思科 ASA 系列常规操作 ASDM 配置指南

软件版本 7.3

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

思科系统公司
www.cisco.com

思科在全球设有 200 多个办事处。
思科网站 www.cisco.com/go/offices 上
提供了各办事处的地址、电话和传真。

文本部分号：不适用，仅供在线使用

思科 ASA 系列常规操作 ASDM 配置指南

目录

附录 43

关于本指南

文档目标

本指南旨在帮助您使用思科自适应安全设备管理器 (ASDM) 为 Cisco ASA 系列配置常规操作。本指南不涵盖所有功能，只介绍了最常见的配置方案。

在本指南中，术语“ASA”一般适用于受支持的型号，除非另有规定。

注 ASDM 支持很多 ASA 版本。ASDM 文档和联机帮助包含 ASA 支持的所有最新功能。如果您运行的是旧版 ASA 软件，该文档可能包含您的版本不支持的功能。同样，如果旧的主要或次要版本的维护版本中增加了某项功能， ASDM 文档中将包含该新功能，即使并非以后推出的所有新版 ASA 都提供该功能。请参阅每一章的功能历史以确定功能的添加时间。有关每个 ASA 版本的 ASDM 最低支持版本，请参阅 *Cisco ASA 系列兼容性*。

相关文档

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

约定

本文档使用下列约定：

约定	说明
粗体	命令和关键字及用户输入的文本以**粗**体显示。
*斜*体	文档标题、新增或强调的术语以及要为其提供值的参数以*斜*体表示。
[ ]	方括号中的元素是可选项。
{x | y | z }	必填的备选关键字括在大括号内，以竖**线**分隔。
[x | y | z]	可选的备选关键字括在方括号内，以竖**线**分隔。
字符串	不加引号的字符集。请勿将字符串用引号引起来，否则会将字符串和引号视为一个整体。
`courier` 字体	系统显示的终端会话和信息以 `courier` 字体显示。
`courier bold` 字体	命令和关键字及用户输入的文本以 **`bold courier`** 字体显示。
`courier italic` 字体	您为其提供值的参数以 *`courier italic`* 字体显示。
< >	非打印字符 （如密码）括在尖括号中。
[ ]	系统提示的默认回复括在方括号中。
!， #	代码行开头的感叹号 (!) 或井号 (#) 表示注释行。

注 表示*读者需要注意的地方。*

提示 表示*以下信息有助于您解决问题。*

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

获取文档和提交服务请求

有关获取文档、使用 Cisco Bug 搜索工具 (BST)、提交服务请求和收集更多信息的信息，请参阅*思科产品文档更新*，网址为：http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html。

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

第 1 部分

ASA 使用入门

思科 ASA 简介

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

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

注 ASDM 支持很多 ASA 版本。ASDM 文档和联机帮助包含 ASA 支持的所有最新功能。如果您运行的是旧版 ASA 软件，该文档可能包含您的版本不支持的功能。同样，如果旧的主要或次要版本的维护版本中增加了某项功能， ASDM 文档中将包含该新功能，即使并非以后推出的所有新版 ASA 都提供该功能。请参阅每一章的功能历史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*》。另请参阅第 1-16 页的特殊服务、弃用的服务和传统服务。

ASDM 要求

ASDM 客户端操作系统和浏览器要求

表 1-1 列出了 ASDM 支持和推荐用于 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 • Vista • 2008 Server • XP	6.0 或更高版本	1.5 或更高版本	不支持	18.0 或更高版本	6.0 或更高版本
Apple OS X 10.4 及更高版本	不支持	1.5 或更高版本	2.0 或更高版本	18.0 或更高版本	6.0 或更高版本
Red Hat Enterprise Linux 5（GNOME 或 KDE）： • 桌面设备 • 带工作站的桌面设备	不适用	1.5 或更高版本	不适用	18.0 或更高版本	6.0 或更高版本

Java 和浏览器兼容性

表 1-2 列出了有关 Java、 ASDM 和浏览器兼容性的说明。

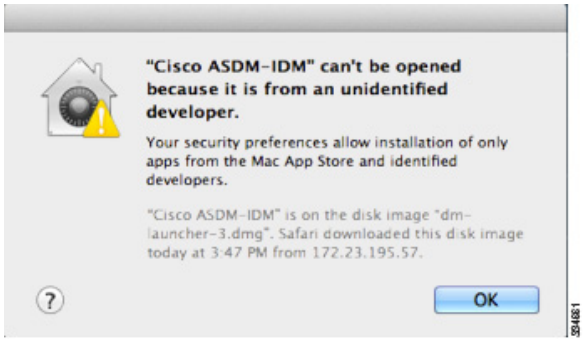
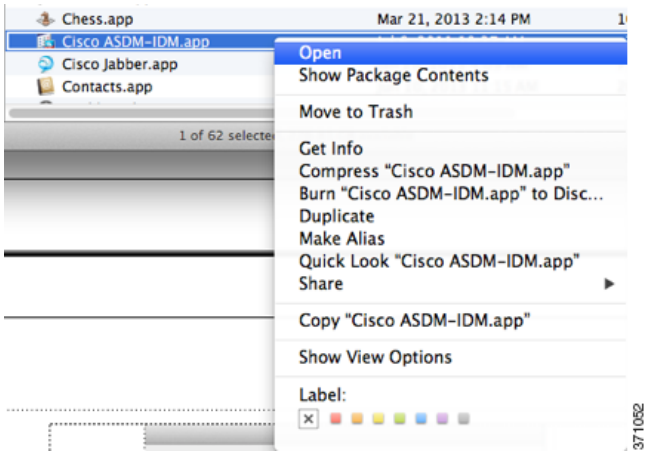
表 1-2　　ASDM 兼容性说明

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： • 在 ASA 上安装由已知 CA 颁发的可信证书。 • 安装自签名证书并使用 Java 进行注册。请访问 http://www.cisco.com/go/asdm-certificate。 • 将 Java 降级到 7 Update 45 或更低版本。 • 或者使用 Java Web Start。 **注**　Java 7 update 51 不支持 ASDM 7.1(5) 及更低版本。如果升级了 Java，但不再能够启动 ASDM 来将其升级到 7.2 版本，可以使用 CLI 来升级 ASDM，或者在 Java 控制面板中为要使用 ASDM 进行管理的每个 ASA 添加安全异常。请参阅“解决方法”一节，网址： http://java.com/en/download/help/java_blocked.xml 添加安全异常后，启动旧版 ASDM，然后升级到 7.2。
	很少情况下，使用 Java Web Start 时无法加载联机帮助	很少情况下，启动联机帮助时，浏览器窗口会加载，但内容不会显示。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**，再点击 **OK**。
7 update 45	使用不可信的证书时， ASDM 将显示一条有关缺失 “权限”属性的黄色警告	由于 Java 中存在漏洞，因此，如果没有在 ASA 上安装可信证书，JAR 清单中将会显示指出缺少权限属性的黄色警告。**可以忽略该警告**；ASDM 7.2 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　　ASDM 兼容性说明 （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。如果 ASA 只有基础加密许可证 (DES)，进而造成 SSL 连接只有弱加密密码，您将无法启动 ASDM。必须卸载 Java 7 并安装 Java 6 (http://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase6-419409.html)。请注意，弱加密和 Java 6 需要解决方法 （见本表的后面部分）。
6	用户名长度不能超过 50 个字符	由于 Java 存在漏洞，因此，使用 Java 6 时， ASDM 不支持长度超过 50 个字符的用户名。 Java 7 支持长度超过这个限制的用户名。
	ASA *或*解决方法需要有强加密许可证 (3DES/AES)	当您首次将浏览器连接到 ASA 以加载 ASDM 初始屏幕时，浏览器会尝试通过 SSL 连接到 ASA。如果 ASA 只有基础加密许可证 (DES)，进而造成 SSL 连接只有弱加密密码，您可能无法访问 ASDM 初始屏幕；大多数浏览器都不支持弱加密密码。因此，如果没有强加密许可证 (3DES/AES)，请采用以下解决方法之一： • 使用已经下载的 ASDM 启动程序或 Java Web Start 快捷方式（如果有）。ASDM 启动程序和 Web Start 快捷方式可与 Java 6 和弱加密配合使用，即使浏览器不会这样做。 • 对于 Windows Internet Explorer，可以启用 DES 作为解决方法。有关详细信息，请访问 http://support.microsoft.com/kb/929708。 • 对于任何操作系统上的 Firefox，可以启用 security.ssl3.dhe_dss_des_sha 设置作为解决方法。有关如何更改隐藏的配置首选项，请访问 http://kb.mozillazine.org/About:config。
全部	• 自签名证书或不可信的证书 • IPv6 • Firefox 和 Safari	如果 ASA 使用自签证书或不可信证书，Firefox 4 及更高版本和 Safari 无法在使用 HTTPS over IPv6 进行浏览时添加安全异常。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 错误启动。 • 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 错误启动”功能而无法启动 ASDM。我们建议重新启用这些算法之一（Configuration > Device Management > Advanced > SSL Settings 面板）；或者，可以使用 **--disable-ssl-false-start** 标志在 Chrome 中禁用 SSL 错误启动 （有关具体操作，请访问 http://www.chromium.org/developers/how-tos/run-chromium-with-flags）。
	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　　ASDM 兼容性说明　（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，将会出现错误屏幕。  1. 要允许 ASDM 运行，请右键单击（或按住 Ctrl 键并点击）**Cisco ASDM-IDM Launcher** 图标，然后选择 **Open**。  2. 将会出现一个类似的错误屏幕；但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，请通过以下链接参阅 *《思科 ASA 兼容性》*：
http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

VPN 兼容性

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

新功能

注　系统日志消息指南中列出了新的、有变化的以及已弃用的系统日志消息。

ASA 9.3(1) 版本 /ASDM 7.3(1) 版本的新功能

发布日期：2014 年 7 月 24 日

表 1-3 列出了 ASA 9.3(1) 版本 /ASDM 7.3(1) 版本的新功能。

表 1-3　ASA 9.3(1) 版本/ASDM 7.3(1) 版本的新功能

功能	说明
防火墙功能	
对 IPv6 的 SIP、 SCCP 和 TLS 代理支持	现在使用 SIP、 SCCP 和 TLS 代理 （使用 SIP 或 SCCP）时可检查 IPv6 流量。 我们未修改任何 ASDM 屏幕。
支持思科统一通信管理器 8.6	ASA 现在可与思科统一通信管理器 8.6 版本互操作（包括 SCCPv21 支持）。 我们未修改任何 ASDM 屏幕。
访问组和 NAT 的规则引擎事务提交模型	一经启用，规则更新在规则编译完成后即可得以应用；不会影响规则匹配性能。 我们引入了以下屏幕：**Configuration > Device Management > Advanced > Rule Engine**
远程访问功能	
XenDesktop 7 对无客户端 SSL VPN 的支持	我们已添加 XenDesktop 7 对无客户端 SSL VPN 的支持。现在，通过自动登录创建书签时，可以指定登录页面 URL 或控制 ID。 我们修改了以下屏幕：**Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**

表 1-3　　ASA 9.3(1) 版本/ASDM 7.3(1) 版本的新功能 （续）

功能	说明
Mobile Enablement Proxy	Mobile Enablement Proxy 是 ISE Mobile Enablement 解决方案的组件，允许外部移动设备以与内部移动设备完全相同的方式参与移动设备管理。 **注**　在即将于 2015 年年初推出的 ISE 中，Mobile Enablement Proxy 要求有 ISE 支持。 我们引入了以下屏幕：**Configuration > Remote Access VPN > AAA/Local Users > MDM Proxy**
AnyConnect 自定义属性增强	自定义属性定义并配置未融入 ASA 的 AnyConnect 功能，如延迟升级。自定义属性配置已得到增强，以允许多个值和更长的值，而且现在需要其类型、名称和值的规格。现在可将其添加至动态访问策略和组策略。升级到 9.3.x 后，以前定义的自定义属性将更新至此增强配置格式。 我们引入或修改了以下屏幕： **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes** **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names** **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced > AnyConnect Client > Custom Attributes** **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add/Edit > AnyConnect Custom Attributes**
桌面平台的 AnyConnect Identity Extensions (ACIDex)	ACIDex，也称为 AnyConnect Endpoint Attributes 或 Mobile Posture，是 AnyConnect VPN 客户端用于向 ASA 传递状况信息的方法。动态访问策略使用这些终端属性向用户进行授权。 现在，AnyConnect VPN 客户端可为桌面操作系统（Windows、Mac OS X 和 Linux）提供平台识别和可供 DAP 使用的 MAC 地址池。 我们修改了以下屏幕：**Configuration > Remote Access VPN > Dynamic Access Policies > Add/Edit > Add/Edit (endpoint attribute)**，对于 **Endpoint Attribute Type**，请选择 **AnyConnect**。其他操作系统位于 **Platform** 下拉列表中，而且 MAC 地址已更改为 **Mac Address Pool**。
VPN 的 TrustSec SGT 分配	现在，远程用户连接时， TrustSec 安全组标记 (SGT) 可添加至 ASA 上的 SGT-IP 表。 我们引入或修改了以下屏幕： **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Edit User > VPN Policy** **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add a Policy**
高可用性功能	
改进了对集群中模块运行状况监控的支持	我们增加了对集群中模块运行状况监控的改进支持。 我们未修改任何 ASDM 屏幕。
禁用硬件模块的运行状况监控	默认情况下， ASA 监控已安装的硬件模块 （例如 ASA FirePOWER 模块）的运行状况。如果您不希望硬件模块故障触发故障转移，可以禁用模块监控。 我们修改了以下屏幕：**Configuration > Device Management > High Availability and Scalability > Failover > Interfaces**

表 1-3　　ASA 9.3(1) 版本/ASDM 7.3(1) 版本的新功能 （续）

功能	说明
平台功能	
ASP 负载均衡	**asp load-balance per-packet** 命令中的新 **auto** 选项使 ASA 能够自适应地在每个接口接收环上打开和关闭 ASP 每数据包负载均衡。这一自动机制可检测是否引入了不对称流量，且有助于避免以下问题： • 因偶发的流量高峰而造成溢出 • 因大量流量过度订用特定接口接收环而造成溢出 • 因相对严重过载的接口接收环而造成溢出 （这种情况下，一个核心无法维持负载） 我们未修改任何 ASDM 屏幕。
SNMP MIB	CISCO-REMOTE-ACCESS-MONITOR-MIB 现在支持 ASASM。
接口功能	
透明模式的网桥组最大数量增加到 250	网桥组最大数量从 8 增加到 250。在单情景模式和多情景模式的每个情景中，最多可配置 250 个网桥组，每组最多 4 个接口。 我们修改了以下屏幕： **Configuration > Device Setup > Interfaces** **Configuration > Device Setup > Interfaces > Add/Edit Bridge Group Interface** **Configuration > Device Setup > Interfaces > Add/Edit Interface**
路由功能	
ASA 集群的 BGP 支持	我们增加了对 BGP 用于 ASA 集群的支持。 我们修改了以下屏幕：**Configuration > Device Setup > Routing > BGP > IPv4 Family > General**
不间断转发的 BGP 支持	我们增加了 BGP 不间断转发支持。 我们修改了以下屏幕： **Configuration > Device Setup > Routing > BGP > General** **Configuration > Device Setup > Routing > BGP > IPv4 Family > Neighbor** **Monitoring > Routing > BGP Neighbors**
通告映射的 BGP 支持	我们添加了对 BGPv4 通告映射的支持。 我们修改了以下屏幕：**Configuration > Device Setup > Routing > BGP > IPv4 Family > Neighbor > Add BGP Neighbor > Routes**
对不间断转发 (NSF) 的 OSPF 支持	添加了对 NSF 的 OSPFv2 和 OSPFv3 支持。 我们添加了以下屏幕： **Configuration > Device Setup > Routing > OSPF > Setup > NSF Properties** **Configuration > Device Setup > Routing > OSPFv3 > Setup > NSF Properties**

表 1-3　　ASA 9.3(1) 版本/ASDM 7.3(1) 版本的新功能 （续）

功能	说明
AAA 功能	
第 2 层安全组标记施加	现在，您可以使用结合了以太网标记的安全组标记来实施策略。 SGT 加以太网标记，也称为第 2 层 SGT 强制，使 ASA 能够使用思科专有以太网帧 (Ether Type 0x8909) 在千兆以太网接口上发送和接收安全组标记，从而将源安全组标记插入纯文本以太网帧。 我们修改了以下屏幕： **Configuration > Device Setup > Interfaces > Add Interface > Advanced** **Configuration > Device Setup > Interfaces > Add Redundant Interface > Advanced** **Configuration > Device Setup > Add Ethernet Interface > Advanced** **Wizards > Packet Capture Wizard** **Tools > Packet Tracer**
AAA Windows NT 域身份验证移除	我们移除了对于远程访问 VPN 用户的 NTLM 支持。 我们修改了以下屏幕：**Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups > Add AAA Server Group**
ASDM 身份证书向导	使用当前的 Java 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。 ASDM 身份证书向导使创建自签名身份证书变得简单。首次启动 ASDM 且没有可信证书时，系统提示通过 Java Web Start 启动 ASDM；这个新向导会自动启动。创建身份证书后，需要将身份证书注册至 Java 控制面板。有关说明，请参阅 https://www.cisco.com/go/asdm-certificate。 我们添加了以下屏幕：**Wizards > ASDM Identity Certificate Wizard**
监控功能	
监控物理接口的汇聚流量	**show traffic** 命令输出已经更新，包括物理接口信息的汇聚流量。要启用该功能，必须先输入 **sysopt traffic detailed-statistics** 命令。

ASA 服务模块如何与交换机配合使用

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

注　不支持 Catalyst 操作系统 (OS)。

ASA 运行自己的操作系统。

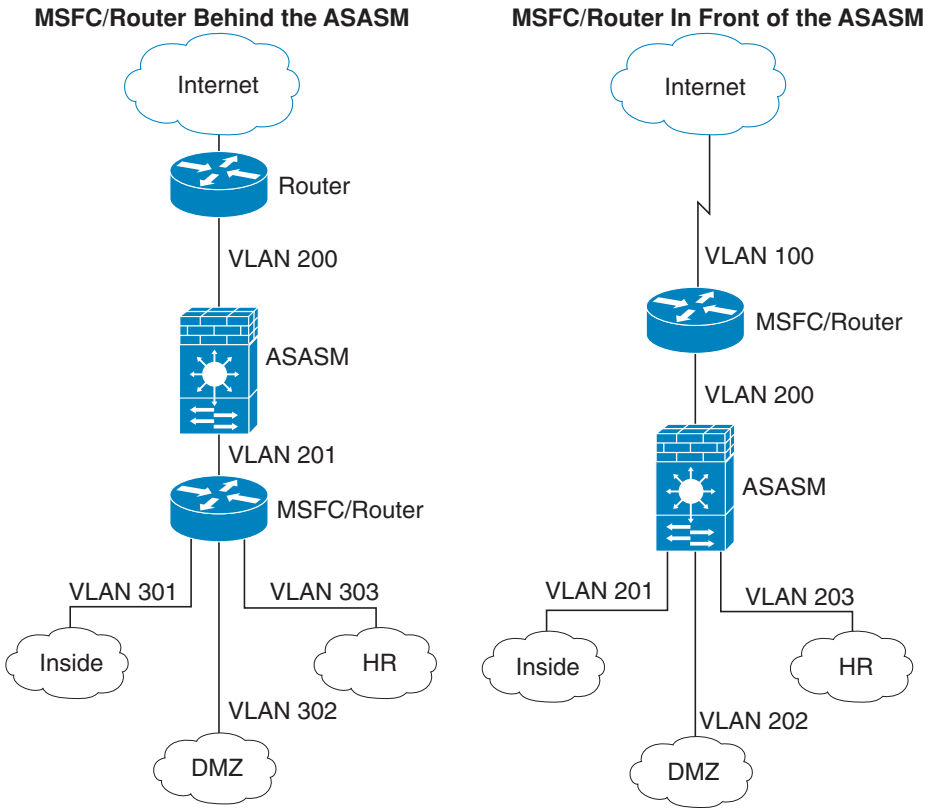
交换机由一个交换处理器 （管理引擎）和一个路由器 (MSFC) 组成。虽然需要将 MSFC 作为系统的一部分，但并不一定要使用它。如果选择使用 MSFC，可以向 MSFC 分配一个或多个 VLAN 接口。或者，可以使用外部路由器来代替 MSFC。

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

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

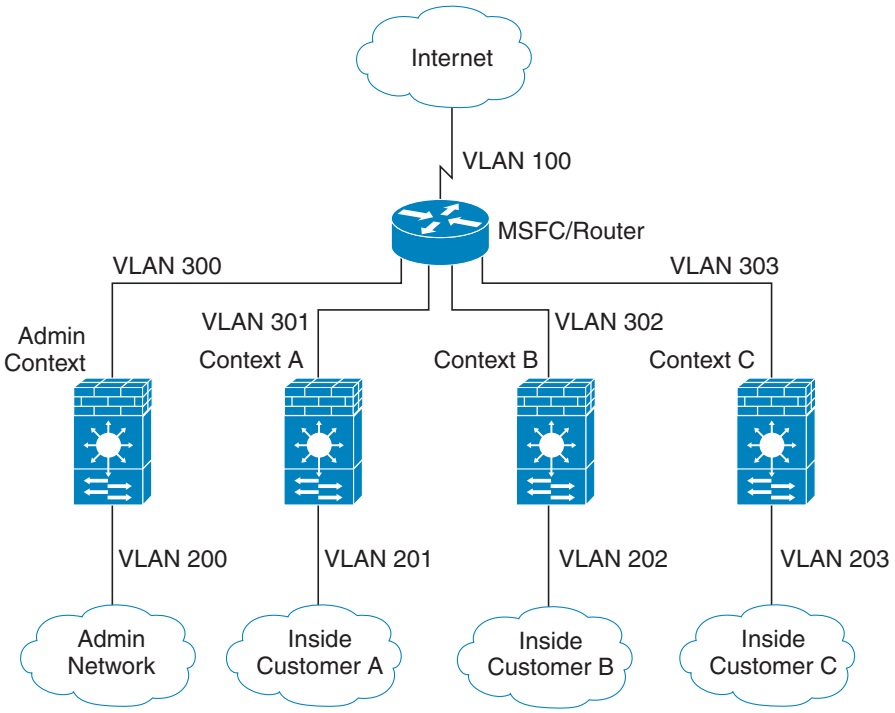
在左侧的示例中，MSFC 或路由器在 VLAN 201、301、302 与 303 之间路由，且没有内部流量可以通过 ASASM，除非是流向互联网的内部流量才可以通过。在右侧的示例中，ASASM 处理和保护内部 VLAN 201、 202 与 203 之间的所有流量。

图 1-1　　MSFC/ 路由器的放置



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

图 1-2　　多情景模式中 MSFC/ 路由器的放置



防火墙功能概述

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

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

- 第 1-12 页的安全策略概述
- 第 1-14 页的防火墙模式概述
- 第 1-14 页的状态检测概述

安全策略概述

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

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，还可以应用以太网类型访问列表来允许非 IP 流量。

应用 NAT

NAT 的其中一些优点包括：

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

保护 IP 分片

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

对直通流量使用 AAA

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

应用 HTTP、 HTTPS 或 FTP 过滤

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

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

运用应用检测

对于在用户数据包嵌入 IP 寻址信息的服务或在动态分配端口上打开辅助信道的服务，需要使用检测引擎。这些协议要求 ASA 执行深度数据包检测。

向受支持的硬件或软件模块发送流量

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

应用 QoS 策略

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

应用连接限制和 TCP 规范化

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

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

启用威胁检测

可以配置扫描威胁检测和基本威胁检测，还可以配置如何使用统计数据来分析威胁。

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

典型的扫描攻击包括测试子网中每个 IP 地址的可访问性的主机 （通过扫描子网中的很多主机或清扫主机或子网中的很多端口）。扫描威胁检测功能确定主机何时执行扫描。与基于流量签名的 IPS 扫描检测不同， ASA 扫描威胁检测功能维护一个包含主机统计数据的庞大数据库；可以分析这些统计数据以执行扫描活动。

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

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

启用僵尸网络流量过滤器

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

配置思科统一通信

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

防火墙模式概述

ASA 在两种不同的防火墙模式中运行：

- 路由
- 透明

在路由模式中， ASA 被视为网络中的路由器跃点。

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

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

状态检测概述

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

注　TCP 状态绕过功能使您可以自定义数据包流量。

但是，状态防火墙 （例如 ASA）会考虑到数据包的状态：

- 这是新连接吗？

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

  会话管理路径负责执行以下任务：

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

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

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

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

- 这是已建立的连接吗？

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

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

  需要第 7 层检测的协议的数据包也可以通过快速路径。

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

VPN 功能概述

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

ASA 执行以下功能：

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

ASA 调用各种标准协议来实现这些功能。

安全情景概述

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

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

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

ASA 集群概述

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

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

特殊服务、弃用的服务和传统服务

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

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

- 第 1-16 页的特殊服务指南
- 第 1-16 页的弃用的服务
- 第 1-16 页的传统服务指南

特殊服务指南

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

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，但配置指南和联机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。

第 2 章

入门

本章介绍如何开始使用思科 ASA。

访问命令行界面的控制台

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。然后，可根据第 36 章，“管理访问”，使用 Telnet 或 SSH 配置远程访问。如果系统已处于多情景模式，则访问控制台端口会将您引导至系统执行空间。

注 有关 ASAv 控制台访问，请参阅 《ASAv 快速入门指南》。

访问设备控制台

按照以下步骤访问设备控制台。

操作步骤

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

有关控制台电缆的详细信息，请参阅 ASA 的硬件指南。

步骤 2　按 **Enter** 键查看以下提示符：

ciscoasa>

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

步骤 3　要访问特权 EXEC 模块，请输入以下命令：

```
ciscoasa> enable
```

系统将显示以下提示符：

```
Password:
```

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

步骤 4　在提示符处输入启用密码。

默认情况下，密码为空，可按 **Enter** 键继续。要更改启用密码，请参阅第 14-1 页的设置主机名、域名及启用和 Telnet 密码。

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
```

提示符将会变为以下形式：

```
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，只需依次连接到交换机（至控制台端口或使用 Telnet 或 SSH 远程连接）和 ASASM。ASASM 不包括出厂默认配置，因此，必须先在 CLI 执行某一配置，然后才能使用 ASDM 访问该配置。本节介绍如何访问 ASASM CLI。

有关连接方法

从交换机 CLI，可使用两种方法连接到 ASASM：

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

  优势包括：

  - 连接在重新加载之间是持久性的，且不会超时。
  - 可在 ASASM 重新加载期间保持连接及查看启动消息。
  - 如果 ASASM 无法加载映像，则可访问 ROMMON。
  - 不需要初始密码配置。

  限制包括：

  - 连接缓慢 （9600 波特）。
  - 每次只能激活一个控制台连接。
  - 返回终端服务器提示符的转义序列为 **Ctrl-Shift-6**, **x** 时，不能与终端服务器一起使用该命令。 **Ctrl - Shift - 6**, **x** 也是 ASASM 控制台和返回交换机提示符的转义序列。因此，如果在这种情况下尝试退出 ASASM 控制台，反而会一直退回到终端服务器提示符。如果将终端服务器重新连接到交换机，则 ASASM 控制台会话仍将处于活动状态；绝不能退出到交换机提示符。必须使用直接串行连接使控制台返回交换机提示符。在此情况下，要么更改终端服务器或 Cisco IOS 软件中的交换机转义字符，要么换用 Telnet **session** 命令。

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

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

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

  优势包括：

  - 可同时拥有多个与 ASASM 的会话。
  - Telnet 会话是快速连接。

  限制包括：

  - ASASM 重新加载时， Telnet 会话即被终止，并且可能会超时。
  - 您不能访问 ASASM，直到它完成加载；不能访问 ROMMON。
  - 必须先设置 Telnet 登录密码；没有默认密码。

登录 ASA 服务模块

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

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

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

操作步骤

步骤 1　从交换机执行以下操作之一：

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

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

  示例：

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

  对于 VSS 中的交换机，请输入 **switch** 参数。

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

  将访问用户 EXEC 模式。

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

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

  系统提示输入登录密码：

  ```
  ciscoasa passwd:
  ```

  示例：

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

  对于 VSS 中的交换机，请输入 **switch** 参数。

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

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

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

  将访问用户 EXEC 模式。

步骤 2　访问特权 EXEC 模式 （拥有最高权限级别）：

enable

示例：

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

在提示符处输入启用密码。默认情况下，密码为空。

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

- 第 36-1 页的配置 ASDM、 Telnet 或 SSH 的 ASA 访问
- 第 14-1 页的设置主机名、域名及启用和 Telnet 密码

注销控制台会话

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

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

操作步骤

步骤 1　要返回交换机 CLI，请键入以下信息：

Ctrl-Shift-6, **x**

您将返回交换机提示符：

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

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

断开活动控制台连接

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

操作步骤

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

```
Router# show users
```

例如，以下命令输出在模块插槽 2 中 0 行上显示用户 “con”：

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

步骤 2　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 特权或用户 EXEC 模式键入 **exit**。如果正处于配置模式，可重复输入 **exit**，直到退出 Telnet 会话。

您将返回交换机提示符：

```
asasm# exit
Router#
```

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

配置 ASDM 访问

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

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

使用出厂默认配置进行 ASDM 访问 （设备、 ASAv）

通过出厂默认配置， ASDM 连接已预配置默认网络设置。

操作步骤

步骤 1　使用以下接口和网络设置连接到 ASDM：

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

注　如果切换至多情景模式，则可使用上述网络设置从管理员情景访问 ASDM。

相关主题

- 第 2-14 页的出厂默认配置
- 第 7-14 页的启用或禁用多情景模式
- 第 2-11 页的启动 ASDM

为设备和 ASAv 自定义 ASDM 访问

如果*一个或多个*以下条件适用，可使用该操作步骤：

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

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

操作步骤

步骤 1　在控制台端口访问 CLI。

步骤 2　（可选）启用透明防火墙模式：

该命令可清除配置。

```
firewall transparent
```

步骤 3　配置 Management 接口

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

示例：

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

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

步骤 4　（对于直连管理主机）为管理网络设置 DHCP 池：

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

示例：

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

确保此范围内不包括管理地址。

步骤 5　（对于远程管理主机）配置管理主机路由：

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

示例：

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

步骤 6　为 ASDM 启用 HTTP 服务器：

http server enable

步骤 7　允许管理主机访问 ASDM：

http *ip_address mask interface_name*

示例：

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

步骤 8　保存配置：

write memory

步骤 9　（可选）将模式设置为多模式：

mode multiple

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

示例

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

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

相关主题

- 第 2-14 页的还原出厂默认配置
- 第 5-8 页的设置防火墙模式 （单模式）
- 第 2-2 页的访问设备控制台
- 第 2-11 页的启动 ASDM
- 第 7 章，“ 多情景模式 ”

为 ASA 服务模块配置 ASDM 访问

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

准备工作

根据 《ASASM 快速入门指南》将 VLAN 接口分配至 ASASM。

操作步骤

步骤 1　连接到 ASASM 并访问全局配置模式。

步骤 2　（可选）启用透明防火墙模式：

```
firewall transparent
```

该命令可清除配置。

步骤 3　视乎您的模式，执行以下操作之一，以配置管理接口：

- 路由模式 - 在路由模式中配置接口：

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

示例：

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

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

- 透明模式 - 配置网桥虚拟接口并分配管理 VLAN 至网桥组：

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

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

示例：

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

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

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

步骤 4　（对于直接管理主机）为管理接口网络上的管理主机启用 DHCP：

dhcpd address *ip_address-ip_address interface_name*
dhcpd enable *interface_name*

示例：

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

确保此范围内不包括管理地址。

步骤 5　（对于远程管理主机）配置管理主机路由：

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

示例：

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

步骤 6　为 ASDM 启用 HTTP 服务器：

http server enable

步骤 7　允许管理主机访问 ASDM：

http *ip_address mask interface_name*

示例：

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

步骤 8　保存配置：

write memory

步骤 9　（可选）将模式设置为多模式：

mode multiple

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

示例

以下路由模式配置可配置 VLAN 1 接口并为管理主机启用 ASDM：

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

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

```
firewall transparent
interface bvi 1
    ip address 192.168.1.1 255.255.255.0
interface vlan 1
    bridge-group 1
    nameif inside
    security-level 100
```

```
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

相关主题

- 第 2-2 页的访问 ASA 服务模块控制台
- 第 7 章，“ 多情景模式 ”
- 第 5-8 页的设置防火墙模式 （单模式）

启动 ASDM

可使用以下两种方法启动 ASDM：

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

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

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

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

操作步骤

步骤 1　在指定为 ASDM 客户端的个人电脑上，输入以下 URL：

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

系统将显示 ASDM 启动页面和以下按钮：

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

步骤 2　要下载启动程序，请执行以下操作：

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

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

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

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

步骤 3　要使用 Java Web Start，请执行以下操作：

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

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

c. 从该快捷方式启动 Java Web Start。

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

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

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 的自签名身份证书，并向 Java 注册证书。

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

在演示模式中使用 ASDM

ASDM 演示模式是一个单独安装的应用，借助该模式，无需实际设备就能运行 ASDM。在此模式中，可执行以下操作：

- 即使正在与实际设备交互，也能通过 VSDM 执行配置和选定的监控任务。
- 使用 ASDM 接口演示 ASDM 或 ASA 功能。
- 通过 CSC SSM 执行配置和监控任务。
- 获得模拟的监控和日志记录数据，包括实时系统日志消息。显示的数据是随机生成的；但是，体验与您连接到实际设备时看到的情况相同。

该模式已经更新，可支持以下功能：

- 对于全局策略，支持单一路由模式中的 ASA 和入侵防御
- 对于 NAT 对象，支持单一路由模式中的 ASA 和防火墙 DMZ。
- 对于僵尸网络流量过滤器，支持单一路由模式中的 ASA 和安全情景。
- IPv6 的站点对站点 VPN （无客户端 SSL VPN 和 IPsec VPN）
- 混杂 IDS （入侵防御）
- 统一通信向导

该模式不支持以下方面：

- 保存 GUI 中显示的配置更改。
- 文件或磁盘操作。
- 历史监控数据。
- 非管理用户。

- 以下功能：
  - 文件菜单：
    Save Running Configuration to Flash
    Save Running Configuration to TFTP Server
    Save Running Configuration to Standby Unit
    Save Internal Log Buffer to Flash
    Clear Internal Log Buffer
  - 工具菜单：
    Command Line Interface
    Ping
    File Management
    Update Software
    File Transfer
    Upload Image from Local PC
    System Reload
  - Toolbar/Status bar > Save
  - Configuration > Interface > Edit Interface > Renew DHCP Lease
  - 故障转移后配置备用设备
- 导致配置重读的操作，其中， GUI 恢复为原始配置：
  - 交换情景
  - 在 Interface 窗格中进行更改
  - NAT 窗格更改
  - Clock 窗格更改

要在演示模式中运行 ASDM，请执行以下步骤。

操作步骤

步骤 1　从以下位置下载 ASDM 演示模式安装程序 asdm-demo-*version*.msi：
http://www.cisco.com/cisco/web/download/index.html。

步骤 2　双击安装程序以安装软件。

步骤 3　双击桌面上的 **Cisco ASDM Launcher** 快捷方式或从 **Start** 菜单将其打开。

步骤 4　选中 **Run in Demo Mode** 复选框。
系统将显示 **Demo Mode** 窗口。

出厂默认配置

出厂默认配置是思科应用于新 ASA 的配置。

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

出厂默认配置仅可用于路由防火墙模式和单一情景模式。

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

- 第 2-14 页的还原出厂默认配置
- 第 2-15 页的还原 ASAv 部署配置
- 第 2-16 页的 ASA 设备默认配置
- 第 2-16 页的 ASAv 部署配置

还原出厂默认配置

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

注　在 ASASM 上，还原出厂默认配置即可轻松擦除配置；无出厂默认配置。

准备工作

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

操作步骤

步骤 1　在主 ASDM 应用窗口，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）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**。

系统将显示确认对话框。

注　该操作还可清除启动映像位置（如存在）以及其余配置。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。下次在还原出厂配置后重新加载 ASA 时，它将从内部闪存的第一个映像启动；如果*内部*闪存中无映像， ASA 将不启动。

步骤 5　点击 **Yes**。

步骤 6　还原默认配置后，将该配置保存到内部闪存。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，即使之前已配置另一个位置。配置清除后，该路径也将清除。

还原 ASAv 部署配置

本节介绍如何还原 ASAv 部署配置。

操作步骤

步骤 1　为了执行故障转移，请关闭备用设备。

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

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

```
write erase
```

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

请勿保存该配置。

步骤 3　重新加载 ASAv，并加载部署配置：

```
reload
```

步骤 4　为了执行故障转移，请开启备用设备。

主用设备重新加载后，开启备用设备。部署配置将同步备用设备。

ASA 设备默认配置

ASA 设备的默认出厂配置可配置以下方面：

  - 管理接口 - Management 0/0 （管理）。
- IP 地址 - 管理地址为 192.168.1.1/24。
- DHCP 服务器 - 已为管理主机启用，以便连接到管理接口的个人电脑可接收介于 192.168.1.2 和 192.168.1.254 之间的地址。
- ASDM 访问 - 允许访问管理主机。

该配置包括以下命令：

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

ASAv 部署配置

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

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

有关独立设备，请参阅以下配置：

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

有关故障转移对中的主要设备，请参阅以下配置：

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

开始配置

要配置和监控 ASA，请执行以下步骤：

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

步骤 2　要使用 IPsec VPN 向导配置 IPSec VPN 连接，请选择 **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。

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。

注　ASDM 最多可支持 512 KB 配置。如果超出此量，可能会遇到性能问题。

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以及其他相关信息。
- 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，请使用关键字 **noconfirm**（如可用），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 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，请选择 **Monitoring > Properties > Device Access**。

操作步骤

步骤 1　在主 ASDM 应用窗口中，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，为该功能提供上下文相关帮助。取消选中该复选框以禁用上下文相关帮助。

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移除这些命令。有关详细信息，请参阅第 3-30 页的不受支持的命令。

操作步骤

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

步骤 2　完成后点击 **OK**。

增加 ASDM 配置内存

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。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。

要增加 ASDM 堆内存大小，请通过执行以下操作步骤修改启动程序快捷方式。

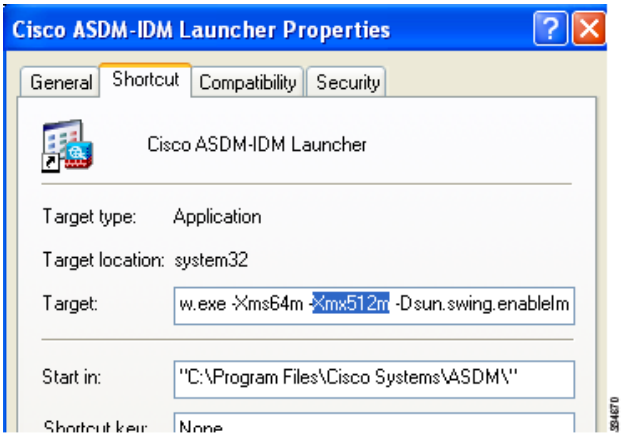
操作步骤

步骤 1　Windows：

a. 右键单击 ASDM-IDM 启动程序的快捷方式，然后选择 **Properties**。

b. 点击 **Shortcut** 选项卡。

c. 在 **Target** 字段中，将参数附上前缀 “-Xmx” 以指定所需的堆大小。例如，如需 768 MB 内存，请将参数更改为 -Xmx768M；如需 1 GB 内存，请将它更改为 -Xmx1G。



步骤 2　Macintosh：

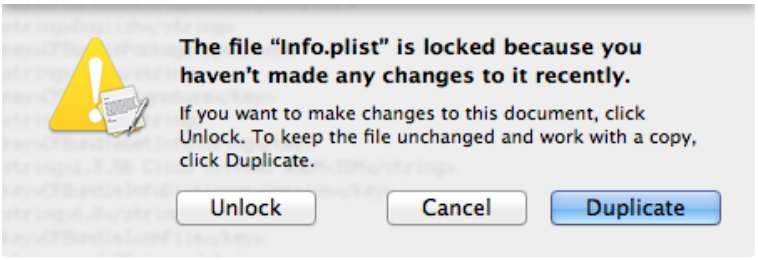
a. 右键单击 **Cisco ASDM-IDM** 图标，然后选择 **Show Package Contents**。

b. 在 **Contents** 文件夹中，双击 **Info.plist** 文件。如果已安装 Developer 工具，它会在 **Property List Editor** 中打开。否则，它将在 **TextEdit** 中打开。

c. 在 **Java > VMOptions** 下方，将字符串附上前缀 “- Xmx” 以指定所需堆的大小。例如，如需 768 MB 内存，请将字符串更改为 -Xmx768M；如需 1 GB 内存，请将它更改为 -Xmx1G。

```
<key>Java</key>
<dict>
        <key>WorkingDirectory</key>
        <string>$APP_PACKAGE/Contents/Resources/Java</string>
        <key>VMOptions</key>
        <string>-Xms64mm -Xmx512mm</string>
        <key>MainClass</key>
        <string>com.cisco.launcher.Launcher</string>
        <key>JVMVersion</key>
        <string>1.5+</string>
```

d. 如果该文件已锁定，则将看到以下错误：



e. 点击 **Unlock** 并保存文件。

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

将配置更改应用于连接

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

例如，如果要从接口移除 QoS **服务策略**，然后重新添加修改版本，则 **show service-policy** 命令仅显示与匹配新服务策略的新连接相关联的 QoS 计数器；旧策略的现有连接不再显示在命令输出中。

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，如连接限制和初始化限制。因此，该命令可移除使用那些限制的任何连接。要查看每台主机的所有当前连接，请参阅 **show local-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），请使用关键字 **all**。要清特定 IP 地址的出站或入站连接，请使用 *ip_address* 参数。

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

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

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

ASDM 图形用户界面

本章描述如何使用 ASDM 用户界面。

关于 ASDM 用户界面

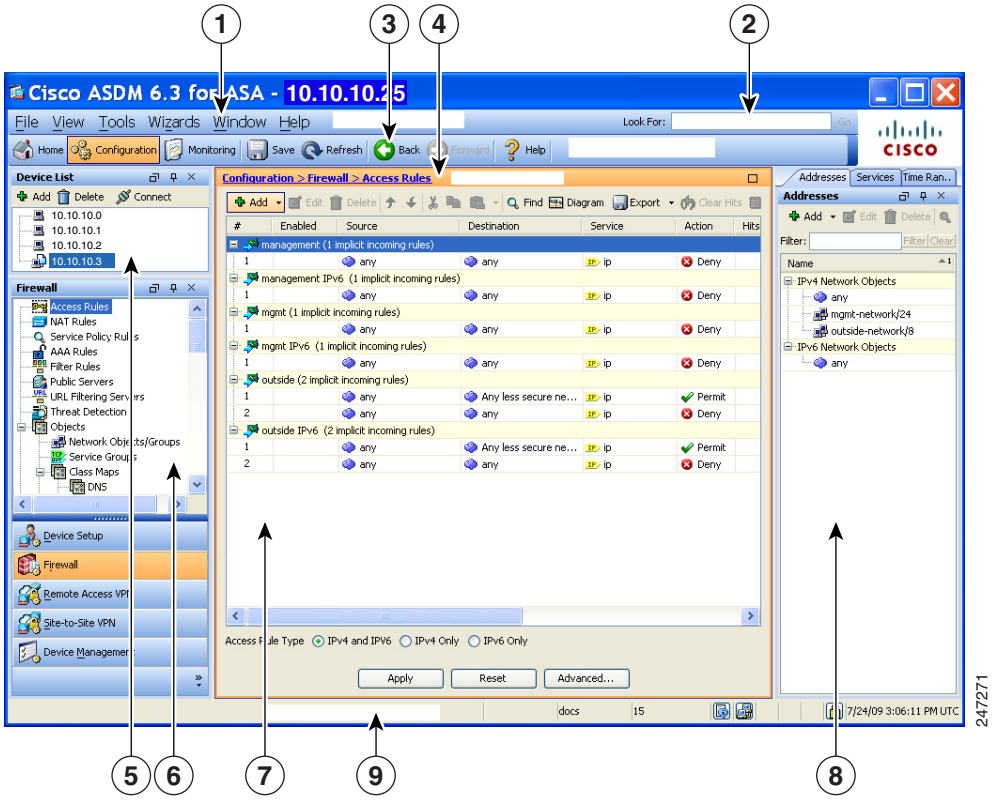
ASDM 用户界面专门用于提供对 ASA 支持的许多功能的轻松方法。 ASDM 用户界面包含以下元素：

- 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，支持对 ASDM 进行导航。从工具栏中，可以访问 **Home**、 **Configuration** 和 **Monitoring** 窗格。您还可以获取帮助并在窗格之间导航。

- 可停靠左**导航**窗格，用于浏览 **Configuration** 和 **Monitoring** 窗格。可以点击标题中的三个按钮之一以最大化或复原此窗格，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**导航**窗格中应用窗口左侧的链接。然后，**Content** 窗格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**导航**窗格中的任何链接。
- **Content** 窗格右上角的最大化和复原按钮，用于隐藏和显示左**导航**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。可以点击标题中的三个按钮之一以最大化或复原此窗格，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、特权级别和 SSL 状态。
- 左**导航**窗格，显示创建访问规则、NAT 规则、AAA 规则、过滤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**。

第 3-2 页的图 3-1 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	Device List 窗格
6	左导航窗格
7	内容窗格
8	右导航窗格
9	状态栏

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，可以使用上一节中描述的菜单、工具栏、可停靠窗格和左右**导航**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**
- **Trend Micro Content Security**
- **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** 以添加或移除按钮，然后点击要从显示的列表中添加或移除的按钮。

- 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

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，请参阅第 3-11 页的键盘快捷键。

ASDM 具有以下菜单：

File 菜单

通过 **File** 菜单可以管理 ASA 配置。下表列出可以使用 **File** 菜单执行的任务。

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。
Refresh	确保 ASDM 具有运行配置的当前副本。
Reset Device to the Factory Default Configuration	将配置复原为出厂默认值。
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	将主单元上运行配置文件的副本发送到故障转移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。

File 菜单项	说明
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。
Clear ASDM Cache	移除本地 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移除密码缓存。
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。下表列出可以使用 **View** 菜单执行的任务。

View 菜单项	说明
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。有关详细信息，请参阅第 3-10 页的 Device List。
Navigation	在 Configuration 和 Monitoring 视图中显示和隐藏**导航**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。有关详细信息，请参阅第 3-9 页的 ASDM Assistant。
SIP Details	显示和隐藏语音网络信息。
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。
Global Pools	显示和隐藏 **Global Pools** 窗格的显示。**Global Pools** 窗格仅适用于 Configuration 视图中的 **NAT Rules** 窗格。
Find in ASDM	查找您搜索的项，如功能或 **ASDM Assistant**。

View 菜单项	说明
Back	返回到上一个窗格。有关详细信息，请参阅第 3-10 页的常用按钮。
Forward	转至以前访问的下一个窗格。有关详细信息，请参阅第 3-10 页的常用按钮。
Reset Layout	将布局还原为默认配置。
Office Look and Feel	更改 Microsoft Office 设置的屏幕字体和颜色。

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	说明
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。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。有关详细信息，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。有关详细信息，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。有关详细信息，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。
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。
Check for ASA/ASDM Updates	通过向导 ASA 升级软件和 ASDM 软件。
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	复原 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 Alerts 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。有关详细信息，请参阅 《VPN 配置指南》。

Tools 菜单项	说明
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。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，请参阅第 3-28 页的定义 ASDM 首选项。
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。下表列出可用的向导及其功能。

Wizards 菜单项	说明
Startup Wizard	指导您分步完成 ASA 的初始配置。
IPsec VPN Wizard	支持在 ASA 上配置 IPsec VPN 策略。有关详细信息，请参阅《VPN 配置指南》。
SSL VPN Wizard	支持在 ASA 上配置 SSL VPN 策略。有关详细信息，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。有关详细信息，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。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。下表列出可以使用 **Help** 菜单执行的任务。

Help 菜单项	说明
Help Topics	打开新浏览器窗口，其中帮助按内容和窗口名称进行组织并在左框架中进行索引。使用这些方法查找有关任何主题的帮助，或者使用 **Search** 选项卡进行搜索。
Help for Current Screen	打开有关该屏幕的情景相关帮助。该向导运行当前打开的屏幕、窗格或对话框。或者，也可以点击**问号 (?) 帮助**图标。
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。
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。下表列出可以使用**工具栏**执行的任务。

工具栏按钮	说明
System/Contexts	显示处于哪个情景中。点击**向下**箭头在左侧窗格中打开情景列表，然后点击**向上**箭头复原情景下拉列表。展开此列表后，点击**向左**箭头折叠窗格，然后点击**向右**箭头复原窗格。从下拉列表中选择 **System** 以管理系统。从下拉列表中选择情景以管理该情景。
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。有关详细信息，请参阅第 3-14 页的 Home 窗格 （单一模式和情景）。在多模式中，系统没有 **Home** 窗格。
Configuration	配置 ASA。点击左**导航**窗格中的功能按钮以配置该功能。
Monitoring	监控 ASA。点击左**导航**窗格中的功能按钮以配置该功能。
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。
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。有关详细信息，请参阅第 3-9 页的 ASDM Assistant。

工具栏按钮	说明
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。
Save	仅对于可写访问的情景将运行配置保存到启动配置。
Help	显示当前打开的屏幕的情景相关帮助。

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。

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　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	故障转移单元的状态 （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 用户的特权。
Commands Ignored by ASDM	点击图标以显示配置中 ASDM 未处理的命令列表。将不从配置中移除这些命令。
Connection to Device	ASDM 到 ASA 的连接状态。有关详细信息，请参阅第 3-10 页的 Connection to Device。
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。

Connection to Device

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 会在配置期间打开另一个连接，然后将其关闭；但是，此对话框并不表示第二个连接。

Device List

Device List 是一个可停靠窗格。可以点击标题中的三个按钮之一以最大化或复原此窗格，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。可以使用此窗格切换到其他设备；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** 以从列表中移除所选设备。

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	放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	放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	从字段中移除信息，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

可以使用键盘来导航 ASDM 用户界面。

表 3-1 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
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

表 3-2 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	请按
下一个字段	Tab
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	Tab
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

表 3-3 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

表 3-4 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	Alt
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	Enter

大多数 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，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 “?”。* 与一个或多个字符相匹配，而 ? 与一个字符相匹配。 **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 和 Bolton
```

以下列表显示可在其中使用查找功能的 ASDM 窗格：

- **AAA Server Groups** 窗格
- **ACL Manager** 窗格 - ACL Manager 窗格中的查找功能不同于其他窗格中的查找功能。有关详细信息，请参阅第 3-13 页的 ACL Manager 窗格中的查找功能。
- **Certificate-to-Conn Profile Maps-Rules** 窗格

- **DAP** 窗格
- **Identity Certificates** 窗格
- **IKE Policies** 窗格
- **IPSec Proposals (Transform Sets)** 窗格
- **Local User** 窗格
- **Portal-Bookmark** 窗格
- **Portal-Customization** 窗格
- **Portal-Port Forwarding** 窗格
- **CA Certificates** 窗格
- **Portal-Smart Tunnels** 窗格
- **Portal-Web Contents** 窗格
- **VPN Connection Profiles** 窗格
- **VPN Group Policies** 窗格

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描述。某些屏幕阅读器 （如 JAWS）仅阅读具有焦点的屏幕对象。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描述。

要启用扩展屏幕阅读器支持，请执行以下步骤：

步骤 1　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**导航**窗格中显示子项的列表。可以点击子项的名称以转至该项。

关于 Help 窗口

要获取所需的信息，请点击下表中列出的适用按钮。

按钮	说明
About ASDM	显示有关 ASDM 的信息，包括使用的主机名、版本号、设备类型、 ASA 软件版本号、特权级别、用户名和操作系统。
Search	在联机帮助主题中搜索信息。
Using Help	描述最高效的使用联机帮助的方法。
Glossary	列出在 ASDM 和 ASA 中找到的术语。
Contents	显示目录。
Screens	按屏幕名称列出帮助文件。
Index	显示在 ASDM 联机帮助中找到的帮助主题的索引。

Home 窗格 （单一模式和情景）

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**。

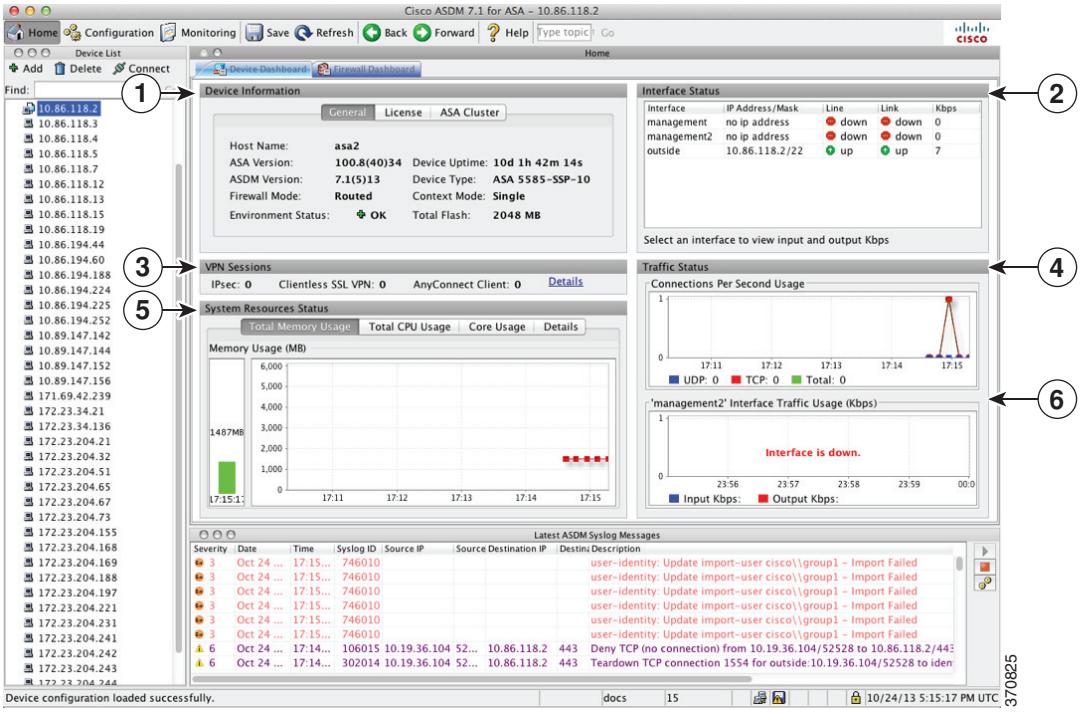
如果您在设备上安装有硬件或软件模块 （如 IPS 或 CX 模块），则对于这些模块存在单独的选项卡。

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。

图 3-2 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	第 3-16 页的 Device Information 窗格
2	第 3-17 页的 Interface Status 窗格
3	第 3-17 页的 VPN Sessions 窗格
4	第 3-17 页的 Traffic Status 窗格
5	第 3-17 页的 System Resources Status 窗格
6	第 3-17 页的 Traffic Status 窗格
-	第 3-10 页的 Device List
-	第 3-18 页的 Latest ASDM Syslog Messages 窗格

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。 ASA 5585-X 提供通过点击 **General** 选项卡中 **Environment Status** 标签右侧的加号 (+) 可获取的一组硬件统计信息。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。

  有关特定硬件统计的详细信息，请参阅特定设备的硬件指南。

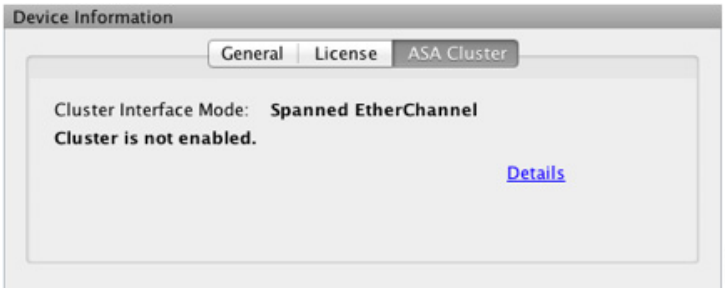
注　如果没有足够的内存升级到 ASA 的最新版本，则系统将显示 **Memory Insufficient Warning** 对话框。请按照此对话框中显示的指导以受支持的方式继续使用 ASA 和 ASDM。点击 **OK** 以关闭此对话框。

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** 以转至 **Monitoring > VPN > VPN Statistics > Sessions** 窗格。

Failover Status 窗格

此窗格显示故障转移状态。

点击 **Configure** 以启动 High Availability and Scalability Wizard。完成向导后，将显示故障转移配置状态 （Active/Active 或 Active/Standby）。

如果配置了故障转移，请点击 **Details** 以打开 **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。

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。

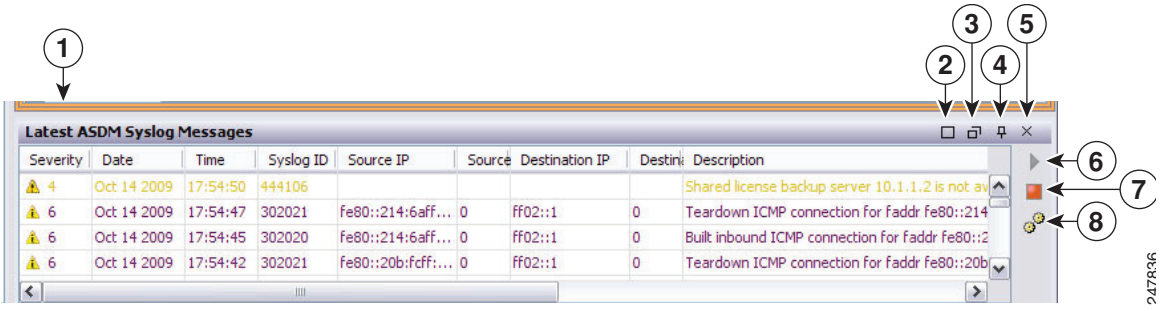
当配置包含多个最低安全级别接口，并且其中任何一个接口命名为 “outside” 时，该接口将用于流量吞吐量图形。否则， ASDM 从最低安全级别接口的字母顺序列表中选取第一个接口。

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	单击右侧的**过滤器**图标以打开 **Logging Filters** 窗格。

- 右键单击事件，然后选择 **Clear Content** 以清除当前消息。
- 右键单击事件，然后选择 **Save Content** 以将当前消息保存到 PC 上的文件。
- 右键单击事件，然后选择 **Copy** 以复制当前内容。
- 右键单击事件，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。在多情景模式中，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	第 3-20 页的 Traffic Overview 窗格
2	第 3-20 页的 Top 10 Access Rules 窗格
3	第 3-20 页的 Top Usage Status 窗格
（未显示）	第 3-21 页的 Top Ten Protected Servers Under SYN Attack 窗格
（未显示）	第 3-21 页的 Top 200 Hosts 窗格
（未显示）	第 3-21 页的 Top Botnet Traffic Filter Hits 窗格

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。运行时统计包含以下*仅显示*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 （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的 **Enable** 按钮。

在 Table 视图中，可以在列表中选择规则，然后右键单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。每个选项卡包含可启用各威胁检测服务的 **Enable** 按钮。可以根据防火墙配置指南将其启用。

Top 10 Services Enable 按钮同时启用端口和协议统计 （必须启用两者才会进行显示）。 **Top 10 Sources** 和 **Top 10 Destinations Enable** 按钮启用主机统计。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。

第四个选项卡 **Top 10 Users** 提供身份防火墙服务统计。身份防火墙服务基于用户的身份提供访问控制。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 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。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。

注意事项　启用统计可以影响 ASA 性能，视启用的统计类型而定。启用主机统计对性能有重大影响，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。不过，启用端口统计影响不大。

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。

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。您还可以查看历史采样数据。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。

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。

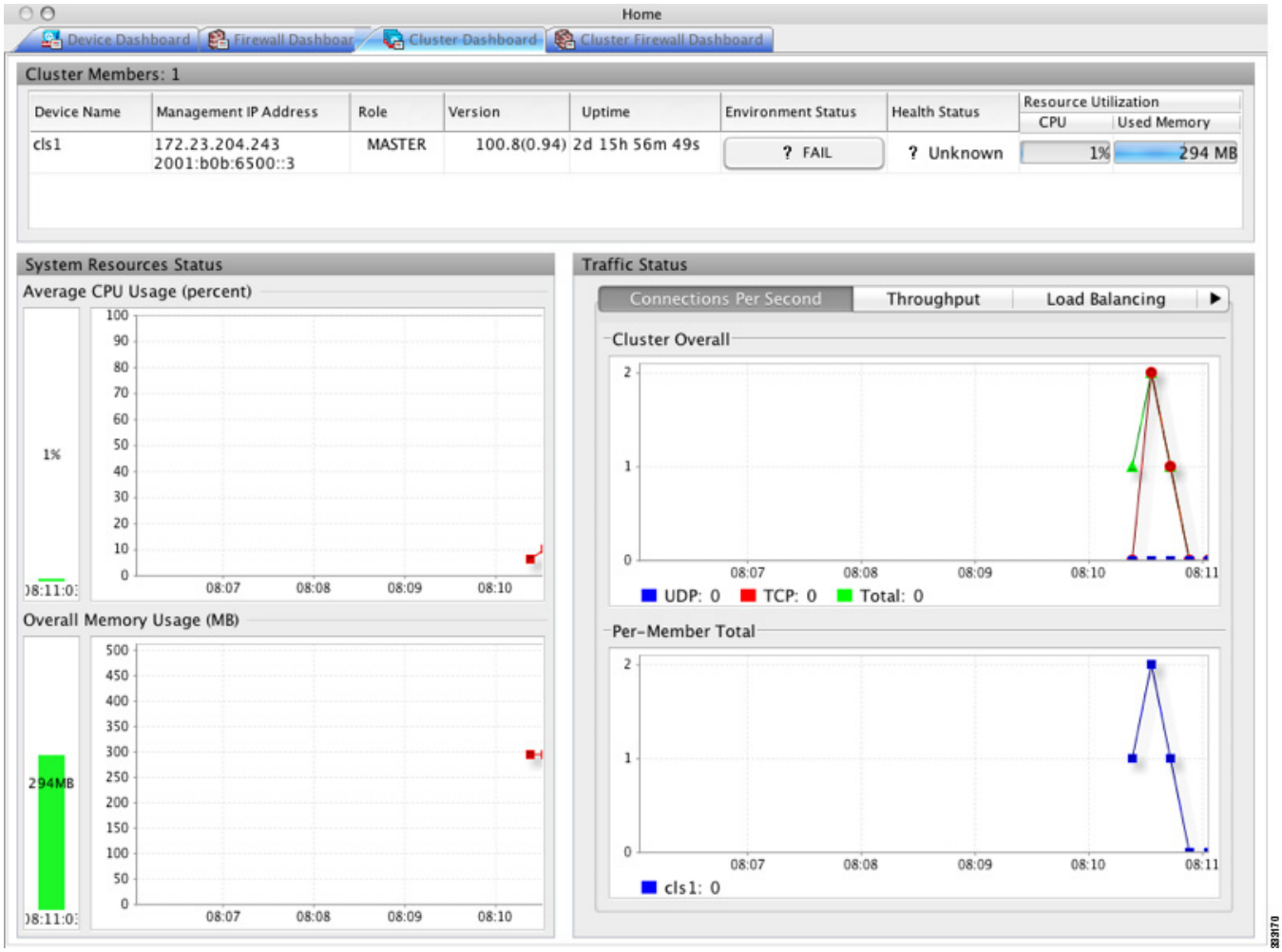
Top Botnet Traffic Filter Hits 窗格

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以来起算的前 10 项不匹配。如果右键单击 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。

有关详细信息，请参阅 《防火墙配置指南》。

Cluster Dashboard 选项卡

Cluster Dashboard 选项卡显示集群成员资格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）及其健康状态 （环境状态、健康状态和资源利用率）。

  注　在多情景模式中，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。

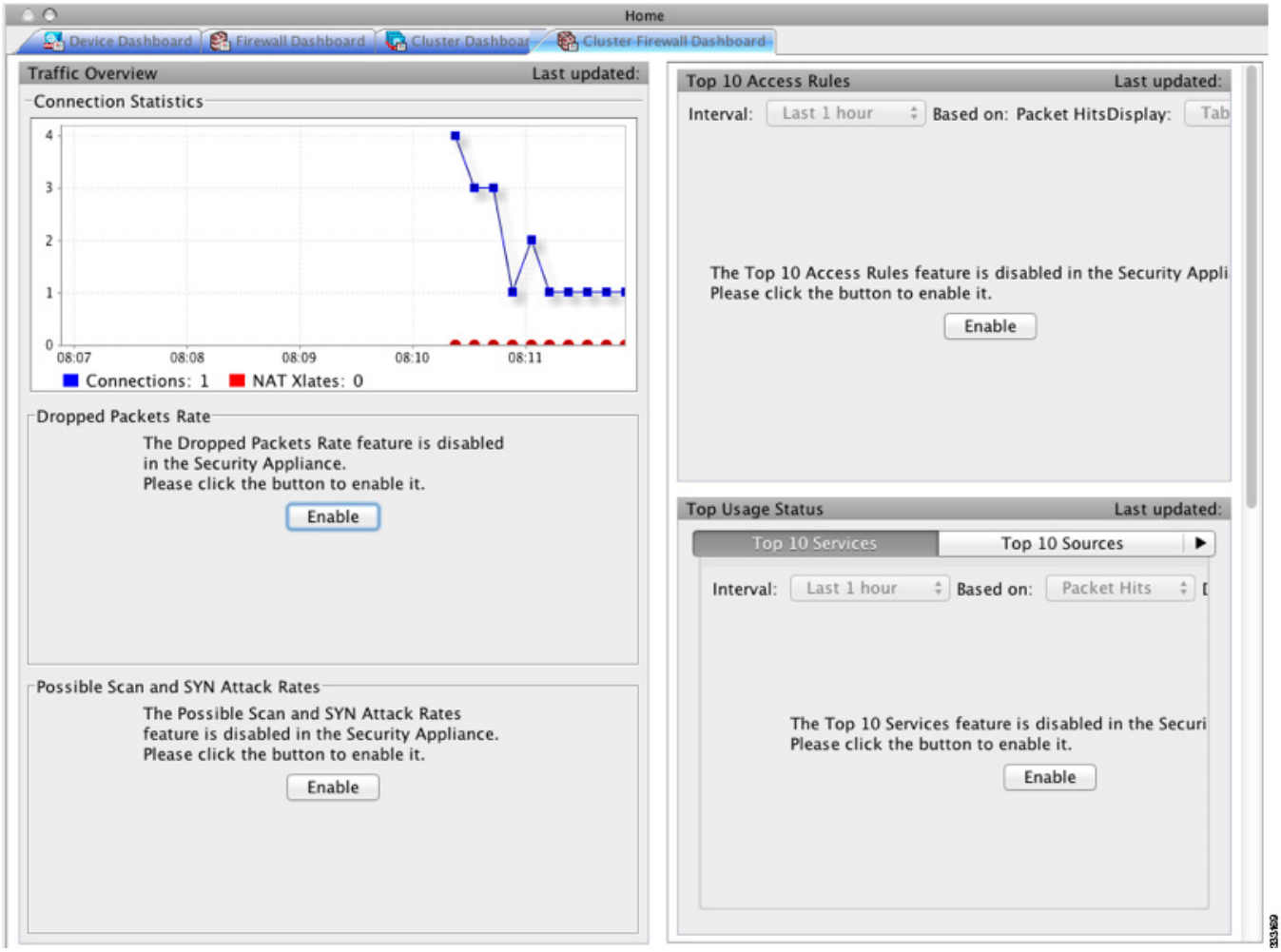
– **Control Link Usage** 选项卡：

  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，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。



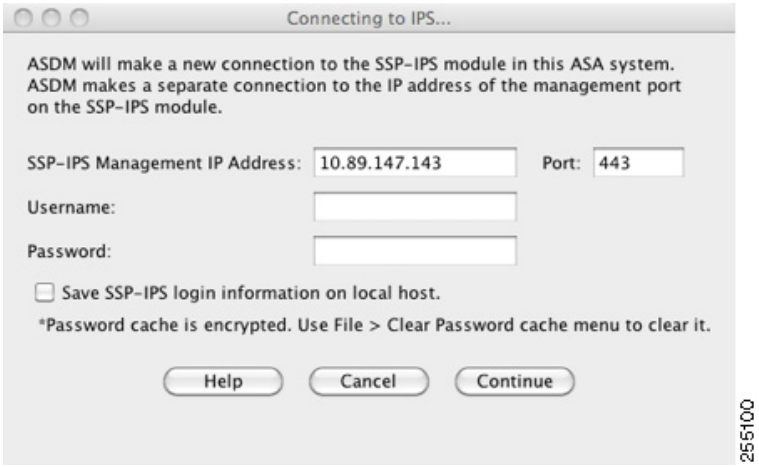
Intrusion Prevention 选项卡

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**。

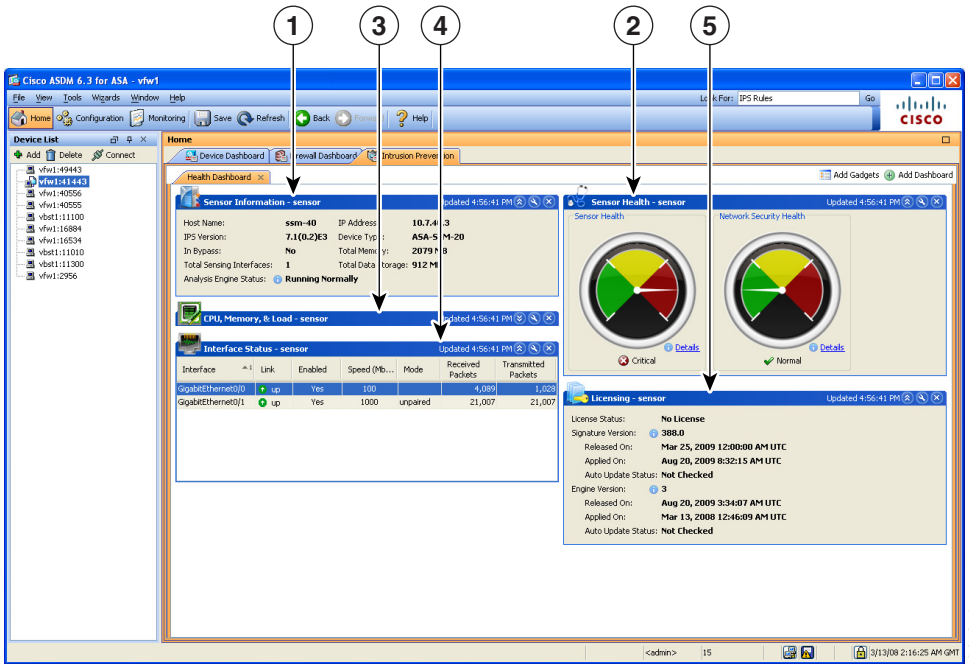
步骤 3　选中 **Save IPS login information on local host** 复选框以将登录信息保存在本地 PC 上。

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。

图 3-5 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)

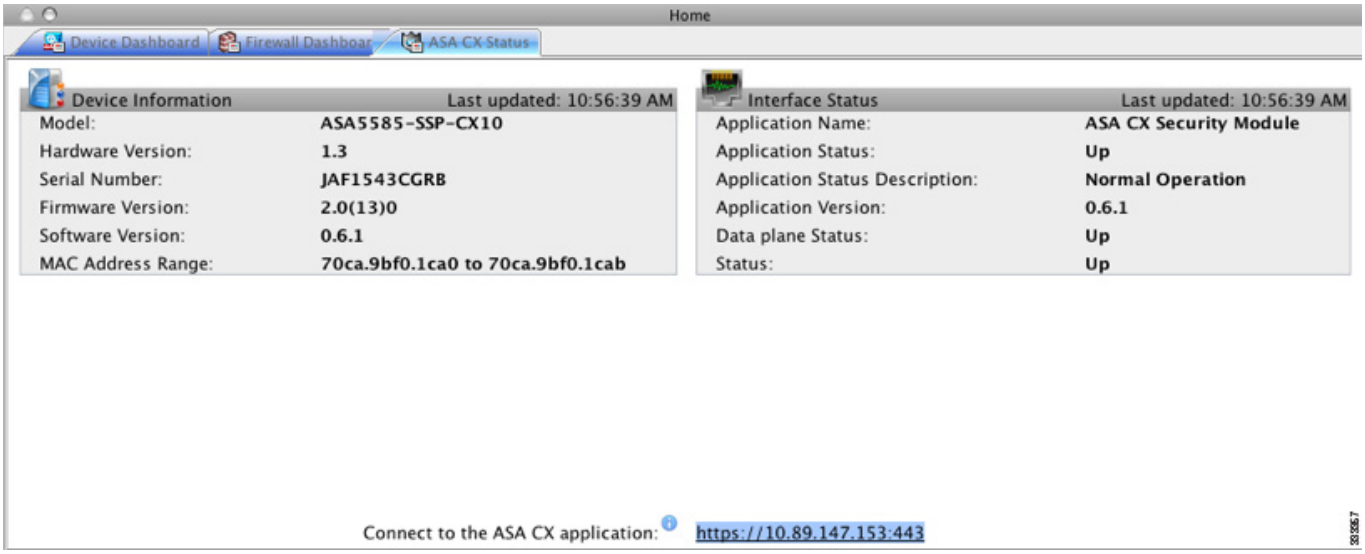


图例

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 Status 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）。如果模块注册到 FireSIGHT 管理中心，则可以点击链接以打开应用并执行进一步分析和模块配置。

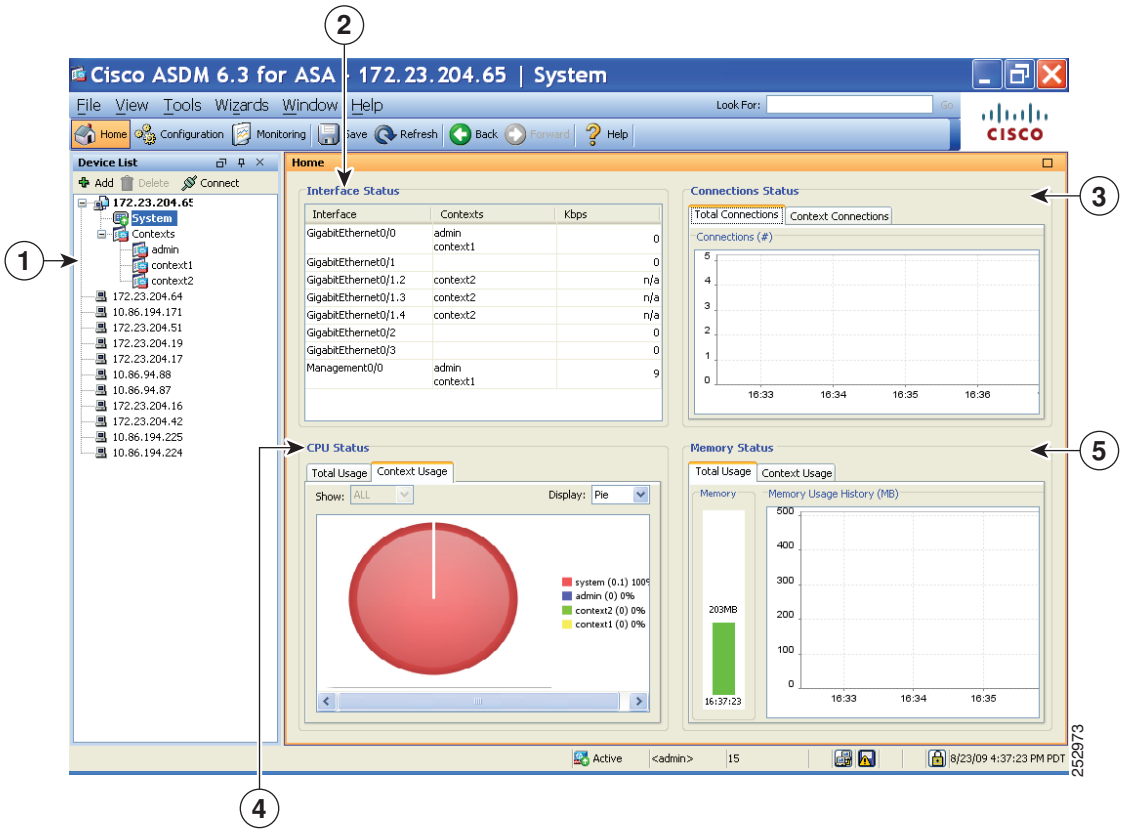
仅当您在设备中安装有 ASA FirePOWER 模块时，才会显示此选项卡。

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。

第 3-27 页的图 3-6 显示 System **Home** 窗格的元素。

图 3-6　　System Home 窗格



图例

GUI 元素	说明
1	System 与 Context 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

通过此功能可定义某些 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　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：

