定这些信息，则 ASA 将选择适当的值。
   - 对于每日订用，请指定要在一天中的什么时间发送信息。如果未指定此信息，则 ASA 将选择适当的值。
   - 对于每小时订用，请指定要在一个小时内的第几分钟发送信息。如果未指定此信息，则 ASA 将选择适当的值。每小时订用仅适用于快照和遥测警报组。

b. 点击 **OK** 以保存配置。

步骤 14　点击 **Test** 以确定所配置的警报是否正常工作。

监控 Anonymous Reporting 和 Smart Call Home

要监控 Anonymous Reporting 和 Smart Call Home 服务，请参阅下列屏幕。

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

Anonymous Reporting 和 Smart Call Home 的历史记录

表 40-1 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。 引入了以下屏幕： Configuration > Device Management > Smart Call Home。
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。 修改了以下屏幕：Configuration > Device Management > Smart Call Home。
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

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

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 41-1　　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 41-1　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 41-2　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 41-3　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 15-11 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 41-4　　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 41-9 页
- 接口标识符，第 41-7 页
- 与 IPv4 兼容的 IPv6 地址，第 41-6 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。

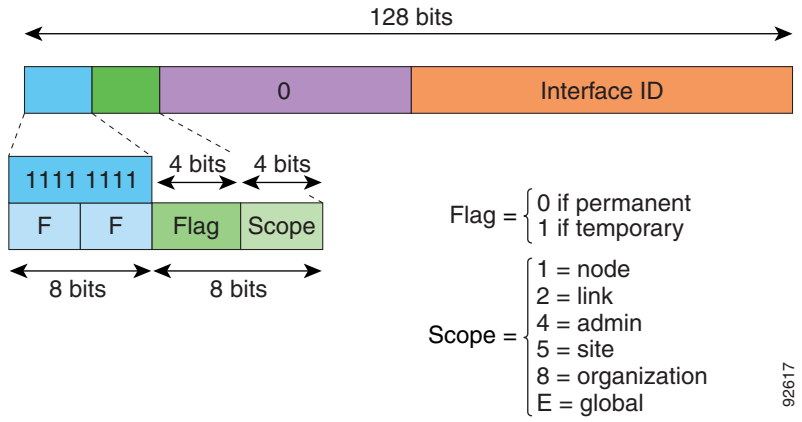
例如，具有 MAC 地址 00E0.b601.3B7A 的接口将会有一个 64 位接口 ID 02E0:B6FF:FE01:3B7A。

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 41-1　　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 41-5　　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 41-6　　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 41-6　　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 41-7　　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 41-7　　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 41-7　　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 41-8　　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 41-9　　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