a. 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。

b. 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."
```

c. 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。

d. 选中 **Enable screen reader support (requires ASDM restart)** 复选框以使屏幕阅读器能够工作。必须重新启动 ASDM 才能启用此选项。

e. 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。

f. 选中 **Preview commands before sending them to the device** 复选框以查看由 ASDM 生成的 CLI 命令。

g. 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。

h. 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。

i. 要允许 **Packet Capture Wizard** 显示捕获的数据包，请输入网络探查器应用的名称，或者点击 **Browse** 以在文件系统中对其进行查找。

步骤 4　在 **Rules Table** 选项卡上，指定以下内容：

a. 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。

b. 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。

c. 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　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。

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。

注　此功能在 PIX 安全设备上不可用。

要查看 ASDM Assistant，请执行以下步骤：

步骤 1　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。

启用历史度量

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

要配置历史度量，请执行以下步骤：

步骤 1　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** 复选框以启用历史度量，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

表 3-5 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。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。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. 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

功能许可证

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

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

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

每个型号的受支持功能许可证

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

本节介绍适用于每个型号的功能许可证：

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

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

注　某些功能互不兼容。有关兼容性信息，请参阅个别功能章节。

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

有关许可证的详细信息，请参阅第 4-14 页的许可证说明。

ASA 5512-X

表 4-1　ASA 5512-X 许可证功能

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

表 4-1　　ASA 5512-X 许可证功能 （续）

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

ASA 5515-X

表 4-2　　ASA 5515-X 许可证功能

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

表 4-2　　ASA 5515-X 许可证功能 （续）

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

ASA 5525-X

表 4-3　　ASA 5525-X 许可证功能

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

ASA 5545-X

表 4-4　　ASA 5545-X 许可证功能

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

ASA 5555-X

表 4-5　　ASA 5555-X 许可证功能

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

带 SSP-10 的 ASA 5585-X

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

表 4-6　　带 SSP-10 的 ASA 5585-X 的许可证功能

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

带 SSP-20 的 ASA 5585-X

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

表 4-7　　带 SSP-20 的 ASA 5585-X 的许可证功能

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

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

带 SSP-40 和 -60 的 ASA 5585-X

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

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

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

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

ASA 服务模块

表 4-9　　ASASM 许可证功能

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

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

带 1 个虚拟 CPU 的 ASAv

表 4-10　　带 1 个虚拟 CPU 的 ASAv 的许可证功能

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

带 4 个虚拟 CPU 的 ASAv

表 4-11　　带 4 个虚拟 CPU 的 ASAv 的许可证功能

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

许可证说明

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

表 4-12　　许可证说明

许可证	备注
AnyConnect Essentials	AnyConnect Essentials 会话包括以下 VPN 类型： • SSL VPN • 使用 IKEv2 的 IPsec 远程访问 VPN 此许可证不支持基于浏览器 （无客户端）的 SSL VPN 访问或思科安全桌面。对于这些功能，请激活 AnyConnect Premium 许可证，而不是 AnyConnect Essentials 许可证。 **注**　借助 AnyConnect Essentials 许可证，VPN 用户可以使用网络浏览器来进行登录，然后下载并启动 (WebLaunch) AnyConnect 客户端。 AnyConnect 客户端软件提供一组相同的客户端功能，无论是通过此许可证，还是通过 AnyConnect Premium 许可证启用。 AnyConnect Essentials 许可证不能在给定 ASA 上与以下许可证同时处于活动状态：AnyConnect Premium 许可证 （所有类型）或高级终端评估许可证。然而，您可以在同一网络中的不同 ASA 上运行 AnyConnect Essentials 和 AnyConnect Premium 许可证。 默认情况下， ASA 使用 AnyConnect Essentials 许可证，但您可以通过先使用 **webvpn**，然后使用 **no anyconnect-essentials** 命令，或者在 ASDM 中使用 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials** 窗格来禁用该许可证，以便使用其他许可证。 另请参阅第 4-17 页的 VPN 许可证和功能兼容性。
AnyConnect for Cisco VPN Phone	通过与 AnyConnect Premium 许可证相结合，此许可证允许通过拥有内置 AnyConnect 兼容性的硬件 IP 电话进行访问。
AnyConnect for Mobile	此许可证允许运行 Windows Mobile 5.0、6.0 和 6.1 的触摸屏移动设备访问 AnyConnect 客户端。如果您希望支持对 AnyConnect 2.3 及以上版本进行移动访问，我们建议使用此许可证。此许可证要求激活以下任一许可证，以便指定允许的 SSL VPN 会话的总数：AnyConnect Essentials 或 AnyConnect Premium。 **移动安全状态支持** 实施远程访问控制和从移动设备收集安全状态数据，需要在 ASA 上安装有一个 AnyConnect Mobile 许可证和一个 AnyConnect Essentials 许可证或 AnyConnect Premium 许可证。此处为根据您所安装的许可证，可以获得的功能。 • AnyConnect Premium 许可证功能 – 在受支持的移动设备上，基于 DAP 属性和所有其他现有终端属性，实施 DAP 策略。这包括允许或拒绝来自移动设备的远程访问。 • AnyConnect Essentials 许可证功能 – 使用 ASDM，对每个组启用或禁用移动设备访问，并配置该功能。 – 显示有关通过 CLI 或 ASDM 连接的移动设备的信息，无需具有实施 DAP 策略，或者拒绝或允许对这些移动设备的远程访问的能力。
AnyConnect Premium	AnyConnect Premium 会话包括以下 VPN 类型： • SSL VPN • 无客户端 SSL VPN • 使用 IKEv2 的 IPsec 远程访问 VPN

表 4-12　　许可证说明 （续）

许可证	备注
AnyConnect Premium Shared	共享许可证允许 ASA 充当多个客户端 ASA 的共享许可证服务器。共享许可证池很大，但每个 ASA 使用的最大会话数，不能超过列出的永久许可证的最大数量。
僵尸网络流量过滤器	要下载动态数据库，需要有强加密 (3DES/AES) 许可证。
加密	无法禁用 DES 许可证。如果您安装了 3DES 许可证， DES 仍可用。您希望仅使用强加密时，要防止使用 DES，请确保配置所有相关命令，以便仅使用强加密。
公司间媒体引擎	当您启用公司间媒体引擎 (IME) 许可证时，可以使用的 TLS 代理会话数最多可为配置的 TLS 代理限制。如果您还安装了高于默认 TLS 代理限制的统一通信 (UC) 许可证，则 ASA 会将该限制设置为 UC 许可证限制与额外会话数 （取决于您的型号）之和。您可以使用 **tls-proxy maximum-sessions** 命令，或者在 ASDM 中使用 **Configuration > Firewall > Unified Communications > TLS Proxy** 窗格来手动配置 TLS 代理限制。要查看您的型号的限制，请输入 **tls-proxy maximum-sessions ?** 命令。如果您还安装了 UC 许可证，则可用于 UC 的 TLS 会话也可供 IME 会话使用。例如，如果配置的限制是 1000 个 TLS 代理会话，并且您购买了 750 个会话的 UC 许可证，则前 250 个 IME 会话不会影响可用于 UC 的会话。如果您需要超过 250 个会话用于 IME，则平台限制剩余的 750 个会话由 UC 和 IME 按照先到先得的原则使用。 • 对于以 “K8” 结尾的许可证部件号， TLS 代理会话数限于 1000 个。 • 对于以 “K9” 结尾的许可证部件号， TLS 代理限制取决于您的配置和平台型号。 **注**　K8 和 K9 是指许可证是否有出口限制：K8 为不受限制， K9 为受限制。 您也可将 SRTP 加密会话用于您的连接： • 对于 K8 许可证， SRTP 会话数限于 250 个。 • 对于 K9 许可证，没有限制。 **注**　仅需要对媒体进行加密 / 解密的呼叫会计入 SRTP 限制；如果将呼叫设置为直通，即使两端均为 SRTP，这些呼叫也不计入限制。
所有类型的接口，最大值	最大整合接口数量；例如， VLAN、物理、冗余、网桥组和 EtherChannel 接口。在配置中定义的每个 **interface** 均根据此限制进行计数。
IPS 模块	IPS 模块许可证允许您在 ASA 上运行 IPS 软件模块。您还需要 IPS 端有 IPS 签名订用。 请参阅以下准则： • 要购买 IPS 签名订用，您需要有预装了 IPS 的 ASA （部件号必须包括 “IPS”，例如 ASA5515-IPS-K9）；您不能为非 IPS 部件号 ASA 购买 IPS 签名订用。 • 对于故障转移，您需要两台设备上的 IPS 签名订用；由于此订用不是 ASA 许可证，因此不在故障转移中共享。 • 对于故障转移， IPS 签名订用要求每台设备具有唯一的 IPS 模块许可证。与其他 ASA 许可证一样， IPS 模块许可证在故障转移集群许可证中技术共享。但是，由于 IPS 签名订用要求，您必须为故障转移中的每台设备，购买单独的 IPS 模块许可证。
其他 VPN	其他 VPN Premium 会话包括以下 VPN 类型： • 使用 IKEv1 的 IPsec 远程访问 VPN • 使用 IKEv1 的 IPsec 站点对站点 VPN • 使用 IKEv2 的 IPsec 站点对站点 VPN 此许可证包括在基础许可证中。

表 4-12　许可证说明 （续）

许可证	备注
整合所有类型的 VPN 总数 （会话）	• 虽然最大总计 VPN 会话数超过最大 VPN AnyConnect 和其他 VPN 会话数，整合的会话数不应超过 VPN 会话限制。如果您超过了最大 VPN 会话数，则可能会使 ASA 过载，因此请务必正确设置网络规模。 • 如果您启动无客户端 SSL VPN 会话，并通过门户启动 AnyConnect 客户端会话，则总共使用了 1 个会话。但是，如果先启动 AnyConnect 客户端 （例如，通过独立客户端），然后登录无客户端 SSL VPN 门户，则使用了 2 个会话。
UC 电话代理会话， UC 代理会话总数	以下应用将 TLS 代理会话用于其连接。这些应用 （而且仅这些应用）使用的每个 TLS 代理会话都会计入 UC 许可证限制： • 电话代理 • 状态联合代理 • 加密语音检查 使用 TLS 代理会话的其他应用不计入 UC 限制，例如，移动优势代理 （无需许可证）和 IME （需要单独的 IME 许可证）。 有些 UC 应用可能将多个会话用于一个连接。例如，如果您用主和备用思科统一通信管理器配置电话，由于存在 2 个 TLS 代理连接，因此会使用 2 个 UC 代理会话。 您可以使用 **tls-proxy maximum-sessions** 命令，或者在 ASDM 中使用 **Configuration > Firewall > Unified Communications > TLS Proxy** 窗格来单独配置 TLS 代理限制。要查看您的型号的限制，请输入 **tls-proxy maximum-sessions ?** 命令。当您应用高于默认 TLS 代理限制的 UC 许可证时，ASA 会自动设置 TLS 代理限制以匹配 UC 限制。TLS 代理限制优先于 UC 许可证限制；如果您将 TLS 代理限制设置为低于 UC 许可证，则您可能无法使用 UC 许可证中的所有会话。 **注**　对于以 “K8” 结尾的许可证部件号 （例如，低于 250 个用户的许可证）， TLS 代理会话数限于 1000 个。对于以 “k9” 结尾的许可证部件号 （例如， 250 个用户或更多用户的许可证）， TLS 代理限制取决于配置，最多可为型号限制。 K8 和 K9 是指许可证是否有出口限制：K8 为不受限制， K9 为受限制。 如果您清除配置 （例如，使用 **clear configure all** 命令），则 TLS 代理限制会被设置为您的型号的默认值；如果此默认值低于 UC 许可证限制，则您会看到要求您使用 **tls-proxy maximum-sessions** 命令再次提高限制的错误消息 （在 ASDM 中，请使用 **TLS Proxy** 窗格）。如果您使用故障切换，并输入 **write standby** 命令，或者在 ASDM 中，在主设备上使用 **File > Save Running Configuration to Standby Unit** 来强制进行配置同步，则 **clear configure all** 命令会在辅助设备上自动生成，因此，您可能会在辅助设备上看到警告消息。由于配置同步会还原在主设备上设置的 TLS 代理限制，您可以忽略该警告。 您也可将 SRTP 加密会话用于您的连接： • 对于 K8 许可证， SRTP 会话数限于 250 个。 • 对于 K9 许可证，没有限制。 **注**　仅需要对媒体进行加密 / 解密的呼叫会计入 SRTP 限制；如果将呼叫设置为直通，即使两端均为 SRTP，这些呼叫也不计入限制。
虚拟 CPU	您必须在 ASAv 上安装虚拟 CPU 许可证。直到您安装许可证，吞吐量限于 100 kbps，这样您可以进行初步的连接测试。正常运行需要虚拟 CPU 许可证。
VLAN，最大值	对于根据 VLAN 限制计数的接口，您必须为它分配一个 VLAN。
VPN 负载均衡	VPN 负载均衡需要强加密 (3DES/AES) 许可证。

VPN 许可证和功能兼容性

表 4-13 展示了可以如何整合 VPN 许可证和功能。

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

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

表 4-13　　VPN 许可证和功能兼容性

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

1. 您只能有一个活动的许可证类型， AnyConnect Essentials 许可证或 AnyConnect Premium 许可证。默认情况下， ASA 包括 2 个会话的 AnyConnect Premium 许可证。如果您安装了 AnyConnect Essentials 许可证，默认情况下将使用该许可证。请参阅 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials 窗格，以便启用 Premium license 来进行代替。
2. AnyConnect Essentials 和 AnyConnect Premium 许可证的移动安全状态支持不同。有关详细信息，请参阅第 4-14 页的表 4-12。

有关功能许可证的信息

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

预安装的许可证

默认情况下，ASA 发货时已安装有一个许可证。此许可证可能是您希望对其添加更多许可证的基础许可证，也可能已安装了您的所有许可证，具体取决于您订购的许可证和您的供应商已为您安装的许可证。请参阅第 4-32 页的监控许可证，以便确定您已安装的许可证。

永久许可证

您可以安装一个永久激活密钥。永久激活密钥在单个密钥中包含所有许可功能。如果您还安装了基于时间的许可证， ASA 会将永久许可证和基于时间的许可证整合为运行许可证。有关 ASA 如何整合这些许可证的详细信息，请参阅第 4-19 页的永久许可证和基于时间的许可证如何整合。

基于时间的许可证

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

基于时间的许可证的激活准则

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

基于时间的许可证的计时器如何工作

- 当您在 ASA 上激活基于时间的许可证时，其计时器会开始倒计时。
- 如果您在基于时间的许可证到期之前停止使用该许可证，计时器会停止。仅当您重新激活基于时间的许可证时，计时器才会重新启动。
- 如果基于时间的许可证处于活动状态，并且您关闭 ASA，则计时器会继续倒计时。如果您打算长时间关闭 ASA，则您应在关闭前停用基于时间的许可证。

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

永久许可证和基于时间的许可证如何整合

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

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

表 4-14　基于时间的许可证的整合规则

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

要查看整合的许可证，请参阅第 4-32 页的监控许可证。

堆叠基于时间的许可证

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

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

例如：

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

类似地：

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

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

虽然不同的许可证不会整合，但当前许可证到期时， ASA 会自动激活已安装的同一功能的许可证（如可用）。有关详细信息，请参阅第 4-20 页的基于时间的许可证的到期。

基于时间的许可证的到期

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

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

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

共享 AnyConnect Premium 许可证

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

有关共享许可服务器和参与者的信息

以下步骤说明共享许可证的工作方式：

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

   注　共享许可备用服务器仅需要参与者许可证。

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

   注　参与者需要能够通过 IP 网络与服务器通信；它不必在同一子网中。

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

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

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

注　ASA 在服务器和参与者之间使用 SSL 来加密所有通信。

参与者和服务器之间的通信问题

有关参与者和服务器之间的通信问题的信息，请参阅以下准则：

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

有关共享许可备用服务器的信息

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

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

当主服务器恢复正常运行时，它将与备用服务器同步，然后接管服务器操作。

备用服务器不处于主用状态时，它会充当主共享许可服务器的普通参与者。

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

故障转移和共享许可证

此部分介绍共享许可证如何与故障转移交互。

- 第 4-22 页的故障转移和共享许可证服务器
- 第 4-23 页的故障转移和共享许可证参与者

故障转移和共享许可证服务器

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

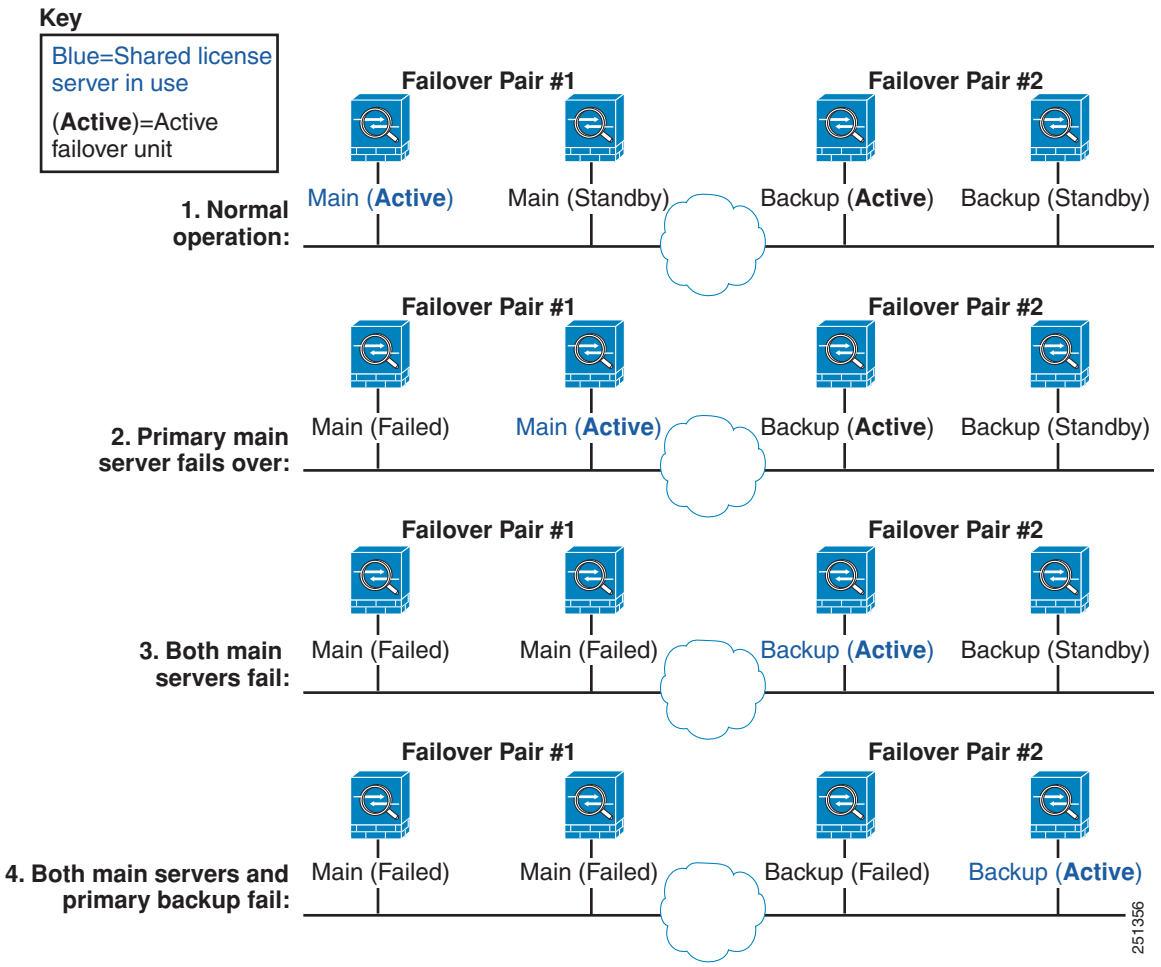
注　备用服务器机制独立于故障转移，但与其兼容。

共享许可证仅在单情景模式中受支持，因此主用 / 主用故障转移不受支持。

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

例如，您有带 2 个故障转移对的网络。第 1 个对包含主许可服务器。第 2 个对包含备用服务器。第 1 个对中的主设备发生故障时，备用设备会立即变为新的主许可服务器。第 2 个对中的备用服务器绝对不会使用。仅当第 1 个对中的两台设备均发生故障时，第 2 个对中的备用服务器才会用作共享许可服务器。如果第 1 个对保持故障状态，并且第 2 个对中的主设备发生故障，则第 2 个对中的备用单元将会用作共享许可服务器（请参阅图 4-1）。

图 4-1　　故障转移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。有关详细信息，请参阅第 4-22 页的有关共享许可备用服务器的信息。

故障转移和共享许可证参与者

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

最大参与者数量

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

故障转移或 ASA 集群许可证

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

故障转移许可证要求和例外情况

故障转移设备不要求每台设备上具有相同的许可证。

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

此规则的例外情况包括：

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

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

ASA 集群许可证要求和例外情况

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

此规则的例外情况包括：

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

故障转移或 ASA 集群许可证如何整合

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

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

  例如，对于故障转移：

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

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

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

  例如，对于 ASA 集群：

  - 您有四台带 SSP-10 的 ASA 5585-X ASA，三台设备都有 50 个情景，一台设备有默认的 2 个情景。由于平台限制是 100 个，整合后的许可证允许最多 100 个情景。因此，您可以在主设备上配置最多 100 个情景；每台从属设备通过配置复制也将拥有 100 个情景。
  - 您有四台带 SSP-60 的 ASA 5585-X ASA，三台设备都有 50 个情景，一台设备有默认的 2 个情景。由于平台限制为 250 个，这些许可证会被整合，从而拥有总计 152 个情景。因此，您可以在主设备上配置最多 152 个情景；每台从属设备通过配置复制也将拥有 152 个情景。
- 对于状态为启用或禁用的许可证，将会使用状态为启用的许可证。
- 对于启用或禁用的基于时间的许可 （而且没有数值层），持续时间是所有许可证的整合持续时间。主 / 主设备首先对其许可证进行倒计时，当其许可证到期时，辅助 / 从属设备将开始对其许可证进行倒计时，依此类推。此规则也适用于主用 / 主用故障转移和 ASA 集群，即使所有设备均以主用状态在运行。

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

要查看整合的许可证，请参阅第 4-32 页的监控许可证。

故障转移或 ASA 集群设备之间的通信丢失

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

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

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

例如：

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

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

升级故障转移对

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

无负载加密型号

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

- 统一通信
- VPN

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

当您查看许可证 （请参阅第 4-32 页的监控许可证）时，将不会列出 VPN 和统一通信许可证。

许可证常见问题

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

A. 能。对于每个功能，您仅能同时使用一个基于时间的许可证。

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

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

Q. 我能否在使基于时间的许可证保持活动的同时，安装新的永久许可证？

A. 能。激活永久许可证不会影响基于时间的许可证。

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

A. 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两台备用服务器的单独故障转移对中。

Q. 我是否需要为故障转移对中的辅助设备，购买相同的许可证？

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

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

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

准则和限制

请参阅激活密钥的以下准则：

情景模式准则

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

防火墙模式准则

所有许可证类型在路由和透明模式中均可用。

故障转移准则

- 共享许可证在主用 / 主用模式中不受支持。有关详细信息，请参阅第 4-22 页的故障转移和共享许可证。
- 请参阅第 4-24 页的故障转移或 ASA 集群许可证。

升级和降级准则

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

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

附加准则和限制

- 激活密钥不会存储在您的配置文件中；它会以隐藏文件的形式，存储在闪存中。
- 激活密钥会与设备的序列号绑定。功能许可证无法在设备之间转移 （硬件发生故障的情况除外）。如果您由于硬件故障必须更换设备，而且 Cisco TAC 涵盖该设备，请联系思科许可团队，以便将您现有的许可证转移至新的序列号。思科许可团队将要求提供产品授权密钥参考编号和现有序列号。
- 一旦购买，您将无法退还许可证，以获取退款或升级的许可证。
- 在单个设备上，您无法将用于相同功能的两个单独许可证相加；例如，如果您购买了一个 25 个会话的 SSL VPN 许可证，此后又购买了 50 个会话的许可证，则您无法使用 75 个会话；您可以使用最多 50 个会话。（您能以升级价格购买更大的许可证，例如从 25 个到 75 个会话；应将这种升级，与将两个单独许可证相加区分开来）。
- 虽然您可以激活所有许可证类型，但有些功能互不兼容。对于 AnyConnect Essentials 许可证，此许可证与以下许可证不兼容：AnyConnect Premium 许可证、共享 AnyConnect Premium 许可证以及高级终端评估许可证。默认情况下，如果您安装了 AnyConnect Essentials 许可证（如果它对于您的模式可用），将使用该许可证，而不是上述许可证。您可以在配置中禁用 AnyConnect Essentials 许可证，以便还原为使用其他许可证，方式是：先使用 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials 窗格。

配置许可证

获取激活密钥

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

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

详细步骤

步骤 1　通过选择 **Configuration > Device Management > Licensing > Activation Key**（在多情景模式中，在系统执行空间中查看序列号）获取您的 ASA 的序列号：

步骤 2　如果您尚未注册至 Cisco.com，请创建帐户。

步骤 3　转至以下许可网站：

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

步骤 4　收到提示时，请输入以下信息：

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

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

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

激活和停用密钥

此部分介绍如何输入新的激活密钥，以及如何激活和停用基于时间的密钥。

先决条件

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

表 4-15　永久许可证重新加载要求

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

限制

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

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

详细步骤

步骤 1　请选择 **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　要输入新的激活密钥 （永久或基于时间的），请在 New Activation Key 字段中输入新的激活密钥。

key 为包括五个部分的十六进制字符串，在每个部分之间有一个空格。前导的 0x 说明符是可选的；所有值都会被认为是十六进制。例如：

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

您可以安装一个永久密钥，以及多个基于时间的密钥。如果您输入一个新的永久密钥，它会覆盖已安装的永久密钥。如果您输入新的基于时间的密钥，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。有关详细信息，请参阅第 4-18 页的基于时间的许可证。

步骤 4　点击 **Update Activation Key**。

在您输入新的激活密钥之后，某些永久许可证会要求您重新加载 ASA。有关需要重新加载的许可证的列表，请参阅第 4-29 页的表 4-15。如果需要，系统会提示您重新加载。

配置共享许可证

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

配置共享许可服务器

此部分介绍如何将 ASA 配置为共享许可服务器。

先决条件

服务器必须具有共享许可服务器密钥。

详细步骤

步骤 1　选择 **Configuration > Device Management > Licenses > Shared SSL VPN Licenses** 窗格。

步骤 2　在 Security Secret 字段中，输入长度为 4 至 128 个 ASCII 字符的共享机密。

拥有此机密的所有参与者，都可以使用许可服务器。

步骤 3　（可选）在 TCP IP Port 字段中，输入端口，服务器会在该端口上侦听来自参与者的 SSL 连接，该端口介于 1 和 65535 之间。

默认值为 TCP 端口 50554。

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

此值会提供给参与者，用于设置它们应与服务器通信的频率。默认值为 30 秒。

步骤 5　在 Interfaces that serve shared licenses 区域中，为参与者会在其上联系服务器的所有接口，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，输入备用服务器的序列号。

c. 如果备用服务器是故障转移对的一部分，在 Secondary backup server serial number 字段中，确定备用设备的序列号。

您仅能确定 1 台备用服务器及其可选的备用设备。

步骤 7　点击 **Apply**。

后续操作

请参阅第 4-32 页的配置共享许可参与者和可选的备用服务器。

配置共享许可参与者和可选的备用服务器

此部分配置共享许可参与者，以便与共享许可服务器通信；此部分还介绍您可以如何可选地将参与者配置为备用服务器。

先决条件

参与者必须具有共享许可参与者密钥。

详细步骤

步骤 1　选择 **Configuration > Device Management > Licenses > Shared SSL VPN Licenses** 窗格。

步骤 2　在 Security Secret 字段中，输入长度为 4 至 128 个 ASCII 字符的共享机密。

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，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. 为参与者在其上联系备用服务器的所有接口，选中 **Shares Licenses** 复选框。

步骤 5　点击 **Apply**。

监控许可证

查看您的当前许可证

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

准则

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

详细步骤

步骤 1　要查看运行许可证，该许可证由永久许可证和所有活动的基于时间的许可证整合而成，请选择 **Configuration > Device Management > Licensing > Activation Key** 窗格并查看 Running Licenses 区域。

在多情景模式中，请选择 **Configuration > Device Management > Activation Key** 窗格，以便在系统执行空间中查看激活密钥。

对于故障转移对，显示的运行许可证是主设备和辅助设备的组合许可证。有关详细信息，请参阅第 4-25 页的故障转移或 ASA 集群许可证如何整合。对于具有数字值的基于时间的许可证（持续时间未被整合），License Duration 列会显示主设备或辅助设备中的最短的基于时间的许可证；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，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）对于故障转移设备，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组合许可证），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，选择 **Monitoring > VPN > Clientless SSL VPN > Shared Licenses**。

许可的功能历史记录

表 4-16 列出了各种功能变更以及实施该等功能变更的平台版本。ASDM 可向后兼容多个平台版本，因此，未列出已添加支持的具体 ASDM 版本。

表 4-16　　许可的功能历史记录

功能名称	平台版本	功能信息
增加的连接数和 VLAN 数量	7.0(5)	增加了以下限制： • ASA5510 基础许可证连接数从 32000 提高至 50000；VLAN 数从 0 提高至 10。 • ASA5510 增强型安全许可证连接数从 64000 提高至 130000；VLAN 数从 10 提高至 25。 • ASA5520 连接数从 130000 提高至 280000；VLAN 数从 25 提高至 100。 • ASA5540 连接数从 280000 提高至 400000；VLAN 数从 100 提高至 200。
SSL VPN 许可证	7.1(1)	引入了 SSL VPN 许可证。
增加的 SSL VPN 许可证数量	7.2(1)	为 ASA 5550 及更高版本引入了 5000 名用户的 SSL VPN 许可证。
ASA 5510 上基础许可证增加的接口数	7.2(2)	对于 ASA 5510 上的基础许可证，最大接口数从 3 个加上管理接口数，增至不受限制。

表 4-16　　许可的功能历史记录 （续）

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

表 4-16　　许可的功能历史记录 （续）

功能名称	平台版本	功能信息
AnyConnect Essentials 许可证	8.2(1)	引入了 AnyConnect Essentials 许可证。此许可证允许 AnyConnect VPN 客户端访问 ASA。此许可证不支持基于浏览器的 SSL VPN 访问或思科安全桌面。对于这些功能，请激活 AnyConnect Premium 许可证，而不是 AnyConnect Essentials 许可证。 **注**　借助 AnyConnect Essentials 许可证，VPN 用户可以使用网络浏览器来进行登录，然后下载并启动 (WebLaunch) AnyConnect 客户端。 AnyConnect 客户端软件提供一组相同的客户端功能，无论是通过此许可证，还是通过 AnyConnect Premium 许可证启用。 AnyConnect Essentials 许可证不能在给定 ASA 上与以下许可证同时处于活动状态：AnyConnect Premium 许可证（所有类型）或高级终端评估许可证。然而，您可以在同一网络中的不同 ASA 上运行 AnyConnect Essentials 和 AnyConnect Premium 许可证。 默认情况下， ASA 使用 AnyConnect Essentials 许可证，但您可以通过先使用 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials 窗格来禁用该许可证，以便使用其他许可证。
SSL VPN 许可证更改为 AnyConnect Premium SSL VPN 版本许可证	8.2(1)	SSL VPN 许可证的名称更改为 AnyConnect Premium SSL VPN 版本许可证。
SSL VPN 共享许可证	8.2(1)	引入了 SSL VPN 共享许可证。多个 ASA 可以根据需要共享 SSL VPN 会话池。
移动代理应用不再需要统一通信代理许可证	8.2(2)	移动代理不再需要 UC 代理许可证。
带 SSP-20 的 ASA 5585-X 的 10 GE I/O 许可证	8.2(3)	我们引入了带 SSP-20 的 ASA 5585-X 的 10 GE I/O 许可证，以便在光纤端口上支持 10 千兆以太网速度。默认情况下， SSP-60 支持 10 千兆以太网速度。 **注**　ASA 5585-X 在 8.3(x) 版本中不受支持。
带 SSP-10 的 ASA 5585-X 的 10 GE I/O 许可证	8.2(4)	我们引入了带 SSP-10 的 ASA 5585-X 的 10 GE I/O 许可证，以便在光纤端口上支持 10 千兆以太网速度。默认情况下， SSP-40 支持 10 千兆以太网速度。 **注**　ASA 5585-X 在 8.3(x) 版本中不受支持。
不相同的故障转移许可证	8.3(1)	在每台设备上不再需要相同的故障转移许可证。用于两台设备的许可证是主设备和辅助设备的组合许可证。 我们修改了以下 屏幕：Configuration > Device Management > Licensing > Activation Key。

表 4-16　　许可的功能历史记录 （续）

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

表 4-16　　许可的功能历史记录 （续）

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

透明或路由防火墙模式

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

可以在多情景模式中为每个情景独立设置防火墙模式。

有关防火墙模式的信息

有关路由防火墙模式的信息

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

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

有关透明防火墙模式的信息

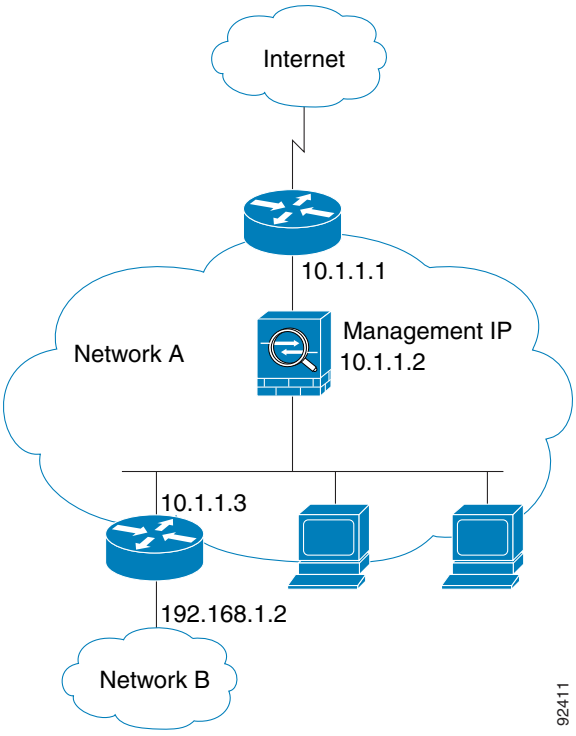
传统上，防火墙是路由跃点，并充当与其中一个屏蔽子网连接的主机的默认网关。另一方面，透明防火墙是第 2 层防火墙，充当 “ 网络嵌入式防火墙 ” 或 “ 隐形防火墙 ”，而不被视为已连接设备的路由器跃点。

在网络中使用透明防火墙

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

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

图 5-1　　透明防火墙网络

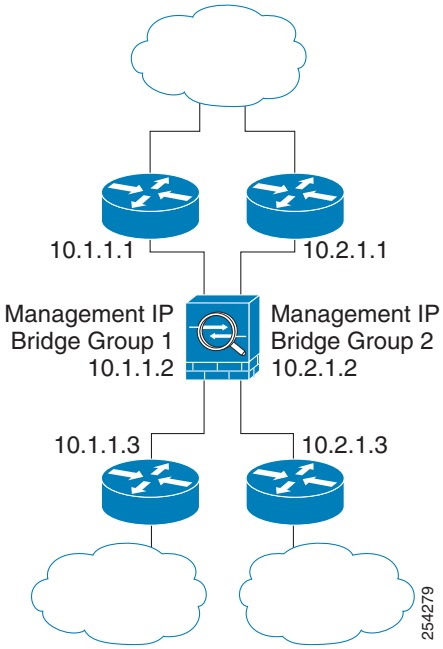


网桥组

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

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

图 5-2　　具有两个网桥组的透明防火墙网络



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

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

管理接口 （ASA 5512-X 及更高版本）

除了每个网桥组管理 IP 地址，还可以添加不属于任何网桥组的单独的管理*插槽 / 端口*接口，这种接口仅允许流向 ASA 的管理流量。有关详细信息，请参阅第 10-2 页的管理接口。

允许第 3 层流量

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

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

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

允许的 MAC 地址

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

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

不允许在路由模式中通过流量

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

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

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

允许路由模式功能通过流量

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

BPDU 处理

为防止环路使用生成树协议，默认情况下允许 BPDU 通过。要阻止 BPDU，需要将以太网类型 ACL 配置为拒绝 BPDU。如果使用故障转移功能，您可能想要阻止 BPDU，以防止交换机端口在拓扑结构改变时进入阻止状态。有关详细信息，请参阅第 8-13 页的透明防火墙模式要求。

MAC 地址与 路由查找

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

但是，路由查找对于以下流量类型是必要的：

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

ARP 检测

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

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

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

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

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

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

MAC 地址表

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

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

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

原始数据包将被丢弃。

防火墙模式的许可要求

下表显示了此功能的许可要求。

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

默认设置

默认模式为路由模式。

透明模式的默认设置

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

准则和限制

情景模式准则

应根据情景设置防火墙模式。

透明防火墙准则

- 在透明防火墙模式中，管理接口以与数据接口相同的方式更新 MAC 地址表；因此，不应将管理和数据接口连接到同一个交换机，除非将其中一个交换机端口配置为路由端口（默认情况下，Catalyst 交换机在所有的 VLAN 交换机端口上共享一个 MAC 地址）。否则，如果流量从物理连接的交换机到达管理接口，ASA 会更新 MAC 地址表，以使用*管理*接口（而不是数据接口）来访问交换机。此操作会导致临时流量中断；出于安全原因，ASA 至少在 30 秒内不会再次更新从交换机到数据接口的数据包 MAC 地址表。
- 各个直连网络必须在同一个子网上。
- 请勿将网桥组管理 IP 地址指定为所连接设备的默认网关；设备需要将位于 ASA 另一端的路由器指定为默认网关。
- 透明防火墙的默认路由（为管理流量提供返回路径需要有该路由）仅适用于来自一个网桥组网络的管理流量。这是因为，默认路由指定网桥组中的接口以及网桥组网络上的路由器 IP 地址，而您只能定义一个默认路由。如果您具有来自多个网桥组网络的管理流量，需要指定静态路由来确定您预期将会发出管理流量的网络。

有关更多准则，请参阅第 13-4 页的透明模式接口的准则和限制。

IPv6 准则

支持 IPv6。

附加准则和限制

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

透明模式中不支持的功能

表 5-1 列出了透明模式中不支持的功能。

表 5-1　　透明模式中不支持的功能

功能	说明
动态 DNS	-
DHCP 中继	透明防火墙可用作 DHCP 服务器，但它不支持 DHCP 中继命令。DHCP 中继并非必要的，因为可以使用两个扩展 ACL 来允许 DHCP 流量通过：一个允许 DCHP 请求从内部接口传输到外部，另一个允许应答从服务器朝着另一个方向传输。
动态路由协议	但是，可以为源自 ASA 的流量添加静态路由。还可以使用扩展 ACL 来允许动态路由协议通过 ASA。
组播 IP 路由	可以在扩展 ACL 中允许组播流量，从而允许这些流量通过 ASA。

表 5-1　　透明模式中不支持的功能 （续）

功能	说明
QoS	-
针对直通流量的 VPN 终止	透明防火墙仅支持用于管理连接的站点到站点 VPN 隧道。它不会针对通过 ASA 的流量终止 VPN 连接。可以使用扩展 ACL 来允许 VPN 流量通过 ASA，但 ASA 不会终止非管理连接。也不支持无客户端 SSL VPN。
统一通信	-

设置防火墙模式 （单模式）

本节介绍如何使用 CLI 更改防火墙模式。对于单模式和多模式中当前连接的情景 （一般为管理员情景），不能在 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；请参阅第 7-18 页的配置安全情景。

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

如果更改模式， ASA 将会清除运行配置 （有关详细信息，请参阅第 5-7 页的准则和限制）。

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

详细步骤

注　要将防火墙模式设置为透明模式，并要在配置被清除后配置 ASDM 管理访问，请参阅第 2-7 页的为设备和 ASAv 自定义 ASDM 访问或第 2-9 页的为 ASA 服务模块配置 ASDM 访问。

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

为透明防火墙配置 ARP 检测

本节介绍如何配置 ARP 检测。

配置 ARP 检测的任务流程

要配置 ARP 检测，请执行以下步骤：

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

步骤 2　按照第 5-10 页的启用 ARP 检测中所述启用 ARP 检测。

添加静态 ARP 条目

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

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

详细步骤

步骤 1　选择 **Configuration > Device Management > Advanced > ARP > ARP Static Table** 窗格。

步骤 2　（可选）要为*动态* ARP 条目设置 ARP 超时，请在 ARP Timeout 字段中输入一个值。

该字段在 ASA 重建 ARP 表之前设置时间段（60 到 4294967 秒）。默认值为 14400 秒。重建 ARP 表会自动更新新的主机信息并移除旧的主机信息。由于主机信息更改频繁，因此您可能想要降低超时值。

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，否则我们不建议启用此功能。此功能有助于缓解针对 ASA 的拒绝服务攻击 (DoS)；任何接口上的用户都可以发出很多 ARP 应答，还可以使用虚假条目来造成 ASA ARP 表过载。

在以下情况下，可能需要使用此功能：

- 使用辅助子网。
- 使用邻接路由器上的代理 ARP 来进行流量转发。

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　要对该地址执行代理 ARP，请选中 **Proxy ARP** 复选框。

如果 ASA 收到对于指定 IP 地址的 ARP 请求，它会使用指定的 MAC 地址作出响应。

步骤 9　点击 **OK**，然后点击 **Apply**。

后续操作

按照第 5-10 页的启用 ARP 检测中所述启用 ARP 检测。

启用 ARP 检测

本节介绍如何启用 ARP 检测。

详细步骤

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

步骤 2　选择要启用 ARP 检测所在的接口行，然后点击 **Edit**。

系统将显示 Edit ARP Inspection 对话框。

步骤 3　要启用 ARP 检测，请选中 **Enable ARP Inspection** 复选框。

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

默认情况下，会以泛洪方式将不匹配静态 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， ASA 将会丢弃数据包。

如果取消选中此复选框，所有不匹配数的据包都将被丢弃，这样会将通过 ASA 的 ARP 限制为仅限于静态条目。

注　管理 0/0 或 0/1 接口或子接口 （如果有）不会以泛洪方式传输数据包，即使此参数被设置使用泛洪传输方式。

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。

- 第 5-11 页的添加静态 MAC 地址
- 第 5-11 页的禁用 MAC 地址学习

添加静态 MAC 地址

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

要将静态 MAC 地址添加到 MAC 地址表中，请执行以下操作步骤：

步骤 1　选择 **Configuration > Device Setup > Bridging > MAC Address Table** 窗格。

步骤 2　（可选）要设置 MAC 地址在超时前在 MAC 地址表中停留的时间，请在 Dynamic Entry Timeout 字段中输入一个值。

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 **Add**。

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 地址相关的源接口。

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 地址学习

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

要禁用 MAC 地址学习，请执行以下步骤：

步骤 1　选择 **Configuration > Device Setup > Bridging > MAC Learning** 窗格。

步骤 2　要禁用 MAC 地址学习，请选择所需的接口行，然后点击 **Disable**。

步骤 3　要重新启用 MAC 地址学习，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。

- 第 5-12 页的数据如何在路由防火墙模式中通过 ASA
- 第 5-17 页的数据如何通过透明防火墙

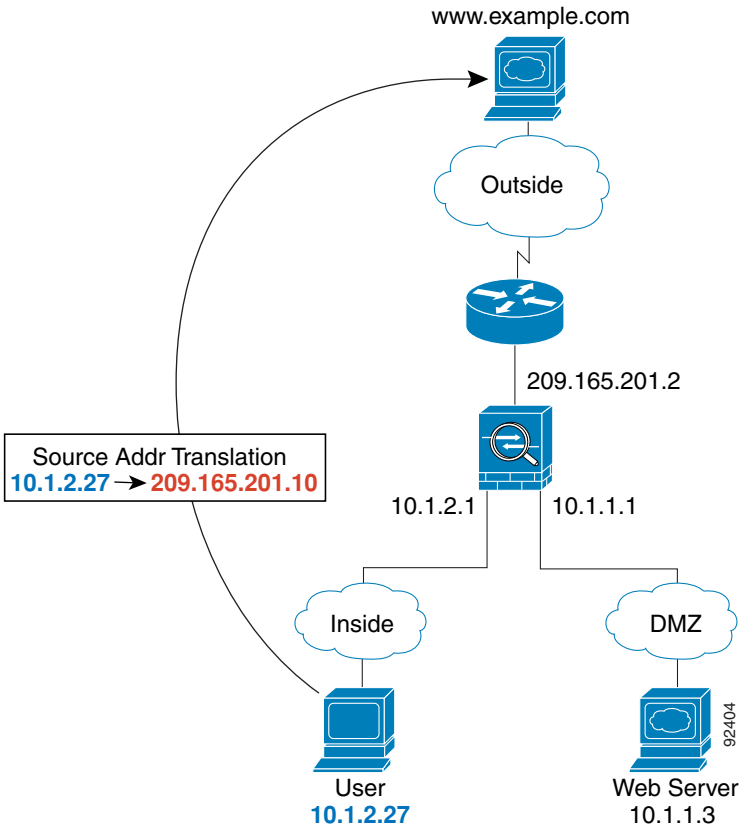
数据如何在路由防火墙模式中通过 ASA

本节介绍数据如何在路由防火墙模式中通过 ASA。

内部用户访问网络服务器

图 5-3 显示了内部用户访问外部网络服务器。

图 5-3　　从内部到外部



以下步骤介绍数据如何通过 ASA （请参阅图 5-3）：

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

   对于多情景模式， ASA 会首先将数据包分类到一个情景中。

3. ASA 将本地源地址 (10.1.2.27) 转换为全局地址 209.165.201.10 （该地址位于外部接口子网上）。

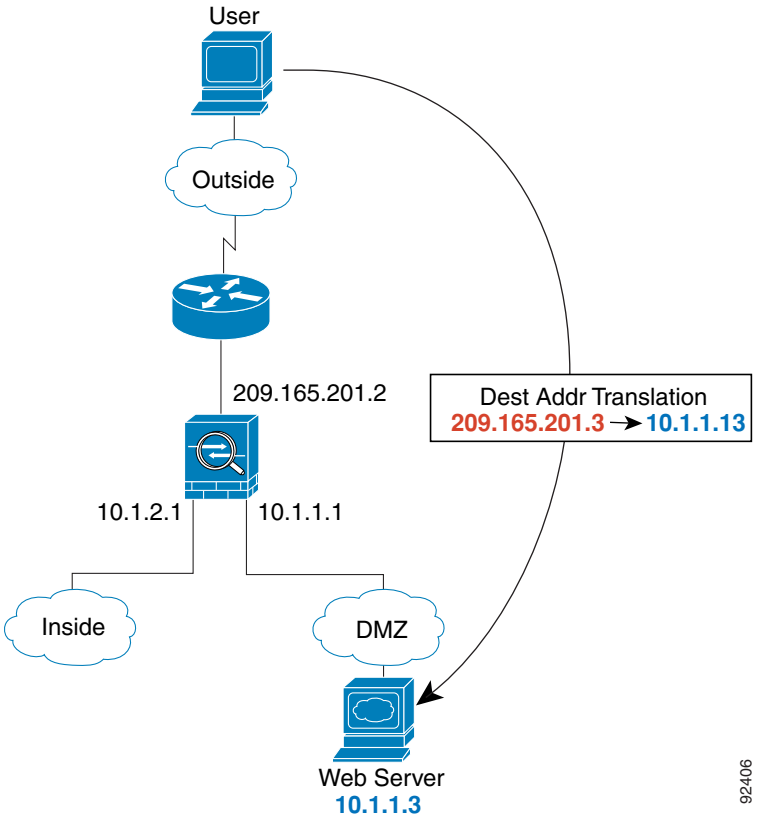
   全局地址可以位于任何子网上，但如果全局地址位于外部接口子网上，路由将会变得简单。

4. 然后， ASA 会记录有关会话已建立的信息，并从外部接口转发数据包。
5. 当 www.example.com 响应请求时，数据包会通过 ASA ；由于会话已建立，因此，数据包会绕过与新连接相关的很多查找。ASA 通过将全局目标地址逆向转换为本地用户地址 10.1.2.27 来执行 NAT。
6. ASA 将数据包转发给内部用户。

外部用户访问 DMZ 上的网络服务器

图 5-4 显示了外部用户访问 DMZ 网络服务器。

图 5-4　从外部到 DMZ



以下步骤介绍数据如何通过 ASA （请参阅图 5-4）：

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

   对于多情景模式， ASA 会首先将数据包分类到一个情景中。

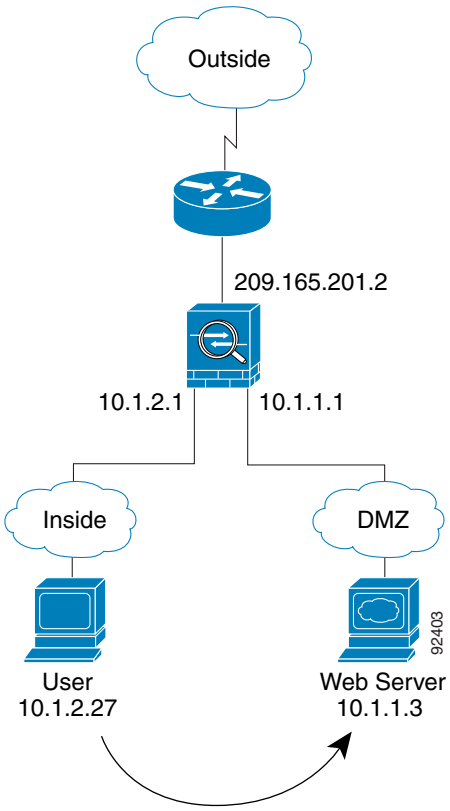
4. 然后， ASA 会将会话条目添加到快速路径，并从 DMZ 接口转发数据包。

5. 当 DMZ 网络服务器响应请求时，数据包会通过 ASA；由于会话已建立，因此，数据包会绕过与新连接相关的很多查找。 ASA 通过将本地源地址转换为 209.165.201.3 来执行 NAT。
6. ASA 将数据包转发给外部用户。

内部用户访问 DMZ 上的网络服务器

图 5-5 显示了内部用户访问 DMZ 网络服务器。

图 5-5　从内部到 DMZ



以下步骤介绍数据如何通过 ASA （请参阅图 5-5）：

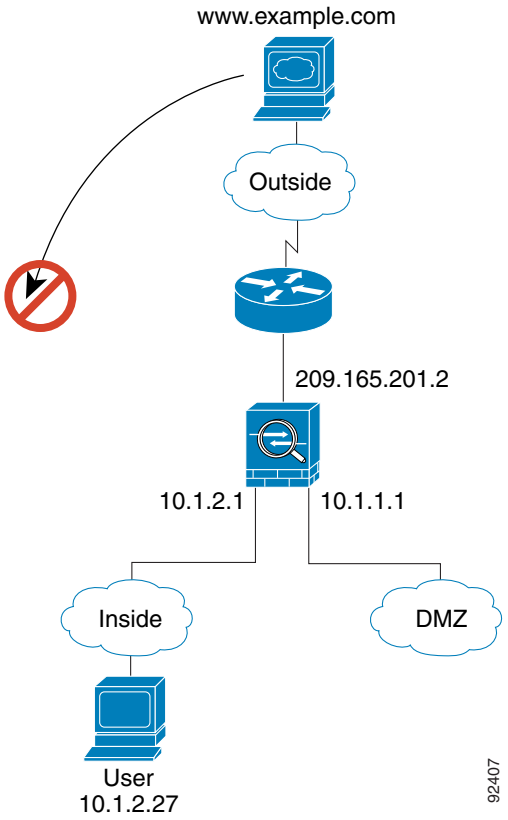
1. 内部网络上的用户使用目标地址 10.1.1.3 从 DMZ 网络服务器请求访问网页。
2. ASA 接收数据包；由于是新会话，因此， ASA 会根据安全策略条款 （访问列表、过滤器、AAA）验证数据包是否获允许。

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

外部用户尝试访问内部主机

图 5-6 显示了外部用户尝试访问内部网络。

图 5-6　从外部到内部



以下步骤介绍数据如何通过 ASA （请参阅图 5-6）：

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

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

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

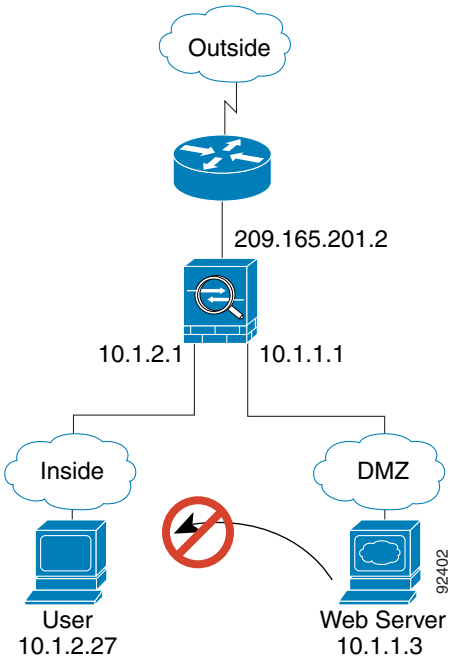
3. 数据包被拒绝，且 ASA 丢弃数据包且记录连接尝试情况。

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

DMZ 用户尝试访问内部主机

图 5-7 显示了 DMZ 中的用户尝试访问内部网络。

图 5-7　　从 DMZ 到内部



以下步骤介绍数据如何通过 ASA （请参阅图 5-7）：

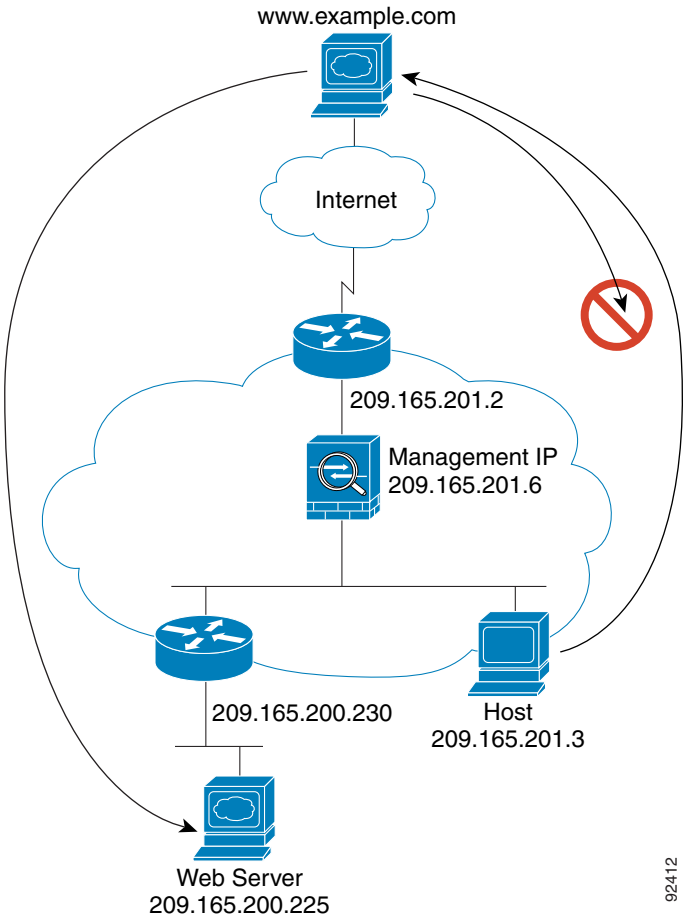
1. DMZ 网络上的用户尝试访问内部主机。由于 DMZ 不必路由互联网上的流量，因此，专用寻址方案不会防止路由。
2. ASA 接收数据包；由于是新会话，因此， ASA 会根据安全策略 （访问列表、过滤器、AAA）验证数据包是否获允许。

   数据包被拒绝，且 ASA 丢弃数据包且记录连接尝试情况。

数据如何通过透明防火墙

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

图 5-8　典型的透明防火墙数据路径



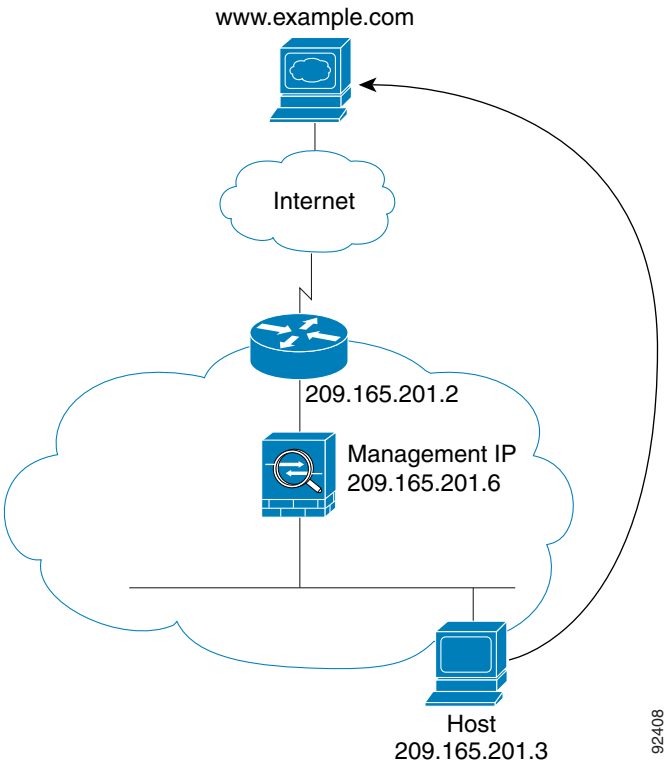
本节介绍数据如何通过 ASA。

- 第 5-18 页的内部用户访问网络服务器
- 第 5-19 页的内部用户使用 NAT 访问网络服务器
- 第 5-20 页的外部用户访问内部网络上的网络服务器
- 第 5-21 页的外部用户尝试访问内部主机

内部用户访问网络服务器

图 5-9 显示了内部用户访问外部网络服务器。

图 5-9　　从内部到外部



以下步骤介绍数据如何通过 ASA （请参阅图 5-9）：

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

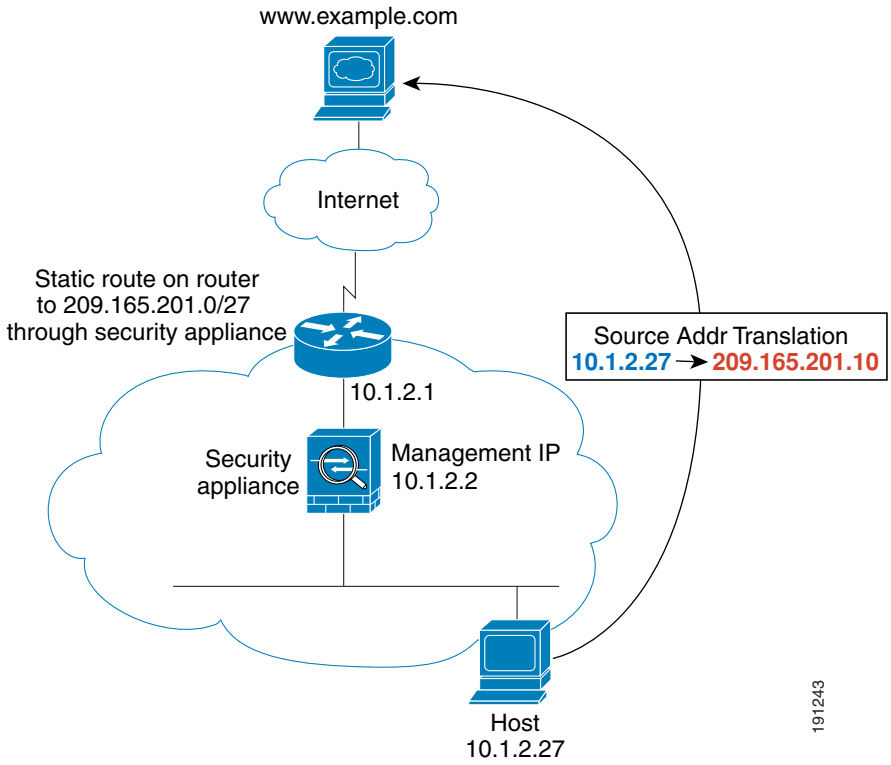
   对于多情景模式， ASA 会首先将数据包分类到一个情景中。
3. ASA 记录有关会话已建立的信息。
4. 如果目标 MAC 地址在其表中，ASA 会将数据包从外部接口转发出去。目标 MAC 地址是上游路由器的地址 (209.165.201.2)。

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

内部用户使用 NAT 访问网络服务器

图 5-10 显示了内部用户访问外部网络服务器。

图 5-10　使用 NAT 从内部到外部



以下步骤介绍数据如何通过 ASA （请参阅图 5-10）：

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

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

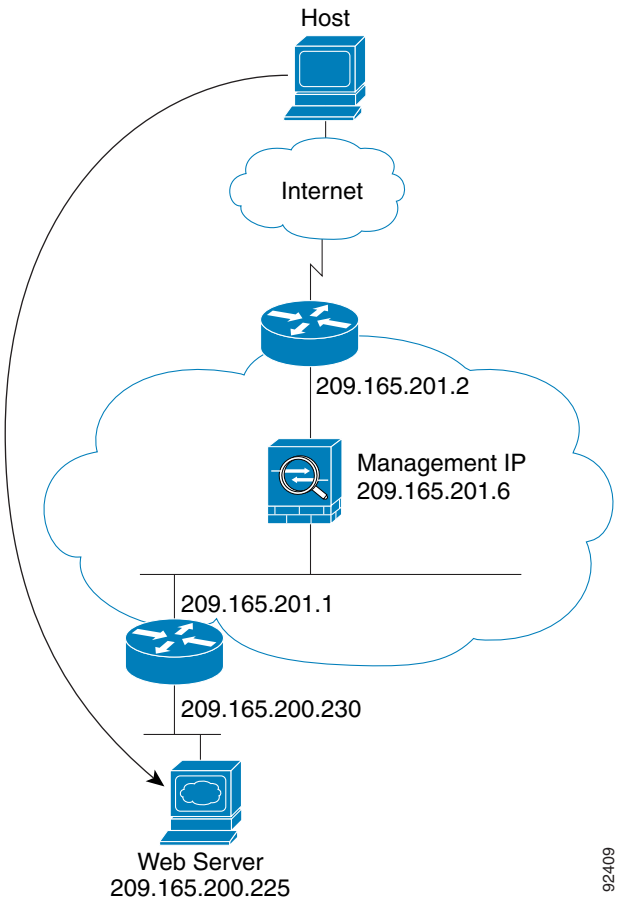
   由于映射地址与外部接口不在相同的网络上，因此，请确保上游路由器具有至映射网络 （该网络指向 ASA）的静态路由。
4. 然后， ASA 会记录有关会话已建立的信息，并从外部接口转发数据包。
5. 如果目标 MAC 地址在其表中，ASA 会将数据包从外部接口转发出去。目标 MAC 地址是上游路由器的地址 (10.1.2.1)。

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

外部用户访问内部网络上的网络服务器

图 5-11 显示了外部用户访问内部网络服务器。

图 5-11　　从外部到内部



以下步骤介绍数据如何通过 ASA （请参阅图 5-11）：

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

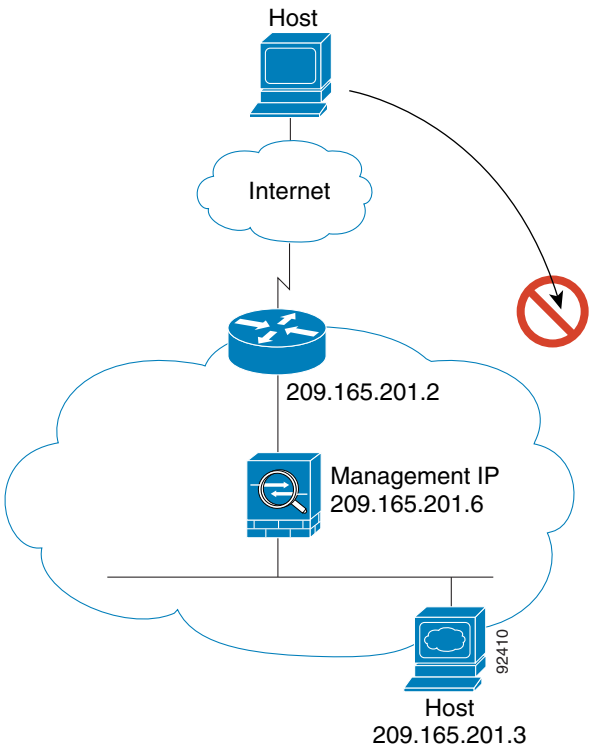
   对于多情景模式， ASA 会首先将数据包分类到一个情景中。
3. ASA 记录有关会话已建立的信息。
4. 如果目标 MAC 地址在其表中，ASA 会将数据包从内部接口转发出去。目标 MAC 地址是下游路由器的地址 (209.165.201.1)。

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

外部用户尝试访问内部主机

图 5-12 显示了外部用户尝试访问内部网络上的主机。

图 5-12　从外部到内部



以下步骤介绍数据如何通过 ASA （请参阅图 5-12）：

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

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

防火墙模式的功能历史记录

表 5-2 列出了各种功能变更以及实施该等功能变更的平台版本。 ASDM 可向后兼容多个平台版本，因此，未列出已添加支持的具体 ASDM 版本。

表 5-2　　防火墙模式的功能历史记录

功能名称	平台版本	功能信息
透明防火墙模式	7.0(1)	透明防火墙是第 2 层防火墙，充当类似于 “ 网络嵌入式防火墙 ” 或 “ 隐形防火墙 ”，而不被视为已连接设备的路由器跃点。 我们引入了以下命令：**firewall transparent**、 **show firewall**。 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。 我们引入了以下命令：**arp**、 **arp-inspection** 和 **show arp-inspection**。
MAC 地址表	7.0(1)	透明防火墙模式使用 MAC 地址表。 我们引入了以下命令：**mac-address-table static**、**mac-address-table aging-time**、 **mac-learn disable** 和 **show mac-address-table**。
透明防火墙网桥组	8.4(1)	如果不想产生安全情景开销，或者要最大限度地使用安全情景，请将接口一起组合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组流量与其他网桥组是隔离开的。可以在单模式或多模式中为每个情境最多配置 8 个网桥组，每个网桥组最多可配置 4 个接口。 **注**　虽然可以在 ASA 5505 上配置多个网桥组，但在 ASA 5505 上，透明模式中 2 个数据接口这一限制意味着只能有效使用 1 个网桥组。 我们修改或引入了以下屏幕： Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > Interfaces > Add/Edit Interface

表 5-2　　防火墙模式的功能历史记录 （续）

功能名称	平台版本	功能信息
针对未连接的子网增加 ARP 缓存	8.4(5)/9.1(2)	默认情况下， ASA ARP 缓存仅包含来自直连子网的条目。现在，可以启用 ARP 缓存，以将非直连子网也包含在内。除非您了解安全风险，否则我们不建议启用此功能。此功能有助于缓解针对 ASA 的拒绝服务攻击 (DoS) ；任何接口上的用户都可以发出很多 ARP 应答，还可以使用虚假条目来造成 ASA ARP 表过载。 在以下情况下，可能需要使用此功能： • 使用辅助子网。 • 使用邻接路由器上的代理 ARP 来进行流量转发。 我们修改了以下屏幕：Configuration > Device Management > Advanced > ARP > ARP Static Table。
多情景模式中的混合防火墙模式支持	8.5(1)/9.0(1)	可以在多情景模式中为每个情景独立设置防火墙模式，因此，有些可以在透明模式中运行，有些可以在路由模式中运行。 我们修改了以下命令：**firewall transparent**。 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 增加到 250。在单情景模式和多情景模式的每个情景中，最多可配置 250 个网桥组，每组最多 4 个接口。 我们修改了以下屏幕： Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > 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 Cisco 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　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

第 14-1 页的设置主机名、域名及启用和 Telnet 密码

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

- 第 12-5 页的配置常规接口参数
- 第 12-12 页的配置 IPv6 寻址

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

第 12-9 页的 PPPoE IP 地址和路由设置

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 地址以用于两个管理流量并供流量通过 ASA。此屏幕可为 BVI 1 设置 IP 地址。

相关主题

第 13-6 页的配置网桥组

其他接口配置

配置其他接口的参数。

相关主题

- 第 12-5 页的配置常规接口参数
- 第 12-16 页的允许同一安全级别通信

静态路由

配置静态路由。

相关主题

第 20-2 页的静态路由配置

DHCP 服务器

配置 DHCP 服务器。

相关主题

第 15-4 页的配置 DHCP 服务器

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。有关详细信息，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

- 第 36-3 页的配置管理访问
- 第 3-30 页的启用历史度量

IPS 基本配置

在单情景模式中，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。有关详细信息，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

第 14-6 页的设置日期和时间

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

第 37-26 页的配置自动更新

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。
- 选择以下任一选项：
  - 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

表 6-1　　启动向导历史

功能名称	平台版本	说明
启动向导	7.0(1)	我们引入了此向导。 我们引入了 **Wizards > Startup Wizard** 屏幕。
IPS 配置	8.4(1)	对于 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。我们添加了 **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。 我们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**

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。

安全情景的相关信息

您可以将单台 ASA 分区为多台称为安全情景的虚拟设备。每个情景都可以作为独立设备，拥有自己的安全策略、接口和管理员。多情景类似于拥有多台独立设备。有关在多情景模式中不受支持的功能，请参阅第 7-13 页的准则和限制。

本节提供安全情景的概述。

安全情景的常见用途

您可能想要在以下情况下使用多安全情景：

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

情景配置文件

本节介绍 ASA 如何实施多情景模式配置。

- 第 7-2 页的情景配置
- 第 7-2 页的系统配置
- 第 7-2 页的管理情景配置

情景配置

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

系统配置

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

管理情景配置

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

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

ASA 如何对数据包分类

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

- 第 7-3 页的有效分类器条件
- 第 7-4 页的分类示例

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

有效分类器条件

本节介绍分类器使用的条件。

- 第 7-3 页的唯一接口
- 第 7-3 页的唯一 MAC 地址
- 第 7-3 页的 NAT 配置

注　对于目标是接口的管理流量，接口 IP 地址将用于分类。

路由表不会被用于数据包分类。

唯一接口

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

唯一 MAC 地址

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

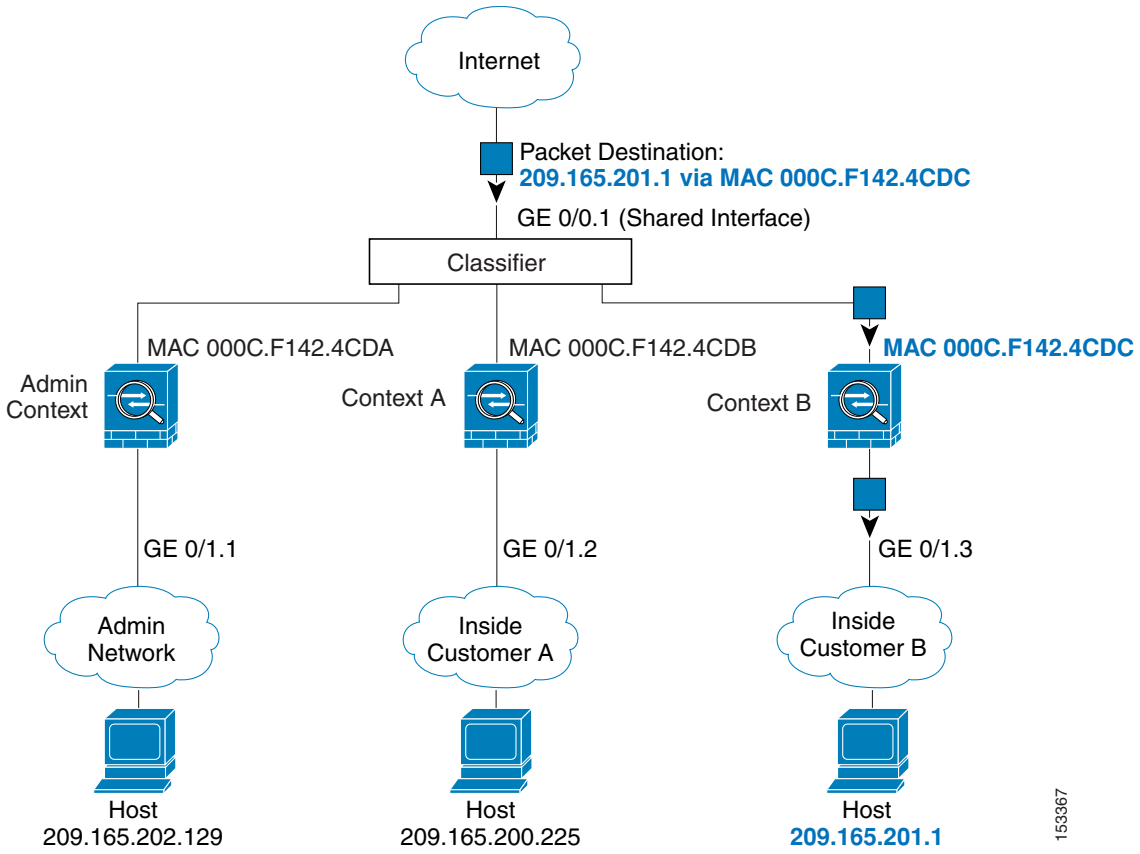
NAT 配置

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

分类示例

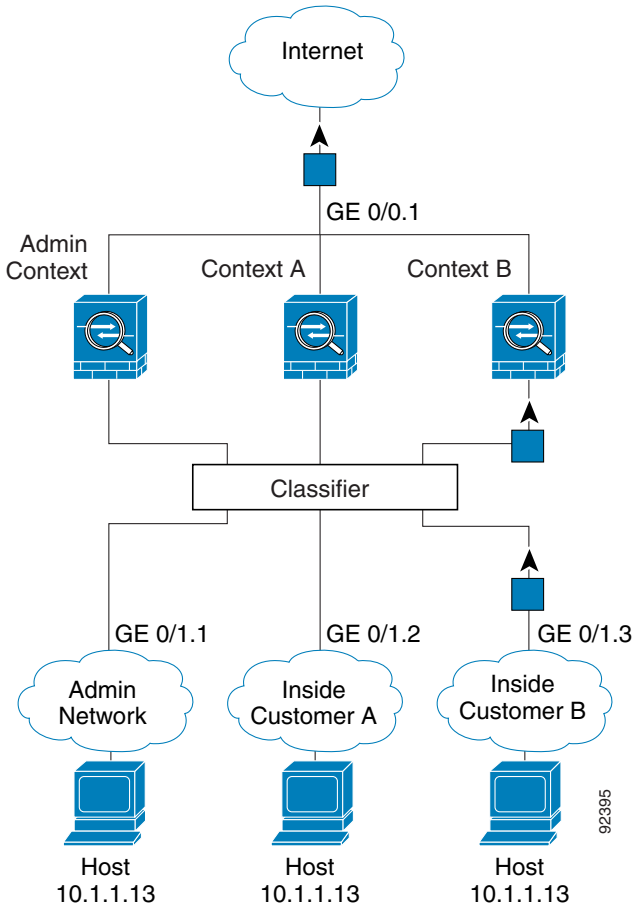
图 7-1 展示了共享一个外部接口的多情景。因为情景 B 包括路由器向其发送数据包的 MAC 地址，分类器会将该数据包分配至情景 B。

图 7-1　使用 MAC 地址的共享接口数据包分类



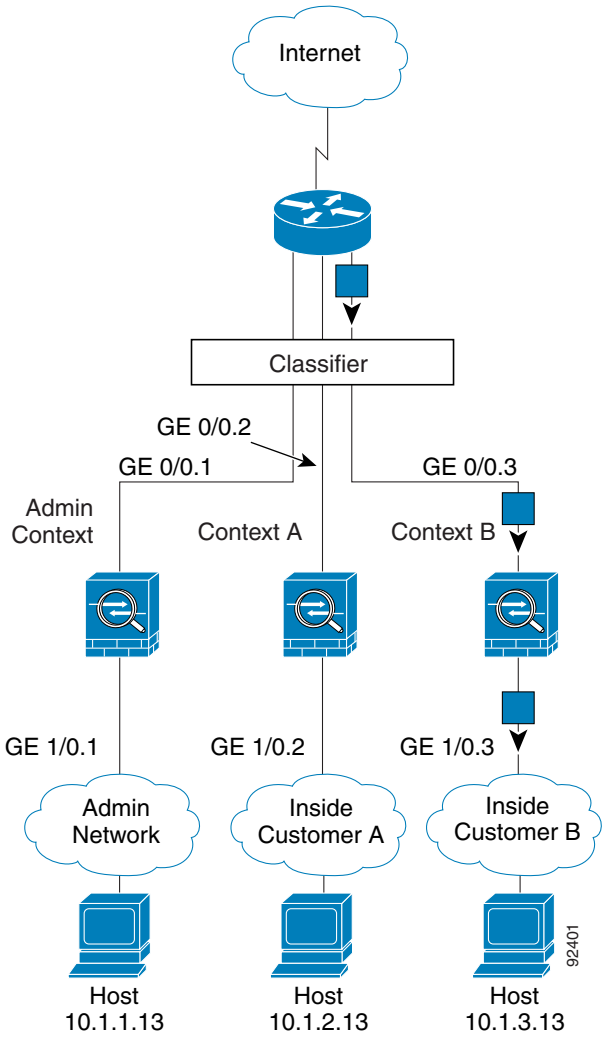
请注意，所有新的传入流量都必须加以分类，即使其来自内部网络。图 7-2 展示了访问互联网的情景 B 内部网络上的主机。因为入口接口是已分配至情景 B 的 Gigabit Ethernet 0/1.3，分类器会将数据包分配至情景 B。

图 7-2　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 7-3 展示了来自互联网，目标为情景 B 内部网络上的一台主机的数据包。因为入口接口是已分配至情景 B 的 Gigabit Ethernet 1/0.3，分类器会将数据包分配至情景 B。

图 7-3　透明防火墙情景



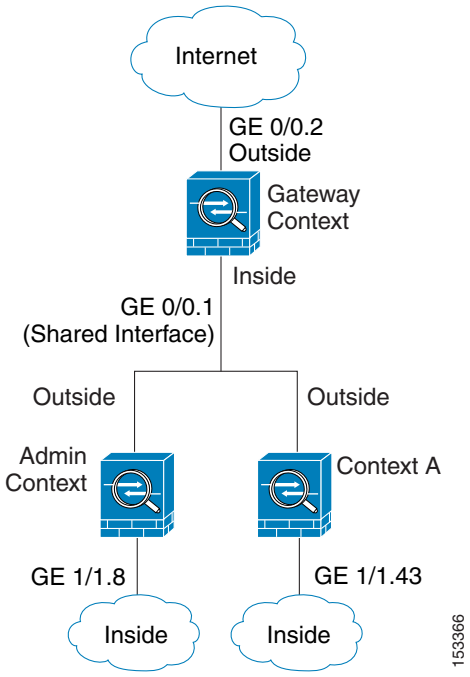
级联安全情景

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

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

图 7-4 展示了网关之后有两个情景的网关情景。

图 7-4　　级联情景



对安全情景的管理访问

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

- 第 7-7 页的系统管理员访问
- 第 7-8 页的情景管理员访问

系统管理员访问

您可以通过两种方式作为系统管理员访问 ASA：

- 访问 ASA 控制台。

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

- 使用 Telnet、 SSH 或 ASDM 访问管理情景。

  要启用 Telnet、 SSH 和 ASDM 访问，请参阅第 36 章，“管理访问”。

作为系统管理员，您可以访问所有情景。

当您从管理员或系统切换到某个情景时，您的用户名会更改为默认的 “enable_15” 用户名。如果您在该情景中配置了命令授权，您需要为 “enable_15” 用户配置授权权限，也可以用您已提供足够权限的不同用户名登录。要使用新用户名登录，请输入 **login** 命令。例如，您可以使用用户名 “admin” 登录至管理情景。管理情景没有任何命令授权配置，但是，所有其他情景都包含命令授权。为方便起见，每个情景配置都包含有拥有最高权限的 “admin” 用户。当您从管理情景切换到情景 A 时，您的用户名会更改为 enable_15，因此，您必须输入 **login** 命令，作为 “admin” 再次登录。当您切换到情景 B 时，必须再次输入 **login** 命令，作为 “admin” 登录。

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

情景管理员访问

您可以使用 Telnet、 SSH 或 ASDM 访问情景。如果您登录非管理情景，则只能访问该情景的配置。您可以提供该情景的单独登录。要启用 Telnet、 SSH 和 ASDM 访问以及配置管理身份验证，请参阅第 36 章，“管理访问”。

资源管理的相关信息

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

资源类

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

资源限制

您可以将个别资源的限制设置为百分比 （如果存在硬性系统限制）或绝对值。

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

默认类

所有未分配至其他类的情景都属于默认类；您不必主动将一个情景分配至默认类。

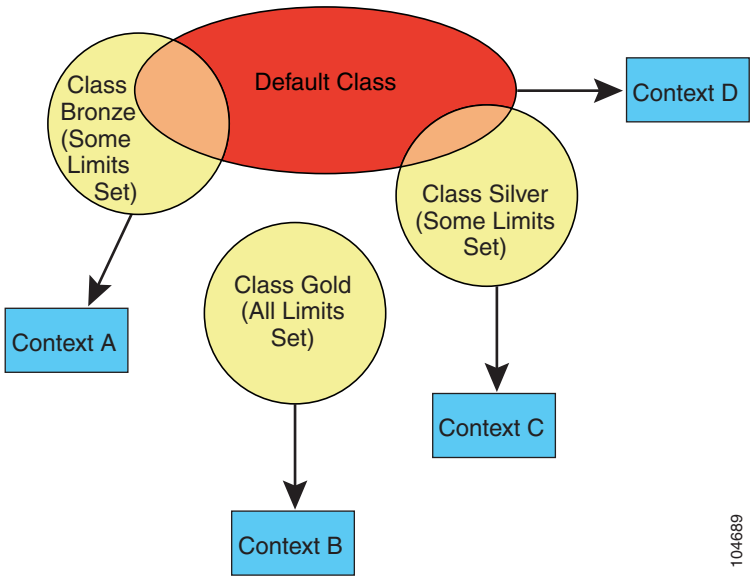
如果某个情景属于默认类之外的其他类，这些类的设置会始终覆盖默认类的设置。但是，如果其他类有任何未定义的设置，则对于这些限制，成员情景会使用默认类的设置。例如，如果您创建一个对所有并发连接有 2% 限制的类，但没有其他限制，则所有其他限制将从默认类继承。相反地，如果您创建一个有着对所有资源的限制的类，则该类不会使用默认类中的任何设置。

对于大多数的资源，默认类会为所有情景提供无限制的资源访问，但以下限制除外：

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

图 7-5 展示了默认类与其他类之间的关系。情景 A 和 C 属于设置了某些限制的类；其他限制会从默认类继承。情景 B 不会从默认类继承任何限制，因为在其类 （Gold 类）中设置了所有限制。情景 D 未分配至某个类，会默认成为默认类的成员。

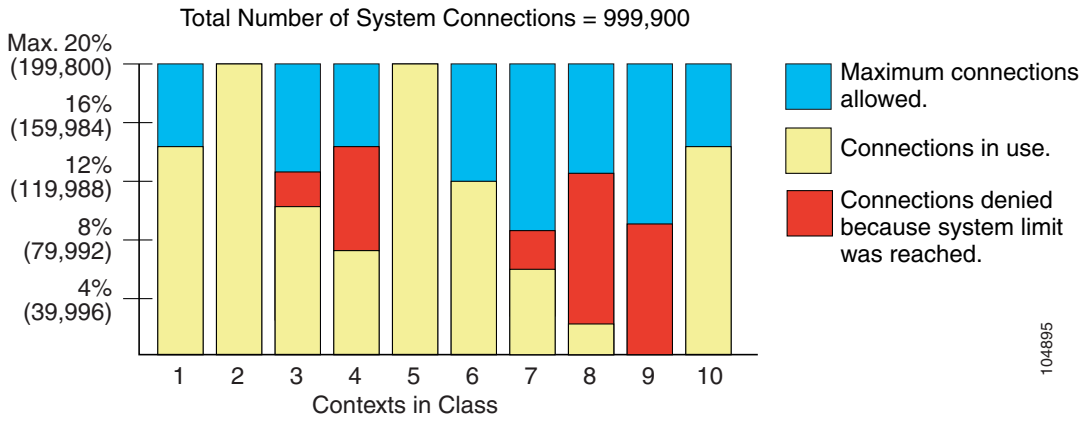
图 7-5　　资源类



使用过度订用的资源

您可以跨所有情景分配超过 100% 的资源 （非突发性 VPN 资源除外），从而过度订用 ASA。例如，您可以设置 Bronze 类，以便将连接限制为每个情景 20%，然后将 10 个情景分配至该类，因而总计为 200%。如果情景并发使用超过系统限制，则每个情景获得的数量少于您想要设置的 20%。（请参阅图 7-6。）

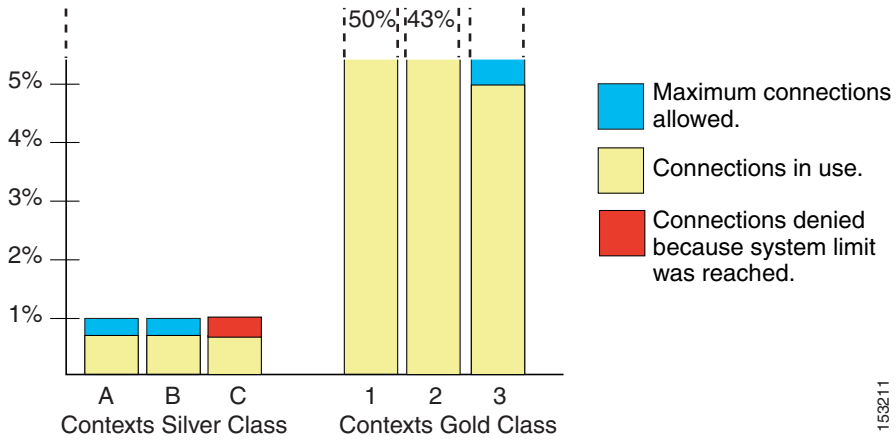
图 7-6　资源过度订用



使用无限制的资源

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

图 7-7　不受限制的资源



MAC 地址的相关信息

为了允许情景共享接口， ASA 会默认为每个共享情景接口分配虚拟 MAC 地址。要自定义或禁用自动生成，请参阅第 7-22 页的自动为情景接口分配 MAC 地址。

MAC 地址用于在情景中对数据包进行分类。如果您共享某个接口，但在每个情景中没有用于该接口的唯一 MAC 地址，则会尝试可能不提供完全覆盖的其他分类方法。有关对数据包进行分类的信息，请参阅第 7-3 页的 ASA 如何对数据包分类。

在生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突的罕见情况下，您可以在情景中为接口手动设置 MAC 地址。要手动设置 MAC 地址，请参阅第 12-10 页的配置 MAC 地址、MTU 和 TCP MSS。

默认 MAC 地址

（8.5(1.7) 和更高版本）自动 MAC 地址生成会默认启用。 ASA 会根据接口 (ASA 5500-X) 或背板 (ASASM) 的 MAC 地址的最后两个字节自动生成前缀。如果需要，您也可以自定义该前缀。

如果您禁用 MAC 地址生成，请参阅以下默认 MAC 地址：

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

另请参阅第 7-12 页的 MAC 地址格式。

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

用手动 MAC 地址交互

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

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

故障转移 MAC 地址

为了用于故障切换， ASA 会为每个接口同时生成主用和备用 MAC 地址。如果主用设备进行故障转移，并且备用设备成为主用设备，新的主用设备将开始使用主用 MAC 地址以最大限度地减少网络中断。有关详细信息，请参阅第 7-12 页的 MAC 地址格式部分。

MAC 地址格式

ASA 会使用以下格式生成 MAC 地址：

A2*xx*.*yyzz*.*zzzz*

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

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

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

对于前缀 1009 (03F1)， MAC 地址为：

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

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

多情景模式的许可要求

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

先决条件

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

准则和限制

本节包括此功能的准则和限制。

防火墙模式准则

在路由和透明防火墙模式中受支持；可以设置每个情景的防火墙模式。

故障转移准则

主用 / 主用模式故障转移仅在多情景模式中受支持。

IPv6 准则

支持 IPv6。

注　跨情景 IPv6 路由不受支持。

不受支持的功能

多情景模式不支持以下功能：

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

附加准则

- 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。
- 如果在闪存根目录中存储情景配置，在某些产品型号上您可能会用尽该目录中的空间，即使当前仍有可用内存也是如此。在这种情况下，请为您的配置文件创建子目录。背景：某些型号（如 ASA 5585-X）的内部闪存使用 FAT16 文件系统，并且，如果您未使用 8.3 兼容的短名称，或使用大写字符，则只能存储数量少于 512 个的文件和文件夹，因为文件系统存储长文件名会用尽空间（请参阅 http://support.microsoft.com/kb/120138/en-us）。

默认设置

- 默认情况下， ASA 处于单情景模式中。
- 请参阅第 7-9 页的默认类。
- 请参阅第 7-11 页的默认 MAC 地址。

配置多情景

本节介绍如何配置多情景模式。

- 第 7-14 页的配置多情景模式的任务流程
- 第 7-14 页的启用或禁用多情景模式
- 第 7-16 页的配置用于资源管理的类
- 第 7-18 页的配置安全情景
- 第 7-22 页的自动为情景接口分配 MAC 地址

配置多情景模式的任务流程

要配置多情景模式，请执行以下步骤：

步骤 1　启用多情景模式。请参阅第 7-14 页的启用或禁用多情景模式。

步骤 2　（可选）配置用于资源管理的类。请参阅第 7-16 页的配置用于资源管理的类。**注意**：对于 VPN 支持，您必须在资源类中配置 VPN 资源；默认类不允许使用 VPN。

步骤 3　在系统执行空间中配置接口。

- ASA 5500-X - 第 10 章，“基本接口配置（ASA 5512-X 及更高版本）”。
- ASASM - 第 2 章，“适用于思科 ASA 服务模块的交换机配置”。

步骤 4　配置安全情景。请参阅第 7-18 页的配置安全情景。

步骤 5　（可选）自定义 MAC 地址分配。请参阅第 7-22 页的自动为情景接口分配 MAC 地址。

步骤 6　完成情景中的接口配置。请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”。

启用或禁用多情景模式

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

ASDM 支持从单模式切换到多模式（如果您使用高可用性和可扩展性向导，并且启用主用 / 主用故障转移）。有关详细信息，请参阅第 8 章，“通过故障转移实现高可用性”。如果您不想使用主用 / 主用故障转移，或者想要切换回单模式，则必须使用 CLI 更改模式；因为更改模式需要确认，您不能使用命令行界面工具。本节介绍如何在 CLI 中更改模式。

- 第 7-15 页的启用多情景模式
- 第 7-15 页的还原单情景模式

启用多情景模式

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

先决条件

备份您的启动配置。当您从单模式转换到多模式时， ASA 会将运行配置转换到两个文件中。系统将不保存原始启动配置。请参阅第 37-12 页的管理文件。

详细步骤

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

还原单情景模式

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

先决条件

在系统执行空间中执行此操作步骤。

详细步骤

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

配置用于资源管理的类

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

先决条件

在系统执行空间中执行此操作步骤。

准则

表 7-1 列出了资源类型和限制。

表 7-1　资源名称和限制

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

表 7-1　资源名称和限制 （续）

资源名称	速率或并发	每个情景的最小和最大数量	系统限制[1]	说明
站点对站点 VPN	并发	不适用	有关对您的产品型号可用的其他 VPN 会话，请参阅第 4-1 页的每个型号的受支持功能许可证。	站点对站点 VPN 会话。您无法过度订用此资源；分配至所有情景的总和不得超出产品型号限制。您分配的此资源会话数保证可供相应情景使用。
SSH	并发	最少 1 个 最多 5 个	100	SSH 会话。
系统日志 / 秒	速率	不适用	不适用	每秒系统日志消息数。
Telnet	并发	最少 1 个 最多 5 个	100	Telnet 会话。
xlates[2]	并发	不适用	不适用	网络地址转换。

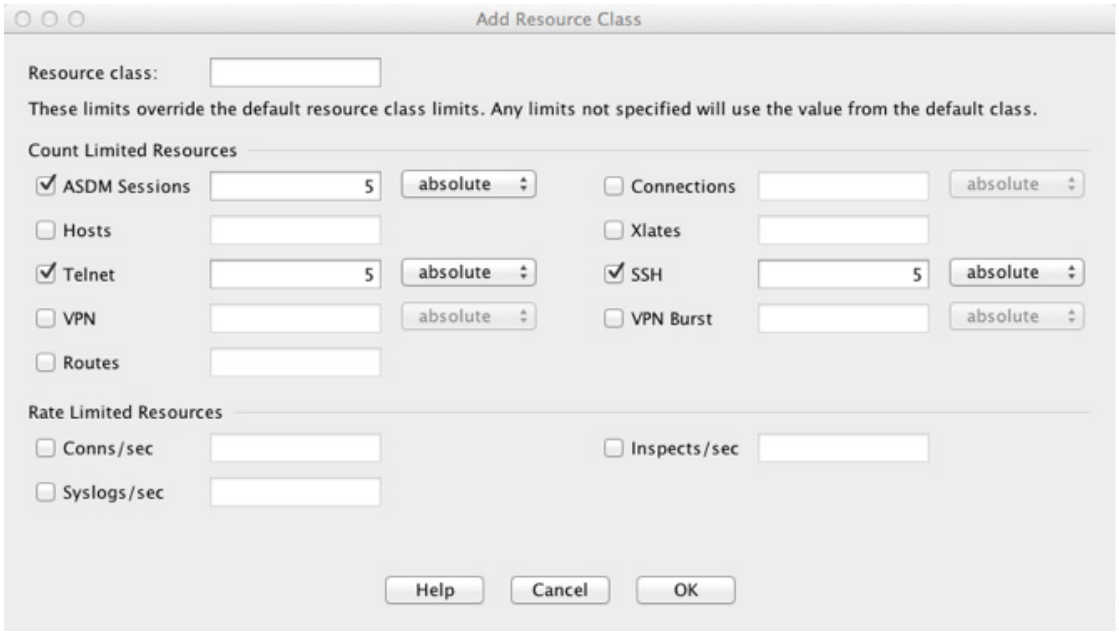
1. 如果此列的值为不适用，则您无法设置该资源的百分比，因为该资源不存在硬性系统限制。
2. 将生成有关限制 （xlates 或 conns 中的较低者）的系统日志消息。例如，如果您将 xlates 限制为 7，将 conns 限制为 9，则 ASA 仅会生成日志消息 321001 (“Resource 'xlates' limit of 7 reached for context 'ctx1'”)，而不会生成 321002 (“Resource 'conn rate' limit of 5 reached for context 'ctx1'”)。

详细步骤

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

步骤 2　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，输入长度最多为 20 个字符的类名称。

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

要查看各个资源类型的说明，请参阅第 7-16 页的表 7-1。

对于没有系统限制的资源，您不能设置百分比；您只能设置绝对值。如果您不设置限制，将从默认类继承限制。如果默认类未设置限制，则表示资源不受限制，或使用系统限制（如有）。对于大多数资源，0 会将限制设置为不受限制。对于 VPN 类型，0 会将限制设置为无。

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

要查看各个资源类型的说明，请参阅第 7-16 页的表 7-1。

如果您不设置限制，将从默认类继承限制。如果默认类未设置限制，则默认为不受限制。0 会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。

先决条件

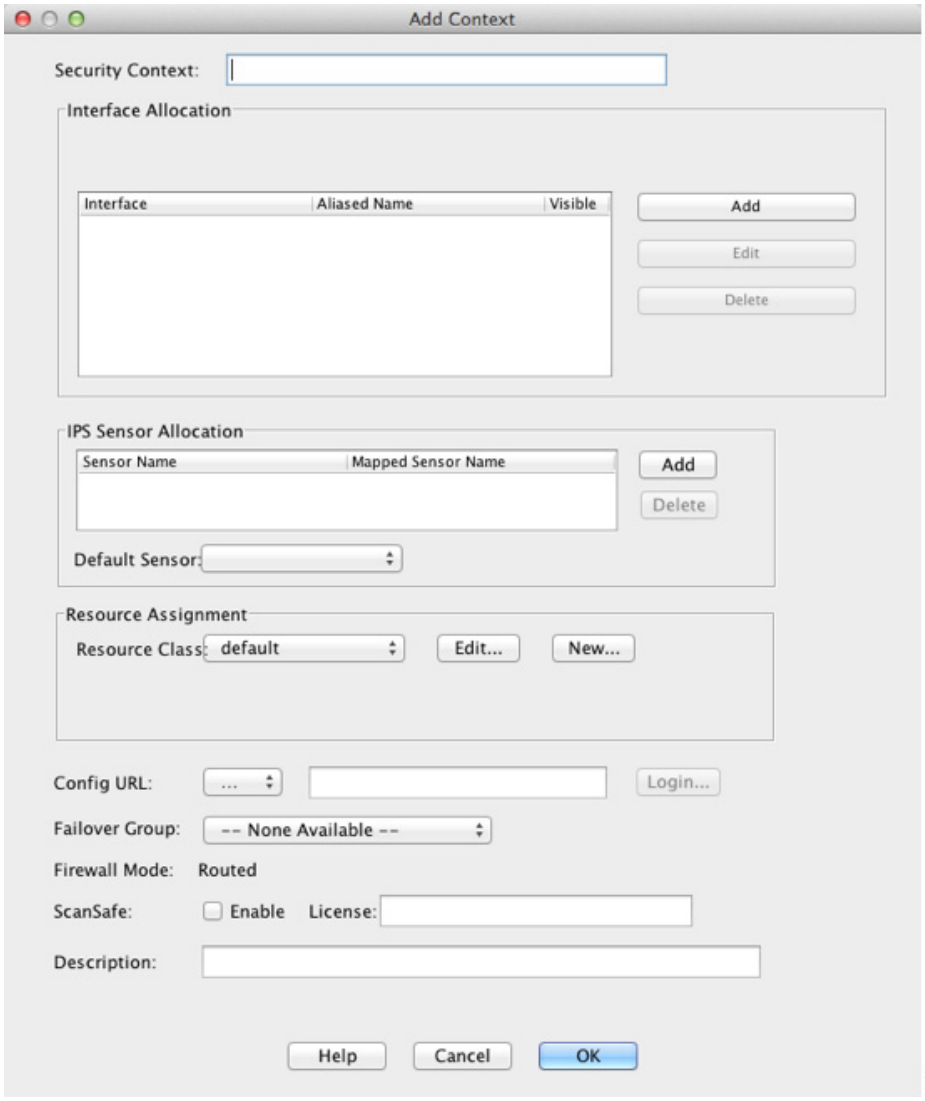
- 在系统执行空间中执行此操作步骤。
- 对于 ASASM，根据第 2 章，“适用于思科 ASA 服务模块的交换机配置”。将 VLAN 分配至交换机上的 ASASM。
- 对于 ASA 5500-X，请根据第 10 章，“基本接口配置（ASA 5512-X 及更高版本）”。配置物理接口参数、VLAN 子接口、EtherChannel 和冗余接口。

详细步骤

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

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

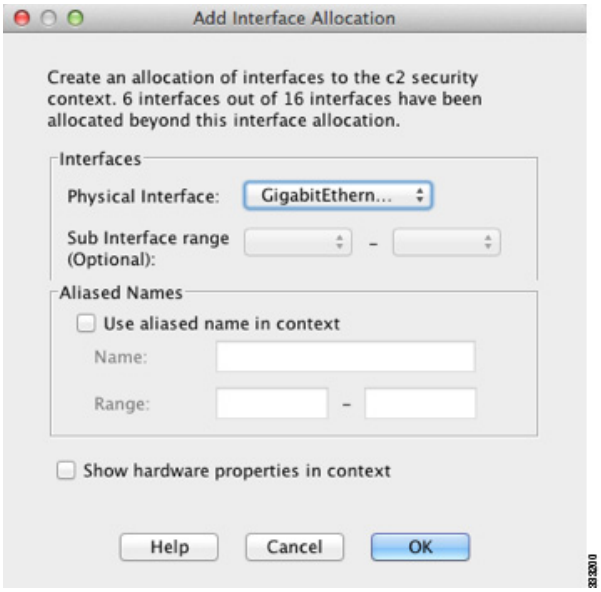
系统将显示 Add Context 对话框。



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。

该名称区分大小写，因此，您可以有名为“customerA”和“CustomerA”的两个情景。“System”或“Null”（大写或小写字母）是保留名称，不能使用。

步骤 4　在 Interface Allocation 区域中，点击 **Add** 按钮，以便将接口分配至情景。



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），也可以分配一个子接口或与从接口关联的一系列子接口。在透明防火墙模式中，仅会显示尚未分配至其他情景的接口。如果主接口已分配至其他情景，则您必须选择子接口。

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 （如可用）。

   在透明防火墙模式中，仅会显示尚未分配至其他情景的子接口。

a. （可选）在 Aliased Names 区域中，选中 **Use Aliased Name in Context** 为此接口设置别名，该别名将代替接口 ID 用于情景配置。

   – 在 Name 字段中，设置别名。

     别名必须以字母开头，以字母结束，并且仅可包含字母、数字或下划线内部字符。此字段允许您指定以字母或下划线结束的名称；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。

     如果您有子接口范围，可以输入添加到名称之后的数字的范围。

b. （可选）要允许情景用户查看物理接口属性 （即使您设置别名），请选中 **Show Hardware Properties in Context**。

c. 点击 **OK** 返回 Add Context 对话框。

步骤 5　（可选）如果您使用 IPS 虚拟传感器，请在 IPS Sensor Allocation 区域中将传感器分配至情景。

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）要将此情景分配至资源类，请从 Resource Assignment > Resource Class 下拉列表中选择类名称。

您可以直接在此区域中添加或编辑资源类。有关详细信息，请参阅第 7-16 页的配置用于资源管理的类。

步骤 7　要设置情景配置位置，请从 Config URL 下拉列表中选择文件系统类型，然后在字段中输入路径，从而确定 URL。

例如，FTP 的组合 URL 格式如下：

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

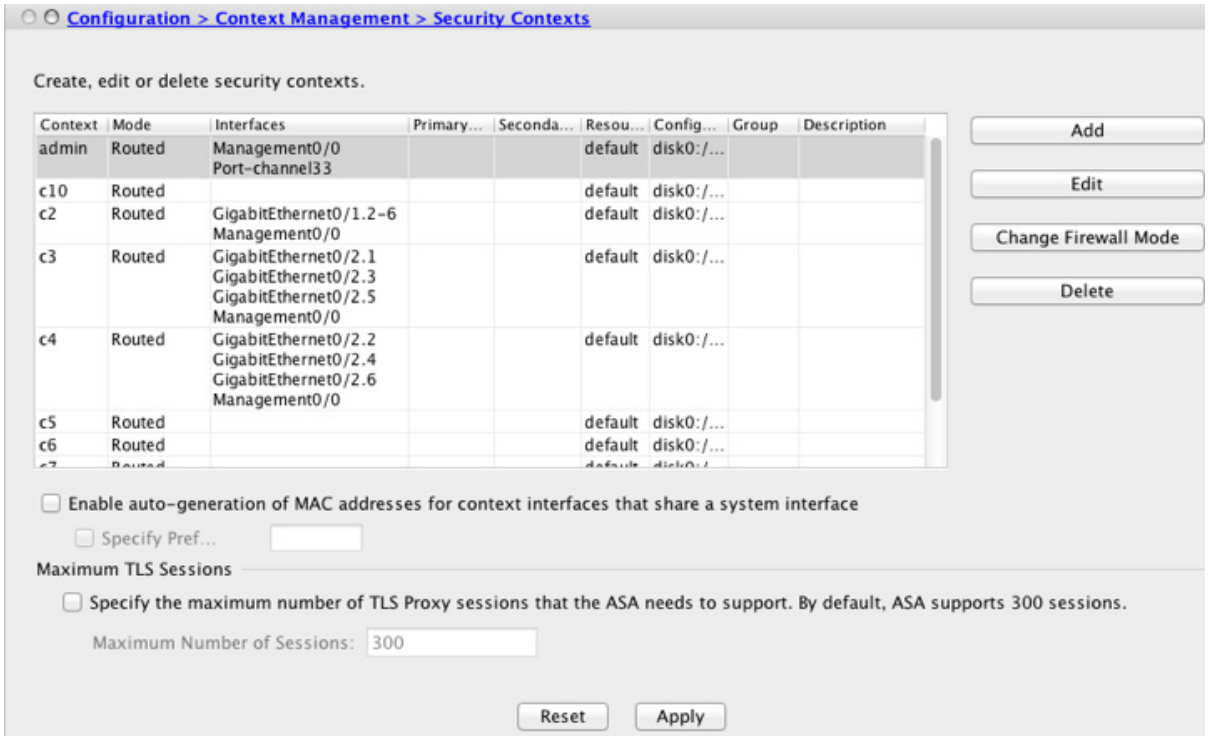
a. （可选）对于外部文件系统，请点击 **Login** 设置用户名和密码。

步骤 8　（可选）要设置主用 / 主用故障转移的故障转移组，请从 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 检查，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。

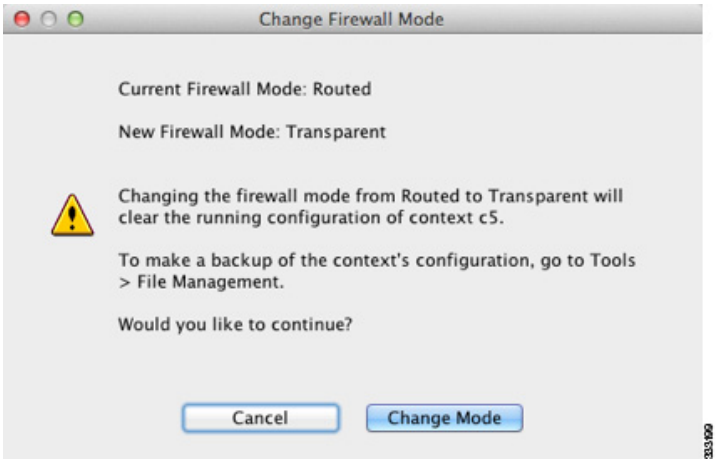
步骤 10　（可选）在 Description 字段中添加说明。

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** 更改为透明防火墙模式。

如果是现有情景，在更改模式之前，请务必备份配置。

注　您不能更改当前在 ASDM 中连接的模式（通常为管理情景）；有关通过命令行设置模式的信息，请参阅第 5-8 页的设置防火墙模式（单模式）。

步骤 13　要自定义 MAC 地址的自动生成，请参阅第 7-22 页的自动为情景接口分配 MAC 地址。

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

自动为情景接口分配 MAC 地址

本节介绍如何配置 MAC 地址的自动生成。

MAC 地址用于在情景中对数据包进行分类。有关详细信息，请参阅第 7-11 页的 MAC 地址的相关信息，尤其是您从早期 ASA 版本升级时。另请参阅第 7-30 页的查看分配的 MAC 地址。

准则

- 当您在情景中为接口配置 命令名称时，将立即生成新 MAC 地址。如果您在配置情景接口后启用此功能，则在您启用之后，会立即为所有接口生成 MAC 地址。如果您禁用此功能，每个接口的 MAC 地址将还原为默认 MAC 地址。例如， GigabitEthernet0/1 子接口还原为使用 GigabitEthernet0/1 的 MAC 地址。
- 在生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突的罕见情况下，您可以在情景中为接口手动设置 MAC 地址。要手动设置 MAC 地址，请参阅第 12-10 页的配置 MAC 地址、MTU 和 TCP MSS。

详细步骤

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

步骤 2　选择 **Configuration > Context Management > Security Contexts**，然后选中 **Mac-Address auto**。如果您未输入前缀，则 ASA 将根据接口 (ASA 5500-X) 或背板 (ASASM) MAC 地址的最后两个字节自动生成前缀。

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。

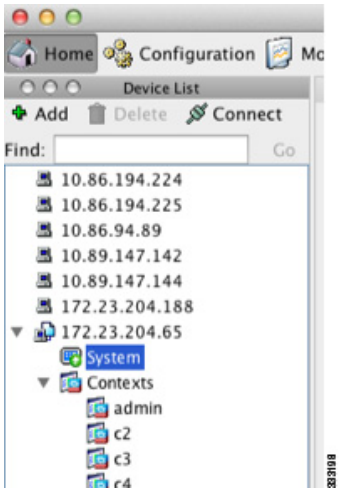
此前缀会被转换为四位数的十六进制数值，并用作 MAC 地址的一部分。有关此前缀使用方式的详细信息，请参阅第 7-12 页的 MAC 地址格式。

在情景和系统执行空间之间切换

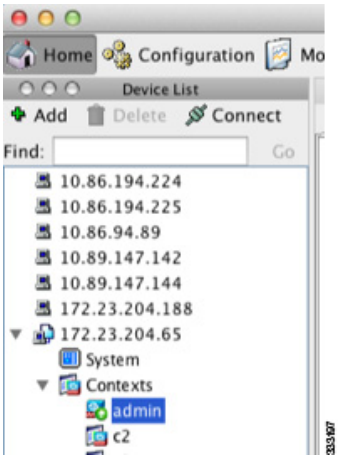
如果您登录到系统执行空间 （或管理情景），则可以在情景之间切换，并在每个情景中执行配置和监控任务。您在配置模式中编辑的运行配置取决于您的位置。 当您处于系统执行空间时，运行配置仅包含系统配置；当您处于某个情景时，运行配置仅包含该情景。

详细步骤

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



步骤 2　要配置一个情景，请在 Device List 窗格中，双击主用设备 IP 地址下的情景名称。



管理安全情景

此部分介绍如何管理安全情景。

- 第 7-24 页的移除安全情景
- 第 7-25 页的更改管理情景
- 第 7-26 页的更改安全情景 URL
- 第 7-27 页的重新加载安全情景

移除安全情景

您不能移除当前管理情景。

注　如果使用故障转移，从您在主用设备上移除情景到该情景在备用设备上被移除之间存在一定延迟。

先决条件

在系统执行空间中执行此操作步骤。

详细步骤

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

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

步骤 3　选择您想要删除的情景，点击 **Delete**。

系统将显示 Delete Context 对话框。

步骤 4　如果您想要以后重新添加此情景，并想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。

如果您要删除配置文件，请使复选框保持选中。

步骤 5　点击 **Yes**。

更改管理情景

系统配置本身不包括任何网络接口或网络设置；相反，当系统需要访问网络资源时 （例如，从服务器下载情景），它将使用被指定为管理员情景的情景之一。

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

注　对于 ASDM，您不能在 ASDM 中更改管理情景，因为您的 ASDM 会话会断开。您可以使用命令行界面工具执行此操作步骤，但请注意，您必须重新连接到新的管理情景。

准则

您可以将任意情景设置为管理情景，只要其配置文件存储在内部闪存中。

先决条件

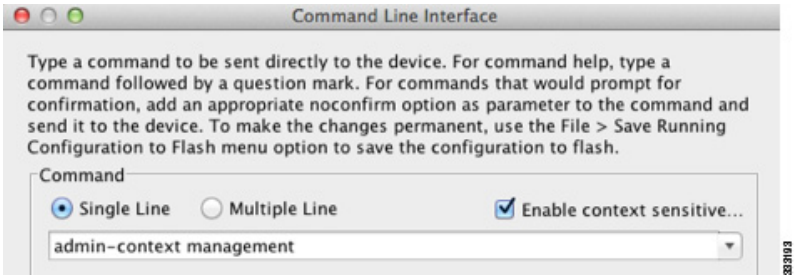
在系统执行空间中执行此操作步骤。

详细步骤

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

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

系统将显示 Command Line Interface 对话框。



步骤 3　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。您必须重新连接到新的管理情景。

注　某些系统配置命令（包括 **ntp server**）会标识属于管理情景的接口名称。如果您更改管理情景，并且新的管理情景中不存在该接口名称，请务必更新引用该接口的所有系统命令。

更改安全情景 URL

本节介绍如何更改情景 URL。

准则

- 在没有通过新的 URL 重新加载配置的情况下，您不能更改安全情景 URL。 ASA 会将新配置与当前运行配置合并。
- 重新输入相同 URL 也会将保存的配置与运行配置合并。
- 合并会将新配置中的所有新命令添加至运行配置。
  - 如果配置相同，则不会发生更改。
  - 如果命令有冲突，或者如果命令影响情景运行，则合并的效果取决于命令。可能出现错误，或者出现意外结果。如果运行配置为空（例如，如果服务器不可用并且从未下载过配置），则会使用新配置。
- 如果您不想合并配置，可以清除运行配置（这会中断通过该情景的所有通信），然后通过新的 URL 重新加载配置。

先决条件

在系统执行空间中执行此操作步骤。

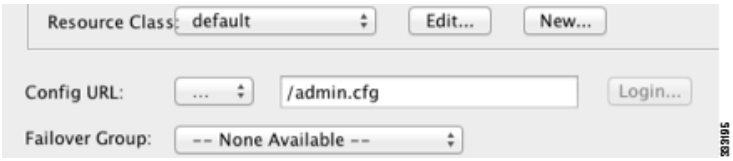
详细步骤

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

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

步骤 3　选择您想要编辑的情景，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，因此情景将会运行。

重新加载安全情景

您可以通过两种方式重新加载情景：

- 清除运行配置，然后导入启动配置。

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

  此操作会清除其他属性，例如，可能对故障排除很有用的内存分配。但是，将情景添加回系统要求您重新指定 URL 和接口。

- 第 7-27 页的通过清除配置来重新加载
- 第 7-28 页的通过删除情景然后重新添加来重新加载

通过清除配置来重新加载

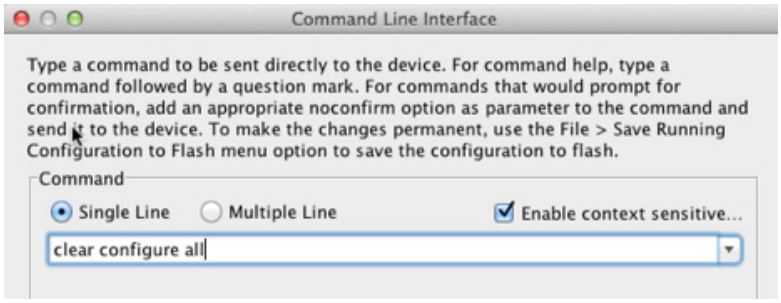
要通过清除情景配置并通过 URL 重新加载配置来重新加载情景，请执行以下操作步骤。

详细步骤

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　选择 **Tools > Command Line Interface**。

系统将显示 Command Line Interface 对话框。



步骤 3　输入以下命令：

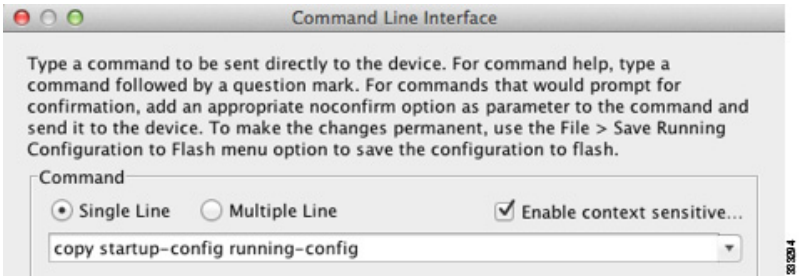
```
clear configure all
```

步骤 4　点击 **Send**。

情景配置会被清除。

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　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。您不能在情景中更改此 URL。

通过删除情景然后重新添加来重新加载

要通过删除情景，然后重新添加来重新加载该情景，请执行以下部分中的操作步骤：

1. 第 7-24 页的移除安全情景。请确保取消选中 **Also delete config URL file from the disk** 复选框。
2. 第 7-18 页的配置安全情景

监控安全情景

本节介绍如何查看和监控情景信息。

监控情景资源使用情况

要从系统执行空间中，监控所有情景的资源使用情况，请执行以下操作步骤：

步骤 1　如果您未处于系统模式，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，以便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 (#) - 显示当前的 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 规则数总和的百分比。
  - 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度。
  - 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度。
  - Syslog Rate (%) - 显示此情景生成的系统日志消息数量占所有情景生成的系统日志消息数量总和的百分比。
  - 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 站点对站点隧道的使用情况。
  - 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，隧道数量的峰值。

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。

- 第 7-30 页的查看系统配置中的 MAC 地址
- 第 7-31 页的查看情景中的 MAC 地址

查看系统配置中的 MAC 地址

本节介绍如何查看系统配置中的 MAC 地址。

准则

如果您手动为接口分配 MAC 地址，但也启用了自动生成，自动生成的地址会继续显示在配置中，即使正在使用的是手动 MAC 地址。如果您随后移除手动 MAC 地址，则会使用所显示的自动生成的地址。

详细步骤

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

步骤 2　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。

详细步骤

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

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

此表显示了正在使用的 MAC 地址；如果您手动分配 MAC 地址，并且也启用了自动生成，则您只能查看系统配置中未使用的自动生成地址。

多情景模式的功能历史记录

表 7-2 列出了各种功能变更以及实施该等功能变更的平台版本。 ASDM 可向后兼容多个平台版本，因此，未列出已添加支持的具体 ASDM 版本。

表 7-2　多情景模式的功能历史记录

功能名称	平台版本	功能信息
多个安全情景	7.0(1)	引入了多情景模式。 我们引入了以下屏幕：Configuration > Context Management。
自动的 MAC 地址分配	7.2(1)	引入了至情景接口的 MAC 地址自动分配。 我们修改了以下屏幕：Configuration > Context Management > Security Contexts。
资源管理	7.2(1)	引入了资源管理。 我们引入了以下屏幕：Configuration > Context Management > Resource Management。
IPS 的虚拟传感器	8.0(2)	运行 IPS 软件 6.0 版本及更高版本的 AIP SSM 可以运行多个虚拟传感器，这意味着您可以在该 AIP SSM 上配置多个安全策略。您可以将每个情景或单模式 ASA 分配至一个或多个虚拟传感器，也可以将多个安全情景分配至相同的虚拟传感器。 我们修改了以下屏幕：Configuration > Context Management > Security Contexts。
增强的自动 MAC 地址分配	8.0(5)/8.2(2)	MAC 地址格式更改为使用前缀，以便使用固定起始值 (A2)，并将不同方案用于故障转移对中的主设备和辅助设备 MAC 地址。现在，MAC 地址在重新加载之后也会保持不变。现在，命令解析器会检查是否已启用自动生成；如果您还想要手动分配 MAC 地址，则不能使用以 A2 开头的手动 MAC 地址。 我们修改了以下屏幕：Configuration > Context Management > Security Contexts。

表 7-2　　多情景模式的功能历史记录 （续）

功能名称	平台版本	功能信息
增加了 ASA 5550 和 5580 的最大情景数量。	8.4(1)	ASA 5550 的最大安全情景数量已从 50 增加到 100。 ASA 5580 的最大安全情景数量已从 50 增加到 250。
自动的 MAC 地址分配默认启用。	8.5(1)	自动的 MAC 地址分配现在已默认启用。 我们修改了以下屏幕：Configuration > Context Management > Security Contexts。
MAC 地址前缀的自动生成	8.6(1)	在多情景模式中， ASA 现在会将自动 MAC 地址生成配置转换为使用默认前缀。 ASA 会根据接口 (ASA 5500-X) 或背板 (ASASM) 的 MAC 地址的最后两个字节自动生成前缀。当您重新加载或重新启用 MAC 地址生成时，系统将自动执行此转换。前缀生成方法有很多的优势，包括更好地保证 MAC 地址在网段上的唯一性。如果您想要更改此前缀，可以使用自定义前缀重新配置此功能。旧版的 MAC 地址生成方法不再可用。 **注**　为了保持故障转移对的无中断升级功能， ASA 在重新加载时 （如果已启用故障转移）*不会*转换现有配置中的 MAC 地址方法。但是，使用故障转移时，我们强烈建议您手动更改为生成的前缀方法，对于 ASASM 尤其如此。如果不使用前缀方法，安装在不同插槽编号中的 ASASM 在故障转移时会发生 MAC 地址更改，并且会出现流量中断。升级后，要使用 MAC 地址生成的前缀方法，请重新启用 MAC 地址自动生成来使用默认前缀。 我们修改了以下屏幕：Configuration > Context Management > Security Contexts
安全情景中的动态路由	9.0(1)	多情景模式中现在支持 EIGRP 和 OSPFv2 动态路由协议。 OSPFv3、 RIP 和组播路由不受支持。
用于路由表条目的新资源类型	9.0(1)	创建了新资源类型 routes，以用于设置每个情景中的最大路由表条目数。 我们修改了以下屏幕：Configuration > Context Management > Resource Class > Add Resource Class
多情景模式中的站点对站点 VPN	9.0(1)	多情景模式中现在支持站点对站点 VPN 隧道。
用于站点对站点 VPN 隧道的新资源类型	9.0(1)	创建了新资源类型 vpn other 和 vpn burst other，以用于设置每个情景中的站点对站点 VPN 隧道最大数目。 我们修改了以下屏幕：Configuration > Context Management > Resource Class > Add Resource Class

通过故障转移实现高可用性

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

关于故障转移

故障转移概述

配置故障转移需要通过专用故障转移链路和有状态链路 （可选）相互连接的两台相同的 ASA。系统会对主用设备和接口的运行状况进行监控，以便确定是否符合特定的故障转移条件。如果符合这些条件，将执行故障转移。

ASA 支持两种故障转移模式：主用 / 主用故障转移和主用 / 备用故障转移。每种故障转移模式都有自己确定和执行故障转移的方法。

- 在主用 / 备用故障转移中，一台设备是主用设备。它会传送流量。备用设备不会主动传送流量。发生故障转移时，主用设备会故障转移到备用设备，后者随即变为主用状态。您可以将主用 / 备用故障转移用于单情景或多情景模式中的 ASA。
- 在主用 / 主用故障转移配置下，两台 ASA 都可以传送网络流量。主用 / 主用故障转移仅适用于多情景模式中的 ASA。在主用 / 主用故障转移中，您可将 ASA 上的安全情景划分为 2 个*故障转移组*。故障转移组就是一个或多个安全情景的逻辑组。一个组会分配到主 ASA 上，处于主用状态；另一个组会分配到辅助 ASA 上，处于主用状态。发生故障转移时，会在故障转移组级别进行。

两种故障转移模式都支持有状态或无状态故障转移。

故障转移系统要求

本部分介绍，在故障转移配置下，对于 ASA 的硬件、软件和许可证要求。

- 第 8-2 页的硬件要求
- 第 8-2 页的软件要求
- 第 8-3 页的许可证要求

硬件要求

故障转移配置下的两台设备必须：

- 型号相同。
- 拥有相同数量和类型的接口。
- 安装有相同的模块 （如有）
- 安装有相同的 RAM。

如果您在故障转移配置中，使用闪存大小不同的设备，请确保闪存较小的设备有足够的空间来容纳软件映像文件和配置文件。如果闪存较小的设备没有足够的空间，从闪存较大的设备向闪存较小的设备进行配置同步将会失败。

软件要求

故障转移配置下的两台设备必须：

- 处于相同的防火墙模式 （路由或透明）。
- 处于相同的情景模式 （单情景或多情景）。
- 具有相同的主要 （第一个数字）和次要 （第二个数字）软件版本。然而，您可以在升级过程中临时使用不同的软件版本；例如，您可以将一台设备从 8.3(1) 版本升级到 8.3(2) 版本，并使故障转移保持活动状态。我们建议将两台设备都升级为相同版本，以便确保长期的兼容性。

有关升级故障转移对上的软件的详细信息，请参阅第 37-6 页的升级故障转移对或 ASA 集群。

- 安装有相同的 AnyConnect 映像。如果在执行无中断升级时，故障转移对具有不匹配的映像，则无客户端 SSL VPN 连接会在升级过程的最终重新启动步骤终止，数据库会显示一个孤立会话，并且 IP 池会显示分配给客户端的 IP 地址 “ 正在使用中 ”。

许可证要求

故障转移配置下的两台设备不需要具有相同的许可证；许可证将整合为故障转移集群许可证。有关详细信息，请参阅第 4-24 页的故障转移或 ASA 集群许可证。

故障转移和有状态故障转移链路

故障转移链路和可选的有状态故障转移链路是两台设备之间的专用连接。

- 第 8-3 页的故障转移链路
- 第 8-4 页的有状态故障转移链路
- 第 8-5 页的避免中断故障转移和数据链路

注意事项　除非您使用 IPsec 隧道或故障转移密钥保护通信，否则所有信息会以明文形式通过故障转移和有状态链路发送。如果使用 ASA 终止 VPN 隧道，此信息包括用于建立隧道的所有用户名、密码和预共享密钥。以明文形式发送该敏感数据可能会带来严重的安全风险。如果您使用 ASA 来终止 VPN 隧道，我们建议使用 IPsec 隧道或故障转移密钥来保护故障转移通信。

故障转移链路

故障转移对中的两台设备会不断地通过故障转移链路进行通信，以便确定每台设备的运行状态。

- 第 8-3 页的故障转移链路数据
- 第 8-3 页的故障转移链路接口
- 第 8-4 页的连接故障转移链路

故障转移链路数据

以下信息将通过故障转移链路传输：

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

故障转移链路接口

您可以将任意未使用的接口 （物理、冗余或 EtherChannel）用作故障转移链路；然而，您不能指定当前已配置名称的接口。故障转移链路接口不会配置为常规网络接口；该接口仅会因为故障转移而存在。此接口仅可用于故障转移链路 （或者也用于有状态链路）。

连接故障转移链路

可以使用以下两种方法之一连接故障转移链路：

- 使用不与任何其他设备处于相同网段（广播域或 VLAN）的交换机作为 ASA 的故障转移接口。
- 使用以太网电缆直接连接设备，无需外部交换机。

如果您不在设备之间使用交换机，当接口出现故障时，两台对等设备之间的链路将会断开。这种情况可能会妨碍故障排除工作，因为您无法轻松确定接口发生故障，导致链路断开的设备。

ASA 在其铜缆以太网端口上支持自动 MDI/MDIX，因此，您可以使用交叉电缆或直通电缆。如果您使用的是直通电缆，接口会自动检测该电缆，并将其中一个发送 / 接收对交换为 MDIX。

有状态故障转移链路

要使用有状态故障转移，您必须配置有状态故障转移链路 （也称为有状态链路），以便传送连接状态信息。

您有三种可用于有状态链路的接口选项：

- 第 8-4 页的专用接口 （建议）
- 第 8-4 页的共享故障转移链路
- 第 8-4 页的共享常规数据接口 （不推荐）

注　请勿将管理接口用于有状态链路。

专用接口 （建议）

您可以将专用接口 （物理、冗余或 EtherChannel）用于有状态链路。可以使用以下两种方法之一连接专用的有状态链路：

- 使用不与任何其他设备处于相同网段（广播域或 VLAN）的交换机作为 ASA 的故障转移接口。
- 使用以太网电缆直接连接设备，无需外部交换机。

  如果您不在设备之间使用交换机，当接口出现故障时，两台对等设备之间的链路将会断开。这种情况可能会妨碍故障排除工作，因为您无法轻松确定接口发生故障，导致链路断开的设备。

  ASA 在其铜缆以太网端口上支持自动 MDI/MDIX，因此，您可以使用交叉电缆或直通电缆。如果您使用的是直通电缆，接口会自动检测该电缆，并将其中一个发送 / 接收对交换为 MDIX。

使用长距离故障转移时，为实现最佳性能，故障转移链路的延迟应该低于 10 毫秒且不超过 250 毫秒。如果延迟超过 10 毫秒，重新传输故障转移消息会导致一些性能降级。

共享故障转移链路

如果您没有足够的接口，可能有必要共享故障转移链路。如果您将故障转移链路用作有状态链路，应使用最快的可用以太网接口。如果该接口存在性能问题，请考虑将一个独立接口专门用于有状态链路。

共享常规数据接口 （不推荐）

与有状态链路共享数据接口，可能会使您易于遭受重播攻击。此外，大量有状态故障转移流量可能会在接口上发送，从而导致该网段上出现性能问题。

将数据接口用作有状态链路，仅在单情景路由模式中受支持。

避免中断故障转移和数据链路

我们建议，让故障转移链路和数据接口使用不同的路径，以便降低所有接口同时发生故障的可能性。如果故障转移链路发生故障， ASA 可使用数据接口来确定是否需要进行故障转移。随后，故障转移操作会被挂起，直到故障转移链路恢复正常。

请参阅以下连接方案，以便设计具有弹性的故障转移网络。

方案 1 - 不推荐

如果单台交换机或一组交换机用于连接两台 ASA 之间的故障转移和数据接口，则交换机或交换机间链路发生故障时，两台 ASA 都将处于主用状态。因此，不推荐使用图 8-1 和图 8-2 中展示的以下两种连接方法。

图 8-1　使用单台交换机进行连接 - 不推荐

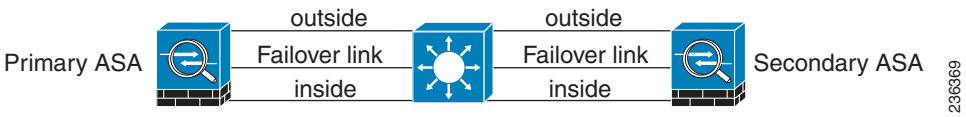
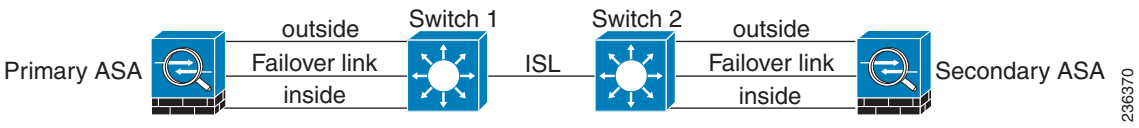


图 8-2　使用两台交换机进行连接 - 不推荐



方案 2 - 推荐

我们不推荐让故障转移链路和数据接口使用相同的交换机。而是应使用不同的交换机或使用直连电缆来连接故障转移链路，如图 8-3 和图 8-4 中所示。

图 8-3　使用不同的交换机进行连接

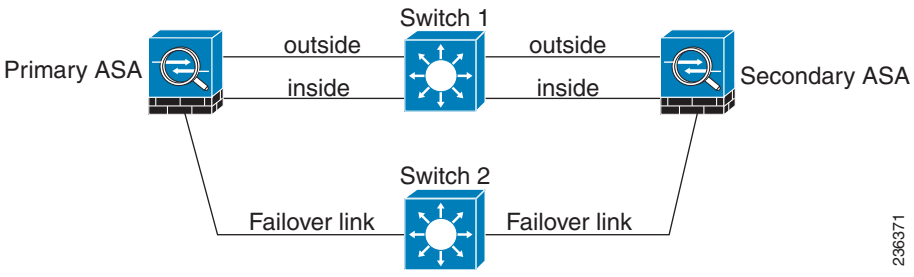
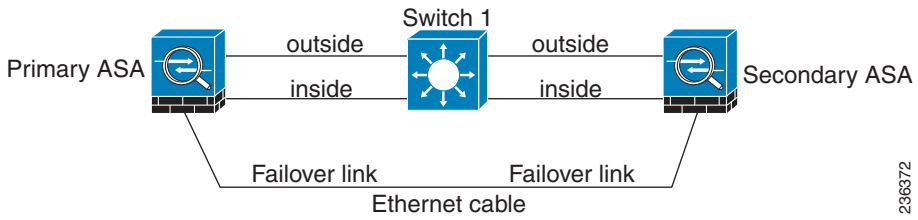


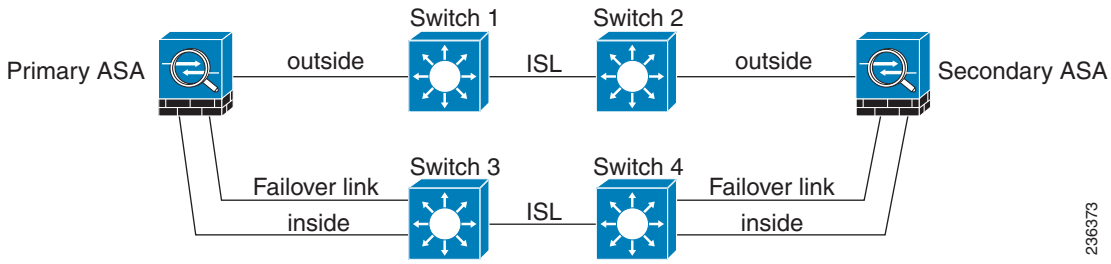
图 8-4　使用电缆进行连接



方案 3 - 推荐

如果 ASA 数据接口连接到多台交换机，则故障转移链路可以连接到其中一台交换机，最好是处于网络的安全一侧 （内部）的交换机，如图 8-5 中所示。

图 8-5　使用安全的交换机进行连接



方案 4 - 推荐

最可靠的故障转移配置使用故障转移链路上的冗余接口，如图 8-6 和图 8-7 中所示。

图 8-6　使用冗余接口进行连接

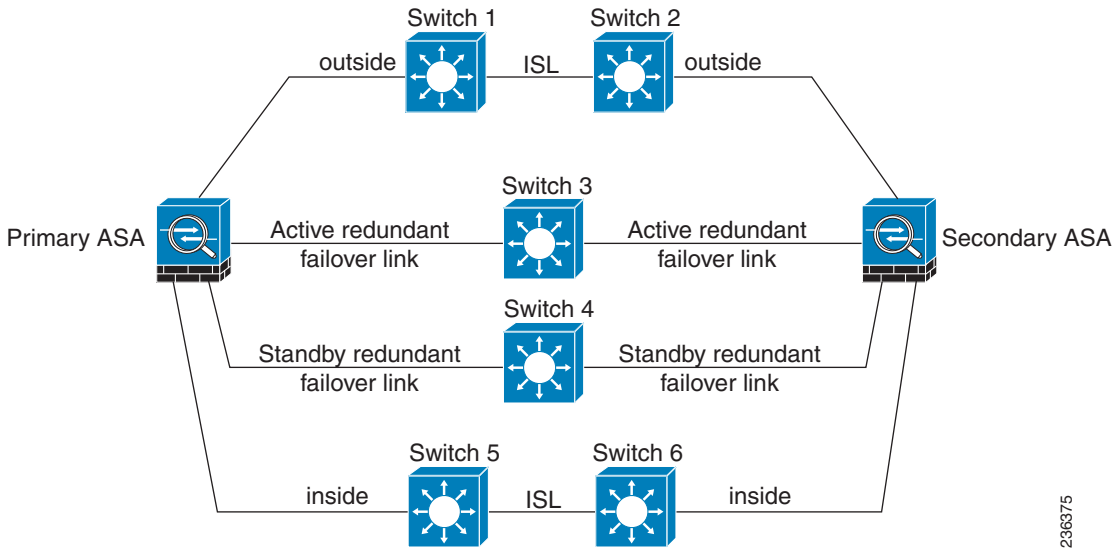
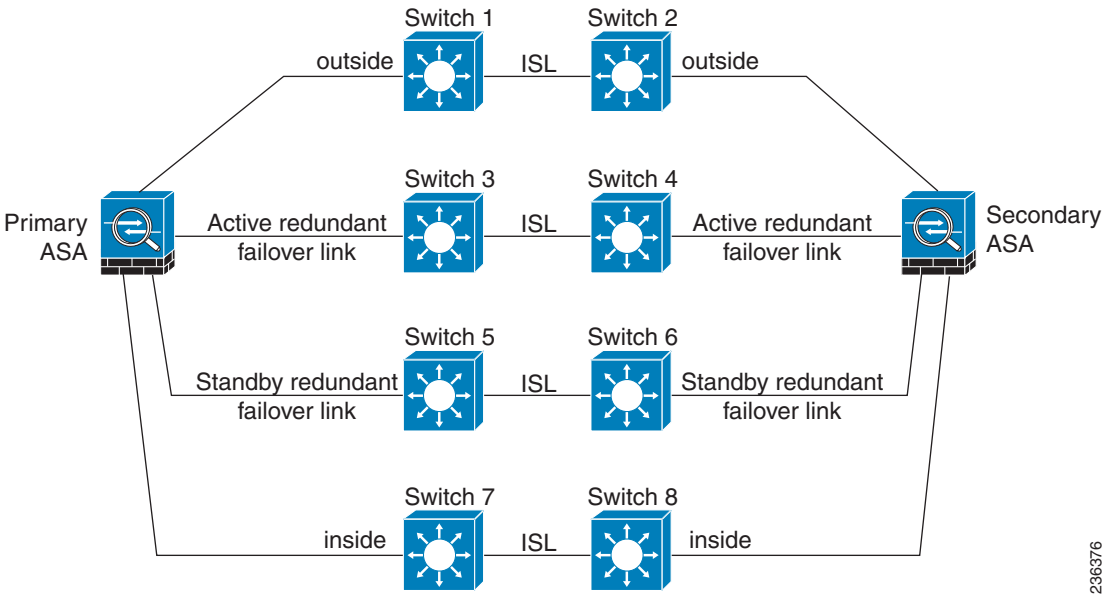


图 8-7　　使用交换机间链路进行连接



MAC 和 IP 地址

当您配置接口时，必须在相同网络上指定一个主用 IP 地址和一个备用 IP 地址。

1. 当主设备或故障转移组进行故障转移时，辅助设备会使用主设备的 IP 地址和 MAC 地址，并开始传送流量。
2. 此时处于备用状态的设备会接管备用 IP 地址和 MAC 地址。

由于网络设备不会发现 MAC 与 IP 地址配对的变化，网络上的任意位置都不会发生 ARP 条目变化或超时。

注　如果辅助设备启动时未检测到主设备，辅助设备将成为主用设备，并使用其自己的 MAC 地址，因为它不知道主设备的 MAC 地址。但是，当主设备变得可用时，辅助（主用）设备会将 MAC 地址更改为主设备的地址，这会导致网络流量中断。同样地，如果使用新硬件替换主设备，也会使用新的 MAC 地址。

使用虚拟 MAC 地址可防范这种中断，因为对于启动时的辅助设备，主用 MAC 地址是已知的，并在采用新的主设备硬件时保持不变。在多情景模式中， ASA 会默认生成虚拟的主用和备用 MAC 地址。有关详细信息，请参阅第 7-11 页的 MAC 地址的相关信息。在单情景模式中，您可以手动配置虚拟 MAC 地址；有关详细信息，请参阅第 8-25 页的配置主用 / 主用故障转移。

如果您没有配置虚拟 MAC 地址，您可能需要清除连接的路由器上的 ARP 表，以便还原流量。ASA 在 MAC 地址变化时，不会为静态 NAT 地址发送无故 ARP，因此，连接的路由器不会知道这些地址的 MAC 地址变化。

注　进行故障转移时，有状态链路的 IP 地址和 MAC 地址不会更改；唯一例外的是，在常规数据接口上配置了有状态链路的情况。

ASA 服务模块 的机箱内和机箱间模块的布置

您可以将主和辅助 ASASM 布置在相同交换机内，也可以将其布置在两台不同的交换机中。以下部分介绍各个选项：

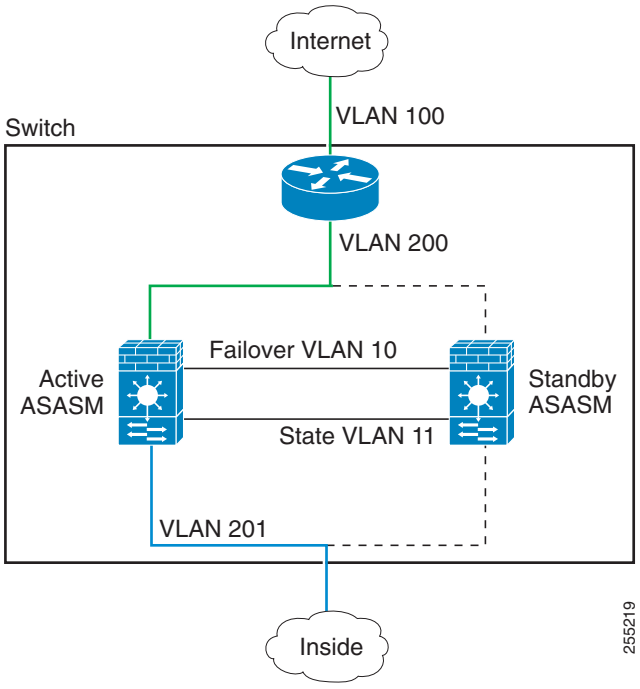
机箱内故障转移

如果您将辅助 ASASM 与主 ASASM 安装在相同交换机中，则可以防御模块级别的故障。要防御交换机级别的故障以及模块级别的故障，请参阅第 8-8 页的机箱间故障转移。

即使两台 ASASM 均已分配相同的 VLAN，仅主用模块会参与联网。备用模块不会传送任何流量。

图 8-8 展示了典型的交换机内配置。

图 8-8　交换机内故障转移



机箱间故障转移

要防御交换机级别的故障，您可以将辅助 ASASM 安装在不同的交换机中。 ASASM 不直接与交换机协调故障转移，但是，它可以协调地配合交换机故障转移操作。请参阅交换机文档，以便配置交换机的故障转移。

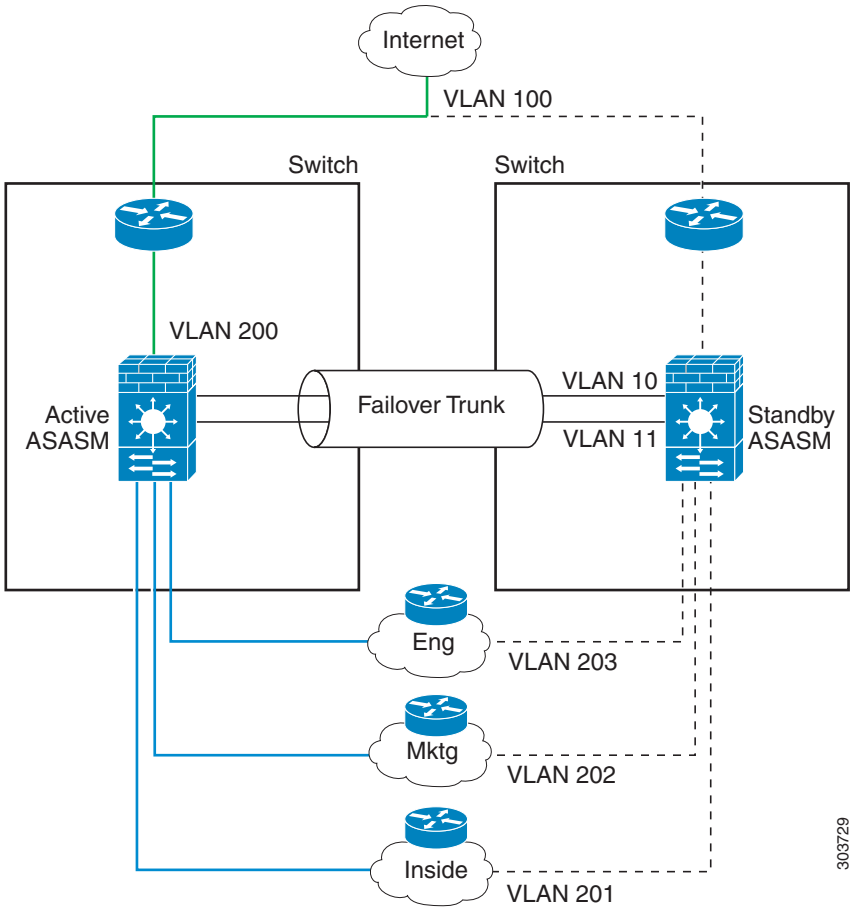
要在 ASASM 之间实现最佳的故障转移通信可靠性，我们建议您在两台交换机之间配置 EtherChannel Trunk 端口，以便承载故障转移和有状态 VLAN。

对于其他 VLAN，您必须确保两台交换机都可以访问所有防火墙 VLAN，并且受监控的 VLAN 能够成功地在两台交换机之间发送 Hello 数据包。

图 8-9 展示了典型的交换机和 ASASM 冗余配置。两台交换机之间的 Trunk 会承载故障转移 ASASM VLAN （VLAN 10 和 11）。

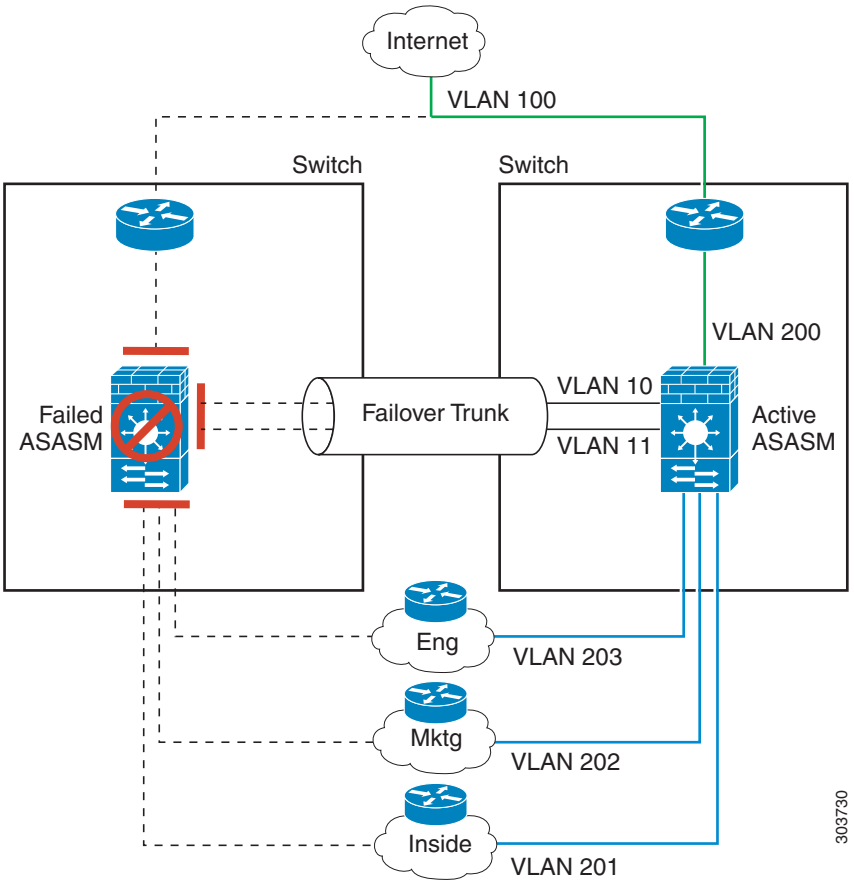
注　ASASM 故障转移与交换机故障转移操作无关；但是，ASASM 可在任何一种交换机故障转移方案下工作。

图 8-9　正常操作



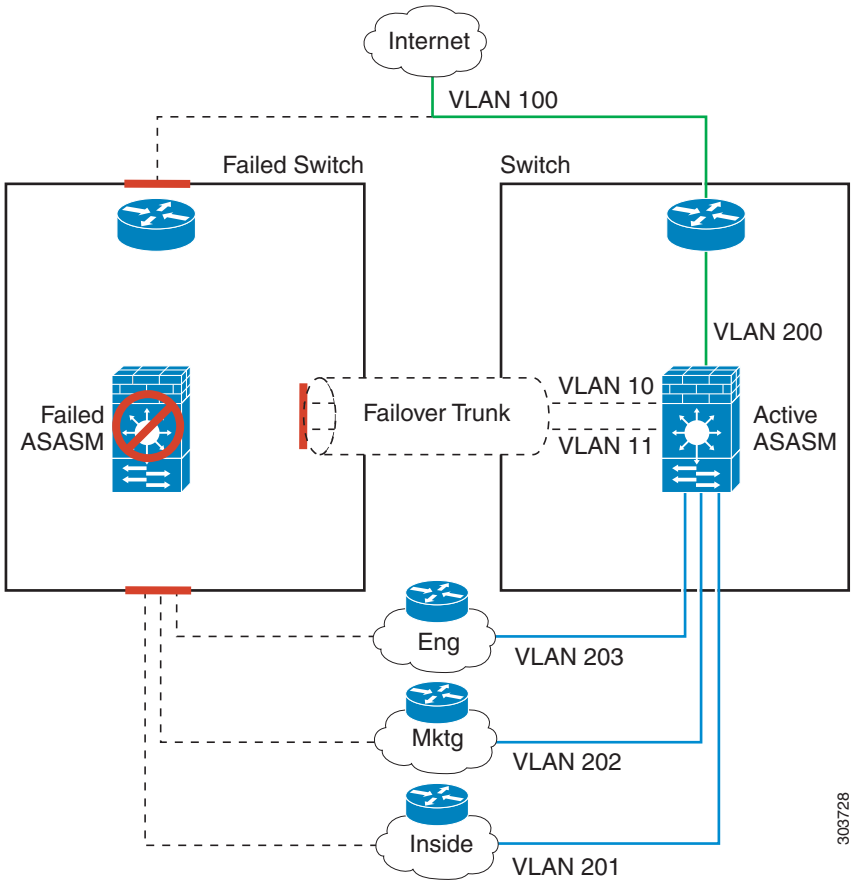
如果主 ASASM 发生故障，则辅助 ASASM 会成为主用设备，并成功传送防火墙 VLAN（图 8-10）。

图 8-10　ASASM 故障



如果整个交换机发生故障，并且 ASASM 也发生故障 （如电源故障），则交换机和 ASASM 均会故障转移到其辅助设备 （图 8-11）。

图 8-11　　交换机故障



无状态和有状态故障转移

ASA 支持主用 / 备用和主用 / 主用模式中的两种类型的故障转移，即无状态和有状态故障转移。

- 第 8-12 页的无状态故障转移
- 第 8-12 页的有状态故障转移

注　无客户端 SSL VPN 的某些配置元素 （如书签和自定义）使用 VPN 故障转移子系统，该子系统是有状态故障转移的一部分。 您必须使用有状态故障转移，在同步故障转移对中的成员之间同步这些元素。不推荐将无状态故障转移用于无客户端 SSL VPN。

无状态故障转移

发生故障转移时，所有活动连接将会被丢弃。在新的主用设备接管时，客户端需要重新建立连接。

注　无客户端 SSL VPN 的某些配置元素 （如书签和自定义）使用 VPN 故障转移子系统，该子系统是有状态故障转移的一部分。 您必须使用有状态故障转移，在同步故障转移对中的成员之间同步这些元素。不推荐将无状态 （常规）故障转移用于无客户端 SSL VPN。

有状态故障转移

启用有状态故障转移时，主用设备会持续将每连接状态信息传送到备用设备，或者在主用 / 主用故障转移中，在主用和备用故障转移组之间传送此信息。发生故障转移之后，相同的连接信息在新主用设备上可用。受支持的最终用户应用不需要通过重新连接来保持同一通信会话。

- 第 8-12 页的受支持的功能
- 第 8-13 页的不受支持的功能

受支持的功能

启用有状态故障转移时，以下状态信息会传送到备用 ASA：

- NAT 转换表
- TCP 连接状态
- UDP 连接状态
- ARP 表
- 第 2 层网桥表 （在透明防火墙模式中运行时）
- HTTP 连接状态 （如果启用了 HTTP 复制） - 默认情况下，启用了有状态故障转移时， ASA 不会复制 HTTP 会话信息。HTTP 会话通常是短期的，因为 HTTP 客户端通常会重试失败的连接尝试，不复制 HTTP 会话可以提高系统性能，而不会产生严重的数据或连接丢失。
- ISAKMP 和 IPsec SA 表
- GTP PDP 连接数据库
- SIP 信令会话
- ICMP 连接状态 - 仅当相应的接口分配给非对称路由组时，才会启用 ICMP 连接复制。
- 动态路由协议 - 有状态故障转移会参与动态路由协议 （如 OSPF 和 EIGRP），因此通过主用设备上的动态路由协议获悉的路由，将会保留在备用设备的路由信息库 (RIB) 表中。发生故障转移事件时，数据包可以正常传输，并且只会对流量产生极小的影响，因为主用辅助 ASA 一开始就具有镜像自主 ASA 的规则。进行故障转移后，新的主用设备上的重新融合计时器会立即启动。随后 RIB 表中的代编号将会增加。在重新融合期间， OSPF 和 EIGRP 路由将使用新的代编号进行更新。一旦计时器到期，过时的路由条目 （由代编号确定）将从表中移除。于是 RIB 将包含新主用设备上的最新的路由协议转发信息。

注　路由仅会因为主用设备上的链路打开或关闭事件而同步。如果备用设备上的链路打开或关闭，从主用设备发出的动态路由可能会丢失。这是预期的正常行为。

- Cisco IP SoftPhone 会话 - 如果在活动 Cisco IP SoftPhone 会话期间发生故障转移，呼叫将保持活动，因为呼叫会话状态信息已复制到备用设备。呼叫被终止时，IP SoftPhone 客户端将丢失与 Cisco Call Manager 的连接。发生此连接丢失是因为，没有备用设备上的 CTIQBE 挂机消息的会话信息。如果 IP SoftPhone 客户端在特定时间内未从 Call Manager 收到响应，则会认为 Call Manager 不可访问，并会注销自身。
- VPN - 进行故障转移后， VPN 最终用户无需重新进行身份验证，或重新连接 VPN 会话。但是，在 VPN 连接上运行的应用程序，在故障转移过程中可能会丢失数据包，并且无法从数据包丢失中恢复。

不受支持的功能

启用有状态故障转移时，以下状态信息*不会*传送至备用 ASA：

- HTTP 连接表 （除非启用了 HTTP 复制）
- 用户身份验证 (uauth) 表
- 属于高级 TCP 状态跟踪的应用检查 - 这些连接的 TCP 状态不会被自动复制。这些连接被复制到备用设备时，将会进行尽力而为的尝试来重新建立 TCP 状态。
- DHCP 服务器地址租用
- 模块的状态信息，如 ASA IPS SSP 或 ASA CX SSP。
- 电话代理连接 - 主用设备发生故障时，呼叫会失败，媒体数据流会停止传输，并且电话会从故障设备注销，并注册到主用设备。呼叫必须重新建立。
- 选定的无客户端 SSL VPN 功能：
  - 智能隧道
  - 端口转发
  - 插件
  - Java Applets
  - IPv6 无客户端或 Anyconnect 会话
  - Citrix 身份验证 （Citrix 用户在故障转移后必须重新进行身份验证）

透明防火墙模式要求

- 第 8-13 页的设备的透明模式要求
- 第 8-14 页的模块的透明模式要求

设备的透明模式要求

当主用设备故障转移到备用设备时，所连接的运行生成树协议 (STP) 的交换机端口在感知到拓扑变化时，会进入阻塞状态 30 秒至 50 秒。当端口处于阻塞状态时，为避免流量丢失，您可以根据交换机端口模式，配置以下任一变通方案：

- 访问模式 - 启用交换机上的 STP PortFast 功能：

```
interface interface_id
  spanning-tree portfast
```

链路打开时，PortFast 功能会立即使端口转换至 STP 转发模式。该端口仍会参与 STP。因此，如果该端口是环路的一部分，则该端口最终会转换为 STP 阻塞模式。

- Trunk 模式 - 使用 EtherType 访问规则阻止 ASA 内部和外部接口上的 BPDU。

  阻止 BPDU 会在交换机上禁用 STP。在您的网络布局中，确保没有任何环路涉及 ASA。

如果以上选项均不可行，则您可以使用以下任一不太理想的变通方案，这些方案可能会影响故障转移功能或 STP 稳定性。

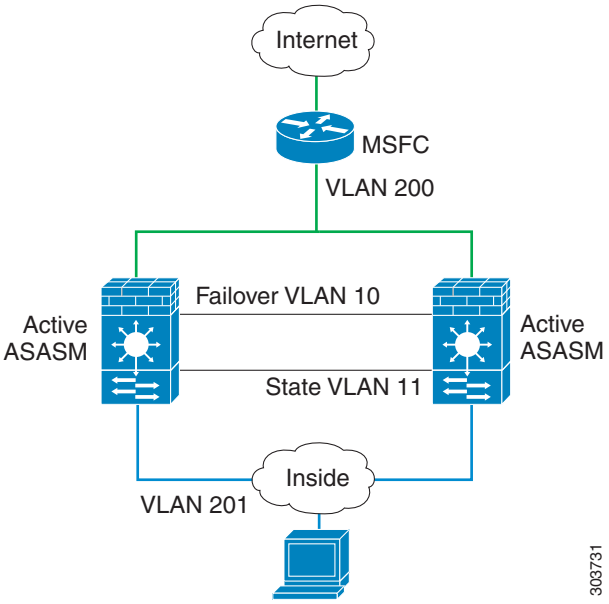
- 禁用接口监控。
- 将接口保持时间增大到一个高值，这将允许 STP 在 ASA 进行故障转移之前融合。
- 降低 STP 计时器的值，以便 STP 在接口保持时间之内融合。

模块的透明模式要求

当您在透明模式中使用故障转移时，为避免出现环路，应允许 BPDU 通过 （默认），并且，您必须使用支持 BPDU 转发的交换机软件。

如果两个模块同时处于活动状态，可能会出现环路，例如，当两个模块同时发现彼此的存在时，或者由于发生故障的故障转移链路。由于 ASASM 会在相同的两个 VLAN 之间桥接数据包，发往外部的内部数据包会被两台 ASASM 不断地复制，这时可能会出现环路 （请参阅图 8-12）。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，在 VLAN 200 和 VLAN 201 之间发送的 BPDU 需要桥接。

图 8-12　　透明模式环路



故障转移运行状况监控

ASA 会监控每台设备的整体运行状况和接口运行状况。本部分包括有关 ASA 如何执行测试以确定每台设备状态的信息。

设备运行状况监控

ASA 会通过监控故障转移链路来确定其他设备的运行状况。当设备在故障转移链路上没有收到三条连续的 Hello 消息时，设备将在每个数据接口 （包括故障转移链路）上发送接口 Hello 消息，以便验证对等设备是否响应。 ASA 采取的操作取决于来自其他设备的响应。请参阅以下的可能操作：

- 如果 ASA 在故障转移链路上收到响应，则不会进行故障转移。
- 如果 ASA 在故障转移链路上未收到响应，但在数据接口上收到响应，则设备不会进行故障转移。故障转移链路会标记为发生故障。您应该尽快还原故障转移链路，因为当故障转移链路发生故障时，设备无法故障转移到备用设备。
- 如果 ASA 未在任何接口上收到响应，则备用设备会切换至主用模式，并将另一个设备分类为故障设备。

接口监控

您可以监控最多 250 个接口 （在多模式中，会在所有情景之间进行分配）。您应该监控重要的接口。例如，在多模式中，您可以配置一个用于监控共享接口的情景。（由于此接口是共享的，因此所有情景都会受益于监控。）

配置的保持时间过半后，如果设备未在受监控的接口上收到 Hello 消息，将会运行以下测试：

1. 链路打开 / 关闭测试 - 接口状态测试。如果链路打开 / 关闭测试表明接口工作正常，ASA 会执行网络测试。这些测试旨在生成网络流量，以便确定发生故障的设备 （如有）。每项测试开始时，每台设备会清除其接口的收到的数据包计数。每项测试结束时，每台设备会检查是否收到了任何流量。如果收到了流量，接口会被视为正常工作。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备都没有收到流量，则会进行下一项测试。
2. 网络活动测试 - 收到的网络活动的测试。设备会对最多 5 秒内收到的所有数据包进行计数。如果在此时间间隔内的任意时刻收到任何数据包，接口会被认为正常工作，并且会停止测试。如果没有收到流量， ARP 测试将会开始。
3. ARP 测试 - 读取设备 ARP 缓存，以获取 2 个最近获得的条目。设备会逐一向这些设备发送 ARP 请求，从而尝试激发网络流量。在每次请求之后，设备会对最多 5 秒内收到的所有流量进行计数。如果收到流量，该接口会被视为正常工作。如果未收到任何流量，系统会将 ARP 请求发送到下一台设备。如果列表结束后，仍未收到任何流量，则会开始 Ping 测试。
4. 广播 Ping 测试 - 发送广播 Ping 请求的 Ping 测试。随后设备会对最多 5 秒内收到的所有数据包进行计数。如果在此时间间隔内的任意时刻收到任何数据包，接口会被认为正常工作，并且会停止测试。

受监控接口可以具有以下状态：

- Unknown - 初始状态。此状态还用于表示无法确定状态。
- Normal - 接口正在接收流量。
- Testing - 在该接口上，五次轮询时间内均未收到 Hello 消息。
- Link Down - 接口或 VLAN 通过管理方式关闭。
- No Link - 接口的物理链路关闭。
- Failed - 在接口上未接收到任何流量，但在对等接口上接收到流量。

如果接口上配置了 IPv4 和 IPv6 地址， ASA 会使用 IPv4 地址执行运行状况监控。

如果接口上仅配置了 IPv6 地址，ASA 会使用 IPv6 邻居发现，而不是 ARP 来执行运行状况监控测试。对于广播 Ping 测试， ASA 会使用所有的 IPv6 节点地址 (FE02::1)。

如果对于某个接口，所有网络测试均失败，但在另一设备上的此接口继续成功传送流量，则此接口会被视为发生故障。如果达到故障接口的阀值，则会进行故障转移。如果另一设备的接口在所有网络测试中也全部失败，则这两个接口会进入 “Unknown” 状态，并且不会计入故障转移限制。

如果接口收到任何流量，则该接口会再次变为正常工作状态。如果不再满足接口故障阈值，发生故障的 ASA 会回到备用模式。

注　如果故障设备未恢复，并且您认为其应该未发生故障，则可通过输入 **failover reset** 命令重置状态。然而，如果故障转移条件仍然存在，设备将再次失败。

故障转移时间

表 8-1 显示了最小、默认和最大故障转移时间。

表 8-1　　ASA 故障转移时间

故障转移条件	最小	默认	最大
主用设备断电或停止正常操作。	800 毫秒	15 秒	45 秒
主用设备主板接口链路发生故障。	500 毫秒	5 秒	15 秒
主用设备 4GE 模块接口链路发生故障。	2 秒	5 秒	15 秒
主用设备 IPS 或 CSC 模块发生故障。	2 秒	2 秒	2 秒
主用设备接口正常运行，但是连接问题导致接口测试。	5 秒	25 秒	75 秒

配置同步

故障转移包含两种类型的配置同步：

- 第 8-16 页的运行配置复制
- 第 8-17 页的命令复制

运行配置复制

当故障转移对中的一台或两台设备启动时，会进行运行配置复制。配置始终会从主用设备同步到备用设备。备用设备完成其初始启动后，会清除其运行配置 （需要与主用设备通信的故障转移命令除外），而主用设备则会向备用设备发送其完整配置。

复制开始时，主用设备上的 ASA 控制台会显示消息 “Beginning configuration replication: Sending to mate”，复制完成时，ASA 会显示消息 “End Configuration Replication to mate”。取决于配置的大小，复制过程可能需要几秒到几分钟时间。

在备用设备上，配置仅存在于运行内存中。您应该将配置保存到闪存。

注　在复制期间，在主用设备上输入的命令可能无法正确复制到备用设备，在备用设备上输入的命令可能会被从主用设备复制的配置覆盖。在配置复制过程中，应避免在任一设备上输入命令。

注　**crypto ca server** 命令和相关子命令不会同步到故障转移对等设备。

注　配置同步不复制以下文件和配置组件，因此，您必须手动复制这些文件，以便它们匹配：

- AnyConnect 映像
- CSD 映像
- AnyConnect 配置文件
- 本地证书颁发机构 (CA)
- ASA 映像
- ASDM 映像

命令复制

启动后，您在主用设备上输入的命令会被立即复制到备用设备。您不需要将主用配置保存到闪存以复制命令。

在主用 / 主用故障转移中，在系统执行空间中输入的更改会从其上的故障转移组 1 处于主用状态的设备复制。

未在要进行命令复制的相应设备上输入更改会导致配置失去同步。在进行下一次初始配置同步时，这些更改可能会丢失。

以下命令会复制到备用 ASA：

- 除 **mode**、 **firewall** 和 **failover lan unit** 外的所有配置命令。
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

以下命令*不会*复制至备用 ASA：

- 所有形式的 **copy** 命令 （**copy running-config startup-config** 除外）
- 所有形式的 **write** 命令 （**write memory** 除外）
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** 和 **pager**

关于主用 / 备用故障转移

主用 / 备用故障转移允许您使用备用 ASA 来接管故障设备的功能。主用设备发生故障时，会变为备用状态，同时备用设备会变为主用状态。

注　对于多情景模式， ASA 可以故障转移整个设备 （包括所有情景），但不能对各个情景单独进行故障转移。

主 / 辅助角色和主用 / 备用状态

故障转移对中两台设备之间的主要差别与哪一设备为主用设备，哪一设备为备用设备，换句话说，使用哪一个 IP 地址以及哪一台设备会主动传送流量有关。

然而，设备之间还存在一些取决于哪一设备为主设备 （在配置中指定），哪一设备为辅助设备的一些差别：

- 如果两台设备同一时间启动 （并且运行状况相同），主设备总是会成为主用设备。
- 主设备的 MAC 地址总是与主用 IP 地址耦合。此规则的例外情况是，辅助设备处于活动状态，而且无法通过故障转移链路获取主设备的 MAC 地址。在这种情况下，会使用辅助设备的 MAC 地址。

启动时的主用设备确定

主用设备会如下确定：

- 如果某台设备启动，并检测到对等体已作为主用设备运行，则该设备会成为备用设备。
- 如果某台设备启动，并且未检测到对等体，则该设备会成为主用设备。
- 如果两台设备同时启动，则主设备成为主用设备，辅助设备成为备用设备。

故障转移事件

在主用 / 备用故障转移中，故障转移会在设备级别进行。即使在多情景模式中运行的系统上，您也无法对个别情景或一组情景进行故障转移。

表 8-2 显示每种故障事件的故障转移操作。对于每种故障事件，该表显示了故障转移策略 （故障转移或不进行故障转移）、主用设备执行的操作、备用设备执行的操作，以及有关故障转移条件和操作的所有特别说明。

表 8-2　　故障转移行为

故障事件	策略	主用设备操作	备用设备操作	备注
主用设备发生故障 （电源或硬件）	故障转移	不适用	变为主用 将主用设备标记为发生故障	在任何受监控接口或故障转移链路上，均未收到 Hello 消息。
以前的主用设备恢复	不进行故障转移	成为备用设备	不进行操作	无。
备用设备发生故障 （电源或硬件）	不进行故障转移	将备用设备标记为发生故障	不适用	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。
故障转移链路在运行期间发生故障	不进行故障转移	将故障转移链路标记为发生故障	将故障转移链路标记为发生故障	您应该尽快还原故障转移链路，因为当故障转移链路发生故障时，设备无法故障转移到备用设备。
故障转移链路在启动时发生故障	不进行故障转移	将故障转移链路标记为发生故障	变为主用	如果故障转移链路在启动时发生故障，则两台设备都会成为主用设备。
有状态链路发生故障	不进行故障转移	不进行操作	不进行操作	如果发生故障转移，状态信息会过时，而且会话会被终止。
主用设备上的接口故障超过阈值	故障转移	将主用设备标记为发生故障	变为主用	无。
备用设备上的接口故障超过阈值	不进行故障转移	不进行操作	将备用设备标记为发生故障	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。

关于主用 / 主用故障转移

本部分介绍主用 / 主用故障转移。

- 第 8-20 页的主用 / 主用故障转移概述
- 第 8-20 页的故障转移组的主 / 辅助角色和主用 / 备用状态
- 第 8-21 页的故障转移事件

主用 / 主用故障转移概述

在主用 / 主用故障转移配置下，两台 ASA 都可以传送网络流量。主用 / 主用故障转移仅适用于多情景模式中的 ASA。在主用 / 主用故障转移中，您可将 ASA 上的安全情景划分为最多 2 个故障转移组。

故障转移组就是一个或多个安全情景的逻辑组。您可以将故障转移组指定为在主 ASA 上处于主用状态，并将故障转移组 2 指定为在辅助 ASA 上处于主用状态。发生故障转移时，会在故障转移组级别进行。例如，根据接口故障模式，故障转移组 1 可能会故障转移到辅助 ASA，相应地，故障转移组 2 可能故障转移到主 ASA。在以下情况下可能发生此事件：故障转移组 1 中的接口在主 ASA 上发生故障，但在辅助 ASA 上正常工作，而故障转移组 2 中的接口在辅助 ASA 上发生故障，但在主 ASA 上正常工作。

管理情景始终是故障转移组 1 的成员。默认情况下，所有未分配的安全情景也是故障转移组 1 的成员。如果希望使用主用 / 主用故障转移，但对多情景不感兴趣，最简单的配置是添加一个额外的情景并将其分配给故障转移组 2。

注　配置主用 / 主用故障转移时，请确保两台设备的整合流量在每台设备的处理能力之内。

注　需要时，可将两个故障转移组分配到一台 ASA，但您将无法利用具有两台主用 ASA 的优势。

故障转移组的主 / 辅助角色和主用 / 备用状态

就像在主用 / 备用故障转移中一样，主用 / 主用故障转移对中的一台设备会被指定为主设备，另一设备会被指定为辅助设备。不同于主用 / 备用故障转移的是，当两台设备同时启动时，该指定不指示哪一台设备会成为主用设备。相反，主 / 辅助指定会做两件事：

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

启动时的故障转移组主用设备确定

故障转移组在其上变为主用状态的设备如下确定：

- 一台设备启动时，如果对等设备不可用，两个故障转移组都会在该设备上变为主用状态。
- 一台设备启动时，如果对等设备处于主用状态 （而且两个故障转移组都处于主用状态），故障转移组将在主用设备上保持主用状态，而无论故障转移组的主设备或辅助设备首选项如何，直到出现以下情形之一：
  - 发生故障转移。
  - 您手动强制执行故障转移。
  - 您为故障转移组配置了抢占，这导致故障转移组在设备变得可用时，自动在首选设备上变为主用状态。
- 两台设备同时启动时，在同步配置后，每个故障转移组都会在其首选设备上变为主用状态。

故障转移事件

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

由于故障转移组可以包含多个情景，并且每个情景可以包含多个接口，因此单个情景中的所有接口都发生故障而不导致相关故障转移组发生故障是有可能的。

表 8-3 显示每种故障事件的故障转移操作。对于每种故障事件，给出了策略 （是否发生故障转移）、主用故障转移组的操作和备用故障转移组的操作。

表 8-3　　主用 / 主用故障转移的故障转移行为

故障事件	策略	主用组操作	备用组操作	备注
设备发生电源或软件故障	故障转移	变为备用，并标记为发生故障	变为主用 将主用设备标记为发生故障	故障转移对中的一台设备发生故障时，该设备上的所有主用故障转移组都会被标记为发生故障，并在对等设备上变为主用。
主用故障转移组上的接口故障超过阈值	故障转移	将主用组标记为发生故障	变为主用	无。
备用故障转移组上的接口故障超过阈值	不进行故障转移	不进行操作	将备用组标记为发生故障	备用故障转移组被标记为发生故障后，主用故障转移组不会尝试进行故障转移，即使超过接口故障阈值也是如此。
以前的主用故障转移组恢复	不进行故障转移	不进行操作	不进行操作	除非配置了故障转移组抢占，否则故障转移组会在其当前设备上保持主用状态。
故障转移链路在启动时发生故障	不进行故障转移	变为主用	变为主用	如果故障转移链路在启动时发生故障，则两台设备上的故障转移组都会变为主用。
有状态链路发生故障	不进行故障转移	不进行操作	不进行操作	如果发生故障转移，状态信息会过时，而且会话会被终止。
故障转移链路在运行期间发生故障	不进行故障转移	不适用	不适用	每台设备都会将故障转移链路标记为发生故障。您应该尽快还原故障转移链路，因为当故障转移链路发生故障时，设备无法故障转移到备用设备。

故障转移许可

主用 / 备用故障转移

型号	许可证要求
ASA 5512-X	增强型安全许可证。
ASAv	标准许可证和高级许可证。
所有其他型号	基础许可证。

故障转移设备不要求每台设备上具有相同的许可证。如果您在两台设备上都有许可证，它们将组合成一个运行的故障转移集群许可证。此规则的例外情况包括：

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

主用 / 主用故障转移

型号	许可证要求
ASA 5512-X	增强型安全许可证。
ASAv	不支持。
所有其他型号	基础许可证。

故障转移设备不要求每台设备上具有相同的许可证。如果您在两台设备上都有许可证，它们将组合成一个运行的故障转移集群许可证。此规则的例外情况包括：

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

故障转移的先决条件

请参阅第 8-2 页的故障转移系统要求。

故障转移准则

情景模式准则

- 主用 / 备用模式在单情景和多情景模式中受支持。
- 主用 / 主用模式仅在多情景模式中受支持。
- 对于多情景模式，除非另外说明，请在系统执行空间中执行所有操作步骤。
- 如果您尝试同时在两个或更多情景中进行配置更改， ASA 故障转移复制将会失败。变通方案是在每个情景中连续进行配置更改。

附加准则和限制

- 发生故障转移事件时，在连接到 ASA 故障转移对的交换机上配置端口安全性，可能会导致通信问题。一个安全端口上配置或获悉的安全 MAC 地址移至另一安全端口，交换机端口安全功能标记违例时，会发生此问题。
- 您可以在一台设备上监控跨所有情景的最多 250 个接口。
- 对于主用 / 主用故障转移，不应在相同 ASR 组中配置相同情景中的两个接口。
- 对于主用 / 主用故障转移，您可以定义最多两个故障转移组。
- 对于主用 / 主用故障转移，移除故障转移组时，您必须最后移除故障转移组 1。故障转移组 1 始终包含管理情景。未分配到故障转移组的所有情景将默认分配到故障转移组 1。您不能移除已显式为其分配情景的故障转移组。

相关主题

- 第 37-27 页的故障转移配置中的自动更新服务器支持

故障转移策略的默认内容

默认情况下，故障转移策略包含以下内容：

- 在有状态故障转移中不进行 HTTP 复制。
- 单个接口故障导致故障转移。
- 接口轮询时间为 5 秒。
- 接口保持时间为 25 秒。
- 设备轮询时间为 1 秒。
- 设备保持时间为 15 秒。
- 虚拟 MAC 地址在多情景模式中启用；在单情景模式中禁用。
- 监控所有物理接口，或者对于 ASASM，所有 VLAN 接口。

配置主用 / 备用故障转移

High Availability and Scalability Wizard 可以分步骤指导您创建主用 / 备用故障转移配置。

操作步骤

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

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，对等地址将被指定为 ASDM 管理接口的备用地址。

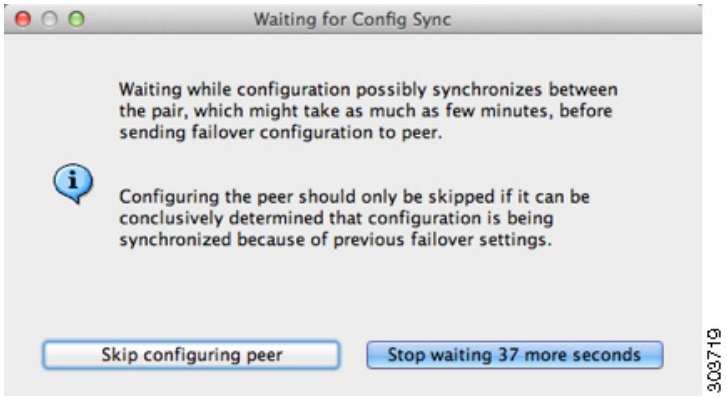
步骤 3　在 **LAN Link Configuration** 屏幕上：

- **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** - 加密故障转移链路上的通信。**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（请参阅第 8-31 页的修改故障转移设置）。

步骤 4　在 **State Link Configuration** 屏幕上，如果您选择将另一个接口用于有状态故障转移：

- **Active IP Address** - 此 IP 地址应处于不同于故障转移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　在您点击 **Finish** 后，向导会显示 **Waiting for Config Sync** 屏幕。



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

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

配置主用 / 主用故障转移

High Availability and Scalability Wizard 可以分步骤指导您创建主用 / 主用故障转移配置。

操作步骤

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

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

默认情况下，对等地址将被指定为 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，您可以添加其他情景。

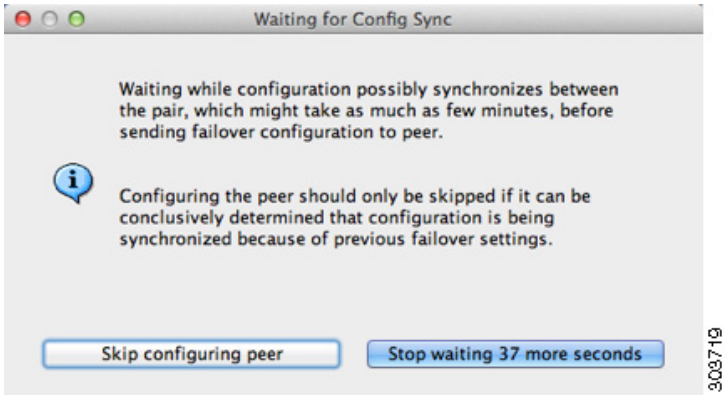
步骤 4　在 **LAN Link Configuration** 屏幕上：

- **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** - 加密故障转移链路上的通信。**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 （请参阅第 8-31 页的修改故障转移设置）。

步骤 5　在 **State Link Configuration** 屏幕上，如果您选择将另一个接口用于有状态故障转移：

- **Active IP Address** - 此 IP 地址应处于不同于故障转移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　在您点击 **Finish** 后，向导会显示 **Waiting for Config Sync** 屏幕。



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

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

配置可选故障转移参数

您可以视需要自定义故障转移设置。

- 第 8-26 页的配置故障转移条件、 HTTP 复制、组抢占、和 MAC 地址
- 第 8-28 页的配置接口监控和备用地址
- 第 8-29 页的配置非对称路由数据包支持 （主用 / 主用模式）

配置故障转移条件、 HTTP 复制、组抢占、和 MAC 地址

有关您可在此部分中更改的许多参数的默认设置，请参阅第 8-23 页的故障转移策略的默认内容。对于主用 / 主用模式，您可以设置每个故障转移组的大多数条件。此部分包括为主用 / 主用模式中的每个故障转移组启用 HTTP 复制；要为主用 / 备用模式配置 HTTP 复制，请参阅第 8-31 页的修改故障转移设置。

准备工作

在多情景模式中，可在系统执行空间中配置这些设置。

操作步骤

步骤 7　选择 **Configuration > Device Management > High Availability and Scalability > Failover > Criteria** 选项卡。

步骤 8　在 **Failover Poll Times** 区域中，配置设备轮询时间：

- **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，必须在故障转移链路上收到 Hello 消息，否则设备会开始对等设备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。您输入的值不得短于轮询时间的 3 倍。

注　此窗格中的其他设置仅适用于主用 / 备用模式。在主用 / 主用模式中，您必须为每个故障转移组配置其余参数。

步骤 9　（仅主用 / 主用模式）点击 **Active/Active** 选项卡，然后选择故障转移组，并点击 **Edit**。

步骤 10　（仅主用 / 主用模式）要更改故障转移组的首选角色，请点击 **Primary** 或 **Secondary**。如果您使用了向导，故障转移组 1 会分配到主设备，故障转移组 2 会分配到辅助设备。如果您需要非标准配置，可以根据需要指定不同的设备首选项。

步骤 11　（仅主用 / 主用模式）要配置故障转移组抢占，请选中 **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，则两个故障转移组都会在该设备上变为主用状态，而无论主设备或辅助设置如何。当指定设备变得可用时，此选项会使故障转移组自动在该设备上变为主用状态。

您可以输入可选的 delay 值，该值指定故障转移组在指定设备上自动变为主用状态之前，在当前设备上保持主用状态的秒数。有效值范围为 1 至 1200。

注　如果启用有状态故障转移，抢占将延迟，直到从故障转移组当前处于主用状态的设备复制连接。

步骤 12　要配置 **Interface Policy**，请选择以下任一选项：

- **Number of failed interfaces that triggers failover** - 定义要触发故障转移，必须达到的特定故障接口数，从 1 到 250。发生故障的受监控接口数超过您指定的值时， ASA 将会进行故障转移。
- **Percentage of failed interfaces that triggers failover** - 定义要触发故障转移，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 将会进行故障转移。

注　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 13　对于主用 / 备用模式，请在 **Failover Poll Time** 区域中配置接口轮询时间。

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。

- **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。

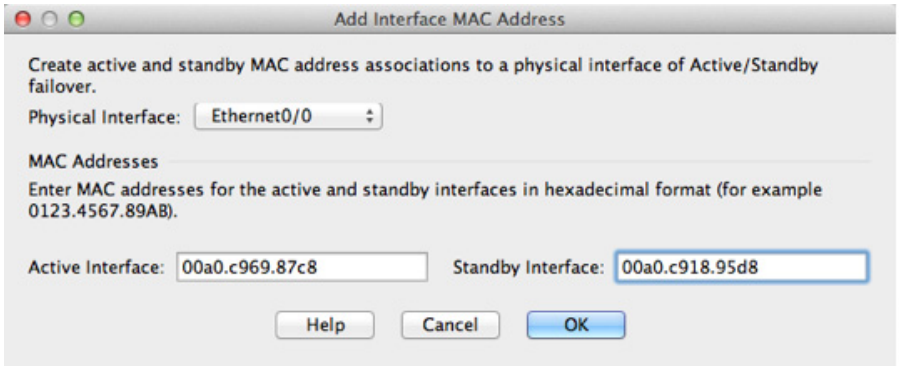
步骤 14　（仅主用 / 主用模式）要启用 HTTP 复制，请选中 **Enable HTTP replication** 复选框。有关主用 / 备用模式，请参阅第 8-31 页的修改故障转移设置。有关这两种模式的 HTTP 复制速率，请参阅第 8-31 页的修改故障转移设置部分。

步骤 15　对于主用 / 备用模式，要配置虚拟 MAC 地址，请点击 **MAC Addresses** 选项卡。

对于主用 / 主用模式，请转至 **Active/Active** 选项卡的底部。

您还可以使用其他方法设置 MAC 地址，但是，我们建议仅使用一种方法。如果您使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。

步骤 16　要添加新的虚拟 MAC 地址条目，请点击 **Add**。



系统将显示 **Add/Edit Interface MAC Address** 对话框。

步骤 17　从 **Physical Interface** 下拉列表中选择接口。

步骤 18　在 **Active MAC Address** 字段中，键入主用接口的新 MAC 地址。

步骤 19　在 **Standby MAC Address** 字段中，键入备用接口的新 MAC 地址。

步骤 20　点击 **OK**。

接口会被添加至该表。

步骤 21　（仅主用 / 主用模式）点击 **OK**。

步骤 22　点击 **Apply**。

步骤 23　（仅主用 / 主用模式）视需要为其他故障转移组，重复此操作步骤。

配置接口监控和备用地址

默认情况下，会在所有物理接口或 （对于 ASASM）所有 VLAN 接口以及在 ASA 上安装的所有硬件模块上启用监控。您可能希望排除连接到非关键网络的接口，以免影响故障转移策略。

如果未在向导中配置备用 IP 地址，您可以手动配置这些 IP 地址。

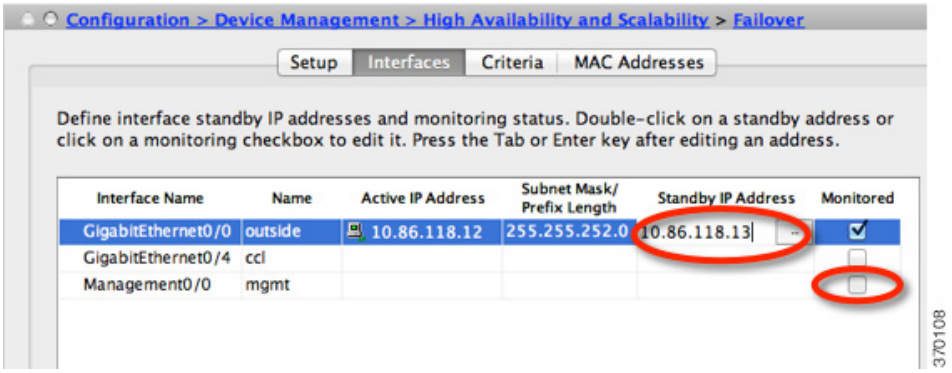
准备工作

- 您可以监控一台设备上的最多 250 个接口 （跨多情景模式中的所有情景）。
- 在多情景模式中，请在每个情景中配置接口。

操作步骤

步骤 1　在单模式中，请选择 **Configuration > Device Management > High Availability > Failover > Interfaces**。

在多情景模式中，在一个情景中选择 **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转移条件的一部分。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转移，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。如果已进行配置，则接口的备用 IP 地址会显示在 Standby IP address 列中。故障转移链路和有状态链路不会显示 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，请选中相应接口的 **Monitored** 复选框。

步骤 4　对于没有备用 IP 地址的每个接口，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 / 主用故障转移下运行时，设备可能会收到其对等设备发起的连接的一个返回数据包。由于收到该数据包的 ASA 没有该数据包的任何连接信息，该数据包会被丢弃。主用 / 主用故障转移对中的两台 ASA 连接到不同的服务提供商，并且出站连接不使用 NAT 地址时，最常发生此丢弃。

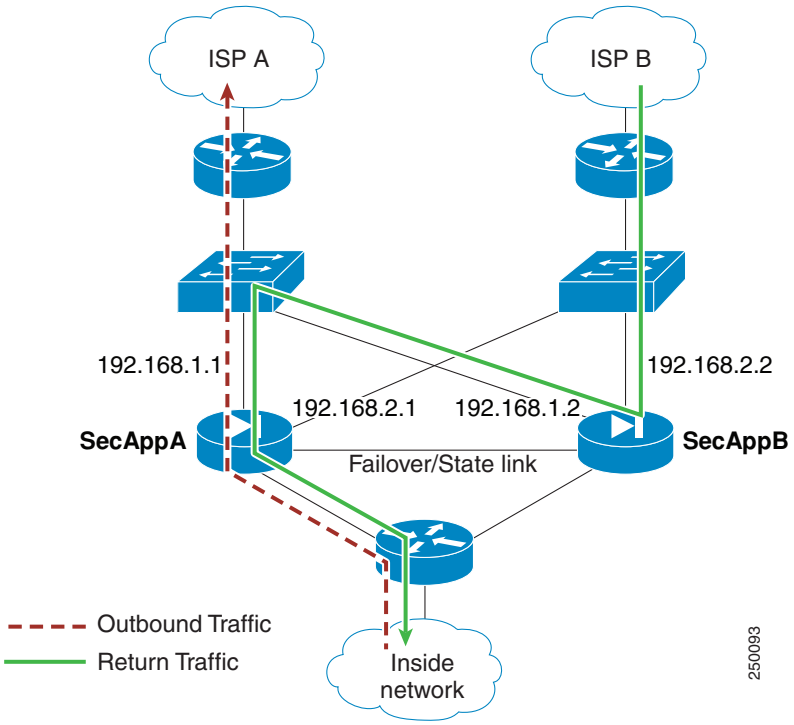
您可以通过允许非对称路由数据包来防止返回数据包。为此，您需要将每台 ASA 上的相似接口分配到同一个 ASR 组。例如，两台 ASA 的内部接口连接到内部网络，但外部接口连接到不同的 ISP。在主设备上，将主用情景外部接口分配给 ASR 组 1；在辅助设备上，将主用情景外部接口分配给相同 ASR 组 1。当主设备外部接口收到到没有其会话信息的数据包时，它会检查相同组中处于备用情景中的另一接口的会话信息；在此示例中，即 ASR 组 1。如果它没有找到匹配项，数据包将会被丢弃。如果它找到匹配项，则会进行以下的操作：

- 如果传入流量来自对等设备，第 2 层标头的部分或全部内容将会被重写，数据包将会被重定向到另一设备。一旦会话处于活动状态，此重定向将会继续。
- 如果传入流量来自相同设备上的不同接口，第 2 层标头的部分或全部内容将会被重写，数据包将会被重新注入数据流。

注　此功能不提供非对称路由；它会将非对称路由数据包还原至正确接口。

图 8-13 展示了一个非对称路由数据包的示例。

图 8-13　　ASR 示例



1. 出站会话使用主用 SecAppA 情景通过 ASA。该会话退出接口 outsideISP-A (192.168.1.1)。
2. 由于上游某处配置了非对称路由，返回流量使用主用 SecAppA 情景通过 ASA 上的接口 outsideISP-B (192.168.2.2) 传回。
3. 由于没有接口 192.168.2.2 上的流量的会话信息，返回流量通常会被丢弃。但是，此接口被配置为 ASR 组 1 的一部分。设备会在配置为相同的 ASR 组 ID 的所有其他接口上查找该会话。

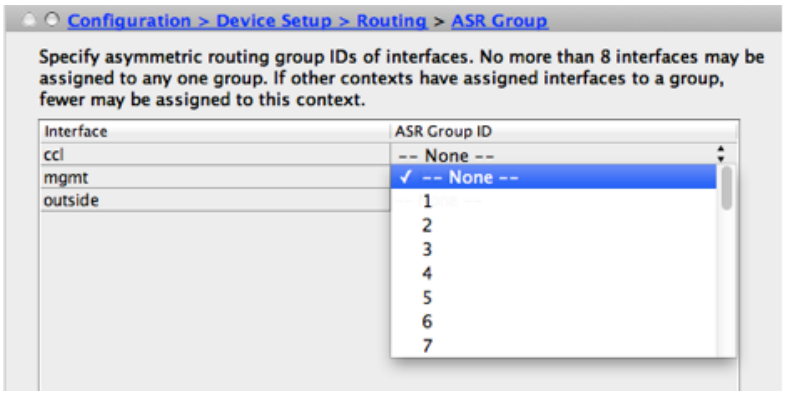
4. 会话信息会在接口 outsideISP-A (192.168.1.2) 上找到，该接口在使用 SecAppB 情景的设备上处于备用状态。有状态故障转移会将会话信息从 SecAppA 复制到 SecAppB。
5. 第 2 层标头会使用接口 192.168.1.1 的信息重写，流量会被重定向，通过接口 192.168.1.2，在该接口上，流量随后会通过设备上的来源接口 （SecAppA 上的 192.168.1.1）返回，而不是将流量丢弃。此转发会视需要继续，直到会话结束。

先决条件

- 有状态故障转移 - 将主用故障转移组中的接口上的会话的状态信息，传送给备用故障转移组。
- 复制 HTTP - HTTP 会话状态信息不会传送给备用故障转移组，因此不存在于备用接口上。为了使 ASA 能够重新路由非对称路由的 HTTP 数据包，您需要复制 HTTP 状态信息。
- 请在主设备和辅助设备上的每个主用情景中，执行此操作步骤。

详细步骤

步骤 1　在主设备主用情景上，请选择 **Configuration > Device Setup > Routing > ASR Groups**。



步骤 2　对于收到非对称路由数据包的接口，请从下拉列表中选择 ASR 组号码。

步骤 3　点击 **Apply** 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　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 组编号。

步骤 7　点击 **Apply** 保存对运行配置所做的更改。

管理故障转移

修改故障转移设置

如果不使用向导，或者要更改设置，您可以手动配置故障转移设置。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：

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

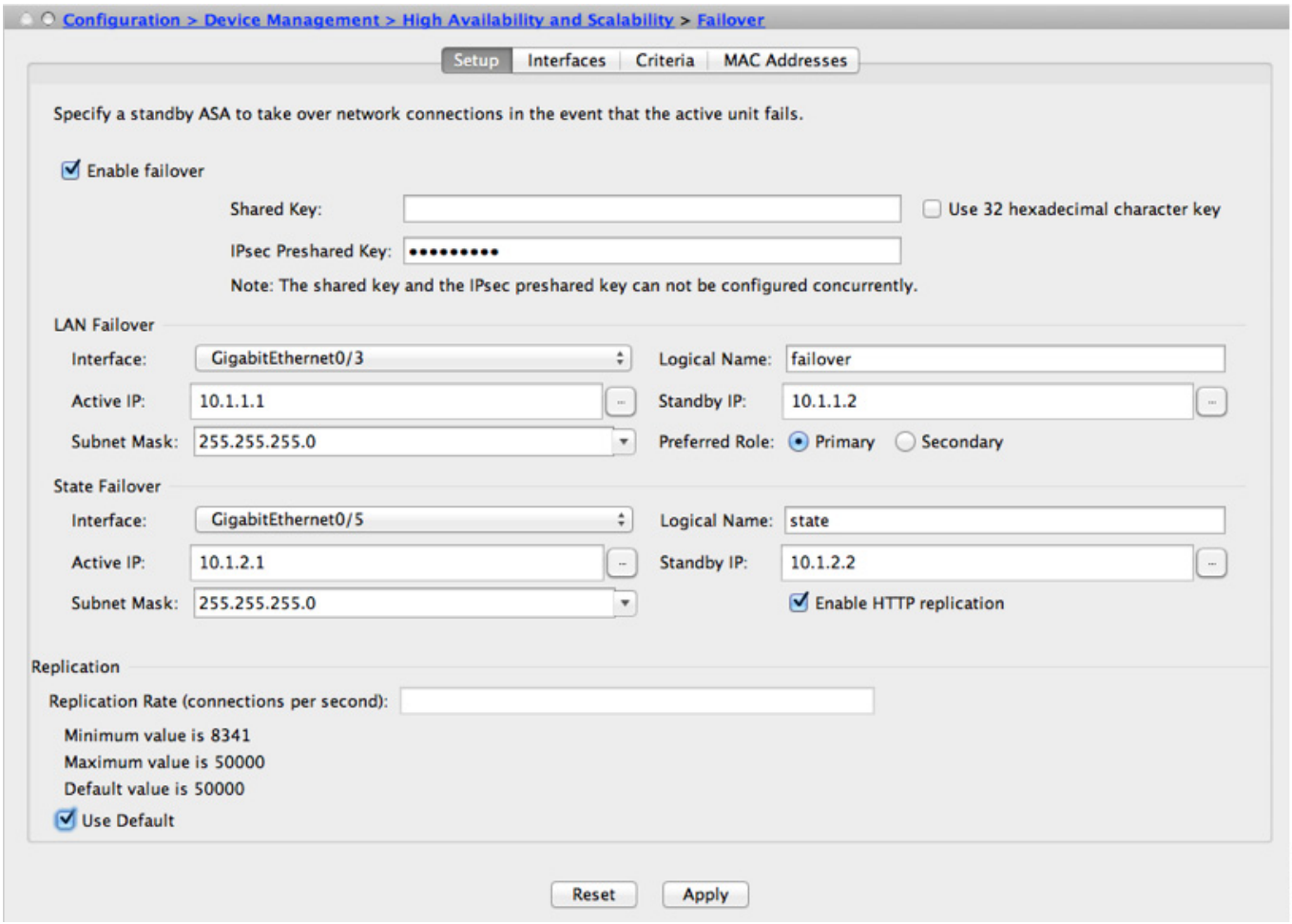
先决条件

在多情景模式中，请在系统执行空间中执行此操作步骤。

详细步骤

步骤 1　在单模式中，请选择 **Configuration > Device Management > High Availability and Scalability > Failover > Setup**。

在多情景模式中，请在系统执行空间中选择 **Configuration > Device Management > Failover > Setup**。



步骤 2　选中 **Enable Failover** 复选框。

注　故障转移实际上并未启用，直到您将更改应用到设备。

步骤 3　要加密故障转移和有状态链路上的通信，请使用以下任一选项：

- IPsec Preshared Key（首选）- 此预共享密钥由 IKEv2 用于在故障转移设备之间的故障转移链路上，建立 IPsec LAN 对 LAN 隧道。注意：故障转移 LAN 对 LAN 隧道不计入 IPsec（其他 VPN）许可证。
- Secret Key - 输入用于加密故障转移通信的密钥。如果将此字段留空，故障转移通信 （包括在命令复制期间发送的配置中的所有密码和密钥）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，设置故障转移链路的以下参数：

- Interface - 选择用于故障转移链路的接口。故障转移需要专用接口，但是，您可以与有状态故障转移共享接口。

  仅未配置的接口或子接口会显示在该列表中，并且可以被选择用作故障转移链路。一旦将接口指定为故障转移链路，您将无法在 Configuration > Interfaces 窗格中编辑该接口。
- Logical Name - 指定用于故障转移通信的接口逻辑名称，如 “failover”。此名称仅提供信息。
- 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**，以便指定此 ASA 的首选角色是主设备还是辅助设备。

步骤 5　（可选）通过执行以下操作步骤配置状态链路：

- Interface - 选择用于有状态链路的接口。您可以选择一个未配置的接口或子接口、故障转移链路或 **--Use Named--** 选项。

  注　我们建议您，将两个独立的专用接口用于故障转移链路和有状态链路。

  如果您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、Standby IP 和 Logical Name。

  如果您选择故障转移链路，则不需要指定 Active IP、Subnet Mask、Logical Name 和 Standby IP 值；系统将使用为故障转移链路指定的值。

  如果您选择 --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逻辑名称，如 “state”。此名称仅提供信息。
- 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，不同于故障转移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。

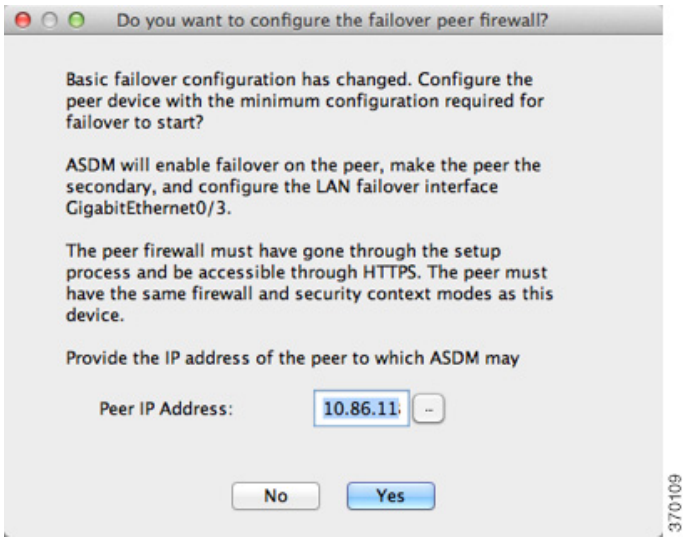
- （可选，仅主用 / 备用） Enable HTTP Replication - 通过选中 **Enable HTTP Replication** 复选框，启用 HTTP 复制。此选项允许有状态故障转移将主用 HTTP 会话复制到备用防火墙。如果您不允许 HTTP 复制，则在发生故障转移时， HTTP 连接将会断开。在主用 / 主用模式中，为每个故障转移组设置 HTTP 复制。请参阅第 8-26 页的配置故障转移条件、 HTTP 复制、组抢占、和 MAC 地址。

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　如果您启用故障转移，您将会看到用于配置故障转移对等设备的对话框。



- 如果您想要以后连接到故障转移对等设备，并手动配置匹配的设置，请点击 **No**。
- 要让 ASDM 自动配置故障转移对等设备上的相关故障转移设置，请点击 **Yes**。在 Peer IP Address 字段中提供对等设备 IP 地址。

强制故障转移

要强制要求备用设备成为主用设备，请执行以下操作步骤。

先决条件

在多情景模式中，请在系统执行空间中执行此操作步骤。

详细步骤

步骤 1　要在设备级别强制进行故障转移：

a.　根据您的情景模式选择屏幕：

- 在单情景模式中，请选择 **Monitoring > Properties > Failover > Status**。
- 在多情景模式中，在 System 中选择 **Monitoring > Failover > System**。

b. 点击以下任一按钮：

- 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）要强制在故障转移组级别进行故障转移：

a. 在 System 中，选择 **Monitoring > Failover > Failover Group #**，其中 # 是您要控制的故障转移组的编号。

b. 点击以下任一按钮：

- 点击 **Make Active**，以便使故障转移组成为此设备上的主用故障转移组。
- 点击 **Make Standby**，以便使故障转移组成为另一设备上的主用故障转移组。

禁用故障转移

要禁用故障转移，请执行以下操作步骤。

先决条件

在多情景模式中，请在系统执行空间中执行此操作步骤。

详细步骤

步骤 1　在单模式中，请选择 **Configuration > Device Management > High Availability and Scalability > Failover > Setup**。

在多情景模式中，请在系统执行空间中选择 **Configuration > Device Management > Failover > Setup**。

步骤 2　取消选中 **Enable Failover** 复选框。

步骤 3　点击 **Apply**。

还原故障设备

要将故障设备还原到无故障状态，请执行以下操作步骤。

先决条件

在多情景模式中，请在系统执行空间中执行此操作步骤。

详细步骤

步骤 1　要在设备级别还原故障转移：

a. 根据您的情景模式选择屏幕：

- 在单情景模式中，请选择 **Monitoring > Properties > Failover > Status**。
- 在多情景模式中，在 System 中选择 **Monitoring > Failover > System**。

b. 点击 **Reset Failover**。

步骤 2　（仅主用 / 主用模式）要在故障转移组级别重置故障转移：

a. 在 System 中，选择 **Monitoring > Failover > Failover Group #**，其中 # 是您要控制的故障转移组的编号。

b. 点击 **Reset Failover**。

重新同步配置

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

监控故障转移

故障转移消息

发生故障转移时，两台 ASA 都会发送系统消息。

故障转移系统日志消息

ASA 发出一系列与优先级为 2 的故障转移有关的系统日志消息，指示一个严重情况。要查看这些信息，请参阅 《系统日志消息指南》。要启用记录，请参阅第 40 章，“日志记录”

注　在故障转移期间，故障转移会在逻辑上关闭然后打开接口，生成系统日志消息 411001 和 411002。这是正常活动。

故障转移调试消息

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

注　由于调试输出在 CPU 进程中分配的高优先级，它可能极大地影响系统性能。为此，请仅使用 **debug fover** 命令来针对特定问题进行故障排除，或在与思科 TAC 的故障排除会话中使用该命令。

SNMP 故障转移陷阱

要接收故障转移的 SNMP 系统日志陷阱，请配置 SNMP 代理发送 SNMP 陷阱到 SNMP 管理站、定义系统日志主机，并将思科系统日志 MIB 汇集到 SNMP 管理站中。有关详细信息，请参阅第 41 章，“SNMP”。

监控故障转移

注 在故障转移事件后，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。

选择 **Monitoring > Properties > Failover** 以监控主用 / 备用故障转移。

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

- 第 8-36 页的系统
- 第 8-37 页的 Failover Group 1 和 Failover Group 2

系统

System 窗格显示系统的故障转移状态。您还可以通过执行以下操作步骤，控制系统的故障转移状态：

- 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 的故障转移状态。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转移组在 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转移组在 ASA 上都进入备用状态。
- 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会重置备用设备。
- Reload Standby - 点击此按钮强制重新加载备用设备。
- Refresh - 点击此按钮以刷新 Failover state of the system 字段中的状态信息。

Failover Group 1 和 Failover Group 2

Failover Group 1 和 Failover Group 2 窗格显示选定组的故障转移状态。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转移状态。

字段

Failover state of Group[*x*] - *仅显示信息*。显示选定故障转移组的故障转移状态。显示的信息与从 **show failover group** 命令收到的输出相同。

可从此窗格执行以下操作：

- Make Active - 点击此按钮使故障转移组在 ASA 上进入主用状态。
- Make Standby - 点击此按钮使故障转移组在 ASA 上进入备用状态。
- 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会重置备用设备。
- Refresh - 点击此按钮以刷新 Failover state of the system 字段中的状态信息。

故障转移功能历史记录

表 8-4 列出了此功能的版本历史记录。

表 8-4　　可选主用 / 备用故障转移设置的功能历史记录

功能名称	版本	功能信息
主用 / 备用故障转移	7.0(1)	引入此功能。
主用 / 主用故障转移	7.0(1)	引入此功能。
故障转移密钥支持使用十六进制值	7.0(4)	现在您可以指定十六进制值用于故障转移链路加密。 我们修改了以下屏幕：Configuration > Device Management > High Availability > Failover > Setup。
支持故障转移密钥的主密码	8.3(1)	故障转移密钥现在支持主密码，该密码用于加密运行配置和启动配置中的共享密钥。如果您要将共享密钥从一台 ASA 复制到另一台（例如，通过 **more system:running-config** 命令），您可以成功复制并粘贴加密的共享密钥。 **注**　**failover key** 共享机密在 **show running-config** 输出中显示为 *****；此已屏蔽的密钥不可复制。 无 ASDM 更改。
添加了故障转移的 IPv6 支持。	8.2(2)	我们修改了以下屏幕： Configuration > Device Management > High Availability > Failover > Setup Configuration > Device Management > High Availability > Failover > Interfaces

表 8-4　可选主用 / 备用故障转移设置的功能历史记录 （续）

功能名称	版本	功能信息
支持 IPsec LAN 对 LAN 隧道加密故障转移和状态链路通信。	9.1(2)	您现在可以将 IPsec LAN 对 LAN 隧道用于故障转移和状态链路加密，而不是对故障转移密钥使用专有加密。 **注**　故障转移 LAN 对 LAN 隧道不计入 IPsec （其他 VPN）许可证。 我们修改了以下屏幕：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转移，可以禁用模块监控。 我们修改了以下屏幕：**Configuration > Device Management > High Availability and Scalability > Failover > Interfaces**

ASA 集群

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

注 使用集群时，有些功能不受支持。请参阅第 9-22 页的集群不支持的功能。

关于 ASA 集群

本节介绍集群架构及其工作原理。

- 第 9-20 页的 ASA 集群如何管理连接
- 第 9-22 页的 ASA 功能和集群

ASA 集群如何融入网络中

集群包含多台 ASA，作为单一设备工作。要用作集群， ASA 需要以下基础设施：

- 独立的高速背板网络，称为*集群控制链路*，用于集群内的通信。
- 对每台 ASA 的管理访问权限，用于进行配置和监控。

将集群接入网络中时，上游和下游路由器需要能够使用以下方法之一使出入集群的数据实现负载均衡：

- 跨网络 EtherChannel （推荐） - 将多个集群成员上的接口分组为一个 EtherChannel ；EtherChannel 在设备之间执行负载均衡。
- 基于策略的路由 （仅适用于路由防火墙模式） - 上游和下游路由器使用路由映射和 ACL 在设备之间执行负载均衡。
- 等价多路径路由 （仅适用于路由防火墙模式） - 上游和下游路由器使用等价静态或动态路由在设备之间执行负载均衡。

相关主题

- 第 9-28 页的 ASA 集群的许可
- 第 9-5 页的集群控制链路
- 第 9-10 页的 ASA 集群管理
- 第 9-11 页的跨网络 EtherChannel （推荐）
- 第 9-15 页的基于策略的路由 （仅适用于路由防火墙模式）
- 第 9-16 页的等价多路径路由 （仅适用于路由防火墙模式）

性能换算系数

将多台设备组成一个集群时，预计可以达到近似如下的性能：

- 合并吞吐量的 70%
- 最大连接数的 60%
- 每秒连接数的 50%

以吞吐量为例，带 SSP-40 的 ASA 5585-X 在单独运行时大约可处理 10 Gbps 的实际防火墙流量。因此，由 8 台设备组成的集群的最大合并吞吐量约为 80 Gbps（8 台设备 x 10 Gbps）的 70%：56 Gbps。

集群成员

集群成员共同作用来实现安全策略和流量的共享。本节介绍每种成员角色的性质。

- 第 9-3 页的引导程序配置
- 第 9-3 页的主设备和从设备角色
- 第 9-3 页的主设备选举

引导程序配置

您要在每台设备上配置最低的引导程序配置，包括集群名称、集群控制链路接口和其他集群设置。第一台启用集群的设备通常会成为*主*设备。在后续设备上启用集群时，这些设备将作为*从*设备加入集群。

主设备和从设备角色

集群的一个成员是主设备。主设备由引导程序配置中的优先级设置决定；优先级可设置为 1 到 100，其中 1 为最高优先级。所有其他成员都是从设备。通常，在首次创建集群时，添加的第一台设备将成为主设备，只因为它是集群中当时唯一的设备。

必须仅在主设备上执行所有配置 （除引导程序配置之外）；随后，配置将被复制到从设备。如果是接口等物理资产，主设备的配置将被镜像到所有从设备。例如，如果将 GigabitEthernet 0/1 配置为内部接口并将 GigabitEthernet 0/0 配置为外部接口，则从设备上也会将这些接口用作内部和外部接口。

有些功能在集群中无法扩展，主设备将处理这些功能的所有流量。

相关主题

- 第 9-23 页的集群的集中功能

主设备选举

集群成员通过集群控制链路通信，如下选举主设备：

1. 为设备启用集群时 （或已经启用集群的设备首次启动时），设备将每 3 秒广播一次选举请求。
2. 优先级较高的其他所有设备将响应选举请求；优先级可设置为 1 到 100，其中 1 为最高优先级。
3. 如果在 45 秒后设备没有收到优先级更高的其他设备的响应，则该设备将成为主设备。

   注　如果有多台设备并列最高优先级，则先使用集群设备名称、再使用序列号来确定主设备。

4. 如果稍后有优先级更高的设备加入集群，该设备不会自动成为主设备；现有主设备将一直作为主设备，除非它停止响应，届时将选举新的主设备。

注　您可以手动强制一台设备成为主设备。对集中功能而言，如果强制更改主设备，则所有连接都将断开，而您必须在新的主设备上重新建立连接。

相关主题

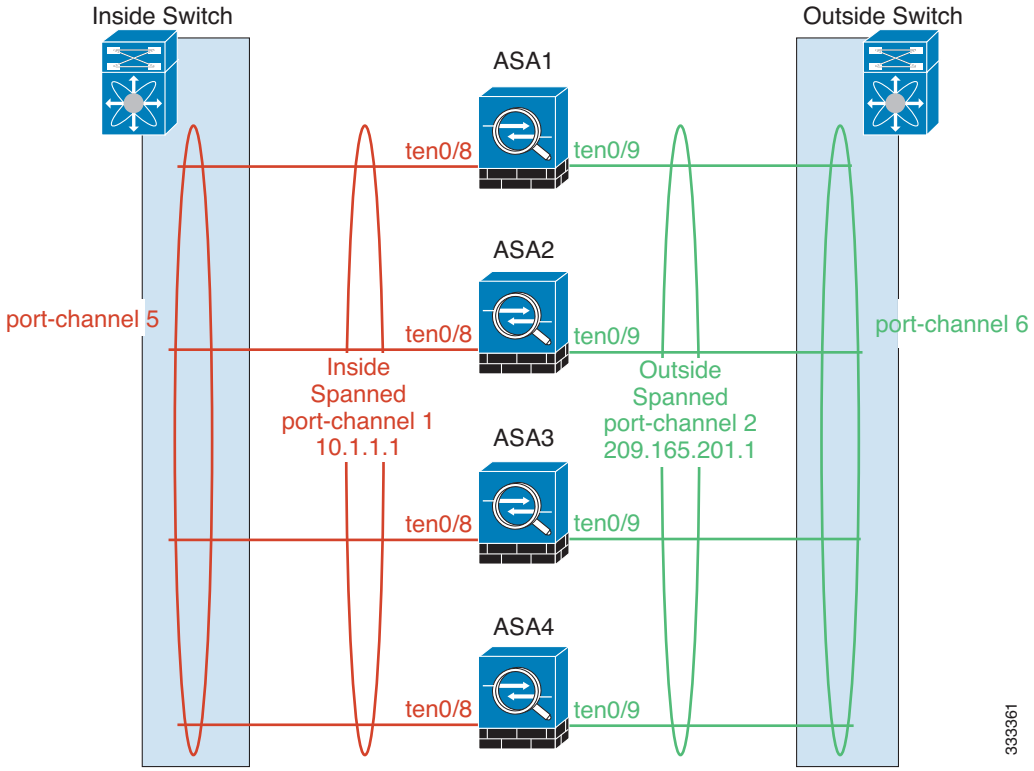
- 第 9-23 页的集群的集中功能

集群接口

可以将数据接口配置为跨网络 EtherChannel 或独立接口。集群中的所有数据接口只能是一种类型。

跨网络 EtherChannel （推荐）

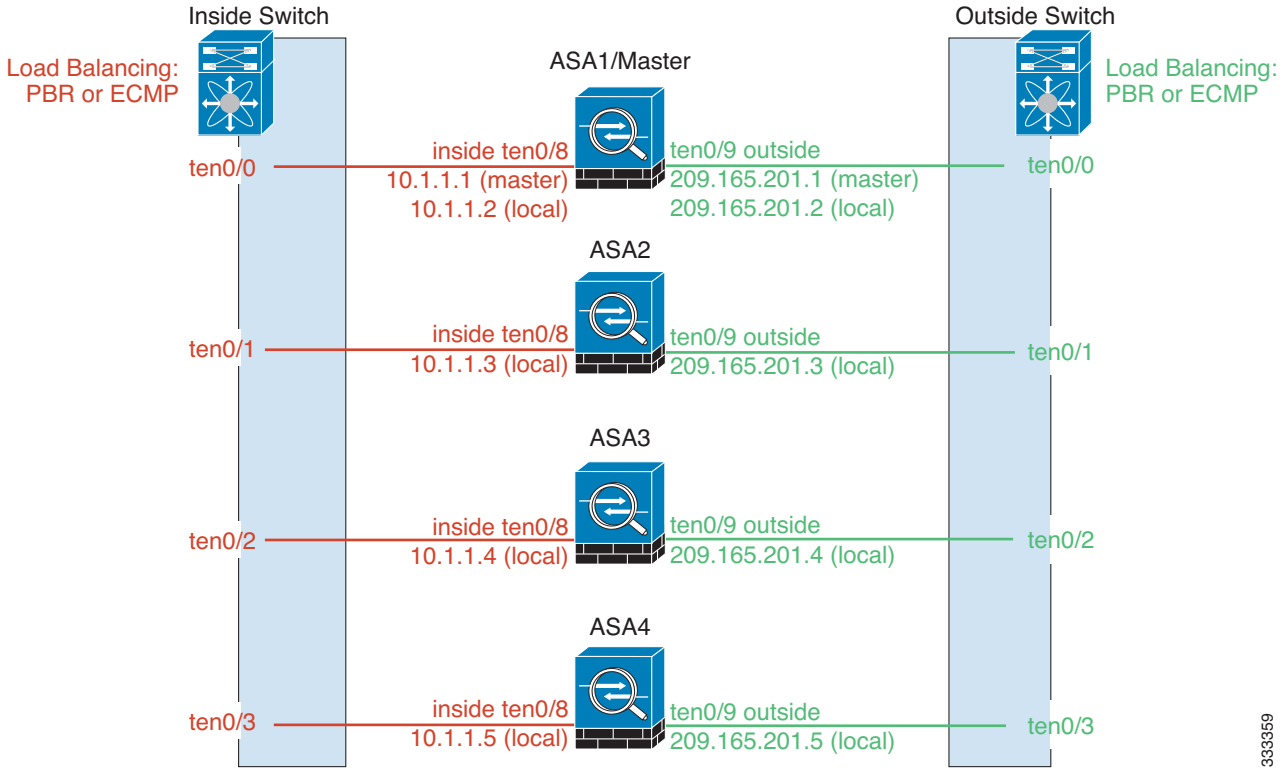
您可以将每台设备的一个或多个接口分组为跨集群中所有设备的 EtherChannel。 EtherChannel 汇聚信道中所有可用活动接口上的流量。在路由模式和透明防火墙模式中都可以配置跨网络 EtherChannel。在路由模式中， EtherChannel 被配置为只有一个 IP 地址的路由接口。在透明模式中， IP 地址被分配到网桥组而非接口。负载均衡属于 EtherChannel 固有的基本操作。



独立接口 （仅适用于路由防火墙模式）

独立接口是正常的路由接口，每个接口都有自己的*本地 IP 地址*。由于接口配置只能在主设备上配置，因此，您可以通过接口配置设置一个 IP 地址池，供集群成员上的给定接口 （包括主设备上的一个接口）使用。集群的*主集群 IP 地址*是集群的固定地址，始终属于当前的主设备。主集群 IP 地址是主设备的辅助 IP 地址；本地 IP 地址始终是用于路由的主要地址。主集群 IP 地址提供对地址的统一管理访问；当主设备更改时，主集群 IP 地址将转移到新的主设备，使集群的管理得以无缝继续。不过，在此情况下必须在上游交换机上分别配置负载均衡。

注　我们建议使用跨网络 EtherChannel 而不要使用独立接口，因为独立接口依靠路由协议来实现流量的负载均衡，而路由协议在链路发生故障时通常收敛速度缓慢。



相关主题

- 第 9-11 页的负载均衡方法

集群控制链路

每台设备至少必须将一个硬件接口专门用作集群控制链路。

- 第 9-5 页的集群控制链路流量概述
- 第 9-6 页的集群控制链路接口和网络
- 第 9-6 页的调整集群控制链路的吞吐量大小
- 第 9-7 页的集群控制链路冗余
- 第 9-7 页的集群控制链路可靠性
- 第 9-7 页的集群控制链路故障

集群控制链路流量概述

集群控制链路流量包括控制流量和数据流量。

控制流量包括：

- 主设备选举。
- 配置复制。
- 运行状况监控。

数据流量包括：

- 状态复制。
- 连接所有权查询和数据包转发。

相关主题

- 第 9-2 页的集群成员
- 第 9-9 页的配置复制
- 第 9-8 页的设备运行状况监控
- 第 9-9 页的数据路径连接状态复制
- 第 9-21 页的在集群中再均衡新的 TCP 连接

集群控制链路接口和网络

您可以将任何数据接口用于集群控制链路，但以下情况除外：

- VLAN 子接口不能用作集群控制链路。
- 管理 *x*/*x* 接口 （无论是作为独立接口还是作为 EtherChannel），都不能用作集群控制链路。
- 对于带 ASA IPS 模块的 ASA 5585-X，不能将模块接口用于集群控制链路；不过，可以使用 ASA 5585-X 网络模块上的接口。

可以使用 EtherChannel 或冗余接口。

如果带 SSP-10 和 SSP-20 的 ASA 5585-X 包含两个万兆以太网接口，建议将一个接口用于集群控制链路，另一个用于数据 （可将子接口用于数据）。尽管此设置无法满足集群控制链路的冗余要求，但可以满足调整集群控制链路使之符合数据接口流量大小的需要。

每条集群控制链路都有一个属于同一子网的 IP 地址。此子网应该与所有其他流量隔离，并且只包括 ASA 集群控制链路接口。

对于有 2 个成员的集群，请勿将集群控制链路从一台 ASA 直接连接到另一台 ASA。如果直接连接两个接口，则当一台设备发生故障时，集群控制链路失效，会导致剩下的那台正常设备也发生故障。而如果通过交换机连接集群控制链路，则集群控制链路仍会对正常设备打开。

相关主题

- 第 9-7 页的集群控制链路冗余
- 第 9-6 页的调整集群控制链路的吞吐量大小

调整集群控制链路的吞吐量大小

您应当调整集群控制链路的吞吐量大小，使之符合每个成员的预期吞吐量。例如，如果使用带 SSP-60 的 ASA 5585-X，集群中每台设备最多可传输 14 Gbps 的流量，则您也应该将接口分配到至少可传输 14 Gbps 流量的集群控制链路。在此情况下，可以将 EtherChannel 中的 2 个万兆以太网接口用于集群控制链路，并将其余接口根据需要用于数据链路。

集群控制链路流量主要由状态更新和转发的数据包组成。集群控制链路在任一给定时间的流量大小不尽相同。例如，如果经过的流量完全由持续时间极短的 TCP 连接组成，则状态更新在经过的流量中所占的比例可能高达 10%。转发流量的大小取决于负载均衡的功效或是否存在大量用于集中功能的流量。例如：

- NAT 会使连接的负载均衡不佳，需要对所有返回流量进行再均衡，将其转发到正确的设备。
- 用于网络访问的 AAA 是集中功能，因此所有流量都会转发到主设备。
- 当成员身份更改时，集群需要对大量连接进行再均衡，因此会暂时耗用大量集群控制链路带宽。

带宽较高的集群控制链路可以帮助集群在发生成员身份更改时更快地收敛，并防止出现吞吐量瓶颈。

注　如果集群中存在大量非对称 （再均衡）流量，应增加集群控制链路的吞吐量大小。

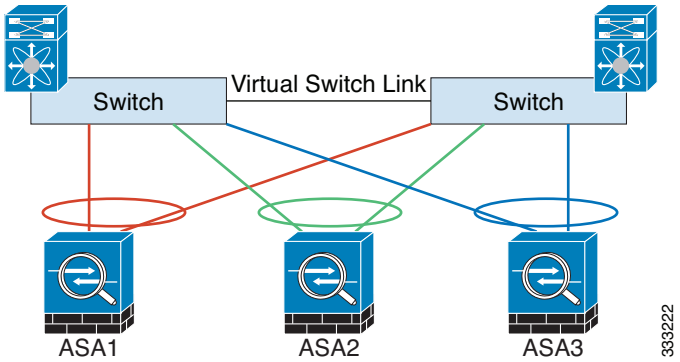
相关主题

- 第 9-16 页的站点间集群。

集群控制链路冗余

我们建议将 EtherChannel 用于集群控制链路，以便在 EtherChannel 中的多条链路上传输流量，同时又仍能实现冗余。

下图显示了如何在虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 环境中使用 EtherChannel 作为集群控制链路。EtherChannel 中的所有链路都是活动链路。如果交换机是 VSS 或 vPC 的一部分，则可将同一个 EtherChannel 中的 ASA 接口连接到 VSS 或 vPC 中单独的交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台单独的交换机的行为就像一台交换机一样。请注意，此 EtherChannel 是设备本地的，而非跨网络 EtherChannel。



集群控制链路可靠性

为了确保集群控制链路的功能，设备之间的往返时间 (RTT) 务必要小于 20 毫秒。此最大延迟能够增强与不同地理位置安装的集群成员的兼容性。要检查延迟，请在设备之间的集群控制链路上执行 ping 操作。

集群控制链路必须可靠，没有数据包顺序错乱或丢弃数据包的情况；例如，站点间部署应使用专用链路。

集群控制链路故障

如果某台设备的集群控制链路线路协议关闭，则集群将被禁用；数据接口关闭。当您修复集群控制链路之后，必须通过重新启用集群来手动重新加入集群。

注　当 ASA 处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。管理接口将保持打开，使用设备从集群 IP 池接收的 IP 地址。但是，如果您重新加载而设备在集群中仍然处于非活动状态，管理接口将无法访问 （因为它届时将使用与主设备相同的主 IP 地址）。您必须使用控制台端口来进行任何进一步配置。

相关主题

第 9-9 页的重新加入集群

ASA 集群中的高可用性

ASA 集群通过监控设备和接口的运行状况并在设备之间复制连接状态来提供高可用性。

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

设备运行状况监控

主设备通过在集群控制链路上定期 （此周期可配置）发送保持连接消息来监控每台从设备。每台从设备也使用相同的机制来监控主设备。

接口监控

每台设备都会监控使用中的所有硬件接口的链路状态，并向主设备报告状态更改。

- 跨网络 EtherChannel - 使用集群链路聚合控制协议 (cLACP)。每台设备都会监控链路状态和 cLACP 协议消息，以便确定 EtherChannel 中的端口是否仍处于活动状态。此状态将会报告给主设备。
- 独立接口 （仅适用于路由模式） - 每台设备都会监控自己的接口并向主设备报告接口状态。

设备或接口故障

启用运行状况监控时，如果某台设备或其接口发生故障，将从集群中删除该设备。如果特定设备上的一个接口发生故障，但其他设备上的相同接口处于活动状态，则会从集群中删除该设备。ASA 在多长时间后从集群中删除成员取决于接口的类型以及该设备是既定成员还是正在加入集群的设备。对于 EtherChannel （无论是否跨网络），如果既定成员上的接口关闭， ASA 将在 9 秒后删除该成员。 ASA 在设备加入集群后的最初 90 秒不监控接口。在此期间的接口状态更改不会导致 ASA 从集群中删除。如果是非 EtherChannel，则无论设备的成员状态如何，都会在 500 毫秒后删除设备。

当集群中的设备发生故障时，该设备承载的连接将无缝转移到其他设备；流量的状态信息将通过集群控制链路共享。

如果主设备发生故障，则优先级最高 （数字最小）的另一个集群成员将成为主设备。

ASA 将自动尝试重新加入集群。

注　当 ASA 处于非活动状态且无法自动重新加入集群时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。管理接口将保持打开，使用设备从集群 IP 池接收的 IP 地址。但是，如果您重新加载而设备在集群中仍然处于非活动状态，管理接口将无法访问 （因为它届时将使用与主设备相同的主 IP 地址）。您必须使用控制台端口来进行任何进一步配置。

相关主题

第 9-9 页的重新加入集群

重新加入集群

当集群成员从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路发生故障 - 解决集群控制链路的问题之后，必须重新启用集群来手动重新加入集群。
- 数据接口发生故障 - ASA 会依次在第 5 分钟、第 10 分钟和第 20 分钟时自动尝试重新加入。如果 20 分钟后仍加入失败， ASA 将禁用集群。解决数据接口问题之后，必须手动启用集群。
- 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

- 第 9-45 页的配置 ASA 集群参数

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 9-1　　在集群中复制的 ASA 功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	仅透明模式。
MAC 地址表	是	仅透明模式。
用户标识	是	包括 AAA 规则 (uauth) 和标识防火墙。
IPv6 邻居数据库	是	—
动态路由	是	—
SNMP 引擎 ID	否	—
VPN （站点到站点）	否	如果主设备发生故障， VPN 会话将断开连接。

配置复制

集群中的所有设备共享一个配置。除初始引导程序配置之外，您只能在主设备上进行配置更改，这些更改将自动复制到集群中的所有其他设备。

ASA 集群管理

使用 ASA 集群的优点之一是易于管理。本节介绍如何管理集群。

管理网络

我们建议将所有设备都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理接口

对于管理接口，我们建议使用一个专用管理接口。您可以将管理接口配置为独立接口 （适用于路由和透明模式）或跨网络 EtherChannel 接口。

即便使用跨网络 EtherChannel 作为数据接口，我们仍然建议使用独立接口作为管理接口。独立接口可以根据需要直接连接到每台设备，而跨网络 EtherChannel 接口则只允许远程连接到当前的主设备。

注　如果使用跨网络 EtherChannel 接口模式并将管理接口配置为独立接口，则无法为管理接口启用动态路由。您必须使用静态路由。

对于独立接口，主集群 IP 地址是集群的固定地址，始终属于当前的主设备。您还要为每个接口配置一个地址范围，以便包括当前主设备在内的每台设备都可以使用该范围内的本地地址。主集群 IP 地址提供对地址的统一管理访问；当主设备更改时，主集群 IP 地址将转移到新的主设备，使集群的管理得以无缝继续。本地 IP 地址用于路由，在排除故障时也非常有用。

例如，您可以连接到主集群 IP 地址来管理集群，该地址始终属于当前的主设备。要管理单个成员，可以连接到本地 IP 地址。

对于 TFTP 或系统日志等出站管理流量，包括主设备在内的每台设备都使用本地 IP 地址连接到服务器。

对于跨网络 EtherChannel 接口，只能配置一个 IP 地址，该 IP 地址始终属于主设备。您无法使用 EtherChannel 接口直接连接到从设备；我们建议将管理接口配置为独立接口，以便您连接到每台设备。请注意，可以使用设备本地 EtherChannel 进行管理。

主设备管理与从设备管理

除了引导程序配置外，所有管理和监控都可以在主设备上进行。您可以从主设备检查所有设备的运行时统计信息、资源使用率或其他监控信息。您也可以向集群中的所有设备发出命令，并将控制台消息从从设备复制到主设备。

如果需要，您可以直接监控从设备。虽然可以从主设备执行文件管理，但您也可以在从设备上执行 （包括备份配置和更新映像）。以下功能不可从主设备使用：

- 监控每台设备的集群特定统计信息。
- 每台设备的系统日志监控。
- SNMP
- NetFlow

RSA 密钥复制

在主设备上创建 RSA 密钥时，该密钥将被复制到所有从设备。如果您有连接到主集群 IP 地址的 SSH 会话，会在主设备发生故障时断开连接。新的主设备使用同一密钥进行 SSH 连接，因此在重新连接到新的主设备时，无需更新缓存的 SSH 主机密钥。

ASDM 连接证书 IP 地址不匹配

默认情况下，ASDM 连接将根据本地 IP 地址使用自签证书。如果使用 ASDM 连接到主集群 IP 地址，则会因证书使用本地 IP 地址而非主集群 IP 地址而显示一则警告消息，指出 IP 地址不匹配。您可以忽略该消息并建立 ASDM 连接。不过，为了避免此类警告，您也可以注册一个包含主集群 IP 地址和 IP 地址池中所有本地 IP 地址的证书。然后，您可将此证书用于每个集群成员。

相关主题

- 第 35 章，“数字证书”

负载均衡方法

可用的负载均衡方法取决于防火墙模式和接口类型。

- 第 9-11 页的跨网络 EtherChannel （推荐）
- 第 9-15 页的基于策略的路由 （仅适用于路由防火墙模式）
- 第 9-16 页的等价多路径路由 （仅适用于路由防火墙模式）

跨网络 EtherChannel （推荐）

您可以将每台设备的一个或多个接口分组为跨集群中所有设备的 EtherChannel。 EtherChannel 汇聚信道中所有可用活动接口上的流量。

- 第 9-11 页的跨网络 EtherChannel 的优点
- 第 9-12 页的最大吞吐量指导原则
- 第 9-12 页的负载均衡
- 第 9-12 页的 EtherChannel 冗余
- 第 9-12 页的连接到 VSS 或 vPC

跨网络 EtherChannel 的优点

我们优先推荐 EtherChannel 负载均衡方法，因其具有以下优点：

- 发现故障更快。
- 收敛速度更快。独立接口依靠路由协议来实现流量的负载均衡，而路由协议在链路发生故障时通常收敛速度缓慢。
- 易于配置。

相关主题

- 第 10-4 页的 EtherChannel

最大吞吐量指导原则

要实现最大吞吐量，建议采取以下措施：

- 使用 “ 对称 ” 的负载均衡哈希算法，亦即来自两个方向的数据包具有相同的哈希值，并将在跨网络 EtherChannel 中发送到同一台 ASA。我们建议将源和目标 IP 地址 （默认设置）或源和目标端口用作哈希算法。
- 将 ASA 连接到交换机时使用相同类型的线路卡，以使应用于所有数据包的哈希算法都相同。

负载均衡

EtherChannel 链路使用专有哈希算法并且根据源或目标 IP 地址以及 TCP 和 UDP 端口号进行选择。

注　在 ASA 上，请勿更改默认的负载均衡算法。在交换机上，建议使用以下算法之一：**source-dest-ip** 或 **source-dest-ip-port** （请参阅思科 Nexus OS 或思科 IOS **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中 ASA 的流量分摊不均。

EtherChannel 中的链路数量会影响负载均衡。

对称的负载均衡有时并不能够实现。如果配置了 NAT，则转发和返回数据包具有不同的 IP 地址和 / 或端口。返回流量将根据哈希值被发送到不同的设备，因此集群不得不将大部分返回流量重定向到正确的设备。

相关主题

- 第 10-20 页的自定义 EtherChannel
- 第 10-6 页的负载均衡
- 第 9-26 页的 NAT 和集群

EtherChannel 冗余

EtherChannel 有内置冗余。它监控所有链路的线路协议状态。如果一条链路发生故障，将在其余链路之间再均衡流量。如果 EtherChannel 中的所有链路在特定设备上发生故障，但其他设备仍然处于活动状态，则会从集群中删除该设备。

连接到 VSS 或 vPC

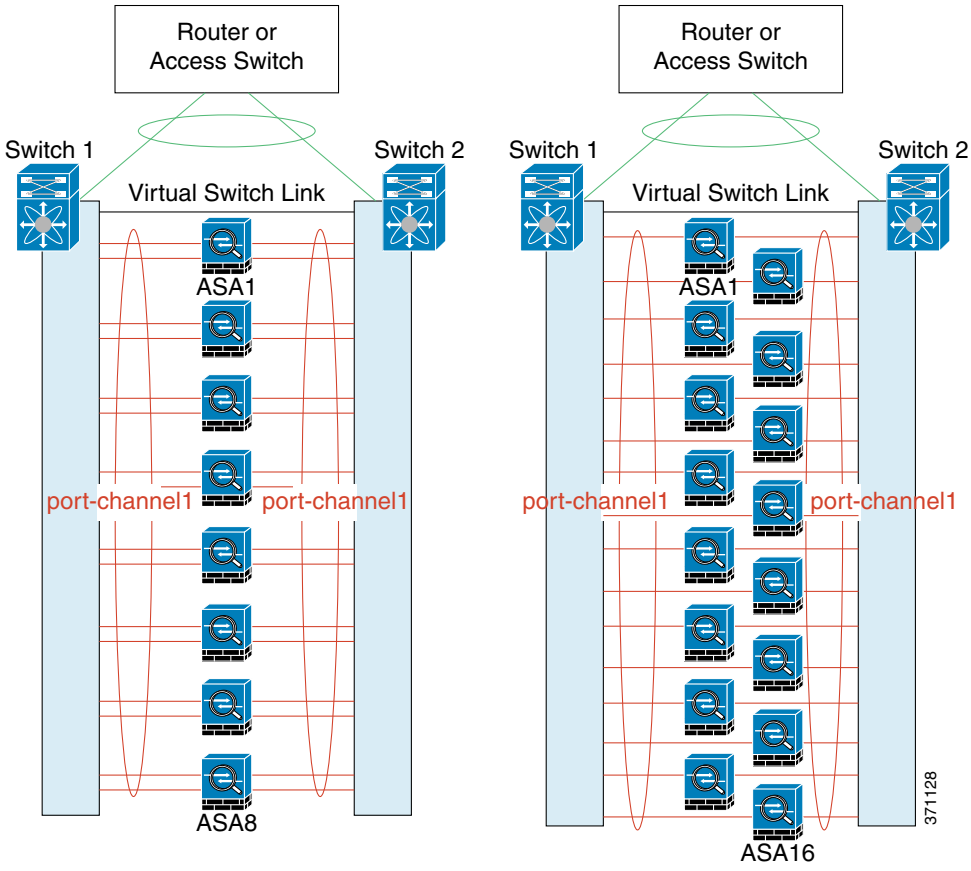
您可以在跨网络 EtherChannel 中包含每台 ASA 的多个接口。每台 ASA 多个接口对于连接到 VSS 或 vPC 中两台交换机的情况特别有用。

根据交换机的不同，最多可在跨网络 EtherChannel 中配置 32 条活动链路。此功能需要 vPC 中的两台交换机都支持各有 16 条活动链路的 EtherChannel （例如带 F2 系列 10 千兆以太网模块的思科 Nexus 7000）。

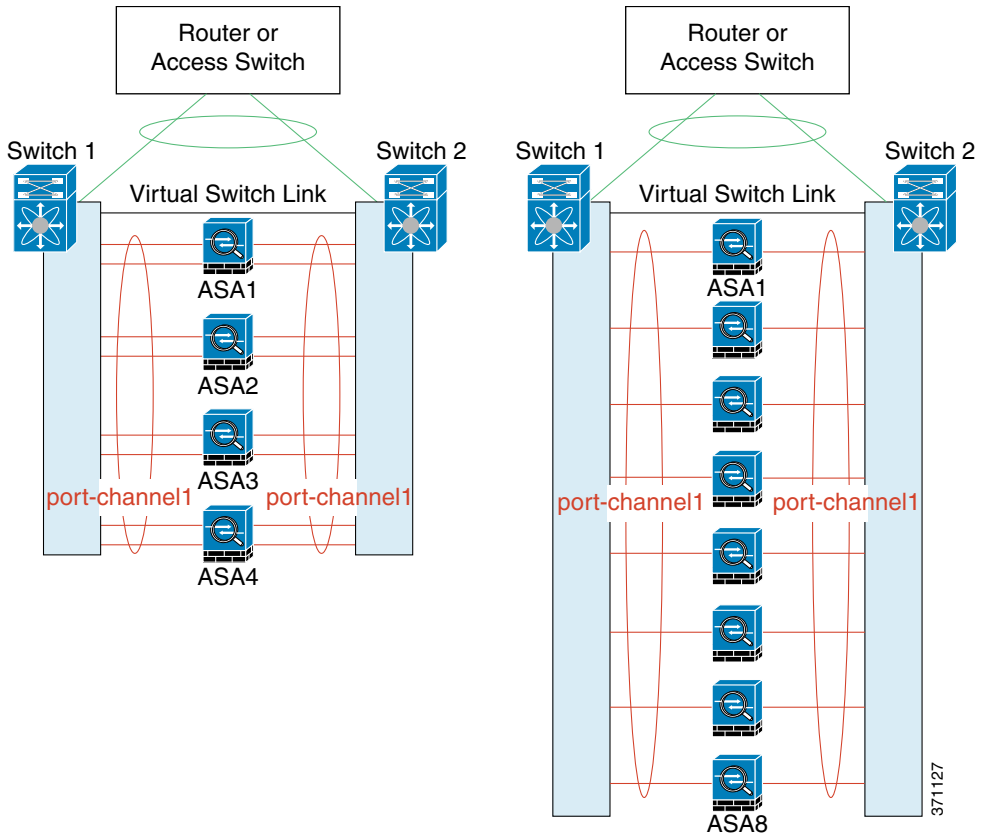
对于支持 EtherChannel 中有 8 条活动链路的交换机，在连接到 VSS/vPC 中的两台交换机时，最多可在跨网络 EtherChannel 中配置 16 条活动链路。

如果要在跨网络 EtherChannel 中使用 8 条以上的活动链路，则无法同时拥有备用链路；支持 9 到 32 条活动链路需要禁用允许使用备用链路的 cLACP 动态端口优先级。如果需要，您仍然可以使用 8 条活动链路和 8 条备用链路，例如在连接到一台交换机时。

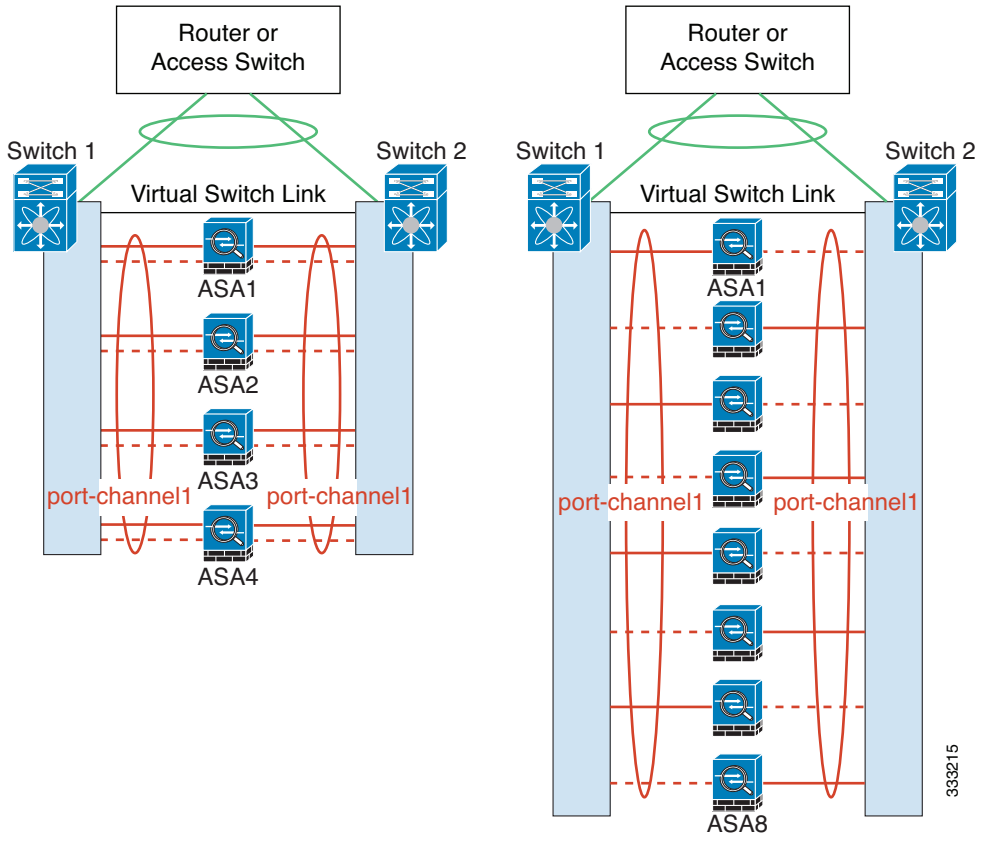
下图所示为 8-ASA 集群和 16-ASA 集群中有 32 条活动链路的跨网络 EtherChannel。



下图所示为 4-ASA 集群和 8-ASA 集群中有 16 条活动链路的跨网络 EtherChannel。



下图所示为 4-ASA 集群和 8-ASA 集群中的有 8 条活动和 8 条备用链路的传统跨网络 EtherChannel。活动链路以实线表示，非活动链路以虚线表示。cLACP 负载均衡可自动选择最佳的 8 条链路作为 EtherChannel 中的活动链路。如图所示， cLACP 可以帮助在链路层面实现负载均衡。



基于策略的路由 （仅适用于路由防火墙模式）

使用独立接口时，每个 ASA 接口都会保留自己的 IP 地址和 MAC 地址。基于策略的路由 (PBR) 是一种负载均衡方法。

如果已经在使用 PBR 并希望充分利用现有的基础设施，建议使用此方法。与跨网络 EtherChannel 相比，此方法也可以提供其他调整选项。

PBR 根据路由映射和 ACL 作出路由决定。您必须在集群中的所有 ASA 之间手动划分流量。由于 PBR 是静态路由，因此可能有时候无法实现最佳的负载均衡效果。要实现最佳性能，建议您通过配置 PBR 策略，将一条连接的转发和返回数据包定向到同一台物理 ASA。例如，如果您有一台思科路由器，使用带对象跟踪的思科 IOS PBR 即可实现冗余。思科 IOS 对象跟踪使用 ICMP ping 监控每台 ASA。然后， PBR 可根据特定 ASA 的可接通性来启用或禁用路由映射。有关详细信息，请参阅以下 URL：

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

注　如果使用此负载均衡方法，则可使用设备本地 EtherChannel 作为独立接口。

等价多路径路由 （仅适用于路由防火墙模式）

使用独立接口时，每个 ASA 接口都会保留自己的 IP 地址和 MAC 地址。等价多路径 (ECMP) 路由是一种负载均衡方法。

如果已经在使用 ECMP 并希望充分利用现有的基础设施，建议使用此方法。与跨网络 EtherChannel 相比，此方法也可以提供其他调整选项。

ECMP 路由可以通过路由度量并列最优的多条 “ 最佳路径 ” 转发数据包。它与 EtherChannel 一样，也可以使用源和目标 IP 地址及 / 或源和目标端口的哈希值将数据包发送到下一跳之一。如果将静态路由用于 ECMP 路由，则 ASA 故障会导致问题；如果继续使用该路由，发往故障 ASA 的流量将丢失。因此，如果使用静态路由，请务必要使用静态路由监控功能，例如对象跟踪。我们还建议使用动态路由协议来添加和删除路由，在这种情况下，您必须配置每台 ASA 使之加入动态路由。

注　如果使用此负载均衡方法，则可使用设备本地 EtherChannel 作为独立接口。

站点间集群

对于站点间安装，只要遵循以下指导原则就可以充分发挥 ASA 集群的作用。

- 第 9-16 页的站点间集群指导原则
- 第 9-17 页的确定数据中心互联的规格
- 第 9-18 页的站点间集群示例

站点间集群指导原则

请参阅有关站点间集群的以下指导原则：

- 在以下接口和防火墙模式中，支持站点间集群：

	防火墙模式	
接口模式	**路由**	**透明**
独立接口	**是**	不适用
跨网络 EtherChannel	否	**是**

- 集群控制链路的延迟必须小于 20 微秒往返时间 (RTT)。
- 集群控制链路必须可靠，没有数据包顺序错乱或丢弃数据包的情况；例如，应该使用专用链路。
- 请勿配置连接再均衡；您不需要将连接再均衡到位于不同站点的集群成员。
- 位于多个站点的成员之间的集群实施没有区别；因此，给定连接的连接角色可以跨越所有站点。这是预期行为。
- 对于透明模式，必须确保两台内部路由器共用同一个 MAC 地址，两台外部路由器也共用同一个 MAC 地址。当位于站点 1 的集群成员将连接转发到位于站点 2 的成员时，目标 MAC 地址会被保留。如果该 MAC 地址与位于站点 1 的路由器相同，则数据包只会到达位于站点 2 的路由器。
- 对于跨网络 EtherChannel 模式，请勿扩展直接连接到站点间 ASA 集群的数据 VLAN ；会造成环路。任何扩展的数据 VLAN 都必须以路由器与集群分隔开来。

相关主题

- 第 9-21 页的在集群中再均衡新的 TCP 连接
- 第 9-20 页的连接角色

确定数据中心互联的规格

您应该在数据中心互联 (DCI) 上为集群控制链路流量保留等同于以下计算结果的带宽：

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

如果各站点的成员数不同，请使用较大的数量进行计算。 DCI 的最低带宽不得低于一个成员的集群控制链路的流量大小。

例如：

- 位于 2 个站点的 4 个成员：
  - 总共 4 个集群成员
  - 每个站点 2 个成员
  - 每个成员 5 Gbps 集群控制链路

  保留的 DCI 带宽 = 5 Gbps (2/2 x 5 Gbps)。
- 对位于 2 个站点的 8 个成员而言，规格加大：
  - 总共 8 个集群成员
  - 每个站点 4 个成员
  - 每个成员 5 Gbps 集群控制链路

  保留的 DCI 带宽 = 10 Gbps (4/2 x 5 Gbps)。
- 位于 3 个站点的 6 个成员：
  - 总共 6 个集群成员
  - 站点 1 有 3 个成员，站点 2 有 2 个成员，站点 3 有 1 个成员
  - 每个成员 10 Gbps 集群控制链路

  保留的 DCI 带宽 = 15 Gbps (3/2 x 10 Gbps)。
- 位于 2 个站点的 2 个成员：
  - 总共 2 个集群成员
  - 每个站点 1 个成员
  - 每个成员 10 Gbps 集群控制链路

  保留的 DCI 带宽 = 10 Gbps （1/2 x 10 Gbps = 5 Gbps ； 但最低带宽不得低于集群控制链路的流量大小 (10 Gbps)）。

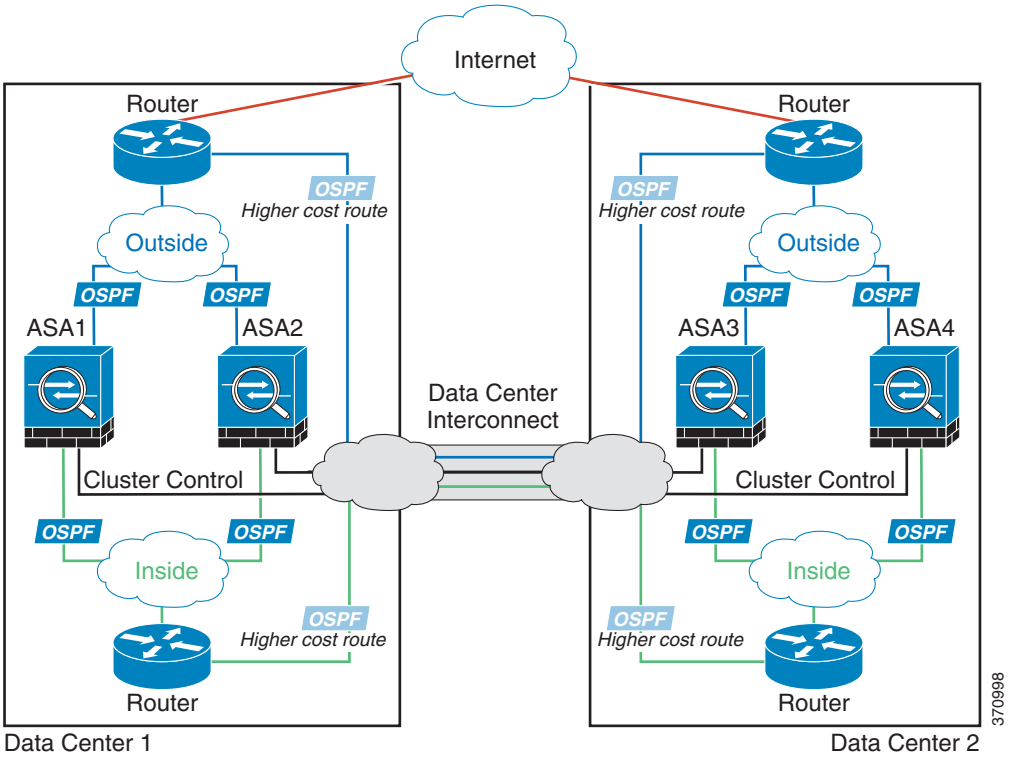
站点间集群示例

以下示例显示支持的集群部署。

- 第 9-18 页的独立接口站点间集群示例
- 第 9-19 页的跨网络 EtherChannel 透明模式站点间集群示例

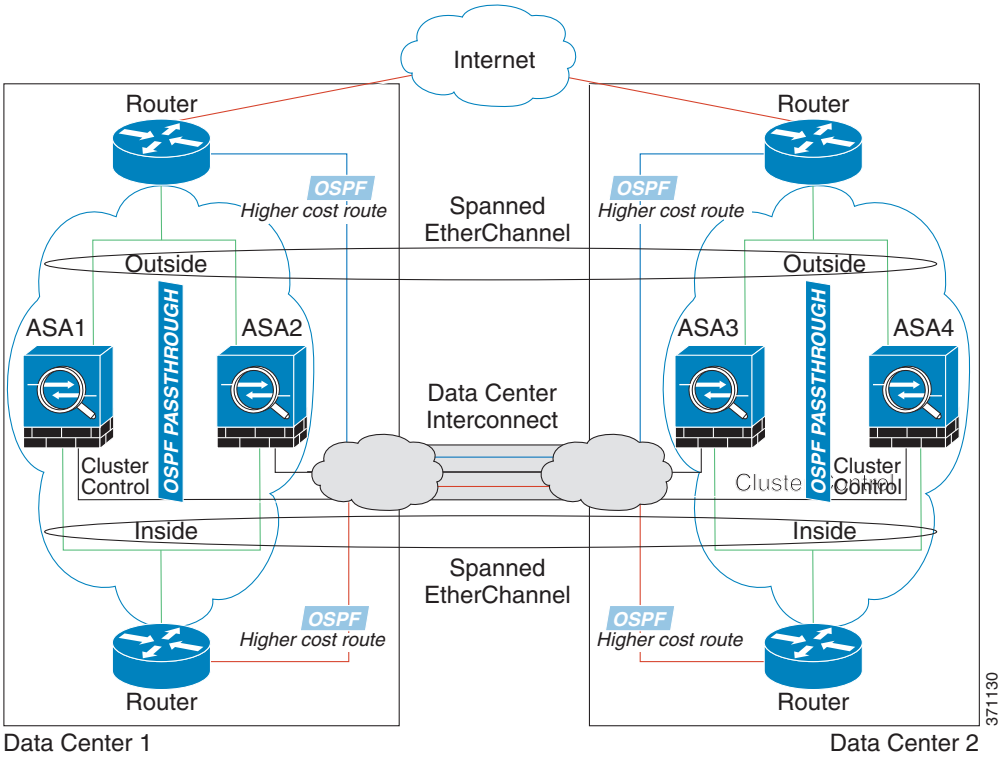
独立接口站点间集群示例

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



跨网络 EtherChannel 透明模式站点间集群示例

以下图例显示了分别位于 2 个数据中心的 2 个 ASA 集群成员。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部的跨网络 EtherChannel 连接到本地交换机。ASAEtherChannel 跨越集群中的所有 ASA。位于每个数据中心的内部和外部路由器使用 OSPF 经过透明的 ASA。与 MAC 地址不同，路由器 IP 地址在所有路由器上都是唯一的。通过指定 DCI 中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有 ASA 集群成员都中断连接。通过 ASA 的开销较低的路由必须经过位于每个站点的同一网桥组才能使集群维持非对称连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的 ASA 集群成员。



位于每个站点的交换机的实施可包括：

- 站点间 VSS/vPC - 在此情景中，一台交换机安装在数据中心 1，另一台交换机安装在数据中心 2。一个方案是将位于每个数据中心的 ASA 集群设备只连接到本地交换机，而 VSS/vPC 流量通过 DCI 传输。在此情况下，连接多半会保持在每个数据中心本地。如果 DCI 可以处理额外的流量，您也可以选择将每台 ASA 设备通过 DCI 连接到两台交换机。在此情况下，流量跨数据中心分摊，因此 DCI 必须非常强健稳定。
- 位于每个站点的本地 VSS/vPC - 为了获得更高的交换机冗余能力，可以在每个站点安装 2 对单独的 VSS/vPC。在此情况下，尽管 ASA 仍然有一个跨网络 EtherChannel 将数据中心 1 的 ASA 仅连接到两台本地交换机，将数据中心 2 的 ASA 连接到本地交换机，但跨网络 EtherChannel 本质上是 “ 分离的 ”。每个本地 VSS/vPC 都会将跨网络 EtherChannel 视为站点本地的 EtherChannel。

ASA 集群如何管理连接

可以将连接负载均衡到多个集群成员。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。

连接角色

为每个连接定义了 3 种不同的 ASA 角色：

- 所有者 - 最初接收连接的设备。所有者负责维护 TCP 状态并处理数据包。一个连接只有一个所有者。
- 导向者 - 处理来自转发者的所有者查找请求，同时也维护连接状态，在所有者发生故障时作为备用设备。当所有者收到新连接时，会根据源 / 目标 IP 地址和 TCP 端口的哈希值选择导向者，然后向导向者发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他设备，该设备会向导向者查询哪一台设备是所有者，以便转发数据包。一个连接只有一个导向者。
- 转发者 - 向所有者转发数据包的设备。如果转发者收到并非其所有的连接的数据包，则会向导向者查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向者也可以是转发者。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN cookie 直接获知所有者，因此无需向导向者查询。（如果禁用 TCP 序列随机化，则不会使用 SYN cookie；必须向导向者查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向者，然后由其发送到所有者。一个连接可有多个转发者；采用良好的负载均衡方法可以做到没有转发者，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。

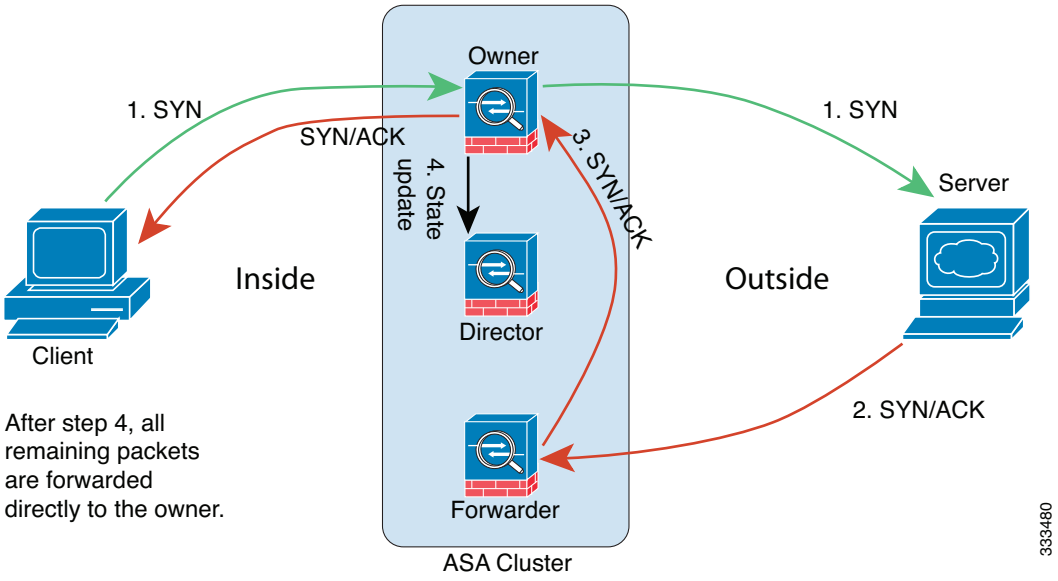
新连接所有权

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

相关主题

数据流示例

以下图例显示了新连接的建立。



1. SYN 数据包从客户端发出，被传送到一台 ASA （基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 ASA （基于负载均衡方法）。此 ASA 是转发者。
3. 由于转发者不是该连接的所有者，因此它将解码 SYN cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向者，然后将 SYN-ACK 数据包转发到客户端。
5. 导向者接收来自所有者的状态更新，创建发往所有者的流量，并记录 TCP 状态信息以及所有者。导向者将充当该连接的备用所有者。
6. 传送到转发者的任何后续数据包都会被转发到所有者。
7. 如果数据包被传送到任何其他设备，它将向导向者查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向者发送状态更新。

在集群中再均衡新的 TCP 连接

如果上游或下游路由器的负载均衡功能导致流量分摊不均衡，可以将过载的设备配置为将新的 TCP 流量重定向到其他设备。现有流量不会被转移到其他设备。

ASA 功能和集群

有些 ASA 功能不受 ASA 集群支持，还有些功能只有在主设备上才受支持。其他功能可能对如何正确使用规定了注意事项。

集群不支持的功能

以下功能在启用集群的情况下无法配置，相关命令会被拒绝。

- 统一通信
- 远程接入 VPN （SSL VPN 和 IPsec VPN）
- 以下应用检查：
  - CTIQBE
  - GTP
  - H323、 H225 和 RAS
  - IPsec 直通
  - MGCP
  - MMP
  - RTSP
  - SIP
  - SCCP (Skinny)
  - WAAS
  - WCCP
- 僵尸网络流量过滤器
- 自动更新服务器
- DHCP 客户端、服务器、中继和代理
- VPN 负载均衡
- 故障转移
- ASA CX 模块

集群的集中功能

以下功能只有在主设备上才受支持，且无法为集群扩展。例如，您有一个由 8 台设备 （带 SSP-60 的 5585-X）组成的集群。“ 其他 VPN” 许可证允许一台带 SSP-60 的 5585-X 最多有 10,000 个站点间 IPsec 隧道。对于由 8 台设备组成的整个集群，您只能使用 10,000 个隧道；此功能无法扩展。

注　集中功能的流量从成员设备通过集群控制链路转发到主设备。

如果使用再均衡功能，则会先将集中功能的流量再均衡到非主设备的设备，然后再将该流量归类为集中功能；如果发生此情况，该流量随后将被发送回主设备。

对集中功能而言，如果主设备发生故障，则所有连接都将断开，而您必须在新的主设备上重新建立连接。

- 站点到站点 VPN
- 以下应用检查：
  - DCERPC
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- 动态路由 （仅适用于跨网络 EtherChannel 模式）
- 组播路由 （仅适用于独立接口模式）
- 静态路由监控
- IGMP 组播控制层面协议的处理 （数据层面转发分布于整个集群中）
- PIM 组播控制层面协议的处理 （数据层面转发分布于整个集群中）
- 网络访问的身份验证和授权。记帐被分散。
- 过滤服务

相关主题

- 第 9-6 页的调整集群控制链路的吞吐量大小
- 第 9-21 页的在集群中再均衡新的 TCP 连接

应用到各设备的功能

以下功能将应用到每台 ASA 设备而非整个集群或主设备。

- QoS - QoS 策略将于配置复制过程中在集群中同步。不过，该策略是在每台设备上独立实施。例如，如果对输出配置管制，则要对流出特定 ASA 的流量应用符合速率和符合突发量值。在由 8 台设备组成且流量均摊的集群中，符合速率实际上变成了集群*速率*的 8 倍。
- 威胁检测 - 威胁检测在各台设备上独立工作；例如，排名统计信息就要视具体设备而定。以端口扫描检测为例，由于扫描的流量将在所有设备间进行负载均衡，而一台设备无法看到所有流量，因此端口扫描检测无法工作。
- 资源管理 - 多情景模式中的资源管理根据本地使用情况在每台设备上分别执行。
- ASA FirePOWER 模块 - ASA FirePOWER 模块之间不存在配置同步或状态共享。您要负责使用 FireSIGHT 管理中心在集群中的 ASA FirePOWER 模块上保持策略的一致性。请勿对集群内的设备使用不同的基于 ASA 接口的区域定义。
- ASA IPS 模块 - IPS 模块之间不存在配置同步或状态共享。有些 IPS 签名需要 IPS 跨多个连接保存状态信息。例如，当 IPS 模块检测到有人打开多个连接到同一台服务器的连接但端口不同时，将使用端口扫描签名。在集群中，这些连接将在多台 ASA 设备之间进行均衡，其中每台设备都有自己的 IPS 模块。由于这些 IPS 模块并不共享状态信息，因此集群可能无法检测端口扫描。

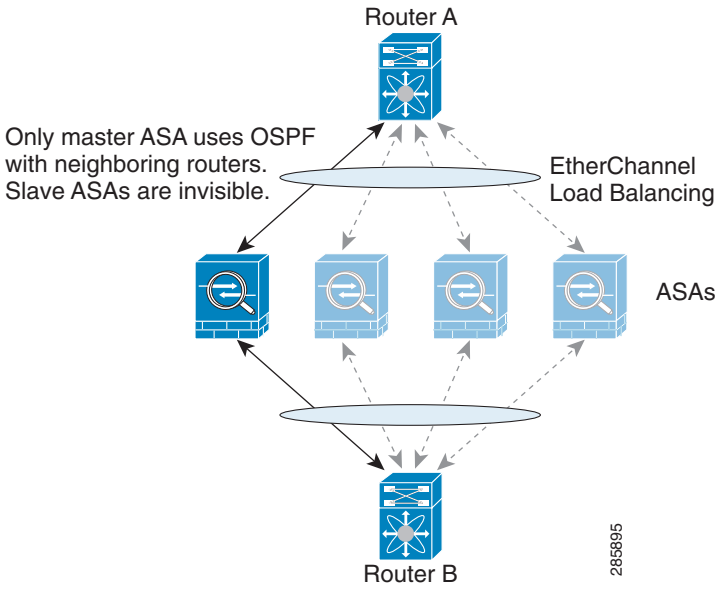
动态路由和集群

- 第 9-24 页的跨网络 EtherChannel 模式中的动态路由
- 第 9-25 页的独立接口模式中的动态路由

跨网络 EtherChannel 模式中的动态路由

在跨网络 EtherChannel 模式中，路由进程仅在主设备上运行，路由通过主设备获知并复制到从设备。如果路由数据包到达从设备，会被重定向到主设备。

图 9-1　跨网络 EtherChannel 模式中的动态路由



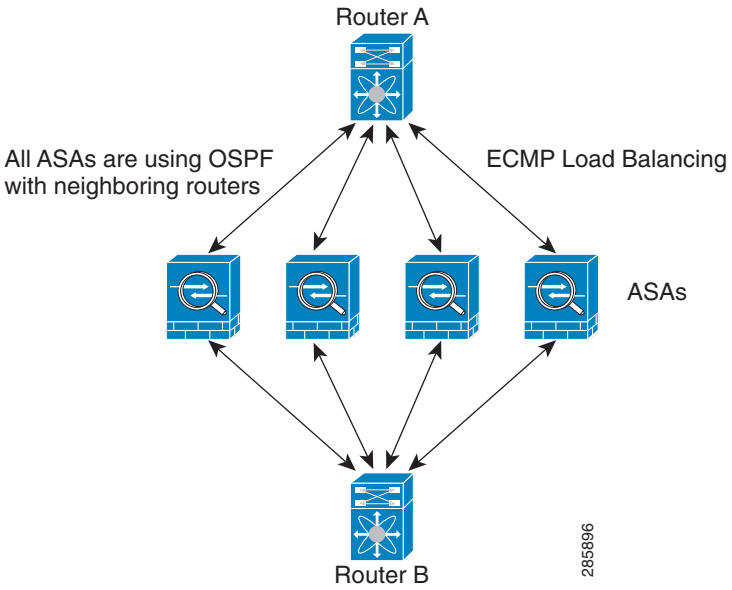
当从设备成员从主设备获知路由后，每台设备将独立作出转发决定。

OSPF LSA 数据库不会从主设备同步到从设备。如果发生主设备切换，邻居路由器将检测到重新启动；切换并非透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。

独立接口模式中的动态路由

在独立接口模式中，每台设备作为独立的路由器运行路由协议，且每台设备独立获知路由。

图 9-2　　独立接口模式中的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一台 ASA。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每台 ASA 在与外部路由器通信时，会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每台设备都有单独的路由器 ID。

组播路由和集群

组播路由的行为因接口模式而异。

- 第 9-25 页的跨网络 EtherChannel 模式中的组播路由
- 第 9-25 页的独立接口模式中的组播路由

跨网络 EtherChannel 模式中的组播路由

在跨网络 EtherChannel 模式中，主设备负责处理所有组播路由数据包和数据包，直到建立快速路径转发为止。在连接建立之后，每台从设备都可以转发组播数据包。

独立接口模式中的组播路由

在独立接口模式中，设备并不独立处理组播。所有数据包和路由数据包都由主设备处理和转发，从而避免数据包复制。

NAT 和集群

NAT 可能会影响集群的整体吞吐量。入站和出站 NAT 数据包可被发送到集群中不同的 ASA，因为负载均衡算法取决于 IP 地址和端口， NAT 会导致入站和出站数据包具有不同的 IP 地址和 / 或端口。当数据包到达并非连接所有者的 ASA 时，会通过集群控制链路被转发到所有者，导致集群控制链路上存在大量流量。

如果您仍想在集群中使用 NAT，请考虑以下指导原则：

- 不使用代理 ARP - 对于独立接口，切勿为映射的地址发送代理 ARP 应答。这可以防止邻接路由器与可能已经不在集群中的 ASA 保持对等关系。对于指向主集群 IP 地址的映射地址，上游路由器需要静态路由或带对象跟踪的 PBR。这对跨网络 EtherChannel 来说不是问题，因为只有一个 IP 地址与集群接口关联。
- 不对独立接口使用接口 PAT - 独立接口不支持接口 PAT。
- 对动态 PAT 使用 NAT 池地址分配 - 主设备在整个集群中预先平均分配地址。如果成员收到连接却没有剩余的地址，即使其他成员仍有可用地址，该连接仍会断开。因此，请确保至少包含与集群中的设备数量相同的 NAT 地址，务必让每台设备都收到一个地址。使用 **show nat pool cluster** 命令查看地址分配。
- 不使用轮询 - 集群不支持 PAT 池轮询。
- 主设备管理的动态 NAT 转换项 - 主设备负责维护转换表并将其复制到从设备。当从设备收到需要动态 NAT 的连接而转换项不在表中时，将向主设备请求该转换项。从设备是该连接的所有者。
- 每会话 PAT 功能 - 每会话 PAT 功能并非集群专用功能，但它能提高 PAT 的可扩展性，而且对集群而言，它允许每台从设备成为 PAT 连接的所有者；相比之下，多会话 PAT 连接则必须转发到主设备并由主设备所有。默认情况下，所有 TCP 流量和 UDP DNS 流量都使用每会话 PAT 转换项。对于 H.323、 SIP 或 Skinny 等需要多会话 PAT 的流量，可禁用每会话 PAT。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。
- 对以下检查不使用静态 PAT -
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - 所有 IP 语音应用

用于网络访问的 AAA 和集群

用于网络访问的 AAA 由三部分组成：身份验证、授权和记帐。身份验证和记帐作为集中功能在集群主设备上实施，数据结构被复制到集群从设备。如果选举出主设备，新的主设备将获得所需的全部信息，让通过身份验证的既定用户及其关联的授权能够继续操作而不中断。发生主设备更改时，用户身份验证的空闲超时和绝对超时会被保留。

记帐作为分散的功能在集群中实施。记帐按每次流量完成，因此在为流量配置记帐时，作为流量所有者的集群设备会将记帐开始和停止消息发送到 AAA 服务器。

系统日志与 NetFlow 和集群

- 系统日志 - 集群中的每台设备都会生成自己的系统日志消息。您可以配置日志记录，使每台设备在系统日志消息的报头字段中使用相同或不同的设备 ID。例如，集群中的所有设备都会复制和共享主机名配置。如果将日志记录配置为使用主机名作为设备 ID，则所有设备生成的系统日志消息都会看似来自一台设备。如果将日志记录配置为使用集群引导程序配置中指定的本地设备名称作为设备 ID，系统日志消息就会看似来自不同设备。
- NetFlow - 集群中的每台设备都会生成自己的 NetFlow 数据流。 NetFlow 采集器只能将每台 ASA 视为单独的 NetFlow 导出器。

相关主题

- 第 40-19 页的在非 EMBLEM 格式系统日志消息中包含设备 ID

SNMP 和集群

SNMP 代理按照本地 IP 地址轮询每台单独的 ASA。您无法轮询集群的合并数据。

应该始终使用本地地址而非主集群 IP 地址进行 SNMP 轮询。如果 SNMP 代理轮询主集群 IP 地址，则当选举出新的主设备时，对新的主设备的轮询将失败。

VPN 和集群

站点到站点 VPN 是集中功能；只有主设备支持 VPN 连接。

注　集群不支持远程接入 VPN。

VPN 功能仅限主设备使用，且不能利用集群的高可用性功能。如果主设备发生故障，所有现有的 VPN 连接都将丢失，VPN 用户将遇到服务中断。选举出新的主设备后，必须重新建立 VPN 连接。

将 VPN 隧道连接到跨网络 EtherChannel 地址时，连接会自动转移到主设备。对于使用 PBR 或 ECMP 时与独立接口的连接，必须始终连接到主集群 IP 地址而非本地地址。

与 VPN 相关的密钥和证书将被复制到所有设备。

FTP 和集群

- 如果 FTP 数据信道和控制信道流量由不同的集群成员所有，数据信道所有者会将空闲超时更新定期发送到控制信道所有者并更新空闲超时值。但是，如果重新加载控制流量所有者并重新托管控制流量，则不会再保持父 / 子流量关系；控制流量空闲超时不会更新。
- 如果将 AAA 用于 FTP 访问，则控制信道流量将集中在主设备上。

思科 TrustSec 和集群

只有主设备可获知安全组标记 (SGT) 信息。然后，主设备将向从设备提供 SGT，从设备可根据安全策略为 SGT 作出匹配项决定。

ASA 集群的许可

型号	许可证要求
ASA 5585-X	集群许可证，最多可支持 16 台设备。 每台设备上都需要集群许可证。对于其他功能许可证，集群设备并不要求每台设备上的许可证相同。如果多台设备上有功能许可证，这些许可证将合并成一个 ASA 集群运行许可证。 **注**　每台设备必须拥有相同的加密许可证和相同的 10 GE I/O 许可证。
ASA 5512-X	增强型安全许可证，支持 2 台设备。 **注**　每台设备必须拥有相同的加密许可证。
ASA 5515-X、 ASA 5525-X、 ASA 5545-X 和 ASA 5555-X	基础许可证，支持 2 台设备。 **注**　每台设备必须拥有相同的加密许可证。
所有其他型号	不支持。

ASA 集群的先决条件

ASA 硬件和软件要求

集群中的所有设备：

- 必须为相同型号且 DRAM 相同。闪存的大小不必相同。
- 必须运行相同的软件，映像升级时除外。支持无中断升级。
- 使用独立接口模式时，集群成员可以位于不同的地理位置 （站点间）。
- 必须处于相同的安全情景模式中，无论是单情景模式还是多情景模式。
- （单情景模式）必须处于相同的防火墙模式中，无论是路由模式还是透明模式。
- 在配置复制之前，新的集群成员对初始集群控制链路通信必须使用与主设备相同的 SSL 加密设置 （**ssl encryption** 命令）。
- 必须有相同的集群和加密许可证， ASA 5585-X 还必须有相同的 10 GE I/O 许可证。

交换机先决条件

- 请务必完成交换机配置后再在 ASA 上配置集群。
- 下表列出了支持与 ASA 集群交互操作的外部硬件和软件。

表 9-2　ASA 集群的外部硬件和软件支持

外部硬件	外部软件	ASA 版本
思科 Nexus 9300	思科 NX-OS 6.1(2)I2(1) 及更高版本	9.2(1) 及更高版本
思科 Nexus 7000	思科 NX-OS 5.2(5) 及更高版本	9.0(1) 及更高版本
思科 Nexus 5000	思科 NX-OS 7.0(1) 及更高版本	9.1(4) 及更高版本

表 9-2　　ASA 集群的外部硬件和软件支持 （续）

外部硬件	外部软件	ASA 版本
带 Supervisor 32、 720 和 720-10GE 的 Catalyst 6500	思科 IOS 12.2(33)SXI7、 SXI8、 SXI9 及更高版本	9.0(1) 及更高版本
Catalyst 3750-X	思科 IOS 15.0(2) 及更高版本	9.1(4) 及更高版本

ASA 先决条件

- 将设备加入管理网络之前，为每台设备提供唯一的 IP 地址。
  - 有关连接到 ASA 并设置管理 IP 地址的详细信息，请参阅 “ 入门 ” 一章。
  - 除用作主设备 （通常为添加到集群中的第一台设备）使用的 IP 地址外，这些管理 IP 地址仅供临时使用。
  - 从设备加入集群后，其管理接口配置将替换为从主设备复制的配置。
- 要在集群控制链路上使用巨型帧 （推荐），必须在启用集群之前启用巨型帧保留。

其他先决条件

建议使用终端服务器访问所有集群成员设备的控制台端口。为了进行初始设置和持续管理 （例如在设备发生故障时），终端服务器对于远程管理非常有用。

相关主题

- 第 9-29 页的 ASA 集群的指导原则
- 第 10-25 页的启用巨型帧支持
- 第 9-3 页的引导程序配置

ASA 集群的指导原则

情景模式

每台成员设备上的模式必须相符。

防火墙模式

对于单情景模式，所有设备上的防火墙模式必须相符。

故障转移

集群不支持故障转移。

IPv6

集群控制链路只有在使用 IPv4 时才受支持。

型号

支持的型号：

- ASA 5585-X

  如果带 SSP-10 和 SSP-20 的 ASA 5585-X 包含两个万兆以太网接口，建议将一个接口用于集群控制链路，另一个用于数据 （可将子接口用于数据）。尽管此设置无法满足集群控制链路的冗余要求，但可以满足调整集群控制链路使之符合数据接口流量大小的需要。

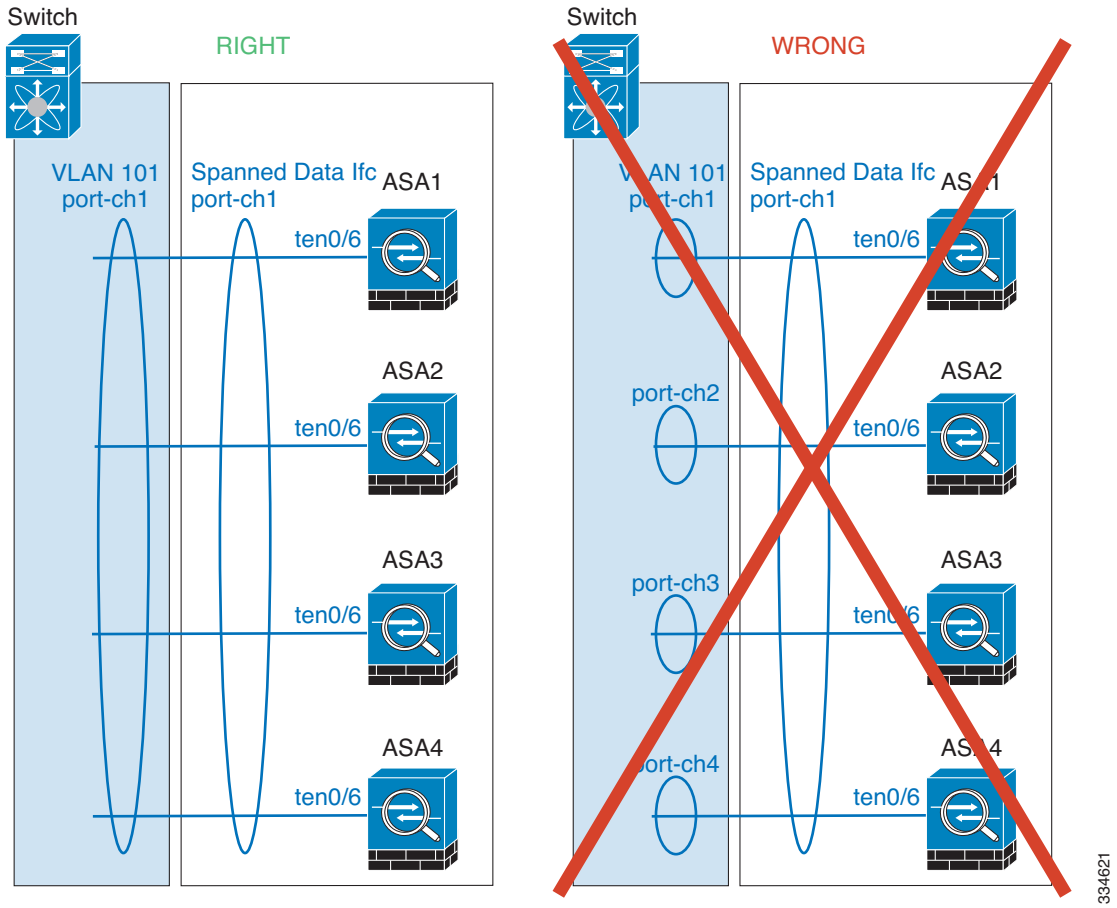
- ASA 5512-X、 ASA 5515-X、 ASA 5525-X、 ASA 5545-X 和 ASA 5555-X

交换机

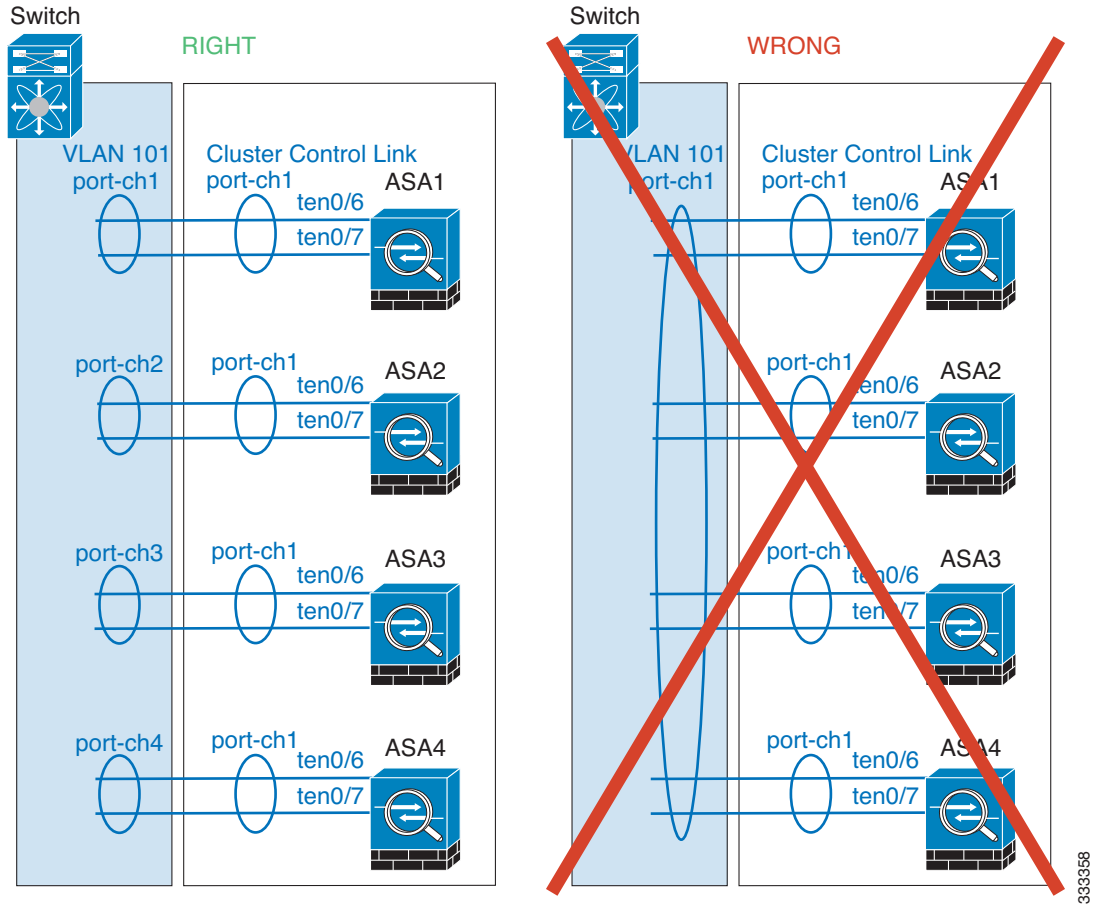
- 在用于集群控制链路接口的交换机上，可以选择在连接到 ASA 的交换机端口上启用生成树 PortFast 来加快新设备加入集群的过程。
- 当交换机上的跨网络 EtherChannel 绑定缓慢时，可以为交换机上的一个独立接口启用快速 LACP 速率。
- 在交换机上，建议使用以下 EtherChannel 负载均衡算法之一：**source-dest-ip** 或 **source-dest-ip-port**（请参阅思科 Nexus OS 和思科 IOS **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中 ASA 的流量分摊不均。*请勿*更改 ASA 上默认的负载均衡算法。
- 如果在交换机上更改 EtherChannel 的负载均衡算法，交换机上的 EtherChannel 接口将暂时停止转发流量，生成树协议重新启动。在流量再次开始传输之前会存在延迟。
- 应该在所有面向集群的 EtherChannel 接口上为思科 Nexus 交换机禁用 LACP Graceful Convergence 功能。
- 有些交换机不支持 LACP 动态端口优先级 （活动链路和备用链路）。您可以禁用动态端口优先级，使跨网络 EtherChannel 具有更高兼容性。
- 集群控制链路路径上的网络要素不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。
- 端口通道绑定中断时间不得超过配置的保持连接间隔。

EtherChannel

- ASA 不支持将 EtherChannel 连接到交换机堆叠。如果跨堆叠连接 ASA EtherChannel，则当主交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。
- 跨网络与 设备本地 EtherChannel 的配置 - 请务必为交换机进行正确的跨网络 EtherChannel 与设备本地 EtherChannel 配置。
  - 跨网络 EtherChannel - 对于跨越所有集群成员的 ASA *跨网络* EtherChannel，所有接口在交换机上合并为一个 EtherChannel。请确保每个接口都属于交换机上的同一个通道组。


Switch
RIGHT
VLAN 101
port-ch1
Spanned Data Ifc
port-ch1
ASA1
ten0/6
ASA2
ten0/6
ASA3
ten0/6
ASA4
ten0/6
Switch
WRONG
Spanned Data Ifc
port-ch1
ASA2
port-ch2
ten0/6
ASA3
port-ch3
ASA4
port-ch4
ten0/6
334621

– 设备本地 EtherChannel - 对于 ASA *设备本地* EtherChannel，包括为集群控制链路配置的任何 EtherChannel，请务必在交换机上配置分散的 EtherChannel；请勿在交换机上将多个 ASA EtherChannel 合并为一个 EtherChannel。



其他指导原则

- 当拓扑结构发生显著更改时（例如添加或删除 EtherChannel 接口，启用或禁用 ASA 或交换机上的接口，添加额外的交换机形成 VSS 或 vPC），应禁用运行状况检查功能。当拓扑结构更改完成且配置更改已同步到所有设备后，可以重新启用运行状况检查功能。
- 将设备添加到现有集群时或重新加载设备时，会有限地暂时丢弃数据包 / 断开连接；这是预期行为。有些时候，丢弃的数据包会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包将使 FTP 客户端挂起。在此情况下，需要重新建立 FTP 连接。
- 如果使用连接到跨网络 EtherChannel 的 Windows 2003 服务器，当系统日志服务器端口关闭且服务器没有限制 ICMP 错误信息时，将会有大量 ICMP 消息被发送回 ASA 集群。这些消息会导致 ASA 集群的某些设备 CPU 使用率极高，进而影响性能。因此，建议限制 ICMP 错误信息。

相关主题

- 第 9-6 页的调整集群控制链路的吞吐量大小
- 第 9-3 页的引导程序配置
- 第 9-22 页的集群不支持的功能
- 第 10-18 页的配置 EtherChannel
- 第 10-10 页的 EtherChannel 准则

ASA 集群的默认设置

- 使用跨网络 EtherChannel 时，将自动生成 cLACP 系统 ID 且系统优先级默认为 1。
- 集群运行状况检查功能默认启用，保持时间为 3 秒。
- 连接再均衡默认禁用。如果启用连接再均衡，交换负载信息的默认间隔时间为 5 秒。

配置 ASA 集群

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

要配置集群，请执行以下任务：

步骤 1　按照第 9-28 页的 ASA 集群的先决条件和第 9-29 页的 ASA 集群的指导原则，在交换机和 ASA 上完成所有预配置。

步骤 2　第 9-33 页的使用电缆连接集群设备并配置上游和下游设备。

步骤 3　第 9-35 页的备份配置 （推荐）。

步骤 4　第 9-35 页的在主设备上配置集群接口模式。只能为集群配置一种类型的接口：跨网络 EtherChannel 或独立接口。

步骤 5　第 9-38 页的 （推荐；在多情景模式中为必须）在主设备上配置接口。如果接口未准备好加入集群，则无法启用集群。在单情景模式中，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中的接口。

步骤 6　第 9-43 页的创建或加入 ASA 集群。

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。配置将被复制到从设备。

使用电缆连接集群设备并配置上游和下游设备

在配置集群之前，需要先使用电缆连接集群控制链路网络、管理网络和数据网络。

注　在配置要加入集群的设备之前，至少需要有一个活动的集群控制链路网络。

此外，还应该配置上游和下游设备。例如，如果使用 EtherChannel，则应为上游和下游设备进行 EtherChannel 配置。

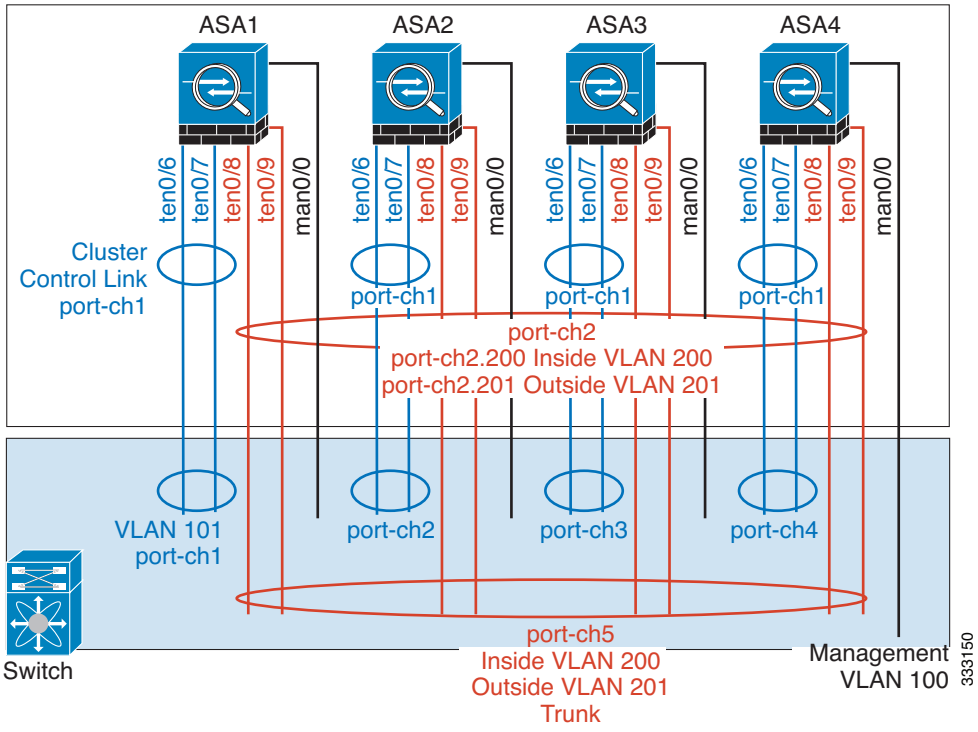
示例

注　本示例使用 EtherChannel 进行负载均衡。如果使用 PBR 或 ECMP，交换机配置会有所不同。

例如，在这 4 台 ASA 5585-X 中，每一台都需要：

- 将设备本地 EtherChannel 中的 2 个万兆以太网接口用于集群控制链路。
- 将跨网络 EtherChannel 中的 2 个万兆以太网接口用于内部和外部网络；每个接口都是 EtherChannel 的 VLAN 子接口。使用子接口可以让内部和外部接口都能充分利用 EtherChannel 的优点。
- 使用 1 个管理接口。

将一台交换机用于内部和外部网络。



用途	逐一连接 4 台 ASA 上的接口	连接到交换机端口
集群控制链路	TenGigabitEthernet 0/6 和 TenGigabitEthernet 0/7	总计 8 个端口 对于每一对 TenGigabitEthernet 0/6 和 TenGigabitEthernet 0/7 接口，配置 4 个 EtherChannel （每台 ASA 1 个 EC）。 这些 EtherChannel 必须全部位于同一个独立的集群控制 VLAN 中，例如 VLAN 101。
内部和外部接口	TenGigabitEthernet 0/8 和 TenGigabitEthernet 0/9	总计 8 个端口 配置一个 EtherChannel （跨所有 ASA）。 现在，在交换机上配置这些 VLAN 和网络；例如配置一个中继，其中 VLAN 200 用于内部而 VLAN 201 用于外部。
管理接口	Management 0/0	总计 4 个端口 将所有接口都放入同一个独立的管理 VLAN 中，例如 VLAN 100。

备份配置 （推荐）

在从设备上启用集群时，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　选择 **Tools > Backup Configurations**。

步骤 2　至少备份正在运行的配置。有关详细的操作步骤，请参阅第 37-22 页的备份本地 CA 服务器。

相关主题

- 第 9-50 页的退出集群

在主设备上配置集群接口模式

只能为集群配置一种类型的接口：跨网络 EtherChannel 或独立接口；不能在集群中混合使用不同的接口类型。

注　如果不从主设备添加从设备，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设备， ASDM 将在从设备上自动设置接口模式。

准备工作

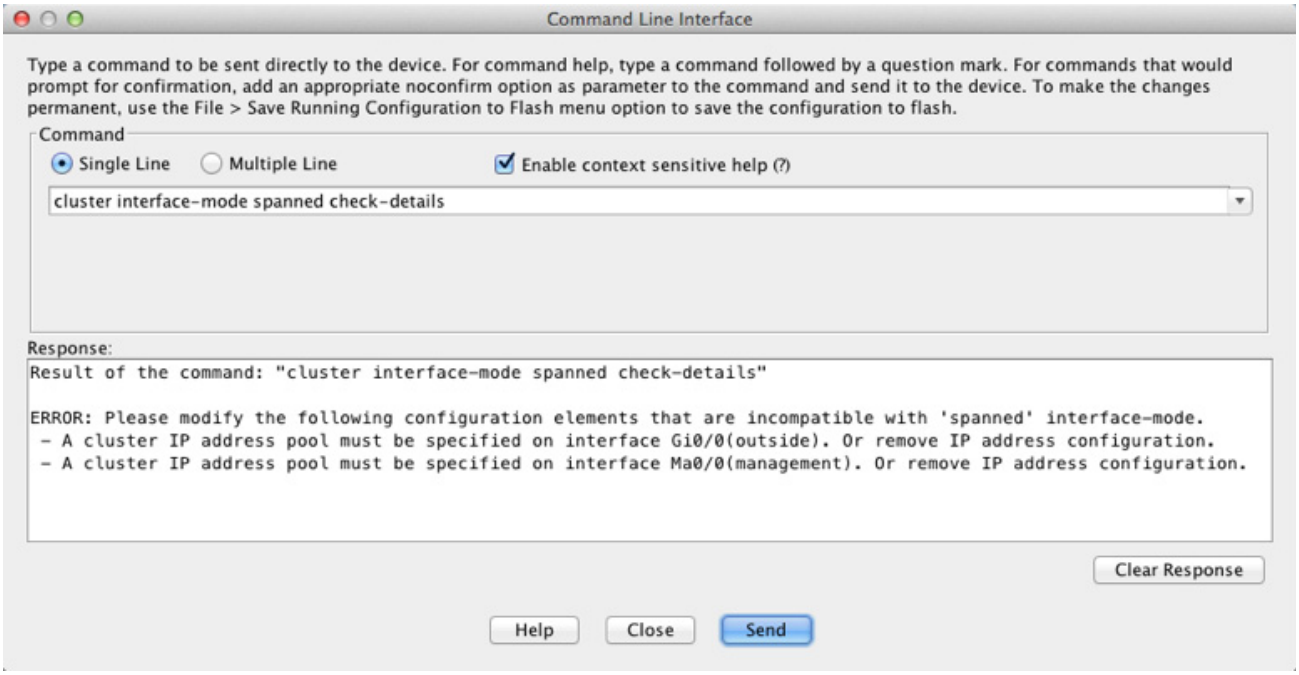
- 您始终可以将管理专用接口配置为独立接口 （推荐），即使是在跨网络 EtherChannel 模式中亦如此。即使是在透明防火墙模式中，管理接口也可以是独立接口。
- 在跨网络 EtherChannel 模式中，如果将管理接口配置为独立接口，将无法为管理接口启用动态路由。您必须使用静态路由。
- 在多情景模式中，必须为所有情景选择一种接口类型。例如，如果使用透明和路由模式的混合情景，则必须将跨网络 EtherChannel 模式用于所有情景，因为这是透明模式允许的唯一接口类型。

操作步骤

步骤 1　在主设备的 ASDM 中，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：

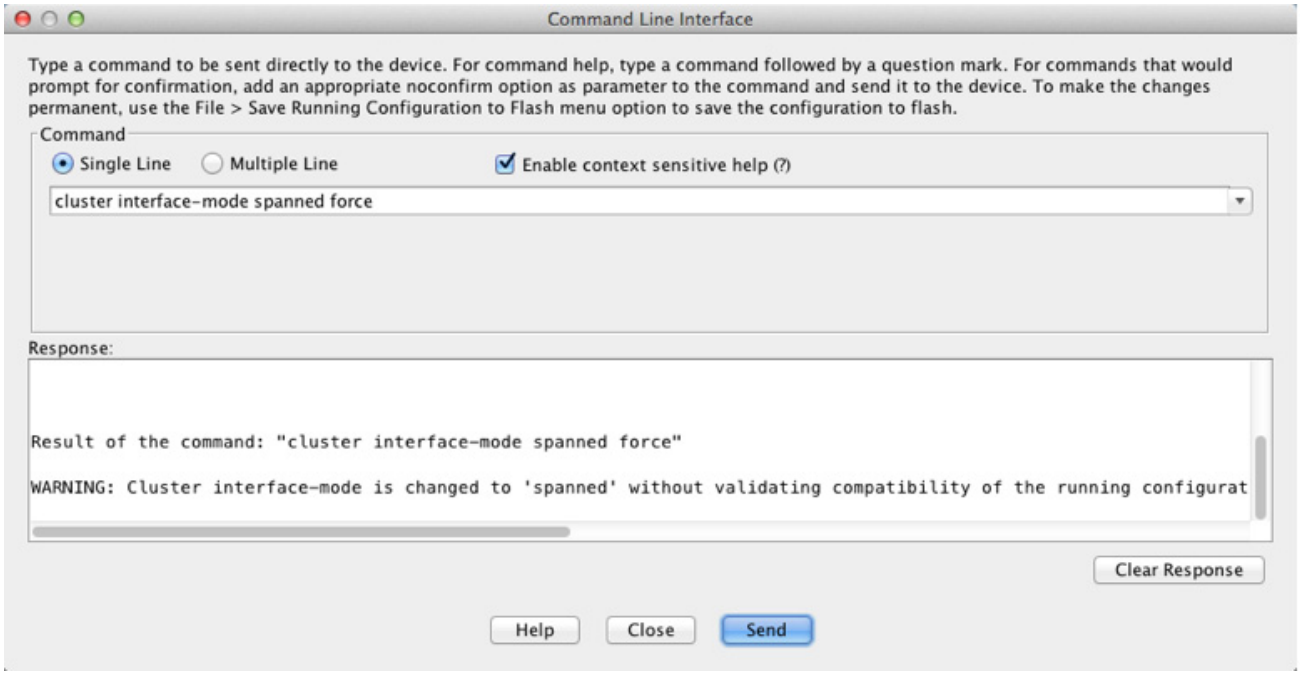


注意事项　设置接口模式之后，可以继续连接到接口；但是，如果您在配置管理接口使其符合集群要求（例如添加集群 IP 池）之前重新加载 ASA，您将无法重新连接，因为与集群不兼容的接口配置已删除。在此情况下，必须连接到控制台端口来修复接口配置。

步骤 2　为集群设置接口模式：

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

示例：



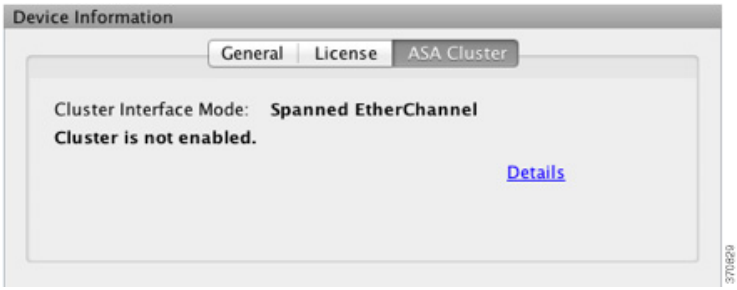
不存在默认设置；您必须明确选择模式。如果尚未设置模式，则无法启用集群。

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，需要手动修复任何配置问题。由于任何接口配置都只能在设置完模式后修复，因此我们建议使用 **force** 选项，这样您至少可以从现有配置着手。设置模式后，可以重新运行 **check-details** 选项来获得更多参考信息。

如果不使用 **force** 选项，当存在任何不兼容的配置时，系统将提示您清除配置并重新加载，从而需要您连接到控制台端口来重新配置管理访问。如果您的配置兼容 （极为罕见），则会更改模式并保留配置。如果不想清除配置，可以键入 **n** 退出命令。

要删除接口模式，请输入 **no cluster interface-mode** 命令。

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

- 第 9-38 页的 （推荐；在多情景模式中为必须）在主设备上配置接口

（推荐；在多情景模式中为必须）在主设备上配置接口

启用集群*之前*，必须修改所有当前配置了 IP 地址的接口，使其准备好加入集群。至少，必须修改 ASDM 当前连接到的管理接口。至于其他接口，可以在启用集群之前或之后配置；我们建议预配置所有接口，以便将完整的配置同步到新的集群成员。在多情景模式中，必须使用本节中的操作步骤修复现有接口或配置新的接口。但是在单情景模式中，您可以跳过本节，在 High Availability and Scalability 向导中配置通用接口参数（请参阅第 9-43 页的创建或加入 ASA 集群）。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。可以将数据接口配置为跨网络 EtherChannel 或独立接口。每种方法使用的负载均衡机制不同。在同一个配置中不能配置两种接口类型，只有管理接口除外，它即使在跨网络 EtherChannel 模式中也可以是独立接口。

- 第 9-38 页的配置独立接口（管理接口的推荐配置）
- 第 9-40 页的配置跨网络 EtherChannel

相关主题

- 第 9-3 页的集群接口

配置独立接口（管理接口的推荐配置）

独立接口是正常的路由接口，每个接口都从 IP 地址池获取自己的 IP 地址。集群的主集群 IP 地址是集群的固定地址，始终属于当前的主设备。

在跨网络 EtherChannel 模式中，建议将管理接口配置为独立接口。独立的管理接口可以根据需要直接连接到每台设备，而跨网络 EtherChannel 接口则只允许连接到当前的主设备。

准备工作

- 除管理专用接口之外，您必须处于独立接口模式中。
- 对于多情景模式，请在每个情景下执行本操作步骤。如果尚未进入情景配置模式，请在 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，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，未来从设备的当前 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　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　选择 **Configuration > Device Setup > 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：

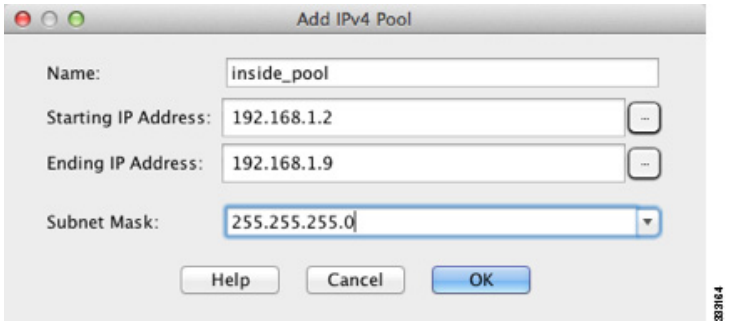
- （对跨网络 EtherChannel 模式中的管理接口为必需项）**Dedicate this interface to management only** - 将一个接口设置为管理专用模式，确保不会有流量流经该接口。默认情况下，管理类型的接口被配置为管理专用。在透明模式中，此命令对管理类型的接口始终启用。
- **Use Static IP** - 不支持 DHCP 和 PPPoE。

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，点击 **IP Address Pool** 字段旁的 **...** 按钮创建集群 IP 池。此时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 **Add**。

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。此地址范围应该对集群的大小而言足够大，例如有 8 个地址。



d. 点击 **OK** 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。

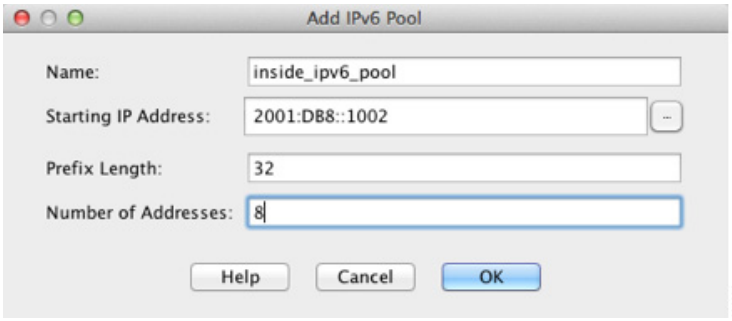
b. 在 **Interface IPv6 Addresses** 区域，点击 **Add**。

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 **Add**。



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** 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** 返回到 Interfaces 窗格。

步骤 6　点击 **Apply**。

相关主题

- 第 9-10 页的管理接口
- 第 9-35 页的在主设备上配置集群接口模式
- 第 9-11 页的负载均衡方法
- 第 10-18 页的配置 EtherChannel
- 第 10-15 页的配置冗余接口
- 第 10-23 页的配置 VLAN 子接口和 802.1Q 中继

配置跨网络 EtherChannel

跨网络 EtherChannel 跨越集群中的所有 ASA，并在 EtherChannel 操作的过程中提供负载均衡。

准备工作

- 必须处于跨网络 EtherChannel 接口模式中。
- 对于多情景模式，请在系统执行空间中开始本操作步骤。如果尚未进入系统配置模式，然后在 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 - 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，建议使用以下算法之一：**source-dest-ip** 或 **source-dest-ip-port**（请参阅思科 Nexus OS 和思科 IOS **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中 ASA 的流量分摊不均。
- 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，请选择 **Configuration > Device Setup > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中选择 **Configuration > Context Management > Interfaces** 窗格。

步骤 2　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挂起状态。 ASDM 不会阻止您添加不匹配的接口。

本操作步骤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键，因为通道组中所有接口的这些参数必须匹配。

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。

  在多情景模式中，如果不同情景之间共享接口，将默认启用自动生成 MAC 地址，因此若要禁用自动生成，只需为共享接口手动设置 MAC 地址即可。请注意，必须为非共享接口手动配置 MAC 地址。如果您还想使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。
- （可选）如果准备将 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达到均衡。

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

注　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。本操作步骤的其余部分适用于子接口。

步骤 7　（多情景模式）完成本操作步骤之前，需要将接口分配到情景。

a. 点击 **OK** 接受所作更改。

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. 选择 **Configuration > Device Setup > 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哪个网桥组。

步骤 10　在 **Interface Name** 字段中输入名称，最长 48 个字符。

步骤 11　在 **Security level** 字段中，输入值为 0（最低）到 100（最高）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，应该为网桥组接口而非 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，应该为网桥组接口而非 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：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** 返回到 **Interfaces** 屏幕。

步骤 15　点击 **Apply**。

相关主题

- 第 9-35 页的在主设备上配置集群接口模式
- 第 13-6 页的配置网桥组
- 第 9-43 页的创建或加入 ASA 集群
- 第 10-18 页的配置 EtherChannel
- 第 10-10 页的 EtherChannel 准则

- 第 9-12 页的连接到 VSS 或 vPC
- 第 10-12 页的启用物理接口并配置以太网参数
- 第 10-23 页的配置 VLAN 子接口和 802.1Q 中继
- 第 7-18 页的配置安全情景
- 第 12-1 页的安全级别
- 第 9-45 页的配置 ASA 集群参数
- 第 9-29 页的 ASA 集群的指导原则

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，然后将从设备添加到该集群。

注　对于主设备，如果要更改 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操作步骤。如果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**。
- 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操作步骤。巨型帧保留需要重新加载 ASA。
- 在连接的交换机上，打算用于集群控制链路接口的接口必须处于打开状态。
- 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　选择 **Wizards > High Availability and Scalability Wizard**。请参阅以下步骤中有关选择向导的指导原则。

步骤 2　在 **Interfaces** 屏幕中，您无法从该屏幕创建新的 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。此参数默认禁用。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。此参数是从主设备复制到从设备的，并非引导程序配置的一部分。

  注　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保持连接消息发送到其他设备。如果设备在保持时间内未收到来自对等设备的任何保持连接消息，则会认为该对等设备没有响应或已损坏。接口运行状况检查将监控链路故障。如果特定设备上的一个接口发生故障，但其他设备上的相同接口处于活动状态，则会从集群中删除该设备。如果一台设备在保留时间内未收到接口状态消息，则 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。

  注　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），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，可以重新启用运行状况检查。

  - **Time to Wait Before Device Considered Failed** - 此值用于确定设备保持连接状态消息的间隔时间，可设置为 .8 到 45 秒；默认值为 3 秒。请注意，保持时间值只影响 *设备*运行状况检查；对于接口运行状况， ASA 使用接口状态 （打开或关闭）。
  - （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。如果将 ASA 保持时间超时设置为比较小的值 （例如 .8 秒），而 ASA 在这些 EtherChannel 接口中的一个接口上发送保持连接消息， ASA 可能会被错误地从集群中删除。启用此选项时， ASA 将在集群控制链路中的所有 EtherChannel 接口上泛洪保持连接消息，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** - 启用从设备到主设备的控制台复制。此功能默认禁用。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。此参数是从主设备复制到从设备的，并非引导程序配置的一部分。
- **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，建议将 MTU 设置为 1600 字节或更大值。如果要使用巨型帧又没有预先启用巨型帧保留，应该先退出向导，启用巨型帧后再重新开始本操作步骤。

步骤 4　点击 **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。

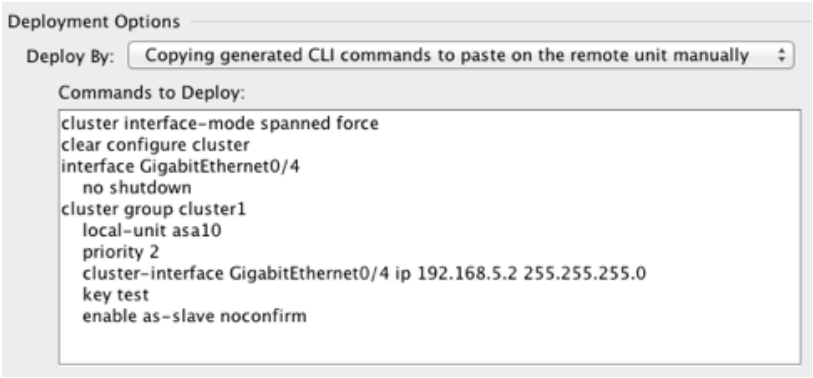
注　在某些情况下，完成向导后加入集群时可能会出现错误。如果 ASDM 断开连接， ASDM 不会收到来自 ASA 的任何后续错误。如果重新连接 ASDM 后集群仍被禁用，应连接到 ASA 控制台端口来确定禁用集群的具体错误情况；例如，集群控制链路可能关闭。

步骤 7　要添加从设备，请点击 **Yes**。

如果从主设备重新运行向导，可在首次启动向导时选择 **Add another member to the cluster** 选项来添加从设备。

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设备的（临时）管理 IP 地址。输入从设备管理 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

- 第 9-45 页的配置 ASA 集群参数
- 第 10-25 页的启用巨型帧支持
- 第 9-40 页的配置跨网络 EtherChannel
- 第 9-38 页的配置独立接口 （管理接口的推荐配置）
- 第 9-8 页的接口监控

管理 ASA 集群成员

部署集群后，可以更改配置和管理集群成员。

- 第 9-45 页的配置 ASA 集群参数
- 第 9-48 页的从主设备添加新的从设备
- 第 9-49 页的成为非活动成员
- 第 9-49 页的从主设备停用从设备成员
- 第 9-50 页的退出集群
- 第 9-51 页的更改主设备
- 第 9-52 页的在集群范围执行命令

配置 ASA 集群参数

如果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，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。本操作步骤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，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操作步骤。如果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　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，该设置将被擦除。在设置完所有参数之前，请勿选中 **Participate in ASA cluster**。

注　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，如要恢复连接，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。每台设备只能配置一个集群。所有集群成员都必须使用同一个名称。
- **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。此参数默认禁用。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。此参数是从主设备复制到从设备的，并非引导程序配置的一部分。
- （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**：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，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保持连接消息发送到其他设备。如果设备在保持时间内未收到来自对等设备的任何保持连接消息，则会认为该对等设备没有响应或已损坏。接口状态消息将检测链路故障。如果特定设备上的一个接口发生故障，但其他设备上的相同接口处于活动状态，则会从集群中删除该设备。如果一台设备在保留时间内未收到接口状态消息，则 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。

注　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），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，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。如果将 ASA 保持时间超时设置为比较小的值 （例如 .8 秒），而 ASA 在这些 EtherChannel 接口中的一个接口上发送保持连接消息， ASA 可能会被错误地从集群中删除。启用此选项时， ASA 将在集群控制链路中的所有 EtherChannel 接口上泛洪保持连接消息，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** - 启用从设备到主设备的控制台复制。此功能默认禁用。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。此参数是从主设备复制到从设备的，并非引导程序配置的一部分。
- **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。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。集群中的 ASA 在 cLACP 协商中协作，使其在交换机看来就好似一台 （虚拟）设备。
  - **Enable static port priority** - 禁用 LACP 中的动态端口优先级。有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。此参数是从主设备复制到从设备的，并非引导程序配置的一部分。
  - **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 需要输入 000C.F142.4CDE。此参数是从主设备复制到从设备的，并非引导程序配置的一部分。但是在启用集群后，您将无法更改此值。
  - **System Priority** - 设置系统优先级，其值为 1 到 65535。此优先级用于确定哪台设备负责作出绑定决定。默认情况下， ASA 使用优先级 1，这是最高优先级。此优先级需要高于交换机上的优先级。此参数是从主设备复制到从设备的，并非引导程序配置的一部分。但是在启用集群后，您将无法更改此值。

步骤 4　选中 **Participate in ASA cluster** 复选框加入集群。

步骤 5　点击 **Apply**。

相关主题

- 第 9-8 页的接口监控
- 第 10-25 页的启用巨型帧支持

从主设备添加新的从设备

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

或者，您也可以选择登录到从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操作步骤。如果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**。
- 如果要通过管理网络发送引导程序配置，请确保从设备有可访问的 IP 地址。

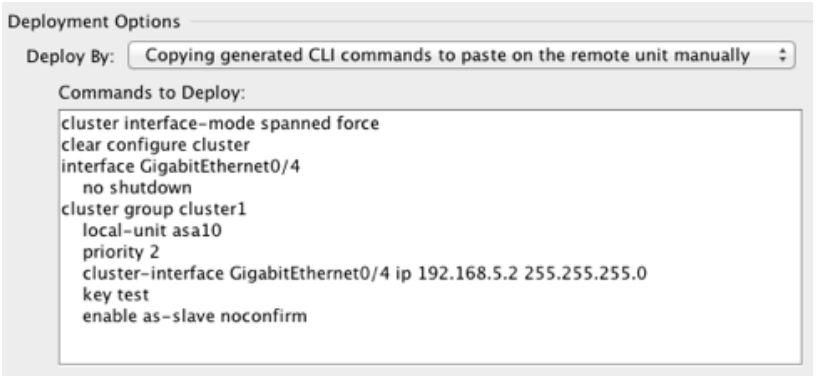
操作步骤

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

步骤 2　点击 **Add**。

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** - 为该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设备的 （临时）管理 IP 地址。输入从设备管理 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

- 第 9-45 页的配置 ASA 集群参数

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。

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操作步骤。如果尚未进入系统配置模式，然后在 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　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　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，如要恢复连接，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

- 第 9-50 页的退出集群

从主设备停用从设备成员

要停用从设备成员，请执行以下步骤。

注　当 ASA 处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。要恢复流量传输，请重新启用集群；或者，您也可以从集群中完全删除该设备。管理接口将保持打开，使用设备从集群 IP 池接收的 IP 地址。但是，如果您重新加载而设备在集群中仍然处于非活动状态，管理接口将无法访问 （因为它届时将使用与主设备相同的主 IP 地址）。您必须使用控制台端口来进行任何进一步配置。

准备工作

对于多情景模式，请在系统执行空间中执行本操作步骤。如果尚未进入系统配置模式，然后在 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　从集群中删除该设备：

```
cluster remove unit unit_name
```

示例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2.To bring it back
to the cluster please logon to that unit and re-enable clustering
```

引导程序配置保持不变，从主设备同步的最新配置也保持不变，因此您可于稍后重新添加该设备而不会丢失配置。如果在从设备上输入此命令删除主设备，将会选举新的主设备。

要查看成员名称，请输入 **cluster remove unit ?**，或输入 **show cluster info** 命令。

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

步骤 2　选择要删除的从设备，然后点击 **Delete**。

从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设备而不会丢失配置。

步骤 3　点击 **Apply**。

相关主题

- 第 9-50 页的退出集群

退出集群

如果要完全退出集群，需要删除整个集群引导程序配置。由于每个成员上的当前配置相同 （从主设备同步），因此退出集群就意味着要么从备份恢复集群前的配置，要么清除现有配置并重新开始配置以免 IP 地址冲突。

准备工作

您必须使用控制台端口；删除集群配置时，所有接口都会关闭，包括管理接口和集群控制链路。

操作步骤

步骤 1　对从设备禁用集群：

```
cluster group cluster_name
no enable
```

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

在从设备上启用集群时，无法进行配置更改。

步骤 2　清除集群配置：

clear configure cluster

ASA 将关闭所有接口，包括管理接口和集群控制链路。

步骤 3　禁用集群接口模式：

no cluster interface-mode

模式并非存储于配置中，因此必须手动重置。

步骤 4　如果有备份配置，可将备份配置复制到正在运行的配置中：

copy *backup_cfg* **running-config**

示例：

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [startup-config]?
ciscoasa(config)#
```

步骤 5　将配置保存到启动配置：

write memory

步骤 6　如果没有备份配置，请重新配置管理访问。例如，确保更改接口 IP 地址，并恢复正确的主机名。

相关主题

- 第 2 章，“入门”

更改主设备

注意事项　要更改主设备，最好的方法是在主设备上禁用集群，等到新的主设备选举后再重新启用集群。如果必须指定要成为主设备的具体设备，请使用本节中的操作步骤。但是请注意，对集中功能而言，如果使用本操作步骤强制更改主设备，则所有连接都将断开，而您必须在新的主设备上重新建立连接。

要更改用主设备，请执行以下步骤。

准备工作

对于多情景模式，请在系统执行空间中执行本操作步骤。如果尚未进入系统配置模式，然后在 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　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

- 第 9-49 页的成为非活动成员
- 第 9-23 页的集群的集中功能

在集群范围执行命令

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，收集所有输出并将其显示在当前设备的控制台上。诸如 **capture** 和 **copy** 之类的其他命令也可以充分利用在集群范围执行的优势。

准备工作

在命令行界面工具中执行本操作步骤：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 ?**（查看除当前设备外的所有名称），或输入 **show cluster info** 命令。

示例

要将相同的捕获文件从集群中所有设备同时复制到 TFTP 服务器，请在主设备上输入以下命令：

```
cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

分别来自每台设备（各一个）的多个 PCAP 文件被复制到 TFTP 服务器。目标捕获文件名会自动附加设备名称，例如 capture1_asa1.pcap、capture1_asa2.pcap 等。在本例中，asa1 和 asa2 是集群设备名称。

以下是 **cluster exec show port-channel summary** 命令的输出示例，显示了集群中每个成员的 EtherChannel 信息：

```
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，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

- 第 3-22 页的 Cluster Dashboard 选项卡
- 第 3-23 页的 Cluster Firewall Dashboard 选项卡

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，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设备上将自动启用此功能。

相关主题

- 第 39-1 页的使用 Packet Capture Wizard 配置和运行捕获

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

- 第 40-19 页的在非 EMBLEM 格式系统日志消息中包含设备 ID

ASA 集群示例

这些示例包括典型部署中所有与集群相关的 ASA 配置。

- 第 9-55 页的 ASA 和交换机配置示例
- 第 9-57 页的单臂防火墙
- 第 9-59 页的流量分离
- 第 9-61 页的包含备用链路 （传统的 8 活动 /8 备用）的跨网络 EtherChannel

ASA 和交换机配置示例

以下配置示例连接 ASA 与交换机之间的下列接口：

ASA 接口	交换机接口
GigabitEthernet 0/2	GigabitEthernet 1/0/15
GigabitEthernet 0/3	GigabitEthernet 1/0/16
GigabitEthernet 0/4	GigabitEthernet 1/0/17
GigabitEthernet 0/5	GigabitEthernet 1/0/18

ASA 配置

每台设备上的接口模式

```
cluster interface-mode spanned force
```

ASA1 主设备引导程序配置

```
interface GigabitEthernet0/0
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit A
 cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
 priority 10
 key emphyri0
 enable noconfirm
```

ASA2 从设备引导程序配置

```
interface GigabitEthernet0/0
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit B
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 11
```

```
 key emphyri0
 enable as-slave
```

主设备接口配置

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

interface GigabitEthernet0/2
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/3
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/4
 channel-group 11 mode active
 no shutdown
!
interface GigabitEthernet0/5
 channel-group 11 mode active
 no shutdown
!
interface Management0/0
 management-only
 nameif management
 ip address 10.53.195.230 cluster-pool mgmt-pool
 security-level 100
 no shutdown
!
interface Port-channel10
 port-channel span-cluster
 mac-address aaaa.bbbb.cccc
 nameif inside
 security-level 100
 ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
 port-channel span-cluster
 mac-address aaaa.dddd.cccc
 nameif outside
 security-level 0
 ip address 209.165.201.1 255.255.255.224
```

思科 IOS 交换机配置

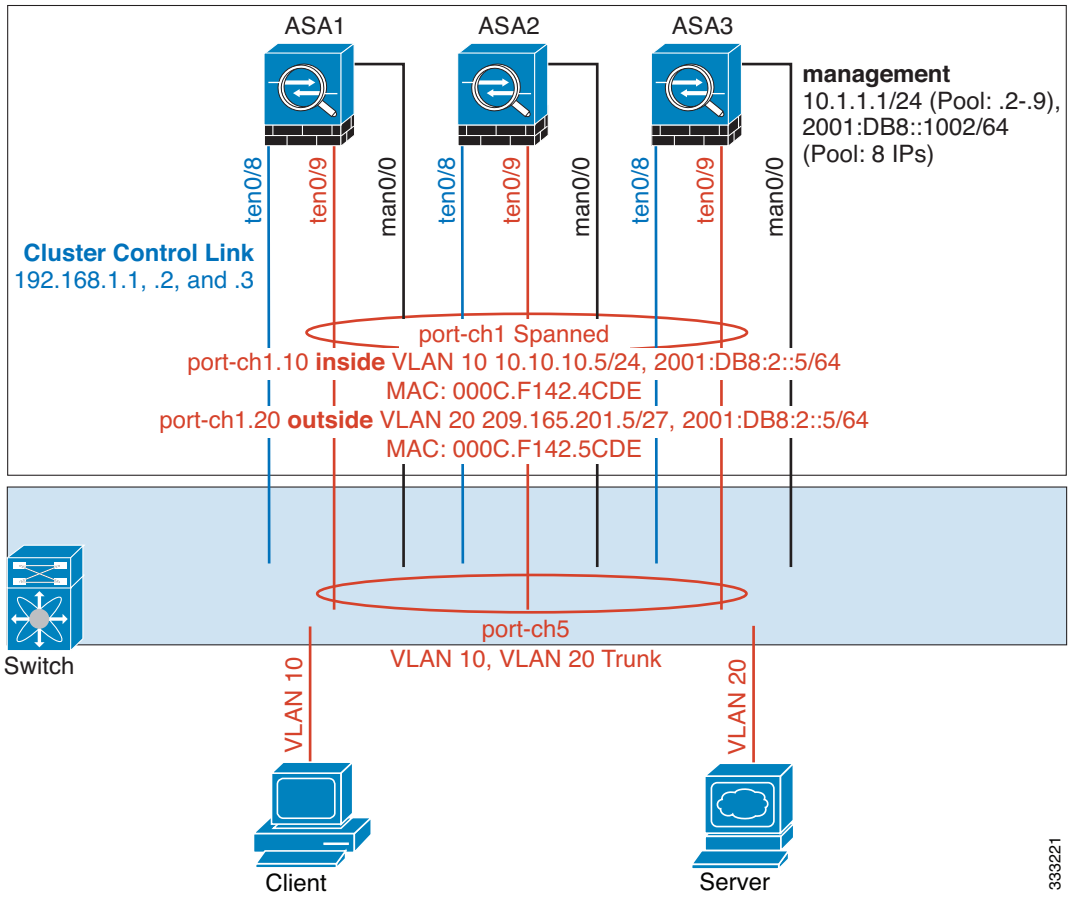
```
interface GigabitEthernet1/0/15
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/16
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/17
 switchport access vlan 401
 switchport mode access
```

```
 spanning-tree portfast
 channel-group 11 mode active
!
interface GigabitEthernet1/0/18
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active

interface Port-channel10
 switchport access vlan 201
 switchport mode access

interface Port-channel11
 switchport access vlan 401
 switchport mode access
```

单臂防火墙



来自不同安全域的数据流量与不同的 VLAN 关联，例如， VLAN 10 用于内部网络而 VLAN 20 用于外部网络。每台 ASA 都有一个连接到外部交换机或路由器的物理端口。启用中继使物理链路上的所有数据包都采用 802.1q 封装。 ASA 是 VLAN 10 与 VLAN 20 之间的防火墙。

使用跨网络 EtherChannel 时，所有数据链路在交换机端分组为一个 EtherChannel。如果一台 ASA 变得不可用，交换机将在其余设备之间再均衡流量。

每台设备上的接口模式

```
cluster interface-mode spanned force
```

ASA1 主设备引导程序配置

```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

cluster group cluster1
    local-unit asa1
    cluster-interface tengigabitethernet0/8 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

ASA2 从设备引导程序配置

```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

cluster group cluster1
    local-unit asa2
    cluster-interface tengigabitethernet0/8 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

ASA3 从设备引导程序配置

```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

cluster group cluster1
    local-unit asa3
    cluster-interface tengigabitethernet0/8 ip 192.168.1.3 255.255.255.0
    priority 3
    key chuntheunavoidable
    enable as-slave
```

主设备接口配置

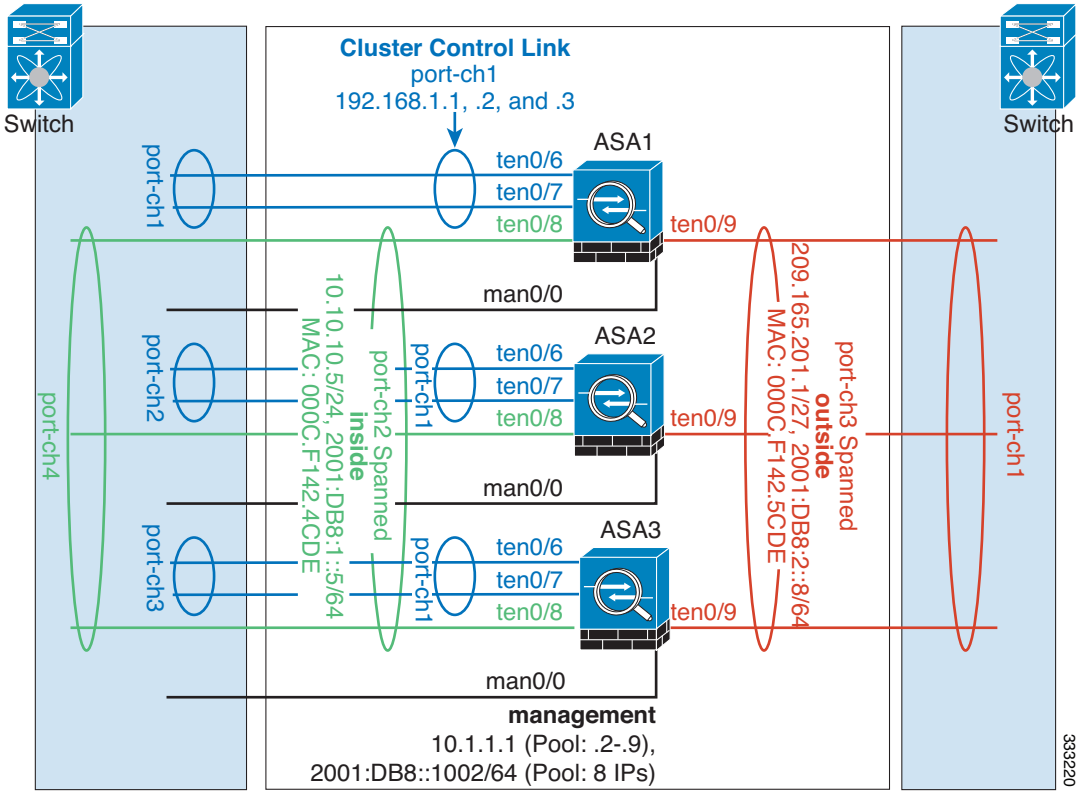
```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown

interface tengigabitethernet 0/9
    channel-group 2 mode active
```

```
    no shutdown
interface port-channel 2
    port-channel span-cluster
interface port-channel 2.10
    vlan 10
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    ipv6 address 2001:DB8:1::5/64
    mac-address 000C.F142.4CDE
interface port-channel 2.20
    vlan 20
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    ipv6 address 2001:DB8:2::8/64
    mac-address 000C.F142.5CDE
```

流量分离



您可能更愿意在内部和外部网络之间采用物理方式分离流量。

如上图所示，左侧有一个跨网络 EtherChannel 连接到内部交换机，而右侧的另一个跨网络 EtherChannel 连接到外部交换机。如果需要，您还可以在每个 EtherChannel 上创建 VLAN 子接口。

每台设备上的接口模式

```
cluster interface-mode spanned force
```

ASA1 主设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

ASA2 从设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

ASA3 从设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa3
    cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
    priority 3
    key chuntheunavoidable
    enable as-slave
```

主设备接口配置

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
```

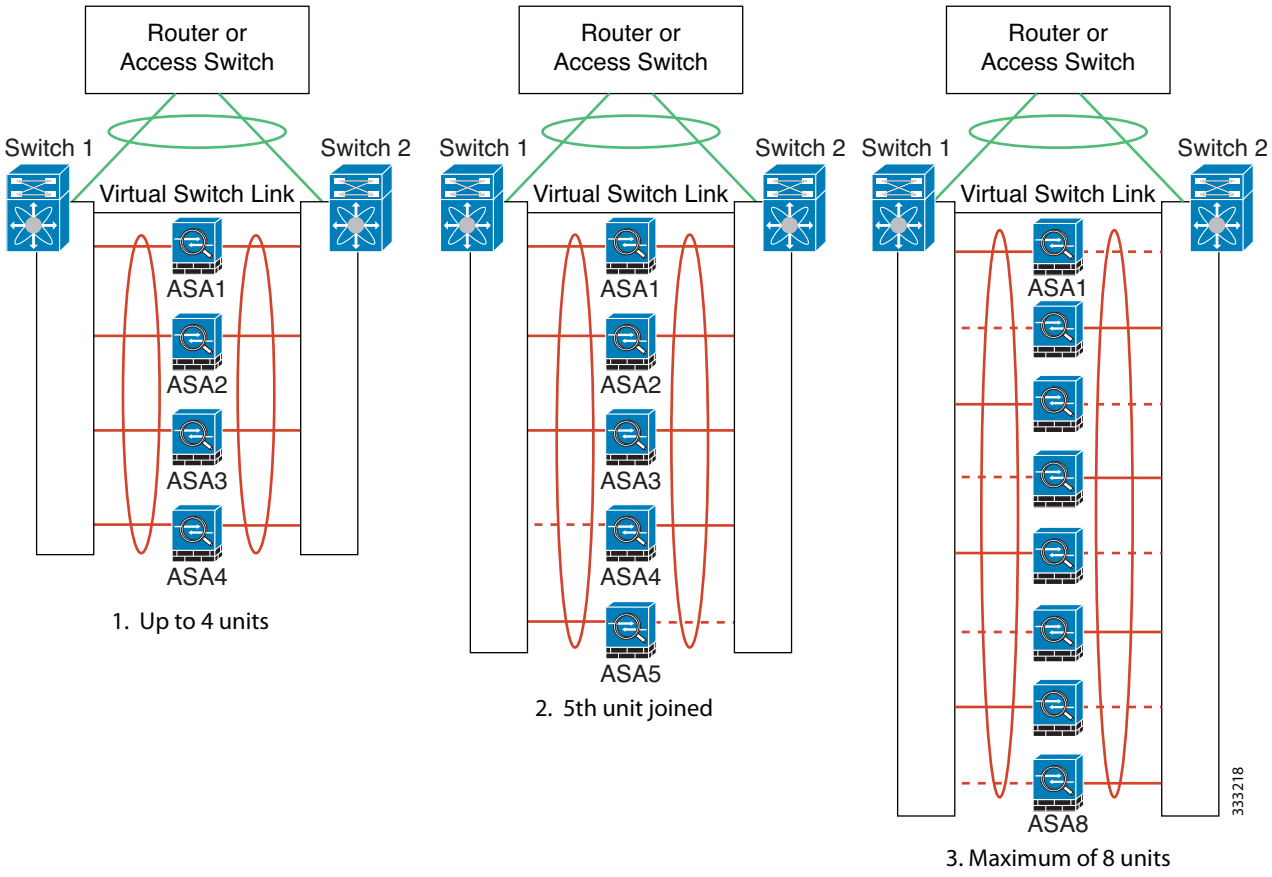
```
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown

interface tengigabitethernet 0/8
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    port-channel span-cluster
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    ipv6 address 2001:DB8:1::5/64
    mac-address 000C.F142.4CDE

interface tengigabitethernet 0/9
    channel-group 3 mode active
    no shutdown
interface port-channel 3
    port-channel span-cluster
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    ipv6 address 2001:DB8:2::8/64
    mac-address 000C.F142.5CDE
```

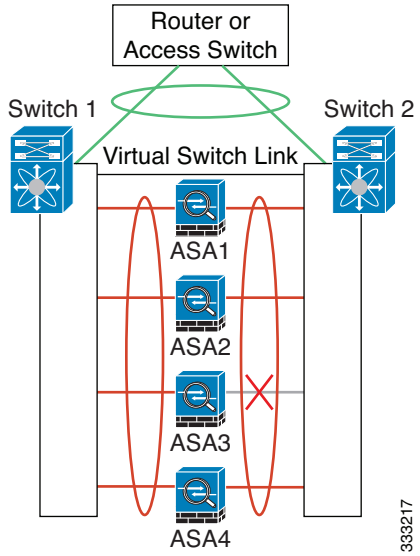
包含备用链路 （传统的 8 活动 /8 备用）的跨网络 EtherChannel

在传统的 EtherChannel 中，最大活动端口数限制为 8 个来自交换机端的端口。如果您在 8-ASA 集群中将每台设备的 2 个端口分配到 EtherChannel，总计 16 个端口，则其中 8 个端口必须处于备用模式。 ASA 使用 LACP 来协商哪些链路应为活动链路，哪些应为备用链路。如果使用 VSS 或 vPC 启用多交换机 EtherChannel，则可实现交换机间冗余。在 ASA 上，所有物理端口将先按插槽号、后按端口号排序。在下图中，排序较低的端口是 “ 主要 ” 端口 （例如 GigabitEthernet 0/0），另一个是 “ 辅助 ” 端口 （例如 GigabitEthernet 0/1）。您必须保证硬件连接对称：如果使用 VSS/vPC，所有主要链路必须在一台交换机上终止，所有辅助链路必须在另一台交换机上终止。下图显示了当更多设备加入集群导致链路总数增加时会发生什么情况：

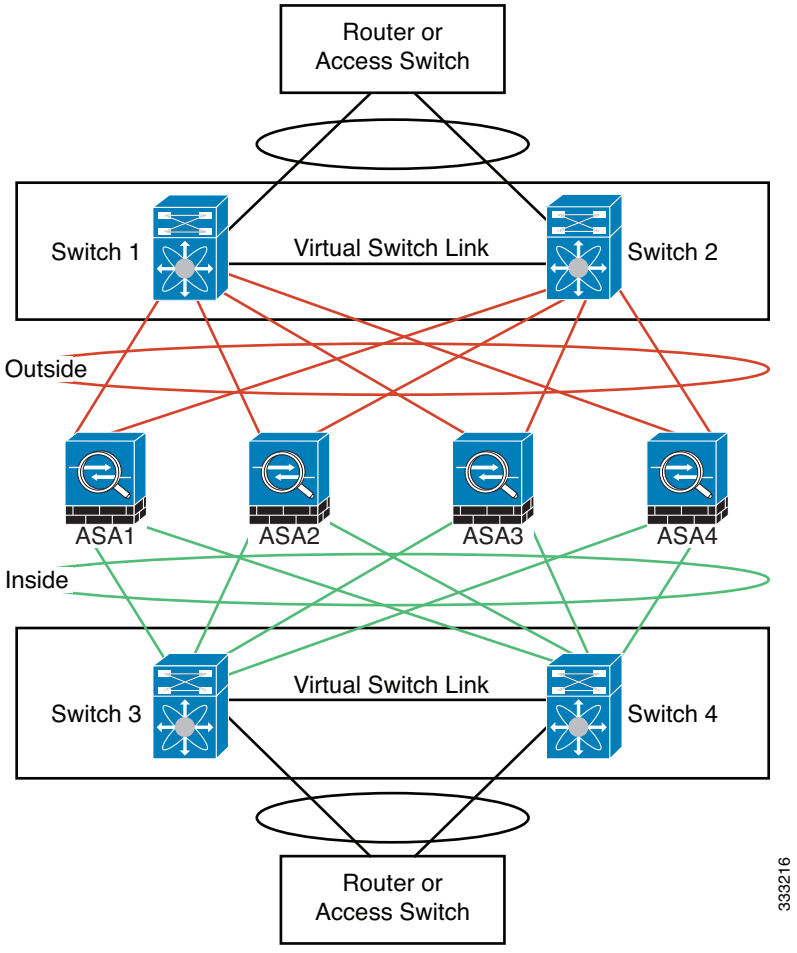


此时的处理原则是，首先将通道中的活动端口数增加到最大值，其次是保持活动的主要端口数与活动的辅助端口数之间的均衡。请注意，当第 5 台设备加入集群时，流量并未在所有设备之间达到均衡。

处理链路或设备故障时也遵循相同的原则。最终的负载均衡状况可能并不尽如人意。下图所示为 4 台设备组成的集群，其中一台设备上有一个链路发生故障。



该网络中可能配置了多个 EtherChannel。下图所示为一个内部 EtherChannel 和一个外部 EtherChannel。如果 EtherChannel 中的主要链路和辅助链路都发生故障，则会从集群中删除 ASA。这可以防止 ASA 在已经与内部网络断开连接的情况下收到来自外部网络的流量。



每台设备上的接口模式

```
cluster interface-mode spanned force
```

ASA1 主设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

ASA2 从设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

ASA3 从设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
```

```
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa3
    cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
    priority 3
    key chuntheunavoidable
    enable as-slave
```

ASA4 从设备引导程序配置

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa4
    cluster-interface port-channel1 ip 192.168.1.4 255.255.255.0
    priority 4
    key chuntheunavoidable
    enable as-slave
```

主设备接口配置

```
ip local pool mgmt 10.1.1.2-10.1.1.9

interface management 0/0
    channel-group 2 mode active
    no shutdown
interface management 0/1
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    security-level 100
    management-only

interface tengigabitethernet 1/6
    channel-group 3 mode active vss-id 1
    no shutdown
interface tengigabitethernet 1/7
    channel-group 3 mode active vss-id 2
    no shutdown
interface port-channel 3
    port-channel span-cluster vss-load-balance
```

```
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    mac-address 000C.F142.4CDE

interface tengigabitethernet 1/8
    channel-group 4 mode active vss-id 1
    no shutdown
interface tengigabitethernet 1/9
    channel-group 4 mode active vss-id 2
    no shutdown
interface port-channel 4
    port-channel span-cluster vss-load-balance
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    mac-address 000C.F142.5CDE
```

ASA 集群的历史记录

功能名称	平台版本	功能信息
ASA 5580 和 5585-X 的 ASA 集群	9.0(1)	通过 ASA 集群，可以将多台 ASA 组合成一个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。 ASA 5580 和 ASA 5585-X 支持 ASA 集群；集群中的所有设备必须为相同型号且硬件规格相同。有关启用集群时不支持的功能列表，请参阅配置指南。 我们引入或修改了以下屏幕： 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 > Interfaces > Add/Edit Interface > Advanced Configuration > Device Setup > Interfaces > Add/Edit Interface > IPv6 Configuration > Device Setup > 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。 我们未修改任何 ASDM 屏幕。

功能名称	平台版本	功能信息
提高了 VSS 和 vPC 对运行状况检查监控的支持	9.1(4)	如果将集群控制链路配置为 EtherChannel（推荐），而且链路连接到 VSS 或 vPC 对，则现在可提高运行状况检查监控的稳定性。对某些交换机（例如思科 Nexus 5000）而言，当 VSS/vPC 中的一台设备正在关闭或启动时，连接到这些交换机的 EtherChannel 成员接口可能看似对 ASA 打开，但在交换机端却并未传输流量。如果将 ASA 保持时间超时设置为比较小的值（例如 .8 秒），而 ASA 在这些 EtherChannel 接口中的一个接口上发送保持连接消息，ASA 可能会被错误地从集群中删除。启用 VSS/vPC 运行状况检查功能时， ASA 将在集群控制链路中的所有 EtherChannel 接口上泛洪保持连接消息，以确保至少有一台交换机可以收到这些消息。 我们修改了以下屏幕：**Configuration > Device Management > High Availability and Scalability > ASA Cluster**
支持集群成员位于不同的地理位置（站点间）；仅限独立接口模式	9.1(4)	使用独立接口模式时，集群成员现在可位于不同的地理位置。 我们未修改任何 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)	在透明防火墙模式中使用跨网络 EtherChannel 模式时，集群成员现在可位于不同的地理位置。不支持在路由防火墙模式中使用跨网络 EtherChannel 的站点间集群。 我们未修改任何 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。您还应该遵循以下指导原则： • 集群控制链路路径上的网络要素不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。 • 端口通道绑定中断时间不得超过配置的保持连接间隔。 我们修改了以下屏幕：**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，现在可以在跨网络 EtherChannel 中配置 16 条活动链路（每台交换机各连接 8 条）。以前，即便使用 VSS/vPC，跨网络 EtherChannel 也只支持 8 条活动链路和 8 条备用链路。 **注**　如果要在跨网络 EtherChannel 中使用 8 条以上的活动链路，则无法同时拥有备用链路；支持 9 到 32 条活动链路需要禁用允许使用备用 链路的 cLACP 动态端口优先级。 我们修改了以下屏幕：**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。 我们未修改任何 ASDM 屏幕。
ASA 集群的 BGP 支持	9.3(1)	我们增加了对 BGP 用于 ASA 集群的支持。 我们修改了以下 ASDM 屏幕：**Configuration > Device Setup > Routing > BGP > IPv4 Family > General**

第 3 部分

接口

基本接口配置 （ASA 5512-X 及更高版本）

本章介绍启动思科 ASA 5512-X 及更高版本接口配置的任务，包括配置以太网设置、冗余接口和 EtherChannel。

注 在多情景模式中，请在系统执行空间中完成本节所述的所有任务。如果尚未在系统执行空间中，请在 Configuration > Device List 窗格中，双击主用设备 IP 地址下方的 **System**。

有关具有特殊要求的 ASA 集群接口，请参阅第 9 章，“ASA 集群 ”

有关启动 ASA 5512-X 及更高版本接口配置的信息

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。要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。对于千兆以太网，当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此， Auto-MDI/MDIX 始终会启用，且您无法禁用它。

处于透明模式中的接口

处于透明模式中的接口属于 “ 网桥组 ”，每个网络都有一个网桥组。 4 个接口最多可以有 8 个网桥组，每个情境或单一模式中有一个。有关网桥组的详细信息，请参阅第 13-1 页的透明模式的网桥组。

管理接口

管理接口概述

可以通过连接到以下接口来管理 ASA：

- 任何直通流量接口
- 专用的管理*插槽 / 端口*接口 （如果适用于所用的型号）

可能需要按照第 36 章，“ 管理访问 ” 中所述配置对接口的管理访问。

管理*插槽 / 端口*界面

表 10-1 显示了每个型号的管理接口。

表 10-1　　每个型号的管理接口

型号	Management 0/0[1]	Management 0/1	Management 1/0	Management 1/1	可针对直通流量进行配置[2]	允许子接口
ASA 5512-X	是	否	否	否	否	否
ASA 5515-X	是	否	否	否	否	否
ASA 5525-X	是	否	否	否	否	否
ASA 5545-X	是	否	否	否	否	否
ASA 5555-X	是	否	否	否	否	否

表 10-1　每个型号的管理接口 （续）

型号	Management 0/0[1]	Management 0/1	Management 1/0	Management 1/1	可针对直通流量进行配置[2]	允许子接口
ASA 5585-X	是	是	是[3]	是[3]	是	是
ASASM	否	否	否	否	不适用	不适用
ASAv	是	否	否	否	否	否

1. 作为默认出厂配置的一部分，已配置了用于 ASDM 访问的 Management 0/0 接口。有关详细信息，请参阅第 2-14 页的出厂默认配置。
2. 默认情况下， Management 0/0 接口配置为用于管理流量。对于处于路由模式中的受支持型号，可以取消这一限制并传递直通流量。如果型号包含其他管理接口，还可以将这些接口用于直通流量。但是，管理接口可能不会进行直通流量方面的优化。
3. 如果在插槽 1 中安装了 SSP，则管理 1/0 接口和管理 1/1 接口仅在插槽 1 中提供对 SSP 的管理访问。

注　如果安装了一个模块，该模块的管理接口仅提供对该模块的管理访问。对于 ASA 5512-X 到 ASA 5555-X，该软件模块将同一个物理 Management 0/0 接口用作 ASA。

将任何接口用于仅管理流量

若想将任何接口 （包括 EtherChannel 接口）用作管理专用接口，只需将该接口配置为用于管理流量。

用于透明模式的管理接口

在透明防火墙模式中，除了允许的最大数量范围内的直通流量接口，还可以将管理接口 （物理接口、子接口[如果所用的型号支持]或由管理接口组成的 EtherChannel 接口 [如果有多个管理接口]）用作单独的管理接口。不能将任何其他接口类型用作管理接口。

在多情景模式中，无法在情景之间共享任何接口，包括管理接口。要为每个情景提供管理，可创建管理接口的子接口，然后向每个情景分配管理子接口。请注意，从 ASA 5512-X 到 ASA 5555-X 都不允许管理接口上有子接口，因此，对于每个情景管理，必须连接到数据接口。

管理接口不属于普通网桥组的一部分。请注意，出于操作目的，管理接口属于不可配置网桥组的一部分。

注　在透明防火墙模式中，管理接口以与数据接口相同的方式更新 MAC 地址表；因此，不应将管理和数据接口连接到同一个交换机，除非将其中一个交换机端口配置为路由端口 （默认情况下，Catalyst 交换机在所有的 VLAN 交换机端口上共享一个 MAC 地址）。否则，如果流量从物理连接的交换机到达管理接口， ASA 会更新 MAC 地址表，以使用 *管理*接口 （而不是数据接口）来访问交换机。此操作会导致临时流量中断；出于安全原因， ASA 至少在 30 秒内不会再次更新从交换机到数据接口的数据包 MAC 地址表。

不支持冗余管理接口

冗余接口不支持作为成员的管理 *插槽 / 端口*接口。也不能将组成非管理接口的冗余接口设置为管理专属接口。

ASA 5512-X 到 ASA 5555-X 上的 Management 0/0 接口

ASA 5512-X 到 ASA 5555-X 上的 Management 0/0 接口具有以下特征：

- 不支持直通流量
- 不支持子接口
- 不支持优先级队列
- 不支持组播 MAC
- 软件模块共享 Management 0/0 接口。 ASA 和模块支持单独的 MAC 地址和 IP 地址。必须在模块操作系统中执行模块 IP 地址的配置。但是，物理特性 （例如启用接口）在 ASA 上进行配置。

冗余接口

一个逻辑冗余接口包括一对物理接口：主用和备用接口。如果主用接口发生故障，备用接口将激活并开始传输流量。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转移，如果需要，可以配置冗余接口和设备级故障转移。

冗余接口 MAC 地址

冗余接口使用您添加的第一个物理接口的 MAC 地址。如果在配置中更改成员接口的顺序，则 MAC 地址发生更改，以匹配现第一个列出的接口的 MAC 地址。或者，无论成员接口 MAC 地址如何，均可以将 MAC 址址分配给冗余接口（请参阅第 12-10 页的配置 MAC 地址、MTU 和 TCP MSS 或第 7-14 页的配置多情景）。如果主用接口故障转移到备用接口，系统将维护同一 MAC 地址，以防流量中断。

EtherChannel

802.3ad EtherChannel 是逻辑接口 （称为端口通道接口），该接口由一组单独的以太网链路 （通道组）组成，使得可以提高单个网络的带宽。配置接口相关功能时，可以像使用物理接口一样来使用端口通道接口。

最多可配置 48 个 EtherChannel。

通道组接口

每个通道组最多可以有 16 个主用接口。对于仅支持 8 个主用接口的交换机，最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。对于 16 个主用接口，请确保交换机支持此功能 （例如，带有 F2 系列 10 千兆以太网模块的思科 Nexus 7000 支持此功能）。

通道组中的所有接口必须具有相同的类型和速度。添加到通道组中的第一个接口确定正确的类型和速度。

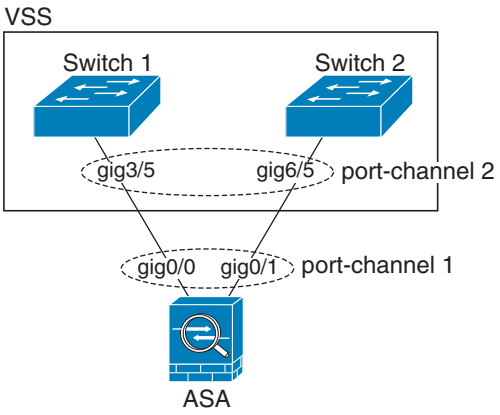
EtherChannel 汇聚信道中所有可用活动接口上的流量。会根据源或目标 MAC 地址、 IP 地址、TCP 端口号、 UDP 端口号和 VLAN 编号，使用专有的哈希算法来选择接口。

连接到另一台设备上的 EtherChannel

连接 ASA EtherChannel 的设备必须同时支持 802.3ad EtherChannel ； 例如，可以连接到 Catalyst 6500 交换机或思科 Nexus 7000。

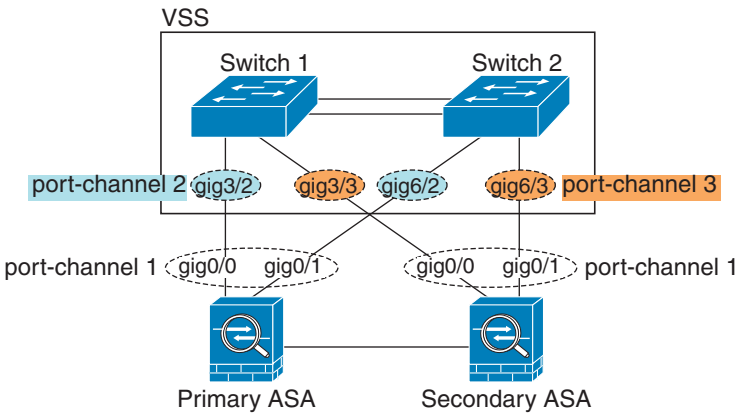
如果交换机属于虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 的一部分，可以在同一个 EtherChannel 内的 ASA 接口连接到 VSS/vPC 中单独交换机。交换机接口属于同一个 EtherChannel 端口通道接口的成员，因为单独交换机的作用方式类似于单个交换机 （请参阅图 10-1）。

图 10-1　　连接到 VSS/vPC



如果在主用 / 备用故障转移部署中使用 ASA，需要在 VSS/vPC 中的交换机上创建单独的 EtherChannel - 为每个 ASA 创建一个 （请参阅图 10-1）。在每个 ASA 上，可以将一个 EtherChannel 连接到两台交换机。即使您可以将所有的交换机接口分组到连接两个 ASA 的一个 EtherChannel 中 （在这种情况下，将不会建立 EtherChannel，因为 ASA 系统 ID 是单独的），并不需要单个 EtherChannel，因为您不希望将流量发送到备用 ASA。

图 10-2　　主用 / 备用故障转移和 VSS/vPC



链路聚合控制协议

链路聚合控制协议 (LACP) 通过在两个网络设备之间交换链路聚合控制协议数据单元 (LACPDU) 来聚合接口。

可以在 EtherChannel 中将每个物理接口配置为：

- Active - 发送并接收 LACP 更新。活动 EtherChannel 可与活动或被动 EtherChannel 建立连接。应使用活动模式，除非需要尽可能减少 LACP 流量。
- Passive - 接收 LACP 更新。被动 EtherChannel 只能与活动 EtherChannel 建立连接。
- On - EtherChannel 始终开启， LACP 未使用。“ 开启 ” 的 EtherChannel 只能与另一个 “ 开启 ” 的 EtherChannel 建立连接。

在没有用户干预的情况下，LACP 会协调对于指向 EtherChannel 的链路的自动添加和删除。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。如果接口发生故障且未检查连接和配置，“ 开启 ” 模式将不能使用通道组中的备用接口。

负载均衡

ASA 通过对数据包的源 IP 地址和目标 IP 地址进行哈希处理，来向 EtherChannel 的接口中分发数据包 （此条件可配置；请参阅第 10-20 页的自定义 EtherChannel）。在取模运算中用得出的哈希值除以活动链路数量，这样得出的余数将确定哪个接口拥有流量。 *hash_value* **mod** *active_links* 结果为 0 的所有数据包将转至 EtherChannel 中的第一个接口，结果为 1 的数据包将转至第二个接口，结果为 2 的数据包将转至第三个接口，依此类推。例如，如果有 15 个活动链路，取模运算将提供 0 到 14 的值。如果有 6 个活动链路，则值为 0 到 5，依此类推。

对于集群中的跨网络 EtherChannel，会逐个 ASA 进行负载均衡。例如，如果 8 个 ASA 之间的跨网络 EtherChannel 中有 32 个主用接口，EtherChannel 中的每个 ASA 有 4 个接口，则仅会在 ASA 上的 4 个接口之间进行负载均衡。

如果主用接口发生故障且不能由备用接口替代，则流量会在剩余的链路之间重新平衡。该故障将会在第 2 层的生成树和第 3 层的路由表中被屏蔽，因此，故障恢复对其他网络设备是透明的。

EtherChannel MAC 地址

属于通道组一部分的所有接口共享同一个 MAC 地址。该功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；他们不知道单个链路。

端口通道接口使用编号最小的通道组接口 MAC 地址作为端口通道 MAC 地址。或者，您可以为端口通道接口手动配置 MAC 地址。在多情景模式中，可将唯一 MAC 地址自动分配给各个接口，包括 EtherChannel 端口接口。在组通道接口成员资格发生变化的情况下，我们建议手动或 （在多情景模式中）自动配置唯一的 MAC 地址。如果移除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址更改至下一个编号最小的接口，从而导致流量中断。

用最大传输单元、 TCP 最大分段大小控制分片

MTU 概述

最大传输单元 (MTU) 指定 ASA 可在给定以太网接口上传输的最大帧负载大小。MTU 值是*没有*以太网报头、FCS 或 VLAN 标记的帧大小。以太网报头为 14 字节，而 FCS 为 4 字节。如果将 MTU 设置为 1500，预期的帧大小 （包括报头）为 1518 字节。如果使用 VLAN 标记 （这样将会增加额外 4 字节），并将 MTU 设置为 1500，预期的帧大小为 1522。请勿为容纳这些报头而将 MTU 的值设得过高。要调整 TCP 报头以便进行封装，请勿更改 MTU 设置，而是应该更改 TCP 最大分段大小 （第 10-7 页的 TCP 最大分段大小概述）。

如果传出的 IP 数据包大于指定 MTU，该数据包会分片成 2 个或更多个帧。片段在目标处 （有时在中间跃点处）重组，而分片可能会导致性能下降。因此， IP 数据包大小应在 MTU 大小范围内，以避免分片。

注　只要有内存空间， ASA 就可接收大于所配置的 MTU 的帧。有关如何增加内存以接收较大的帧，请参阅第 10-25 页的启用巨型帧支持。

默认 MTU

ASA 上的默认 MTU 为 1500 字节。此值不包括以太网报头、CRC、VLAN 标记等的 18 个或更多字节。

路径 MTU 发现

ASA 支持路径 MTU 发现 （如 RFC 1191 中所定义），从而使两个主机之间的网络路径中的所有设备均可协调 MTU，以便它们可以标准化路径中的最低 MTU。

设置 MTU 和巨型帧

请参阅第 12-10 页的配置 MAC 地址、MTU 和 TCP MSS。对于多情景模式，请在每个情景中设置 MTU。

请参阅第 10-25 页的启用巨型帧支持。对于多情景模式，请在系统执行空间中设置巨型帧支持。

请参阅以下准则：

- 与流量路径上的 MTU 相匹配 - 我们建议将所有 ASA 接口以及流量路径的其他设备接口上的 MTU 设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 适应巨型帧 - 如果启用巨型帧，最多可以将 MTU 设置为 9198 字节。

TCP 最大分段大小概述

TCP 最大分段尺寸 (TCP MSS) 是 TCP 负载在添加任何 TCP 报头*之前*的大小。UDP 数据包不会受到影响。建立连接时，客户端和服务器会在三次握手期间交换 TCP MSS 值。

可以在 ASA 上设置 TCP MSS。如果一个连接的任意终端要求 TCP MSS 的值大于 ASA 上设置的值，则 ASA 将用 ASA 最大值覆盖请求数据包内的 TCP MSS。如果主机或服务器不请求 TCP MSS，则 ASA 会假设 RFC 793 的默认值为 536 字节，但不会修改数据包。您还可以配置最小 TCP MSS ；如果主机或服务器请求一个非常小的 TCP MSS，则 ASA 可将该值调高。默认情况下，最小 TCP MSS 未启用。

例如，可以将默认 MTU 配置为 1500 字节。主机请求 1700 的 MSS。如果 ASA 的最大 TCP MSS 是 1380，ASA 会将 TCP 请求数据包中的 MSS 值更改为 1380。然后，服务器会发送 1380 字节的数据包。

默认 TCP MSS

默认情况下，ASA 上的最大 TCP MSS 是 1380 字节。此默认值符合 VPN 连接的要求（在 VPN 连接中，报头最多可增加 120 字节）；此值在默认 MTU （1500 字节）范围内。

设置 VPN 和非 VPN 流量的 TCP MSS

请参阅第 12-10 页的配置 MAC 地址、MTU 和 TCP MSS。对于多情景模式，请在每个情景中设置 TCP MSS。

请参阅以下准则：

- 非 VPN 流量 - 如果不使用 VPN 且不需要额外的报头空间，应该禁用 TCP MSS 限制并接受连接终端之间建立的值。由于连接终端一般是从 MTU 获得 TCP MSS，因此，非 VPN 数据包通常符合此 TCP MSS。
- VPN 流量 - 将最大 TCP MSS 设置为 MTU - 120。例如，如果使用巨型帧并将 MTU 设置为较大的值，需要将 TCP MSS 设置为符合新的 MTU。

ASA 5512-X 及更高版本接口的许可要求

型号	许可证要求
ASA 5512-X	VLAN： 基础许可证：50 增强型安全许可证：100 所有类型的接口： 基础许可证：716 增强型安全许可证：916
ASA 5515-X	VLAN： 基础许可证：100 所有类型的接口： 基础许可证：916
ASA 5525-X	VLAN： 基础许可证：200 所有类型的接口： 基础许可证：1316
ASA 5545-X	VLAN： 基础许可证：300 所有类型的接口： 基础许可证：1716

型号	许可证要求
ASA 5555-X	VLAN： 基础许可证：500 所有类型的接口： 基础许可证：2516
ASA 5585-X	VLAN： 基础许可证和增强型安全许可证：1024 SSP-10 和 SSP-20 的接口速度： 基础许可证 - 适用于光纤接口的 1 千兆以太网 10 GE I/O 许可证 （增强型安全许可证） - 适用于光纤接口的 10 千兆以太网 （默认情况下， SSP-40 和 SSP-60 支持 10 千兆以太网。） 所有类型的接口： 基础许可证和增强型安全许可证：4612

注　对于根据 VLAN 限制计数的接口，您必须为它分配一个 VLAN。

所有类型的接口均包括最大数量的组合接口；例如， VLAN、物理、冗余、网桥组和 EtherChannel 接口。在配置中定义的每个 **interface** 均根据此限制进行计数。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在多情景模式中，应在系统执行空间中配置物理接口 （如第 10-11 页的开始接口配置 （ASA 5512-X 及更高版本）中所述）。然后，在情景执行空间中配置逻辑接口参数 （如第 12 章，“路由模式接口”或第 13 章，“透明模式接口”中所述）。

防火墙模式准则

- 对于透明模式，可以为每个情景或单模式设备最多配置 8 个桥接组。
- 每个网桥组最多可包括 4 个接口。
- 对于多情景透明模式，每个情景必须使用不同的接口；不能在情景之间共享一个接口。

故障转移准则

- 如果要将冗余接口或 EtherChannel 接口用作故障转移链路，必须在故障转移对中的两台设备上预配置要使用接口；不能在主要设备上配置该接口并期望它会复制到辅助设备，因为*复制需要使用故障转移链路本身*。
- 如果将冗余接口或 EtherChannel 接口用于状态链路，不需要进行特殊配置；配置可从主要设备中如常复制。

- 可以。如果活动成员接口故障转移到备用接口，该活动不会在监控设备级故障转移时导致冗余接口或 EtherChannel 接口出现故障。仅在所有物理接口都出现故障的情况下，冗余接口或 EtherChannel 接口才会出现故障 （对于 EtherChannel 接口，可配置允许出现故障的成员接口数量）。
- 如果将 EtherChannel 接口用于故障转移或状态链路，然后防止无序数据包，则只会使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。不能作为故障转移链路处于使用状态的 EtherChannel 配置。要更改配置，需要在进行更改时关闭 EtherChannel 或临时禁用故障转移；这两种操作都可在持续时间内防止故障转移发生。
- 不能与数据接口共享一个故障转移接口或状态接口。

集群准则

- 要配置跨网络 EtherChannel，请参阅第 9-40 页的配置跨网络 EtherChannel。
- 要配置单个集群接口，请参阅第 9-38 页的配置独立接口 （管理接口的推荐配置）。

冗余接口准则

- 最多可以配置 8 个冗余接口对。
- 所有 ASA 配置均引用逻辑冗余接口，而不是成员物理接口。
- 不能将冗余接口用作 EtherChannel 的一部分，也不能将 EtherChannel 用作冗余接口的一部分。不能在冗余接口和 EtherChannel 接口中使用相同的物理接口。但是，如果这两种接口不是使用相同的物理接口，可以在 ASA 上配置这两种接口。
- 如果关闭主用接口，则将激活备用接口。
- 冗余接口不支持作为成员的管理*插槽 / 端口*接口。也不能将组成非管理接口的冗余接口设置为管理专属接口。
- 有关故障转移准则，请参阅第 10-9 页的故障转移准则。
- 有关集群准则，请参阅第 10-10 页的集群准则。

EtherChannel 准则

- 最多可配置 48 个 EtherChannel。
- 每个通道组最多可以有 16 个主用接口。对于仅支持 8 个主用接口的交换机，最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。
- 通道组中的所有接口必须具有相同的类型和速度。添加到通道组中的第一个接口确定正确的类型和速度。
- 连接 ASA EtherChannel 的设备必须同时支持 802.3ad EtherChannel ；例如，可以连接到 Catalyst 6500 交换机或思科 Nexus 7000 交换机。
- ASA 不支持带有 VLAN 标记的 LACPDU。如果使用思科 IOS **vlan dot1Q tag native** 命令在相邻的交换机上启用本地 VLAN 标记， ASA 将会丢弃附上了标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。在多情景模式中，这些消息不包含在数据包捕获范围内，因此，对这个问题的诊断并不容易。
- ASA 不支持将 EtherChannel 连接到交换机堆叠。如果跨堆叠连接 ASA EtherChannel，则当主交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。
- 所有 ASA 配置均引用逻辑 EtherChannel 接口，而不是成员物理接口。
- 不能将冗余接口用作 EtherChannel 的一部分，也不能将 EtherChannel 用作冗余接口的一部分。不能在冗余接口和 EtherChannel 接口中使用相同的物理接口。但是，如果这两种接口不是使用相同的物理接口，可以在 ASA 上配置这两种接口。

- 有关故障转移准则，请参阅第 10-9 页的故障转移准则。
- 有关集群准则，请参阅第 10-10 页的集群准则。

默认设置

本节列出了接口的默认设置 （如果没有出厂默认配置）。有关出厂默认配置的信息，请参阅第 2-14 页的出厂默认配置。

接口的默认状态

接口的默认状态取决于类型和情景模式。

在多情景模式中，所有分配的接口均默认启用，无论系统执行空间中接口的状态如何。但是，为使流量通过接口，还必须在系统执行空间中启用接口。如果关闭系统执行空间中的接口，则该接口将在共享它的所有情景中处于关闭状态。

在单模式中或系统执行空间中，接口具有以下默认状态：

- 物理接口 - 已禁用。
- 冗余接口 - 已启用。但是，对于通过冗余接口的流量，还必须启用成员物理接口。
- 子接口 - 已启用。但是，对于通过子接口的流量，还必须启用物理接口。
- EtherChannel 端口通道接口 - 已启用。但是，要使流量能够通过 EtherChannel 接口，还必须启用通道组物理接口。

默认速度和双工

- 默认情况下，铜缆 (RJ-45) 接口的速度和双工设置为自动协商。
- 对于 5585-X 的光纤接口，会针对自动链路协商设置速度。

默认连接器类型

有些型号包含两个连接器类型：铜缆 RJ-45 和光纤 SFP。 RJ-45 是默认接口。可以将 ASA 配置为使用光纤 SFP 连接器。

默认 MAC 地址

默认情况下，物理接口使用烧录 MAC 地址，物理接口的所有子接口均使用相同的烧录 MAC 地址。

开始接口配置 （ASA 5512-X 及更高版本）

- 第 10-12 页的开始接口配置的任务流程
- 第 10-12 页的启用物理接口并配置以太网参数
- 第 10-15 页的配置冗余接口
- 第 10-18 页的配置 EtherChannel
- 第 10-23 页的配置 VLAN 子接口和 802.1Q 中继
- 第 10-25 页的启用巨型帧支持
- 第 10-26 页的将使用中的接口转换为冗余接口或 EtherChannel 接口

开始接口配置的任务流程

注　如果拥有现有配置，并且要将使用中的接口转换为冗余接口或 EtherChannel 接口，请脱机执行配置使用 CLI 以最大程度减少中断。请参阅第 10-26 页的将使用中的接口转换为冗余接口或 EtherChannel 接口。

要开始配置接口，请执行以下步骤：

步骤 1　（多情景模式）在系统执行空间中完成本节所述的所有任务。如果尚未处于系统配置模式中，请在 Configuration > Device List 窗格中，双击主用设备 IP 地址下方的 **System**。

步骤 2　启用物理接口，或者更改以太网参数。请参阅第 10-12 页的启用物理接口并配置以太网参数。

默认情况下，物理接口已禁用。

步骤 3　（可选）配置冗余接口对。请参阅第 10-15 页的配置冗余接口。

逻辑冗余接口将一个主用接口和一个备用物理接口进行配对。如果主用接口发生故障，备用接口将激活并开始传输流量。

步骤 4　（可选）配置 EtherChannel。请参阅第 10-18 页的配置 EtherChannel。

一个 EtherChannel 将多个以太网接口分组到一个逻辑接口中。

步骤 5　（可选）配置 VLAN 子接口。请参阅第 10-23 页的配置 VLAN 子接口和 802.1Q 中继。

步骤 6　（可选）根据第 10-25 页的启用巨型帧支持启用巨型帧支持。

步骤 7　（仅限多情景模式）要在系统执行空间中完成接口配置，请执行第 7 章，“多情景模式”中所述的以下任务：

- 要将接口分配给情景，请参阅第 7-18 页的配置安全情景。
- （可选）要将唯一的 MAC 地址自动分配给情景接口，请参阅第 7-22 页的自动为情景接口分配 MAC 地址。

MAC 地址用于在情景中对数据包进行分类。如果共享一个接口但每个情景中没有该接口的唯一 MAC 地址，将会使用目标 IP 地址对数据包进行分类。或者，可以按照第 12-10 页的配置 MAC 地址、 MTU 和 TCP MSS 中所述在情景中手动分配 MAC 地址。

步骤 8　根据第 12 章，“路由模式接口”或第 13 章，“透明模式接口”完成接口配置。

启用物理接口并配置以太网参数

本节介绍如何执行以下操作：

- 启用物理接口
- 设置特定的速度和双工 （如果有）
- 启用暂停帧以进行流量控制

先决条件

对于多情景模式，请在系统执行空间中完成本操作步骤。如果尚未处于系统配置模式中，请在 Configuration > Device List 窗格中，双击主用设备 IP 地址下方的 **System**。

详细步骤

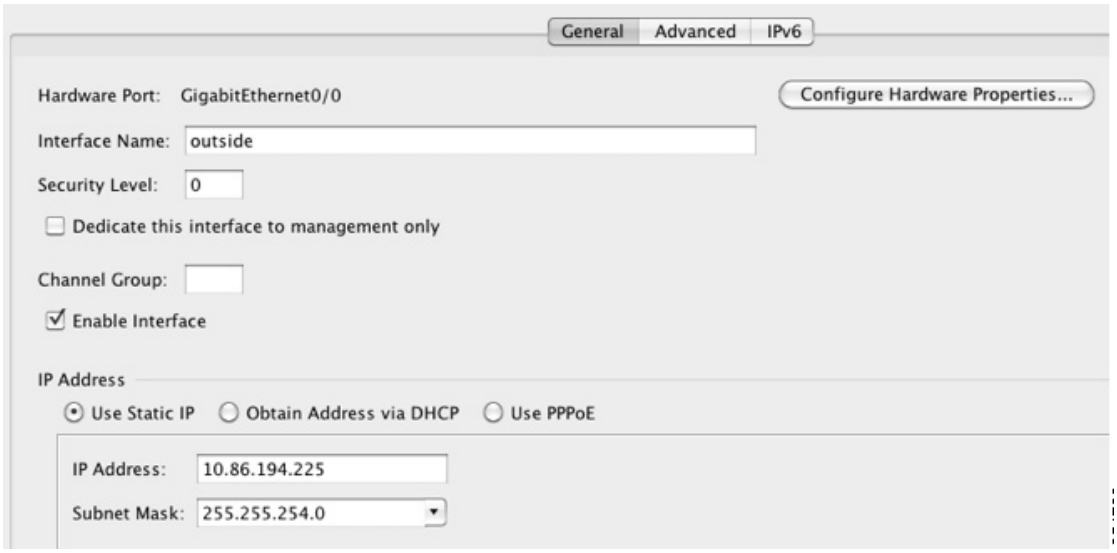
步骤 1　视情景模式而定：

- 对于单情景模式，请选择 **Configuration > Device Setup > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中选择 **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。



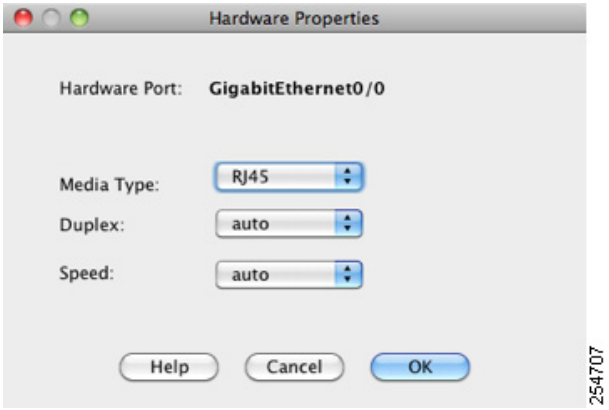
注　在单模式中，此操作步骤仅涉及 Edit Interface 对话框中的参数子集；要配置其他参数，请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”。请注意，在多情景模式中，需要在完成接口配置之前将接口分配给情景。请参阅第 7-14 页的配置多情景。

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 （不包括回车键）。例如，对于故障转移或状态链路，说明固定为 “LAN Failover Interface”、“STATE Failover Interface” 或 “LAN/STATE Failover Interface”。无法编辑该说明。如将此接口设为故障转移或状态链路，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. 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　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，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。请参阅第 10-2 页的 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。暂停 (XOFF) 和 XON 帧根据 FIFO 缓冲区的使用量由 NIC 硬件自动生成。如果缓冲区使用量超过高水位，会发送暂停帧。默认的 *high_water* 值为 128 KB （10 千兆以太网）和 24 KB （千兆以太网）；可以将此值设置为介于 0 到 511 （10 千兆以太网）或介于 0 到 47 KB （千兆以太网）之间的值。发送暂停后，当缓冲区使用量降低到低水位以下时，可发送 XON 帧。默认的 *low_water* 值为 64 KB （10 千兆以太网）和 16 KB （千兆以太网）；可以将此值设置为介于 0 到 511 （10 千兆以太网）或介于 0 到 47 KB （千兆以太网）之间的值。链路伙伴可能会在接收 XON 后或 XOFF 到期后耗用流量，具体由暂停帧中的计时器值控制。默认的 *pause_time* 值为 26624；可以将此值设置为介于 0 到 65535 之间的值。如果缓冲区使用量始终在高水位之上，将会重复发送暂停帧 （具体由暂停刷新阈值控制）。

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　仅支持 802.3x 中定义的流量控制帧。不支持基于优先级的流量控制。

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

步骤 6　点击 **OK** 以接受接口更改。

后续操作

可选任务：

- 配置冗余接口对。请参阅第 10-15 页的配置冗余接口。
- 配置 EtherChannel。请参阅第 10-18 页的配置 EtherChannel。
- 配置 VLAN 子接口。请参阅第 10-23 页的配置 VLAN 子接口和 802.1Q 中继。
- 配置巨型帧支持。请参阅第 10-25 页的启用巨型帧支持。

必需执行的任务：

- 对于多情景模式，请将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 7-14 页的配置多情景。
- 对于单情景模式，请完成接口配置。请参阅第 12 章，“ 路由模式接口 ”或第 13 章，“ 透明模式接口 ”

配置冗余接口

一个逻辑冗余接口包括一对物理接口：主用和备用接口。如果主用接口发生故障，备用接口将激活并开始传输流量。可以配置冗余接口来提高 ASA 的可靠性。此功能独立于设备级故障转移，如有必要，可以配置冗余接口以及故障转移。

本节介绍如何配置冗余接口。

配置冗余接口

本节介绍如何创建冗余接口。默认情况下，冗余接口已启用。

准则和限制

- 最多可以配置 8 个冗余接口对。
- 冗余接口延迟值可配置，但在默认情况下， ASA 根据其成员接口的物理类型继承默认延迟值。
- 另请参阅第 10-10 页的冗余接口准则。

先决条件

- 两个成员接口必须为相同的物理类型。例如，两个都必须是千兆以太网接口。
- 不能将已配置了名称的物理接口添加到冗余接口。若要这样做，必须先在 Configuration > Device Setup > Interfaces 窗格中移除名称。
- 对于多情景模式，请在系统执行空间中完成本操作步骤。如果尚未处于系统配置模式中，请在 Configuration > Device List 窗格中，双击主用设备 IP 地址下方的 **System**。

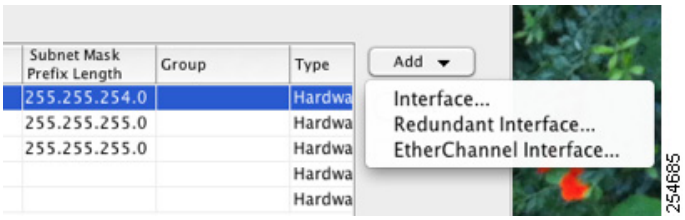
注意事项 如果使用已在配置中的物理接口，移除该接口的名称将会清除引用该接口的任何配置。

详细步骤

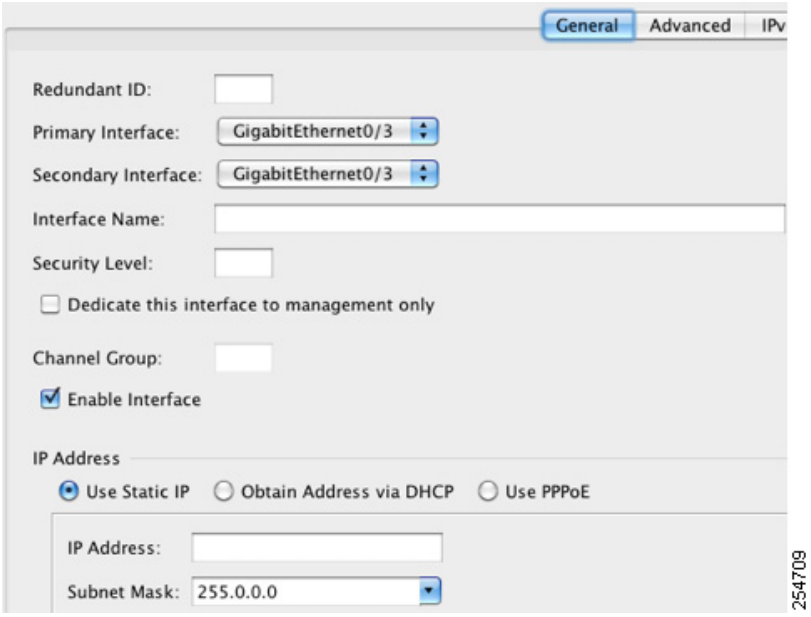
步骤 1　视情景模式而定：

- 对于单情景模式，请选择 **Configuration > Device Setup > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中选择 **Configuration > Context Management > Interfaces** 窗格。

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



系统将显示 Add Redundant Interface 对话框。



注　在单情景模式中，此操作步骤仅涉及 Edit Redundant Interface 对话框中的参数子集；要配置其他参数，请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”。请注意，在多情景模式中，需要在完成接口配置之前将接口分配给情景。请参阅第 7-14 页的配置多情景。

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

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

请务必选择没有子接口而且未分配给情景的接口。冗余接口不支持作为成员的管理*插槽 / 端口*接口。

步骤 5　从 Secondary Interface 下拉列表中，选择要用作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。要禁用该接口，请取消选中此复选框。

步骤 7　要添加描述，请在 Description 字段中输入文本。

一行描述最多可包含 240 个字符 （不包括回车键）。在多情景模式中，系统描述与情景描述无关。例如，对于故障转移或状态链路，说明固定为 “LAN Failover Interface”、“STATE Failover Interface” 或 “LAN/STATE Failover Interface”。不能编辑这种描述。如果使接口处于故障转移或状态链路状态，固定描述会覆盖您在此输入的任何描述。

步骤 8　点击 **OK**。

将返回 Interfaces 窗格。现在成员接口在接口 ID 左侧显示锁定，表明只可以为其配置基本参数。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

后续操作

可选任务：

- 配置 VLAN 子接口。请参阅第 10-23 页的配置 VLAN 子接口和 802.1Q 中继。
- 配置巨型帧支持。请参阅第 10-25 页的启用巨型帧支持。

必要任务：

- 对于多情景模式，请将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 7-14 页的配置多情景。
- 对于单情景模式，请完成接口配置。请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”。

更改主用接口

默认情况下，主用接口 （如果有）是配置中列出的第一个接口。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 redundant*number* **detail | grep Member**

例如：

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

要更改主用接口，请输入以下命令：

redundant-interface redundant*number* **active-member** *physical_interface*

其中， **redundant***number* 参数是冗余接口 ID，例如 **redundant1**。

physical_interface 是想激活的成员接口 ID。

配置 EtherChannel

本节介绍如何创建 EtherChannel 端口通道接口，如何将接口分配给 EtherChannel，以及如何自定义 EtherChannel。

将接口添加到 EtherChannel

本节介绍如何创建 EtherChannel 端口通道接口并向 EtherChannel 分配接口。默认情况下，端口通道接口已启用。

准则和限制

- 最多可配置 48 个 EtherChannel。
- 每个通道组最多可以有 16 个主用接口。对于仅支持 8 个主用接口的交换机，最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。
- 要配置集群的跨网络 EtherChannel，请参阅第 9-40 页的配置跨网络 EtherChannel 而不是此操作步骤。
- 另请参阅第 10-10 页的 EtherChannel 准则。

先决条件

- 通道组中的所有接口必须具有相同的类型、速度和双工。不受支持半双工。
- 不能将已配置了名称的物理接口添加到通道组。若要这样做，必须先在 Configuration > Device Setup > Interfaces 窗格中移除名称。
- 对于多情景模式，请在系统执行空间中完成本操作步骤。如果尚未处于系统配置模式中，请在 Configuration > Device List 窗格中，双击主用设备 IP 地址下方的 **System**。

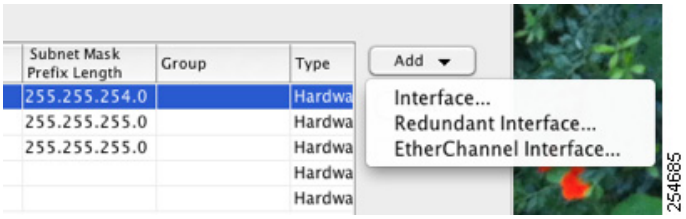
注意事项　如果使用已在配置中的物理接口，移除该接口的名称将会清除引用该接口的任何配置。

详细步骤

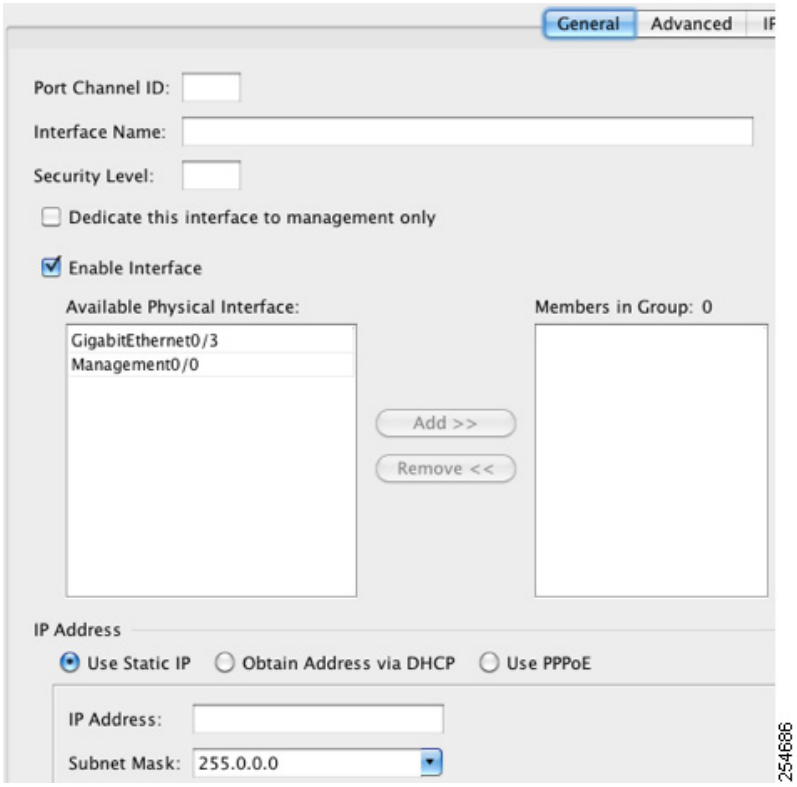
步骤 1　视情景模式而定：

- 对于单情景模式，请选择 **Configuration > Device Setup > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中选择 **Configuration > Context Management > Interfaces** 窗格。

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



系统将显示 Add EtherChannel Interface 对话框。



注　在单模式中，此操作步骤仅涉及 Edit EtherChannel Interface 对话框中的参数子集；要配置其他参数，请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”。请注意，在多情景模式中，需要在完成接口配置之前将接口分配给情景。请参阅第 7-14 页的配置多情景。

步骤 3　在 Port Channel ID 字段中，输入一个介于 1 到 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 >>** 以将该接口移到 Members in Group 区域。

在透明模式中，如果用多个管理接口创建一个通道组，可以将 EtherChannel 用作管理专用接口。

注　如果要将 EtherChannel 模式设置为 On，最初只能包含一个接口。完成此操作步骤后，编辑成员接口，并将模式设置为 On。应用更改，然后编辑 EtherChannel 以添加更多的成员接口。

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挂起状态。 ASDM 不会阻止您添加不匹配的接口。

步骤 6　点击 **OK**。

将返回 Interfaces 窗格。现在成员接口在接口 ID 左侧显示锁定，表明只可以为其配置基本参数。EtherChannel 接口已添加到该表中。

步骤 7　点击 **Apply**。所有成员接口均自动启用。

后续操作

可选任务：

- 自定义 EtherChannel 接口。请参阅第 10-20 页的自定义 EtherChannel。
- 配置 VLAN 子接口。请参阅第 10-23 页的配置 VLAN 子接口和 802.1Q 中继。

必要任务：

- 对于多情景模式，请将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 7-14 页的配置多情景。
- 对于单情景模式，请完成接口配置。请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”。

自定义 EtherChannel

本节介绍如何设置 EtherChannel 中的最大接口数量， EtherChannel 要成为主用接口所需的最小操作接口数量、负载均衡算法以及其他可选参数。

详细步骤

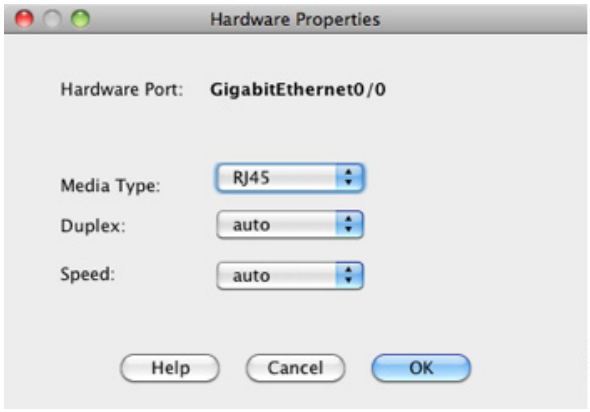
步骤 1　视情景模式而定：

- 对于单情景模式，请选择 **Configuration > Device Setup > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中选择 **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键，因为通道组中所有接口的这些参数必须匹配。



a. 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** 或 **Auto** （具体取决于接口类型）。 EtherChannel 不支持半双工。

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，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。请参阅第 10-2 页的 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。

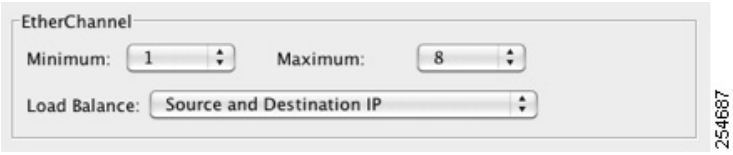
如果流量激增，数据包会在激增量超过 NIC 上的 FIFO 缓冲区的缓冲容量且接收环缓冲的情况下发生中断。启用暂停帧来进行流量控制可缓解此问题。暂停 (XOFF) 和 XON 帧根据 FIFO 缓冲区的使用量由 NIC 硬件自动生成。如果缓冲区使用量超过高水位，会发送暂停帧。高水位默认值为 128 KB ； 可以将此值设置为一个介于 0 到 511 之间的值。发送暂停后，当缓冲区使用量降低到低水位以下时，可发送 XON 帧。低水位默认值为 64 KB ； 可以将此值设置为一个介于 0 到 511 之间的值。链路伙伴可能会在接收 XON 后或 XOFF 到期后耗用流量，具体由暂停帧中的暂停时间值控制。默认暂停时间值为 26624 ； 可以将此值设置为介于 0 到 65535 之间的值。如果缓冲区使用量始终在高水位之上，将会重复发送暂停帧 （具体由暂停刷新阈值控制）。

要更改低低水位、高水位和暂停时间的默认值，请取消选中 **Use Default Values** 复选框。

注　仅支持 802.3x 中定义的流量控制帧。不支持基于优先级的流量控制。

e. 要接受硬件属性更改，请点击 **OK**。

步骤 4　要自定义 EtherChannel，请点击 **Advanced** 选项卡。



a. 在 EtherChannel 区域，从 Minimum 下拉列表中选择 EtherChannel 要作为主用接口所需的最小主用接口数量 （1 到 16）。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量（1 到 16）。默认值为 16。如果交换机不支持 16 个主用接口，请务必将此命令设置为 8 或更小的值。

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 地址来平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，请选择另一组标准。例如，如果流量严重偏向于相同的源 IP 地址和目标 IP 地址，那么，分配给 EtherChannel 中的接口的流量将失去平衡。更改为其他算法可使流量分布更均匀。有关负载均衡的详细信息，请参阅第 10-6 页的负载均衡。

步骤 5　点击 **OK**。

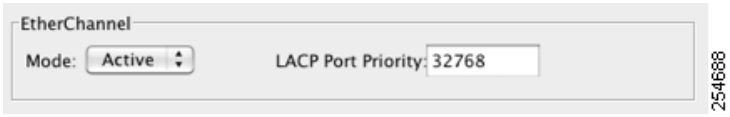
将返回 Interfaces 窗格。

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 （默认设置）。有关主用模式、备用模式和开启模式的信息，请参阅第 10-6 页的链路聚合控制协议。

d. 在 LACP Port Priority 字段中，将端口优先级设置为一个介于 1 到 65535 之间的值。默认值为 32768。数值越大，优先级越低。如果分配的接口多于可用的接口， ASA 将使用此设置决定哪些接口是主用接口，哪些是备用接口。如果所有接口的端口优先级设置都是相同的，则优先级由接口 ID （插槽 / 端口）确定。最低的接口 ID 优先级最高。例如，千兆以太网 0/0 的优先级高于千兆以太网 0/1 的优先级。

如果要将某个接口优先确定为主用接口，即使它具有较高的接口 ID，请将此命令设置为具有较低的值。例如，要使千兆以太网 1/3 在千兆以太网 0/7 之前变为主用接口，请将 1/3 接口上的优先级值更改为 12345，将 0/7 接口上的这个值更改为默认值 32768。

如果 EtherChannel 另一端的设备端口存在优先级冲突，将会使用系统优先级来确定使用哪些端口优先级。要设置系统优先级，请参阅步骤 9。

步骤 7　点击 **OK**。

将返回 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，将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，请选择 **Configuration > Device Setup > EtherChannel** 窗格。
- 对于多情景模式，请在系统执行空间中选择 **Configuration > Context Management > EtherChannel** 窗格。

b. 在 LACP System Priority 字段中，输入一个介于 1 到 65535 之间的优先级值。

默认值为 32768。

后续操作

可选任务：

- 配置 VLAN 子接口。请参阅第 10-23 页的配置 VLAN 子接口和 802.1Q 中继。
- 配置巨型帧支持。请参阅第 10-25 页的启用巨型帧支持。

必要任务：

- 对于多情景模式，请将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 7-14 页的配置多情景。
- 对于单情景模式，请完成接口配置。请参阅第 12 章，“ 路由模式接口 ”或第 13 章，“ 透明模式接口 ”

配置 VLAN 子接口和 802.1Q 中继

子接口可用于将物理接口、冗余接口或 EtherChannel 接口分成标记有不同 VLAN ID 的多个逻辑接口。具有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 可使在给定的物理接口上保持流量分离，因此，可以增加可用于网络的接口数量，而无需添加额外的物理接口或 ASA。此功能对多情景模式尤其有用，使得可以向每个情景分配唯一的接口。

准则和限制

- 最大子接口数 - 要确定您的型号可使用多少个 VLAN 子接口，请参阅第 10-8 页的 ASA 5512-X 及更高版本接口的许可要求。
- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常也不想要物理接口传输流量，因为物理接口将传递未标记的数据包。此属性对冗余接口对中的主用物理接口以及 EtherChannel 链路同样适用。由于必须启用物理接口、冗余接口或 EtherChannel 接口才能使子接口允许流量通过，因此，请不要为接口配置名称，以确保物理接口、冗余接口或 EtherChannel 接口不允许流量通过。如果要使物理接口、冗余接口或 EtherChannel 接口允许未标记的数据包通过，可以如常配置 name。有关完成接口配置的详细信息，请参阅第 12 章，“ 路由模式接口 ”或第 13 章，“ 透明模式接口 ”。
- （ASA 5512-X 到 ASA 5555-X）不能在 Management 0/0 接口上配置子接口。
- ASA 不支持动态中继协议 (DTP)，因此，必须无条件地将连接的交换机端口配置到中继上。

先决条件

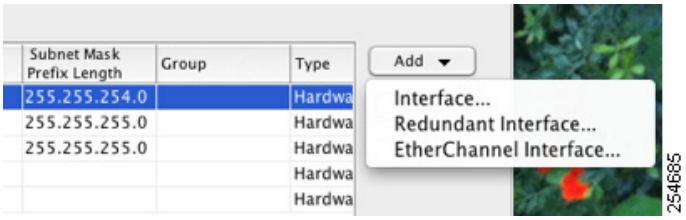
对于多情景模式，请在系统执行空间中完成本操作步骤。如果尚未处于系统配置模式中，请在 Configuration > Device List 窗格中，双击主用设备 IP 地址下方的 **System**。

详细步骤

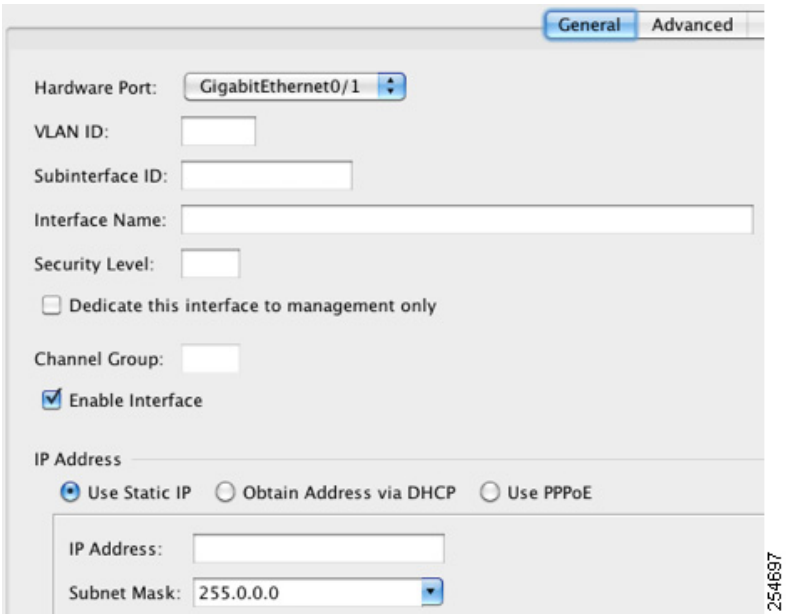
步骤 1　视情景模式而定：

- 对于单情景模式，请选择 **Configuration > Device Setup > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中选择 **Configuration > Context Management > Interfaces** 窗格。

步骤 2　选择 **Add > Interface**。



系统将显示 Add Interface 对话框。



注　在单模式中，此操作步骤仅涉及 Edit Interface 对话框中的参数子集；要配置其他参数，请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”。请注意，在多情景模式中，需要在完成接口配置之前将接口分配给情景。请参阅第 7-14 页的配置多情景。

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。要禁用该接口，请取消选中此复选框。

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

某些 VLAN ID 可能保留在连接的交换机上，因此，请检查交换机文档了解详细信息。在多情景模式中，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 到 4294967293 之间的整数）。

允许的子接口数量因平台而异。此 ID 一旦设置便不可更改。

步骤 7　（可选）在 Description 字段中，输入该接口的说明。

一行描述最多可包含 240 个字符 （不包括回车键）。在多情景模式中，系统描述与情景描述无关。例如，对于故障转移或状态链路，说明固定为 “LAN Failover Interface”、“STATE Failover Interface” 或 “LAN/STATE Failover Interface”。不能编辑这种描述。如果使接口处于故障转移或状态链路状态，固定描述会覆盖您在此输入的任何描述。

步骤 8　点击 **OK**。

将返回 Interfaces 窗格。

后续操作

可选任务：

- 配置巨型帧支持。请参阅第 10-25 页的启用巨型帧支持。

必要任务：

- 对于多情景模式，请将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 7-14 页的配置多情景。
- 对于单情景模式，请完成接口配置。请参阅第 12 章，“ 路由模式接口 ”或第 13 章，“ 透明模式接口 ”。

启用巨型帧支持

巨型帧是指大于标准最大字节数 （1518 字节）的以太网数据包 （包括第 2 层报头和 FCS），最大可达 9216 字节。可通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配更多内存可能会限制对其他功能的最充分利用，如 ACL。有关详细信息，请参阅第 10-6 页的用最大传输单元、 TCP 最大分段大小控制分片。

先决条件

- 在多情景模式中，请在系统执行空间中设置此选项。
- 如果更改此设置，需要重新加载 ASA。
- 请务必为需要向高于默认值 1500 的值传输巨型帧的每个接口设置 MTU ；例如，将该值设置为 9198。请参阅第 12-10 页的配置 MAC 地址、MTU 和 TCP MSS。在多情景模式中，请在每个情景中设置 MTU。
- 请务必调整 TCP MSS，以对非 VPN 流量禁用此功能，或者根据 MTU 增加 TCP MSS 的值（如第 12-10 页的配置 MAC 地址、 MTU 和 TCP MSS 中所述）。

详细步骤

- 多模式 - 要启用巨型帧支持，请选择 **Configuration > Context Management > Interfaces**，并点击 **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型帧。要手动启用或禁用该设置，请选择 **Configuration > Device Setup > Interfaces**，并点击 **Enable jumbo frame support** 复选框。

后续操作

- 对于多情景模式，请将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 7-14 页的配置多情景。
- 对于单情景模式，请完成接口配置。请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”

将使用中的接口转换为冗余接口或 EtherChannel 接口

如果拥有现有配置，并想要利用当前所用接口的冗余或 EtherChannel 接口功能，在转换到逻辑接口时，将会出现一段停机时间。

本节简要介绍如何在最短的停机时间内将现有的接口转换为冗余接口或 EtherChannel 接口。有关详细信息，请参阅第 10-15 页的配置冗余接口和第 10-18 页的配置 EtherChannel。

- 第 10-26 页的详细步骤 （单模式）
- 第 10-31 页的详细步骤 （多模式）

详细步骤 （单模式）

出于以下理由，我们建议在脱机状态下将配置更新为文本文件，并重新导入整个配置：

- 由于不能将已命名的接口添加为冗余接口或 EtherChannel 接口的成员，因此必须移除接口的名称。移除接口的名称后，引用该名称的任何命令都将被删除。由于引用接口名称的命令在整个配置中普遍存在且影响多个功能，因此，围绕新接口名称重新配置所有功能时，如果从 CLI 或 ASDM 中正在使用的接口移除名称，将会严重损坏配置和长时间停机。
- 在脱机状态下更改配置可以对新逻辑接口使用原来的接口名称，从而无需改变引用接口名称的功能配置。只需要更改接口配置。
- 清除运行配置并立即应用新配置可最大程度减少接口的停机时间。这样将无需等待实时配置接口。

步骤 1　连接 ASA；如果要使用故障转移，请连接到主用 ASA。

步骤 2　如果要使用故障转移，请选择 **Configuration > Device Management > High Availability > Failover** 并取消选中 **Enable failover** 复选框来禁用故障转移。点击 **Apply**，并在出现警告后继续操作。

步骤 3　选择 **Tools > Backup Configurations** 并将运行配置备份到本地计算机中，以复制运行配置。然后，可以展开压缩文件并在文本编辑器中编辑 running-config.cfg 文件。

如果在编辑时出错，请务必保存旧配置的额外副本。

步骤 4　对于要添加到冗余接口或 EtherChannel 接口的每个使用中的接口，请在 **interface** 命令下将所有命令剪切并粘贴到接口配置部分的结尾，以用于创建新逻辑接口。以下命令是唯一的例外，这些命令应与物理接口配置放在一起：

- **media-type**
- **speed**

- **duplex**
- **flowcontrol**

注　只能将*物理*接口添加到 EtherChannel 或冗余接口；不能为物理接口配置 VLAN。

请务必在给定的 EtherChannel 或冗余接口中为所有接口匹配上述值。请注意，EtherChannel 接口的双工设置必须为 Full 或 Auto。

例如，接口配置如下。粗体的命令是要用于三个新 EtherChannel 接口的命令，应该将这些命令剪切并粘贴到接口部分的结尾。

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 no shutdown
!
interface Management0/1
 shutdown
 no nameif
 no security-level
 no ip address
```

步骤 5　在每个粘贴的命令部分上方，通过输入以下命令之一创建新逻辑接口：

- **interface redundant** *number* [1-8]
- **interface port-channel** *channel_id* [1-48]

例如：

```
...

interface port-channel 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 no shutdown
!
interface port-channel 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface port-channel 3
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 no shutdown
```

步骤 6　向新逻辑接口分配物理接口：

- 冗余接口 - 在新的 **interface redundant** 命令下输入以下命令：

  member-interface *physical_interface1*
  member-interface *physical_interface2*

  其中，物理接口是同一种类型的任意两个接口 （之前使用的或未使用的）。不能将管理接口分配给冗余接口。

  例如，要利用现有布线，应继续按其原来的角色使用之前使用的接口，以作为内部和外部冗余接口的一部分：

  ```
  interface redundant 1
   nameif outside
   security-level 0
   ip address 10.86.194.225 255.255.255.0
   member-interface GigabitEthernet0/0
   member-interface GigabitEthernet0/2

  interface redundant 2
   nameif inside
   security-level 100
   ip address 192.168.1.3 255.255.255.0
   member-interface GigabitEthernet0/1
   member-interface GigabitEthernet0/3
  ```

- EtherChannel 接口 - 在要添加到 EtherChannel 的每个接口下输入以下命令 （之前使用的或未使用的）。最多可以为每个 EtherChannel 分配 16 个接口，但只有 8 个接口可作为主用接口；其他接口在故障情况下处于备用状态。

  channel-group *channel_id* **mode active**

  例如，要利用现有布线，应继续按其原来的角色使用之前使用的接口，以作为内部和外部 EtherChannel 接口的一部分：

  ```
  interface GigabitEthernet0/0
   channel-group 1 mode active
  ```

```
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 shutdown
 no nameif
 no security-level
 no ip address

...
```

步骤 7　在 **shutdown** 命令前面添加 **no**，启用当前属于逻辑接口一部分的之前未使用的每个接口。例如，最终 EtherChannel 配置如下：

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 no shutdown
 no nameif
 no security-level
```

```
 no ip address
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface port-channel 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
!
interface port-channel 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
!
interface port-channel 3
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
```

注　导入新配置后，可配置其他可选的 EtherChannel 参数。请参阅第 10-18 页的配置 EtherChannel。

步骤 8　保存整个新配置 （包括更改的接口部分）。

步骤 9　使用更改后的配置重新压缩备份文件夹。

步骤 10　选择 **Tools > Restore Configurations**，然后选择更改后的配置压缩文件。请务必替换现有的运行配置；请勿合并这些配置。有关详细信息，请参阅第 37-22 页的还原备份。

步骤 11　选择 **Configuration > Device Management > High Availability > Failover** 并选中 **Enable failover** 复选框，以重新启用故障转移。当系统提示您是否要配置基本故障转移设置时，请点击 **Apply**，然后点击 **No**。

详细步骤 （多模式）

出于以下理由，我们建议在脱机状态下将系统和情景配置更新为文本文件，并重新导入这些配置：

- 由于不能将分配的接口添加为冗余接口或 EtherChannel 接口的成员，因此，必须从任何情景中解除接口分配。解除接口分配后，引用该接口的任何情景命令都将被删除。由于引用接口的命令在整个配置中普遍存在且影响多个功能，因此，围绕新接口重新配置所有功能时，如果从 CLI 或 ASDM 中正在使用的接口移除分配，将会严重损坏配置和长时间停机。
- 在脱机状态下更改配置可以对新逻辑接口使用原来的接口名称，从而无需改变引用接口名称的功能配置。只需要更改接口配置。
- 清除运行系统配置并立即应用新配置可最大程度减少接口的停机时间。这样将无需等待实时配置接口。

步骤 1　连接到 ASA 并更改系统；如果要使用故障转移，请连接到主用 ASA。

步骤 2　如果要使用故障转移，请选择 **Configuration > Device Management > High Availability > Failover** 并取消选中 **Enable failover** 复选框来禁用故障转移。点击 **Apply**，并在出现警告后继续操作。

步骤 3　在系统中，选择 **File > Show Running Configuration in New Window** 并将显示输出复制到文本编辑器，以复制运行配置。

如果在编辑时出错，请务必保存旧配置的额外副本。

例如，系统配置中具有以下接口配置和分配，且两个情景之间共享接口。

System

```
interface GigabitEthernet0/0
    no shutdown
interface GigabitEthernet0/1
    no shutdown
interface GigabitEthernet0/2
    shutdown
interface GigabitEthernet0/3
    shutdown
interface GigabitEthernet0/4
    shutdown
interface GigabitEthernet0/5
    shutdown
interface Management0/0
    no shutdown
interface Management1/0
    shutdown
!
context customerA
    allocate-interface gigabitethernet0/0 int1
    allocate-interface gigabitethernet0/1 int2
    allocate-interface management0/0 mgmt
context customerB
    allocate-interface gigabitethernet0/0
    allocate-interface gigabitethernet0/1
    allocate-interface management0/0
```

步骤 4　获取将使用新 EtherChannel 或冗余接口的*所有*情景配置的副本。请参阅第 37-19 页的备份和还原配置或其他文件。

例如，下载以下情景配置 （显示接口配置）：

CustomerA Context

```
interface int1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
!
interface int2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface mgmt
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 management-only
```

CustomerB Context

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.20.15.5 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.6.78 255.255.255.0
!
interface Management0/0
 nameif mgmt
 security-level 100
 ip address 10.8.1.8 255.255.255.0
 management-only
```

步骤 5　在系统配置中，按照第 10-15 页的配置冗余接口或第 10-18 页的配置 EtherChannel 中所述创建新逻辑接口。请务必在要用作逻辑接口一部分的任何附加物理接口上输入 **no shutdown** 命令。

注　只能将*物理*接口添加到 EtherChannel 或冗余接口；不能为物理接口配置 VLAN。

请务必在给定的 EtherChannel 或冗余接口中匹配所有接口的物理接口参数 （例如，速度和双工）。请注意， EtherChannel 接口的双工设置必须为 Full 或 Auto。

例如，新配置如下：

System

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
```

```
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 no shutdown
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 no shutdown
!
interface port-channel 1
interface port-channel 2
interface port-channel 3
```

步骤 6　更改每个情景的接口分配，以使用新的 EtherChannel 或冗余接口。请参阅第 7-18 页的配置安全情景。

例如，要利用现有布线，应继续按其原来的角色使用之前使用的接口，以作为内部和外部冗余接口的一部分：

```
context customerA
    allocate-interface port-channel1 int1
    allocate-interface port-channel2 int2
    allocate-interface port-channel3 mgmt
context customerB
    allocate-interface port-channel1
    allocate-interface port-channel2
    allocate-interface port-channel3
```

注　如果尚未这样做，可能要借此机会将映射名称分配给接口。例如， customerA 的配置完全不需要更改；只需要将该配置重新应用于 ASA。但是， customerB 配置需要更改所有的接口 ID ；如果为 customerB 分配映射名称，仍需要在情景配置中更改接口 ID，但映射名称可能会有助于将来进行接口更改。

步骤 7　对于不使用映射名称的情景，请将情景配置更改为使用新的 EtherChannel 或冗余接口 ID。（使用映射接口名称的情景不需要任何更改。）

例如：

CustomerB Context

```
interface port-channel1
 nameif outside
 security-level 0
 ip address 10.20.15.5 255.255.255.0
```

```
!
interface port-channel2
 nameif inside
 security-level 100
 ip address 192.168.6.78 255.255.255.0
!
interface port-channel3
 nameif mgmt
 security-level 100
 ip address 10.8.1.8 255.255.255.0
 management-only
```

步骤 8　用新的情景配置文件覆盖旧文件。例如，对于闪存中的情景，请在系统中选择 **Tools > File Management**，然后选择 **File Transfer > Between Local PC and Flash**。此工具可用于选择各个配置文件并将其复制到本地计算机。此更改仅影响启动配置；运行配置仍使用旧的情景配置。

步骤 9　将整个新系统配置 （包括更改的接口部分）复制到剪贴板。

步骤 10　在 ASDM 中，选择 **Tools > Command Line Interface**，然后点击 **Multiple Line** 单选按钮。

步骤 11　输入 **clear configure all** 作为第一行，在其后粘贴新配置，然后点击 **Send**。 **clear** 命令在应用新配置前清除运行配置 （系统和情景）。

通过 ASA 的流量将会停止。将会重新加载所有的新情景配置。重新加载完毕后，通过 ASA 的流量将会恢复。

步骤 12　关闭 Command Line Interface 对话框，然后选择 **File > Refresh ASDM with the Running Configuration**。

步骤 13　选择 **Configuration > Device Management > High Availability > Failover** 并选中 **Enable failover** 复选框，以重新启用故障转移。当系统提示您是否要配置基本故障转移设置时，请点击 **Apply**，然后点击 **No**。

监控接口

- 请参阅第 12-19 页的 ARP 表。
- 请参阅第 12-21 页的 MAC 地址表。
- 请参阅第 12-22 页的接口图形。

后续操作

- 在多情景模式中：
  a. 将接口分配给情景，并将唯一的 MAC 地址自动分配给情景接口。请参阅第 7 章，“多情景模式”
  b. 按照第 12 章，“路由模式接口”或第 13 章，“透明模式接口”中所述完成接口配置。
- 对于单情景模式，请按照第 12 章，“路由模式接口”或第 13 章，“透明模式接口”中所述完成接口配置。

ASA 5512-X 及更高版本接口的功能历史记录

表 10-2 列出了此功能的版本历史记录。

表 10-2　　接口的功能历史记录

功能名称	版本	功能信息
增加的 VLAN 数量	7.0(5)	增加了以下限制： • ASA5510 基础许可证的 VLAN 数从 0 增加到 10。 • ASA5510 增强型安全许可证的 VLAN 数从 10 增加到 25。 • ASA5520 的 VLAN 数从 25 增加到 100。 • ASA5540 的 VLAN 数从 100 增加到 200。
ASA 5510 上基础许可证增加的接口数	7.2(2)	对于 ASA 5510 上的基础许可证，最大接口数从 3 个加上管理接口数，增至不受限制。
增加的 VLAN 数量	7.2(2)	提高了以下型号的 VLAN 上限：ASA 5510 的 （对于基础许可证，从 10 提高到 50 ；对于增强型安全许可证，从 25 提高到 100）、 ASA 5520 （从 100 提高到 150）、ASA 5550 （从 200 提高到 250）。
对于 ASA 5510 增强型安全许可证的千兆以太网支持	7.2(3)	现在， ASA 5510 ASA 通过增强型安全许可证为端口 0 和 1 提供 GE （千兆以太网）支持。如果从基础许可证升级至增强型安全许可证，则外部 Ethernet 0/0 和 Ethernet0/1 端口的容量将从原始的 FE （快速以太网）(100 Mbps) 增加到 GE (1000 Mbps)。接口名称仍保持为 Ethernet 0/0 和 Ethernet0/1。
冗余接口	8.0(2)	逻辑冗余接口将一个主用接口和一个备用物理接口进行配对。如果主用接口发生故障，备用接口将激活并开始传输流量。可以配置冗余接口来提高 ASA 的可靠性。此功能独立于设备级故障转移，但您可以在必要时配置冗余接口和故障转移。最多可以配置 8 个冗余接口对。
对 ASA 5580 的巨型数据包支持	8.1(1)	思科 ASA 5580 支持巨型帧。巨型帧是一个以太网数据包，其大小大于标准的最大值 1518 字节 （包括第 2 层报头和 FCS），最大可达 9216 字节。可通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配更多内存可能会限制对其他功能的最充分利用，如 ACL。 ASA 5585-X 也支持此功能。 我们修改了以下屏幕：Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced。
为 ASA 5580 增加的 VLAN 数	8.1(2)	ASA 5580 支持的 VLAN 数量从 100 增加到 250。

表 10-2　　接口的功能历史记录 （续）

功能名称	版本	功能信息
在 ASA 5580 的 10 千兆以太网接口上支持暂停帧以进行流量控制	8.2(2)	现可为流量控制启用暂停 (XOFF) 帧。 ASA 5585-X 也支持此功能。 我们修改了以下屏幕： （单情景模式）Configuration > Device Setup > 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)	现在，可以在所有型号的千兆以太网接口上启用暂停 (XOFF) 帧以进行流量控制。 我们修改了以下屏幕： （单情景模式）Configuration > Device Setup > Interfaces > Add/Edit Interface > General （多情景模式，系统） Configuration > Interfaces > Add/Edit Interface。
EtherChannel 支持	8.4(1)	可以为八个主用接口各配置多达 48 个 802.3ad EtherChannel。 我们修改或引入了以下屏幕： Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add/Edit EtherChannel Interface Configuration > Device Setup > Interfaces > Add/Edit Interface Configuration > Device Setup > EtherChannel **注**　ASA 5505 不支持 EtherChannel。
一个 EtherChannel 中支持 16 个活动链路	9.2(1)	现在，在一个 EtherChannel 中最多可以配置 16 个活动链路。以前可以有 8 个活动链路和 8 个备用链路。确保交换机可以支持 16 个活动链路（例如，可使用带有 F2 系列 10 千兆以太网模块的思科 Nexus 7000）。 **注**　如果从较低 ASA 版本进行升级，为了实现兼容，可将最大主用接口数量设置为 8。 我们修改了以下屏幕：Configuration > Device Setup > Interfaces > Add/Edit EtherChannel Interface > Advanced。

基本接口配置 (ASAv)

本章包含启动思科 ASAv 接口配置的任务，包括配置以太网设置、冗余接口和 VLAN 子接口。

有关启动 ASAv 接口配置的信息

ASAv 接口和虚拟 NIC

作为虚拟化平台上的访客， ASAv 使用基础物理平台的网络接口。每个 ASAv 接口映射到一个虚拟 NIC (vNIC)。

ASAv 接口

ASAv 包括以下千兆以太网接口：

- Management 0/0
- GigabitEthernet 0/0 至 0/8。注意，如果将 ASAv 部署为故障转移对的一部分，则 GigabitEthernet 0/8 用于故障转移链路。

受支持的 vNIC

ASAv 支持以下 vNIC：

vNIC 类型	虚拟机监控程序支持		ASAv 版本	备注
	Vmware	KVM		
VMXNET3	是	否	9.2(1) 及更高版本	如在使用 VMXNET3，则需禁用 Large Receive Offload (LRO)，以免 TCP 性能不佳。请参阅以下有关 VMware 支持的文章： http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1027511 http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=2055140
e1000	是	是	9.2(1) 及更高版本	默认值。

ASAv 接口与 VMware 中 vNIC 的一致性

vSphere Client Virtual Machine Properties 屏幕 （右键单击 ASAv 实例，并选择 **Edit Settings**）显示每个网络适配器和已分配的网络。但是，该屏幕不会显示 ASAv 接口 ID （仅网络适配器 ID）。请参阅网络适配器 ID 与 ASAv ID 的以下一致性：

网络适配器 ID	ASAv 接口 ID
网络适配器 1	Management0/0
网络适配器 2	GigabitEthernet0/0
网络适配器 3	GigabitEthernet0/1
网络适配器 4	GigabitEthernet0/2
网络适配器 5	GigabitEthernet0/3
网络适配器 6	GigabitEthernet0/4
网络适配器 7	GigabitEthernet0/5
网络适配器 8	GigabitEthernet0/6
网络适配器 9	GigabitEthernet0/7
网络适配器 10	GigabitEthernet0/8

处于透明模式中的接口

处于透明模式中的接口属于 “ 网桥组 ”，每个网络都有一个网桥组。处于透明模式中的接口属于 “ 网桥组 ”，每个网络都有一个网桥组。有关网桥组的详细信息，请参阅第 13-1 页的透明模式的网桥组。

管理接口

管理接口概述

可以通过连接到以下接口来管理 ASA：

- 任何直通流量接口
- 专用 Management 0/0 接口

可能需要按照第 36 章，“ 管理访问 ”中所述配置对接口的管理访问。

将任何接口用于仅管理流量

可将任何接口用作管理专属接口，只需将其配置为用于管理流量。

用于透明模式的管理接口

在透明防火墙模式中，除了允许的最大直通流量接口数，还可以将 Management 0/0 接口 （物理接口或子接口）用作单独的管理接口。不能将任何其他接口类型用作管理接口。管理接口不属于普通网桥组的一部分。请注意，出于操作目的，管理接口属于不可配置网桥组的一部分。

注　在透明防火墙模式中，管理接口以与数据接口相同的方式更新 MAC 地址表；因此，不应将管理和数据接口连接到同一个交换机，除非将其中一个交换机端口配置为路由端口 （默认情况下，Catalyst 交换机在所有的 VLAN 交换机端口上共享一个 MAC 地址）。否则，如果流量从物理连接的交换机到达管理接口， ASA 会更新 MAC 地址表，以使用 *管理*接口 （而不是数据接口）来访问交换机。此操作会导致临时流量中断；出于安全原因， ASA 至少在 30 秒内不会再次更新从交换机到数据接口的数据包 MAC 地址表。

不支持直通流量

Management 0/0 接口始终设置为仅管理；该接口不可用于直通流量支持。

冗余接口

一个逻辑冗余接口包括一对物理接口：主用和备用接口。如果主用接口发生故障，备用接口将激活并开始传输流量。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转移，如果需要，可以配置冗余接口和设备级故障转移。

冗余接口 MAC 地址

冗余接口使用您添加的第一个物理接口的 MAC 地址。如果在配置中更改成员接口的顺序，则 MAC 地址发生更改，以匹配现第一个列出的接口的 MAC 地址。或者，无论成员接口 MAC 地址如何，均可以将 MAC 址址分配给冗余接口（请参阅第 12-10 页的配置 MAC 地址、MTU 和 TCP MSS 或第 7-14 页的配置多情景）。如果主用接口故障转移到备用接口，系统将维护同一 MAC 地址，以防流量中断。

用最大传输单元、 TCP 最大分段大小控制分片

MTU 概述

最大传输单元 (MTU) 指定 ASA 可在给定以太网接口上传输的最大帧负载大小。MTU 值是*没有*以太网报头、FCS 或 VLAN 标记的帧大小。以太网报头为 14 字节，而 FCS 为 4 字节。如果将 MTU 设置为 1500，预期的帧大小 （包括报头）为 1518 字节。如果使用 VLAN 标记 （这样将会增加额外 4 字节），并将 MTU 设置为 1500，预期的帧大小为 1522。请勿为容纳这些报头而将 MTU 的值设得过高。对于容纳封装 TCP 报头的信息，请勿修改 MTU 设置；相反，请更改 TCP 最大分片大小 (第 11-5 页的 TCP 最大分段大小概述)。

注　只要有内存空间， ASA 就可接收大于所配置的 MTU 的帧。有关如何增加内存以接收较大的帧，请参阅第 11-14 页的启用巨型帧支持。

默认 MTU

ASA 上的默认 MTU 为 1500 字节。此值不包括以太网报头、CRC、VLAN 标记等的 18 个或更多字节。

路径 MTU 发现

ASA 支持路径 MTU 发现 （如 RFC 1191 中定义），允许两台主机之间网络路径中的所有设备均与 MTU 协调，以便能够对路径中的最小 MTU 进行标准化。

设置 MTU 和巨型帧

请参阅第 12-10 页的配置 MAC 地址、 MTU 和 TCP MSS。

请参阅第 11-14 页的启用巨型帧支持。

请参阅以下准则：

- 与流量路径上的 MTU 相匹配 - 我们建议将所有 ASA 接口以及流量路径的其他设备接口上的 MTU 设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧 - 如果启用巨型帧，则可将 MTU 设置为高达 9000 字节。

TCP 最大分段大小概述

TCP 最大分段尺寸 (TCP MSS) 是 TCP 负载在添加任何 TCP 报头*之前*的大小。UDP 数据包不会受到影响。建立连接时，客户端和服务器会在三次握手期间交换 TCP MSS 值。

可以在 ASA 上设置 TCP MSS。如果一个连接的任意终端要求 TCP MSS 的值大于 ASA 上设置的值，则 ASA 将用 ASA 最大值覆盖请求数据包内的 TCP MSS。如果主机或服务器不请求 TCP MSS，则 ASA 会假设 RFC 793 的默认值为 536 字节，但不会修改数据包。您还可以配置最小 TCP MSS ；如果主机或服务器请求一个非常小的 TCP MSS，则 ASA 可将该值调高。默认情况下，最小 TCP MSS 未启用。

例如，可以将默认 MTU 配置为 1500 字节。主机请求 1700 的 MSS。如果 ASA 的最大 TCP MSS 是 1380，ASA 会将 TCP 请求数据包中的 MSS 值更改为 1380。然后，服务器会发送 1380 字节的数据包。

默认 TCP MSS

默认情况下，ASA 上的最大 TCP MSS 是 1380 字节。此默认值符合 VPN 连接的要求（在 VPN 连接中，报头最多可增加 120 字节）；此值在默认 MTU （1500 字节）范围内。

设置 VPN 和非 VPN 流量的 TCP MSS

请参阅第 12-10 页的配置 MAC 地址、 MTU 和 TCP MSS。

请参阅以下准则：

- 非 VPN 流量 - 如果不使用 VPN 且不需要额外的报头空间，应该禁用 TCP MSS 限制并接受连接终端之间建立的值。由于连接终端一般是从 MTU 获得 TCP MSS，因此，非 VPN 数据包通常符合此 TCP MSS。
- VPN 流量 - 将最大 TCP MSS 设置为 MTU - 120。例如，如果使用巨型帧并将 MTU 设置为较大的值，需要将 TCP MSS 设置为符合新的 MTU。

ASAv 接口的许可要求

型号	许可证要求
带 1 个虚拟 CPU 的 ASAv	VLAN： 　　标准许可证和高级许可证：50 所有类型的接口： 　　标准许可证和高级许可证：716
带 4 个虚拟 CPU 的 ASAv	VLAN： 　　标准许可证和高级许可证：200 所有类型的接口： 　　标准许可证和高级许可证：1316

注　对于根据 VLAN 限制计数的接口，您必须为它分配一个 VLAN。

所有类型的接口均包括最大数量的组合接口；例如， VLAN、物理、冗余和网桥组接口。在配置中定义的每个 **interface** 均根据此限制进行计数。

准则和限制

本节包括此功能的准则和限制。

防火墙模式准则

- 对于透明模式，您可以配置多达 8 个网桥组。
- 每个网桥组最多可包括 4 个接口。

故障转移准则

- 如果将冗余接口用作故障转移链路，则必须在故障转移对中的两台设备上对其进行预配置；由于*故障转移链路本身需用于复制*，因此，您不能在主要设备上对其进行配置，也不能期望将其复制到次要设备。
- 如果将冗余接口用于状态链路，无需特别配置；该配置可照常从主要设备复制。
- 请务必引用逻辑冗余接口名称。如果主用成员接口故障转移到备用接口，监控设备级故障转移时，本活动不导致冗余接口故障。只有当所有物理接口均发生故障时，冗余接口才会发生故障。
- 不能与数据接口共享一个故障转移接口或状态接口。

冗余接口准则

- 最多可以配置 8 个冗余接口对。
- 所有 ASA 配置均引用逻辑冗余接口，而不是成员物理接口。
- 如果关闭主用接口，则将激活备用接口。
- 冗余接口不能设置为仅管理。
- 有关故障转移准则，请参阅第 11-6 页的故障转移准则。

默认设置

本节列出了接口的默认设置 （如果没有出厂默认配置）。有关出厂默认配置的信息，请参阅第 2-14 页的出厂默认配置。

接口的默认状态

- 物理接口 - 已禁用。
- 冗余接口 - 已启用。但是，对于通过冗余接口的流量，还必须启用成员物理接口。
- 子接口 - 已启用。但是，对于通过子接口的流量，还必须启用物理接口。

默认速度和双工

- 默认情况下，接口的速度和双工设置为自动协商。

默认 MAC 地址

默认情况下，物理接口使用烧录 MAC 地址，物理接口的所有子接口均使用相同的烧录 MAC 地址。

默认 vNIC

所有接口均使用 E1000 仿真。

开始接口配置 (ASAv)

开始接口配置的任务流程

要开始配置接口，请执行以下步骤：

步骤 1　启用物理接口，或者更改以太网参数。请参阅第 11-8 页的启用物理接口并配置以太网参数。

默认情况下，物理接口已禁用。

步骤 2　（可选）配置冗余接口对。请参阅第 11-10 页的配置冗余接口。

逻辑冗余接口将一个主用接口和一个备用物理接口进行配对。如果主用接口发生故障，备用接口将激活并开始传输流量。

步骤 3　（可选）配置 VLAN 子接口。请参阅第 11-12 页的配置 VLAN 子接口和 802.1Q 中继。

步骤 4　（可选）根据第 11-14 页的启用巨型帧支持启用巨型帧支持。

启用物理接口并配置以太网参数

本节介绍如何执行以下操作：

- 启用物理接口
- 设置特定速度和双工
- 为流量控制启用暂停帧

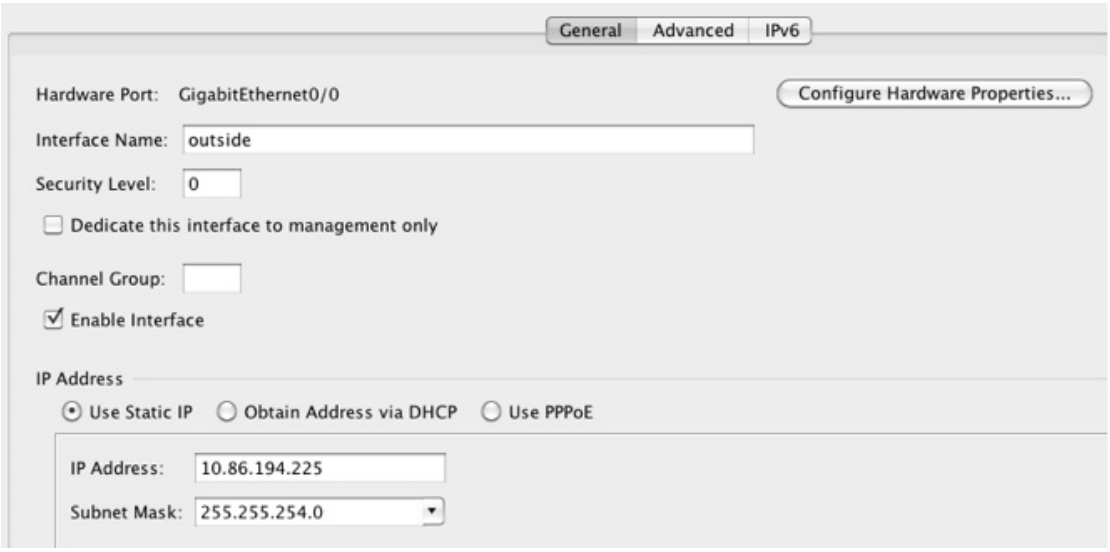
详细步骤

步骤 1　选择 **Configuration > Device Setup > 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。



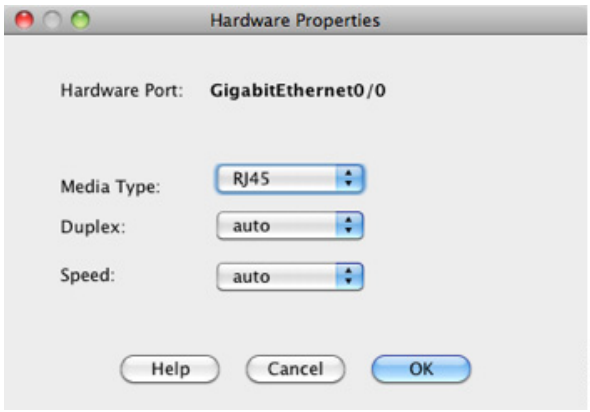
注　此操作步骤仅涉及 Edit Interface 对话框上参数的子集；要配置其他参数，请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”

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（不包括回车键）。例如，对于故障转移或状态链路，说明固定为“LAN Failover Interface”、“STATE Failover Interface”或“LAN/STATE Failover Interface”。无法编辑该说明。如将此接口设为故障转移或状态链路，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**。



注　媒体类型始终为 RJ - 45。

a. 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）。

b. 要设置速度，请从 Speed 下拉列表中选择一个值。

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

d. 要为流量控制启用暂停 (XOFF) 帧，请选中 **Enable Pause Frame** 复选框。

如果存在流量突发，则当突发超过 NIC 上 FIFO 缓冲区和接收环形缓冲区上的缓冲容量时，将丢弃数据包。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 24 KB；该值可以设置在 0 至 47 KB 之间。发送暂停后，如果缓冲区使用率降低至低于低水位标记，则可发送 XON 帧。默认情况下，*low_water* 值为 16 KB；该值可以设置在 0 至 47 KB 之间。收到 XON 之后，或者 XOFF 到期后，链路伙伴可恢复流量，但受暂停帧中的计时器值控制。默认的 *pause_time* 值为 26624；可以将此值设置为介于 0 到 65535 之间的值。如果缓冲区使用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　系统仅支持 802.3x 中定义的流量控制帧。系统不支持基于优先级的流量控制。

步骤 6　点击 **OK** 以接受接口更改。

后续操作

可选任务：

- 配置冗余接口对。请参阅第 11-10 页的配置冗余接口。
- 配置 VLAN 子接口。请参阅第 11-12 页的配置 VLAN 子接口和 802.1Q 中继。
- 配置巨型帧支持。请参阅第 11-14 页的启用巨型帧支持。

必需执行的任务：

- 完成接口配置。请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”

配置冗余接口

一个逻辑冗余接口包括一对物理接口：主用和备用接口。如果主用接口发生故障，备用接口将激活并开始传输流量。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转移，如有必要，可以配置冗余接口以及故障转移。

本节介绍如何配置冗余接口。

配置冗余接口

本节介绍如何创建冗余接口。默认情况下，冗余接口已启用。

准则和限制

- 最多可以配置 8 个冗余接口对。
- 冗余接口延迟值可配置，但在默认情况下， ASA 根据其成员接口的物理类型继承默认延迟值。
- 另请参阅第 11-7 页的冗余接口准则。

先决条件

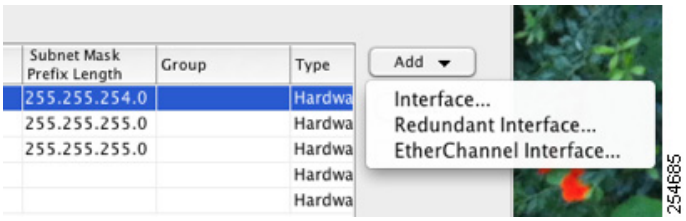
- 两个成员接口必须为相同的物理类型。例如，两个都必须是千兆以太网接口。
- 不能将已配置了名称的物理接口添加到冗余接口。若要这样做，必须先在 Configuration > Device Setup > Interfaces 窗格中移除名称。

注意事项　如果使用已在配置中的物理接口，移除该接口的名称将会清除引用该接口的任何配置。

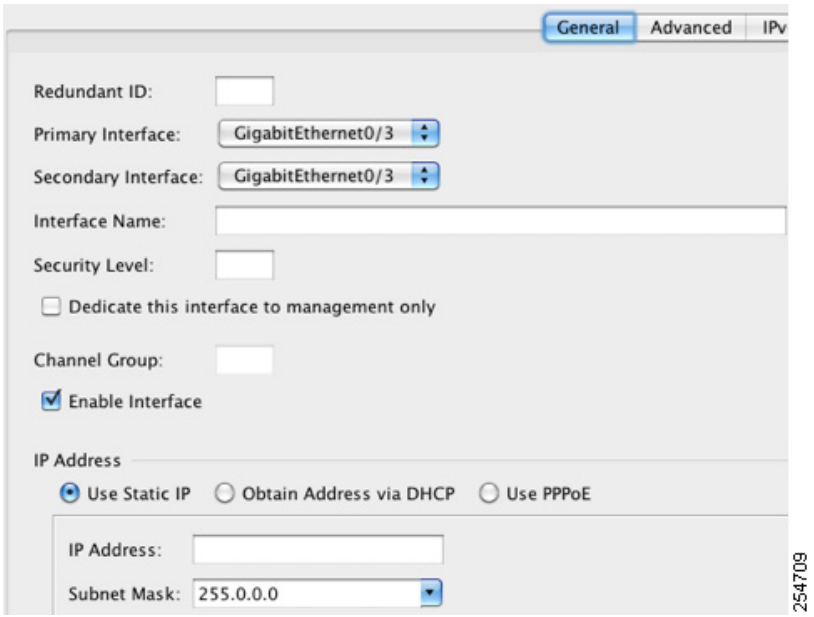
详细步骤

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

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



系统将显示 Add Redundant Interface 对话框。



注　此操作步骤仅涉及 Edit Redundant Interface 对话框参数的子集；要配置其他参数，请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”。

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

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

请务必选择没有子接口而且未分配给情景的接口。

步骤 5　从 Secondary Interface 下拉列表中，选择要设置为次要接口的物理接口。

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

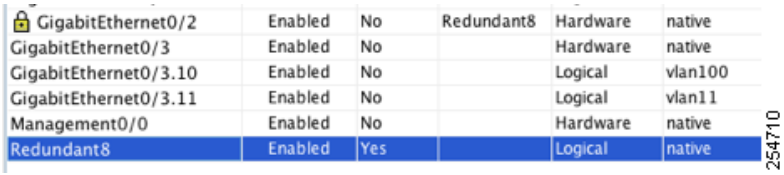
默认情况下，该接口已启用。要禁用该接口，请取消选中此复选框。

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 （不包括回车键）。例如，对于故障转移或状态链路，说明固定为 “LAN Failover Interface”、“STATE Failover Interface” 或 “LAN/STATE Failover Interface”。无法编辑该说明。如将此接口设为故障转移或状态链路，则固定说明将覆盖在此处输入的任何说明。

步骤 8　点击 **OK**。

将返回 Interfaces 窗格。现在成员接口在接口 ID 左侧显示锁定，表明只可以为其配置基本参数。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

后续操作

可选任务：

- 配置 VLAN 子接口。请参阅第 11-12 页的配置 VLAN 子接口和 802.1Q 中继。
- 配置巨型帧支持。请参阅第 11-14 页的启用巨型帧支持。

必需执行的任务：

- 完成接口配置。请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”

更改主用接口

默认情况下，主用接口 （如果有）是配置中列出的第一个接口。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 redundant*number* **detail | grep Member**

例如：

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

要更改主用接口，请输入以下命令：

redundant-interface redundant*number* **active-member** *physical_interface*

其中， **redundant***number* 参数是冗余接口 ID，例如 **redundant1**。

physical_interface 是想激活的成员接口 ID。

配置 VLAN 子接口和 802.1Q 中继

子接口可将物理或冗余接口划分为用不同 VLAN ID 标记的多个逻辑接口。具有一个或多个 VLAN 子接口的接口被自动配置为 802.1Q 中继。由于 VLAN 可将流量分开保持在特定的物理接口上，您可以增加网络可用的接口数，而无需添加额外的物理接口或 ASA。

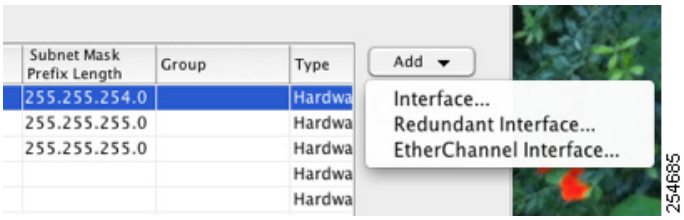
准则和限制

- 最大子接口数 - 要确定您的型号可使用多少个 VLAN 子接口，请参阅第 11-6 页的 ASAv 接口的许可要求。
- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常也不想要物理接口传输流量，因为物理接口将传递未标记的数据包。该属性也适用于冗余接口对中的主用物理接口。由于必须启用物理或冗余接口才能使子接口传输流量，因此，请勿为该接口配置名称并，以确保物理或冗余接口不传输流量。如果要让物理或冗余接口传递未标记数据包，则可照常配置 name 。有关完成接口配置的详细信息，请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”。

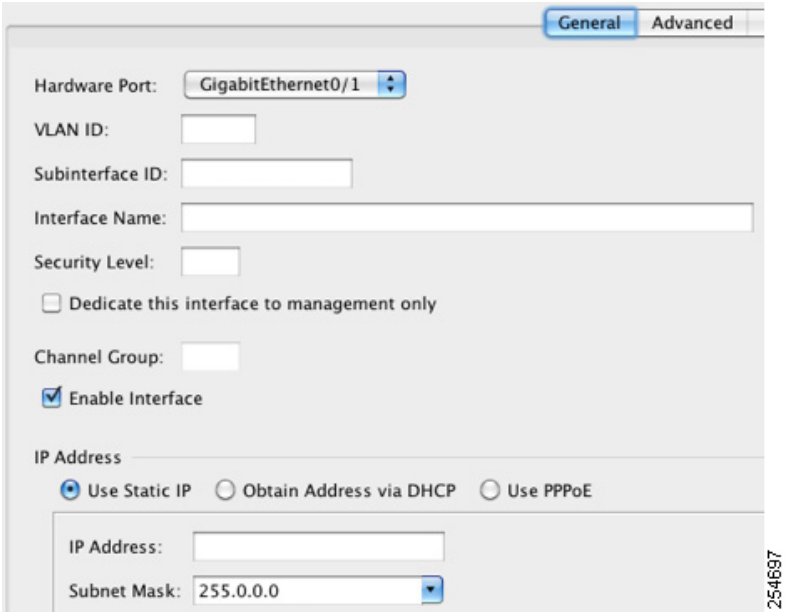
详细步骤

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

步骤 2　选择 **Add > Interface**。



系统将显示 Add Interface 对话框。



注　此操作步骤仅涉及 Edit Interface 对话框上参数的子集；要配置其他参数，请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”

步骤 3　从 Hardware Port 下拉列表中，选择要将子接口添加到的物理或冗余接口。

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。要禁用该接口，请取消选中此复选框。

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

某些 VLAN ID 可能保留在连接的交换机上，因此，请检查交换机文档了解详细信息。

步骤 6　在 Subinterface ID 字段中，请输入介于 1 与 4294967293 之间的整数作为子接口 ID。

允许的子接口数量因平台而异。此 ID 一旦设置便不可更改。

步骤 7　（可选）在 Description 字段中，输入该接口的说明。

一行说明最多可包含 240 个字符 （不包括回车键）。例如，对于故障转移或状态链路，说明固定为 “LAN Failover Interface”、“STATE Failover Interface” 或 “LAN/STATE Failover Interface”。无法编辑该说明。如将此接口设为故障转移或状态链路，则固定说明将覆盖在此处输入的任何说明。

步骤 8　点击 **OK**。

将返回 Interfaces 窗格。

后续操作

可选任务：

- 配置巨型帧支持。请参阅第 11-14 页的启用巨型帧支持。

必需执行的任务：

- 完成接口配置。请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”

启用巨型帧支持

巨型帧是指大于标准最大字节数 （1518 字节）的以太网数据包 （包括第 2 层报头和 FCS），最大可达 9216 字节。可通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配更多内存可能会限制对其他功能的最充分利用，如 ACL。有关详细信息，请参阅第 11-4 页的用最大传输单元、 TCP 最大分段大小控制分片。

先决条件

- 如果更改此设置，需要重新加载 ASA。
- 请务必不需要传输巨型帧的每个接口将 MTU 设为大于 1500 的值；例如，将该值设置为 9000。请参阅第 12-10 页的配置 MAC 地址、 MTU 和 TCP MSS。
- 请务必调整 TCP MSS，或禁止将其用于非，或根据第 12-10 页的配置 MAC 地址、 MTU 和 TCP MSS 按照 MTU 予将其递增。

详细步骤

将 MTU 设置为大于 1500 字节将自动启用巨型帧。要手动启用或禁用该设置，请选择 **Configuration > Device Setup > Interfaces**，并点击 **Enable jumbo frame support** 复选框。

后续操作

完成接口配置。请参阅第 12 章，“路由模式接口”或第 13 章，“透明模式接口”

监控接口

ARP 表

Monitoring > Interfaces > ARP Table 窗格显示 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。

字段

- Interface - 列出与映射关联的接口名称。
- IP Address - 显示 IP 地址 。
- MAC Address - 显示 MAC 地址。
- Proxy ARP - 代理 ARP 在接口上启用时，显示 Yes。代理 ARP 未在接口上启用时，则显示 No。
- Clear - 清除动态 ARP 表条目。静态条目不会被清除。
- Refresh - 使用来自 ASA 的当前信息刷新表，并更新 Last Updated 日期和时间。
- Last Updated - *仅显示*。表明显示更新的日期和时间。

MAC 地址表

Monitoring > Interfaces > MAC Address Table 窗格显示静态和动态 MAC 地址条目。有关 MAC 地址表和添加静态条目的详细信息，请参阅第 11-15 页的 MAC 地址表。

字段

- Interface - 显示与条目关联的接口名称。
- MAC Address - 显示 MAC 地址。
- Type - 显示条目为静态或动态。
- Age - 显示条目的持续时间 （以分钟为单位）。要设置超时，请参阅第 11-15 页的 MAC 地址表。
- Refresh - 使用来自 ASA 的当前信息刷新表格。

接口图形

在 Monitoring > Interfaces > Interface Graphs 窗格中，您可以以图形或表格的形式查看接口统计信息。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。

字段

- Available Graphs for - 列出可用于监控的统计信息的类型。一个图形窗格中可显示多达四种统计数据。您可以同时打开多个图形窗格。
  - Byte Counts - 显示接口上输入和输出的字节数。
  - Packet Counts - 显示接口上输入和输出的数据包数。
  - Packet Rates - 显示接口上输入和输出数据包的速率。
  - Bit Rates - 显示接口输入和输出的比特率。
  - Drop Packet Count - 显示接口上丢弃的数据包数。

  为物理接口显示以下附加统计信息：
  - Buffer Resources - 显示以下统计信息：

    Overruns - 由于输入速率超过 ASA 处理数据的能力， ASA 无法将收到的数据转交给硬件缓冲区的次数。

    Underruns - 发射器运行速度比 ASA 处理速度更快的次数。

    No Buffer - 收到因主系统没有缓冲区空间而丢弃的数据包的次数。将该次数与忽略的计数进行比较。以太网络中的广播风暴常常导致无输入缓冲区事件。
  - Packet Errors - 显示以下统计信息：

    CRC - 循环冗余校验错误数。如果一个工作站发送帧，它会在帧尾附加一个 CRC。该 CRC 根据帧中的数据由算法生成。如果修改源和目标之间的帧，则 ASA 将提示 CRC 不匹配。大量的 CRC 通常由冲突或发送错误数据的工作站引起。

    Frame - 帧错误数量。坏帧包括长度不正确或帧校验和错误的数据包。此错误通常由冲突或以太网设备故障引起。

    Input Errors - 输入错误的总数，包括此处列出的其他类型。与输入相关的其他错误也可能导致输入错误计数增加，而且一些数据报可能存在多个错误；因此，这个总数可能超过列出的其他类型的错误次数。

    Runts - 因小于 64 字节的最小数据包大小而被丢弃的数据包数。超短帧通常由冲突引起。也可能由布线不当和电气干扰引起。

    Giants - 因超过最大数据包大小而被丢弃的数据包数。例如，大于 1518 字节的所有以太网数据包均被视为超长帧。

    Deferred - 仅用于 FastEthernet 接口。因链路上的活动而导致在传输之前被延迟的帧数。
  - Miscellaneous - 显示已接收广播的统计信息。
  - Collision Counts - 仅用于 FastEthernet 接口。显示以下统计信息：

    Output Errors - 由于超过了已配置的最大冲突数而未传输的帧数。只有在网络流量过大时，该计数器才会递增。

    Collisions - 由于以太网冲突 （单一和多个冲突）而重新传输的消息数。这种情况通常出现在被过度扩展的 LAN 上 （以太网或收发器电缆过长，站点之间存在两个以上的中继器，或级联多端口收发器过多）。发生冲突的数据包仅按输出数据包计数一次。

Late Collisions - 由于正常冲突时窗外发生的冲突而未传输的帧数。延迟冲突是在数据包传输过程中延迟检测到的冲突。通常，这些情况都不会发生。如果两台以太网主机尝试同时通信，它们应在数据包中早就发生冲突且两者都作出让步，或者第二台主机应看到第一台主机正在通信并等待。如果遇到延迟冲突，设备将迅速做出反应并尝试在以太网上发送数据包，而 ASA 只完成了数据包部分发送。ASA 不会重新发送数据包，因为可能已经释放了储存数据包第一部分的缓冲区。这实际上不是个问题，因为网络协议专门用于通过重新发送数据包来解决冲突。但是，发生延迟冲突表明网络中存在问题。常见问题包括超出规格范围运行的大型重复网络和以太网络。

- Input Queue - 显示输入队列中的数据包数（当前和最大数据包数），包括以下统计信息：

  Hardware Input Queue - 硬件队列中的数据包数。

  Software Input Queue - 软件队列中的数据包数。

- Output Queue - 显示输出队列中的数据包数（当前和最大数据包数），包括以下统计信息：

  Hardware Output Queue - 硬件队列中的数据包数。

  Software Output Queue - 软件队列中的数据包数。

- Add - 将选定的统计信息类型添加到选定的图形窗格。
- Remove - 从选定的图形窗格中移除选定的统计信息类型。如果您正在移除的项目是从另一个窗格添加的，并且未返回 Available Graphs 窗格，该按钮名称将更改为 Delete。
- Show Graphs - 显示要添加统计类型的图形窗格名称。如果您已经打开了某个图形窗格，默认情况下，将列出新的图形窗格。如果要将统计类型添加到一个已经打开的图形，请选择已经打开的图形窗格名称。 Selected Graphs 窗格将显示图形中已包括的统计信息，您也可以添加其他类型到该窗格。图形窗格为 ASDM 命名，后接接口 IP 地址和名称 “Graph”。后续图形命名为 “Graph (2)”，依此类推。
- Selected Graphs - 显示要在选定的图形窗格中显示的统计信息类型。最多可包括四种类型：
  - Show Graphs - 显示图形窗格或用额外的统计信息类型（如已添加）更新图形。

图形 / 表格

Monitoring > Interfaces > Interface Graphs > Graph/Table 窗格显示选定统计信息的图形。 Graph 窗格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。如果启用 History Metrics（请参阅第 3-30 页的启用历史度量），则可以查看过去时间段的统计信息。

字段

- View - 设置图形或表格的时间段。要查看任何非实时时间段，请启用 History Metrics（请参阅第 3-30 页的启用历史度量）。数据根据以下选项的规格予以更新：
  - 实时，每隔 10 秒钟更新数据
  - 过去 10 分钟，每隔 10 秒钟更新数据
  - 过去 60 分钟，每隔 1 分钟更新数据
  - 过去 12 小时，每隔 12 分钟更新数据
  - 过去 5 天，每隔 2 小时更新数据
- Export - 以逗号分隔值的形式导出图形。如果 Graph 窗格中有多个图形或表格，系统将显示 Export Graph Data 对话框。选中名称旁边的复选框，即可选择列出的一个或多个图形和表格。
- Print - 打印图形或表格。如果 Graph 窗格中有多个图形或表格，系统将显示 Print Graph 对话框。从 Graph/Table Name 列表中选择要打印的图形或表格。
- Bookmark - 通过 Graphs 窗格上所有图形和表格的单个链接，以及通过每个图形或表格的单独链接打开一个浏览器窗口。您可以将这些 URL 复制为浏览器书签。打开图形 URL 时，ASDM 不一定在运行；浏览器将启动 ASDM 并显示图形。

后续操作

根据第 12 章，“路由模式接口”或第 13 章，“透明模式接口”完成接口配置。

ASAv 接口的功能历史记录

表 11-1　接口的功能历史记录

功能名称	平台版本	功能信息
ASAv 支持	9.2(1)	引入了 ASAv。

路由模式接口

本章包含在路由防火墙模式中为所有型号完成接口配置的任务。

注 对于多情景模式，请在情景执行空间完成本节中的任务。在 Configuration > Device List 窗格中，双击主用设备 IP 地址项下的情景名称。

在路由模式中完成接口配置的相关信息

安全级别

每个接口必须有一个安全级别，范围为 0 （最低）至 100 （最高）。例如，应将最安全的网络（如内部主机网络）指定为级别 100。而连接到互联网的外部网络连接可指定为 0 级。其他网络（如 DMZ）可指定为中间的级别。可将多个接口分配至同一安全级别。有关详细信息，请参阅第 12-16 页的允许同一安全级别通信。

安全级别可控制以下行为：

- 网络访问 - 默认情况下，从安全性较高的接口到安全性较低的接口 （出站）有一个隐式许可。安全性较高接口上的主机可以访问安全性较低接口上的所有主机。可通过将 ACL 应用于接口来限制访问。

  如果为相同安全接口启用通信 （请参阅第 12-16 页的允许同一安全级别通信），则隐式许可就允许这些接口访问安全级别相同或较低的其他接口。

- 检查引擎 - 某些应用检查引擎取决于安全级别。对于相同安全接口，检查引擎适用于任何一个方向的流量。
  - NetBIOS 检查引擎 - 仅适用于出站连接。
  - SQL*Net 检查引擎 - 如果一个主机对之间存在 SQL*Net（以前称为 OraServ）端口的控制连接，则仅允许通过 ASA 进行入站数据连接。
- 过滤 - HTTP(S) 和 FTP 过滤仅适用于出站连接 （从较高级别到较低级别）。

  如果为相同安全接口启用通信，则可以过滤任何一个方向的流量。
- **established** 命令 - 如已建立从安全级别较高主机到安全级别较低主机的连接，则该命令允许连接从安全级别较低主机返回至安全级别较高主机。

  如果为相同安全接口启用通信，则可以为两个方向配置 **established** 命令。

双堆栈 （IPv4 和 IPv6）

思科 ASA 支持在同一接口上配置 IPv6 和 IPv4。您无需输入任何特殊命令来执行此操作；只需按通常的方式输入 IPv4 配置命令和 IPv6 配置命令即可。确保配置一条同时适用于 IPv4 和 IPv6 的默认路由。

在路由模式中完成接口配置的许可要求

型号	许可证要求
ASA 5512-X	VLAN： 基础许可证：50 增强型安全许可证：100 所有类型的接口： 基础许可证：716 增强型安全许可证：916
ASA 5515-X	VLAN： 基础许可证：100 所有类型的接口： 基础许可证：916
ASA 5525-X	VLAN： 基础许可证：200 所有类型的接口： 基础许可证：1316
ASA 5545-X	VLAN： 基础许可证：300 所有类型的接口： 基础许可证：1716

型号	许可证要求
ASA 5555-X	VLAN： 基础许可证：500 所有类型的接口： 基础许可证：2516
ASA 5585-X	VLAN： 基础许可证和增强型安全许可证：1024 SSP-10 和 SSP-20 的接口速度： 基础许可证 - 适用于光纤接口的 1 千兆以太网 10 GE I/O 许可证 （增强型安全许可证） - 适用于光纤接口的 10 千兆以太网 （默认情况下， SSP-40 和 SSP-60 支持 10 千兆以太网。） 所有类型的接口： 基础许可证和增强型安全许可证：4612

注　对于根据 VLAN 限制计数的接口，您必须为它分配一个 VLAN。

所有类型的接口构成最大数量的组合接口；例如， VLAN 接口、物理接口、冗余接口，桥组接口和 EtherChannel 接口。在配置中定义的每个 **interface** 均根据此限制进行计数。

型号	许可证要求
ASASM	VLAN： 基础许可证：1000

准则和限制

本节包括此功能的准则和限制。

情景模式准则

- 对于多情景模式中的 ASA 5512-X 和更高版本，请根据第 10 章，“基本接口配置 （ASA 5512-X 及更高版本）”在系统执行空间中配置物理接口。然后按照本章内容在情景执行空间中配置逻辑接口参数。对于多情景模式中的 ASASM，请按照第 2 章，“适用于思科 ASA 服务模块的交换机配置”配置交换机端口和交换机上的 VLAN，然后为 ASASM 分配 VLAN。

  ASAv 不支持多情景模式。
- 在多情景模式中，只能配置已根据第 7-14 页的配置多情景分配给系统配置中情景的情景接口。
- 多情景模式中不支持 PPPoE。

防火墙模式准则

支持路由防火墙模式。有关透明模式，请参阅第 13 章，“透明模式接口”

故障转移准则

请勿采用本章中的操作步骤完成故障转移接口的配置。要配置故障转移和状态链路，请参阅第 8 章，“通过故障转移实现高可用性”。在多情景模式中，故障转移接口在系统配置中进行配置。

IPv6 准则

支持 IPv6。

适合 ASASM 的 VLAN ID 准则

可向配置中添加任何 VLAN ID，但是，只有通过交换机分配至 ASA 的 VLAN 才能传输流量。要查看分配至 ASA 的所有 VLAN，请使用 **show vlan** 命令。

如果为尚未通过交换机分配至 ASA 的 VLAN 添加接口，则该接口将处于关闭状态。将 VLAN 分配至 ASA 时，接口将更改为可用状态。要获得有关接口状态的详细信息，请使用 **show interface** 命令。

默认设置

本节列出了接口的默认设置 （如果没有出厂默认配置）。有关出厂默认配置的信息，请参阅第 2-14 页的出厂默认配置。

默认安全级别

默认安全级别为 0。如将一个接口指定为 “ 内部 ”，且未明确设置安全级别，则 ASA 将安全级别设置为 100。

注　如果更改接口的安全级别，且不想在使用新安全信息之前等待现有连接超时，则可使用 **clear local-host** 命令清除连接。

ASASM 接口的默认状态

- 在单情景模式或系统执行空间中， VLAN 接口默认启用。
- 在多情景模式中，所有分配的接口均默认启用，无论系统执行空间中接口的状态如何。但是，为使流量通过接口，还必须在系统执行空间中启用接口。如果关闭系统执行空间中的接口，则该接口将在共享它的所有情景中处于关闭状态。

巨型帧支持

默认情况下，ASASM 支持巨型帧。请根据第 12-10 页的配置 MAC 地址、MTU 和 TCP MSS 为所需的数据包大小配置 MTU。

在路由模式中完成接口配置

用于完成接口配置的任务流

步骤 1　根据型号设置接口：

- ASA 5512-X 和更高版本 - 第 10 章，“基本接口配置（ASA 5512-X 及更高版本）”
- ASASM - 第 2 章，“适用于思科 ASA 服务模块的交换机配置”
- ASAv - 第 11 章，“基本接口配置 (ASAv)”

步骤 2　（多情景模式）根据第 7-14 页的配置多情景将接口分配给情景。

步骤 3　（多情景模式）在 Configuration > Device List 窗格中，双击主用设备 IP 地址项下的情景名称。

步骤 4　配置通用接口参数，包括接口名称、安全级别和 IPv4 地址。请参阅第 12-5 页的配置常规接口参数。

步骤 5　（可选）配置 MAC 地址和 MTU。请参阅第 12-10 页的配置 MAC 地址、 MTU 和 TCP MSS。

步骤 6　（可选）配置 IPv6 寻址。请参阅第 12-12 页的配置 IPv6 寻址。

步骤 7　（可选）通过允许两个接口之间的通信，或通过允许流量进入和退出同一接口，来允许相同安全级别通信。请参阅第 12-16 页的允许同一安全级别通信。

配置常规接口参数

此操作步骤介绍如何设置名称、安全级别、 IPv4 地址和其他选项。

对于 ASA 5512-X 和更高版本及 ASAv，必须为以下接口类型配置接口参数：

- 物理接口
- VLAN 子接口
- 冗余接口
- EtherChannel 接口

对于 ASASM，必须为以下接口类型配置接口参数：

- VLAN 接口

准则和限制

如在使用故障转移，请勿使用此操作步骤命名为故障转移和 Stateful Failover 通信预留的接口。要配置故障转移和状态链路，请参阅第 8 章，“通过故障转移实现高可用性”。

限制

- 多情景模式中不支持 PPPoE。
- PPPoE 和 DHCP 在 ASASM 上不受支持。

先决条件

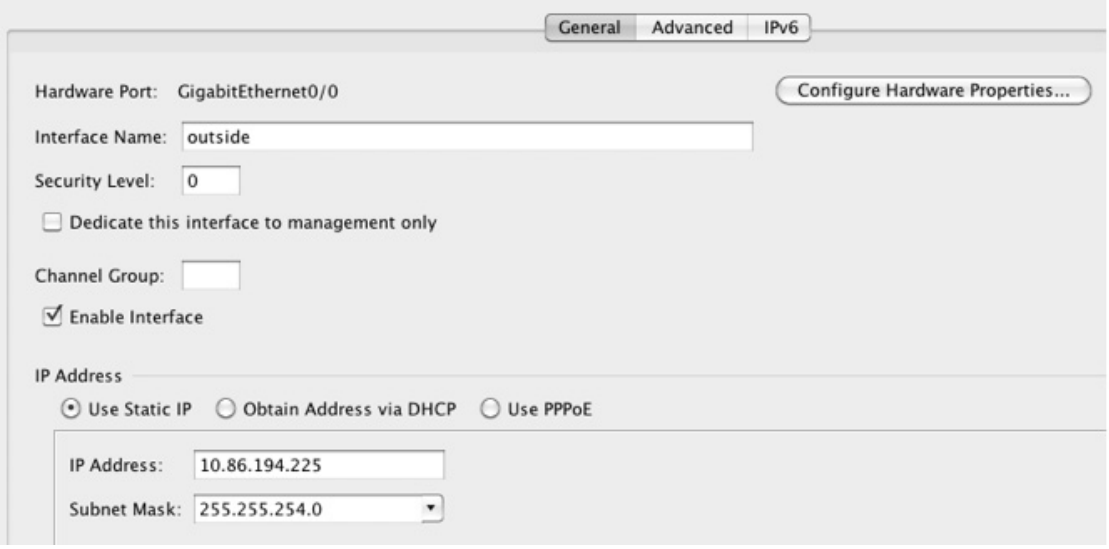
- 根据型号设置接口：
  - ASA 5512-X 和更高版本 - 第 10 章，“基本接口配置 （ASA 5512-X 及更高版本）”
  - ASASM - 第 2 章，“适用于思科 ASA 服务模块的交换机配置”
  - ASAv - 第 11 章，“基本接口配置 (ASAv)”
- 在多情景模式中，只能配置已根据第 7-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。要从系统切换至情景配置，请在 Configuration > Device List 窗格中双击有效设备 IP 地址下的情景名称。

详细步骤

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

步骤 2　选择接口行，然后点击 **Edit**。

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



步骤 3　在 Interface Name 字段中输入名称，最长 48 个字符。

步骤 4　在 Security level 字段中，输入值为 0 （最低）到 100 （最高）的级别。

有关详细信息，请参阅第 12-1 页的安全级别。

步骤 5　（可选；不适用于冗余接口）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。

管理专属接口不接受直通流量。有关 ASA 5585-X 的详细信息，请参阅第 12-6 页的先决条件。

（ASA 5512-X 到 ASA 5555-X）您无法在管理 0/0 接口上禁用此选项。

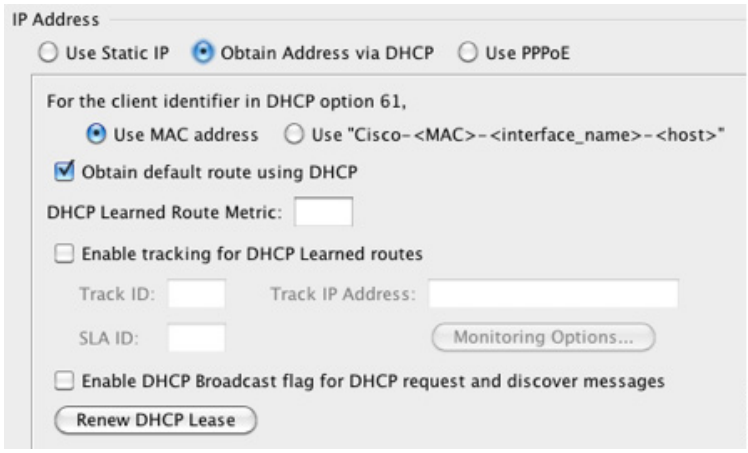
注　Channel Group 字段为只读字段，指明该接口是否为 EtherChannel 的一部分。

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，选择下列选项之一。

注　用于故障转移时，您必须手动设置 IP 地址和备用地址；不支持 DHCP 和 PPPoE。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 地址未纳入 DHCP 请求数据包中，则将不分配 IP 地址。

b. 要使用为选项 61 生成的字符串，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）要指定到获悉路由的管理距离，请在 DHCP Learned Route Metric 字段中输入一个介于 1 和 255 之间的值。如果将此字段留空，则获悉路由的管理距离为 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 - 输入跟踪目标的 IP 地址。通常，这是路由的下一跳网关的 IP 地址，但也可能是接口上可用的任何网络对象。

注　路由跟踪仅在单一路由模式中可用。

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

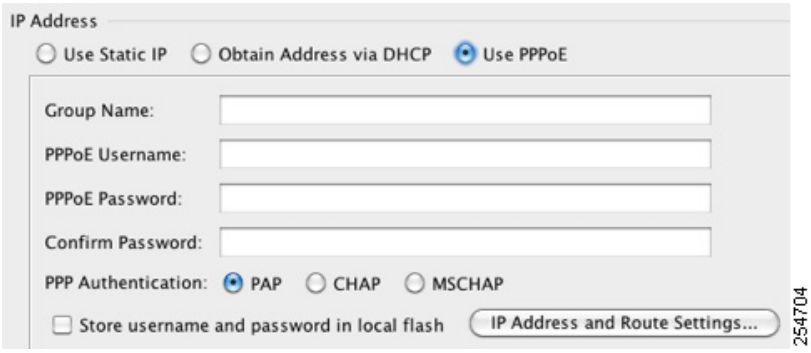
Monitor Options - 点击此按钮，打开 Route Monitoring Options 对话框。在 Route Monitoring Options 对话框中，您可以配置跟踪对象监控进程的参数。

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**。

如果广播标记已设为 1，则 DHCP 服务器将侦听该标记并广播回复数据包。

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输明文用户名和密码，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 CHAP 不加密数据。MSCHAP 与 CHAP 类似，但比 CHAP 更加安全，因为服务器只对加密密码进行存储和比较，而 CHAP 使用的是明文密码。 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 中的特定位置。如果某台自动更新服务器将 **clear configure** 命令发送到 ASA，接着连接中断，则 ASA 可以从 NVRAM 读取用户名和密码，并重新验证访问集中器。

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。有关详细信息，请参阅第 12-9 页的 PPPoE IP 地址和路由设置。

步骤 8　（可选）在 Description 字段中，输入该接口的说明。

一行说明最多可包含 240 个字符 （不包括回车键）。例如，对于故障转移或状态链路，说明固定为 “LAN Failover Interface”、“STATE Failover Interface” 或 “LAN/STATE Failover Interface”。无法编辑该说明。如将此接口设为故障转移或状态链路，则固定说明将覆盖在此处输入的任何说明。

注　（ASA 5512-X 以及更高版本）有关 Configure Hardware Properties 按钮的详细信息，请参阅第 10-12 页的启用物理接口并配置以太网参数。

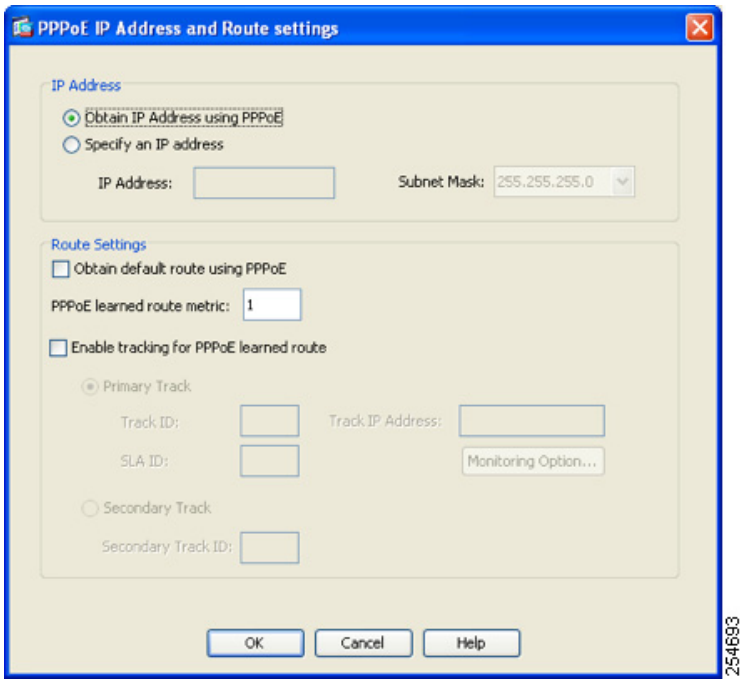
步骤 9　点击 **OK**。

后续操作

- （可选）配置 MAC 地址和 MTU。请参阅第 12-10 页的配置 MAC 地址、 MTU 和 TCP MSS。
- （可选）配置 IPv6 寻址。请参阅第 12-12 页的配置 IPv6 寻址。

PPPoE IP 地址和路由设置

您可以使用 Configuration > Interfaces > Add/Edit Interface > General > PPPoE IP Address and Route Settings > PPPoE IP Address and Route Settings 对话框，选择用于 PPPoE 连接的寻址和跟踪选项。



字段

- IP Address area - 选择使用 PPP 获取 IP 地址或指定 IP 地址，包含以下字段：
  - Obtain IP Address using PPP - 选择启用 ASA 来使用 PPP 获取 IP 地址。
  - Specify an IP Address - 指定 ASA 将使用的 IP 地址和掩码，而不是与 PPPoE 服务器协商从而动态分配地址。
- Route Settings Area - 配置路由和跟踪设置，包含以下字段：
  - 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 - 为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，则获悉路由的管理距离为 1。
  - Enable tracking - 选中此复选框为通过 PPPoE 获悉的路由启用路由跟踪。

注　路由跟踪仅在单一路由模式中可用。

- Primary Track - 选择此选项以配置主要 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 - 输入跟踪目标的 IP 地址。通常，这是路由的下一跳网关的 IP 地址，但也可能是接口上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，打开 Route Monitoring Options 对话框。在 Route Monitoring Options 对话框中，您可以配置跟踪对象监控进程的参数。
- Primary Track - 选择此选项以配置辅助 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。

配置 MAC 地址、 MTU 和 TCP MSS

本节介绍如何为接口配置 MAC 地址及如何设置 MTU 和 TCP MSS。

有关 MAC 地址的信息

默认情况下，物理接口使用烧录 MAC 地址，物理接口的所有子接口均使用相同的烧录 MAC 地址。

对于 ASASM，所有 VLAN 使用背板提供的同一个 MAC 地址。

冗余接口使用您添加的第一个物理接口的 MAC 地址。如果在配置中更改成员接口的顺序，则 MAC 地址发生更改，以匹配现第一个列出的接口的 MAC 地址。如果使用此命令将一个 MAC 地址分配给冗余接口，则无论成员接口 MAC 地址如何，均将使用该分配的 MAC 地址。

对于 EtherChannel，属于通道组的所有接口均共享相同 MAC 地址。该功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；他们不知道单个链路。端口通道接口使用编号最小的通道组接口 MAC 地址作为端口通道 MAC 地址。或者，您可以为端口通道接口手动配置 MAC 地址。在多情景模式中，可将唯一 MAC 地址自动分配给各个接口，包括 EtherChannel 端口接口。在组通道接口成员资格发生变化的情况下，我们建议手动或（在多情景模式中）自动配置唯一的 MAC 地址。如果移除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址更改至下一个编号最小的接口，从而导致流量中断。

在多情景模式中，如果在情景之间共享接口，则可将唯一 MAC 地址分配给每个情景的接口。借助于此功能， ASA 可轻松地将数据包分类到适当的情景中。可使用没有唯一 MAC 地址的共享接口，但受到一些限制。有关详细信息，请参阅第 7-3 页的 ASA 如何对数据包分类。可手动分配每个 MAC 地址，或者也可为情景中共享接口自动生成 MAC 地址。要自动生成 MAC 地址，请参阅第 7-22 页的自动为情景接口分配 MAC 地址。如果自动生成 MAC 地址，则可使用此操作步骤覆盖生成的地址。

对于单情景模式，或对于不在多情景模式中共享的接口，您可能要向子接口分配唯一 MAC 地址。例如，您的服务提供商可能根据 MAC 地址执行访问控制。

关于 MTU 和 TCP MSS 的信息

请参阅第 10-6 页的用最大传输单元、 TCP 最大分段大小控制分片。

先决条件

- 根据型号设置接口：
  - ASA 5512-X 和更高版本 - 第 10 章，“基本接口配置 （ASA 5512-X 及更高版本）”
  - ASASM - 第 2 章，“适用于思科 ASA 服务模块的交换机配置”
  - ASAv - 第 11 章，“基本接口配置 (ASAv)”
- 在多情景模式中，只能配置已根据第 7-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。要从系统切换至情景配置，请在 Configuration > Device List 窗格中双击有效设备 IP 地址下的情景名称。

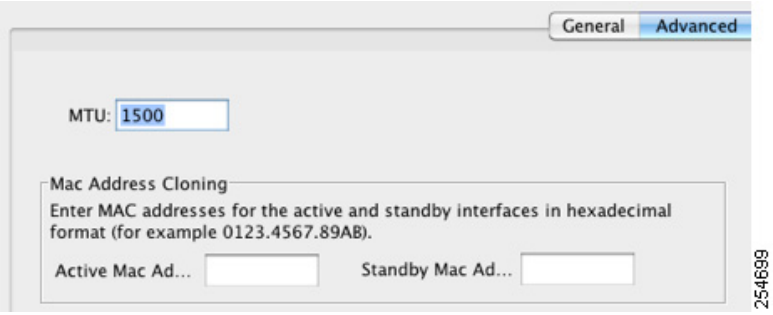
详细步骤

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

步骤 2　选择接口行，然后点击 **Edit**。

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

步骤 3　点击 **Advanced** 选项卡。



步骤 4　要设置 MTU 或启用巨型帧支持 （仅限受支持的型号），请在 MTU 字段输入 300 与 9198 字节之间的数值 （对于 ASAv，为 9000）。

默认值为 1500 字节。

注　为冗余或端口通道接口设置 MTU 时， ASA 将设置应用于所有成员接口。

- 对于在单情景模式中支持句型帧的型号 - 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型帧支持。如将所有接口的 MTU 值均设置回小于 1500 的值，则将禁用巨型帧支持。
- 对于在多情景模式中支持句型帧的型号 - 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型帧支持。请参阅第 10-25 页的启用巨型帧支持。

注　启用或禁用巨型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。如果您还想使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。

步骤 6　如果使用故障转移，请在 Standby Mac Address 字段输入备用 MAC 地址。如果主用设备发生故障转移，且备用设备变为主用设备，则新的主用设备开始使用有效 MAC 地址，以最大限度地减少网络中断，同时，原来的主用设备使用备用地址。

步骤 7　要设置 TCP MSS，请选择 **Configuration > Firewall > Advanced > TCP Options**。设置以下选项：

- Force Maximum Segment Size for TCP - 将最大 TCP 分段大小设置为介于 48 与任何最大数值之间的字节数。默认值为 1380 字节。可禁用此功能，只需将字节数设置为 0。
- Force Minimum Segment Size for TCP - 覆盖最大分段大小，使其不小于已设置的字节数，介于 48 至任何最大数值之间。此功能默认已禁用 （设置为 0）。

步骤 8　有关 **Secure Group Tagging**，请参阅第 33-20 页的启用 SGT plus Ethernet Tagging。

后续操作

（可选）配置 IPv6 寻址。请参阅第 12-12 页的配置 IPv6 寻址。

配置 IPv6 寻址

本节介绍如何配置 IPv6 寻址。

有关 IPv6 的信息

本节包括有关如何配置 IPv6 的信息。

IPv6 寻址

可为 IPv6 配置两种类型的单播地址：

- 全局 - 全局地址是可在公用网络上使用的公用地址。
- 本地链路 - 本地链路地址是只能在直连网络上使用的专用地址。路由器不使用本地链路地址转发数据包；它们仅用于在特定物理网段上通信。它们可用于执行地址配置或 ND 功能，如地址解析和邻居发现。

至少需要配置本地链路地址， IPv6 才会起作用。如果您配置了全局地址，则接口上会自动配置本地链路地址，因此您无需专门配置本地链路地址。如果不配置全局地址，则需要自动或手动配置本地链路地址。

Modified EUI-64 接口 ID

RFC 3513：互联网协议第 6 版 (IPv6) 寻址架构要求所有单播 IPv6 地址 （以二进制值 000 开头的地址除外）的接口标识符部分长度为 64 位，结构格式为 Modified EUI-64 格式。ASA 可为连接到本地链路的主机强制执行该要求。

在接口上启用此功能时，该接口接收的 IPv6 数据包源地址将根据源 MAC 地址进行验证，以确保接口标识符使用 Modified EUI-64 格式。如果 IPv6 数据包不将 Modified EUI - 64 格式用于接口标识符，则将丢弃数据包，并生成以下系统日志消息：

```
%ASA-3-325003: EUI-64 source address check failed.
```

只有在创建流量时才能执行地址格式验证。不检查来自现有流量的数据包。此外，只能对本地链路上的主机执行地址验证。从路由器后面的主机接收的数据包将无法通过地址格式验证，且被丢弃，因为它们的源 MAC 地址将为路由器 MAC 地址，而不是主机 MAC 地址。

配置全局 IPv6 地址

要配置全局 IPv6 地址，请执行以下步骤。

注　配置全局地址将自动配置本地链路地址，因此，无需另行配置它。

限制

ASA 不支持 IPv6 任播地址。

先决条件

- 根据型号设置接口：
  - ASA 5512-X 和更高版本 - 第 10 章，“ 基本接口配置 （ASA 5512-X 及更高版本） ”
  - ASASM - 第 2 章，“ 适用于思科 ASA 服务模块的交换机配置 ”
  - ASAv - 第 11 章，“ 基本接口配置 (ASAv)”
- 在多情景模式中，只能配置已根据第 7-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。要从系统切换至情景配置，请在 Configuration > Device List 窗格中双击有效设备 IP 地址下的情景名称。

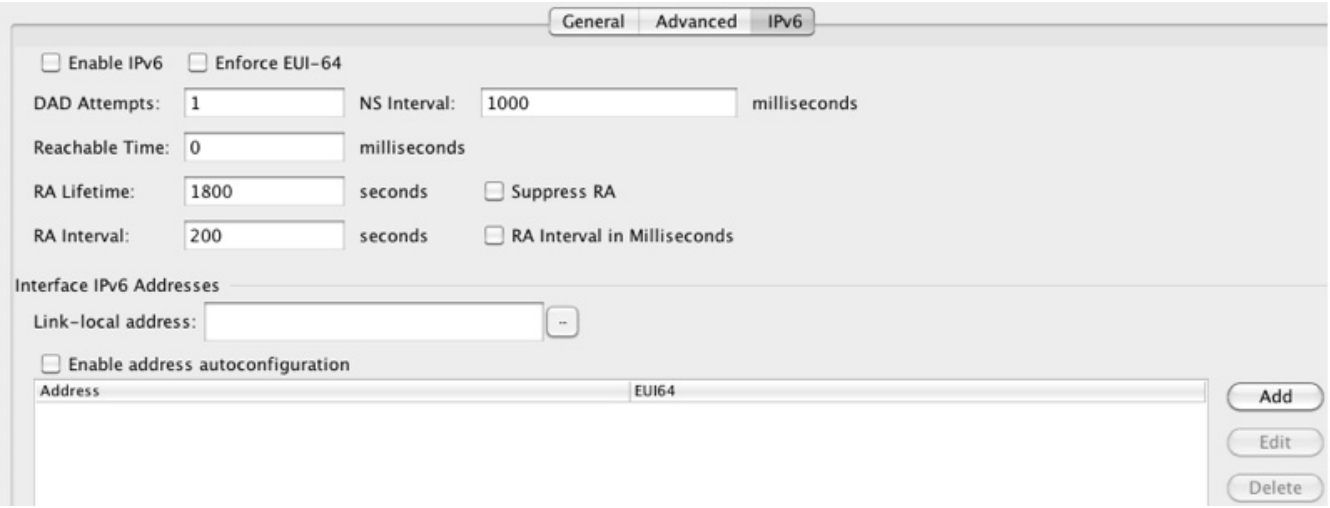
详细步骤

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

步骤 2　选择接口，然后点击 **Edit**。

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

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 Modified EUI-64 格式的接口标识符，请选中 **Enforce EUI-64** 复选框。

有关详细信息，请参阅第 12-13 页的 Modified EUI-64 接口 ID。

步骤 6　（可选）在顶部区域，通过参考第 26 章，“IPv6 邻居发现”自定义 IPv6 配置。

步骤 7　使用以下方法之一，配置全局 IPv6 地址。

- 无状态自动配置 - 在 Interface IPv6 Addresses 区域，选中 **Enable address autoconfiguration** 复选框。

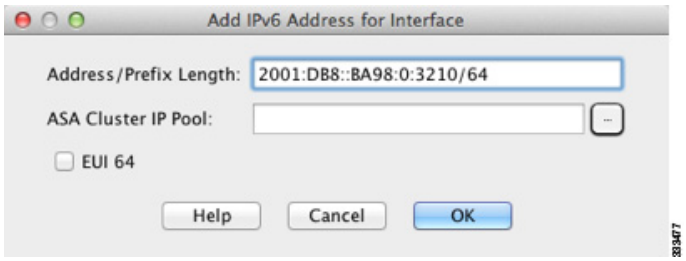
  在接口上启用无状态自动配置时，将基于 Router Advertisement 消息中接收到的前缀来配置 IPv6 地址。启用无状态自动配置时，将基于修改的 EUI-64 接口 ID，自动生成接口的本地链路地址。

  注　尽管 RFC 4862 明确要求配置为无状态自动配置的主机不发送 Router Advertisement 消息，但在此情况下，ASA 实际上会发送 Router Advertisement 消息。请查看 **Suppress RA chck box** 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，输入完整的全局 IPv6 地址 （包括接口 ID），或输入 IPv6 前缀以及 IPv6 前缀的长度。如果您只输入前缀，请务必选中 **EUI 64** 复选框，以采用修改的 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）。有关 IPv6 寻址的详细信息，请参阅第 43-4 页的 IPv6 地址。

注　有关 ASA 集群 IP 池的详细信息，请参阅第 9-38 页的配置独立接口 （管理接口的推荐配置）。

c. 点击 **OK**。

步骤 8　（可选）要配置 IPv6 路由器通告中包含的 IPv6 前缀，请参阅第 26-10 页的配置路由器通告中的 IPv6 前缀。

步骤 9　点击 **OK**。

系统将返回 Configuration > Device Setup > Interfaces 窗格。

配置 IPv6 邻居发现

要配置 IPv6 邻居发现，请参阅第 26 章， “IPv6 邻居发现 ”。

（可选）自动配置本地链路地址

如果不想要配置全局地址，且只需配置本地链路地址，则可以选择根据接口 MAC 地址生成本地链路地址 （Modified EUI-64 格式。由于 MAC 地址使用 48 位，因此，必须插入额外的位数，以填充接口 ID 所需的 64 位。）

要手动分配本地链路地址 （不推荐），请参阅第 12-16 页的 （可选）手动配置本地链路地址。

有关其他 IPv6 选项，包括强制执行 Modified EUI-64 格式和 DAD 设置，请参阅第 12-13 页的配置全局 IPv6 地址。

要自动配置接口的本地链路地址，请执行以下步骤：

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

步骤 2　选择接口，然后点击 **Edit**。

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

步骤 3　点击 **IPv6** 选项卡。

步骤 4　在 IPv6 配置区域，选中 **Enable IPv6** 复选框。

此选项启用 IPv6，并且根据接口 MAC 地址采用修改的 EUI-64 格式自动生成本地链路地址。

步骤 5　点击 **OK**。

（可选）手动配置本地链路地址

如果您不想配置全局地址，而且只需配置本地链路地址，您可以选择手动定义本地链路地址。请注意，我们建议根据 Modified EUI-64 格式自动分配本地链路地址。例如，如果其他设备强制使用 Modified EUI-64 格式，则手动分配的本地链路地址可能导致数据包被丢弃。

要自动分配本地链路地址 （推荐），请参阅第 12-15 页的 （可选）自动配置本地链路地址。

有关其他 IPv6 选项，包括强制执行 Modified EUI-64 格式和 DAD 设置，请参阅第 12-13 页的配置全局 IPv6 地址。

要为接口分配本地链路地址，请执行以下步骤：

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

步骤 2　选择接口，然后点击 **Edit**。

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

步骤 3　点击 **IPv6** 选项卡。

步骤 4　要设置本地链路地址，请在 Link-local address 字段中输入地址。

本地链路地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。 有关 IPv6 寻址的详细信息，请参阅第 43-4 页的 IPv6 地址。

步骤 5　点击 **OK**。

允许同一安全级别通信

默认情况下，同一个安全级别的接口不能相互通信，而且数据包无法进入和退出同一接口。本节介绍当接口为同一安全级别时如何启用接口间通信。

有关接口间通信的信息

允许同一安全级别的接口之间相互通信具有以下优势：

- 您可以配置超过 101 个通信接口。

  如果您为每个接口使用不同级别，而且不将任何接口分配到同一安全等级，则可以每个级别（0 到 100）仅配置一个接口。
- 您希望流量能够在同一安全级别的各接口之间自由流动而无需 ACL。

如果启用同一安全级别接口通信，则仍可照常配置不同安全级别的接口。

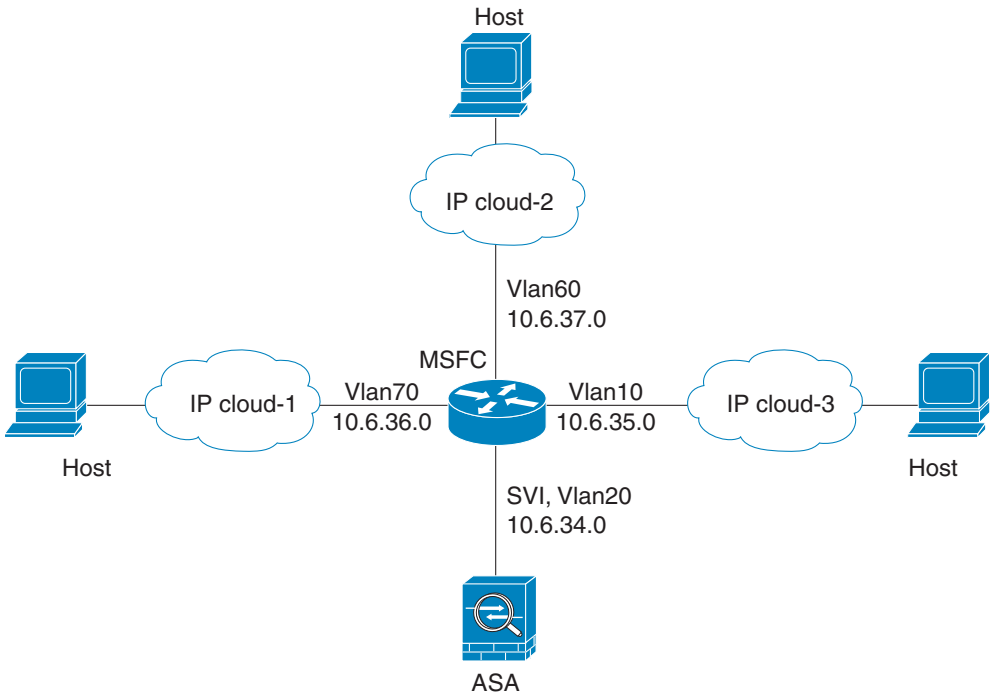
有关接口内通信的信息

接口内通信可能对从某一接口进入、却从同一接口流出的 VPN 流量有用。这种情况下， VPN 流量可能未加密，也可能被重新加密以用于另一个 VPN 连接。例如，如果有星型 VPN 网络，其中 ASA 为中心节点，远程 VPN 网络为分支节点，为使一个分支节点能与另一个分支节点进行通信，流量必须先进入 ASA，然后流出，再进入另一个分支节点。

注　此功能允许的所有流量仍将受到防火墙规则的制约。请勿创建可能导致回传流量不流经 ASA 的非对称路由情景。

对于 ASASM，在启动此功能之前，您首先必须正确配置 MSFC，以便将数据包发送到 ASA 的 MAC 地址，而不是直接通过交换机发送到目标主机。图 12-1 显示了同一接口上的主机需要通信的网络。

图 12-1　同一接口上的主机之间的通信



以下示例配置显示了思科 IOS **route-map** 命令，该命令用于在如图 12-1 中所示的网络中启用策略路由：

```
route-map intra-inter3 permit 0
    match ip address 103
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter2 permit 20
    match ip address 102
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter1 permit 10
    match ip address 101
    set interface Vlan20
    set ip next-hop 10.6.34.7
```

详细步骤

- 要启用同一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**。
- 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**。

关闭和打开接口

本节介绍如何关闭和打开接口。

默认情况下，所有接口均已启用。在多情景模式中，如果禁用或重新启用情景内的接口，则只有该情景接口受到影响。但是，如果禁用或重新启用系统执行空间中的接口，则将影响所有情景中的该接口。

详细步骤

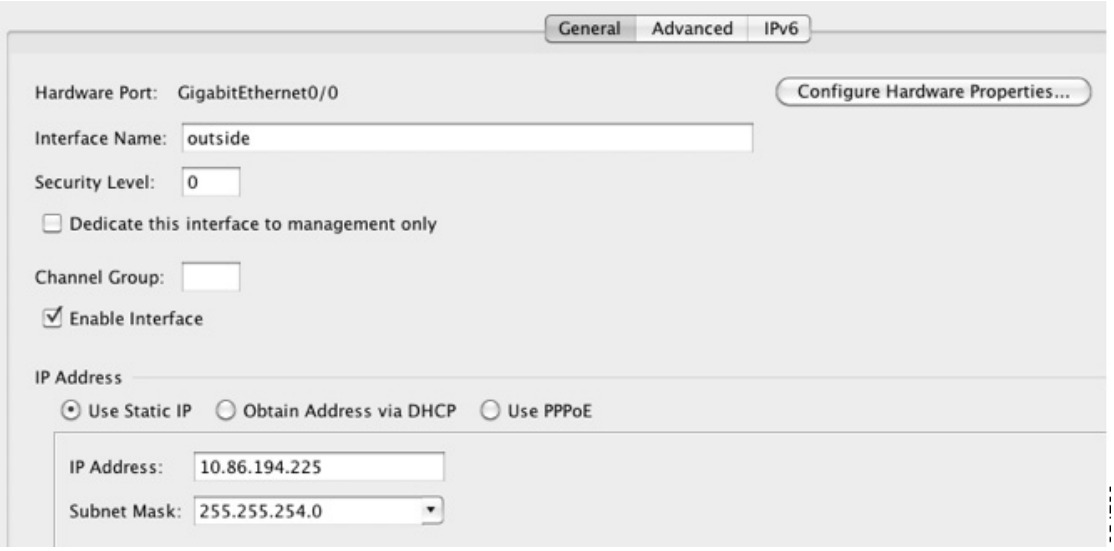
步骤 1　视情景模式而定：

- 对于单情景模式，请选择 **Configuration > Device Setup > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中选择 **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 VLAN 接口，然后点击 **Edit**。

系统将显示 Edit Interface 对话框。



步骤 3　要启用或禁用接口，请选中或取消选中 **Enable Interface** 复选框。

监控接口

- 第 12-24 页的 PPPoE 客户端
- 第 12-24 页的接口连接

ARP 表

Monitoring > Interfaces > ARP Table 窗格显示 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。

字段

- Interface - 列出与映射关联的接口名称。
- IP Address - 显示 IP 地址。
- MAC Address - 显示 MAC 地址。
- Proxy ARP - 代理 ARP 在接口上启用时，显示 Yes。代理 ARP 未在接口上启用时，则显示 No。
- Clear - 清除动态 ARP 表条目。静态条目不会被清除。
- Refresh - 使用来自 ASA 的当前信息刷新表，并更新 Last Updated 日期和时间。
- Last Updated - *仅显示*。表明显示更新的日期和时间。

DHCP

ASA 可以监控 DHCP 状态，包括分配给客户端的地址、 ASA 接口的租约信息以及 DHCP 统计信息。

DHCP 服务器表

Monitoring > Interfaces > DHCP > DHCP Server Table 列出分配给 DHCP 客户端的 IP 地址。

字段

- IP Address - 显示分配给客户端的 IP 地址。
- Client-ID - 显示客户端 MAC 地址或 ID。
- Lease Expiration - 显示 DHCP 租约到期的日期。租约表示客户端可以使用分配的 IP 地址的持续时间。此外，还根据 Last Updated display-only 字段中的时间戳指定剩余时间 （以秒为单位）。
- Number of Active Leases - 显示 DHCP 租约的总数。
- Refresh - 刷新来自 ASA 的信息。
- Last Updated - 显示表中数据最近更新的时间。

DHCP 客户端租约信息

如果从 DHCP 服务器获取 ASA 接口的 IP 地址，则 Monitoring > Interfaces > DHCP > DHCP Server Table > DHCP Client Lease Information 窗格将显示 DHCP 租约的相关信息。

字段

- Select an interface - 列出 ASA 接口。选择您要查看 DHCP 租约的接口。如果接口有多个 DHCP 租约，请选择要查看的接口和 IP 地址对。
- Attribute and Value - 列出接口 DHCP 租约的属性和值。
  - Temp IP addr - *仅显示*。分配给接口的 IP 地址。
  - Temp sub net mask - *仅显示*。分配给接口的子网掩码。
  - DHCP lease server - *仅显示*。 DHCP 服务器地址。
  - state - *仅显示*。 DHCP 租约的状态，如下所述：

    Initial - 初始化状态，在此状态下， ASA 开始获取租约。租约期满时或租赁协商失败时，也显示此状态。

    Selecting - ASA 正在等候接收来自一个或多个 DHCP 服务器的 DHCPOFFER 消息，从而选择其中某个消息。

    Requesting - ASA 正在等候其发出过请求的服务器的回复。

    Purging - ASA 正在删除出错的租约。

    Bound - ASA 获得了一份有效租约，处于正常运行中。

    Renewing - ASA 正在尝试更新租约。 ASA 定期向当前的 DHCP 服务器发送 DHCPREQUEST 消息，并等候答复。

    Rebinding - ASA 无法使用原始服务器更新租约，此时正在发送 DHCPREQUEST 消息，直到收到任何服务器的回复或租约期满为止。

    Holddown - ASA 已经开始删除租约。

    Releasing - ASA 向服务器发送释放消息，表示不再需要 IP 地址。
  - Lease - *仅显示*。由 DHCP 服务器指定的、接口可以使用该 IP 地址的持续时间。
  - Renewal - *仅显示*。直到接口自动尝试更新该租约为止的持续时间。
  - Rebind - *仅显示*。直到 ASA 尝试重新绑定到某个 DHCP 服务器为止的持续时间。如果 ASA 无法与原始 DHCP 服务器通信，并且租约时间已过 87.5%，则发生重新绑定。 ASA 随即通过广播 DHCP 请求尝试与任何可用的 DHCP 服务器取得联系。
  - Next timer fires after - *仅显示*。直到内部计时器触发为止的时间 （以秒为单位）。
  - Retry count - *仅显示*。如果 ASA 正在尝试建立租约，此字段显示 ASA 尝试过发送 DHCP 信息的次数。例如，如果 ASA 处于 Selecting 状态，则此值表示 ASA 发送过发现消息的次数。如果 ASA 处于 Requesting 状态，则此值表示 ASA 发送过请求消息的次数。
  - Client-ID - *仅显示*。与服务器进行的所有通信所采用的客户端 ID。
  - Proxy - *仅显示*。指定此接口是否为 VPN 客户端的一个代理 DHCP 客户端， True 或 False。
  - Hostname - *仅显示*。客户端主机名。

DHCP 统计信息

Monitoring > Interfaces > DHCP > DHCP Statistics 窗格显示 DHCP 服务器功能的统计信息。

字段

- Message Type - 列出已发送或已接收的 DHCP 消息类型：
  - BOOTREQUEST
  - DHCPDISCOVER
  - DHCPREQUEST
  - DHCPDECLINE
  - DHCPRELEASE
  - DHCPINFORM
  - BOOTREPLY
  - DHCPOFFER
  - DHCPACK
  - DHCPNAK
- Count - 显示已处理特定消息的次数。
- Direction - 显示消息类型为已发送或已接收。
- Total Messages Received - 显示 ASA 已接收的消息总数。
- Total Messages Sent - 显示 ASA 已发送的消息总数。
- Counter - 显示通用 DHCP 统计数据，包括以下内容：
  - DHCP UDP Unreachable Errors
  - DHCP Other UDP Errors
  - Address Pools
  - Automatic Bindings
  - Expired Bindings
  - Malformed Messages
- Value - 显示各计数器项目的数值。
- Refresh - 更新 DHCP 表的列表。
- Last Updated - 显示表中数据最近更新的时间。

MAC 地址表

Monitoring > Interfaces > MAC Address Table 窗格显示静态和动态 MAC 地址条目。有关 MAC 地址表和添加静态条目的详细信息，请参阅第 12-21 页的 MAC 地址表。

字段

- Interface - 显示与条目关联的接口名称。
- MAC Address - 显示 MAC 地址。
- Type - 显示条目为静态或动态。
- Age - 显示条目的持续时间 （以分钟为单位）。要设置超时，请参阅第 12-21 页的 MAC 地址表。
- Refresh - 使用来自 ASA 的当前信息刷新表格。

动态 ACL

Monitoring > Interfaces > Dynamic ACLs 窗格显示在功能上与用户配置的 ACL 相同 （由 ASA 自动创建、激活和删除的 ACL 除外）的动态 ACL 表。这些 ACL 不会显示在配置中，仅在此表中可见。这些 ACL 可以通过 ACL 报头中的 “(dynamic)” 关键字识别。

当您在该表中选择某个 ACL 时，该 ACL 的相关内容将显示在底部文本字段中。

字段

- ACL - 显示动态 ACL 的名称。
- Element Count - 显示 ACL 中元素的数量
- Hit Count - 显示 ACL 中全部元素的总计命中次数。

接口图形

在 Monitoring > Interfaces > Interface Graphs 窗格中，您可以以图形或表格的形式查看接口统计信息。如果某个接口在情景间被共享，则 ASA 仅显示当前情景中的统计信息。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。

字段

- Available Graphs for - 列出可用于监控的统计信息的类型。在单个图形窗口中，您最多可以选择四种统计信息类型。您可以同时打开多个图形窗口。
  - Byte Counts - 显示接口上输入和输出的字节数。
  - Packet Counts - 显示接口上输入和输出的数据包数。
  - Packet Rates - 显示接口上输入和输出数据包的速率。
  - Bit Rates - 显示接口输入和输出的比特率。
  - Drop Packet Count - 显示接口上丢弃的数据包数。

  为物理接口显示以下附加统计信息：
  - Buffer Resources - 显示以下统计信息：

    Overruns - 由于输入速率超过 ASA 处理数据的能力， ASA 无法将收到的数据转交给硬件缓冲区的次数。

    Underruns - 发射器运行速度比 ASA 处理速度更快的次数。

    No Buffer - 收到因主系统没有缓冲区空间而丢弃的数据包的次数。将该次数与忽略的计数进行比较。以太网络中的广播风暴常常导致无输入缓冲区事件。
  - Packet Errors - 显示以下统计信息：

    CRC - 循环冗余校验错误数。如果一个工作站发送帧，它会在帧尾附加一个 CRC。该 CRC 根据帧中的数据由算法生成。如果修改源和目标之间的帧，则 ASA 将提示 CRC 不匹配。大量的 CRC 通常由冲突或发送错误数据的工作站引起。

    Frame - 帧错误数量。坏帧包括长度不正确或帧校验和错误的数据包。此错误通常由冲突或以太网设备故障引起。

    Input Errors - 输入错误的总数，包括此处列出的其他类型。与输入相关的其他错误也可能导致输入错误计数增加，而且一些数据报可能存在多个错误；因此，这个总数可能超过列出的其他类型的错误次数。

Runts - 因小于 64 字节的最小数据包大小而被丢弃的数据包数。超短帧通常由冲突引起。也可能由布线不当和电气干扰引起。

Giants - 因超过最大数据包大小而被丢弃的数据包数。例如，大于 1518 字节的所有以太网数据包均被视为超长帧。

Deferred - 仅用于 FastEthernet 接口。因链路上的活动而导致在传输之前被延迟的帧数。

- Miscellaneous - 显示已接收广播的统计信息。
- Collision Counts - 仅用于 FastEthernet 接口。显示以下统计信息：

  Output Errors - 由于超过了已配置的最大冲突数而未传输的帧数。只有在网络流量过大时，该计数器才会递增。

  Collisions - 由于以太网冲突 （单一和多个冲突）而重新传输的消息数。这种情况通常出现在被过度扩展的 LAN 上 （以太网或收发器电缆过长，站点之间存在两个以上的中继器，或级联多端口收发器过多）。发生冲突的数据包仅按输出数据包计数一次。

  Late Collisions - 由于正常冲突时窗外发生的冲突而未传输的帧数。延迟冲突是在数据包传输过程中延迟检测到的冲突。通常，这些情况都不会发生。如果两台以太网主机尝试同时通信，它们应在数据包中早就发生冲突且两者都作出让步，或者第二台主机应看到第一台主机正在通信并等待。如果遇到延迟冲突，设备将迅速做出反应并尝试在以太网上发送数据包，而 ASA 只完成了数据包部分发送。ASA 不会重新发送数据包，因为可能已经释放了储存数据包第一部分的缓冲区。这实际上不是个问题，因为网络协议专门用于通过重新发送数据包来解决冲突。但是，发生延迟冲突表明网络中存在问题。常见问题包括超出规格范围运行的大型重复网络和以太网络。

- Input Queue - 显示输入队列中的数据包数 （当前和最大数据包数），包括以下统计信息：

  Hardware Input Queue - 硬件队列中的数据包数。

  Software Input Queue - 软件队列中的数据包数。

- Output Queue - 显示输出队列中的数据包数 （当前和最大数据包数），包括以下统计信息：

  Hardware Output Queue - 硬件队列中的数据包数。

  Software Output Queue - 软件队列中的数据包数。

- Add - 将选定的统计信息类型添加到选定的图形窗口。
- Remove - 从选定的图形窗口中移除选定的统计信息类型。如果您正在移除的项目是从另一个面板添加的，并且未返回 Available Graphs 窗格，则按按钮名称将更改为 Delete。
- Show Graphs - 显示要添加统计类型的图形窗口名称。如果您已经打开了某个图形窗口，默认情况下，将列出新的图形窗口。如果要将统计类型添加到一个已经打开的图形，请选择已经打开的图形窗口名称。 Selected Graphs 窗格将显示图形中已包括的统计信息，您也可以添加其他类型到该窗格。图形窗口为 ASDM 命名，后接接口 IP 地址和名称 “Graph”。后续图形命名为 “Graph (2)”，以此类推。
- Selected Graphs - 显示要在选定的图形窗口中显示的统计信息类型。最多可包括四种类型。
  - Show Graphs - 显示图形窗口或用额外的统计信息类型 （如已添加）更新图形。

图形 / 表格

Monitoring > Interfaces > Interface Graphs > Graph/Table 窗口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。如果启用 History Metrics （请参阅第 3-30 页的启用历史度量），则可以查看过去时间段的统计信息。

字段

- View - 设置图形或表格的时间段。要查看任何非实时时间段，请启用 History Metrics （请参阅第 3-30 页的启用历史度量）。数据根据以下选项的规格予以更新：
  - 实时，每隔 10 秒钟更新数据
  - 过去 10 分钟，每隔 10 秒钟更新数据
  - 过去 60 分钟，每隔 1 分钟更新数据
  - 过去 12 小时，每隔 12 分钟更新数据
  - 过去 5 天，每隔 2 小时更新数据
- Export - 以逗号分隔值的形式导出图形。如果 Graph 窗口中有多个图形或表格，系统将显示 Export Graph Data 对话框。选中名称旁边的复选框，即可选择列出的一个或多个图形和表格。
- Print - 打印图形或表格。如果 Graph 窗口中有多个图形或表格，系统将显示 Print Graph 对话框。从 Graph/Table Name 列中选择要打印的图形或表格。
- Bookmark - 通过 Graphs 窗口上所有图形和表格的单个链接，以及通过每个图形或表格的单独链接打开一个浏览器窗口。您可以将这些 URL 复制为浏览器书签。打开图形 URL 时，ASDM 不一定在运行；浏览器将启动 ASDM 并显示图形。

PPPoE 客户端

Monitoring > Interfaces > PPPoE Client > PPPoE Client Lease Information 窗格显示当前 PPPoE 连接的相关信息。

字段

Select a PPPoE interface - 选择您想要查看 PPPoE 客户端租约信息的接口。

Refresh - 从 ASA 加载最新的 PPPoE 连接信息，用于显示。

*接口*连接

只有配置了静态路由跟踪时，才在 Monitoring > Interfaces 树显示 Monitoring > Interfaces > *interface* 连接节点。如果跟踪了多条路由，则包含被跟踪路由的每个接口都将有一个节点。

关于路由跟踪信息的详细信息，请参阅以下内容：

- 第 12-25 页的跟踪状态
- 第 12-25 页的监控统计信息

跟踪状态

Monitoring > Interfaces > interface connection > Track Status for 窗格显示被跟踪对象的相关信息。

字段

- Tracked Route - *仅显示*。显示与跟踪进程关联的路由。
- Route Statistics - *仅显示*。显示对象的可达性、可达性最后发生更改的时间、操作返回码以及执行跟踪的进程。

监控统计信息

Monitoring > Interfaces > interface connection > Monitoring Statistics for 窗格显示 SLA 监控进程的统计信息。

字段

- SLA Monitor ID - *仅显示*。显示 SLA 监控进程的 ID。
- SLA statistics - *仅显示*。显示 SLA 监控统计信息，例如上次修改进程的时间，尝试的操作次数，跳过的操作次数，等等。

路由模式中接口的功能历史记录

表 12-1 列出了此功能的版本历史记录。

表 12-1　　接口的功能历史记录

功能名称	版本	功能信息
增加的 VLAN 数量	7.0(5)	增加了以下限制： • ASA5510 基础许可证的 VLAN 数从 0 增加到 10。 • ASA5510 增强型安全许可证的 VLAN 数从 10 增加到 25。 • ASA5520 的 VLAN 数从 25 增加到 100。 • ASA5540 的 VLAN 数从 100 增加到 200。
增加的 VLAN 数量	7.2(2)	ASA 5505 上增强型安全许可证 VLAN 的最大数量从 5（3 个全功能； 1 个故障转移；一个限定于备用接口）增加至 20 个全功能接口。此外，中继端口数量从 1 增加到 8。现在已有 20 个全功能接口，无需使用备用接口命令削弱备用 ISP 接口的功能；可使用全功能接口替代它。备用接口命令对于 Easy VPN 配置仍非常有用。 以下型号的 VLAN 数量限制也有增加：ASA 5510 （对于基础许可证，从 10 增加到 50，对于增强型安全许可证，从 25 增加到 100）、 ASA 5520 （从 100 增加到 150）和 ASA 5550 （从 200 增加到 250）。

表 12-1　　接口的功能历史记录 （续）

功能名称	版本	功能信息
对于 ASA 5510 增强型安全许可证的千兆以太网支持	7.2(3)	ASA 5510 目前通过增强型安全许可证支持端口 0 和 1 的 GE （千兆以太网）。如果从基础许可证升级至增强型安全许可证，则外部 Ethernet 0/0 和 Ethernet0/1 端口的容量将从原始的 FE （快速以太网） (100 Mbps) 增加到 GE (1000 Mbps)。接口名称仍保持为 Ethernet 0/0 和 Ethernet0/1。
对 ASA 5505 的本地 VLAN 支持	7.2(4)/8.0(4)	现在可将本地 VLAN 纳入 ASA 5505 中继端口。 我们修改了以下屏幕：Configuration > Device Setup > Interfaces > Switch Ports > Edit Switch Port。
对 ASA 5580 的巨型数据包支持	8.1(1)	思科 ASA 5580 支持巨型帧。巨型帧是一个以太网数据包，其大小大于标准的最大值 1518 字节 （包括第 2 层报头和 FCS），最大可达 9216 字节。可通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配更多内存可能会限制对其他功能的最充分利用，如 ACL。 我们修改了以下屏幕：Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced。
为 ASA 5580 增加的 VLAN 数	8.1(2)	ASA 5580 支持的 VLAN 数量从 100 增加到 250。
对透明模式的 IPv6 支持	8.2(1)	已为透明防火墙模式引入 IPv6 支持。
对 ASA 5580 10 千兆以太网接口上流量控制的暂停帧支持	8.2(2)	现可为流量控制启用暂停 (XOFF) 帧。 我们修改了以下屏幕： （单情景模式）Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced （多情景模式，系统） Configuration > Interfaces > Add/Edit Interface

第 13 章

透明模式接口

本章包含的任务是在透明防火墙模式中为所有型号完成接口配置。

注 对于多情景模式，请在情景执行空间完成本节中的任务。在 Configuration > Device List 窗格中，双击主用设备 IP 地址项下的情景名称。

有关透明模式接口的信息

透明模式的网桥组

如果不想产生安全情景开销，或者要最大限度地使用安全情景，请将接口一起组合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组的流量互为隔离；流量不会路由至 Cisco ASA 内的其他网桥组，而且，流量必须先退出 ASA，然后才能由外部路由器路由回 ASA 中的另一个网桥组。虽然每个网桥组的桥接功能互为独立，但许多其他功能可以供所有网桥组共享。例如，所有网桥组共享系统日志服务器或 AAA 服务器配置。如需完全分隔安全策略，请将安全情景与每个情景中的一个网桥组配合使用。每个情景或单个模式中至少需要一个网桥组。

每个网桥组均需要一个管理 IP 地址。有关另一种管理方法，请参阅第 10-2 页的管理接口。

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

安全级别

每个接口必须有一个安全级别，范围为 0 （最低）至 100 （最高）。例如，应将最安全的网络（如内部主机网络）指定为级别 100。而连接至互联网的外部网络连接可指定为 0 级。其他网络（如 DMZ）可指定为中间的级别。可将接口分配至同一安全级别。有关详细信息，请参阅第 13-18 页的允许同一安全级别通信。

安全级别可控制以下行为：

- 网络访问 - 默认情况下，从安全性较高的接口到安全性较低的接口 （出站）有一个隐式许可。安全性较高接口上的主机可以访问安全性较低接口上的所有主机。可通过将 ACL 应用于接口来限制访问。

  如果为相同安全接口启用通信 （请参阅第 13-18 页的允许同一安全级别通信），则隐式许可就允许这些接口访问安全级别相同或较低的其他接口。

- 检查引擎 - 某些应用检查引擎取决于安全级别。对于相同安全接口，检查引擎适用于任何一个方向的流量。
  - NetBIOS 检查引擎 - 仅适用于出站连接。
  - SQL*Net 检查引擎 - 如果一个主机对之间存在 SQL*Net（以前称为 OraServ）端口的控制连接，则仅允许通过 ASA 进行入站数据连接。
- 过滤 - HTTP(S) 和 FTP 过滤仅适用于出站连接 （从较高级别到较低级别）。

  如果为相同安全接口启用通信，则可以过滤任何一个方向的流量。
- **established** 命令 - 如已建立从安全级别较高主机到安全级别较低主机的连接，则该命令允许连接从安全级别较低主机返回至安全级别较高主机。

  如果为相同安全接口启用通信，则可以为两个方向配置 **established** 命令。

透明模式接口的许可要求

型号	许可证要求
ASA 5512-X	VLAN： 基础许可证：50 增强型安全许可证：100 所有类型的接口： 基础许可证：716 增强型安全许可证：916
ASA 5515-X	VLAN： 基础许可证：100 所有类型的接口： 基础许可证：916

型号	许可证要求
ASA 5525-X	VLAN： 基础许可证：200 所有类型的接口： 基础许可证：1316
ASA 5545-X	VLAN： 基础许可证：300 所有类型的接口： 基础许可证：1716
ASA 5555-X	VLAN： 基础许可证：500 所有类型的接口： 基础许可证：2516
ASA 5585-X	VLAN： 基础许可证和增强型安全许可证：1024 SSP-10 和 SSP-20 的接口速度： 基础许可证 - 适用于光纤接口的 1 千兆以太网 10 GE I/O 许可证 （增强型安全许可证） - 适用于光纤接口的 10 千兆以太网 （默认情况下， SSP-40 和 SSP-60 支持 10 千兆以太网。） 所有类型的接口： 基础许可证和增强型安全许可证：4612

注　对于根据 VLAN 限制计数的接口，您必须为它分配一个 VLAN。

所有类型的接口均包括最大数量的组合接口；例如， VLAN、物理、冗余、网桥组和 EtherChannel 接口。在配置中定义的每个 **interface** 均根据此限制进行计数。

型号	许可证要求
ASASM	VLAN： 基础许可证：1000

透明模式接口的准则和限制

本节包括有关此功能的准则和限制。

情景模式准则

- 对于多情景模式中的 ASA 5512-X 和更高版本，请根据第 10 章，“基本接口配置（ASA 5512-X 及更高版本）”在系统执行空间中配置物理接口。然后按照本章内容在情景执行空间中配置逻辑接口参数。对于多情景模式中的 ASASM，请按照第 2 章，“适用于思科 ASA 服务模块的交换机配置”配置交换机端口和交换机上的 VLAN，然后为 ASASM 分配 VLAN。

  ASAv 不支持多情景模式。
- 您只能配置已分配给系统配置中情景的情景接口。

防火墙模式准则

- 可以在单情景模式或多情景模式的每个情景中配置多达 250 个网桥组。请注意，必须使用至少 1 个网桥组；数据接口必须属于网桥组。
- 每个网桥组最多可包括 4 个接口。
- 对于 IPv4，每个网桥组都需要一个管理 IP 地址以用于两个管理流量并供流量通过 ASA。

  与路由模式（每个接口需要一个 IP 地址）不同，透明防火墙向整个网桥组分配一个 IP 地址。 ASA 使用此 IP 地址作为源自 ASA 的数据包（如系统消息或 AAA 通信）的源地址。除网桥组管理地址外，还可以选择性地为某些型号配置管理接口；有关详细信息，请参阅第 10-2 页的管理接口。

  管理 IP 地址必须与所连接的网络位于相同的子网上。您不能将该子网设置为主机子网 (255.255.255.255)。 ASA 不支持辅助网络上的流量；仅支持与管理 IP 地址相同的网络上的流量。有关管理 IP 子网的详细信息，请参阅第 13-6 页的配置网桥组。
- 对于 IPv6，至少需要为直通流量的每个接口配置本地链路地址。为了实现完整功能，包括管理 ASA 的能力，需要为每个网桥组配置全局 IPv6 地址。
- 对于多情景模式，每个情景必须使用不同的接口；不能在情景之间共享接口。
- 对于多情景模式，每个情景通常使用不同的子网。可以使用重叠子网，但是网络拓扑需要路由器和 NAT 配置，以便从路由角度使用重叠子网。

故障转移准则

请勿采用本章中的操作步骤完成故障转移接口的配置。要配置故障转移和状态链路，请参阅第 8 章，“通过故障转移实现高可用性”。在多情景模式中，故障转移接口在系统配置中进行配置。

IPv6 准则

透明模式中不支持 IPv6 任播地址。

适合 ASASM 的 VLAN ID 准则

可向配置中添加任何 VLAN ID，但是，只有通过交换机分配至 ASA 的 VLAN 才能传输流量。要查看分配至 ASA 的所有 VLAN，请使用 **show vlan** 命令。

如果为尚未通过交换机分配至 ASA 的 VLAN 添加接口，则该接口将处于关闭状态。将 VLAN 分配至 ASA 时，接口将更改为可用状态。要获得有关接口状态的详细信息，请使用 **show interface** 命令。

透明模式接口的默认设置

本节列出了接口的默认设置 （如果没有出厂默认配置）。有关出厂默认配置的信息，请参阅第 2-14 页的出厂默认配置。

默认安全级别

默认安全级别为 0。如将一个接口指定为 “ 内部 ”，且未明确设置安全级别，则 ASA 将安全级别设置为 100。

注　如果更改接口的安全级别，且不想在使用新安全信息之前等待现有连接超时，则可使用 **clear local - host** 命令清除连接。

ASASM 接口的默认状态

- 在单情景模式或系统执行空间中， VLAN 接口默认启用。
- 在多情景模式中，所有分配的接口均默认启用，无论系统执行空间中接口的状态如何。但是，为使流量通过接口，还必须在系统执行空间中启用接口。如果关闭系统执行空间中的接口，则该接口将在共享它的所有情景中处于关闭状态。

巨型帧支持

默认情况下，ASASM 支持巨型帧。请根据第 13-12 页的配置 MAC 地址、MTU 和 TCP MSS 为所需的数据包大小配置 MTU。

在透明模式中完成接口配置

用于完成接口配置的任务流

步骤 1　根据型号设置接口：

- ASA 5512-X 和更高版本 - 第 13 章，“ 透明模式接口 ”
- ASASM- 第 2 章，“ 适用于思科 ASA 服务模块的交换机配置 ”
- ASAv- 第 11 章，“ 基本接口配置 (ASAv)”

步骤 2　（多情景模式）根据第 7-14 页的配置多情景将接口分配给情景。

步骤 3　（多情景模式）在 Configuration > Device List 窗格中，双击主用设备 IP 地址项下的情景名称。

步骤 4　配置一个或多个网桥组，包括 IPv4 地址。请参阅第 13-6 页的配置网桥组。

步骤 5　配置常规接口参数，包括其所属的网桥组、接口名称和安全级别。请参阅第 13-7 页的配置常规接口参数。

步骤 6　（可选）配置管理接口。请参阅第 13-10 页的配置管理接口 （ASA 5512-X 和更高版本及 ASAv）。

步骤 7　（可选）配置 MAC 地址和 MTU。请参阅第 13-12 页的配置 MAC 地址、 MTU 和 TCP MSS。

步骤 8　（可选）配置 IPv6 寻址。请参阅第 13-14 页的配置 IPv6 寻址。

步骤 9　（可选）通过允许两个接口之间的通信，或通过允许流量进入和退出同一接口，来允许相同安全级别通信。请参阅第 13-18 页的允许同一安全级别通信。

配置网桥组

每个网桥组均需要一个管理 IP 地址。 ASA 使用此 IP 地址作为源自网桥组的数据包的源地址。管理 IP 地址必须与所连接的网络位于相同的子网上。对于 IPv4 流量，传递任何流量均需要管理 IP 地址。对于 IPv6 流量，至少必须配置本地链路地址以传递流量，但要实现完整功能 （包括远程管理和其他管理操作），建议采用全局管理地址。

准则和限制

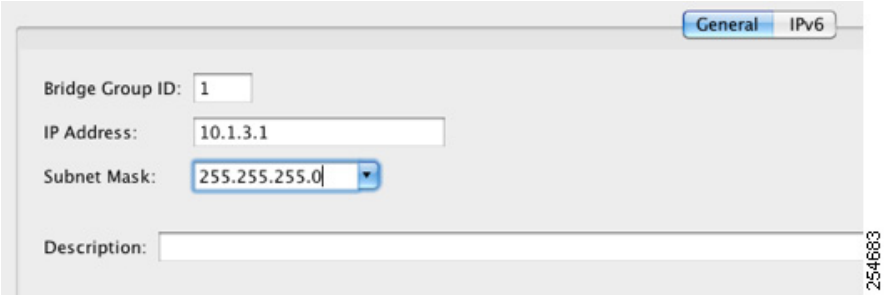
可以在单情景模式或多情景模式的每个情景中配置多达 250 个网桥组。请注意，必须使用至少 1 个网桥组；数据接口必须属于网桥组。

注　对于单独的管理接口 （对于受支持的型号），一个无法配置的网桥组 (ID 301) 将自动添加至您的配置。此网桥组未纳入网桥组限制中。

详细步骤

步骤 1　选择 **Configuration > Interfaces** 窗格，然后选择 **Add > Bridge Group Interface**。

系统将显示 Add Bridge Group 对话框。



步骤 2　在 Bridge Group ID 字段中，输入介于 1 与 250 之间的网桥组 ID。

步骤 3　在 IP Address 字段中，输入管理 IPv4 地址。

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。

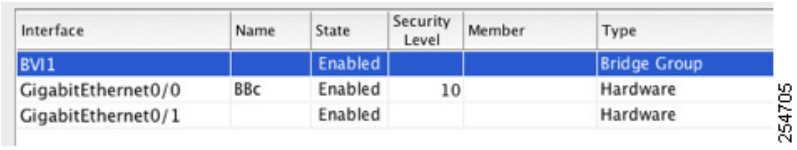
步骤 4　在 Subnet Mask 字段中，输入子网掩码或从菜单中选择一个。

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 个的其他子网 （每个分别用于上游路由器、下游路由器和透明防火墙），如 /30 子网 (255.255.255.252)。 ASA 向子网中的第一个和最后一个地址或从其丢弃所有 ARP 数据包。因此，如果使用 /30 子网，且将已预留的地址从该子网分配给上游路由器，则 ASA 将丢弃从下游路由器到上游路由器的 ARP 请求。

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　网桥组虚拟接口 (BVI) 连同物理接口和子接口已添加至接口表。



Interface	Name	State	Security Level	Member	Type
BVI1		Enabled			Bridge Group
GigabitEthernet0/0	BBc	Enabled	10		Hardware
GigabitEthernet0/1		Enabled			Hardware

254705

后续操作

配置常规接口参数。请参阅第 13-7 页的配置常规接口参数。

配置常规接口参数

本操作步骤介绍如何为每个透明接口设置名称、安全级别和网桥组。

要配置单独的管理界面，请参阅第 13-10 页的配置管理接口 （ASA 5512-X 和更高版本及 ASAv）。

对于 ASA 5512-X 和更高版本及 ASAv，必须为以下接口类型配置接口参数：

- 物理接口
- VLAN 子接口
- 冗余接口
- EtherChannel 接口

对于 ASASM，必须为以下接口类型配置接口参数：

- VLAN 接口

准则和限制

- 可为每个网桥组配置多达四个接口。
- 有关安全级别的信息，请参阅第 13-2 页的安全级别。
- 如在使用故障转移，请勿使用此操作步骤命名为故障转移和 Stateful Failover 通信预留的接口。要配置故障转移和状态链路，请参阅第 8 章，“通过故障转移实现高可用性”。

先决条件

- 根据型号设置接口：
  - ASA 5512-X 和更高版本 - 第 10 章，“基本接口配置 （ASA 5512-X 及更高版本）”
  - ASASM- 第 2 章，“适用于思科 ASA 服务模块的交换机配置”
  - ASAv- 第 11 章，“基本接口配置 (ASAv)”
- 在多情景模式中，只能配置已根据第 7-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。要从系统切换至情景配置，请在 Configuration > Device List 窗格中 双击有效设备 IP 地址下的情景名称。

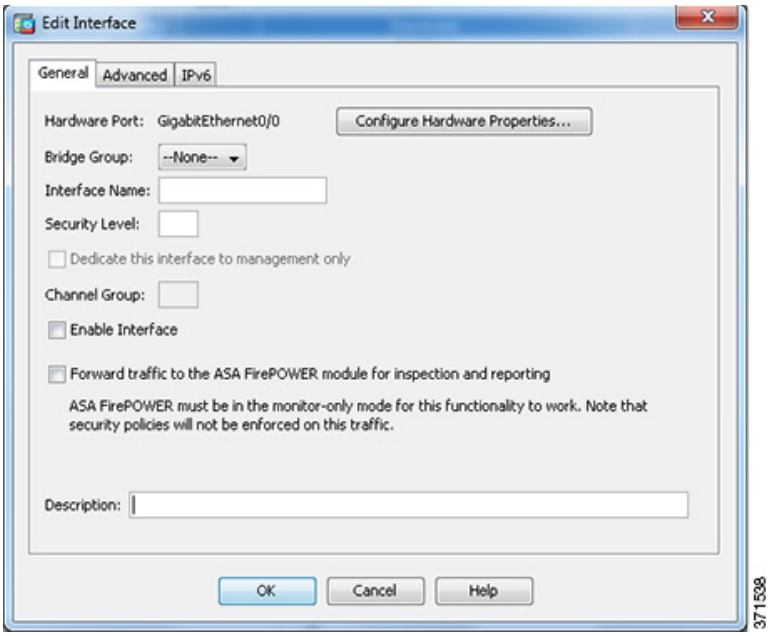
详细步骤

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

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系统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，其中的 General 选项卡已选定。



请勿对管理接口执行此操作步骤；要配置管理接口，请参阅第 13-10 页的配置管理接口 （ASA 5512-X 和更高版本及 ASAv）。

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

步骤 4　在 Interface Name 字段中输入名称，最长 48 个字符。

步骤 5　在 Security Level 字段中，输入值为 0 （最低）到 100 （最高）的级别。

有关详细信息，请参阅第 13-2 页的安全级别。

注　请勿点击 **Dedicate this interface to management only** 复选框；有关该选项，请参阅第 13-10 页的配置管理接口 （ASA 5512-X 和更高版本及 ASAv）。

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

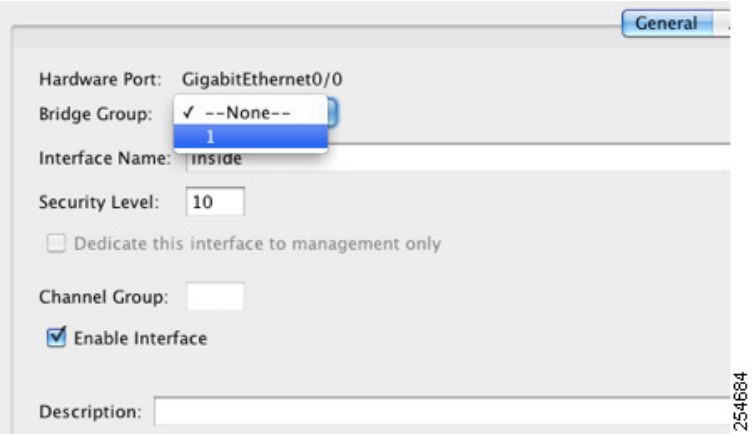
注　Channel Group 字段为只读字段，指明该接口是否为 EtherChannel 的一部分。

步骤 7　（可选）如果安装 ASA CX 或 ASA FirePOWER 模块，且要在非生产 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，请参阅防火墙配置指南中的模块章节。

步骤 8　（可选）在 Description 字段中，输入该接口的说明。

单行中的说明最多可包含 240 个字符 （无需回车）。对于故障转移或状态链路，则说明将固定为 “LAN Failover Interface”、“STATE Failover Interface” 或 “LAN/STATE Failover Interface” 等内容。无法编辑该说明。如将此接口设为故障转移或状态链路，则固定说明将覆盖在此处输入的任何说明。

注　（ASA 5512-X 和更高版本，单情景模式）有关 Configure Hardware Properties 按钮的信息，请参阅第 10-12 页的启用物理接口并配置以太网参数。



步骤 9　点击 **OK**。

后续操作

- （可选）配置管理接口。请参阅第 13-10 页的配置管理接口 （ASA 5512-X 和更高版本及 ASAv）。
- （可选）配置 MAC 地址和 MTU。请参阅第 13-12 页的配置 MAC 地址、 MTU 和 TCP MSS。
- （可选）配置 IPv6 寻址。请参阅第 13-14 页的配置 IPv6 寻址。

配置管理接口 （ASA 5512-X 和更高版本及 ASAv）

可在单情景模式或每个情景中配置一个与网桥组接口分离的管理接口。有关详细信息，请参阅第 10-2 页的管理接口。

限制

- 请参阅第 10-2 页的管理接口。
- 请勿将此接口分配给网桥组；不可配置的网桥组 (ID 101) 将自动添加到您的配置中。此网桥组未纳入网桥组限制中。
- 如果您的型号不包括管理接口，则必须从数据接口管理透明防火墙；请跳过此操作步骤。（例如，在 ASASM 上。）
- 在多情景模式中，无法在情景之间共享任何接口，包括管理接口。要为每个情景提供管理，可创建管理接口的子接口，然后向每个情景分配管理子接口。请注意，从 ASA 5512-X 到 ASA 5555-X 都不允许管理接口上有子接口，因此，对于每个情景管理，必须连接至数据接口。

先决条件

- 完成第 10 章，“ 基本接口配置 （ASA 5512-X 及更高版本） ”中的操作步骤
- 在多情景模式中，只能配置已根据第 7-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。要从系统切换至情景配置，请在 Configuration > Device List 窗格中双击有效设备 IP 地址下的情景名称。

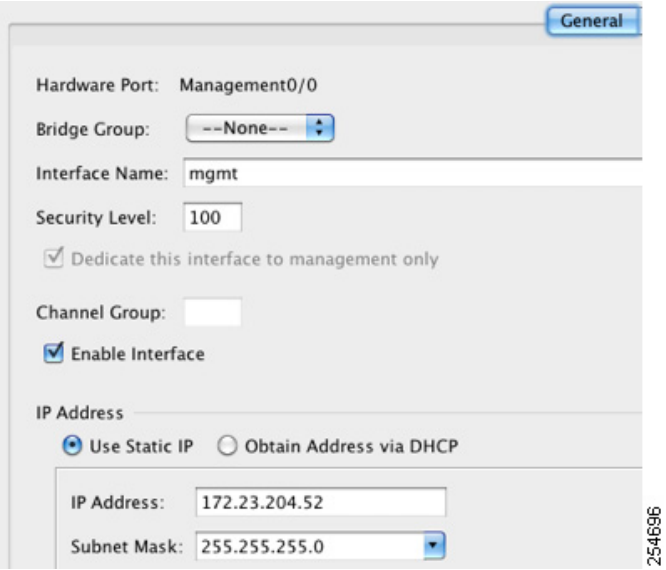
详细步骤

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

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系统执行空间中情景的接口。

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，其中的 General 选项卡已选定。



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

步骤 4　在 Interface Name 字段中输入名称，最长 48 个字符。

步骤 5　在 Security Level 字段中，输入值为 0 （最低）到 100 （最高）的级别。

有关详细信息，请参阅第 13-2 页的安全级别。

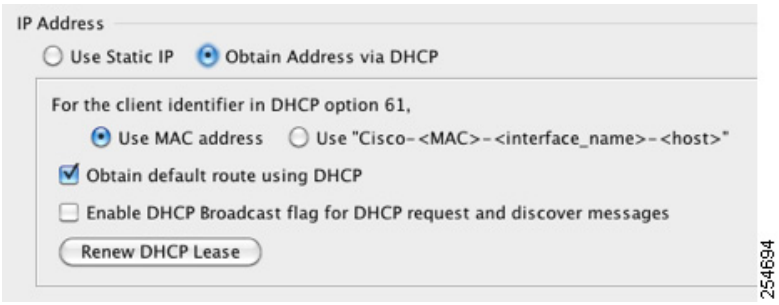
注　**Dedicate this interface to management only** 复选框已默认启用且不可配置。

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，请使用下列选项之一。

注　如需与故障转移组合使用，则必须手动设置 IP 地址和备用地址； DHCP 不受支持。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 地址未纳入 DHCP 请求数据包中，则将不分配 IP 地址。

b. 要使用为选项 61 生成的字符串，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**。

如果广播标记已设为 1，则 DHCP 服务器将侦听该标记并广播回复数据包。

e. （可选）要续租，请点击 **Renew DHCP Lease**。

步骤 8　（可选）在 Description 字段中，输入该接口的说明。

单行中的说明最多可包含 240 个字符，无需回车。

注　（ASA 5512-X 和更高版本，单情景模式）有关 Configure Hardware Properties 按钮的信息，请参阅第 10-12 页的启用物理接口并配置以太网参数。

步骤 9　点击 **OK**。

后续操作

- （可选）配置 MAC 地址和 MTU。请参阅第 13-12 页的配置 MAC 地址、 MTU 和 TCP MSS。
- （可选）配置 IPv6 寻址。请参阅第 13-14 页的配置 IPv6 寻址。

配置 MAC 地址、 MTU 和 TCP MSS

本节介绍如何为接口配置 MAC 地址及如何设置 MTU 和 TCP MSS。

有关 MAC 地址的信息

默认情况下，物理接口使用烧录 MAC 地址，物理接口的所有子接口均使用相同的烧录 MAC 地址。

对于 ASASM，所有 VLAN 使用背板提供的同一个 MAC 地址。

冗余接口使用您添加的第一个物理接口的 MAC 地址。如果在配置中更改成员接口的顺序，则 MAC 地址发生更改，以匹配现第一个列出的接口的 MAC 地址。如果使用此命令将一个 MAC 地址分配给冗余接口，则无论成员接口 MAC 地址如何，均将使用该分配的 MAC 地址。

对于 EtherChannel，属于通道组的所有接口均共享相同 MAC 地址。该功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；他们不知道单个链路。端口通道接口使用编号最小的通道组接口 MAC 地址作为端口通道 MAC 地址。或者，您可以为端口通道接口手动配置 MAC 地址。在多情景模式中，可将唯一 MAC 地址自动分配给各个接口，包括 EtherChannel 端口接口。在组通道接口成员资格发生变化的情况下，我们建议手动或（在多情景模式中）自动配置唯一的 MAC 地址。如果移除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址更改至下一个编号最小的接口，从而导致流量中断。

在多情景模式中，如果在情景之间共享接口，则可将唯一 MAC 地址分配给每个情景的接口。借助于此功能， ASA 可轻松地将数据包分类到适当的情景中。可使用没有唯一 MAC 地址的共享接口，但受到一些限制。有关详细信息，请参阅第 7-3 页的 ASA 如何对数据包分类。可手动分配每个 MAC 地址，或者也可为情景中共享接口自动生成 MAC 地址。要自动生成 MAC 地址，请参阅第 7-22 页的自动为情景接口分配 MAC 地址。如果自动生成 MAC 地址，则可使用此操作步骤覆盖生成的地址。

对于单情景模式，或对于不在多情景模式中共享的接口，您可能要向子接口分配唯一 MAC 地址。例如，您的服务提供商可能根据 MAC 地址执行访问控制。

关于 MTU 和 TCP MSS 的信息

请参阅第 10-6 页的用最大传输单元、 TCP 最大分段大小控制分片。

先决条件

- 根据型号设置接口：
  - ASA 5512-X 和更高版本 - 第 10 章，“基本接口配置 （ASA 5512-X 及更高版本）”
  - ASASM- 第 2 章，“适用于思科 ASA 服务模块的交换机配置”
  - ASAv- 第 11 章，“基本接口配置 (ASAv)”
- 在多情景模式中，只能配置已根据第 7-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。要从系统切换至情景配置，请在 Configuration > Device List 窗格中双击有效设备 IP 地址下的情景名称。

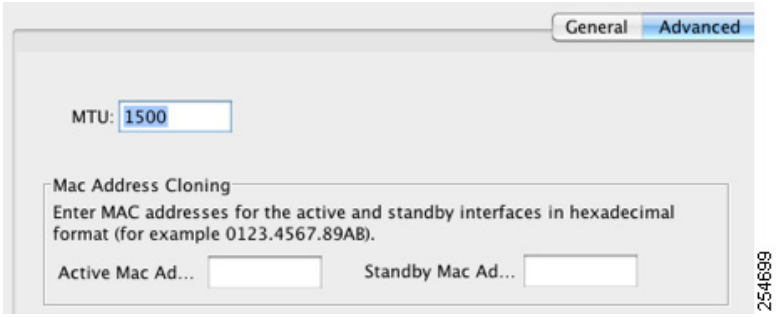
详细步骤

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

步骤 2　选择接口行，然后点击 **Edit**。

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

步骤 3　点击 **Advanced** 选项卡。



步骤 4　要设置 MTU 或启用巨型帧支持 （仅限受支持的型号），请在 MTU 字段输入 300 与 9198 字节之间的数值 （对于 ASAv，为 9000）。

默认值为 1500 字节。

注　为冗余或端口通道接口设置 MTU 时， ASA 将设置应用于所有成员接口。

- 对于在单情景模式中支持句型帧的型号 - 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型帧支持。如将所有接口的 MTU 值均设置回小于 1500 的值，则将禁用巨型帧支持。
- 对于在多情景模式中支持句型帧的型号 - 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型帧支持。请参阅第 10-25 页的启用巨型帧支持。

注　启用或禁用巨型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。如果您还想使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。

步骤 6　如果使用故障转移，请在 Standby Mac Address 字段输入备用 MAC 地址。如果主用设备发生故障转移，且备用设备变为主用设备，则新的主用设备开始使用有效 MAC 地址，以最大限度地减少网络中断，同时，原来的主用设备使用备用地址。

步骤 7　要设置 TCP MSS，请选择 **Configuration > Firewall > Advanced > TCP Options**。设置以下选项：

- Force Maximum Segment Size for TCP - 将最大 TCP 分段大小设置为介于 48 与任何最大数值之间的字节数。默认值为 1380 字节。可禁用此功能，只需将字节数设置为 0。
- Force Minimum Segment Size for TCP - 覆盖最大分段大小，使其不小于已设置的字节数，介于 48 至任何最大数值之间。此功能默认已禁用 （设置为 0）。

步骤 8　有关 **Secure Group Tagging**，请参阅第 33-20 页的启用 SGT plus Ethernet Tagging。

后续操作

（可选）配置 IPv6 寻址。请参阅第 13-14 页的配置 IPv6 寻址。

配置 IPv6 寻址

本节介绍如何配置 IPv6 寻址。

有关 IPv6 的信息

本节包括有关如何配置 IPv6 的信息。

IPv6 寻址

可为 IPv6 配置两种类型的单播地址：

- 全局 - 全局地址是可在公用网络上使用的公用地址。需要为每个网桥组配置该地址，而不是每个接口。还可为管理接口配置全局 IPv6 地址。
- 本地链路 - 本地链路地址是只能在直连网络上使用的专用地址。路由器不使用本地链路地址转发数据包；它们仅用于在特定物理网段上通信。它们可用于执行地址配置或 ND 功能，如地址解析和邻居发现。由于本地链路地址仅在网段上可用，且与接口 MAC 地址绑定，因此，需要为每个接口配置本地链路地址。

至少需要配置本地链路地址， IPv6 才会起作用。如果配置全局地址，则会在每个接口上自动配置本地链路地址，因此，无需再特别配置本地链路地址。如果不配置全局地址，则需要自动或手动配置本地链路地址。

Modified EUI-64 接口 ID

RFC 3513：互联网协议第 6 版 (IPv6) 寻址架构要求所有单播 IPv6 地址 （以二进制值 000 开头的地址除外）的接口标识符部分长度为 64 位，结构格式为 Modified EUI-64 格式。ASA 可为连接至本地链路的主机强制执行该要求。

在接口上启用此功能时，该接口接收的 IPv6 数据包源地址将根据源 MAC 地址进行验证，以确保接口标识符使用 Modified EUI-64 格式。如果 IPv6 数据包不将 Modified EUI - 64 格式用于接口标识符，则将丢弃数据包，并生成以下系统日志消息：

```
%ASA-3-325003: EUI-64 source address check failed.
```

只有在创建流量时才能执行地址格式验证。不检查来自现有流量的数据包。此外，只能对本地链路上的主机执行地址验证。从路由器后面的主机接收的数据包将无法通过地址格式验证，且被丢弃，因为它们的源 MAC 地址将为路由器 MAC 地址，而不是主机 MAC 地址。

不受支持的命令

以下 IPv6 命令在透明防火墙模式中不支持，因为它们需要路由器功能：

- **ipv6 address autoconfig**
- **ipv6 nd prefix**
- **ipv6 nd ra-interval**
- **ipv6 nd ra-lifetime**
- **ipv6 nd suppress-ra**

配置全局 IPv6 地址

要为网桥组或管理接口配置全局 IPv6 地址，请执行以下步骤。

注　配置全局地址将自动配置本地链路地址，因此，无需另行配置它。

限制

ASA 不支持 IPv6 任播地址。

先决条件

- 根据型号设置接口：
  - ASA 5512-X 和更高版本 - 第 10 章，“基本接口配置（ASA 5512-X 及更高版本）”
  - ASASM- 第 2 章，“适用于思科 ASA 服务模块的交换机配置”
  - ASAv- 第 11 章，“基本接口配置 (ASAv)”
- 在多情景模式中，只能配置已根据第 7-14 页的配置多情景分配给系统配置中情景的情景接口。
- 在多情景模式中，请在情景执行空间中完成此操作步骤。要从系统切换至情景配置，请在 Configuration > Device List 窗格中双击有效设备 IP 地址下的情景名称。

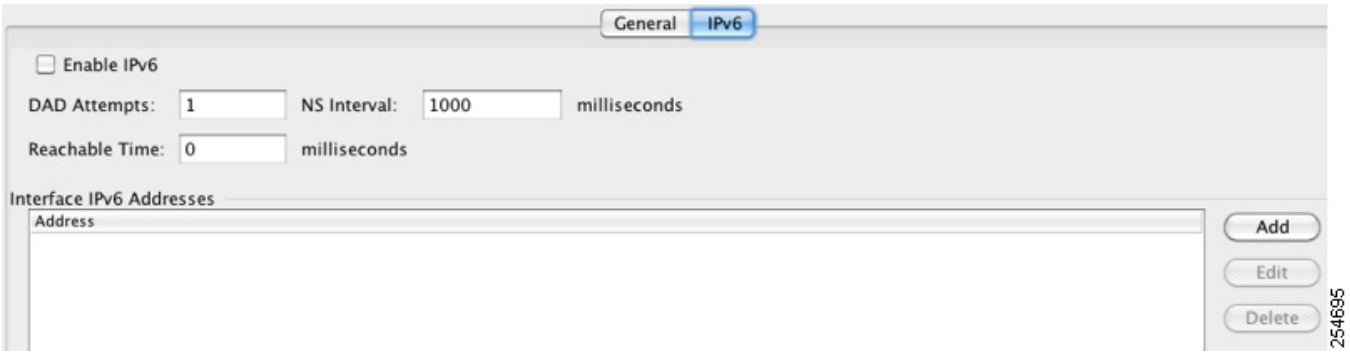
详细步骤

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

步骤 2　选择 BVI 或管理接口，然后点击 **Edit**。

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

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 Modified EUI-64 格式的接口标识符，请选中 **Enforce EUI-64** 复选框。

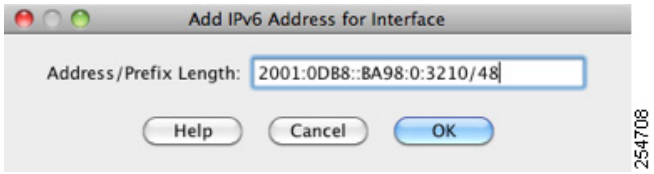
有关详细信息，请参阅第 13-15 页的 Modified EUI-64 接口 ID。

步骤 6　（可选）在顶部区域，通过参考第 26 章，“IPv6 邻居发现”自定义 IPv6 配置

步骤 7　要配置全局 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，输入全局 IPv6 地址和 IPv6 前缀长度。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅第 43-4 页的 IPv6 地址。

c. 点击 **OK**。

步骤 8　点击 **OK**。

系统将返回 Configuration > Device Setup > Interfaces 窗格。

配置 IPv6 邻居发现

要配置 IPv6 邻居发现，请参阅第 26 章，“IPv6 邻居发现 ”。

（可选）自动配置本地链路地址

如果不想要配置全局地址，且只需配置本地链路地址，则可以选择根据接口 MAC 地址生成本地链路地址 （Modified EUI-64 格式。由于 MAC 地址使用 48 位，因此，必须插入额外的位数，以填充接口 ID 所需的 64 位。）

要手动分配本地链路地址 （不推荐），请参阅第 13-18 页的 （可选）手动配置本地链路地址。

有关其他 IPv6 选项，包括强制执行 Modified EUI-64 格式和 DAD 设置，请参阅第 13-16 页的配置全局 IPv6 地址。

要为管理接口或网桥组成员接口自动配置本地链路地址，请执行以下步骤：

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

步骤 2　选择 BVI 或管理接口，然后点击 **Edit**。

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

步骤 3　点击 **IPv6** 选项卡。

步骤 4　在 IPv6 配置区域中，选中 **Enable IPv6**。

此选项可启用 IPv6，并根据接口 MAC 地址使用 Modified Eui-64 接口 ID 自动为成员接口生成本地链路地址。

步骤 5　点击 **OK**。

（可选）手动配置本地链路地址

如果不想要配置全局地址，且只需在物理接口或子接口上配置本地链路地址，则可以选择手动定义本地链路地址。请注意，我们建议根据 Modified EUI-64 格式自动分配本地链路地址。例如，如果其他设备强制使用 Modified EUI-64 格式，则手动分配的本地链路地址可能导致数据包被丢弃。

要自动分配本地链路地址 （推荐），请参阅第 13-17 页的 （可选）自动配置本地链路地址。

有关其他 IPv6 选项，包括强制执行 Modified EUI-64 格式和 DAD 设置，请参阅第 13-16 页的配置全局 IPv6 地址。

要向物理接口或子接口 （包括管理接口）分配本地链路地址，请执行以下步骤：

步骤 1　选择 **Configuration > Device Setup > Interfaces** 窗格。

步骤 2　选择接口，然后点击 **Edit**。

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

步骤 3　点击 **IPv6** 选项卡。

步骤 4　要设置本地链路地址，请在 Link-local address 字段中输入地址。

本地链路地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。有关 IPv6 寻址的详细信息，请参阅第 43-4 页的 IPv6 地址。

步骤 5　点击 **OK**。

允许同一安全级别通信

默认情况下，同一个安全等级的接口不能相互通信，而且数据包无法进入和退出同一接口。本节介绍当接口为同一安全级别时如何启用接口间通信。

有关接口间通信的信息

如果想要流量不用 ACL 就能在所有同一安全级别接口之间自由流动，允许同一安全级别的接口间相互通信将非常有用。

如果启用同一安全级别接口通信，则仍可照常配置不同安全级别的接口。

详细步骤

要使同一安全级别的接口之间的相互通信，请在 Configuration > Interfaces 窗格中选中 **Enable traffic between two or more interfaces which are configured with same security level**。

关闭和打开接口

本节介绍如何关闭和打开接口。

默认情况下，所有接口均已启用。在多情景模式中，如果禁用或重新启用情景内的接口，则只有该情景接口受到影响。但是，如果禁用或重新启用系统执行空间中的接口，则将影响所有情景中的该接口。

详细步骤

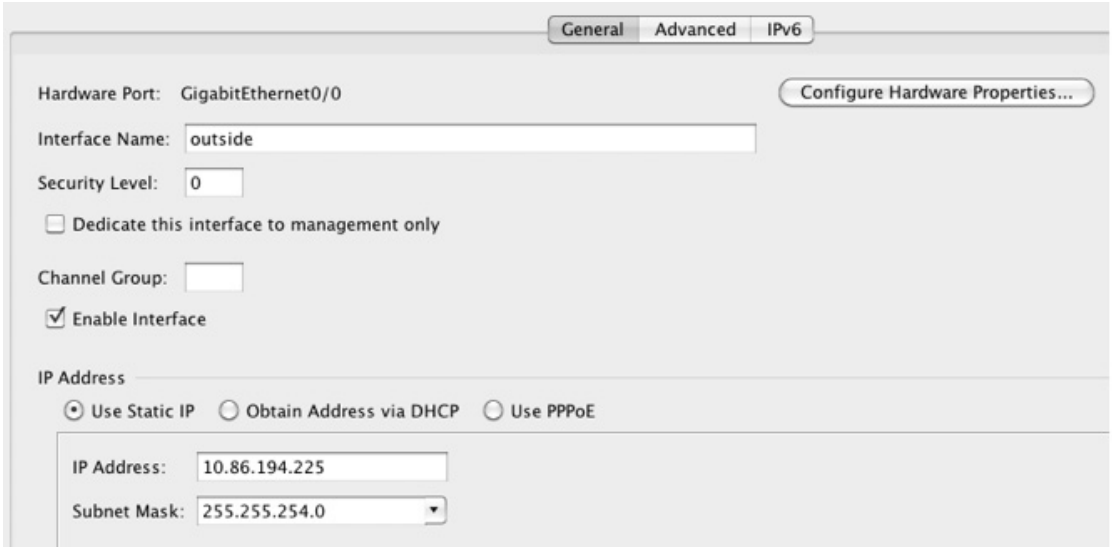
步骤 1　视情景模式而定：

- 对于单情景模式，请选择 **Configuration > Device Setup > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中选择 **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 VLAN 接口，然后点击 **Edit**。

系统将显示 Edit Interface 对话框。



步骤 3　要启用或禁用接口，请选中或取消选中 **Enable Interface** 复选框。

监控接口

- 请参阅第 12-19 页的 ARP 表。
- 请参阅第 12-19 页的 DHCP。
- 请参阅第 12-21 页的 MAC 地址表。
- 请参阅第 12-22 页的动态 ACL。
- 请参阅第 12-22 页的接口图形。
- 请参阅第 12-24 页的 PPPoE 客户端。
- 请参阅第 12-24 页的接口连接。

透明模式接口的功能历史

表 13-1 列出了各种功能变更以及实施该等功能变更的平台版本。 ASDM 可向后兼容多个平台版本，因此，未列出已添加支持的具体 ASDM 版本。

表 13-1　　透明模式接口的功能历史

功能名称	平台版本	功能信息
增加的 VLAN 数量	7.0(5)	增加了以下限制： • ASA5510 基础许可证的 VLAN 数从 0 增加到 10。 • ASA5510 增强型安全许可证 VLAN 数从 10 增加到 25。 • ASA5520 的 VLAN 数从 25 增加到 100。 • ASA5540 的 VLAN 数从 100 增加到 200。
增加的 VLAN 数量	7.2(2)	ASA 5505 上增强型安全许可证 VLAN 的最大数量从 5（3 个全功能； 1 个故障转移；一个限定于备用接口）增加至 20 个全功能接口。此外，中继端口数量从 1 增加到 8。现在已有 20 个全功能接口，无需使用备用接口命令削弱备用 ISP 接口的功能；可使用全功能接口替代它。备用接口命令对于 Easy VPN 配置仍非常有用。 以下型号的 VLAN 数量限制也有增加：ASA 5510 （对于基础许可证，从 10 增加到 50，对于增强型安全许可证，从 25 增加到 100）、 ASA 5520 （从 100 增加到 150）和 ASA 5550 （从 200 增加到 250）。
对于 ASA 5510 增强型安全许可证的千兆以太网支持	7.2(3)	ASA 5510 目前通过增强型安全许可证支持端口 0 和 1 的 GE （千兆以太网）。如果从基础许可证升级至增强型安全许可证，则外部 Ethernet 0/0 和 Ethernet0/1 端口的容量将从原始的 FE （快速以太网） (100 Mbps) 增加到 GE (1000 Mbps)。接口名称仍保持为 Ethernet 0/0 和 Ethernet0/1。
对 ASA 5505 的本地 VLAN 支持	7.2(4)/8.0(4)	现在可将本地 VLAN 纳入 ASA 5505 中继端口。 我们修改了以下屏幕：Configuration > Device Setup > Interfaces > Switch Ports > Edit Switch Port。
对 ASA 5580 的巨型数据包支持	8.1(1)	思科 ASA 5580 支持巨型帧。巨型帧是一个以太网数据包，其大小大于标准的最大值 1518 字节 （包括第 2 层报头和 FCS），最大可达 9216 字节。可通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配更多内存可能会限制对其他功能的最充分利用，如 ACL。 我们修改了以下屏幕：Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced。
增加了 ASA 5580 VLAN 的数量	8.1(2)	ASA 5580 支持的 VLAN 数量从 100 增加到 250。
对透明模式的 IPv6 支持	8.2(1)	已为透明防火墙模式引入 IPv6 支持。

表 13-1　　透明模式接口的功能历史 （续）

功能名称	平台版本	功能信息
对 ASA 5580 10 千兆以太网接口上流量控制的暂停帧支持	8.2(2)	现可为流量控制启用暂停 (XOFF) 帧。 我们修改了以下屏幕： （单情景模式）Configuration > Device Setup > Interfaces > Add/Edit Interface > General （多情景模式，系统） Configuration > Interfaces > Add/Edit Interface。
透明模式的网桥组	8.4(1)	如果不想产生安全情景开销，或者要最大限度地使用安全情景，请将接口一起组合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组流量与其他网桥组是隔离开的。在单情景模式或每个情景中可配置多达八个网桥组，每组四个接口。 我们修改或引入了以下屏幕： Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > Interfaces > Add/Edit Interface
透明模式的网桥组最大数量增加到 250	9.3(1)	网桥组最大数量从 8 增加到 250。可在单情景模式或多情景模式中每个情景中配置多达 250 个网桥组，每个网桥组最多 4 个接口。 我们修改了以下屏幕： Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > Interfaces > Add/Edit Interface

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、域名及启用和 Telnet 密码

要设置主机名、域名及启用和 Telnet 密码，请执行以下步骤。

准备工作

- 在多情景模式中，可在系统和情景执行空间中配置主机名和域名。
- 启用和 Telnet 密码可在每个情景中设置；它们在系统中不可用。在多情景模式中发起从交换机到 ASASM 的会话时， ASASM 使用管理员情景中设置的登录密码。
- 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。

操作步骤

步骤 1 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，如果建立与多个设备的会话，则该主机名有助于跟踪命令输入位置。该主机名还用于系统日志消息。

对于多情景模式，在系统执行空间中设置的主机名均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显示在命令行中；但它可用于标题。

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至非限定名称。例如，如果将域名设置为 “example.com”，并以非限定名称 “jupiter” 指定系统日志服务器，则 ASA 将名称限定为 “jupiter.example.com”。

步骤 4　更改特权模式（启用）密码。默认密码为空。

如果不配置启用身份验证，则可使用启用密码进入特权 EXEC 模式。

如果不配置 HTTP 身份验证，还可使用启用密码以空白用户名登录 ASDM。

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，该登录密码可用于 Telnet 访问。通过 **session** 命令从交换机访问 ASASM 时也可使用该密码。

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** 以保存更改。

恢复启用和 Telnet 密码

忘记启用或 Telnet 密码时，可恢复它们。操作步骤因设备类型不同而异。必须使用 CLI 执行该任务。

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，然后再启动。

步骤 3　启动之后，在系统提示进入 ROMMON 模式时按下 **Escape** 键。

步骤 4　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，并询问是否要更改它：

```
Current Configuration Register: 0x00000041
Configuration Summary:
boot default image from Flash
  ignore system configuration

Do you wish to change this configuration?y/n [n]: y
```

步骤 6　记录当前配置寄存器值，以便稍后恢复。

步骤 7　在提示符处输入 **Y** 以更改值。

ASA 提示输入新值。

步骤 8　接受所有设置的默认值，但 “disable system configuration?” 值除外。

步骤 9　在提示符处输入 **Y**。

步骤 10　通过输入以下命令重新加载 ASA：

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```

ASA 加载默认配置，而非启动配置。

步骤 11　通过输入以下命令访问特权 EXEC 模式：

```
ciscoasa# enable
```

步骤 12　系统提示输入密码时，按下 **Enter**。

密码为空。

步骤 13　通过输入以下命令加载启动配置：

```
ciscoasa# copy startup-config running-config
```

步骤 14　通过输入以下命令访问全局配置模式：

```
ciscoasa# configure terminal
```

步骤 15　通过输入以下命令，根据需要在默认配置中更改密码：

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

步骤 16　通过输入以下命令加载默认配置：

```
ciscoasa(config)# no config-register
```

默认配置寄存器值为 0x1。有关配置寄存器的详细信息，请参阅命令参考。

步骤 17　通过输入以下命令，将新密码保存至启动配置：

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

恢复 ASA 5506、 5506-W 和 ASA 5508 上的密码

要恢复 ASA 5506、 5506-W 和 5508 的密码，请执行以下步骤：

操作步骤

步骤 1　连接到 ASA 控制台端口。

步骤 2　关闭 ASA，然后再启动。

步骤 3　启动之后，在系统提示进入 ROMMON 模式时按下 **Escape** 键。

步骤 4　要更新配置寄存器值，请输入以下命令：

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

ASA 显示当前配置寄存器值和配置选项列表。记录当前配置寄存器值，以便稍后恢复。

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ...... auto-boot index 1 image in disks
```

步骤 5　通过输入以下命令重新加载 ASA：

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASA 加载默认配置，而非启动配置。

步骤 6　通过输入以下命令访问特权 EXEC 模式：

```
ciscoasa# enable
```

步骤 7　系统提示输入密码时，按下 **Enter**。

密码为空。

步骤 8　通过输入以下命令加载启动配置：

```
ciscoasa# copy startup-config running-config
```

步骤 9　通过输入以下命令访问全局配置模式：

```
ciscoasa# configure terminal
```

步骤 10　通过输入以下命令，根据需要在默认配置中更改密码：

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

步骤 11　通过输入以下命令加载默认配置：

```
ciscoasa(config)# no config-register
```

默认配置寄存器值为 0x1。有关配置寄存器的详细信息，请参阅命令参考。

步骤 12　通过输入以下命令，将新密码保存至启动配置：

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

恢复 ASAv 上的密码或映像

要恢复 ASAv 上的密码或映像，请执行以下步骤：

操作步骤

步骤 1　将运行的配置复制到 ASAv 上的备份文件：

copy running - config *filename*

示例：

```
ciscoasa# copy running-config backup.cfg
```

步骤 2　重新启动 ASAv：

reload

步骤 3　从 GNU GRUB 菜单，按向下箭头，选择 **<filename> with no configuration load** 选项，然后按下 **Enter**。文件名为 ASAv 上的默认启动映像文件名。默认启动映像永远不会通过 **fallback** 命令自动启动。然后加载选定的启动映像。

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

示例：

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

步骤 4　将备份配置文件复制至运行的配置。

copy *filename* **running-config**

示例：

```
ciscoasa (config)# copy backup.cfg running-config
```

步骤 5　重置密码。

enable password

示例：

```
ciscoasa(config)# enable password cisco123
```

步骤 6　保存新配置。

write memory

示例：

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

禁用密码恢复

注　无法在 ASAv 上禁用密码恢复。

要禁用密码恢复以确保未授权用户无法使用密码恢复机制危害 ASA，请执行以下步骤。

准备工作

在 ASA 上， **no service password-recovery** 命令可防止通过在配置完整无损的情况下进入 ROMMON 模式。进入 ROMMON 模式时， ASA 提示擦除所有闪存文件系统。不先执行该擦除操作就无法进入 ROMMON 模式。如果选择不擦除闪存文件系统， ASA 就会重新加载。因为密码恢复取决于使用 ROMMON 模式和维护现有配置，因此，该擦除可防止恢复密码。但是，禁用密码恢复会防止未授权用户查看配置或插入不同的密码。在此情况下，要将系统恢复到操作状态，请加载新映像和备份配置文件 （如可用）。

service password-recovery 命令显示在配置文件中仅供参考。在 CLI 提示符处输入命令时，设置保存在 NVRAM 中。更改该设置的唯一方式就是在 CLI 提示符处输入命令。通过不同版本的命令加载新配置不会更改设置。如在将 ASA 配置为在启动时忽略 （为密码恢复作准备）启动配置的情况下禁用密码恢复，则 ASA 就会更改设置，以照常加载启动配置。如果使用故障转移，且将备用设备配置为忽略启动配置，则在 **no service password recovery** 命令复制到备用设备时也对配置寄存器作出相同更改。

操作步骤

步骤 1　禁用密码恢复。

```
no service password-recovery
```

示例：

```
ciscoasa (config)# no service password-recovery
```

设置日期和时间

注　请勿设置 ASASM 的日期和时间；它可从主机交换机接收这些设置。

- 第 14-6 页的使用 NTP 服务器设置日期和时间
- 第 14-7 页的手动设置日期和时间

使用 NTP 服务器设置日期和时间

NTP 用于实施分层服务器系统，可在网络系统中提供精确的同步时间。时间敏感性操作需要这种精确度，如验证 CRL，包括精确时间戳。可配置多个 NTP 服务器。 ASA 选择层级最低的服务器，作为衡量数据可靠性的方式。

NTP 服务器生成的时间将覆盖手动设置的任何时间。

准备工作

在多情景模式中，只能在系统配置中设置时间。

操作步骤

步骤 1　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。如果多个服务器准确度相似，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 将使用这个更准确的服务器。

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员情景接口。要确保稳定性，请选择 **None**（默认接口），以更改管理员情景（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 与 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，密钥字符串最长可达 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** 以保存更改。

手动设置日期和时间

要手动设置日期和时间，请执行以下步骤。

准备工作

在多情景模式中，只能在系统配置中设置时间。

操作步骤

步骤 1　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 Eastern Time、 Central Time、 Mountain Time 或 Pacific Time zone，则时间将自动调整为夏令时，从三月第二个星期日 2:00 a.m 开始到十一月第一个星期日 2:00 a.m. 结束。

注　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。然后使用一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，无需更改任何功能。使用主密码的功能包括：

- OSPF
- EIGRP
- VPN 负载均衡
- VPN （远程访问和站点对站点）
- 故障转移
- AAA 服务器
- 日志记录
- 共享许可证

注　如果已启用故障转移，但未设置故障转移共享密钥，则在更改主密码时就会显示错误消息，通知您必须输入故障转移共享密钥，以防主密码更改以纯文本形式发送。

选择 **Configuration > Device Management > High Availability > Failover**，在 Shared Key 字段输入任意字符，或者，如已选择故障转移十六进制密钥，则请输入 32 个十六进制数字 (0-9A-Fa-f)，退格符号除外。然后点击 **Apply**。

添加或更改主密码

要添加或更改主密码，请执行以下步骤。

准备工作

该操作步骤只能在安全会话中进行，例如通过控制台、 SSH 或通过 HTTPS 连接 ASDM。

操作步骤

步骤 1　选择以下选项之一：

- 在单一情景模式中，选择 **Configuration > Device Management > Advanced > Master Passphrase**。
- 在多情景模式中，选择 **Configuration > Device Management > Device Administration > Master Passphrase** 。

步骤 2　选中 **Advanced Encryption Standard (AES) password encryption** 复选框。

如果无有效主密码，则在点击 **Apply** 时将显示警告消息。可点击 **OK** 或 **Cancel** 以继续。

如果稍后禁用密码加密，所有的现有加密密码将保持不变，则只要主密码存在，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 到 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它。如果不知道密码，请参阅第 14-10 页的移除主密码。
- 此操作步骤只能在安全会话中进行；如通过 Telnet、 SSH，或通过 HTTPS 连接 ASDM。

操作步骤

步骤 1　选择以下选项之一：

- 在单一情景模式中，选择 **Configuration > Device Management > Advanced > Master Passphrase**。
- 在多情景模式中，选择 **Configuration > Device Management > Device Administration > Master Passphrase**。

步骤 2　选中 **Advanced Encryption Standard (AES) password encryption** 复选框。

如果无有效主密码，则在点击 **Apply** 时将显示警告语句。单击 **OK** 或 **Cancel** 以继续。

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它。

步骤 5　将 **New master passphrase** 和 **Confirm master passphrase** 字段留空。

步骤 6　点击 **Apply**。

移除主密码

无法恢复主密码。如果主密码丢失或未知，则可将其移除。

操作步骤

步骤 1　移除主密钥和包括加密密码的配置。

write erase

示例：

```
ciscoasa(config)# write erase
```

步骤 2　通过启动配置重新加载 ASA，无需任何主密钥或加密密码。

reload

示例：

```
ciscoasa(config)# reload
```

配置 DNS 服务器

需要配置 DNS 服务器，以便 ASA 能够将主机名解析为 IP 地址。

- 第 14-10 页的设置 DNS 服务器
- 第 14-11 页的监控 DNS 缓存

设置 DNS 服务器

某些 ASA 功能需要使用 DNS 服务器，以按域名访问外部服务器；例如，Botnet Traffic Filter 功能需要用 DNS 服务器访问动态数据库服务器并解析静态数据库中的条目。通过其他功能，如 **ping** 或 **traceroute** 命令，可输入要 ping 或 traceroute 的名称，而且， ASA 能够通过与 DNS 服务器进行通信来解析名称。许多 SSL VPN 和证书命令也支持名称。

还必须配置 DNS 服务器，以在访问规则中使用完全限定域名 (FQDN) 网络对象。

注　ASA 有限支持使用 DNS 服务器，具体取决于功能。

准备工作

确保为启用 DNS 域名查找所在的任何接口配置合适的路由和访问规则，以便能够达到 DNS 服务器。

操作步骤

步骤 1　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：

- **配置一个 DNS 服务器组**。
- **配置多个 DNS 服务器组**。

步骤 4　执行以下任一操作：

- 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 到 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，以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 DNS 检查均已启用。

步骤 8　点击 **Apply** 以保存更改。

监控 DNS 缓存

ASA 对来自外部 DNS 查询的 DNS 信息提供本地缓存，这些查询是为某些无客户端 SSL VPN 和证书命令发送的。首先在本地缓存中查找每个 DNS 转换请求。如果本地缓存中有该信息，则将返回生成的 IP 地址。如果本地缓存无法解析该请求，则将 DNS 查询发送至已配置的各个 DNS 服务器。如果外部 DNS 服务器解析请求，则生成的 IP 地址与其相应的主机名一起存储在本地缓存中。

如需监控 DNS 缓存，请参阅以下命令：

- **show dns-hosts**

  此命令显示 DNS 缓存，包括从 DNS 服务器中动态获悉的条目，以及使用 **name** 命令手动输入的名称和 IP 地址。

调整 ASP （加速安全路径）性能和行为

ASP 是实现层，在此使策略和配置付诸实施。除了在通过思科技术支持中心进行故障排除期间，其他操作均与该层无直接关系。但是，可以调整几项与性能和可靠性相关的行为。

- 第 14-12 页的选择规则引擎事务提交模型
- 第 14-12 页的启用 ASP 负载均衡

选择规则引擎事务提交模型

默认情况下，更改基于规则的策略 （如访问规则）时，更改会立即生效。但是，这种即时性将稍微降低性能。对于每秒连接速率较高的环境中超大型规则列表，性能降低更加显著，例如，在 ASA 每秒处理 18,000 次连接的同时更改拥有 25,000 条规则的策略。

由于规则引擎要编译规则以实现更快的规则查找，因此，性能将受到影响。默认情况下，系统在评估连接尝试时也搜索未编译规则，以便能够应用新规则；由于规则未编译，因此，搜索需要更长时间。

可更改此行为，以便规则引擎在执行规则更改、继续使用原规则直至新规则编译完成并可供使用时使用事务性模型。通过事务性模型，在规则编译期间性能应不会下降。下表阐明行为差异。

模型	编译前	编译中	编译后
默认值	匹配原规则。	匹配新规则。 （每秒连接速率降低。）	匹配新规则。
事务性	匹配原规则。	匹配原规则。 （每秒连接速率不受影响）	匹配新规则。

事务性模型的另一个优势是，替换接口上的 ACL 时，删除原 ACL 和应用新 ACL 之间无间隙。该功能减少了可接受连接在操作期间被断开的可能性。

提示 如果为某种规则类型启用事务性模型，则将生成系统日志以标记编译的开始和结束。这些系统日志的编号从 780001 到 780004。

要为规则引擎启用事务提交模型，请选择 **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
- 相对严重超载的接口接收环引起的超限，其中，单个核心无法承受负载。

asp load-balance per-packet 命令允许多个核心同时对接收自单个接口接收环的数据包施加作用。如果系统丢弃数据包，并且 **show cpu** 命令输出远远小于 100%，则此命令可能有助于您的吞吐量（如果数据包属于许多无关连接）。 **auto** 选项使 ASA 能够自动打开和关闭每数据包负载均衡。

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。

选择 **Configuration > Device > Management > Advanced > ASP**，然后选中 **Enable per-packet ASP load balance** 复选框。

选中 **Dynamically enable or disable ASP load balancing based on traffic monitoring** 复选框，在 ASA 5585 上自动启用 ASP 负载均衡。

基本设置历史

功能名称	平台版本	说明
主密码	8.3(1)	我们引入了此功能。主密码可供您用加密格式安全地存储纯文本密码，并提供一个对所有密码进行加密或掩蔽的通用密钥，无需更改任何功能。 我们引入了以下屏幕：Configuration > Device Management > Advanced > Master Passphrase。Configuration > Device Management > Device Administration > Master Passphrase。
默认 Telnet 密码的移除	9.0(2)/9.1(2)	为了提高 ASA 管理访问的安全性，已移除 Telnet 的默认登录密码；使用 Telnet 登录之前必须手动设置密码。 **注**　如果不配置 Telnet 用户身份验证，登录密码仅用于 Telent。 以前清除密码时， ASA 恢复默认值 “cisco”。现在清除密码时，密码即被移除。 登录密码还用于从交换机到 ASASM 的 Telnet 会话（请参阅 **session** 命令）。对于初始 ASASM 访问，必须使用 **service-module session** 命令，直到设置登录密码。 我们未修改任何 ASDM 屏幕。
ASP 负载均衡	9.3(2)	我们引入了此功能。 ASP 负载均衡机制允许 CPU 的多个核心接收并独立处理来自接口接收环的数据包，从而降低丢包率和提高吞吐量。 我们引入了以下屏幕：Configuration > Device Management > Advanced > ASP Load 主密码 Balancing。

DHCP 服务

本章介绍如何配置 DHCP 服务器或 DHCP 中继。

关于 DHCP 服务器

DHCP 为 DHCP 客户端提供网络配置参数，如 IP 地址。Cisco ASA 可为连接到 ASA 接口的 DHCP 客户端提供 DHCP 服务器。 DHCP 服务器直接为 DHCP 客户端提供网络配置参数。

客户端使用预留的链路范围组播地址查找 DHCP 服务器，以请求分配配置信息，该地址表明客户端和服务器应连接到同一链路。但是，在某些情况下，关注的是易管理性、经济性或可扩展性，我们建议您允许 DHCP 客户端向未连接到同一链路的服务器发送消息。可能驻留在客户端网络的 DHCP 中继代理可在客户端与服务器之间中转消息。中继代理操作对客户端来说是透明的。

IPv4 DHCP 客户端使用广播而非组播地址到达服务器。DHCP 客户端侦听 UDP 端口 68 上的消息；DHCP 服务器侦听 UDP 端口 67 上的消息。

在 RFC 3315 中为 IPv6 指定的 DHCP (DHCPv6) 可使 IPv6 DHCP 服务器向 IPv6 节点 （即 DHCP 客户端）发送配置参数，如网络地址或前缀和 DNS 服务器地址。 DHCPv6 使用以下组播地址：

- All_DHCP_Relay_Agents_and_Servers (FF02::1:2) 是客户端与相邻的 （即在连的）中继代理和服务器进行通信所使用的链路范围组播地址。所有 DHCPv6 服务器和中继代理均为此组播组的成员。
- DHCPv6 中继服务和服务器侦听 UDP 端口 547 上的消息。 ASA DHCPv6 中继代理在 UDP 端口 547 和 All_DHCP_Relay_Agents_and_Servers 组播地址上侦听。

关于 DHCP 中继代理

可配置 DHCP 中继代理以向一个或多个 DHCP 服务器转发接口上收到的 DHCP 请求。DHCP 客户端使用 UDP 广播发送其初始 DHCPDISCOVER 消息，因为它们没有与其所连接网络有关的信息。如果客户端位于不包含服务器的网段，则通常 UDP 广播不会由 ASA 进行转发，因为它不转发广播流量。

可通过配置接收广播来将 DHCP 请求转发到另一个接口上 DHCP 服务器的 ASA 接口来对此情况做出补救。

DHCP 服务的许可要求

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

对于所有 ASA 型号， DHCP 客户端地址的最大数量因许可证而异。

- 如果上限是 10 台主机，则最大可用 DHCP 池为 32 个地址。
- 如果上限是 50 台主机，则最大可用 DHCP 池为 128 个地址。
- 如果主机数量无限制，则最大可用 DHCP 池为 256 个地址。

DHCP 服务准则

防火墙模式准则

在透明防火墙模式中不受支持。有关详细信息，请参阅第 15-3 页的 DHCP 中继准则。

IPv6 准则

不支持特定接口 DHCP 中继服务器的 IPv6。

DHCP 服务器准则

- 最大可用 DHCP 池为 256 个地址。
- 只能在 ASA 的每个接口配置一个 DHCP 服务器。每个接口均可使用其自己的地址池。但是，其他 DHCP 设置 （如 DNS 服务器、域名、选项、 ping 超时和 WINS 服务器）以全局方式配置，且供 DHCP 服务器在所有接口上使用。
- 无法在已启用服务器的接口上配置 DHCP 客户端或 DHCP 中继服务。此外， DHCP 客户端必须直接连接到已启用服务器的接口。
- ASA 不支持 QIP DHCP 服务器与 DHCP 代理服务组合使用。
- 如也启用 DHCP 服务器，则不能启用中继代理。
- ASA DHCP 服务器不支持 BOOTP 请求。在多情景模式中，不能在多个情景中所使用接口上启用 DHCP 服务器或 DHCP 中继服务。

- 在收到 DHCP 请求后， ASA 向 DHCP 服务器发送发现消息。此消息包括在组策略中已通过 **dhcp-network-scope** 命令配置的 IP 地址 （在子网内）。如果服务器有属于该子网的地址池，则服务器将向 IP 地址 - 而非发现消息的源 IP 地址发送要约消息和池信息。
- 客户端连接后， ASA 向服务器列表中的所有服务器发送发现消息。此消息包括在组策略中已通过 **dhcp-network-scope** 命令配置的 IP 地址 （在子网内）。 ASA 选择收到的第一条要约并丢弃其他要约。如果服务器有属于该子网的地址池，则服务器将向 IP 地址 - 而非发现消息的源 IP 地址发送要约消息和池信息。如果需要更新地址，则其将尝试与租赁服务器 （从其获得地址的服务器）更新地址。如果 DHCP 更新在指定次数的重试（四次尝试）后失败，则 ASA 将在过了预定时间段之后移至 DHCP 重新绑定阶段。在重新绑定阶段， ASA 向组中所有服务器同时发送请求。在高可用性环境中，租赁信息是共享的，因此，其他服务器可以确认租赁，并且 ASA 将返回到绑定状态。在重新绑定阶段，如未收到服务器列表中任何服务器的响应 （三次重试后），则 ASA 将清除此类条目。

  例如，如果服务器有一个范围在 209.165.200.225 到 209.165.200.254 之间的池，掩码为 255.255.255.0，**dhcp-network-scope** 命令指定的 IP 地址为 209.165.200.1，则服务器将要约消息中的该池发送给 ASA。

  dhcp-network-scope 命令设置仅适用于 VPN 用户。

DHCP 中继准则

- 在单一模式和每个情景中，最多可以配置 10 台 DHCPv4 中继服务器，这些服务器为全局和特定接口服务器的组合，其中每个接口最多允许 4 台服务器。
- 在单一模式和每个情景中，最多可以配置 10 台 DHCPv6 中继服务器。不支持 IPv6 的特定接口服务器。
- 如也启用 DHCP 服务器功能，则不能启用中继代理。
- 如已启用 DHCP 中继服务，且定义了多台 DHCP 中继服务器，则 ASA 将向每个已定义的 DHCP 中继服务器转发客户端请求。来自服务器的回复也会转发到客户端，直到解除客户端 DHCP 中继绑定。如果 ASA 接收到以下任意 DHCP 消息：ACK、 NACK、 ICMP 不可达或拒绝，则绑定解除。
- 不能启用接口上作为 DHCP 代理服务运行的 DHCP 中继服务。必须首先移除 VPN DHCP 配置，否则将显示错误消息。在同时启用 DHCP 中继和 DHCP 代理服务后，将出现此错误。确保已启用 DHCP 中继或 DHCP 代理服务，但不能同时启用两者。
- 在透明防火墙模式中， DHCP 中继服务不可用。但是，可通过使用访问列表允许 DHCP 流量通过。要在透明模式中允许 DHCP 请求和回复通过 ASA，则需要配置两个访问列表，一个允许从内部接口到外部接口的 DCHP 请求，另一个允许来自其他方向的服务器的回复。
- 对于 IPv4，客户端必须直接连接到 ASA 且不能通过另一个中继代理或路由器发送请求。对于 IPv6， ASA 支持来自另一个中继服务器的数据包。
- 对于多情景模式，不能在多个情景使用的接口上启用 DHCP 中继。
- DHCP 客户端必须与 ASA 中继请求的 DHCP 服务器位于不同接口。

配置 DHCP 服务器

本节介绍如何配置 ASA 提供的 DHCP 服务器。

步骤 1 启用 DHCP 服务器。请参阅第 15-4 页的启用 DHCP 服务器。

步骤 2 配置高级 DHCP 选项。请参阅第 15-5 页的配置高级 DHCP 选项。

步骤 3 配置 DHCPv4 中继代理或 DHCPv6 中继代理。请参阅第 15-6 页的配置 DHCPv4 中继代理或第 15-7 页的配置 DHCPv6 中继代理。

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 选择 **Configuration > Device Management > DHCP > DHCP Server**。

步骤 2 选择一个接口，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 （主要和次要）。
- 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。有关详细信息，请参阅第 15-5 页的配置高级 DHCP 选项。

d. 请选中 **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 服务器还应该执行以下更新操作：

- 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，以便用 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 （单位为秒）。有效值范围为 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 等到 DHCP ping 尝试超时所需时间 （单位为毫秒）。有效值范围为 10 到 10000 毫秒。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，请参阅第 15-5 页的配置高级 DHCP 选项。

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** 以保存更改。

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。

可以使用高级 DHCP 选项向 DHCP 客户端提供 DNS、WINS 和域名参数。也可以使用 DHCP 自动配置设置获得这些值或手动定义这些值。如果使用多种方法定义此信息，则按以下序列将其传递给 DHCP 客户端：

1. 手动配置的设置。
2. 高级 DHCP 选项设置。
3. DHCP 自动配置设置。

例如，可以手动定义想要 DHCP 客户端接收的域名，然后启用 DHCP 自动配置。尽管 DHCP 自动配置要结合 DNS 和 WINS 服务器发现域，但手动定义的域名将与已发现的 DNS 和 WINS 服务器名称一起传递到 DHCP 客户端，因为手动定义的域名将取代通过 DHCP 自动配置过程发现的域名。

操作步骤

步骤 1　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住，选项参数限定于受该选项支持的哪些参数。对于所有其他选项，仅显示选项编号，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，仅受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 选项列表中移除。

- 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　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　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（现场转储文件），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，输入一个偶位数且无空格的十六进制字符串。无需使用 0x 前缀。

  注　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** 以保存更改。

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。可以配置以下类型的服务器：

- 接口特定 DHCP 服务器 - DHCP 请求进入特定接口后， ASA 仅向接口特定服务器中继请求。
- 全局 DHCP 服务器 - DHCP 请求进入未让接口特定服务器得以配置的接口后， ASA 将向所有全局服务器中继请求。如果接口有接口特定服务器，则将不使用全局服务器。

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　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。此操作使客户端能设置将指向 ASA 的其默认路由，即使 DHCP 服务器指定了另一个路由器。如果数据包内无默认路由器选项，则 ASA 将添加一个包含接口地址的选项。
- **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 **Add**。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特定 DHCP 服务器。

a. 点击 **Add**。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，对于全局 DHCP 服务器，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）。 IPv6 不受特定接口服务器支持。
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** 以保存设置。

监控 DHCP 服务

有关如何监控 DHCP 服务，请参阅以下屏幕：

- **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**

  此窗格显示已配置动态 DHCP 客户端 IP 地址。
- **Monitoring > Interfaces > DHCP > DHCP Statistics**

  此窗格显示 DHCP 消息类型、计数器、值、方向、接收的消息和发送的消息。
- **Tools > Command Line Interface**

  此窗格将非交互式命令发送至 ASA 并列出结果。

DHCP 服务的历史记录

表 15-1　DHCP 服务的历史记录

功能名称	平台版本	说明
DHCP	7.0(1)	ASA 可以向连接到 ASA 接口的 DHCP 客户端提供 DHCP 服务器或 DHCP 中继服务。 我们引入了以下屏幕： Configuration > Device Management > DHCP > DHCP Relay. Configuration > Device Management > DHCP > DHCP Server.
DHCP for IPv6 (DHCPv6)	9.0(1)	已添加对 IPv6 的支持。 我们修改了以下屏幕：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。 IPv6 不受单个接口 DHCP 中继之支持。 我们修改了以下屏幕：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。 我们修改了以下屏幕：Configuration > Device Management > DHCP > DHCP Relay。
DHCP 重新绑定功能	9.1(4)	在 DHCP 重新绑定阶段，客户端尝试重新绑定到隧道组列表中的其他 DHCP 服务器。在此版本之前，当 DHCP 租约未能更新时，客户端不重新绑定到备用服务器。 我们未修改任何 ASDM 屏幕。

动态 DNS

本章介绍如何配置动态 DNS (DDNS) 更新方法。

关于 DDNS

DDNS 更新将 DNS 与 DHCP 相集成。这两种协议互为补充：DHCP 实现 IP 地址分配集中化和自动化； DDNS 更新按预定义时间间隔自动记录已分配地址与和主机名之间的关联。DDNS 允许频繁更新不断变化的地址与主机名的关联。例如，移动主机可以自由地在网络中移动而无需用户或管理员干预。DDNS 在 DNS 服务器上为名称与地址之间的相互映射提供必需的动态更新和同步。

DDNS 名称与地址之间的映射以两种资源记录 (RR) 保留在 DHCP 服务器上：A RR 将名称映射至 IP 地址，而 PTR RR 将地址映射至名称。执行 DDNS 更新的两个方法中 - RFC 2136 定义的 IETF 标准和通用 HTTP 方法 - ASA 支持 IETF 方法。

相关主题

- 第 15-4 页的配置 DHCP 服务器

DDNS 更新配置

最常见的两种 DDNS 更新配置如下：

- DHCP 客户端更新 A RR，而 DHCP 服务器更新 PTR RR。
- DHCP 服务器既更新 A RR 也更新 PTR RR。

通常， DHCP 服务器代表客户端维护 DNS PTR RR。可将客户端配置为执行所有所需 DNS 更新。可将服务器配置为是否履行这些更新。 DHCP 服务器必须了解客户端的完全限定域名 (FQDN) 才能更新 PTR RR。客户端使用一个名为 Client FQDN 的 DHCP 选项向服务器提供 FQDN。

UDP 数据包大小

DDNS 允许 DNS 请求方通告其 UDP 数据包的大小并促进传输大于 512 八位字节的数据包。当一个 DNS 服务器收到通过 UDP 提出的请求时，它会从 OPT RR 识别 UDP 数据包的大小，并将其回应扩展为包含尽可能多的资源记录，但不能超过请求方指定的 UDP 数据包大小上限。对于 BIND， DNS 数据包的大小不得超过 4096 字节，对于 Windows 2003 DNS 服务器，则不得超过 1280 字节。有多个其他 **message-length maximum** 命令可用：

- 现有全局限制：**message-length maximum 512**
- 客户端或服务器特定限制：**message-length maximum client 4096 and message-length maximum server 4096**
- OPT RR 字段中指定的动态值：**message-length maximum client auto**

如果三个命令同时存在，则 ASA 允许自动配置的长度不超过已配置客户端或服务器最大支持数量。对于所有其他 DNS 流量，则使用 message - length maximum。

DDNS 准则

情景模式准则

仅在透明模式中支持 DNS Client 窗格。

配置 DDNS

本节介绍如何配置 DDNS。

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　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 至 364 中选择更新尝试之间的天数。
- 从 0 至 23 中选择更新尝试之间的小时数 （取整数）。
- 从 0 至 59 中选择更新尝试之间的分钟数 （取整数）。
- 从 0 至 59 中选择更新尝试之间的秒数 （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　选择下列选项之一存储 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　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　选择以下选项之一存储资源记录更新：

- 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　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** 以放弃更改并输入新设置。

监控 DDNS

如需监控 DDNS 状态，请参阅以下屏幕：

- **Tools > Command Line Interface**

  此窗格将非交互式命令发送至 ASA 并列出结果。

DDNS 历史记录

表 16-1　　DDNS 历史记录

功能名称	版本	功能信息
DDNS	7.0(1)	我们引入了此功能。 我们引入了以下屏幕： Configuration > Device Management> DNS > DNS Client。 Configuration > Device Management > DNS > Dynamic DNS。

第 5 部分

对象和 ACL

访问控制对象

对象指配置中可重用的组件。您可以在思科 ASA 配置中定义和使用对象来代替内联 IP 地址、服务、名称等。您可以使用对象轻松维护配置，因为您只需要修改某一位置的对象，便可以使该对象在引用它的所有其他位置显示出来。如未使用对象，必要时您必须逐一修改每项功能的参数，而不是一次性修改完成。例如，如果网络对象定义了 IP 地址和子网掩码，当您要更改地址时，您只需要在对象定义中进行更改，而无需在引用该 IP 地址的各项功能中逐一更改。

对象准则

IPv6 准则

在以下限制条件下支持 IPv6：

- ASA 不支持 IPv6 嵌套网络对象组，因此您无法将含有 IPv6 条目的对象划分在另一个 IPv6 对象组下。
- 您可以将 IPv4 和 IPv6 条目混合在同一网络对象组中；但您无法使用混合对象组进行 NAT。

附加准则和限制

- 由于对象和对象组共享同一命名空间，因此对象名称必须唯一。当您可能要创建名为“Engineering”的网络对象组以及名为“Engineering”的服务对象组时，您需要在至少其中一个对象组名称的末尾添加一个标识符（或“标记”），使其名称唯一。例如，可以使用名称“Engineering_admins”和“Engineering_hosts”，使对象组名称保持唯一，同时有助于进行识别。
- 对象名称限于 64 个字符，包括字母、数字和如下字符：.!@#$%^&()-_{}。对象名称区分大小写。
- 如果在命令中使用对象，您无法将对象移除或留空，除非启用 前向引用（在访问规则高级设置中）。

配置对象

以下各节介绍了如何配置主要用于访问控制的对象。

配置网络对象和组

网络对象和组可以识别 IP 地址或主机名。您可以使用访问控制列表中的这些对象来简化规则。

配置网络对象

网络对象可以包含主机、网络 IP 地址、 IP 地址范围或完全限定域名 (FQDN)。

您也可以启用对象的 NAT 规则 （FQDN 对象除外）。有关配置对象 NAT 的详细信息，请参阅防火墙配置指南。

操作步骤

步骤 1　选择 **Configuration > Firewall > Objects > Network Objects/Group**。

步骤 2　执行以下任一操作：

- 选择 **Add > Network Object**，添加新的对象。输入名称和说明 （后者为可选项）。
- 选择现有的对象，然后点击 **Edit**。

步骤 3　基于对象 **Type** 和 **IP version** 字段配置对象的地址。

- **Host** - 单个主机的 IPv4 或 IPv6 地址。例如， 10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **Network** - 网络的地址。对于 IPv4，请添加掩码，例如， **IP address** = 10.0.0.0 **Netmask** = 255.0.0.0。对于 IPv6，请添加前缀，例如 **IP Address** = 2001:DB8:0:CD30:: **Prefix Length** = 60。
- **Range** - 地址的范围。您可以指定 IPv4 或 IPv6 范围。请勿添加掩码和前缀。
- **FQDN** - 完全限定域名，即主机的名称，例如 www.example.com。

步骤 4　点击 **OK**，然后点击 **Apply**。

您现在即可使用该网络对象来创建规则。如果编辑对象，则使用该对象的任何规则都将自动继承更改。

配置网络对象组

网络对象组可以包含多个网络对象以及内联网络或主机。网络对象组可以同时包含 IPv4 和 IPv6 地址。

但是，你无法使用包含 IPv4 和 IPv6 的混合对象组进行 NAT，也无法使用包含 FQDN 对象的对象组。

操作步骤

步骤 1　选择 **Configuration > Firewall > Objects > Network Objects/Groups**。

步骤 2　执行以下任一操作：

- 选择 **Add > Network Object Group**，添加新的对象。输入名称和说明 （后者为可选项）。
- 选择现有的对象，然后点击 **Edit**。

步骤 3　使用以下方法的任意组合将网络对象添加到组：

- **Existing Network Objects/Groups** - 选择已定义的任何网络对象或组，然后点击 **Add** 将其添加到组。
- **Create New Network Object Member** - 输入适用于新网络对象的条件，然后点击 **Add**。如果为对象命名，则当应用更改时，会创建新的对象并添加到组中。添加主机或网络时，名称为可选项。

步骤 4　添加所有成员对象之后，点击 **OK**，然后点击 **Apply**。

您现在即可在创建规则时使用该网络对象。对于已编辑的对象组，使用该组的任何规则都将自动继承更改。

配置服务对象和服务组

服务对象和组可标识协议和端口。您可以使用访问控制列表中的这些对象来简化规则。

- 第 17-3 页的配置服务对象
- 第 17-4 页的配置服务组

配置服务对象

服务对象可包含单一协议、 ICMP、 ICMPv6、 TCP 或 UDP 端口或端口范围。

操作步骤

步骤 1　选择 **Configuration > Firewall > Objects > Service Object/Group**。

步骤 2　执行以下任一操作：

- 选择 **Add > Service Object**，添加新的对象。输入名称和说明 （后者为可选项）。
- 选择现有的对象，然后点击 **Edit**。

步骤 3　选择服务类型，并填写所需的详细信息：

- Protocol - 介于 0 到 255 之间的编号或已知名称，如 **ip**、**tcp**、**udp**、**gre** 等。有关编号、名称及其含义的列表，请参阅第 43-10 页的协议和应用。
- ICMP, ICMP6 - 您可以将消息类型和代码字段留空，以匹配任何 ICMP/ICMP 第 6 版消息。或者，您可以按名称或编号 (0 - 255) 指定 ICMP 类型，以便将对象限于该消息类型。如果指定类型，则可以选择为该类型指定一个 ICMP 代码 (1-255)。如果不指定代码，则将使用所有代码。有关 ICMP 类型的列表，请参阅第 43-14 页的 ICMP 类型。
- TCP, UDP - 或者，您可以指定源端口、目标端口或两者。可以按名称或编号指定端口 （有关列表，请参阅第 43-10 页的 TCP 和 UDP 端口）。您可以添加以下操作符：
  - **<** - 小于。例如， <80。
  - **>** - 大于。例如， >80。
  - **!=** - 不等于。例如， !=80。
  - **-** (hyphen) - 值的包含范围。例如， 100-200。

步骤 4　点击 **OK**，然后点击 **Apply**。

配置服务组

服务对象组可以包括协议组合，必要时包括适用于 TCP 或 UDP 的可选源端口和目标端口。

准备工作

您可以使用通用服务对象组来建立所有服务的模型 （如本节所介绍）。不过，您仍然可以配置 ASA 8.3(1) 版本之前可用的服务组对象的类型。上述旧版对象包括 TCP/UDP/TCP-UDP 端口组、协议组和 ICMP 组。这些组的内容与通用服务对象组中的关联配置等效， ICMP 组除外，因为这些组不支持 ICMP6 和 ICMP 代码。如果您仍要使用这些旧版对象，请参阅 Cisco.com 网站上命令参考中的 **object-service** 命令说明以了解详细说明。

操作步骤

步骤 1　选择 **Configuration > Firewall > Objects > Service Objects/Groups**。

步骤 2　执行以下任一操作：

- 选择 **Add > Service Group**，添加新的对象。输入名称和说明 （后者为可选项）。
- 选择现有的对象，然后点击 **Edit**。

步骤 3　使用以下方法的任意组合将服务对象添加到组：

- **Existing Service Objects/Groups** - 选择已定义的任何服务对象或组，然后点击 **Add** 将其添加到组。
- **Create New Service Object Member** - 输入适用于新服务对象的条件，然后点击 **Add**。如果为对象命名，则当应用更改时，会创建新的对象并添加到组；否则，未命名的对象仅为该组的成员。您无法为 TCP-UDP 对象命名；这些对象仅为组的成员。

步骤 4　添加所有成员对象之后，点击 **OK**，然后点击 **Apply**。

您现在即可在创建规则时使用该服务对象。对于已编辑的对象组，使用该组的任何规则都将自动继承更改。

配置本地用户组

您可以创建本地用户组，通过将组列入扩展 ACL 中，在支持身份防火墙的功能中使用本地用户组，进而用于访问规则等。

ASA 为 Active Directory 域控制器中全局定义的用户组将 LDAP 查询发送到 Active Directory 服务器。 ASA 会导入这些组，将其用于基于身份的规则。但是， ASA 可能已将未全局定义的网络资源本地化，这些网络资源需要具有本地化安全策略的本地用户组。本地用户组可包含嵌套组和从 Active Directory 导入的用户组。 ASA 可整合本地和 Active Directory 组。

用户可以属于本地用户组和从 Active Directory 导入的用户组。

由于您能够在 ACL 中直接使用用户名和用户组，因此只有在以下情况下您才需配置本地用户组：

- 要创建 LOCAL 数据库中定义的一组用户。
- 要创建在 AD 服务器定义的单一用户组中未捕获的一组用户或用户组。

有关如何启用身份防火墙的详细信息，请参阅第 32 章，“身份防火墙”。

操作步骤

步骤 1　选择 **Configuration > Firewall > Objects > Local User Groups**。

步骤 2　执行以下任一操作：

- 选择 **Add**，添加新的对象。输入名称和说明 （后者为可选项）。
- 选择现有的对象，然后点击 **Edit**。

步骤 3　使用下列任意一种方法，将用户或组添加到对象：

- **Select existing users or groups** - 选择包含用户或组的域，从列表中选择用户名或组名，然后点击 **Add**。对于长列表，您可以使用 Find 框方便查找用户。这些名称是从服务器中为所选域拉出来的。
- **Manually type user names** - 您可以简单地在底部编辑框中键入用户名或组名，然后点击 **Add**。使用此方法时，如果您未指定域，所选域名会被忽略，并且将使用默认域。对于用户名，格式为 *domain_name\username* ；对于组，则带双斜号 \\，格式为 *domain_name\\group_name*。

步骤 4　添加所有成员对象之后，点击 **OK**，然后点击 **Apply**。

您现在即可在创建规则时使用该用户对象组。对于已编辑的对象组，使用该组的任何规则都将自动继承更改。

配置安全组对象组

您可以创建安全组对象组，通过将组列入扩展 ACL 中，在支持 思科 TrustSec 的功能中使用安全组对象组，进而用于访问规则等。

与思科 TrustSec 集成后，ASA 可以从 ISE 下载安全组信息。ISE 可以提供思科 TrustSec 标记到用户的身份映射以及思科 TrustSec 标记到服务器的资源映射，从而充当身份储存库。您可以在 ISE 上集中部署和管理安全组 ACL。

但是， ASA 可能已将未全局定义的网络资源本地化，这些网络资源需要具有本地化安全策略的本地安全组。本地安全组可以包含从 ISE 下载的嵌套安全组。 ASA 可以整合本地和中央安全组。

要在 ASA 上创建本地安全组，请创建一个本地安全对象组。本地安全对象组可以包含一个或多个嵌套安全对象组、安全 ID 或安全组名称。您还可以创建 ASA 中不存在的 新安全 ID 或安全组名称。

您可以使用在 ASA 中创建的安全对象组来控制对网络资源的访问。您可以将安全对象组作为访问组或服务策略的一部分。

有关如何集成 ASA 和 Trustsec 的详细信息，请参阅第 33 章， “ASA 和思科 TrustSec”。

提示　如果使用 ASA 未知的标记和名称来创建组，则使用该组的任何规则都将处于非活动状态，直到您使用 ISE 对标记或名称解析成功为止。

操作步骤

步骤 1　选择 **Configuration > Firewall > Objects > Security Group Object Groups**。

步骤 2　执行以下任一操作：

- 选择 **Add** ，添加新的对象。输入名称和说明 （后者为可选项）。
- 选择现有的对象，然后点击 **Edit**。

步骤 3　使用下列任意一种方法，将安全组添加到对象：

- **Select existing local security group object groups** - 从已定义的对象列表中选择，然后点击 **Add**。对于长列表，您可以使用 Find 框方便查找对象。
- **Select security groups discovered from ISE** - 从现有组列表中选择组，然后点击 **Add**。
- **Manually add security tags or names** - 您可以简单地在底部编辑框中键入标记号或安全组名称，然后点击 **Add**。标记为一个介于 1 和 65533 之间的数字，由 ISE 通过 IEEE 802.1X 身份验证、网络身份验证或 MAC 身份验证旁路 (MAB) 分配给设备。安全组名称在 ISE 上创建，为安全组提供用户友好的名称。此安全组表将 SGT 映射到安全组名称。有关有效标记和名称，请查阅 ISE 配置。

步骤 4　添加所有成员对象之后，点击 **OK**，然后点击 **Apply**。

您现在即可在创建规则时使用该安全组对象组。对于已编辑的对象组，使用该组的任何规则都将自动继承更改。

配置时间范围

时间范围对象定义了由起始时间、结束时间和可选循环条目组成的特定时间。您可以将这些对象用于 ACL 规则，从而提供对特定功能或资产基于时间的访问。例如，您可以创建一条仅允许在工作时间对特定服务器进行访问的访问规则。

注　您可以在时间范围对象中列入多个定期条目。如果时间范围规定了绝对值和周期值，则只有在达到绝对起始时间后才开始评估周期值，而且在绝对结束时间到达后便不再对其进行评估。

创建时间范围并不会限制对设备的访问。该操作步骤仅定义时间范围。您随后必须在访问控制规则中使用该对象。

操作步骤

步骤 1　选择 **Configuration > Firewall > Objects > Time Ranges**。

步骤 2　执行以下任一操作：

- 选择 **Add**，添加新的时间范围。输入名称和说明 （后者为可选项）。
- 选择现有的时间范围，然后点击 **Edit**。

步骤 3　选择总体起始和结束时间。

默认为立即开始且永不结束，但是您可以设置特定日期和时间。您输入的时间包含在时间范围内。

步骤 4　（可选）配置总体活动时间内的循环时间段，例如时间范围将在一周内的某些日期或每周循环间隔内处于活动状态。

a. 点击 **Add**，或选择现有时间段并点击 **Edit**。

b. 执行以下任一操作：

- 点击 **Specify days of the week and times on which this recurring range will be active**，并从列表中选择日期和时间。
- 点击 **Specify a weekly interval when this recurring range will be active**，并从列表中选择日期和时间。

c. 点击 **OK**。

步骤 5　点击 **OK**，然后点击 **Apply**。

监控对象

对于网络、服务和安全组对象，您可以分析单个对象的使用情况。在 **Configuration > Firewall > Objects** 文件夹中，找到对象所在页面，然后点击 **Where Used** 按钮。

对于网络对象，也可以点击 Not Used 按钮，查找在任何规则以及其他对象中都未使用的对象。该屏幕提供了一个删除这些未使用对象的快捷方式。

对象的历史记录

功能名称	平台 版本	说明
对象组	7.0(1)	对象组可简化 ACL 的创建和维护。
正则表达式和策略映射	7.2(1)	引入了正则表达式和策略映射，将其用于检查策略映射下。引入了以下命令：**class-map type regex**、 **regex** 和 **match regex**。
对象	8.3(1)	引入了对象支持功能。

功能名称	平台 版本	说明
用于身份防火墙的用户对象组	8.4(2)	引入了用于身份防火墙的用户对象组。
用于思科 TrustSec 的安全组对象组	8.4(2)	引入了用于思科 TrustSec 的安全组对象组
IPv4 和 IPv6 混合网络对象组	9.0(1)	之前，网络对象组只能包含全 IPv4 地址或全 IPv6 地址。现在网络对象组可以同时包含 IPv4 和 IPv6 地址。 **注**　　您无法使用混合对象组进行 NAT。
用于按 ICMP 代码过滤 ICMP 流量的扩展 ACL 和对象增强	9.0(1)	现在您可以根据 ICMP 代码允许 / 拒绝 ICMP 流量。 我们引入或修改了以下屏幕： Configuration > Firewall > Objects > Service Objects/Groups Configuration > Firewall > Access Rule

访问控制列表

访问控制列表 (ACL) 在许多不同的功能中使用。作为访问规则应用到接口或全局应用时，这些列表可允许或拒绝通过设备的流量。对于其他功能， ACL 可选择功能所适用的流量，执行匹配服务而非控制服务。

以下各节介绍了 ACL 的基本信息以及如何配置和监控 ACL。在 防火墙配置指南 中详细介绍了作为访问规则全局应用或应用到接口的 ACL。

关于 ACL

访问控制列表 (ACL) 通过一个或多个特征识别流量，包括源和目标 IP 地址、 IP 协议、端口、EtherType 及其他参数，视 ACL 类型而定。ACL 可用于各种功能。ACL 由一个或多个访问控制条目 (ACE) 组成。

ACL 类型

ASA 使用以下类型的 ACL：

- 扩展 ACL - 扩展 ACL 是您将使用的主要类型。这些 ACL 用于访问规则以允许和拒绝通过设备的流量，并在许多功能中用于流量匹配，包括服务策略、 AAA 规则、 WCCP、僵尸网络流量过滤器、 VPN 组和 DAP 策略。在 ASDM 中，这些功能大部分都有各自的规则页面，并且无法使用您在 ACL 管理器中定义的扩展 ACL，但 ACL 管理器将显示在这些页面上创建的 ACL。请参阅第 18-6 页的配置扩展 ACL。
- EtherType ACL - EtherType ACL 适用于透明防火墙的第 2 层非 IP 流量。您可以使用这些规则，根据第 2 层数据包中的 EtherType 值允许或丢弃流量。通过 EtherType ACL，您可以控制设备上的非 IP 流量。请参阅 《防火墙配置指南》中的 “ 访问规则 ” 章节。
- Webtype ACL - Webtype ACL 用于过滤无客户端 SSL VPN 流量。这些 ACL 可基于 URL 或目标地址拒绝访问。请参阅第 18-9 页的配置 Webtype ACL。
- 标准 ACL - 标准 ACL 只能基于目标地址识别流量。使用这种 ACL 的功能较少：路由映射和 VPN 过滤器。由于 VPN 过滤器还允许扩展访问列表，因此限制将标准 ACL 用于路由映射。请参阅第 18-8 页的配置标准 ACL。

下表列出了 ACL 的一些常见用途及使用的类型。

表 18-1　ACL 类型和常见用途

ACL 用途	ACL 类型	说明
控制 IP 流量的网络访问 （路由和透明模式）	扩展	ASA 不允许任何从低安全性接口到高安全性接口的流量，除非扩展 ACL 明确允许。 **注**　要访问 ASA 接口以进行管理访问，您无需 ACL 允许主机 IP 地址。您只需要根据第 36 章，“管理访问”配置管理访问。
识别 AAA 规则的流量	扩展	AAA 规则使用 ACL 识别流量。
为给定用户增强 IP 流量的网络访问控制	扩展，按用户从 AAA 服务器下载	您可以配置 RADIUS 服务器以下载要应用于用户的动态 ACL，或服务器可以发送您已在 ASA 上配置的 ACL 名称。
VPN 访问和过滤	扩展 标准	用于远程访问和站点到站点 VPN 的组策略使用标准或扩展 ACL 进行过滤。远程访问 VPN 还将扩展 ACL 用于客户端防火墙配置和动态访问策略。
为模块化策略框架识别流量类映射中的流量	扩展	ACL 可用于识别类映射中的流量，该用途用于支持模块化策略框架的功能。支持模块化策略框架的功能包括 TCP 和常规连接设置，以及检查。
对于透明防火墙模式，控制非 IP 流量的网络访问	EtherType	您可以配置一个基于其 EtherType 来控制流量的 ACL。
识别路由过滤和重分布	标准 扩展	各种路由协议将标准 ACL 用于 IPv4 地址（扩展 ACL 用于 IPv6 地址）的路由过滤和重分布 （通过路由映射）。
无客户端 SSL VPN 过滤	Webtype	您可以配置 Webtype ACL 以过滤 URL 和目标。

ACL 管理器

ACL 管理器有两种显示方式：

- 例如，在主窗口中，通过选择 **Configuration > Firewall > Advanced > ACL Manager** 显示。在这种情况下， ACL 管理器仅显示扩展 ACL。此类 ACL 包括您在 Access Rules、 Service Policy Rules 和 AAA Rules 页面创建的规则所产生的 ACL。请注意，您在 ACL 管理器中进行的编辑不会对这些规则造成负面影响；您在此处进行的更改将在其他页面上反映。
- 在要求 ACL 的策略上，通过点击字段旁边的 **Manage** 按钮显示。在这种情况下，ACL 管理器可以为标准 ACL 和扩展 ACL 提供单独的选项卡，前提是该策略允许任一类型的 ACL。否则，视图将被过滤为仅显示标准、扩展或 Webtype ACL。 ACL 管理器绝不会显示 EtherType ACL。

标准 ACL 和 Webtype ACL 具有单独的页面，因此，您可以在主窗口中配置这些 ACL。这些页面在功能上相当于不含名称的 ACL 管理器：

- 标准 ACL - **Configuration > Firewall > Advanced > Standard ACL**。
- Webtype ACL - **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACL**。

ACL 名称

每个 ACL 都有一个名称或数字 ID，如 outside_in、OUTSIDE_IN 或 101。名称限于不超过 241 个字符。请考虑全部使用大写字母，以便在查看运行配置时时更方便地查找名称。

制定一个可帮助您识别 ACL 的预期用途的命名约定。例如， ASDM 使用约定 *interface-name_purpose_direction*，例如， outside_access_in，用于在入站方向应用于 “ 外部 ” 接口的 ACL。

一般来说，ACL ID 为数字。标准 ACL 的范围为 1 - 99 或 1300 - 1999。扩展 ACL 的范围为 100 - 199 或 2000 - 2699。 ASA 不强制执行这些范围，但如果您要使用编号，可能要遵守这些约定以便与运行 IOS 软件的路由器保持一致。

访问控制条目顺序

ACL 由一个或多个 ACE 组成。除非您明确将 ACE 插入给定行，否则您为给定 ACL 名称输入的每个 ACE 都将附加到 ACL 的末尾。

ACE 的顺序非常重要。当 ASA 决定是转发还是丢弃数据包时， ASA 会按照条目所列顺序对每个 ACE 测试数据包。找到匹配项后，不会再检查 ACE。

因此，如果将一条更具体的规则放在一条更通用的规则之后，则该更具体的规则可能永远不会被命中。例如，如果要允许网络 10.1.1.0/24，但要丢弃该子网上来自主机 10.1.1.15 的流量，则拒绝 10.1.1.15 的 ACE 必须排在允许 10.1.1.0/24 的 ACE 之前。如果允许 10.1.1.0/24 的 ACE 排在前面，则将允许 10.1.1.15，并且用以拒绝的 ACE 将永远不会被匹配。

根据需要使用 Up 和 Down 按钮重新排列规则。

允许 / 拒绝与匹配 / 不匹配

访问控制条目 “ 允许 ” 或 “ 拒绝 ” 与规则匹配的流量。将 ACL 应用到确定是允许流量通过 ASA 还是丢弃流量的功能时，例如全局和接口访问规则， “ 允许 ” 和 “ 拒绝 ” 即表示实际的允许和拒绝。

对于其他功能，例如服务策略规则， “ 允许 ” 和 “ 拒绝 ” 实际上表示 “ 匹配 ” 或 “ 不匹配 ”。在这些情况下， ACL 选择的是应接收该功能服务的流量，例如，应用检查或重定向到服务模块。 “ 被拒绝 ” 流量即不匹配 ACL 的流量，因而将不会接收该服务。（例如，在 ASDM 中，服务策略规则实际上使用 “ 匹配 / 不匹配 ”， AAA 规则使用 “ 验证 / 不验证 ”，但在 CLI 中，始终是 “ 允许 / 拒绝 ”。）

访问控制隐式拒绝

所有 ACL 的末尾都有一条隐式拒绝语句。因此，对于那些应用于接口的流量控制 ACL，如果未明确允许某个类型的流量，则该流量将被丢弃。例如，如果您要允许所有用户通过 ASA 访问网络，某个或多个特定地址除外，则需要拒绝那些特定地址并允许其他地址。

对于用于为某项服务选择流量的 ACL，您必须明确 “ 允许 ” 流量；对于该服务，任何未被 “ 允许的 ” 流量都将不会被匹配接受服务； “ 被拒绝 ” 流量将绕过该服务。

对于 EtherType ACL， ACL 末尾的隐式拒绝不会影响 IP 流量或 ARP ；例如，如果您允许 EtherType 8037，则 ACL 末尾的隐式拒绝语句不会立即阻止之前使用扩展 ACL 允许的任何 IP 流量 （或隐性允许从高安全性接口到低安全性接口的流量）。但是，如果您通过 EtherType ACE *明确*拒绝所有流量，则 IP 和 ARP 流量将被拒绝；仅仍然允许物理协议流量，如自动协商。

使用 NAT 时用于扩展 ACL 的 IP 地址

使用 NAT 或 PAT 时，您将转换地址或端口，通常是在内部和外部地址之间进行映射。如果您需要创建适用于已转换的地址或端口的扩展 ACL，则需要确定是要使用实际 （未转换）地址或端口，还是要使用已映射地址或端口。具体要求因功能而异。

使用实际地址和端口意味着如果 NAT 配置发生更改，您无需更改 ACL。

使用实际 IP 地址的功能

以下命令和功能可以在 ACL 中使用实际 IP 地址，即使接口上所示的地址是映射地址：

- 访问规则 （由 **access-group** 命令引用的扩展 ACL）
- 服务策略规则 （模块化策略框架 **match access-list** 命令）
- 僵尸网络流量过滤器流量分类 （**dynamic-filter enable classify-list** 命令）
- AAA 规则 （**aaa ... match** 命令）
- WCCP （**wccp redirect-list group-list** 命令）

例如，如果您为内部服务器 10.1.1.5 配置了 NAT，以便其在外部 209.165.201.5 上具有公开可路由的 IP 地址，则允许外部流量访问内部服务器的访问规则需要引用服务器的实际 IP 地址 (10.1.1.5)，而不是映射地址 (209.165.201.5)。

使用映射 IP 地址的功能

以下功能使用 ACL，但这些 ACL 使用接口上所示的映射值：

- IPsec ACL
- **capture** 命令 ACL
- 每用户 ACL
- 路由协议 ACL
- 所有其他功能 ACL

基于时间的 ACE

您可以将时间范围对象应用到扩展 ACE 和 Webtype ACE，以便规则仅在特定时期内处于活动状态。通过这些类型的规则，您可以区分在一天中某些时间点可接受但在其他时间点不可接受的活动。例如，您可以在工作时间内提供附加限制，而在下班后或在午餐时间则不限制。相反，您基本上可以在非工作时间关闭网络。有关创建时间范围对象的详细信息，请参阅第 17-6 页的配置时间范围。

注　用户可能会在指定结束时间后遇到约 80 至 100 秒的延迟，以使 ACL 处于非活动状态。例如，如果指定的结束时间是 3:50，因为结束时间包含在内，因此将在 3:51:00 与 3:51:59 之间的任何时间点选取命令。选取命令后， ASA 将完成所有当前运行的任务，然后执行命令以停用 ACL 服务。

ACL 准则

防火墙模式准则

扩展 ACL 和标准 ACL 均支持路由和透明防火墙模式。

Webtype ACL 仅支持路由模式。

EtherType ACL 仅支持透明模式。

IPv6 准则

扩展 ACL 和 Webtype ACL 允许 IPv4 和 IPv6 地址混合使用。

标准 ACL 不允许 IPv6 地址。

EtherType ACL 不包含 IP 地址。

（仅限扩展 ACL。）不支持身份防火墙、 FQDN 和思科 TrustSec ACL 的功能

以下功能使用 ACL，但无法接受带身份防火墙 （指定用户或组名称）、 FQDN （完全限定域名），或思科 TrustSec 值的 ACL：

- **route-map** 命令
- VPN **crypto map** 命令
- VPN **group-policy** 命令， **vpn-filter** 除外
- WCCP
- DAP

附加准则和限制

- 指定网络掩码的方法与思科 IOS 软件 **access-list** 命令不同。 ASA 使用网络掩码 （例如，255.255.255.0 用于 C 类掩码）。思科 IOS 掩码使用通配位 （例如， 0.0.0.255）。

配置 ACL

以下各节介绍了如何配置各种类型的通用 ACL，用作访问规则 （包括 EtherType）、服务策略规则、 AAA 规则和其他用途 （其中 ASDM 为基于规则的策略提供专用页面）的 ACL 除外。有关为上述其他用途配置规则的详细信息，请参阅防火墙配置指南。

- 第 18-6 页的配置扩展 ACL
- 第 18-8 页的配置标准 ACL
- 第 18-9 页的配置 Webtype ACL

配置扩展 ACL

扩展 ACL 被表示为 ACE 的命名容器。要创建新的 ACL，您必须先创建一个容器。之后，您可以添加 ACE，编辑现有 ACE 并使用 ACL 管理器中的表将 ACE 重新排序。

扩展 ACL 可以同时包含 IPv4 和 IPv6 地址。

操作步骤

步骤 1　选择 **Configuration > Firewall > Advanced > ACL Manager**。

步骤 2　如果创建新的 ACL，请选择 **Add > Add ACL**，填写名称，然后点击 **OK**。

ACL 容器将被添加到表中。您可以稍后对 ACL 容器重命名，只需选择该容器并点击 **Edit** 即可。

步骤 3　执行以下任一操作：

- 要将 ACE 添加到 ACL 末尾，请选择 ACL 名称或其中的任意 ACE 并选择 **Add > Add ACE**。
- 要将 ACE 插入特定位置，请选择现有的 ACE 并选择 **Add > Insert**，以将 ACE 添加到规则上方，或选择 **Add > Insert After**。
- 要编辑规则，请选择规则并点击 **Edit**。

步骤 4　填写 ACE 属性。要选择的主要选项如下：

- **Action: Permit/Deny** - 是否允许 （选择）或拒绝 （取消选择，不匹配）所述流量。
- **Source/Destination criteria** - 源 （原始地址）和目标 （流量的目标地址）的定义。通常您要配置主机或子网的 IPv4 或 IPv6 地址，您可以使用网络或网络对象组进行表示。您还可以为源指定用户或用户组名称。此外，如果您要将规则限制在比所有 IP 流量更窄的范围，则可以使用 Service 字段识别特定类型的流量。如果您实施思科 TrustSec，则可以使用安全组定义源和目标。

有关所有可用选项的详细信息，请参阅第 18-6 页的扩展 ACE 属性。

ACE 定义完成后，请点击 **OK**，将规则添加到表中。

步骤 5　点击 **Apply**。

扩展 ACE 属性

将 ACE 添加到扩展 ACL 或进行编辑时，您可以配置以下属性。在大部分字段中，您可以点击编辑方框右侧的 “...” 按钮，选择、创建或编辑字段可用的对象。

- **Action: Permit/Deny** - 是否允许 （选择）或拒绝 （取消选择，不匹配）所述流量。
- **Source Criteria** - 尝试匹配的流量的起源特征。 Source 必须配置，但其他属性可选。
  - **Source** - 源的 IPv4 或 IPv6 地址。默认值为 **any**，该值会匹配所有 IPv4 或 IPv6 地址；您可以使用 **any4** 以只将 IPv4 作为目标，或使用 **any6** 以只将 IPv6 作为目标。您可以指定单个主机地址 （如 10.100.10.5 或 2001:DB8::0DB8:800:200C:417A）、一个子网（10.100.10.0/24 或 10.100.10.0/255.255.255.0 格式，或对于 IPv6 为 2001:DB8:0:CD30::/60 格式）、网络对象或网络对象组的名称或接口的名称。
  - **User** - 如果您启用身份防火墙，则可以将用户或用户组指定为流量源。用户当前使用的 IP 地址将匹配规则。您可以指定用户名 (DOMAIN\user)、用户组 （DOMAIN\\group，注意 \\ 表示组名称）或用户对象组。对于此字段，点击 “**...**”，从 AAA 服务器组中选择名称比直接键入名称更为容易。

  - **Security Group** - 如果您启用思科 TrustSec，则可以指定安全组名称或标记 (1 - 65533)，或安全组对象。
  - **More Options > Source Service** - 如果您将 TCP 或 UDP 指定为目标服务，则可以选择性地为 TCP、 UDP 或 TCP-UDP 指定预定义的服务对象，或使用您自己的对象。通常，您只需定义目标服务，而不定义源服务。请注意，如果您定义源服务，则目标服务协议必须与其匹配 （例如，带与不带端口定义的 TCP）。

- **Destination Criteria** - 尝试匹配的流量的目标特征。 Destination 必须配置，但其他属性可选。
  - **Destination** - 目标的 IPv4 或 IPv6 地址。默认值为 **any**，该值会匹配所有 IPv4 或 IPv6 地址；您可以使用 **any4** 以只将 IPv4 作为目标，或使用 **any6** 以只将 IPv6 作为目标。您可以指定单个主机地址 （如 10.100.10.5 或 2001:DB8::0DB8:800:200C:417A）、一个子网（10.100.10.0/24 或 10.100.10.0/255.255.255.0 格式，或对于 IPv6 为 2001:DB8:0:CD30::/60 格式）、网络对象或网络对象组的名称或接口的名称。
  - **Security Group** - 如果您启用思科 TrustSec，则可以指定安全组名称或标记 (1 - 65533)，或安全组对象。
  - **Service** - 流量的协议，如 IP、TCP、UDP，或者 TCP 和 UDP 的端口。默认值为 IP，但您可以选择更具体的协议以将更精细的流量作为目标。通常，您可以选择某些类型的服务对象。对于 TCP 和 UDP，您可以指定端口，如 tcp/80、tcp/http、tcp/10-20（适用于端口范围）、tcp-udp/80（匹配端口 80 上的任意 TCP 或 UDP 流量）等等。有关指定服务的详细信息，请参阅第 18-8 页的扩展 ACE 中的服务规格。

- **Description** - ACE 用途的说明，每行最多 100 个字符。您可以输入多行；每一行将作为备注添加到 CLI 中，并且备注放在 ACE 之前。

  注　如果您将含非英文字符的备注添加到一个平台 （如 Windows）上，然后尝试从另一个平台 （如 Linux）将这些备注移除，则您可能无法编辑或删除它们，因为原特征可能无法被正确识别。此限制由底层平台依赖性所导致，其以不同方式对不同语言进行编码。

- **Enable Logging**； **Logging Level**； **More Options > Logging Interval** - 记录选项定义了如何为规则生成系统日志消息。您可以实施以下记录选项：
  - **Deselect Enable Logging** - 为规则禁用记录。系统将不会为匹配此规则的流量发出任何类型的日志消息。
  - **Select Enable Logging with Logging Level = Default** - 为规则提供默认记录。系统将为每个被拒绝的数据包发出系统日志消息 106023。如果设备受到攻击，发出此消息的频率可能会影响服务。
  - **Select Enable Logging with Non-Default Logging Level** - 提供一条汇总系统日志消息 106100，而非 106023。在第一次命中后，系统将发出消息 106100，然后在 **More Options > Logging Interval** 中配置的每个间隔（默认值为每隔 300 秒，您可以指定 1 - 600 秒）后再次发出消息，显示在间隔过程中的命中次数。建议的记录级别为 **Informational**。

    汇总拒绝消息可以减少攻击的影响，并且有可能方便您分析消息。如果您受到拒绝服务攻击，则可能会看到消息 106101，表示用于为消息 106100 生成命中次数的缓存拒绝流的数量已超过某个间隔内的最大值。此时，设备将在下一个间隔前停止收集统计信息以减轻攻击。

- **More Options > Enable Rule** - 规则在设备上是否处于活动状态。被禁用的规则在规则表中带删除线文本显示。禁用规则可以让您在不删除规则的情况下停止将其应用到流量，以便您可以在以后需要时重新启用。
- **More Options > Time Range** - 时间范围对象的名称，该对象定义了规则应在一天中的某些时间或一周中的某些天处于活动状态。如果不指定时间范围，规则将始终处于活动状态。

扩展 ACE 中的服务规格

对于扩展 ACE 中的目标服务，您可以指定以下任一条件。选项都相似，但对于源服务，具有更多的限制，即限于 TCP、 UDP 或 TCP - UDP 条件。

- Object name - 任意类型的服务对象或服务对象组的名称。这些对象可以包含以下所述的大部分规格，您可以轻松地在 ACL 中重用服务定义。存在许多预定义的对象，因此，您也许可以找到所需的对象，而无需手动键入规格或创建对象。
- Protocol - 一个介于 1 - 255 之间的数字，或一个已知名称，如 as **ip**、**tcp**、**udp**、**gre** 等等。有关编号、名称及其含义的列表，请参阅第 43-10 页的协议和应用。
- TCP、UDP、TCP-UDP 端口 - 您可以在关键字 **tcp**、**udp** 和 **tcp-udp** 中包含端口规格。您可以通过关键字 tcp-udp 同时为两个协议定义端口，而不必单独指定。您可以使用以下方法指定端口：
  - 单个端口 - tcp/80、 udp/80、 tcp-udp/80 或已知服务名称，如 tcp/www or udp/snmp。有关端口和关键字的列表，请参阅第 43-10 页的 TCP 和 UDP 端口。
  - 端口范围 - tcp/1-100、 udp/1-100、 tcp-udp/1-100，匹配端口 1 - 100 （含）。
  - 不等于端口号 - 将 != 添加到规格的开头，例如， !=tcp/80 表示匹配任意 TCP 流量， TCP 端口 80 (HTTP) 除外。
  - 小于端口号 - 添加 <，例如， <tcp/150 表示匹配任何端口号小于 150 的 TCP 流量。
  - 大于端口号 - 添加 >，例如， >tcp150 以匹配任何端口号大于 150 的 TCP 流量。

  注　对于 DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC 和 Talk，每一项都要求一个针对 TCP 的定义和一个针对 UDP 的定义。TACACS+ 要求一个针对 TCP 上端口 49 的定义。

- ICMP、 ICMP6 消息 - 您可以将特定消息 （如 ping 回应请求和回复消息），甚至消息代码为目标。存在许多涵盖 ICMP （适用于 IPv4）和 ICMP6 （适用于 IPv6）的预定义对象，因此您也许不需要手动定义标准。格式如下：

  icmp/*icmp_message_type*[/*icmp_message_code*]

  icmp6/*icmp6_message_type*[/*icmp6_message_code*]

  其中消息类型为 1 - 255 或已知名称，而代码为 0 - 255。确保您选择的数字与实际类型 / 代码相匹配，否则 ACE 将永远不会被匹配。有关 ICMP 类型的列表，请参阅第 43-14 页的 ICMP 类型。

配置标准 ACL

标准 ACL 被表示为 ACE 的命名容器。要创建新的 ACL，您必须先创建一个容器。之后，您可以添加 ACE，编辑现有 ACE 并使用标准 ACL 表对 ACE 重新排序。如果您在配置使用 ACL 的策略的同时配置 ACL，该表格可以在 ACL 管理器中显示为一个选项卡，在这种情况下，除了到达窗口的方式不同外，操作步骤基本相同。

标准 ACL 仅使用 IPv4 地址，并且仅定义目标地址。

操作步骤

步骤 1　选择 **Configuration > Firewall > Advanced > Standard ACL**。

步骤 2　如果创建新的 ACL，请选择 **Add > Add ACL**，填写名称，然后点击 **OK**。

ACL 容器将被添加到表中。您无法重命名标准 ACL。

步骤 3　执行以下任一操作：

- 要将 ACE 添加到 ACL 末尾，请选择 ACL 名称或其中的任意 ACE 并选择 **Add > Add ACE**。
- 要将 ACE 插入特定位置，请选择现有的 ACE 并选择 **Add > Insert**，以将 ACE 添加到规则上方，或选择 **Add > Insert After**。
- 要编辑规则，请选择规则并点击 **Edit**。

步骤 4　填写 ACE 属性。选项如下：

- **Action: Permit/Deny** - 是否允许 （选择）或拒绝 （取消选择，不匹配）所述流量。
- **Address** - 定义流量的目标地址。您可以指定一个主机地址 （如 10.100.1.1）、一个网络（10.100.1.0/24 或 10.100.1.0/255.255.255.0 格式），或可以选择网络对象 （只需将对象的内容加载到 Address 字段即可）。
- **Description** - ACE 用途的说明，每行最多 100 个字符。您可以输入多行；每一行将作为备注添加到 CLI 中，并且备注放在 ACE 之前。

注　如果您将含非英文字符的备注添加到一个平台 （如 Windows）上，然后尝试从另一个平台 （如 Linux）将这些备注移除，则您可能无法编辑或删除它们，因为原特征可能无法被正确识别。此限制由底层平台依赖性所导致，其以不同方式对不同语言进行编码。

ACE 定义完成后，请点击 **OK**，将规则添加到表中。

步骤 5　点击 **Apply**。

配置 Webtype ACL

Webtype ACL 用于过滤无客户端 SSL VPN 流量，限制用户对特定网络、子网、主机和网络服务器的访问。如果不定义过滤器，将允许所有连接。Webtype ACL 被表示为 ACE 的命名容器。要创建新的 ACL，您必须先创建一个容器。之后，您可以添加 ACE，编辑现有 ACE 并使用网络 ACL 表对 ACE 重新排序。如果您在配置使用 Webtype ACL 的策略的同时配置 Webtype ACL，该表格可以显示为 ACL 管理器，在这种情况下，除了到达窗口的方式不同外，操作步骤基本相同。

除了 URL 规格之外， Webtype ACL 可以同时包含 IPv4 和 IPv6 地址。

操作步骤

步骤 1　选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACL**。

步骤 2　如果创建新的 ACL，请选择 **Add > Add ACL**，填写名称，然后点击 **OK**。

ACL 容器将被添加到表中。您可以稍后对 ACL 容器重命名，只需选择该容器并点击 **Edit** 即可。

步骤 3　执行以下任一操作：

- 要将 ACE 添加到 ACL 末尾，请选择 ACL 名称或其中的任意 ACE 并选择 **Add > Add ACE**。
- 要将 ACE 插入特定位置，请选择现有的 ACE 并选择 **Add > Insert**，以将 ACE 添加到规则上方，或选择 **Add > Insert After**。
- 要编辑规则，请选择规则并点击 **Edit**。

步骤 4　填写 ACE 属性。要选择的主要选项如下：

- **Action: Permit/Deny** - 是否允许 （选择）或拒绝 （取消选择，不匹配）所述流量。
- **Filter** - 基于目标的流量匹配条件。您可以通过选择协议并输入服务器名称和路径及文件名（后面两者可选）来指定 URL，或可以指定目标 IPv4 或 IPv6 地址和 TCP 服务。

有关所有可用选项的详细信息，请参阅第 18-10 页的 Webtype ACE 属性。

ACE 定义完成后，请点击 **OK**，将规则添加到表中。

步骤 5　点击 **Apply**。

Webtype ACE 属性

将 ACE 添加到 Webtype ACL 或进行编辑时，您可以配置以下属性。在大部分字段中，您可以点击编辑方框右侧的 “...” 按钮，选择、创建或编辑字段可用的对象。

对于给定的 ACE，您可以基于 URL 或 Address 进行过滤，但不能同时基于两者进行过滤。

- **Action: Permit/Deny** - 是否允许 （选择）或拒绝 （取消选择，不匹配）所述流量。
- **Filter on URL** - 基于目标 URL 匹配流量。选择协议并输入服务器名称和路径和文件名（后面两者可选）。例如， http://www.example.com，或者要涵盖所有服务器，请输入 http://*.example.com。以下是一些有关指定 URL 的提示和限制：
  - 选择 **any** 将匹配所有 URL。
  - Permit url any 将允许所有具有 protocol://server-ip/path 格式的 URL 并将阻止不匹配该模式的流量，如端口转发。应该有一个 ACE 允许连接至所需端口 （如果是 Citrix，为端口 1494），以避免发生隐式拒绝。
  - 智能隧道和 ica 插件不会受带 permit url any 值的 ACL 的影响，因为它们仅匹配 smart-tunnel:// 和 ica:// types。
  - 您可以使用以下协议：cifs://、 citrix://、 citrixs://、 ftp://、 http://、 https://、 imap4://、 nfs://、 pop3://、 smart-tunnel:// 和 smtp://。您还可以在协议中使用通配符；例如， htt* 匹配 http 和 https，星号 “*” 匹配所有协议。例如， *://*.example.com 会将任何类型的基于 URL 的流量匹配到 example.com 网络。
  - 如果您指定一个 smart-tunnel:// URL，则仅可以包含服务器名称。URL 不能包含路径。例如， smart-tunnel://www.example.com 可以接受，但 smart-tunnel://www.example.com/index.html 却不可接受。
  - 星号 “*” 匹配 none 或任意数量的字符。要匹配任意 http URL，请输入 http://*/*。

  - 问号 “?” 完全匹配任意字符。
  - 方括号 “[]” 为范围运算符，匹配范围中的任意字符。例如，要同时匹配 http://www.cisco.com:80/ 和 http://www.cisco.com:81/，请输入 **http://www.cisco.com:8[01]/**。

- **Filter on Address and Service** - 基于目标地址和服务匹配流量。
  - **Address** - 目标的 IPv4 或 IPv6 地址。要匹配所有地址，您可以使用 **any**，将匹配所有 IPv4 或 IPv6 地址；使用 **any4** 仅匹配 IPv4，或使用 **any6** 仅匹配 IPv6。您可以指定单个主机地址 （如 10.100.10.5 或 2001:DB8::0DB8:800:200C:417A）、一个子网（10.100.10.0/24 或 10.100.10.0/255.255.255.0 格式，或对于 IPv6 为 2001:DB8:0:CD30::/60 格式），或选择网络对象，该网络对象将使用对象内容填写字段。
  - **Service** - 一种 TCP 服务规格。默认为无端口的 **tcp**，但您可以指定单个端口 （如 tcp/80 或 tcp/www）或端口范围（如 tcp/1-100）。您可以包含运算符；例如，!=tcp/80 排除端口 80； <tcp/80 是端口号小于 80 的所有端口； >tcp/80 是端口号大于 80 的所有端口。
- **Enable Logging**； **Logging Level**； **More Options > Logging Interval** - 记录选项定义了如何为实际拒绝流量的规则生成系统日志消息。您可以实施以下记录选项：
  - **Deselect Enable Logging** - 为规则禁用记录。系统将不会为被该规则拒绝的流量发出任何类型的日志消息。
  - **Select Enable Logging with Logging Level = Default** - 为规则提供默认记录。系统将为每个被拒绝的数据包发出系统日志消息 106103。如果设备受到攻击，发出此消息的频率可能会影响服务。
  - **Select Enable Logging with Non-Default Logging Level** - 提供一条汇总系统日志消息 106102，而非 106103。在第一次命中后，系统将发出消息 106102，然后在 **More Options > Logging Interval** 中配置的每个间隔（默认值为每隔 300 秒，您可以指定 1 - 600 秒）后再次发出消息，显示在间隔过程中的命中次数。建议的记录级别为 **Informational**。
- **More Options > Time Range** - 时间范围对象的名称，该对象定义了规则应在一天中的某些时间或一周中的某些天处于活动状态。如果不指定时间范围，规则将始终处于活动状态。

Webtype ACL 的示例

以下是一些用于 Webtype ACL 的基于 URL 的规则示例。

操作	过滤器	效果
拒绝	url http://*.yahoo.com/	拒绝访问所有 Yahoo!
拒绝	url cifs://fileserver/share/directory	拒绝访问指定位置中所有文件。
拒绝	url https://www.example.com/ directory/file.html	拒绝访问指定文件。
允许	url https://www.example.com/directory	允许访问指定位置。
拒绝	url http://*:8080/	拒绝通过端口 8080 以 HTTPS 方式访问任何位置。
拒绝	url http://10.10.10.10	拒绝以 HTTPS 方式访问 10.10.10.10。
允许	url any	允许访问任意 URL。通常用于拒绝 URL 访问的 ACL 之后。

监控 ACL

ACL 管理器、标准 ACL、 Webtype ACL 和 EtherType ACL 表格可以显示 ACL 的合并视图。但要准确了解设备上的配置，请使用以下命令。选择 **Tools > Command Line Interface**，输入命令。

命令	用途
show access-list [*name*]	显示访问列表，包括每个 ACE 的行号和命中次数。包含 ACL 名称或您将看到所有访问列表。
show running-config access-list [*name*]	显示当前正在运行的访问列表配置。包含 ACL 名称或您将看到所有访问列表。

ACL 功能历史

功能名称	版本	说明
扩展 ACL、标准 ACL、 Webtype ACL	7.0(1)	ACL 用于控制网络访问或为多项功能指定要采取操作的流量。扩展访问控制列表用于通过设备的访问控制和其他几种功能。标准 ACL 用于路由映射和 VPN 过滤器。Webtype ACL 用于无客户端 SSL VPN 过滤。 EtherType ACL 控制第 2 层非 IP 流量。 添加了 ACL 管理器 和其他页面用于配置 ACL。
扩展 ACL 中的实际 IP 地址	8.3(1)	使用 NAT 或 PAT 时，对于几种功能， ACL 中不再使用映射地址和端口。您必须为这些功能使用实际、未转换的地址和端口。使用实际地址和端口意味着如果 NAT 配置发生更改，您无需更改 ACL。有关详细信息，请参阅第 18-4 页的使用 NAT 时用于扩展 ACL 的 IP 地址。
支持在扩展 ACL 中使用身份防火墙	8.4(2)	您现在可以将身份防火墙用户和组用于源和目标。您可以将身份防火墙 ACL 与访问规则、 AAA 规则配合使用，并可将其用于 VPN 身份验证。
IS-IS 流量的 EtherType ACL 支持	8.4(5)、9.1(2)	在透明防火墙模式中， ASA 现在可以使用 EtherType ACL 控制 IS-IS 流量。 我们修改了以下屏幕：Configuration > Device Management > Management Access > EtherType Rules。
支持在扩展 ACL 中使用思科 TrustSec	9.0(1)	您现在可以将思科 TrustSec 安全组用于源和目标。您可以将身份防火墙 ACL 与访问规则配合使用。

功能名称	版本	说明
为 IPv4 和 IPv6 统一扩展 ACL 和 Webtype ACL	9.0(1)	扩展 ACL 和 Webtype ACL 现在支持 IPv4 和 IPv6 地址。您甚至可以为源和目标同时指定 IPv4 和 IPv6 地址。已更改关键字 **any** 以代表 IPv4 和 IPv6 流量。已添加 **any4** 和 **any6** 关键字以分别表示仅 IPv4 和仅 IPv6 流量。IPv6 特定 ACL 已废弃。现有 IPv6 ACL 已迁移到扩展 ACL。请参阅版本说明以了解有关迁移的详细信息。 我们修改了以下屏幕： Configuration > Firewall > Access Rules Configuration > Remote Access VPN > Network (Client) Access > Group Policies > General > More Options
用于按 ICMP 代码过滤 ICMP 流量的扩展 ACL 和对象增强	9.0(1)	现在您可以根据 ICMP 代码允许 / 拒绝 ICMP 流量。 我们引入或修改了以下屏幕： Configuration > Firewall > Objects > Service Objects/Groups Configuration > Firewall > Access Rule

第 6 部分

IP 路由

路由概述

本章介绍有关路由如何在思科 ASA 内部运行的基本概念以及支持的路由协议。

有关路由

所谓路由就是指通过互联网络把信息从源地点移到目标地点的活动。在途中，经常至少遇到一个中间节点。路由包含两项基本活动：确定最佳路由路径和通过互联网络传输信息组 （通常称为数据包）。在路由进程情景中，后者称为分组交换。尽管数据包交换相对简单，路径的确定过程却可能非常复杂。

交换

交换算法相对简单；大多数路由协议都采用相同的算法。在大多数情况下，主机确定必须将数据包发送到另一台主机。源主机通过某种方式获取路由器地址后，将带有具体地址的数据包发送到一个指定路由器物理 （媒体访问控制 [MAC] 层）地址，此时带有目标主机的协议 （网络层）地址。

路由器检查数据包的目标协议地址时，确定是否知道如何将数据包转发到下一跳。如果路由器不知道如何转发数据包，通常会丢失数据包。但是，如果路由器知道如何转发数据包，则将目标物理地址更改为下一跳的物理地址并发送数据包。

下一跳可能是最终目标主机。如果不是，下一跳通常是另一条路由器，该路由器也执行同样的交换决策进程。当数据包通过互联网络传输时，其物理地址会发生更改，但是，其协议地址保持不变。

路径确定

路由协议使用尺度来评估数据包传输的最佳路径。尺度为度量的标准 （例如路径带宽，路由算法使用路径带宽来确定到达目标地址的最佳路径。）为帮助确定路径进程，路由算法初始化和维护诸多包含路由信息的路由表。路由信息取决于所使用的路由算法。

路由算法用多种信息来填充路由表。目标或下一跳关联告知路由器，通过将数据包发送到到达终端目标途中代表下一跳的特定路由器，便可以最优路径到达特定目标。当路由器收到传入数据包时，会检查目标地址并尝试将此地址与下一跳关联。

路由表还包含其他信息，例如有关路径可取性的数据。路由器通过比较尺度确定最佳路径，而尺度又取决于所使用路由算法的设计。

路由器之间互相通信，并通过传输各种消息来维护路由表。路由更新消息通常包括路由表全部或部分内容。通过分析来自所有其他路由器的路由更新，路由器可以创建一份详细的网络拓扑图。链路状态通告为路由器之间发送的另一种消息，用以将发送方链路的状态告知其他路由器。链路信息还可用于创建完整网络拓扑图，使路由器能够确定到达网络目标的最佳路径。

注　非对称路由仅能用于多情景模式中的主用 / 主用故障转移。

支持的路由类型

路由器可以使用多种路由类型。 ASA 使用以下类型的路由：

- 第 19-2 页的静态与动态
- 第 19-2 页的单路径与多路径
- 第 19-3 页的平面结构与层次结构
- 第 19-3 页的链路状态与距离向量

静态与动态

静态路由算法几乎算不上是算法，而是网络管理员在路由开始之前建立的表映射。除非网络管理员对这些映射进行修改，否则映射不会发生改变。使用静态路由的算法易于设计，适合用于网络流量相对可预测和网络设计相对简单的环境。

静态路由系统无法对网络更改作出反应，因而通常被认为不适合大型且不断变化的网络。大多数主要的路由算法为动态路由算法，这些算法通过分析传入的路由更新消息来适应变化的网络环境。如果有消息表明网络发生更改时，路由软件将重新计算路由并发出新的路由更新消息。这些消息渗入网络中，促使路由器重新运行自身的算法并相应地更改路由表

您可以酌情使用静态路由对动态路由算法进行补充。例如，将默认路由器 （所有无法路由的数据包都被发送到该路由器）指定为所有无法路由的数据包的储存地，以确保所有消息都至少以某种方式进行处理。

单路径与多路径

某些综合路由协议支持指向同一目标的多条路径。与单路径算法不同，多路径算法允许流量在多条线路上多路复用。多路径算法的优势是完全在于较高的吞吐量和可靠性，通常称为负载共享。

平面结构与层次结构

某些路由算法在平面结构中运行而其他算法则使用路由层次结构。在平面路由系统中，路由器是所有其他路由器的对等体。在层次结构路由系统中，某些路由器形成了实际上的路由选择主干。来自非主干路由器的数据包可以传输到主干路由器，在此数据包通过主干传输直到到达目标的大致区域。此时，数据包通过一个或者多个非主干路由器，从最后一个主干路由器传输到终端目标。

路由系统常常指定逻辑节点组，称为域、自治系统或者区域。在层次结构系统中，某个域中的一些路由器可以和其他域的路由器通信，而其他路由器只可以同本域中的路由器通信。在大型网络中，还可能存在其他的层次结构级别，其中位于最高层次结构级别的路由器形成路由主干。

层次结构路由的主要优点在于，它优化了大多数公司的体系结构，从而可以很好地支持这些公司的流量模式。大多数网络通信发生在小型公司组 （域）中。由于域内路由器只需要知道该域中的其他路由器，所以可以简化这些路由器的路由算法，并根据所使用的路由算法相应地减少路由更新流量。

链路状态与距离向量

链路状态算法 （也称最短路径优先算法）在互联网络中将路由信息以泛洪形式发送给所有节点。然而，每台路由器只发送说明其自身链路状态的路由表部分内容。在链路状态算法中，每台路由器在其路由表中构建整个网络的情景。距离向量算法 （也称为 Bellman-Ford 算法）要求每台路由器只向其相邻的路由器发送其路由表的全部或部分内容。实质上，链路状态算法将小的更新发送到各处，而距离向量算法只将较大的更新发送给相邻的路由器。距离向量算法仅知道其相邻路由器。通常，链路状态算法会配合 OSPF 路由协议使用。

路由如何在 ASA 中运行

ASA 使用路由表和 XLATE 表来决定路由。为了处理目标 IP 转换流量，即反向转换流量，ASA 搜索现有的 XLATE 或静态转换来选择传出接口。

- 第 19-3 页的传出接口选择进程
- 第 19-4 页的下一跳选择进程

传出接口选择进程

选择进程按以下操作进行：

1. 如果已经存在目标 IP 转换 XLATE，则数据包的传出接口由 XLATE 表而非路由表来确定。
2. 如果不存在目标 IP 转换 XLATE，但是存在匹配的静态转换，则传出接口由静态 NAT 规则确定并创建一个 XLATE，不会使用路由表。
3. 如果不存在目标 IP 转换 XLATE，并且不存在匹配的静态转换，则不对数据包进行目标 IP 转换。 ASA 通过查询路由选择传出接口来处理该数据包，然后执行源 IP 转换 （必要时）。

   对于常规的动态出站 NAT，使用路由表对初始传出数据包进行路由然后创建 XLATE。仅使用现有 XLATE 转发传入的返回数据包。对于静态 NAT，始终使用现有 XLATE 或静态转换规则来传输目标转换传入数据包。

下一跳选择进程

在使用之前描述的任一方法选择传出接口之后，要进行附加的路由查询，以找到合适的下一跳，该下一跳属于之前选择的传出接口。如果路由表中没有明确属于所选接口的路由，则数据包会被丢失并生成等级 6 系统日志消息 110001 (no route to host)，即使存在另有一条用于既定目标网络但属于不同传出接口的路由。如果找到属于所选传出接口的路由，数据包将被转发到相应的下一跳。

只有对可以使用单个传出接口访问的多个下一跳， ASA 才能实现负载共享。负载共享无法共享多个传出接口。

如果在 ASA 中使用动态路由，并且路由表在 XLATE 创建后发生变化 （例如路由摆动），则使用原先的 XLATE 而非路由表转发目标转换流量，直至 XLATE 超时。如果原先的路由被从原先的接口移除并通过路由进程挂接到另一个接口，则流量要么被转发到错误的接口，要么被丢谟并生成等级 6 系统日志消息 110001 (no route to host)。

当 ASA 自身没有路由摆动但是某条路由进程在其周围摆动，并使用不同接口通过 ASA 发送属于相同流量的源转换数据包时，同样的问题也可能发生。目标转换的返回数据包可能被通过错误的传出接口转发回来。

在某些安全流量配置中，任何流量可能根据流量里起始数据包的方向被进行源转换或目标转换，因此该问题很有可能发生。当在路由摆动后发生该问题时，可使用 **clear xlate** 命令手动解决或等待 XLATE 超时自动解决该问题。可以减少 XLATE 超时 （必要时）。为了保证该问题极少出现，请确保 ASA 上及其周围不存在路由摆动。即确保属于同一流量的目标转换数据包始终以相同的方式通过 ASA 转发。

支持的路由互联网协议

ASA 支持多种用于路由的互联网协议。本节对每个协议只做简单介绍。

- 增强型内部网关路由协议 (EIGRP)

  作为思科的专利协议， EIGRP 实现和 IGRP 路由的兼容性和无缝互操作性。自动再分配机制允许将 IGRP 路由导入到增强型 IGRP，反之亦然，因此，能够逐渐将增强型 IGRP 添加到现有的 IGRP 网络。

  有关配置 EIGRP 的详细信息，请参阅第 24-3 页的配置 EIGRP。

- 开放最短路径优先 (OSPF)

  OSPF 是由互联网工程任务小组 (IETF) 的内部网关协议 (IGP) 工作小组开发、面向互联网络协议 (IP) 网络的路由协议。 OSPF 使用链路状态算法构建和计算到所有已知目标的最短路径。OSPF 区域中的每台路由器包含相同的链路状态数据库，该数据库是由每台路由器可使用的接口和可到达的邻居组成的列表。

  有关配置 OSPF 的详细信息，请参阅第 23-5 页的配置 OSPFv2。

- 路由信息协议 (RIP)

  RIP 是一种使用跳数作为尺度的距离向量协议。RIP 被广泛用于路由全局互联网中的流量，并且作为一种内部网关协议 (IGP)，该协议在单个自动系统里进行路由。

  有关配置 RIP 的详细信息，请参阅旧版功能指南。

- 边界网关协议 (BGP)

  BGP 是一种自治系统间路由协议。BGP 用于交换互联网的路由信息，是在互联网服务提供商 (ISP) 之间使用的协议。客户连接到 ISP， ISP 使用 BGP 交换客户和 ISP 路由。在自治系统 (AS) 之间使用时， BGP 称为外部 BGP (EBGP)。如果服务提供商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

  有关配置 BGP 的详细信息，请参阅第 22-3 页的配置 BGP。

有关路由表

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，请选择 **Monitoring > Routing > Routes**。

在该窗格中，每一行代表一条路由。

如何填充路由表

ASA 路由表可由静态定义的路由、直连路由以及 RIP、EIGRP、OSPF 和 BGP 路由协议发现的路由来填充。除了路由表内的静态和连接路由， ASA 还可以运行多条路由协议，因此同一条路由可能被以不同方式发现或输入。当到达同一目标的两条路由都被添加到路由表中，将按以下方法确定哪条路由将被保留在路由表中：

- 如果两条路由有不同的网络前缀长度 （网络掩码），则两条路由都被视为唯一的路由并被输入到路由表中。然后由数据包转发逻辑确定使用哪一条路由。

  例如，如果 RIP 和 OSPF 进程发现以下路由：

  - RIP：192.168.32.0/24
  - OSPF：192.168.32.0/19

  即使 OSPF 路由具有更好的管理距离，但是因为两条路由有不同的前缀长度 （子网掩码），两条路由都将被添加到路由表中。这两条路由被视为不同目标，并且由数据包转发逻辑确定采用哪一个路由。

- 如果 ASA 从单个协议获悉到达同一目标的多条路径，例如 RIP，则具有更优尺度的 RIP （由路由协议确定）将被输入到路由表中。

  尺度为关联具体路由的值，路由从最高优先到最低优先进行排序。用于确定尺度的参数取决于路由协议。尺度最低的路径被选为最佳路径并添加到路由表中。如果存在多条相等尺度的路径到达同一目标，则在这些等价路径上进行负载均衡。

- 如果 ASA 从多条路由协议获悉目标，则比较路由的管理距离，管理距离更短的路由将被输入到路由表中。

路由的管理距离

您可以更改由路由协议发现或被重新分配到路由协议的路由的管理距离。如果来自两个不同路由协议的两条路由具有相同的管理距离，则具有较低*默认*管理距离的路由将被输入到路由表中。对于 EIGRP 和 OSPF 路由，如果 EIGRP 路由和 OSPF 路由具有相同的管理距离，则默认选择 EIGRP 路由。

当存在来自不同协议的两条或更多不同的路由到达同一目标，ASA 使用管理距离作为路由参数来选择最佳路径。由于路由协议基于算法的尺度和其他协议不同，因此有时无法为不同路由协议生成的到达同一目标的两条路由确定最佳路径。

每个路由协议通过使用管理距离值来进行优先级排序。表 19-1 显示了 ASA 支持的路由协议的默认管理距离。

表 19-1　　支持的路由协议的默认管理距离

路由源	默认管理距离
已连接的接口	0
静态路由	1
EIGRP 汇总路由	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部路由	170
内部 BGP	200
未知	255

管理距离值越小，协议的优先等级越高。例如，如果 ASA 同时接收来自 OSPF 路由进程 （默认管理距离 - 110）和 RIP 路由进程 （默认管理距离 - 120）到达某个网络的路由， ASA 将选择 OSPF 路由，因为 OSPF 具有更高的优先级。在这种情况下，路由器将路由的 OSPF 版本添加到路由表。

在本示例中，如果 OSPF 派生路由的源丢失 （例如，由于电源关闭）， ASA 将使用 RIP 派生路由，直到 OSPF 派生路由再次出现。

管理距离为本地设置项。例如，如果您使用 **distance-ospf** 命令改变通过 OSPF 获取路由的路由管理距离，该更改只会影响输入了该命令的 ASA 上的路由表。管理距离不会在路由更新中被通告。

管理距离不会影响路由进程。 EIGRP、 OSPF、 RIP 和 BGP 路由进程只通告被路由进程发现或被重新分配到路由进程的路由。例如，即使 OSPF 路由进程发现的路由被用于 ASA 路由表， RIP 路由进程也会通告 RIP 路由。

备用路由

当由于另一条路由被添加导致初始尝试将路由添加到路由表失败时，则注册一条备用路由。如果添加到路由表的路由发生故障，路由表维护进程呼叫所有注册了备用路由的路由协议进程并要求它们重新在路由表中添加此路由。如果存在多条协议为该故障路由注册了备用路由，则根据管理距离选择优先路由。

鉴于以上进程，当动态路由协议发现的路由发生故障时，您可以创建添加到路由表的浮动静态路由。浮动静态路仅仅为比 ASA 上运行的动态路由协议配置有更大管理距离的静态路由。当动态路由进程发现的相应路由发生故障时，静态路由将被添加到路由表。

如何制定转发决策

传输决策按以下方式来制定：

- 如果目标不匹配路由表中的任何条目，将通过为默认路由指定的接口转发数据包。如果尚未配置默认路由，数据包将被丢弃。
- 如果目标匹配路由表中的单个条目，将通过与该路由关联的接口转发数据包。
- 如果目标匹配路由表中的多个条目，并且所有条目具有相同的网络前缀长度，则具有相同网络前缀却有不同接口的两个条目无法同时存在路由表中。
- 如果目标匹配路由表中的多个条目，并且这些条目具有不同的网络前缀长度，则将通过与具有较长网络前缀长度的路由相关联的接口转发数据包。

例如，发往 192.168.32.1 的数据包到达路由表中拥有以下路由的 ASA 接口：

```
ciscoasa# show route
        ....
        R   192.168.32.0/24 [120/4] via 10.1.1.2
        O   192.168.32.0/19 [110/229840] via 10.1.1.3
        ....
```

在这种情况下，发往 192.168.32.1 的数据包将被直接发送到 10.1.1.2，因为 192.168.32.1 属于 192.168.32.0/24 网络。它也属于路由表中的其他路由，但 192.168.32.0/24 在路由表中的前缀最长（24 位 VS 19 位）。在转发数据包时，较长前缀始终优先于较短的前缀。

动态路由和故障转移

静态路由系统无法对网络更改作出反应，因而通常被认为不适合大型且不断变化的网络。大多数主要的路由算法为动态路由算法，这些算法通过分析传入的路由更新消息来适应变化的网络环境。如果有消息表明网络发生更改时，路由软件将重新计算路由并发出新的路由更新消息。这些消息渗入网络中，促使路由器重新运行自身的算法并相应地更改路由表

您可以酌情使用静态路由对动态路由算法进行补充。例如，将默认路由器 （所有无法路由的数据包都被发送到该路由器）指定为所有无法路由的数据包的储存地，以确保所有消息都至少以某种方式进行处理。

当路由表在主用设备上发生改变时，备用设备上的动态路由同步变化，也就是说，主用设备上的所有添加、删除或更改会被立即传送到备用设备。如果在主设备进入主用状态有一段时间之后，备用设备也进入主用状态，则路由在故障转移批量同步进程中会被同步，因此，在主用 / 备用故障转移对上的路由表应该显示为一样的。

关于静态路由以及如何配置静态路由的详细信息，请参阅第 20-2 页的静态路由配置。

动态路由和集群

在集群中，动态路由被充分集成，不同设备之间共享路由 （每个集群最多允许 8 台设备）。路由表条目也在集群中的设备之间被复制。

当设备从从设备过渡到主设备时， RIB 表初始序号 （32 位序列号）也相应增加。完成过渡后，新的主设备最初拥有的 RIB 表条目为之前主设备的镜像。此外，在新的主设备上启动再收敛计时器。当 RIB 表的初始序号增加时，所有的现有条目将被视为过时。 IP 数据包转发继续正常进行。在新的主设备上，动态路由开始用新的初始序号更新现有的路由条目或创建新路由条目。带有当前初始序号的已修改条目或新创建条目表明它们已经被更新且与所有从设备同步。在再收敛计时器超时后，RIB 表中的旧条目被移除。OSPF 路由、RIP 路由以及 EIGRP 路由的 RIB 表条目也和从设备同步。

只有当某台设备加入集群时，才会从主设备到加入的设备进行批量同步。

对于动态路由更新，当主设备通过 OSPF、RIP、EIGRP 获悉新的路由时，主设备通过可靠的消息发送将更新消息发送给所有从设备。从设备在接收集群路由更新消息之后更新 RIB 表。

对于支持的动态路由协议（OSPF、RIP 和 EIGRP），来自从设备上第 2 层负载均衡接口的路由数据包被转发给主设备。只有主设备才能发现和处理动态路由协议数据包。当从设备请求执行批量同步时，所有通过第 2 层负载均衡接口获悉的路由条目都将被复制。

当通过主设备上第 2 层负载均衡接口获悉新的路由条目时，新条目被广播到所有从设备。当网络拓扑变化导致现有路由条目被修改时，被修改的条目被同步到所有从设备。当网络拓扑变化导致现有路由条目被移除时，被移除的条目被同步到所有从设备。

当为动态路由同时部署和配置了第 2 层以及第 3 层负载均衡接口时，从设备仅拥有路由进程中部分的拓扑和相邻信息 （包括从第 3 层负载均衡接口获得的详细信息），因为对于第 2 层负载均衡接口来说，只有 RIB 表条目和主设备同步。您必须将网络的第 2 层和第 3 层配置为属于不同的路由进程，并且重新分配来自每个路由进程的负载。

表 19-2 提供了对支持配置的概述。Yes 表明两个进程构成的组合（到第 2 层的进程和到第 3 层的进程）起作用， No 表明两个进程构成的组合不起作用。

表 19-2　　支持配置概述

第 2 层或第 3 层	OSPF （第 3 层）	EIGRP （第 3 层）	RIP （第 3 层）
OSPF （第 2 层）	是	是	是
EIGRP （第 2 层）	是	否	是
RIP （第 2 层）	是	是	否

集群中的所有设备必须处于同一模式：单情景模式或多情景模式。在多情景模式中，主从同步在同步消息中包含所有情景和所有情景中的 RIB 条目。

在集群中，如果您已配置第 3 层接口，还必须配置路由器地址池设置。

有关动态路由和集群的详细信息，请参阅第 9 章， “ASA 集群 ”。

多情景模式中的动态路由

在多情景模式中，每个情景维护一个独立的路由表和路由协议数据库。因而您可以在每个情景中单独配置 OSPFv2 和 EIGRP。您可以在某些情景中配置 EIGRP 以及在相同或不同的情景中配置 OSPFv2。在混合情景模式中，您可以在路由模式的情景中启用任何动态路由协议。多情景模式不支持 RIP 和 OSPFv3。

下表列出了 EIGRP 及 OSPFv2 的属性、用于给 OSPFv2 和 EIGRP 进程分配路由的路由映射、以及在 OSPFv2 中用于过滤路由更新 （多情景模式中进入或离开某个区域）的前缀列表：

EIGRP	OSPFv2	路由映射 和前缀列表
每个情景支持一个实例。	每个情景支持两个实例。	不适用
在系统情景中禁用。		不适用
两个情景可能使用相同的或不同的自治系统编号。	两个情景可能使用相同或不同的区域 ID。	不适用
两个情景的共享接口可能会运行多个 EIGRP 实例。	两个情景的共享接口可能会运行多个 OSPF 实例。	不适用
支持共享接口间 EIGRP 实例的交互。	支持共享接口间 OSPFv2 实例的交互。	不适用
在单模式中可用的所有 CLI 在多情景模式中也可用。		
每个 CLI 仅对其被使用的情景起作用。		

路由资源管理

我们已经介绍过名叫 *routes* 的资源类，该资源类指定了能够存在于某个情景中的路由表条目的最大数量。因而解决了一个情景影响另一个情景中可用的路由表条目的问题，您也可以对每个情景中的路由条目最大数量进行更好的控制。

由于没有明确的系统限制，您只能为该资源限制指定一个绝对值，不能使用百分比限制。此外，每个情景中没有最小限制和最大限制，因此，默认类不会进行更改。如果您在某个情景中为静态或动态路由协议 （连接、静态、 OSPF、 EIGRP 和 RIP）添加新的路由但情景的资源限制已被耗尽，则路由添加失败，并且生成系统日志消息。

禁用代理 ARP 请求

将 IP 流量发送到同一以太网网络上的其他设备时，主机需要知道该设备的 MAC 地址。ARP 是将 IP 地址解析为 MAC 地址的第 2 层协议。主机发送 ARP 请求 “Who is this IP address?”，拥有 IP 地址的设备回答 “I own that IP address; here is my MAC address”。

当设备使用自身的 MAC 地址响应 ARP 请求时，会使用代理 ARP，即使该设备不具有 IP 地址。当您配置 NAT 并指定与 ASA 接口处于相同网络里的映射地址时，ASA 使用代理 ARP。流量能到达主机的唯一方法为， ASA 使用代理 ARP 来声称 MAC 地址已被分配到目标映射地址。

在极少数情况下，您可能想要为 NAT 地址禁用代理 ARP。

如果您的 VPN 客户端地址池与现有网络重叠， ASA 默认在所有接口上发送代理 ARP 请求。如果您在同一个第 2 层域上有另一个接口，它将看到 ARP 请求，并以其接口的 MAC 地址来回应。结果是，通往内部主机的 VPN 客户端的返回流量将流向错误的接口，然后被丢弃。在这种情况下，您需要在不需要的接口上禁用代理 ARP 请求。

操作步骤

步骤 1　选择 **Configuration > Device Setup > Routing > Proxy ARP/Neighbor Discovery**。

系统将在 Interface 字段列出接口名称。**Enabled** 字段显示对于 NAT 全局地址，代理 ARP/ 邻居发现是否被启用 (Yes) 或被禁用 (No)。

步骤 2　要在选定接口上启用代理 ARP/ 邻居发现，请点击 **Enable**。默认情况下，代理 ARP/ 邻居发现在所有接口上启用。

步骤 3　要在选定接口上禁用代理 ARP/ 邻居发现，请点击 **Disable**。

步骤 4　点击 **Apply**，将设置保存到运行配置中。

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。

有关静态路由和默认路由

要将流量路由到无连接主机或网络，您必须定义一条到主机或网络的静态路由，或至少定义一条默认路由到不直接与 ASA 连接的任意网络，例如，网络和 ASA 之间有一台路由器。

如果没有定义静态路由或默认路由，流向无连接主机或网络的流量将生成以下系统日志消息：

```
%ASA-6-110001: No route to dest_address from source_address
```

在以下情况下，您可能想要在单情景模式中使用静态路由：

- 网络使用 EIGRP、 RIP 或 OSPF 中不同的路由器发现协议。
- 网络规模小，您可以轻松管理静态路由。
- 您不希望流量或 CPU 开销与路由协议相关联。

最简单的方法是配置一条默认路由，将所有流量发送到上游路由器，由路由器确定如何路由流量。但是，在某些情况下，默认网关可能无法到达目标网络，因此，您还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法直接将流量发送到不直接与 ASA 连接的任何内部网络。

在透明防火墙模式中，对于源自 ASA 并且要发往非直接相连的网络的流量，您需要配置一条默认路由或静态路由，以便 ASA 知道通过哪个接口发送流量。源自 ASA 的流量可能包括与系统日志服务器、Websense 或 N2H2 服务器或 AAA 服务器的通信。如果有服务器无法通过单条默认路由进行访问，则必须配置静态路由。此外，对于同一负载均衡接口， ASA 最多支持 3 条等价路由。

静态路由和默认路由准则

故障转移准则

支持动态路由协议的状态故障转移。

附加准则

- ASDM 透明模式不支持 IPv6 静态路由。
- 在集群中，只有主设备支持静态路由监控。有关集群的详细信息，请参阅第 9 章，“ASA 集群 ”。

静态路由配置

静态路由算法基本上是指网络管理员在路由开始之前建立的表映射。除非网络管理员对这些映射进行修改，否则映射不会发生改变。使用静态路由的算法易于设计，适合用于网络流量相对可预测和网络设计相对简单的环境。鉴于此，静态路由系统无法对网络更改作出反应。

即使指定的网关变得不可用，静态路由仍然保留在路由表中。如果指定的网关变得不可用，您需要手动从路由表移除静态路由。然而，如果指定接口发生故障，静态路由将从路由表移除，并且当接口恢复时再复原到路由表。

注　如果您创建静态路由比 ASA 上运行的路由协议具有更大的管理距离，则到达该路由协议发现的指定目标的路由优先于静态路由。只有当动态发现路由从路由表移除时，才使用静态路由。

您最多可以为每个接口定义 3 个等价路由到达同一目标。多个接口上间不支持等价多路径 (ECMP)。有了 ECMP，路由之间的流量没必要平均分配，流量基于散列源和目标 IP 地址的算法被分配到指定网关。

静态 Null0 路由配置

通常，使用 ACL 来过滤流量，您可以根据报头包含的信息、过滤数据包。在数据包过滤过程中，ASA 防火墙检查数据包报头做出过滤决策，由此增加一些数据包处理开销并影响性能。

静态 Null0 路由是过滤的补充解决方案。静态 Null0 路由用于将不必要或不想要的流量转发到黑洞。空接口 Null0 用于创建黑洞。静态路由是为不想要的目标而创建，静态路由配置指向空接口。对于任何流量，如果其目标地址和黑洞静态路由具有最佳匹配，都将被自动丢弃。不同于 ACL，静态 Null0 不会导致任何性能降级。

静态 Null0 路由配置用于防止路由环路。 BGP 利用静态 Null0 配置用于远程触发黑洞路由。

例如：

```
route null0 192.168.2.0 255.255.255.0
```

要配置静态路由，请选择以下任一选项：

- 第 20-3 页的添加或编辑静态路由
- 第 20-5 页的配置静态路由跟踪
- 第 20-5 页的删除静态路由

添加或编辑静态路由

操作步骤

步骤 1　在 ASDM 主窗口中，选择 **Configuration > Device Setup > Routing > Static Routes**。

步骤 2　点击以下任一单选按钮，选择要过滤的路由：

- **Both**（过滤 IPv4 和 IPv6）。
- **仅 IPv4**
- **仅 IPv6**

默认情况下，已选中 Both 单选按钮，IPv4 和 IPv6 地址均出现在窗格中。要限制对配置有 IPv4 地址的路由的查看选择，请点击 **IPv4** 单选按钮。要限制对配置有 IPv6 地址的路由的查看选择，请点击 **IPv6** 单选按钮。

步骤 3　点击 **Add** 或 **Edit**。

系统将显示 Add 或 Edit Static Route 对话框。

步骤 4　从 Interface 下拉列表中，选择 Interface 字段中启用的内部或外部网络接口名称。

- **management**（内部接口）
- **outside**（外部接口）

步骤 5　在 IP Address 字段中，键入目标网络的内部或外部网络 IP 地址。

对于 IPv4 地址，输入 **0.0.0.0** 以指定默认路由。 0.0.0.0 IP 地址可缩写为 0。或者，点击省略号浏览地址。

对于 IPv6 地址，输入两个冒号 (**::**) 以指定默认路由。或者，点击省略号浏览地址。

步骤 6　在 Gateway IP 字段中，输入网关路由器的 IP 地址，作为该路由的下一跳地址。

要输入默认路由，请将 IP 地址和子网掩码设置为 **0.0.0.0** 或其缩写形式 **0**。

或者，点击省略号浏览地址。

注　如果将来自某 ASA 接口的 IP 地址作为网关 IP 地址，ASA 将 以 ARP 处理数据包中的指定 IP 地址而非网关 IP 地址。

为静态路由指定的地址是在进入 ASA 和执行 NAT 之前的数据包内的地址。

步骤 7　从目标网络的下拉列表中选择子网掩码。根据要选择过滤的路由 （IPv4、 IPv6 或两者），执行以下任一步骤：

- 对于 IPv4 静态路由（或 IPv4 和 IPv6 静态路由），输入应用于 IP 地址的网络掩码地址。输入 **0.0.0.0** 以指定默认路由。 **0.0.0.0** 子网掩码可缩写为 **0**。
- 对于仅 IPv6 静态路由，输入一个前缀长度。

步骤 8　在 Metric 字段，键入尺度或管理距离。

尺度或距离为路由的管理距离。如果未指定值，默认值为 1。管理距离是一个用来比较不同路由协议之间路由的参数。静态路由的默认管理距离为 1，使静态路由优先于动态路由协议发现的路由，但不优先于直接连接的路由。

OSPF 发现路由的默认管理距离为 110。如果静态路由与动态路由的管理距离相同，静态路由将优先。直连路由始终优先于静态路由或动态发现路由。

步骤 9　（可选）在 Options 区域，为静态路由选择以下任一选项：

- **None** 不为静态路由指定选项。该设置为默认设置。
- **Tunneled** 将路由指定为 VPN 流量的默认隧道网关。此设置仅用于默认路由。对于每台设备，您只能配置一条隧道路由。在透明模式中不支持隧道选项。
- **Tracked** 指定路由被跟踪。同时显示跟踪对象 ID 和跟踪目标地址。仅在单个路由模式中支持被跟踪选项。为被跟踪选项指定以下设置：
  - 在 Track ID 字段中，为路由跟踪进程输入一个唯一的标识符。
  - 在 Track IP Address/DNS Name 字段中，输入被跟踪目标的 IP 地址或主机名。该地址通常为下一跳路由网关的 IP 地址，然而也可能是从该接口可以访问的任何网络对象。
  - 在 SLA ID 字段中，为 SLA 跟踪进程输入一个唯一的标识符。

注　对于 IPv6，不支持 Tracked 选项。

步骤 10　（可选）点击 **Monitoring Options**。

系统将显示 Route Monitoring Options 对话框。此处，您可以更改跟踪对象的以下监控属性：

- Frequency：修改 ASA 应该多久测试跟踪目标的存在，以秒为单位。有效值范围为 1 至 604800 秒。默认值为 60 秒。
- Threshold：输入表明超过阈值事件的时间，以毫秒为单位。该值不能超过超时值。
- Timeout：修改路由监控操作等待来自请求数据包的响应的时间，以毫秒为单位。有效值范围为 0 至 604800000 毫秒。默认值为 5000 毫秒。
- Data Size：修改用于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 至 16384。

注　此设置仅指定负载的大小；不指定整个数据包的大小。

- ToS：为回应请求 IP 报头中的服务字节类型选择一个值。有效值范围为 0 至 255。默认值为 0。
- Number of Packets：选择为每个测试发送的回应请求数量。有效值范围为 1 至 100。默认值为 1。

步骤 11　点击 **OK**。

步骤 12　点击 **Apply**，保存配置。

系统将在 Static Routes 窗格中显示添加或编辑的路由信息。一旦保存了新配置的路由，监控进程随即开始。

配置静态路由跟踪

操作步骤

注　静态路由跟踪仅限于 IPv4 路由。

步骤 1　选择利益目标。确保目标会响应回应请求。

步骤 2　选择 **Configuration > Device Setup > Routing > Static Routes**，打开 Static Routes 窗格。

步骤 3　点击 **Add**，根据已选利益目标的可用性配置将使用的静态路由。您必须为该路由输入接口、IP 地址、子网掩码、网关和尺度设置。

步骤 4　在 Options 区域，为该路由点击 **Tracked** 单选按钮。

步骤 5　配置跟踪属性。您必须输入唯一的跟踪 ID、唯一 SLA ID 以及利益目标的 IP 地址。

步骤 6　（可选）要配置监控属性，在 Add Static Route 对话框中点击 **Monitoring Options**。

步骤 7　点击 **OK**，保存更改。

一旦保存了被跟踪的路由，监控进程随即开始。

步骤 8　重复第 1 至 7 步创建辅助路由。

辅助路由是和跟踪路由到达相同目标的静态路由，只是通过不同的接口或网关。您必须给该路由分配比跟踪路由更大的管理距离 （尺度）。

步骤 9　点击 **OK**，保存更改。

删除静态路由

操作步骤

步骤 1　选择 **Configuration > Device Setup > Routing > Static Routes**.

步骤 2　在 Static Routes 窗格中，选择要删除的路由。

默认情况下，已选中 **Both** 单选按钮， IPv4 和 IPv6 地址均出现在窗格中。

- 要限制对配置有 IPv4 地址的路由的查看选择，请点击 **IPv4** 单选按钮。
- 要限制对配置有 IPv6 地址的路由的查看选择，请点击 **IPv6** 单选按钮。

步骤 3　点击 **Delete**。

已删除的路由将从 Static Routes 窗格中的路由表中移除。

步骤 4　点击 **Apply**，将更改保存到配置。

配置默认静态路由

默认路由对网关 IP 地址进行标识， ASA 将所有不具有已获悉或静态路由的数据包发送到该网关地址。默认静态路由是指将 0.0.0.0/0 作为目标 IP 地址的静态路由。标识具体目标的路由优先于默认路由。

注　在 7.0(1) 版本及更高版本中，如果您在具有不同尺度的不同接口上同时配置两条默认路由，则从具有更高尺度的接口到 ASA 的连接将发生故障，但是，从具有有较尺度的低口到 ASA 的连接则会成功，如同预期结果一样。

您最多可以为每台设备定义 3 个等价默认路由条目。如果定义多个等价默认路由条目，会导致发送到默认路由的流量被在指定网关间进行分配。定义多条默认路由时，您必须为每个条目指定同一接口。

如果您尝试定义不止 3 条等价默认路由或定义与先前定义的默认路由有不同接口的默认路由，您将收到以下消息：

```
"ERROR: Cannot add route entry, possible conflict with existing routes."
```

您可以为隧道流量定义单独的默认路由以及标准默认路由。当您创建了一条带有**隧道** 选项的默认路由时，来自终止于无法使用已获悉或静态路由进行路由的 ASA 的隧道的所有流量都将被发送到该路由。对于来自隧道的流量，该路由覆盖任何其他的已配置的或已获悉的默认路由。

默认静态路由配置的限制

以下限制应用于带有隧道选项的默认路由：

- 请勿在隧道路由的传出接口上启用单播 RPF （**ip verify reverse - path** 命令），因为该设置会导致会话失败。
- 请勿在隧道路由的传出接口上启用 TCP 拦截，因为该设置会导致会话失败。
- 请勿使用带有隧道路由的 VoIP 检测引擎 (CTIQBE、 H.323、 GTP、 MGCP、 RTSP、 SIP、 SKINNY)、 DNS 检测引擎或 DCE RPC 检测引擎，因为这些检测引擎会忽略隧道路由。
- 您无法定义多 条带有隧道选项的默认路由。
- 不支持隧道流量 ECMP。

操作步骤

步骤 1　在 ASDM 主窗口，选择 **Configuration > Device Setup > Routing > Static Routes**。

步骤 2　点击 **Add** 或 **Edit**。

步骤 3　在 Options 区域，选择 **Tunneled**。

步骤 4　点击 **OK**。

配置 IPv6 默认和静态路由

如果已为 IPv6 启用直连主机连接的接口并且 IPv6 ACLs 允许流量通过， ASA 将自动在这些主机之间路由 IPv6 流量。

操作步骤

步骤 1　在 ASDM 主窗口，选择 **Configuration > Device Setup > Routing > Static Routes**。

步骤 2　点击 **IPv6 only** 单选按钮。

步骤 3　点击 **Add** 或 **Edit**。

步骤 4　点击 **OK**。

监控静态路由或默认路由

使用静态路由的其中一个问题是，没有内在机制确定路由处于打开还是关闭状态。即使下一跳网关变得不可用，这些路由依然保留在路由表中。只有 ASA 上的关联接口发生故障时，静态路由才会从路由表中移除。

如果主要路由发生故障，静态路由跟踪功能可以用来跟踪静态路由的可用性和添加备用路由。例如，您可以定义一条到 ISP 网关的默认路由和一条到辅助 ISP 的备用默认路由，以防主要 ISP 变得不可用。

ASA 通过将静态路由与您定义的监控目标相关联来实施该功能，并使用 ICMP 回应请求监控目标。如果在指定时间内没有收到回应回复，对象将被视为关闭并且将从路由表移除相关联的路由。先前配置的备用路由将代替被移除的路由。

选择监控目标时，您需要确保该目标可回应 ICMP 回应请求。该目标可能是您选择的任何网络对象，但是，您应考虑使用以下各项：

- ISP 网关 （双 ISP 支持）地址
- 下一跳网关地址 （如果您关注网关的可用性）
- 目标网络上的服务器通信，例如 AAA 服务器， ASA 需要与该服务器进行通信。
- 目标网络上的持久网络对象

注　最好不要用台式或笔记本电脑，因为您可能会在晚上关闭这些电脑。

您可以为静态定义路由或通过 DHCP 或 PPPoE 获取的默认路由配置静态路由跟踪。您只能在配置了路由跟踪的多个接口上启用 PPPoE 客户端。

操作步骤

步骤 1　选择 **Monitoring > Routing > Routes**。

在 Routes 窗格中，每一行代表一条路由。可以按 IPv4 连接、 IPv6 连接或两者进行过滤。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、路由连接接口和管理距离。

步骤 2　要更新当前列表，请点击 **Refresh**。

静态路由或默认路由的示例

以下示例展示如何创建一条静态路由，该路由将以 10.1.1.0/24 为目标的所有流量发送到与内部接口连接的路由器 10.1.2.45，定义 3 条将流量定向到外部接口的 3 个不同网关的等价静态路由，并将默认路由添加到隧道流量。然后 ASA 在指定网关间分配流量。

步骤 1　在 ASDM 主窗口，选择 **Configuration > Device Setup > Routing > Static Routes**。

步骤 2　从 Interface 下拉列表中，选择 **Management**。

步骤 3　在 IP Address 字段中，输入 **10.1.1.0**。

步骤 4　从 Mask 下拉列表中，选择 **255.255.255.0**。

步骤 5　在 Gateway IP 字段中，输入 **10.1.2.45 1**。

创建了一条静态路由，该路由将以 10.1.1.0/24 为目标的所有流量发送到与内部接口连接的路由器 10.1.2.45。

步骤 6　点击 **OK**。

步骤 7　选择 **Configuration > Device Setup > Routing > Static Routes**.

步骤 8　点击 **Add**。

步骤 9　在 IP Address 字段中，输入目标网络的 IP Address。

在这种情况下，路由 IP 地址为：192.168.2.1、 192.168.2.2、 192.168.2.3 和 192.168.2.4。添加 192.168.2.4 时，在 Options 区域点击 **Tunneled** 单选按钮。

步骤 10　在 Gateway IP Address 字段中，输入下一跳路由器地址的网关 IP 地址。

为静态路由指定的地址是在进入 ASA 和执行 NAT 之前的数据包内的地址。

步骤 11　从 NetMask 下拉列表中，选择目标网络的子网掩码。

步骤 12　点击 **OK**。

静态路由和默认路由的功能历史

ASDM 可向后兼容多个平台版本，因此，未列出已添加支持的具体 ASDM 版本。

表 20-1　　静态路由和默认路由的功能历史

功能名称	平台版本	功能信息
路由	7.0(1)	引入了静态路由和默认路由。 引入了以下屏幕：Configuration > Device Setup > Routing。
集群	9.0(1)	仅在主设备上支持静态路由监控。
静态 Null0 路由配置	9.2(1)	向 Null0 接口发送流量会导致发往指定网络的数据包被丢弃。此功能对于配置 BGP 的远程触发黑洞 (RTBH) 作用甚大。 修改了以下屏幕： Configuration > Device Setup > Routing > Static Routes> Add > Add Static Route

路由映射

有关路由映射

在将路由重新分发给 OSPF、 RIP、 EIGRP 或 BGP 路由进程时使用路由映射。为 OSPF 路由进程生成默认路由时也使用路由映射。路由映射定义允许将源自指定路由协议的哪些路由重新分发给目标路由进程。

路由映射与广为人知的 ACL 有许多相同功能。以下是两者共有的一些特征：

- 它们都是个别语句的有序序列，各有一个允许或拒绝结果。 ACL 或路由映射的评估包括采用预先确定顺序的列表扫描，以及每条语句匹配条件的评估。一旦找到第一个语句匹配即中止列表扫描，并且会执行与语句匹配关联的操作。
- 它们都是通用机制 - 条件匹配和匹配解释由应用的方式决定。应用于不同任务的相同路由映射可能以不同方式进行解释。

以下是路由映射与 ACL 之间的一些差异：

- 路由映射经常使用 ACL 作为匹配条件。
- ACL 评估的主要结果为肯定或否定回答 - 即 ACL 允许或拒绝输入数据。应用于重新分发时，ACL 确定特定路由能 （路由匹配 ACL Permit 语句）否 （路由匹配 Deny 语句）重新分发。重新分发到另一协议时，典型的路由映射不仅允许 （部分）重新分发的路由，而且还修改与路由关联的信息。
- 路由映射比 ACL 更加灵活，可以根据 ACL 无法验证的条件对路由进行验证。例如，路由映射可以验证路由的类型是否为内部。
- 根据设计约定，每个 ACL 以隐式 Deny 语句结尾；路由映射没有类似约定。如果在匹配尝试期间达到路由映射的结尾，则结果取决于路由映射的特定应用。幸运的是，应用于重新分发的路由映射与 ACL 的行为方式相同：如果路由与路由映射中的任何子句均不匹配，则路由重新分发会被拒绝，如同路由映射末尾包含 Deny 语句一样。

动态协议 **redistribute** 命令可供您应用路由映射。在 Cisco ASDM 中，当添加或编辑新的路由映射时，可以找到用于重新分发的此功能 （请参阅第 21-4 页的定义路由映射）。如果要在重新分发期间修改路由信息或者如果需要比 ACL 能够提供的功能更强大的匹配功能，路由映射是首选。如果只是需要根据路由的前缀或掩码选择性地允许一些路由，我们建议您使用路由映射直接在 **redistribute** 命令中映射到 ACL （或等效前缀列表）。如果根据路由的前缀或掩码使用路由映射选择性地允许一些路由，通常可以使用更多配置命令来实现相同目标。

注　必须使用标准 ACL 作为路由映射的匹配条件。使用扩展式 ACL 将不起作用，且将永不重新分发路由。我们建议您以 10 为间隔对子句编号以保留编号空间，以便将来需要插入子句。

Permit 和 Deny 子句

路由映射可以有 Permit 和 Deny 子句。在 **route-map ospf-to-eigrp** 命令中，有一个 Deny 子句（序号为 10）和两个 Permit 子句。 Deny 子句可拒绝来自重新分发的路由匹配。因此，请遵守以下规则：

- 如果在使用 Permit 子句的路由映射中使用 ACL，则将重新分发 ACL 允许的路由。
- 如在路由映射 Deny 子句中使用 ACL，则将不重新分发 ACL 允许的路由。
- 如果在路由映射 Permit 或 Deny 子句中使用 ACL，并且 ACL 拒绝路由，则找不到路由映射子句匹配，并将评估下一个路由映射子句。

Match 和 Set 子句值

每个路由映射子句均有两种类型的值：

- 匹配值选择应将此子句应用到的路由。
- 设定值修改将重新分发到目标协议的信息。

对于要重新分发的每个路由，路由器首先评估路由映射中子句的匹配条件。如果匹配条件成功，则将根据 Permit 或 Deny 子句的指示重新分发或拒绝路由，其某些属性可能被从 ASDM 中 Set Value 选项卡或从 **set** 命令设定的值修改。如果匹配条件失败，则此子句不适用于路由，软件会根据路由映射中下一个子句继续评估路由。路由映射的扫描会继续进行，直到 **match** 命令找到子句，或者 ASDM 中的 Match Clause 选项卡中设置的 Match 子句与路由匹配，或者到达路由映射的末尾。

如果存在以下条件之一，则每个子句中的匹配或设定值会缺少或重复多次：

- 如果子句中存在多个 **match** 命令或 ASDM 中的 Match Clause 值，则一切必须针对给定路由成功才能使该路由与子句匹配 （换句话说，逻辑 AND 算法适用于多个匹配命令）。
- 如果 **match** 命令或 ASDM 中的 Match Clause 值在一个命令中引用多个对象，则其中之一应匹配（应用逻辑 OR 算法）。例如，在 **match ip address 101 121** 命令中，如果 ACL 101 或 ACL 121 允许路由，则路由即被允许。
- 如果 **match** 命令或 ASDM 中的 Match Clause 值不存在，则所有路由均与子句匹配。在上述示例中，到达子句 30 的所有路由均匹配；因此，永远不会到达路由映射的结尾。
- 如果 **set** 命令或 ASDM 中的 Set Value 在路由映射 Permit 子句中不存在，则将重新分发路由，而不会修改其当前属性。

注　请勿在路由映射 Deny 子句中配置 **set** 命令，因为 Deny 子句禁止路由重新分发 - 将不修改信息。

没有 **match** 或 **set** 命令或 ASDM 中的 Match Value 或 Set Value 选项卡中设置的值，路由映射子句会执行操作 空 permit 子句允许重新分发剩余路由，而不会做出修改。空 deny 子句不允许重新分发其他路由 （如果路由映射完成扫描但未找到显式匹配，此为默认操作）。

BGP Match 和 BGP Set 子句

除了如上所述的匹配和设定值之外， BGP 还为路由映射提供其他匹配和设置功能。

BGP 目前支持以下新的路由映射 Match 子句：

- match as-path
- match community
- match policy-list
- match tag

BGP 目前支持以下新的路由映射 Set 子句：

- set as-path
- set automatic-tag
- set community
- set local-preference
- set origin
- set weight

对于要重新分发的每个 BGP 路由，ASA 首先评估路由映射中子句的 BGP 匹配条件。如果 BGP 匹配条件成功，则将根据 Permit 或 Deny 子句的指示重新分发或拒绝路由，其某些属性可能被从 ASDM 中 BGP Set Clause 选项卡或从 **set** 命令设定的值修改。如果匹配条件失败，则此子句不适用于路由，软件会根据路由映射中下一个子句继续评估路由。路由映射的扫描会继续进行，直到 **match** 命令找到子句、ASDM 中的 BGP Match Clause 选项卡中的设置与路由匹配，或者到达路由映射的末尾。

路由映射准则

防火墙模式

仅在路由防火墙模式中受支持。透明防火墙模式不受支持。

附加准则

路由映射不支持包括用户、用户组和完全限定域名对象的 ACL。

定义路由映射

当指定允许将源自指定路由协议的哪些路由重新分发到目标路由进程时，必须定义路由映射。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，选择 **Configuration > Device Setup > Routing > Route Maps**。

步骤 2　点击 **Add**。

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。路由映射名称是您分配给特定路由的名称。序列号是您在 ASA 中添加或删除路由映射条目的顺序。

注　如果正在编辑现有路由映射， Route Map Name 和 Sequence Number 字段已填写。

步骤 4　要拒绝路由匹配重新分发，请点击 **Deny**。如在路由映射 Deny 子句中使用 ACL，则将不重新分发 ACL 允许的路由。要允许路由匹配重新分发，请点击 **Permit**。如果路由映射 Permit 子句中使用 ACL，则将重新分发 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，则找不到路由映射子句匹配，并会评估下一个路由映射子句。

步骤 5　点击 **Match Clause** 选项卡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**。
  - 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度量。
  - 在 Metric Value 字段中，键入度量值。可以输入多个值，用逗号分隔。此设置可供您匹配包含指定度量的任何路由。度量值范围在 0 到 4294967295 之间。
- 选中 **Match Route Type** 复选框以启用或禁用匹配路由类型。有效路由类型为 External1、External2、 Internal、 Local、 NSSA-External1 和 NSSA-External2。启用之后，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度量值，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度量类型，并从下拉列表中选择度量类型。

步骤 7　点击 **BGP Match Clause** 选项卡以选择应将此子句应用至的路由，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。将不为出站路由映射通告未与至少一个 Match 社区相匹配的路由。
  - 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，这增加了自治系统路径长度。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 至 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** 以将某社区添加到现有社区。
  - 点击 **None** 以从通过路由映射的前缀移除社区属性。
- 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** 复选框以指定满足路由映射 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。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

本节说明如何自定义路由映射。

定义路由以匹配特定目标地址

操作步骤

步骤 1　在 ASDM 中，选择 **Configuration > Device Setup > Routing > Route Maps**。

步骤 2　点击 **Add**。

系统将显示 Add Route Map 对话框。从该对话框，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度量。
  - 在 Metric Value 字段中，键入度量值。可以输入多个值，用逗号分隔。此设置可供您匹配包含指定度量的任何路由。度量值范围在 0 到 4294967295 之间。
- 选中 **Match Route Type** 复选框以启用或禁用匹配路由类型。有效路由类型为 External1、External2、 Internal、 Local、 NSSA-External1 和 NSSA-External2。启用之后，即可从列表中选择多个路由类型。

配置前缀规则

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，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，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　输入可选的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**。

新的或修改后的前缀规则将显示在列表中。

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** 以保存更改。

配置前缀列表

ABR 类型 3 LSA 过滤扩展了 ABR 的功能，即运行 OSPF 在不同 OSPF 区域之间过滤类型 3 LSA。配置前缀列表后，仅指定的前缀从一个 OSPF 区域发送到另一个 OSPF 区域。所有其他前缀均局限于各自的 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。

前缀列表的多个条目匹配指定的前缀时，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，将它们置于靠近列表的顶部。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，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**。

为路由操作配置度量值

要为路由操作配置度量值，请执行以下步骤：

操作步骤

步骤 1　在 ASDM 中，选择 **Configuration > Device Setup > Routing > Route Maps**。

步骤 2　点击 **Add**。

系统将显示 Add Route Map 或 Edit Route Map 对话框。从该对话框，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 将使用您添加路由映射条目的顺序。

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度量值，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度量类型，并从下拉列表中选择度量类型。

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，选择 **Configuration > Device Setup > Routing > Route Maps**。

步骤 2　点击 **Add**。

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** 作为度量值。

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** 作为度量值。

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 21-1　　路由映射的功能历史记录

功能名称	平台版本	功能信息
路由映射	7.0(1)	我们引入了此功能。 我们引入了以下屏幕：Configuration > Device Setup > Routing > Route Maps。
对静态和动态路由映射的增强支持	8.0(2)	增加了对动态和静态路由映射的增强支持。
多情景模式中的动态路由	9.0(1)	路由映射在多情景模式中受支持。
支持 BGP	9.2(1)	我们引入了此功能。 我们更新了以下屏幕：Configuration > Device Setup > Routing > Route Maps，增加了 2 个选项卡：BGP match clause 和 BGP set clause。

BGP

本章节介绍如何配置思科 ASA，以使用边界网关协议 (BGP) 来路由数据、执行身份验证以及重新分发路由信息。

关于 BGP

BGP 是一种自治系统间的路由协议。自治系统是一个或一组接受共同管理并采用共同路由策略的网络。 BGP 用于交换互联网的路由信息，是在互联网服务提供商 (ISP) 之间使用的协议。

何时使用 BGP

客户网络 （例如，大学和公司）通常使用 OSPF 等内部网关协议 (IGP) 在它们的网络内部交换路由信息。客户连接到 ISP， ISP 使用 BGP 交换客户和 ISP 路由。在自治系统 (AS) 之间使用时，BGP 称为外部 BGP (EBGP)。如果服务提供商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

路由表更改

在 BGP 邻居之间首次建立 TCP 连接时， BGP 邻居会交换完整路由信息。当检测到对路由表所做的更改时， BGP 路由器向它们的邻居仅发送已更改的路由。 BGP 路由器不发送定期路由更新，BGP 路由更新仅通告到达目标网络的最佳路径。

当存在多个到达某个特定目标的路由时，通过 BGP 学习的路由的属性可用于确定到达该目标的最佳路径。这些属性称为 BGP 属性，可用于路由选择过程：

- 权重 - 这是思科定义的路由器本地属性。权重属性不通告给相邻路由器。如果路由器获悉有多个到达同一目标的路由，则首选权重最高的路由。

- 本地首选项 - 本地首选项属性用于从本地 AS 中选择出口点。与权重属性不同，本地首选项属性在整个本地 AS 中传播。如果有多个来自 AS 的出口点，本地首选项属性最高的出口点用作特定路由的出口点。
- 多出口鉴别器 - 多出口鉴别器 (MED) 或度量属性可用作对外部 AS 关于进入正在通告此度量的 AS 的首选路径的建议。因为正在接收 MED 的外部 AS 也可能正在使用其他 BGP 选择路由，所以它被称作建议。首选 MED 度量较低的路由。
- 源 - 源属性指示 BGP 获悉某个特定路由的方式。源属性可能拥有三个可能值其中之一，并用于路由选择。
  - IGP - 此路由是源 AS 的内部路由。当使用网络路由器配置命令向 BGP 注入路由时，设置该值。
  - EGP - 此路由通过外部边界网关协议 (EBGP) 获悉。
  - 不完整 - 路由源未知或通过其他方式获悉。当路由被重新分发到 BGP 时，会出现不完整源。
- AS_path - 当路由通告通过自治系统时，将 AS 编号添加到此路由通告已经穿越的 AS 编号有序列表。仅拥有最短 AS_path 列表的路由安置在 IP 路由表中。
- 下一跳 - EBGP 下一跳属性是用于到达通告路由器的 IP 地址。对于 EBGP 对等体，下一跳地址是对等体之间的连接 IP 地址。对于 IBGP， EBGP 下一跳地址将携带至本地 AS 中。
- 社区 - 社区属性提供一种目标 （称为社区）的分组方式，可对社区应用路由决策 （例如，接受、首选项和重新分发）。路由映射用于设定社区属性。预定义的社区属性如下所示：
  - no-export - 不向 EBGP 对等体通告此路由。
  - no-advertise - 不向任何对等体通告此路由。
  - internet - 向互联网社区通告此路由；网络中的所有路由器均属于它。

BGP 路径选择

BGP 可能从不同来源接收同一路由的多个通告。BGP 仅选择一个路径作为最佳路径。选择此路径时， BGP 将选定的路径放在 IP 路由表中，并将此路径传播给其邻居。 BGP 按列出的顺序使用以下条件选择某个目标的路径：

- 如果路径指定的下一跳不可访问，则放弃此次更新。
- 首选权重最高的路径。
- 如果权重相同，则首选本地首选项最高的路径。
- 如果本地首选项相同，则首选此路由器上运行的 BGP 发起的路径。
- 如果未发起路由，则首选 AS_path 最短的路由。
- 如果所有路径的 AS_path 长度相同，则首选源类型最低的路径（其中， IGP 低于 EGP， EGP 低于不完整路径）。
- 如果源代码相同，则首选 MED 属性最低的路径。
- 如果路由的 MED 相同，则首选外部路径而非内部路径。
- 如果路径依然相同，则首选穿过最近的 IGP 邻居的路径。
- 如果两个路径都是外部路径，则首选第一个接收的路径 （最早的路径）。
- 首选拥有由 BGP 路由器 ID 指定的最低 IP 地址的路径。
- 如果多条路径的发起方或路由器 ID 相同，则首选集群列表长度最短的路径。
- 首选来自最低邻居地址的路径。

BGP 准则

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

不支持透明防火墙模式。 BGP 仅在路由器模式中受支持。

故障转移准则

在单情景模式和多情景模式中支持有状态故障转移。

注 启用集群时，不支持故障转移。

集群准则

BGP 仅在 L2 （以太网信道类型）和 L3 （单个接口类型）集群模式中受支持。

注 在用户情景中删除和重新应用 BGP 配置时，允许 60 秒的延迟，使从 / 备用 ASA 装置同步。

IPv6 准则

支持 IPv6。优雅重启不受 IPv6 地址系列支持。

配置 BGP

本节介绍如何在系统上启用和配置 BGP 进程。

操作步骤

步骤 1 在 ASDM 中，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。请参阅第 22-4 页的启用 BGP。

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。请参阅第 22-5 页的定义 BGP 路由进程的最佳路径。

步骤 4 在 **BGP > Policy Lists** 选项卡上，为 BGP 路由配置策略列表。请参阅第 22-5 页的配置策略列表。

步骤 5 在 **BGP > AS Path Filters** 选项卡上，为 BGP 路由配置 AS 路径过滤器。请参阅第 22-6 页的配置 AS 路径过滤器。

步骤 6 在 **BGP > Community Rules** 选项卡上为 BGP 路由配置社区规则。请参阅第 22-7 页的配置社区规则。

步骤 7 在 **BGP > IPv4 Family** 选项卡上配置 IPv4 地址系列设置。请参阅第 22-8 页的配置 IPv4 地址系列设置。

启用 BGP

本节介绍启用 BGP 路由、建立 BGP 路由进程和配置一般 BGP 参数所需的步骤。

操作步骤

步骤 1　对于单一模式，在 ASDM 中，选择 **Configuration > Device Setup > Routing > BGP > General**。

注　对于多模式，在 ASDM 中，选择 **Configuration > Context Management > BGP**。启用 BGP 后，通过选择 **Configuration > Device Setup > Routing > BGP > General**，切换到安全情景，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治编号。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值。有效值范围为 1 至 254。

步骤 5　（可选）选中 **Log neighbor changes** 复选框，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，评估网络稳定性。

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。这可以阻止错误配置或未经授权的对等体以仿佛路由源自另一个自治系统的方式通告路由，从而阻止错误定向流量。

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，用点隔开。0-65553 的 AS 编号表示为十进制数字，大于 65535 的 AS 编号使用点表示法表示。

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 邻居在不发送保持连接消息后保持活动的时间间隔。在此保持连接时间间隔结束时，如果未发送消息，则宣布 BGP 对等体无效。默认值为 60 秒。

b. 在 **Hold Time** 字段中，输入 BGP 邻居在发起和配置 BGP 连接时保持活动的时间间隔。默认值为 180 秒。

c. （可选）在 **Min.Hold Time** 字段中，输入 BGP 邻居在发起和配置 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，请执行以下操作：

a. 选中 **Enable Graceful Restart** 复选框，启用 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。有关最佳路径的更多信息，请参阅第 22-2 页的 BGP 路径选择。

操作步骤

步骤 1　在 ASDM 中，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，指定一个介于 0 与 4294967295 之间的值。默认值为 100。值越高，表示首选项更高。此首选项将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，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。只有当路径中没有外部自治系统时，才比较 MED。

步骤 6　选中 **Treat missing MED as the least preferred one** 复选框，将缺失的 MED 属性视为拥有无限值，从而使此路径最不受欢迎；因此，拥有缺失 MED 的路径最不受欢迎。

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，将评估和处理此策略列表中的所有匹配语句。通过一个路由映射可以配置两个或更多策略列表。策略列表也可以与任何其他早已存在的匹配共存，并设置在同一路径映射内部、策略列表外部配置的语句。本节介绍配置策略列表所需的步骤。

操作步骤

步骤 1　在 ASDM 中，选择 **Configuration > Device Setup > Routing > BGP > Policy Lists**。

步骤 2　点击 **Add**。

系统将显示 **Add Policy List** 对话框。从此对话框中，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、匹配度量以及匹配标记号。

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，分发使其下一跳脱离指定接口之一的路由，并执行以下某项操作：

- 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和定位接口。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，配置以下项：

a. 选中 **Match Address** 复选框，重新分发任何拥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，在数据包上执行策略路由。

指定访问列表 / 前缀列表，或者点击省略号以手动浏览和定位访问列表。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，重新分发任何拥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和定位访问列表。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被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和定位访问列表。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和定位 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和定位社区规则。选择一条或多条社区规则，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** 复选框以重新分发拥有指定度量的路由。如果指定多个度量，则路由可以通过任一度量匹配。

步骤 10　选中 **Match Tag Numbers** 复选框以重新分发路由表中匹配指定标记的路由。如果指定多个标记号，则路由可以通过任一度量匹配。

步骤 11　点击 **OK**。

步骤 12　点击 **Apply**。

配置 AS 路径过滤器

AS 路径过滤器可供您使用访问列表过滤路由更新消息，查看更新消息中的单个前缀。如果更新消息中的前缀匹配过滤条件，则该单个前缀将被过滤掉或接受，具体取决于已将过滤器条目配置为执行什么操作。本节介绍配置 AS 路径过滤器所需的步骤。

注　**as-path 访问列表**不同于常规防火墙 ACL。

操作步骤

步骤 1　在 ASDM 中，选择 **Configuration > Device Setup > Routing > BGP > AS Path Filters**。

步骤 2　点击 **Add**。

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匹配您选择的字符串。

步骤 7　点击 **OK**。

步骤 8　点击 **Apply**。

配置社区规则

社区指的是一组共享某个通用属性的目标。您可以使用社区列表，创建要在路由映射中的匹配子句中使用的社区组。像访问列表一样，可以创建一系列的社区列表。系统将检查语句，直至找到匹配为止。只要满足一个语句，测试即可结束。本节介绍配置社区规则所需的步骤。

操作步骤

步骤 1　在 ASDM 中，选择 **Configuration > Device Setup > Routing > BGP > Community Rules**。

步骤 2　点击 **Add**。

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：

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** (well-known community) 复选框，以指定互联网社区。向所有对等体（内部和外部）通告带此社区的路由。

c. （可选）选中 **Do not advertise to any peers** (well-known community) 复选框，以指定无通告社区。不向任何对等体 （内部或外部）通告带此社区的路由。

d. （可选）选中 **Do not export to next AS** (well-known community) 复选框，以指定无导出社区。仅向同一自治系统中的对等体或者仅向联盟中的其他子自治系统通告带此社区的路由。不向外部对等体通告这些路由。

步骤 7　要添加已扩展社区规则：

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** 以检查已构建的正则表达式是否匹配您选择的字符串。

步骤 8　点击 **OK**。

步骤 9　点击 **Apply**。

配置 IPv4 地址系列设置

BGP 的 IPv4 设置可以从 BGP 配置设置中的 IPv4 系列选项设定。IPv4 系列部分包括以下子部分：一般设置、汇聚地址设置、过滤设置和邻居设置。每一这些子部分均可供您自定义 IPv4 系列专用参数。

本节介绍如何自定义 BGP IPv4 系列设置。

配置 IPv4 系列一般设置

本节介绍配置一般 IPv4 设置所需的步骤。

操作步骤

步骤 1 在 ASDM 中，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** 下拉列表选择**路由**映射的名称。点击 **Manage** 以添加和配置路由映射。

步骤 5 （可选）选中 **Generate Default Route** 复选框，**以**配置 BGP 路由进程，使其分发默认路由（网络 0.0.0.0）。

步骤 6 （可选）选中 **Summarize subnet routes into network-level routes** 复选框，以将子网路由自动摘要配置进网络层路由。

步骤 7 （可选）选中 **Advertise inactive routes** 复选框，以通告未安置在路由信息库 (RIB) 中的路由。

步骤 8 （可选）选中 **Redistribute iBGP into an IGP** 复选框，以将 iBGP 重新分发配置进内部网关协议 (IGP)，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 路由器的扫描时间间隔 （单位：秒）。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，指定路由表中安置的更新下一跳路由上的检查延迟时间间隔。

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，选中 **iBGP multipaths** 复选框。

步骤 12 点击 **Apply**。

配置 IPv4 系列汇聚地址设置

本节介绍将特定路由汇聚定义为一个路由所需的步骤。

操作步骤

步骤 1　在 ASDM 中，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 **Add**。

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，为汇聚计时器指定一个值 （单位：秒）。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，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 **Add**。

系统将显示 Add Filter 窗格。

步骤 4　从 Direction 下拉列表选择方向。此方向将指定过滤器应该应用到入站更新还是出站更新。

步骤 5　从 Access List 下拉列表选择访问列表。点击 **Manage** 发添加新 ACL。

步骤 6　从 Protocol 下拉列表选择协议。仅在选择出站方向时适用。

步骤 7　从 Process ID 下拉列表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，选择 **Configuration > Device Setup > Routing > BGP > IPv4 Family**。

步骤 2 点击 **Neighbor**。

步骤 3 点击 **Add**。

步骤 4 点击左侧窗格中的 **General**。

步骤 5 在 **IP Address** 字段中，输入 BGP 邻居 IP 地址。此 IP 地址已添加到 BGP 邻居表中。

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) 优雅重启功能。

步骤 11 点击左侧窗格中的 **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**，以按需添加 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。执行以下任一操作：
  - 点击 **Terminate peering when prefix limit is exceeded**，在达到前缀限制时停止 BGP 邻居。在 Restart interval 字段中，指定 BGP 邻居重新启动前的时间间隔。
  - 点击 **Give only warning message when prefix limit is exceeded**，在达到最大前缀限制时生成日志消息。在这里， BGP 邻居将不会被终止。

步骤 17 在左侧窗格中点击 **Routes**。

步骤 18 在 Advertisement Interval 字段中，输入发送 BGP 路由更新的最小时间间隔 （单位：秒）。

步骤 19 （可选）选中 **Generate Default route** 复选框，允许本地路由器将默认路由 0.0.0.0 发送到邻居以用作默认路由。

- 从 Route map 下拉列表，选择允许有条件地注入路由 0.0.0.0 的路由映射。点击 **Manage** 以添加和配置路由映射。

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，选择在达到存在映射或非存在映射的条件时通告的路由映射。

c. 执行以下任一操作：

- 点击 **Exist Map**，选择路由映射。此路由映射将与 BGP 表中的路由进行比较，确定通告映射路由是否被通告。
- 点击 **Non-exist Map**，选择路由映射。此路由映射将与 BGP 表中的路由进行比较，确定通告映射路由是否被通告。

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　点击左侧窗格中的 **Timers**。

步骤 23　（可选）选中 **Set timers for the BGP peer** 复选框，以设置保持连接频率、抑制时间和最小抑制时间。

- 在保持连接 frequency 字段中，输入 ASA 向邻居发送保持连接消息的频率 （单位：秒）。有效值介于 0 与 65535 之间。默认值为 60 秒。
- 在 Hold time 字段中，输入 ASA 在未接收到保持连接消息后宣布对等体无效的时间间隔 （单位：秒）。默认值为 180 秒。
- （可选）在 Min Hold time 字段，输入 ASA 在未接收到保持连接消息后宣布对等体无效的最小时间间隔 （单位：秒）。

步骤 24　点击左侧窗格中的 **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　密码区分大小写，当启用 **service password-encryption** 命令时，最大长度为 25 个字符；不启用 **service password-encryption** 命令时，最大长度为 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。您不能指定 number-space-anything 格式的密码。数字后的空格会导致身份验证失败。

步骤 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，以将此路由器配置为 BGP 发言邻居或对等组的下一跳。

步骤 28　执行以下任一操作：

- 点击 **Allow connections with neighbor that is not directly connected**，以接受并尝试到驻留在未直接连接的网络上的外部对等体的 BGP 连接。
  - （可选）在 TTL hops 字段中输入存在时间。有效值介于 1 和 255 之间。
  - （可选）选中 **Disable connection verification** 复选框，禁用连接验证，与使用环回接口的单跳对等体建立 eBGP 对等会话。
- 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，选择 ASA 将接受的 BGP 版本。

注　版本可以设为 2，强制软件仅使用第 2 版与指定邻居。默认情况下使用第 4 版，如有要求，可以动态地协商降级至第 2 版本。

步骤 31　（可选）选中 **TCP Path MTU Discovery** 复选框，为 BGP 会话启用 TCP 传输会话。

步骤 32　从 TCP transport mode 下拉列表，选择 TCP 连接模式。

步骤 33　点击左侧窗格中的 **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 与 65535 之间。
- （可选）选中 **Do not prepend local AS number for routes received from neighbor** 复选框。不向从 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。不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

本节介绍定义将由 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，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 **Add**。

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 下拉列表选择网络或子网掩码。

步骤 6　从 Route Map 下拉列表选择为过滤要通告的网络而应当检查的路由映射。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另一个路由域重新分发到 BGP 的条件所需的步骤。

操作步骤

步骤 1　在 ASDM 中，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 **Add**。

系统将显示 Add Redistribution 窗格。

步骤 4　从 Source Protocol 下拉列表选择想要重新分发到 BGP 域的协议。

步骤 5　从 Process ID 下拉列表选择源协议的进程 ID。

步骤 6　（可选）在 Metric 字段输入已重新分发路由的度量。

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当检查的路由映射。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，从 OSPF 网络重新分发路由。

注　此步骤仅适用于从 OSPF 网络进行重新分发。

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，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 **Add**。

系统将显示 Add Conditionally injected route 窗格。

步骤 4　从 Inject Map 下拉列表选择指定要注入本地 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，将已注入的路由配置为继承汇聚路由的属性。

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，请执行以下步骤：

注 要禁用 BGP Log 消息，请在路由器配置模式中输入 **no bgp log-neighbor-changes** 命令。这会禁用邻居变更消息的日志记录。在 BGP 路由进程的路由器配置模式中输入此命令。
默认情况下，已记录邻居变更。

- **Monitoring > Routing > BGP Neighbors**

  每行均代表一个 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、空闲等）、正常运行时间、优雅重启功能、重启时间和过时路径时间。

- **Monitoring > Routing > BGP Routes**

  每行均代表一个 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、路由本地首选项值、权重和路径。

BGP 历史记录

表 22-1 列出了各种功能变更以及实施该等功能变更的平台版本。ASDM 向后兼容多个平台版本，因此，未列出已添加支持的特定 ASDM 版本。

表 22-1 BGP 功能历史

功能名称	平台版本	功能信息
BGP 支持	9.2(1)	添加了以下支持：可以使用边界网关协议路由数据、执行身份验证以及重新分发和监控路由信息。 我们引入以下 ASDM 屏幕： Configuration > Device Setup > Routing > BGP Monitoring > Routing > BGP Neighbors, Monitoring > Routing > BGP Routes 我们修改了以下 ASDM 屏幕： Configuration > Device Setup > Routing > Static Routes> Add > Add Static Route Configuration > Device Setup > Routing > Route Maps> Add > Add Route Map
ASA 集群的 BGP 支持	9.3(1)	我们添加了对 L2 和 L3 集群的支持。 我们修改了以下 ASDM 屏幕：Configuration > Device Setup > Routing > BGP > IPv4 Family > General

表 22-1　　BGP 功能历史　（续）

功能名称	平台版本	功能信息
不间断转发的 BGP 支持	9.3(1)	我们添加了对不间断转发的支持。 我们修改了以下 ASDM 屏幕：Configuration > Device Setup > Routing > BGP > General, Configuration > Device Setup > Routing > BGP > IPv4 Family > Neighbor、Monitoring > Routing > BGP Neighbors
通告映射的 BGP 支持	9.3(1)	我们添加了对 BGPv4 通告映射的支持。 我们修改了以下 ASDM 屏幕：Configuration > Device Setup > Routing > BGP > IPv4 Family > Neighbor > Add BGP Neighbor > Routes

OSPF

本章描述如何配置思科 ASA 以使用开放式最短路径优先 (OSPF) 路由协议来路由数据，执行身份验证和重新分发路由信息。

本章包含以下各节：

关于 OSPF

OSPF 是一种使用链路状态而非距离矢量进行路径选择的内部网关路由协议。OSPF 传播链路状态通告而非路由表更新。由于仅交换 LSA 而不是整个路由表，因此 OSPF 网络比 RIP 网络更快收敛。

OSPF 使用链路状态算法构建和计算到所有已知目标的最短路径。OSPF 区域中的每台路由器包含相同的链路状态数据库，该数据库是由每台路由器可使用的接口和可到达的邻居组成的列表。

OSPF 相比于 RIP 包括以下优点：

- OSPF 链路状态数据库更新的发送频率低于 RIP 更新，并且随着过时信息的超时，链路状态数据库即时而非逐步更新。
- 路由决策基于成本，它表明通过特定接口发送数据包所需的开销。 ASA 根据链路带宽而非到目标的跃点数计算接口的成本。可以配置成本来指定首选路径。

最短路径优先算法的缺点是需要大量 CPU 周期和内存。

ASA 可以在不同接口集上同时运行 OSPF 协议的两个进程。如果您具有使用相同 IP 地址的接口（NAT 允许这些接口共存，但是 OSPF 不允许重叠的地址），则可以要运行两个进程。或者，可能要在内部运行一个进程，在外部运行另一个进程，并且在两个进程之间重新分发路由的子集。同样，可能需要将专用地址与公用地址分离。

可以将路由从一个 OSPF 路由进程、 RIP 路由进程或从在启用了 OSPF 的接口上配置的静态路由和已连接路由重新分发到另一个 OSPF 路由进程中。

ASA 支持以下 OSPF 功能：

- 区域内、区域间和外部 （I 类和 II 类）路由。
- 虚拟链路。
- LSA 泛洪。
- OSPF 数据包身份验证 （密码和 MD5 身份验证）。
- 将 ASA 配置为指定路由器或指定备用路由器。 ASA 也可以设置为 ABR。
- 末节区域和次末节区域。
- 区域边界路由器 3 类 LSA 过滤。

OSPF 支持 MD5 和明文邻居身份验证。如有可能，应该将身份验证与所有路由协议配合使用，因为在 OSPF 和其他协议 （如 RIP）之间的路由重新分发可能会被攻击者用于破坏路由信息。

如果使用 NAT，如果 OSPF 是在公共和专用区域上运行，并且如果要求地址过滤，则需要运行两个 OSPF 进程，一个进程对应于公共区域，一个进程对应于专用区域。

在多个区域中具有接口的路由器称为区域边界路由器 (ABR)。充当网关以在使用 OSPF 的路由器之间与使用其他路由协议的路由器之间重新分发流量的路由器称为自治系统边界路由器 (ASBR)。

ABR 使用 LSA 将有关可用路由的信息发送到其他 OSPF 路由器。使用 ABR 3 类 LSA 过滤，可以具有单独的以 ASA 为 ABR 的专用和公共区域。可以将 3 类 LSA（区域间路由）从一个区域过滤到另一个区域，借此能够将 NAT 和 OSPF 一起使用而不通告专用网络。

注 只能过滤 3 类 LSA。如果在专用网络中将 ASA 配置为 ASBR，它将发送描述专用网络的 5 类 LSA，后者会泛洪至整个 AS，包括公共区域。

如果采用 NAT 但 OSPF 仅在公共区域中运行，则可以在专用网络内将公共网络的路由作为默认或 5 类 AS 外部 LSA 重新分发。但是，需要为受 ASA 保护的专用网络配置静态路由。此外，不应在同一 ASA 接口上混用公用和专用网络。

可以同时在 ASA 上运行两个 OSPF 路由进程、一个 RIP 路由进程和一个 EIGRP 路由进程。

快速呼叫数据包 OSPF 支持

快速呼叫数据包 OSPF 支持功能提供在小于 1 秒的间隔内发送呼叫数据包的配置方法。此类配置在开放式最短路径优先 (OSPF) 网络中会导致更快的收敛。

快速呼叫数据包 OSPF 支持的先决条件

OSPF 必须已在网络中进行配置或与快速呼叫数据包 OSPF 支持功能同时配置。

有关快速呼叫数据包 OSPF 支持的信息。

以下各节描述与快速呼叫数据包 OSPF 支持相关的概念：

- OSPF 呼叫间隔和停顿间隔
- OSPF 快速呼叫数据包
- OSPF 快速呼叫数据包的好处

OSPF 呼叫间隔和停顿间隔

OSPF 呼叫数据包是 OSPF 进程向其 OSPF 邻居发送以保持与这些邻居的连接的数据包。呼叫数据包按照可配置间隔 （以秒为单位）进行发送。对于以太网链路，默认值为 10 秒；对于非广播链路，默认值为 30 秒。呼叫数据包包含在停顿间隔内为其接收到呼叫数据包的所有邻居的列表。停顿间隔也是可配置间隔 （以秒为单位），并且默认为呼叫间隔值的四倍。所有呼叫间隔的值在网络中都必须相同。同样，所有停顿间隔的值在网络中也必须都相同。

这两种间隔通过表明链路可运行来保持连接。如果路由器在停顿间隔内没有从邻居接收到呼叫数据包，它将声明该邻居关闭。

OSPF 快速呼叫数据包

OSPF 快速呼叫数据包是指按照小于 1 秒的间隔发送的呼叫数据包。要了解快速呼叫数据包，您应该已经了解 OSPF 呼叫数据包与停顿间隔之间的关系。请参阅第 23-3 页的 OSPF 呼叫间隔和停顿间隔。

通过使用 **ospf dead-interval** 命令来获取 OSPF 快速呼叫数据包。停顿间隔设置为 1 秒，并且 hello-multiplier 值设置为在该 1 秒期间要发送的呼叫数据包的数量，从而提供亚秒或 “ 快速 ” 呼叫数据包。

当在接口上配置了快速呼叫数据包时，此接口发出的呼叫数据包中通告的呼叫间隔设置为 0。系统将忽略通过此接口接收到的呼叫数据包中的呼叫间隔。

无论停顿间隔设置为 1 秒 （对于快速呼叫数据包）还是设置为任何其他值，它在分段上都必须一致。只要在停顿间隔内发送了至少一个呼叫数据包，呼叫乘数对于整个分段便无需相同。

OSPF 快速呼叫数据包的好处

OSPF 快速呼叫数据包功能的好处是 OSPF 网络将比没有快速呼叫数据包的情况更快收敛。通过此功能可在 1 秒内检测丢失的邻居。它在开放式系统互连 (OSI) 物理层和数据链路层可能未检测到邻居丢失的 LAN 分段中尤其有用。

OSPFv2 与 OSPFv3 之间的实施差异

OSPFv3 不与 OSPFv2 向后兼容。要使用 OSPF 路由 IPv4 和 IPv6 流量，必须同时运行 OSPFv2 和 OSPFv3。它们会共存但不相互交互。

OSPFv3 提供的其他功能包括：

- 逐条链路进行协议处理。
- 移除寻址语义。
- 添加泛洪范围。
- 支持每条链路多个实例。
- 使用 IPv6 链路本地地址执行网络发现和其他功能。

- 以前缀和前缀长度表示 LSA。
- 添加两种 LSA 类型。
- 处理未知 LSA 类型。
- 使用 OSPFv3 路由协议流量的 IPsec ESP 标准支持身份验证，如 RFC-4552 所指定。

OSPF 准则

情景模式准则

OSPFv2 支持单情景和多情景模式。

OSPFv3 仅支持单情景模式。

防火墙模式准则

OSPF 仅支持路由防火墙模式。 OSPF 不支持透明防火墙模式。

故障转移准则

OSPFv2 和 OSPFv3 支持有状态故障转移。

IPv6 准则

- OSPFv2 不支持 IPv6。
- OSPFv3 支持 IPv6。
- OSPFv3 使用 IPv6 进行身份验证。
- ASA 将 OSPFv3 路由安装到 IPv6 RIB 中，前提是它是最佳路由。
- 可以在 **capture** 命令中使用 IPv6 ACL 滤除 OSPFv3 数据包。

集群准则

- OSPFv2 和 OSPFv3 支持集群。
- 不支持 OSPFv3 加密。如果尝试在集群环境中配置 OSPFv3 加密，系统将显示错误消息。
- 在跨接口模式中，在管理专属接口上不支持动态路由。
- 在单个接口模式中，请确保将主单元和从属单元建立为 OSPFv2 或 OSPFv3 邻居。
- 当配置 OSPFv2 和 EIGRP 时，可以使用跨接口模式或单个接口模式；不能同时使用这两种模式。
- 在单个接口模式中，只能在主单元的共享接口上的两个情景之间建立 OSPFv2 邻接。仅在点对点链路上支持配置静态邻居；因此，在接口上仅允许一个邻居声明。
- 路由器 ID 在 OSPFv2、OSPFv3 和 EIGRP 路由器配置模式中是可选的。如果没有显式设置路由器 ID，则会自动生成路由器 ID 并将其设置为各集群单元中任意数据接口上的最高 IPv4 地址。
- 如果尚未配置集群接口模式，则仅允许将单个点分十进制 IPv4 地址作为路由器 ID，并会禁用 **cluster pool** 选项。
- 如果集群接口模式设置为跨接口配置，则仅允许将单个点分十进制 IPv4 地址作为路由器 ID，并会禁用 **cluster pool** 选项。
- 如果集群接口模式设置为单个接口配置，则必需 **cluster pool** 选项，并且不允许将单个点分十进制 IPv4 地址作为路由器 ID。

- 将集群接口模式从跨接口配置更改为单个接口配置（反之亦然）而不指定 **check-detail** 或 **nocheck** 选项时，将移除整个配置，包括路由器 ID。
- 如果任何动态路由协议路由器 ID 与新接口模式不兼容，则控制台上会显示错误消息，并且接口模式 CLI 失败。该错误消息中对应于每个动态路由协议（OSPFv2、OSPFv3 和 EIGRP）包含一行内容，并会列出出现不兼容配置时所处的每个情景的名称。
- 如果为 **cluster interface mode** 命令指定 **nocheck** 选项，即使所有路由器 ID 配置可能与新模式不兼容，也允许更改接口模式。
- 启用集群后，将重复路由器 ID 兼容性检查。如果检测到任何不兼容情况，则 **cluster enable** 命令会失败。管理员需要先更正不兼容的路由器 ID 配置，然后才能启用集群。
- 当某个单元作为从属单元进入集群时，建议为 **cluster interface mode** 命令指定 **nocheck** 选项，以避免任何路由器 ID 兼容性检查失败。从属单元仍然从主单元继承路由器配置。
- 当集群中发生主身份角色更改时，将出现以下行为：
  - 在跨接口模式中，路由器进程仅在主单元上处于活动状态，在从属单元上处于挂起状态。各集群单元具有同一路由器 ID，因为已从主单元对配置进行同步。因此，在角色更改期间，相邻路由器不会注意到集群的路由器 ID 发生的任何更改。
  - 在单个接口模式中，路由器进程在所有单个集群单元上都处于活动状态。各集群单元从已配置的集群池中选择其自己独特的路由器 ID。集群中的主身份角色更改不会以任何方式更改路由拓扑。

附加准则

- OSPFv2 和 OSPFv3 在接口上支持多个实例。
- OSPFv3 在非集群环境中通过 ESP 头支持加密。
- OSPFv3 支持非负载加密。
- OSPFv2 根据 RFC 4811、 4812 和 3623 定义分别支持思科 NSF 无中断重新启动和 IETF NSF 无中断重新启动机制。
- OSPFv3 根据 RFC 5187 定义支持无中断重新启动机制。

配置 OSPFv2

本节描述如何在 ASA 上启用 OSPFv2 进程。

启用 OSPFv2 后，需要定义路由映射。有关详细信息，请参阅第 21-4 页的定义路由映射。然后，生成默认路由。有关详细信息，请参阅第 20-2 页的静态路由配置。

为 OSPFv2 进程定义路由映射后，可以根据特定需要对其进行定制。要了解任何在 ASA 上定制 OSPFv2 进程，请参阅第 23-6 页的定制 OSPFv2。

要启用 OSPFv2，需要创建 OSPFv2 路由进程，指定与该路由进程关联的 IP 地址的范围，然后指定与 IP 地址范围关联的区域 ID。

可以启用最多两个 OSPFv2 进程实例。每个 OSPFv2 进程具有其自己的关联区域和网络。

要启用 OSPFv2，请执行以下步骤：

操作步骤

步骤 1 在 ASDM 主窗口中，选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

在 OSPF Setup 窗格中，可以启用 OSPF 进程，配置 OSPF 区域和网络，以及定义 OSPF 路由摘要。

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，可以为每个情景启用最多两个 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、Adjacency Changes、Administrative Route Distances、Timers 和 Default Information Originate 设置。

- 通过 **Area/Networks** 选项卡，可以显示其为 ASA 上的各 OSPF 进程包含的区域和网络。从该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，请参阅第 23-13 页的配置 OSPFv2 区域参数以获取详细信息。
- 通过 **Route Summarization** 选项卡，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 配置为通告摘要路由，包括该区域内属于指定范围的所有单独网络。有关详细信息，请参阅第 23-10 页的配置 OSPFv2 区域之间的路由摘要。

配置 OSPF 快速呼叫数据包

本节描述如何配置 OSPF 快速呼叫数据包。

操作步骤

定制 OSPFv2

本节说明如何定制 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。

注　如果要通过定义允许将来自指定路由协议的哪些路由重新分发到目标路由进程中来重新分发路由，必须首先生成默认路由。请参阅第 20-2 页的静态路由配置，然后根据第 21-4 页的定义路由映射定义路由映射。

要将静态、已连接、 RIP 或 OSPFv2 路由重新分发到 OSPFv2 进程中，请执行以下步骤：

操作步骤

步骤 1　在 ASDM 主窗口中，选择 **Configuration > Device Setup > Routing > OSPF > Redistribution**。

Redistribution 窗格显示将路由从一个路由进程重新分发到 OSPF 路由进程中的规则。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 （如果有）将为所选条目打开 Add/Edit OSPF Redistribution Entry 复选框。

注　后面所有步骤都是可选的。

通过 Add/Edit OSPF Redistribution Entry 对话框，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。可以选择以下选项之一：

- 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。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 1 类 NSAA 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 NSAA 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度量值。有效值范围为 1 至 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，如果未指定度量值，则会将度量从一个进程携带至另一个进程。将其他进程重新分发到 OSPF 进程时，如果未指定度量值，则默认度量为 20。

步骤 7 为 Metric Type 选择以下选项之一。

- 如果度量是 1 类外部路由，请选择 **1**。
- 如果度量是 2 类外部路由，请选择 **2**。

步骤 8 在 Tag Value 字段中输入标记值。

标记值是附加到 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 至 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，请参阅第 21-4 页的定义路由映射。

步骤 13 点击 **OK**。

将路由重新分发到 OSPFv2 中时配置路由摘要

将来自其他协议的路由重新分发到 OSPF 中时，将在外部 LSA 中单独通告每个路由。但是，可以将 ASA 配置为对于为指定网络地址和掩码包含的所有重新分发的路由通告单个路由。此配置可减小 OSPF 链路状态数据库的大小。

可以抑制与指定 IP 地址 / 掩码对相匹配的路由。标记值可用作用于通过路由映射控制重新分发的值。

要配置路由摘要，可以执行以下操作：

- 第 23-9 页的添加路由摘要地址
- 第 23-9 页的添加或编辑 OSPF 摘要地址

添加路由摘要地址

Summary Address 窗格显示有关为每个 OSPF 路由进程配置的摘要地址的信息。

可以汇总从其他路由协议获知的路由。用于通告摘要的度量是所有更具体路由的最小度量。摘要路由帮助减小路由表的大小。

对 OSPF 使用摘要路由会导致 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　OSPF 不支持摘要地址 0.0.0.0 0.0.0.0。

要在一个摘要路由上配置适用于为网络地址和掩码包含的所有重新分发的路由的软件通告，请执行以下步骤：

操作步骤

步骤 1　在 ASDM 主页中，选择 **Configuration > Device Setup > Routing > OSPF > Summary Address**。

步骤 2　点击 **Add**。

系统将显示 Add OSPF Summary Address Entry 对话框。可以向 Summary Address 表中的现有条目添加新条目。编辑现有条目时，无法更改某些摘要地址信息。

步骤 3　从 OSPF Process 下拉列表中选择与摘要地址关联的指定 OSPF 进程 ID。编辑现有条目时，无法更改此信息。

步骤 4　在 IP Address 字段中输入摘要地址的 IP 地址。编辑现有条目时，无法更改此信息。

步骤 5　从 Netmask 下拉列表中选择摘要地址的网络掩码。编辑现有条目时，无法更改此信息。

步骤 6　选中 **Advertise** 复选框以通告摘要路由。取消选中此复选框以抑制属于摘要地址的路由。默认情况下，会选中此复选框。

标记值显示附加到各外部路由的 32 位十进制值。 OSPF 本身未使用该值，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 摘要地址

操作步骤

步骤 1　在 ASDM 主窗口中，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，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，无法更改某些摘要地址信息。

步骤 3　从 OSPF Process 下拉列表中选择与摘要地址关联的指定 OSPF 进程 ID。编辑现有条目时，无法更改此信息。

步骤 4　在 IP Address 字段中输入摘要地址的 IP 地址。编辑现有条目时，无法更改此信息。

步骤 5 从 Netmask 下拉列表中选择摘要地址的网络掩码。编辑现有条目时，无法更改此信息。

步骤 6 选中 **Advertise** 复选框以通告摘要路由。取消选中此复选框以抑制属于摘要地址的路由。默认情况下，会选中此复选框。

配置 OSPFv2 区域之间的路由摘要

路由摘要是通告地址的整合。此功能导致通过区域边界路由器向其他区域通告单个摘要路由。在 OSPF 中，区域边界路由器将一个区域中的网络通告到另一个区域中。如果以某种方式分配区域中的网络号来使其连续，则可以将区域编辑路由器配置为通告摘要路由，包括该区域内属于指定范围的所有单独网络。

要定义摘要路由的地址范围，请执行以下步骤：

操作步骤

步骤 1 在 ASDM 主窗口中，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，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，无法更改某些摘要地址信息。

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 字段中输入摘要地址的 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，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：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，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，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，请参阅第 23-13 页的配置 OSPFv2 区域参数。默认情况下会禁用区域身份验证。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 至 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。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。有关详细信息，请参阅第 23-17 页的定义静态 OSPFv2 邻居。
- 无需定义指向加密终端的静态路由。有关详细信息，请参阅第 20-2 页的静态路由配置。
- 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成本。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期间过滤传出 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。该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。有效值范围为 1 至 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。请保守地设置该值，否则可能会产生不必要的重新传输。该值对于串行线路和虚拟链路应该较大。有效值范围为 1 至 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。有效值范围为 1 至 8192 秒。默认值为 1 秒。

步骤 15　在 Detecting Lost Neighbors 部分中，执行以下操作之一：

- 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间隔（以秒为单位）。有效值范围为 1 至 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

可以配置多个 OSPF 区域参数。这些区域参数 （显示在以下任务列表中）包括设置身份验证，定义末节区域以及向默认摘要路由分配特定成本。身份验证提供基于密码的区域非授权访问防御。

末节区域是有关外部路由的信息未发送到的区域。相反，ABR 生成了到自治系统外部目标的末节区域中的默认外部路由。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，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 Area Type 选项之一：

- **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 复选框来选择防止摘要 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 复选框来选择防止摘要 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。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 区域的默认成本。

有效值范围为 0 至 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。在转换期间支持摘要和过滤。

如果您是必须将使用 OSPFv2 的中心站点连接到对 NSSA 使用其他路由协议的远程站点的 ISP 或网络管理员，则可以简化管理。

在 NSSA 实施前，企业站点边界路由器和远程路由器之间的连接不能作为 OSPFv2 末节区域运行，因为远程站点的路由无法重新分发到末节区域中，并且需要保持两种路由协议。通常会运行简单协议 （如 RIP）并使用其处理重新分发。在使用 NSSA 的情况下，可以通过将企业路由器和远程路由器之间的区域定义为 NSSA 来将 OSPFv2 扩展至覆盖远程连接。

使用此功能之前，请遵循以下准则：

- 可以设置用于到达外部目标的 7 类默认路由。配置时，路由器会生成到 NSSA 或 NSSA 区域边界路由器中的 7 类默认路由。
- 同一区域内的每个路由器都必须同意区域为 NSSA ；否则，路由器无法相互通信。

操作步骤

步骤 1　在 ASDM 主页中，选择 **Configuration > Device Setup > Routing > OSPF > Setup**。

步骤 2　点击 **Area/Networks** 选项卡。

步骤 3　点击 **Add**。

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 复选框来选择防止摘要 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。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 区域的默认成本。

有效值范围为 0 至 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　在 ASDM 主页中，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）。如果未输入 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　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 的单个接口集群中的路由器 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，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。如果未配置 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　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

需要定义静态 OSPFv2 邻居来通过点对点非广播网络通告 OSPFv2 路由。通过此功能，可以跨现有 VPN 连接广播 OSPFv2 通告，而不必将通告封装在 GRE 隧道中。

开始之前，必须创建到 OSPFv2 邻居的静态路由。有关创建静态路由的详细信息，请参阅第 20 章，“静态路由和默认路由”。

操作步骤

步骤 1　在 ASDM 主窗口中，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，可以定义新静态邻居或更改现有静态邻居的信息。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

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。

要配置路由计算计时器，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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，可以修改用于配置 LSA 节奏计时器和 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）。有效值范围为 0 至 600000 毫秒。
- 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。有效值范围为 0 至 600000 毫秒。

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。

要记录 OSPFv2 邻居启动或关闭，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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。默认情况下会选中此设置。
- 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。默认情况下会取消选中此设置。

步骤 5　点击 **OK**。

注　必须启用日志记录以发送邻居启动或关闭消息。

在 OSPF 中配置过滤

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。此类型的区域过滤可以应用在特定 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 过滤可提高对 OSPF 区域之间路由重新分发的控制。

注　系统仅过滤源于 ABR 的 3 类 LSA。

要在 OSPF 中配置过滤，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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，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，某些过滤信息无法更改。

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 下拉列表中选择过滤的流量方向。

选择 Inbound 以过滤传入 OSPF 区域的 LSA，或者选择 Outbound 以过滤传出 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，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，请参阅第 21-7 页的配置前缀列表和第 21-8 页的为路由操作配置度量值。

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，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。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，通过点击以下选项之一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，请参阅第 23-13 页的配置 OSPFv2 区域参数。默认情况下会禁用区域身份验证。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 至 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，通过从以下选项中进行选择来指定数据包的间隔时间：

- **Hello Interval**，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。该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。有效值范围为 1 至 65535 秒。默认值为 10 秒。
- **Retransmit Interval**，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。请保守地设置该值，否则可能会产生不必要的重新传输。该值对于串行线路和虚拟链路应该较大。有效值范围为 1 至 65535 秒。默认值为 5 秒。
- **Transmit Delay**，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。有效值范围为 1 至 65535 秒。默认值为 1 秒。
- **Dead Interval**，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 至 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

本部分描述如何配置 OSPFv3 路由进程。

启用 OSPFv3

要启用 OSPFv3，需要创建 OSPFv3 路由进程，创建 OSPFv3 的区域，启用 OSPFv3 的接口，然后将路由重新分发到目标 OSPFv3 路由进程中。

要启用 OSPFv3，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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。可以启用最多两个 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** 以保存更改。

步骤 5　要继续，请参阅第 23-22 页的配置 OSPFv3 区域参数。

配置 OSPFv3 接口参数

如有必要，可以更改某些特定于接口的 OSPFv3 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：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。

要为 IPv6 配置 OSPFv3 接口参数，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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。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成本。

步骤 18　在 Priority 字段中输入路由器优先级，这有助于为网络确定 指定的路由器。有效值范围为 0 至 255。

步骤 19　接收到 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，会启用 OSPF MTU 不匹配检测。

步骤 20　选中 **Filter outgoing link state advertisements** 复选框以过滤到 OSPFv3 接口的传出 LSA。默认情况下，所有传出 LSA 都泛洪至该接口。

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。有效值范围为 1 至 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）。有效值范围为 1 至 65535 秒。默认值为 1 秒。

步骤 25　点击 **OK**。

步骤 26　点击 **Apply** 以保存更改。

配置 OSPFv3 区域参数

要配置 OSPFv3 区域参数，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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**。要移除所选区域，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　要允许将摘要 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度量。默认值为 10。有效度量值范围为 0 至 16777214。

步骤 11　从 Metric Type 下拉列表中选择度量类型。度量类型是与通告到 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 字段中输入成本。

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）输入摘要路由的度量或成本，它在 OSPF SPF 计算期间用于确定目标的最短路径。有效值范围为 0 至 16777215。

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 类摘要 LSA。

步骤 21　点击 **OK**。

步骤 22　要继续，请参阅第 23-23 页的配置虚拟链路邻居。

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，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**。要移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）。该值必须对于连接到公用网络的所有路由器和接入服务器都相同。有效值范围为 1 至 8192。

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。该值必须对于连接到公用网络的所有路由器和接入服务器都相同。有效值范围为 1 至 8192。默认值为 10。

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** 以保存更改。

配置 OSPFv3 被动接口

要配置 OSPFv3 被动接口，请执行以下步骤：

步骤 1 在 ASDM 主窗口中，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，可以在接口上启用被动 OSPFv3 路由。被动路由帮助控制 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** 以保存更改。

配置 OSPFv3 管理距离

要为 IPv6 路由配置 OSPFv3 管理距离，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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，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，指定 OSPV 的区域间路由作为 IPv6 路由。
- Intra Area，指定 OSPF 的区域内路由作为 IPv6 路由。
- External，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** 以保存更改。

配置 OSPFv3 计时器

可以为 OSPFv3 设置 LSA 到达计时器、 LSA 步调设置计时器和调速计时器。

要设置 ASA 接受来自 OSPFv3 邻居的同一 LSA 的最短间隔，请执行以下步骤：

要配置 LSA 泛洪数据包步调设置，请执行以下步骤：

要更改将 OSPFv3 LSA 收集到组中并刷新、校验和或老化的间隔，请执行以下步骤：

要配置 LSA 重新传输数据包步调设置，请执行以下步骤：

LSA 和 SPF 调速提供一种动态机制在网络不稳定期间降低 OSPFv3 中的 LSA 更新速度，并通过提供 LSA 速率限制 （以毫秒为单位）允许更快的 OSPFv3 收敛。

要配置 LSA 和 SPF 调速计时器，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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，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，指定前后两次接受从邻居到达的同一 LSA 之间必须经过的最小延迟（以毫秒为单位）。范围为 0 至 6000,000 毫秒。默认值为 1000 毫秒。
- LSA Flood Pacing，指定在前后两次更新之间泛洪队列中的 LSA 设置步调的间隔时间 （以毫秒为单位）。可配置范围为 5 至 100 毫秒。默认值为 33 毫秒。

- LSA Group Pacing，指定将 LSA 收集到组中并刷新、检验和或老化的间隔 （以秒为单位）。有效值范围为 10 至 1800。默认值为 240。
- LSA Retransmission Pacing，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）。可配置范围为 5 至 200 毫秒。默认值为 66 毫秒。
- LSA Throttle Initial，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，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，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　对于 LSA 调速，如果最小时间或最大时间小于第一次出现值，则 OSPFv3 会自动更正为第一次出现值。同样，如果指定的最大延迟小于最小延迟，则 OSPFv3 会自动更正为最小延迟值。

- SPF Throttle Initial，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，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，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　对于 SPF 调速，如果最小时间或最大时间小于第一次出现值，则 OSPFv3 会自动更正为第一次出现值。同样，如果指定的最大延迟小于最小延迟，则 OSPFv3 会自动更正为最小延迟值。

步骤 5　点击 **OK**。

步骤 6　点击 **Apply** 以保存更改。

定义静态 OSPFv3 邻居

需要定义静态 OSPFv3 邻居来通过点对点非广播网络通告 OSPF 路由。通过此功能，可以跨现有 VPN 连接广播 OSPFv3 通告，而不必将通告封装在 GRE 隧道中。

开始之前，必须创建到 OSPFv3 邻居的静态路由。有关创建静态路由的详细信息，请参阅第 20 章，“静态路由和默认路由”。

要定义静态 OSPFv3 邻居，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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，可以定义新静态邻居或更改现有静态邻居的信息。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

要将路由器配置为在 OSPFv3 邻居启动或关闭时发送系统日志消息，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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，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** 以保存更改。

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：

步骤 1　在 ASDM 主窗口中，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**。

计算摘要路由成本

要根据 RFC 1583 计算摘要路由成本，执行以下步骤：

步骤 1 在 ASDM 主窗口中，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

要生成到 OSPFv3 路由域中的默认路由，请执行以下步骤：

步骤 1 在 ASDM 主窗口中，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度量。有效度量值范围为 0 至 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：

- 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** 以保存更改。

配置 IPv6 摘要前缀

要配置 IPv6 摘要前缀，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，选择 **Configuration > Device Setup > Routing > OSPFv3 > Summary Prefix**。

步骤 2　要添加新摘要前缀，请点击 **Add**。要修改现有摘要前缀，请点击 **Edit**。要移除摘要前缀，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记值。

步骤 7　点击 **OK**。

步骤 8　点击 **Apply** 以保存更改。

重新分发 IPv6 路由

要将已连接路由重新分发到 OSPFv3 进程中，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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**。要移除所选参数集，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 字段中输入度量值。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，如果未指定度量值，则会将度量从一个进程携带至另一个进程。将其他进程重新分发到 OSPF 进程时，如果未指定度量值，则默认度量为 20。

步骤 6　从 Metric Type 下拉列表中选择度量类型。可用选项为 None、 1 和 2。

步骤 7　（可选）在 Tag 字段中输入标记值。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。有效值范围为 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过滤。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记，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，然后选中以下复选框之一：

- **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 类外部路由导入到 OSPFv3 中
- **External 2**，表示自治系统的外部路由，但会作为 2 类外部路由导入到 OSPFv3 中
- **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** 以保存更改。

配置无中断重新启动

ASA 可能会遇到一些已知的故障情况，这些故障情况不应影响跨交换平台转发的数据包。不间断转发 (NSF) 功能允许在还原路由协议信息的同时沿已知路由继续转发数据。此功能在以下情况下有用：存在组件故障 （即，在故障转移 (HA) 模式中主用单元崩溃而备用单元接管，在集群模式中主要单元崩溃而从属单元被选为新的主要单元），或者已计划无中断软件升级。

在 OSPFv2 和 OSPFv3 上均支持无中断重新启动。通过使用 NSF Cisco（RFC 4811 和 RFC 4812）或 NSF IETF (RFC 3623)，可以在 OSPFv2 上配置无中断重新启动。可以使用 graceful-restart (RFC 5187) 在 OSPFv3 上配置无中断重新启动。

配置 NSF 无中断重新启动功能涉及两个步骤：配置功能和将设备配置为具有 NSF 功能或可感知 NSF。具有 NSF 功能的设备可以向邻居表明其自己的重新启动活动，而可感知 NSF 的设备可以帮助重新启动邻居。

根据某些条件，可以将设备配置为具有 NSF 功能或可感知 NSF：

- 设备可以配置为可感知 NSF，而与其所处的模式无关。
- 设备必须处于 Failover 或 Spanned Etherchannel (L2) 集群模式中才能配置为具有 NSF 功能。
- 为使设备可感知 NSF 或具有 NSF 功能，应将其配置为能够根据需要处理不透明链路状态通告 (LSA)/ 本地链路信令 (LLS) 块。

注　如果为 OSPFv2 配置了快速呼叫，则在主用单元重新加载且备用单元激活时不会发生无中断重新启动。这是因为角色更改所需的时间超过配置的停顿间隔。

为 OSPFv2 配置无中断重新启动

对于 OSPFv2、Cisco NSF 和 IETF NSF，存在两种无中断重新启动机制。一次只能为 ospf 实例配置其中一种无中断重新启动机制。可感知 NSF 的设备既可以配置为 Cisco NSF 助手，也可以配置为 IETF NSF 助手，但是一次只能在 Cisco NSF 或 IETF NSF 模式中为 ospf 实例配置具有 NSF 功能的设备。

为 OSPFv2 配置 Cisco NSF 无中断重新启动

要为 OSPFv2 配置 Cisco NSF 无中断重新启动（适用于具有 NSF 功能或可感知 NSF 的设备），请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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。

注　默认情况下会选中此项。取消选中此项将在可感知 NSF 的设备上禁用 Cisco NSF 助手模式。

步骤 5　点击 **OK**。

步骤 6　点击 **Apply** 以保存更改。

为 OSPFv2 配置 IETF NSF 无中断重新启动

要为 OSPFv2 配置 IETF NSF 无中断重新启动 （适用于具有 NSF 功能或可感知 NSF 的设备），请执行以下步骤

步骤 1　在 ASDM 主窗口中，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 字段中输入重新启动间隔。

注　默认值为 120 秒。对于小于 30 秒的重新启动间隔，将终止无中断重新启动。

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。

注　默认情况下会选中此项。取消选中此项将在可感知 NSF 的设备上禁用 IETF NSF 助手模式。

步骤 5　点击 **OK**。

步骤 6　点击 **Apply** 以保存更改。

为 OSPFv3 配置无中断重新启动

为 OSPFv3 配置 NSF 无中断重新启动功能涉及两个步骤：将一个设备配置为具有 NSF 功能，然后将另一个设备配置为可感知 NSF。要为 OSPFv3 配置无中断重新启动，请执行以下步骤输入以下命令：

步骤 1 在 ASDM 主窗口中，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 字段中输入重新启动间隔值。

注 默认值为 120 秒。对于小于 30 秒的重新启动间隔，将终止无中断重新启动。

步骤 4 在 Configuring Graceful Restart Helper 下，选中 **Enable Graceful Restart Helper** 复选框。

注 默认情况下会选中此项。取消选中此项将在可感知 NSF 的设备上禁用无中断重新启动助手模式。

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。

注 启用时，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：它检测到会泛洪至正在重新启动的路由器的 LSA 发生更改，或者如果在启动无中断重新启动过程后正在重新启动的路由器的重新传输列表中有已更改的 LSA。

步骤 6 点击 **OK**。

步骤 7 点击 **Apply** 以保存更改。

移除 OSPF 配置

要移除已启用的整个 OSPFv2 配置，执行以下步骤：

步骤 1 在 ASDM 主窗口中，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**。

要移除已启用的整个 OSPFv3 配置，执行以下步骤：

步骤 1 在 ASDM 主窗口中，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 的配置示例

以下示例显示如何使用各种可选进程启用和配置 OSPFv2：

步骤 1　在 ASDM 主窗口中，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，选择 **Configuration > Device Setup > Routing > OSPF > Redistribution**。

步骤 9　点击 **Add**。

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度量值。

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，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　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，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 的配置

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，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，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，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** 以保存更改。

监控 OSPF

您可以显示特定统计，如 IP 路由表、缓存和数据库的内容。您还可以使用所提供的信息确定资源利用率和解决网络问题。您也可以显示有关节点可达性的信息并发现设备数据包通过网络所采用的路由路径。

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，选择 **Monitoring > Routing > OSPF LSAs**。

步骤 2 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，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，选择 **Monitoring > Routing > OSPFv3 LSAs**。

步骤 2 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，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。

附加参考资料

RFC

RFC	标题
2328	OSPFv2
4552	OSPFv3 Authentication
5340	OSPF for IPv6

OSPF 功能历史记录

表 23-1 列出了各种功能变更以及实施该等功能变更的平台版本。ASDM 向后兼容多个平台版本，因此，未列出已添加支持的特定 ASDM 版本。

表 23-1　　OSPF 功能历史记录

功能名称	平台版本	功能信息
OSPF 支持	7.0(1)	添加了对使用开放式最短路径优先 (OSPF) 路由协议来路由数据、执行身份验证以及重新分发和监控路由信息的支持。 我们引入了以下屏幕：Configuration > Device Setup > Routing > OSPF。
多情景模式中的动态路由	9.0(1)	在多情景模式中支持 OSPFv2 路由。 我们修改了以下屏幕：Configuration > Device Setup > Routing > OSPF > Setup
集群		对于 OSPFv2 和 OSPFv3，在集群环境中支持批量同步、路由同步和跨网络 EtherChannel 负载均衡。
IPv6 的 OSPFv3 支持		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 23-1 OSPF 功能历史记录 （续）

功能名称	平台版本	功能信息
OSPF 支持快速呼叫	9.2(1)	OSPF 支持快速呼叫数据包功能，从而产生在 OSPF 网络中导致更快收敛的配置。 我们修改了以下屏幕：Configuration > Device Setup > Routing > OSPF > Interface > Edit OSPF Interface Advanced Properties
计时器		添加了新 OSPF 计时器；启用了旧 OSPF 计时器。 我们修改了以下屏幕：Configuration > Device Setup > Routing > OSPF > Setup > Edit OSPF Process Advanced Properties
使用访问列表过滤路由		现在支持使用 ACL 过滤路由。 我们引入了以下屏幕：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
对不间断转发 (NSF) 的 OSPF 支持	9.3(1)	添加了对 NSF 的 OSPFv2 和 OSPFv3 支持。 我们添加了以下屏幕：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 Cisco ASA，以路由数据、执行身份验证和重新分发路由信息。

有关 EIGRP 的信息

EIGRP 是思科开发的 IGRP 增强版。与 IGRP 和 RIP 不同， EIGRP 不发送定期路由更新。仅在网络拓扑发生变化时才会发送 EIGRP 更新。将 EIGRP 与其他路由协议区分开来的主要功能包括快速聚合、支持可变长度子网掩码、支持部分更新以及支持多个网络层协议。

运行 EIGRP 的路由器存储所有的邻居路由表，以便迅速适应备用路由。如果不存在合适的路由，则 EIGRP 会查询其邻居以发现备用路由。这些查询会一直传播，直到找到备用路由。支持可变长度子网掩码功能允许在网络号边界自动摘要路由。此外，可以将 EIGRP 配置为在任何接口的任何位边界摘要。 EIGRP 不会定期发送更新。而仅在路由度量发生变化时才发送部分更新。部分更新的传播是自动绑定的，以便仅更新需要该信息的路由器。得益于这两项功能， EIGRP 与 IGRP 相比可显著减少占用的带宽。

邻居发现是 ASA 用于动态获悉直接连接的网络中其他路由器的过程。 EIGRP 路由器发送组播 Hello 数据包，通告其在网络中的存在状态。当 ASA 收到来自新邻居的 Hello 数据包时，会将其包含初始化位集的拓扑表发送至邻居。当邻居收到包含初始化位集的拓扑更新时，邻居将其拓扑表发回到 ASA。

Hello 数据包作为组播消息发送。预期不对 Hello 消息作出响应。但对静态定义的邻居除外。如果您使用 **neighbor** 命令或在 ASDM 中配置 Hello 时间间隔以配置邻居，则发送到该邻居的 Hello 消息将作为单播消息发送。路由更新和确认作为单播消息发送。

此邻居关系建立之后，除非网络拓扑发生变化，否则不会交换路由更新。邻居关系通过 Hello 数据包来维护。从邻居收到的每个 Hello 数据包均包括保持时间。这是 ASA 预期收到来自该邻居的 Hello 数据包的时间。如果 ASA 在保持时间内未收到由该邻居通告的 Hello 数据包，则 ASA 会将该邻居视为不可用。

EIGRP 协议使用四种关键算法技术，包括邻居发现 / 恢复、可靠的传输协议 (RTP) 和对于路由计算非常重要的 DUAL。 DUAL 将所有路由保存至拓扑表中的目标，而不仅是最低成本路由。最低成本路由会插入路由表。其他路由保留在拓扑表中。如果主路由发生故障，可以从可行后继路由中选择另一个路由。后继路由是指用于具有到达目标的最低成本路径的数据包转发的邻居路由器。可行性计算可确保路径不是路由环路的一部分。

如果未在拓扑表中找到可行后继路由，则必须进行路由重新计算。路由重新计算期间， DUAL 会查询 EIGRP 邻居获取路由，该邻居反过来查询其邻居。没有用于路由的可行后继路由的路由器会返回不可达消息。

路由重新计算期间，DUAL 会将路由标记为活动状态。默认情况下，ASA 等待三分钟接收来自其邻居的响应。如果 ASA 未收到来自邻居的响应，则路由会标记为陷入活动状态。拓扑表中指向无响应邻居的所有路由均作为可行性后继路被移除。

注 如果无 GRE 隧道， EIGRP 邻居关系就不会通过 IPSec 隧道得以支持。

使用集群

有关集群与 EIGRP 配合使用的信息，请参阅第 19-8 页的动态路由和集群。

EIGRP 许可要求

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

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

仅在路由防火墙模式中受支持。透明防火墙模式不受支持。

故障转移准则

在单情景模式和多情景模式中支持有状态故障转移。

IPv6 准则

不支持 IPv6。

集群准则

- 当配置为同时使用 EIGRP 和 OSPFv2 时，支持跨越式 EtherChannel 和单个接口集群。
- 在单个接口集群设置中， EIGRP 邻接关系只能在主要设备共享接口上的两个情景之间建立。分别手动配置对应每个集群节点的多个邻居语句，即可解决此问题。

附加准则

- 由于组播流量的情景间交换不受支持，因此 EIGRP 实例不能跨共享接口彼此建立邻接关系。
- 最多支持一个 EIGRP 进程。

要配置 EIGRP 进程的任务列表

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，选择 **Configuration > Device Setup > Routing > EIGRP**。

步骤 2　选中 Process Instances 选项卡中的 **Enable this EIGRP process** 复选框，启用 EIGRP 路由进程。请参阅第 24-4 页的启用 EIGRP 或第 24-5 页的启用 EIGRP 末节路由。

步骤 3　在 Setup > Networks 选项卡中定义将参与 EIGRP 路由的网络和接口。有关详细信息，请参阅第 24-6 页的为 EIGRP 路由进程定义网络。

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。有关详细信息，请参阅第 24-12 页的在 EIGRP 中过滤网络。

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。还可以将静态和连接的路由重新分发给 EIGRP 路由进程。有关详细信息，请参阅第 24-11 页的将路由重新分发到 EIGRP 中。

步骤 6　（可选）在 Static Neighbor 窗格中定义静态 EIGRP 邻居。

有关详细信息，请参阅第 24-10 页的定义 EIGRP 邻居。

步骤 7　（可选）在 Summary Address 窗格中定义摘要地址。

有关定义摘要地址的详细信息，请参阅第 24-8 页的在接口上配置摘要汇聚地址。

步骤 8　（可选）在 Interfaces 窗格中定义接口特定的 EIGRP 参数。这些参数包括 EIGRP 消息身份验证、保持时间、 Hello 时间间隔、时延度量和使用水平分割。有关详细信息，请参阅第 24-7 页的配置 EIGRP 的接口。

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。有关详细信息，请参阅第 24-14 页的在 EIGRP 中配置默认信息。

配置 EIGRP

本节介绍如何在系统中启用 EIGRP 进程。启用 EIGRP 之，请参阅以下各节了解如何在系统中自定义 EIGRP 进程。

启用 EIGRP

仅能在 ASA 中启用一个 EIGRP 路由进程。

要启用 EIGRP，请执行以下步骤

步骤 1 在 ASDM 主窗口中，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 选项卡可供您为每个情景启用 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，请参阅第 24-4 页的启用 EIGRP 和第 24-5 页的启用 EIGRP 末节路由。
- Networks 选项卡可供您指定 EIGRP 路由进程所用的网络。对于参与 EIGRP 路由的接口，它必须在网络条目定义的地址范围内。对于要通告的直接连接和静态网络，它们也必须位于网络条目的范围内。有关详细信息，请参阅第 24-6 页的为 EIGRP 路由进程定义网络。
- Passive Interfaces 选项卡可供您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 表列出已配置为被动接口的每个接口。

步骤 2 选中 **Enable this EIGRP process** 复选框。

仅能在设备上启用一个 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)，之后才能保存更改。

步骤 3 在 EIGRP Process 字段中，为 EIGRP 进程输入自治系统 (AS) 编号。 AS 编号可以在 1 至 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、默认度量、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 要新增网络条目，请点击 **Add**。

系统将显示 Add EIGRP Network 对话框。要移除网络条目，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 要更改某个网络条目，必须首先移除该条目，然后新增条目。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式路由器。一般而言，除了发送末节路由器的默认路由，分布式路由器不需要发送任何其他信息。

仅指定的路由从末节路由器传播到分布式路由器。作为末节路由器，ASA 以 “ 不可达 ” 消息响应对摘要、已连接路由、重新分发的静态路由、外部路由和内部路由的所有查询。当 ASA 配置为末节时，它会发送特殊对等信息数据包到所有邻居路由器，报告其作为末节路由器的状态。收到通知其末节状态之数据包的任何邻居都将不会查询末节路由器是否存在任何路由，且具有末节对等体的路由器也将不查询该对等体。末节路由器依赖于分布式路由器发送正确的更新到所有对等体。

要启用 ASA 作为 EIGRP 末节路由进程，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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 编号可以在 1 至 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 的 Stub 区域中，选择以下一个或多个 EIGRP 末节路由进程：

- 仅末节接收 - 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之一。
- 连接的末节 - 通告连接的路由。
- 末节静态 - 通告静态路由。
- 重新分发的末节 - 通告重新分发的路由。
- 末节摘要 - 通告摘要路由。

步骤 6　点击 **OK**。

步骤 7　点击 **Networks** 选项卡。

步骤 8　点击 **Add** 以新增网络条目。

系统将显示 Add EIGRP Network 对话框。要移除网络条目，请选择表中的某个条目并点击 **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　要更改某个网络条目，必须首先移除该条目，然后新增条目。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

本节说明如何自定义 EIGRP 路由。

为 EIGRP 路由进程定义网络

网络表可供您指定 EIGRP 路由进程所用的网络。对于参与 EIGRP 路由的接口，它必须在网络条目定义的地址范围内。对于要通告的直接连接和静态网络，它们也必须位于网络条目的范围内。

网络表显示为 EIGRP 路由进程配置的网络。表的每一行显示为指定的 EIGRP 路由进程配置的网络地址和关联的掩码。

要添加或定义网络，请执行以下步骤：

步骤 1 在 ASDM 主窗口中，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 编号可以在 1 至 65535 之间。

步骤 4 点击 **Networks** 选项卡。

步骤 5 点击 **Add** 以新增网络条目。

系统将显示 Add EIGRP Network 对话框。要移除网络条目，请选择表中的某个条目并点击 **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 要更改某个网络条目，必须首先移除该条目，然后新增条目。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**。

配置 EIGRP 的接口

如果不希望接口参与 EIGRP 路由，但是该接口连接到希望通告的网络，则可以配置包括接口所连接网络的 ASA ，并使用阻止接口发送或接收 EIGRP 更新。

要配置 EIGRP 的接口，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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　选择 **Configuration > Device Setup > Routing > EIGRP > Interfaces**。

此时，Interface 窗格出现，其中显示了 EIGRP 接口配置。Interface Parameters 表显示 ASA 中的所有接口，可供您逐一为每个接口修改以下设置：

- 身份验证密钥和模式。
- EIGRP Hello 时间间隔和保持时间。
- 用于 EIGRP 最度计算的接口时延度量。
- 接口上水平分割的使用情况。

步骤 5　双击接口条目以选定它，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 编号可以在 1 至 65535 之间。

步骤 7　在 Hello Interval 字段中，输入 EIGRP Hello 数据包在接口上发送的时间间隔。

有效值范围为 1 至 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。有效值范围为 1 至 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。延迟时间为数十微秒。有效值范围为 1 至 16777215。

步骤 11　选中 **Enable MD5 Authentication** 复选框，为 EIGRP 进程消息启用 MD5 身份验证。

步骤 12　输入密钥或密钥 ID 值。

- 在 Key 字段中，输入密钥以对 EIGRP 更新进行身份验证。密钥最多可以包含 16 个字符。
- 在 Key ID 字段中，输入密钥标识值。有效值范围为 1 至 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。

要配置被动接口，请执行以下步骤：

注　在 ASDM 中， Passive Interface 表列出已配置为被动接口的每个接口。

步骤 1 在 ASDM 主窗口中，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 从下拉列表中选择想要配置的接口。

步骤 6 选中 **Suppress routing updates on all interfaces** 复选框以将所有接口均指定为被动接口。即使接口未显示在 Passive Interface 表中，当选中该复选框后，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。选择想要设置为被动的接口并点击 **Add**。要移除被动接口，请选择表中的某个接口并点击 **Delete**。

步骤 8 点击 **OK**。

在接口上配置摘要汇聚地址

可逐一为每个接口上配置摘要地址。如果要创建不发生在网络号边界上的摘要地址，或者想要在自动路由摘要禁用的情况下在 ASA 上使用摘要地址，则需要手动定义摘要地址。如果路由表中有更具体的路由，则 EIGRP 将用相当于所有更上体路由最小值的度量将摘要地址通告出接口。

要创建摘要地址，请执行以下操作：

步骤 1 在 ASDM 主窗口中，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 上的所有接口，可供您逐一为每个接口修改设置。有关这些设置的详细信息，请参阅第 24-7 页的配置 EIGRP 的接口。

步骤 2 要配置接口的 EIGRP 参数，请双击某个接口条目或选择一个条目并点击 **Edit**。

步骤 3 点击 **OK**。

步骤 4 选择 **Configuration > Device Setup > Routing > EIGRP > Summary Address**。

Summary Address 窗格将显示静态定义的 EIGRP 摘要地址表。默认情况下， EIGRP 将子网路由摘要至网络级别。可以从 Summary Address 窗格创建摘要至子网级别的静态定义的 EIGRP 摘要地址。

步骤 5 点击 **Add** 以新增 EIGRP 摘要地址，或者点击 **Edit** 以编辑表中现有 EIGRP 摘要地址。

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 编号可以在 1 至 65535 之间。

步骤 7 在 Interface 下拉列表中，选择要从其中通告摘要地址的接口。

步骤 8 在 IP Address 字段中，输入摘要路由的 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，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。可以逐一为每个接口修改此值。

要更改接口延迟值，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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 上的所有接口，可供您逐一为每个接口修改设置。有关这些设置的详细信息，请参阅第 24-7 页的配置 EIGRP 的接口。

步骤 2　双击某个接口条目或者选择某个接口条目并点击 **Edit**，以配置接口的 EIGRP 参数的延迟值。

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，为数十微秒。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 路由身份验证提供来自 EIGRP 路由协议的路由更新 MD5 身份验证。每个 EIGRP 数据包中的 MD5 密钥摘要可防止从未批准的来源引入未经授权或虚假的路由消息。

将逐一为每个接口配置 EIGRP 路由身份验证。必须使用相同的身份验证模式和密钥配置接口上为 EIGRP 消息身份验证配置的所有 EIGRP 邻居，才能建立邻接关系。

注　必须先启用 EIGRP 路由身份验证，然后才能启用 EIGRP。

要在接口上启用 EIGRP 身份验证，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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 编号可以在 1 至 65535 之间。

步骤 4　点击 **Networks** 选项卡。

步骤 5　点击 **Add** 以新增网络条目。

系统将显示 Add EIGRP Network 对话框。要移除网络条目，请选择表中的某个条目并点击 **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，输入参与 EIGRP 路由进程的网络的 IP 地址。

注　要更改某个网络条目，必须首先移除该条目，然后新增条目。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 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 上的所有接口，可供您逐一为每个接口修改设置。有关这些设置的详细信息，请参阅第 24-7 页的配置 EIGRP 的接口。

步骤 11 选中 **Enable MD5 Authentication** 复选框，为 EIGRP 进程消息启用 MD5 身份验证。选中此复选框后，请提供下列其中一项：

- 在 Key 字段中，输入密钥以对 EIGRP 更新进行身份验证。密钥最多可以包含 16 个字符。
- 在 Key ID 字段中，输入密钥标识值。有效值范围为 1 至 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 邻居位于非广播网络内，如隧道，则必须手动定义该邻居。当手动定义 EIGRP 邻居时， Hello 数据包作为单播消息发送至该邻居。

要手动定义 EIGRP 邻居，请执行以下步骤：

步骤 1 在 ASDM 主窗口中，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 编号可以在 1 至 65535 之间。

步骤 4 选择 **Configuration > Device Setup > Routing > EIGRP > Static Neighbor**。

此时， Static Neighbor 窗格出现，其中显示静态定义的 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，邻居通过邻居发现过程被动态发现。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 地址以及邻居借以可用的接口。

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，邻居通过该接口变得可用。

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

可以将 RIP 和 OSPF 发现的路由重新分发到 EIGRP 路由进程中。您还可以将静态路由和已连接路由重新分发到 EIGRP 路由进程中。如果已连接路由位于 EIGRP 配置中**网络**语句范围内，则不需要进行重新分发它们。

注　仅适用于 RIP：开始此操作步骤之前，必须创建路由映射，以进一步定义将指定路由协议中哪些路由重新分发到 RIP 路由进程。有关创建路由映射的详细信息，请参阅第 21 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：

步骤 1　在 ASDM 主窗口中，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 编号可以在 1 至 65535 之间。

步骤 4　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，不需要配置度量，但建议这样做。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** 以新增重新分发规则。如果正在编辑现有的重新分发规则，请转至第 6 步。

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** 以编辑现有的 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，点击路由进程的以下协议之一旁边的单选按钮：

- **Static**，可将静态路由重新分发到 EIGRP 路由进程。位于网络语句范围内的静态路由将自动重新分发到 EIGRP ； 不需要为其定义重新分发规则。
- **Connected**，可将已连接的路由重新分发到 EIGRP 路由进程。属于网络语句范围内的已连接路由将自动重新分发到 EIGRP ； 不需要为其定义重新分发规则。
- **RIP**，可将由 RIP 路由进程发现的路由重新分发到 EIGRP。
- **OSPF**，可将由 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度量之一：

- **Bandwidth**， EIGRP 带宽度量，单位为千位每秒。有效值范围为 1 至 4294967295。
- **Delay**， EIGRP 时延度量，单位为 10 微秒。有效值范围为 0 至 4294967295。
- **Reliability**， EIGRP 可靠性度量。有效值范围为 0 至 255 ； 255 表示百分百的可靠性。
- **Loading**， EIGRP 有效带宽 （正在加载）度量。有效值范围为 1 至 255 ； 255 表示已加载百分百。
- **MTU**，路径的 MTU。有效值范围为 1 至 65535。

步骤 10　从 Route Map 下拉列表中选择路由映射，以定义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 21 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，以进一步指定哪些 OSPF 路由重新分发到 EIGRP 路由进程：

- **Match Internal**，匹配已指定 OSPF 进程内部的路由。
- **Match External 1**，匹配已指定 OSPF 进程外部的 1 类路由。
- **Match External 2**，匹配已指定 OSPF 进程外部的 2 类路由。
- **Match NSSA-External 1**，匹配已指定 OSPF NSSA 外部的 1 类路由。
- **Match NSSA-External 2**，匹配已指定 OSPF NSSA 外部的 2 类路由。

步骤 12　点击 **OK**。

在 EIGRP 中过滤网络

注　开始此过程之前，必须创建标准 ACL，以定义要通告的路由。也就是说，创建标准 ACL，以定义要从发送或接收更新中过滤的路由。

要在 EIGRP 中过滤网络，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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 编号可以在 1 至 65535 之间。

步骤 4　选择 **Configuration > Device Setup > Routing > EIGRP > Filter Rules**。

此时， Filter Rule 窗格出现，其中显示为 EIGRP 路由进程配置的路由过滤规则。过滤规则可供您控制 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可将过滤应用于外部接口上收到的所有 EIGRP 更新。传出方向且 OSPF 10 指定为路由协议的过滤规则可将过滤规则应用到重新分发到出站 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。如果正在编辑已存在的过滤规则，请跳至第 6 步。

系统将显示 Add Filter Rules 对话框。

步骤 6　要编辑过滤规则，请在表中选定它并点击 **Edit**。

系统将显示 Edit Filter Rules 对话框。也可双击过滤规则以编辑它。要移除过滤规则，请在表中选定它并点击 **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。

对于过滤源自传入 EIGRP 路由更新的路由的规则，选择 **in**。选择 **out** 可过滤源自 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源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将应用到的接口。

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 以允许通告指定的网络；选择 Deny 以阻止通告指定的网络。

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，请使用子网掩码为 **0.0.0.0** 的 IP 地址 **0.0.0.0** 与网络掩码。

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 Hello 时间间隔和保持时间

ASA 定期发送 Hello 数据包，用于发现邻居以及获悉邻居何时变得不可达或不起作用。默认情况下，每 5 秒发送一次 Hello 数据包。

Hello 数据包通告 ASA 保持时间。保持时间向 EIGRP 邻居指示应将邻居视为 ASA 可达的时间长度。如果邻居在通告的保持时间内未收到 Hello 数据包，则 ASA 将被视为不可达。默认情况下，通告的保持时间是 15 秒 （Hello 时间间隔的三倍）。

Hello 时间间隔和通告的保持时间均按每个接口逐一进行配置。我们建议将保持时间设置为至少相当于 Hello 时间间隔的三倍。

要配置 Hello 时间间隔和通告的保持时间，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，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　选择 **Configuration > Device Setup > Routing > EIGRP > Interfaces**。

此时， Interface 窗格显示，其中显示了所有 EIGRP 接口配置。

步骤 5　双击接口条目，或选择该接口条目并单击 **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，该编号从启用 EIGRP 路由进程时设置的系统编号填充。

步骤 7　在 Hello Interval 字段中，输入 EIGRP Hello 数据包在接口上发送的时间间隔。

有效值范围为 1 至 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。

有效值范围为 1 至 65535 秒。默认值为 15 秒。

步骤 9　点击 **OK**。

禁用自动路由摘要

默认情况下已启用自动路由摘要。 EIGRP 路由进程在网络号边界摘要。如果存在非邻接网络，这可能引起路由问题。

例如，如果路由器同时连接到 192.168.1.0、 192.168.2.0 和 192.168.3.0 网络，且这些网络全部参与 EIGRP，则 EIGRP 路由进程会为这些路由创建摘要地址 192.168.0.0。如果另一个路由器添加到网络 192.168.10.0 和 192.168.11.0，且这些网络均参与 EIGRP，则它们也会摘要为 192.168.0.0。为防止流量路由到错误位置的可能性，应在创建冲突性摘要地址的路由器上禁用自动路由摘要。

要在 ASDM 中禁用自动路由摘要，请执行以下步骤：

步骤 1 在 ASDM 主窗口中，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 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。如将 ASA 配置为禁止接收默认信息，则将导致候选默认路由位在收到的路由中被拦截。如将 ASA 配置为禁止发送默认信息，则可禁用通告路由中默认路由位的设置。

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，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 执行以下任一操作：

- 点击 **Add** 以新建一个条目。
- 要编辑条目，请在表中双击它，或在表中选定并点击 **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** - 规则过虑源自传入 EIGRP 更新的默认路由信息。
- **out** - 规则过滤源自传出 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。网络规则可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。为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

水平分割控制 EIGRP 更新和查询数据包的发送。在接口上启用水平分割时，不会为此接口是下一跳的目标发送更新和查询数据包。以这种方式控制更新和查询数据包可减少路由环路的可能性。

默认情况下，水平分割在所有接口上均已启用。

水平分割可阻止路由器通告的路由信息从产生该信息的所有接口传出。此行为通常可优化多个路由设备之间的通信，尤其是在链路中断时。但是，使用非广播网络时，可能存在此行为不令人意的的情况。对于这些情况，包括配置了 EIGRP 的网络，可能需要禁用水平分割。

如果在某一接口上禁用水平分割，则必须也为该接口上所有路由器和接入服务器禁用水平分割。

要禁用 EIGRP 水平分割，请执行以下步骤：

步骤 1　在 ASDM 主窗口中，选择 **Configuration > Device Setup > Routing > EIGRP > Interfaces**。

此时， Interface 窗格出现，其中显示了 EIGRP 接口配置。

步骤 2　双击接口条目，或选择该接口条目并单击 **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，该编号从启用 EIGRP 路由进程时设置的系统编号填充。

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

要重新启动 EIGRP 进程或清除重新分发或计数器，请执行以下步骤：

步骤 1 在 ASDM 主窗口中，选择 **Configuration > Device Setup > Routing > EIGRP > Setup**。

系统将显示 EIGRP Setup 窗格。

步骤 2 点击 **Reset**。

监控 EIGRP

可以使用以下命令监控 EIGRP 路由进程。有关命令输出的示例和说明，请参阅命令参考。此外，您可以禁用邻居变更消息和邻居警告消息的日志记录。

要监控或禁用多个 EIGRP 路由统计信息，请执行以下步骤：

步骤 1 在 ASDM 主窗口中，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、邻居所连接的接口、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。可能的状态变化列表如下：

- NEW ADJACENCY - 新邻居已建立。
- PEER RESTARTED - 另一个邻居发起邻居关系重置。接收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变化， EIGRP 邻居正在重置。
- INTERFACE DELAY CHANGED - 由于接口上延迟参数发生手动配置变化， EIGRP 邻居正在重置。
- INTERFACE BANDWIDTH CHANGED - 由于接口上接口带宽发生手动配置变化， EIGRP 邻居正在重置。
- STUCK IN ACTIVE - 由于 EIGRP 陷入活动状态， EIGRP 邻居正在重置。陷入活动状态导致邻居发生重置。

步骤 2 点击想要监控的 EIGRP 邻居。

步骤 3 要移除当前邻居列表，请点击 **Clear Neighbors**。

步骤 4 要刷新当前邻居列表，请点击 **Refresh**。

注 默认情况下，邻居更改消息和邻居警告消息均已记录。

EIGRP 的功能历史记录

表 24-1 列出了各种功能变更以及实施该等功能变更的平台版本。ASDM 向后兼容多个平台版本，因此，未列出已添加支持的特定 ASDM 版本。

表 24-1 EIGRP 的功能历史记录

功能名称	平台版本	功能信息
EIGRP 支持	7.0(1)	增加了使用增强型内部网关路由协议 (EIGRP) 对路由数据、执行身份验证和重新分发及监控路由信息的支持。 我们引入了以下屏幕：Configuration > Device Setup > Routing > EIGRP。
多情景模式中的动态路由	9.0(1)	EIGRP 路由在多情景模式中受支持。 我们修改了以下屏幕：Configuration > Device Setup > Routing > EIGRP > Setup。
集群	9.0(1)	对于 EIGRP，在集群环境中支持批量同步、路由同步和第 2 层负载均衡。
EIGRP 自动摘要	9.2(1)	默认情况下， Auto-Summary 字段现已禁用。 我们修改了以下屏幕：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。

有关组播路由的信息

组播路由是一种带宽节省技术，通过同时向数千个公司收件人和家庭传送单一信息流来减少流量。使用组播路由的应用包括视频会议、公司通信、远程教育以及软件、股票报价和新闻的分发。

组播路由协议将源流量传送给多个接收者，而不会对源或接收者造成任何额外负担，而且是同类技术当中占用网络带宽最少的。组播数据包通过启用了协议无关组播 (PIM) 及其他支持性组播协议的思科路由器在网络中复制，是目前为止向多个接收者传输数据的最高效方式。

ASA 支持末节组播路由和 PIM 组播路由。但是，不能在一个 ASA 上都配置这两种路由。

注 UDP 和非 UDP 传输均支持组播路由。但是，非 UDP 传输没有进行快速路径优化。

末节组播路由

末节组播路由提供动态主机注册并促进组播路由。如果针对末节组播路由进行了配置， ASA 将用作 IGMP 受托代理。ASA 将 IGMP 消息转发到上游组播路由器（上游组播路由器设置组播数据的传输），而不是完全参加组播路由。如果 ASA 针对末节组播路由进行了配置，则不能针对 PIM 进行配置。

ASA 支持 PIM-SM 和双向 PIM。PIM-SM 是一个组播路由协议，它使用基础单播路由信息库或支持组播的独立路由信息库。它为每个组播组构建以单一交汇点为根的单向共享树，或者为每个组播源创建最短路径树。

PIM 组播路由

双向 PIM 是 PIM-SM 的一种变体，用于构建连接组播源和接收者的双向共享树。双向树使用在每个组播拓扑链路上运行的 DF 选择进程来构建。在 DF 的帮助下，组播数据从源转发到交汇点，再从那里沿着共享树发送到接收者，而无需源特定状态。 DF 选择在交汇点发现过程中发生，并向交汇点提供默认路由。

注　如果 ASA 是 PIM 交汇点，请将 ASA 的逆向转换外部地址用作交汇点地址。

组播组概念

组播基于组概念。任意一组接收者对接收特定数据流表现出兴趣。这样的组没有任何物理边界或地理边界 - 主机可位于互联网上的任何位置。有兴趣接收流向特定组的数据的主机必须使用 IGMP 加入该组。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，请参阅第 25-12 页的配置组播组。

组播地址

组播地址指定已加入某个组的任意一组 IP 主机，并希望接收发送到该组的流量。

集群

组播路由支持集群。在第 2 层集群中，在快速路径转发建立之前，主设备会发送所有的组播数据包和数据包。在建立快速路径转发后，从设备可能会转发组播数据包。所有数据流都是全流量。同时还支持末节转发流。由于第 2 层集群中仅有一台设备接收组播数据包，因此，常常会重定向到主设备。在第 3 层集群中，设备不会独立工作。所有的数据和路由数据包均由主设备处理和转发。从设备会丢弃已发送的所有数据包。

有关集群的更多信息，请参阅第 9 章， “ASA 集群 ”。

组播路由的许可要求

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

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景模式中受支持。在多情景模式中，非共享接口和共享接口不受支持。

防火墙模式准则

仅在路由防火墙模式中受支持。透明防火墙模式不受支持。

IPv6 准则

不支持 IPv6。

附加准则

在集群中，对于 IGMP 和 PIM，此功能仅在主设备上受支持。

启用组播路由

通过启用组播路由，可以在 ASA 上启用组播路由。默认情况下，启用组播路由可以在所有接口上启用 IGMP 和 PIM。 IGMP 用于了解直连子网上是否存在组成员。主机通过发送 IGMP 报告消息加入组播组。 PIM 用于维护转发表，以转发组播数据报。

注　组播路由仅支持 UDP 传输层。

要启用组播路由，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，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。可以逐个接口禁用组播。

表 25-1 根据 ASA 的 RAM 容量列出了特定组播表的最大条目数。一旦达到这些限制，将会放弃所有新条目。

表 25-1　　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

注　末节组播路由和 PIM 不能同时受支持。

用作末节区域网关的 ASA 不需要加入到 PIM。相反，可以将该 ASA 配置为 IGMP 受托代理，并使其会从连接到一个接口的主机将 IGMP 消息转发到另一个接口上的上游组播路由器。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

要转发有关主机加入和离开的消息，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，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** 以保存更改。

步骤 4　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将组播流量与单播流量分隔开。例如，如果源和目标之间的路由不支持组播路由，可以通过如下方法来解决这个问题：使用 GRE 隧道在它们之间配置两个组播设备，并通过该隧道发送组播数据包。

使用 PIM 时， ASA 期望用于接收数据包的接口和用于将单播数据包发送回到源的接口是同一个接口。在某些情况下 （例如，绕过不支持组播路由的路由），您可能希望单播数据包和组播数据包使用不同的路径。

静态组播路由不能通告或重分布。

要配置静态组播路由或末节区域的静态组播路由，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，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，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　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) 将其组成员报告给直连组播路由器。

IGMP 用于在特定 LAN 上的一个组播组中动态注册单个主机。主机通过向其本地组播路由器发送 IGMP 消息来识别组成员。在 IGMP 下，路由器监听 IGMP 消息，并定期发出查询以发现特定子网上哪些组处于活动状态还是非活动状态。

IGMP 将组地址 （D 类 IP 地址）用作组标识符。主机组地址的范围可以是 224.0.0.0 到 239.255.255.255。地址 224.0.0.0 不分配给任何组。地址 224.0.0.1 分配给子网上的所有系统。地址 224.0.0.2 分配给子网上的所有路由器。

如果在 ASA 上启用组播路由， IGMP V2 将会在所有接口上自动启用。

注　使用 **show run** 命令时，接口配置中只会显示 **no igmp** 命令。如果设备配置中显示 **multicast-routing** 命令，则 IGMP 会在所有接口上自动启用。

本节介绍如何逐个接口配置可选的 IGMP 设置。

- 第 25-6 页的禁用接口上的 IGMP
- 第 25-6 页的配置 IGMP 组成员
- 第 25-7 页的配置静态加入的 IGMP 组
- 第 25-7 页的控制对组播组的访问

- 第 25-8 页的限制接口上的 IGMP 状态数量
- 第 25-8 页的修改发送到组播组的查询消息
- 第 25-9 页的更改 IGMP 版本

禁用接口上的 IGMP

可以禁用特定接口上的 IGMP。如果知道特定接口上没有组播接口，并且想要防止 ASA 通过该接口发送主机查询消息，则此信息很有用。

要禁用接口上的 IGMP，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，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

可以将 ASA 配置为组播组的成员。配置 ASA 加入组播组会使上游路由器维护该组的组播路由表信息，并保持该组的路径处于活动状态。

注　如果要将特定组的组播数据包转发给接口，且无需 ASA 将这些数据包接受为该组的一部分，请参阅第 25-7 页的配置静态加入的 IGMP 组。

要使 ASA 加入组播组，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，选择 **Configuration > Device Setup > Routing > Multicast > IGMP > Join Group**。

系统将显示 Join Group 窗格。

步骤 2　点击 **Add** 或 **Edit**。

可以在 Add IGMP Join Group 对话框中将接口配置为组播组的成员。可以在 Edit IGMP Join Group 对话框中更改现有的成员信息。

步骤 3　在 Interface Name 字段中，从下拉列表中选择接口名称。如果在编辑现有条目，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。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，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，但该接口不是组播组的成员。

要在接口上配置静态加入的组播组，请执行以下操作步骤：

步骤 1　在主 ASDM 窗口中，选择 **Configuration > Device Setup > Routing > Multicast > IGMP > Static Group**。

系统将显示 Static Group 窗格。

步骤 2　点击 **Add** 或 **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。如果在编辑现有条目，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

要控制 ASA 上的主机可加入的组播组，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，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实施，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。使用 Add Access Group 对话框可以向 Access Group Table 中添加新的访问组。使用 Edit Access Group 对话框可以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相关的接口名称。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，以从选定接口过滤组播组。

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

可以对每个接口限制 IGMP 成员报告造成的 IGMP 状态数量。超出所配置限制的成员报告不会输入到 IGMP 缓存中，多余成员报告的流量不会转发。

要限制接口上的 IGMP 状态数量，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，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，输入可加入接口的最大主机数量。有效值范围为 0 到 500。默认值是 500。将此值设置为 0 可防止获悉的组被添加，但仍允许手动定义成员。

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 上存储的成员信息。如果 ASA 发现组播组中没有本地成员仍与接口相连接，它会停止向连接的网络转发该组的组播数据包，并会向数据包源发送回删除消息。

默认情况下，子网上的 PIM 指定路由器负责发送查询消息。默认情况下，每 125 秒发送一次消息。

默认情况下，更改查询响应时间时， IGMP 查询中通告的最大查询响应时间为 10 秒。如果 ASA 不在此时间内接收对于主机查询的响应，它就会删除该组。

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：

步骤 1　在主 ASDM 窗口中，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 主机查询消息的间隔时间 （以秒为单位）。有效值范围为 1 到 3600 秒。默认值是 125 秒。

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）。有效值范围为 60 到 300 秒。默认值是 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。

要控制哪个版本的 IGMP 在接口上运行，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，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。

注　PAT 不支持 PIM。 PIM 协议不使用端口， PAT 只能与使用端口的协议配合使用。

本节介绍如何配置可选的 PIM 设置。

- 第 25-9 页的在接口上启用和禁用 PIM
- 第 25-10 页的配置静态交汇点地址
- 第 25-11 页的配置指定路由器优先级
- 第 25-11 页的配置和过滤 PIM 注册消息
- 第 25-12 页的配置 PIM 消息间隔时间
- 第 25-12 页的配置路由树
- 第 25-13 页的过滤 PIM 邻居

在接口上启用和禁用 PIM

可以在特定接口上启用或禁用 PIM。要在接口上启用或禁用 PIM，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，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。

注　ASA 不支持 Auto-RP 或 PIM BSR

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：

注　ASA 始终会在 PIM hello 消息中通告双向功能，无论实际的双向配置如何。

步骤 1　在主 ASDM 窗口中，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 或 Edit Rendezvous Point 对话框。使用 Add Rendezvous Point 对话框可以向 Rendezvous Point 表添加新条目。使用 Edit Rendezvous Point 对话框可以更改现有的 RP 条目。此外，还可以点击 **Delete** 以从表中移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。
- 不能为多于一个 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中运行，请选中 **Use bi-directional forwarding** 复选框。如果指定的组播组要在双向模式中运行， Rendezvous Point 窗格将显示 Yes ；如果指定的组播组要在稀疏模式中运行，该窗格将显示 No。在双向模式中，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，请参阅第 25-12 页的配置组播组。

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：

步骤 1　在主 ASDM 窗口中，选择 **Configuration > Device Setup > Routing > Multicast > PIM > Protocol**。

步骤 2　在 Protocol 窗格的表中选择要为 PIM 启用的接口，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**。

配置和过滤 PIM 注册消息

当 ASA 作为 RP 时，您可以禁止特定的组播源注册到 ASA，从而防止未授权的源注册到 RP。Request Filter 窗格可用于定义 ASA 将会接受 PIM 注册消息的组播源。

要过滤 PIM 注册消息，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，选择 **Configuration > Device Setup > Routing > Multicast > PIM > Request Filter**。

步骤 2　点击 **Add**。

可以在 Request Filter Entry 对话框中定义当 ASA 用作 RP 时可注册到 ASA 的组播源。可根据源 IP 地址和目标组播地址创建过滤规则。

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 消息间隔时间

路由器查询消息用于选择 PIM DR。 PIM DR 负责发送路由器查询消息。默认情况下，每隔 30 秒发送一次路由器查询消息。此外， ASA 每隔 60 秒发送一次 PIM 加入消息或删除消息。

要更改这些间隔时间，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，选择 **Configuration > Device Setup > Routing > Multicast > PIM > Protocol**。

步骤 2　在 Protocol 窗格的表中选择要为 PIM 启用的接口，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，输入接口发送 PIM hello 消息的频率 （以秒为单位）。

步骤 4　在 Prune Interval 字段中，输入接口发送 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 叶子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。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 叶子路由器树，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，选择 **Configuration > Device Setup > Routing > Multicast > PIM > Route Tree**。

步骤 2　点击以下任一单选按钮：

- **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。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，请参阅第 25-12 页的配置组播组。

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，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 或 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 以创建过滤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**。

过滤 PIM 邻居

可以定义可成为 PIM 邻居的路由器。通过过滤可成为 PIM 邻居的路由器，可以实现以下目的：

- 防止未授权的路由器成为 PIM 邻居。
- 防止连接的末节路由器加入到 PIM。

要定义可成为 PIM 邻居的邻居，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，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。 Add/Edit/Insert Neighbor Filter Entry 对话框可用于为组播边界 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，除非使用邻居过滤条目允许通过。

步骤 5　在 IP Address 文本字段中，输入要允许或拒绝的组播 PIM 组的 IP 地址。有效的组地址范围是 224.0.0.0 到 239.255.255.255.255。

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（如果有）。 PIM 双向邻居过滤器是定义可参与 DF 选择的邻居设备的 ACL。如果接口未配置 PIM 双向邻居过滤器，则没有限制。如果配置了 PIM 双向邻居过滤器，则只有 ACL 允许的邻居可参加 DF 选择进程。

如果 PIM 双向邻居过滤器配置应用于 ASA，名称为 *interface-name*_multicast 的运行配置中会显示 ACL，其中， *interface-name* 是应用组播边界过滤器的接口的名称。如果已存在使用该名称的 ACL，将会给名称加上一个数字（例如，inside_multicast_1）。此 ACL 定义哪些设备可成为 ASA 的 PIM 邻居。

双向 PIM 使组播路由器可以保留减少的状态信息。要选择 DF，必须为 bidir 双向启用分段中的所有组播路由器。

PIM 双向邻居过滤器允许指定应参与 DF 选择的路由器，同时仍允许所有路由器加入到稀疏模式域，从而实现从纯稀疏模式网络到 bidir 网络的过渡。支持 bidir 的路由器可以从它们本身当中选择 DF，即使分段上有非 bidir 路由器。非 bidir 路由器上的组播边界可防止 bidir 组中的 PIM 消息和数据泄漏到 bidir 子集云中或从 bidir 子集云泄漏出去。

如果启用了 PIM 双向邻居过滤器， ACL 允许的路由器将被视为具有双向功能。因此，以下说法均是正确的：

- 如果一个获允许的邻居不支持 bidir，将不会发生 DF 选择。
- 如果一个被拒绝的邻居支持 bidir，将不会发生 DF 选择。
- 如果一个被拒绝的邻居不支持 bidir，可能会发生 DF 选择。

要定义可成为 PIM 双向邻居过滤器的邻居，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，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，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 选择进程。选择 Deny 可阻止指定设备参与 DF 选择进程。

步骤 6　在 IP Address 文本字段中，输入要允许或拒绝的组播 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 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

地址范围定义域边界，从而使具有 IP 地址相同的 RP 的域不会相互泄漏。可在大型域内的子网边界以及域与互联网之间的边界上执行范围界定。

可以通过以下做法在接口上为组播组地址设置使用管理权限界定的边界：在 ASDM 中选择 **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权限界定的地址。此地址范围可在不同组织管理的域中重用。此类地址被视为本地地址，而不是全局唯一地址。

标准 ACL 定义受影响地址的范围。设置边界后，不允许组播数据包从任一方向流经边界。边界允许同一个组播组地址在不同的管理域中重用。

可以在使用管理权限界定的边界配置、检查和过滤 Auto-RP 发现消息和通知消息。 Auto-RP 数据包中被边界 ACL 拒绝的任意 Auto-RP 组范围通知都会被移除。仅在 Auto-RP 组范围中的所有地址获边界 ACL 允许的情况下， Auto-RP 组范围通知才可以通过边界。如果有任何地址未获允许，在 Auto-RP 消息被转发前，将会过滤整个组范围并将其从 Auto-RP 消息中移除。

要配置组播边界，请执行以下步骤：

步骤 1　在主 ASDM 窗口中，选择 **Configuration > Routing > Multicast > MBoundary**。

MBoundary 窗格可用于配置使用管理权限界定的组播地址的组播边界。组播边界限制组播数据包流量，并允许在不同的管理域中重用同一个组播组地址。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。可以使用此对话框添加和移除过滤器 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 拒绝的源中过滤 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**。

组播路由的配置示例

以下示例显示如何使用各个可选过程启用和配置组播路由：

步骤 1　在主 ASDM 窗口中，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，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，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　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，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**。

可以在 Add IGMP Join Group 对话框中将接口配置为组播组的成员。可以在 Edit IGMP Join Group 对话框中更改现有的成员信息。

步骤 12　在 Interface Name 字段中，从下拉列表中选择接口名称。如果在编辑现有条目，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**。

附加参考资料

有关路由的其他信息，请参阅以下各节：

- 第 25-16 页的相关文档
- 第 25-17 页的 RFC

相关文档

相关主题	文档标题
用于实施 SMR 功能的 IGMP 和组播路由标准的技术详细信息	IETF draft-ietf-idmr-igmp-proxy-01.txt

RFC

RFC	标题
RFC 2113	IP 路由器告警选项
RFC 2236	IGMPv2
RFC 2362	PIM-SM
RFC 2588	IP 组播和防火墙

组播路由的功能历史记录

表 25-2 列出了各种功能变更以及实施该等功能变更的平台版本。 ASDM 可向后兼容多个平台版本，因此，未列出已添加支持的具体 ASDM 版本。

表 25-2　组播路由的功能历史记录

功能名称	平台版本	功能信息
组播路由支持	7.0(1)	增加了对于组播路由数据、身份验证以及使用组播路由协议重发布和监控路由信息的支持。 引入了以下屏幕：Configuration > Device Setup > Routing > Multicast。
集群支持	9.0(1)	增加了集群支持。

第 26 章

IPv6 邻居发现

有关 IPv6 邻居发现的信息

IPv6 邻居发现过程使用 ICMPv6 消息和请求节点组播地址，确定同一网络 （本地链路）中邻居的链路层地址、验证邻居的可读性及跟踪相邻路由器。

节点 （主机）使用邻居发现确定已知驻留在连接的链路上邻居的链路层地址并快速清除变为无效的缓存值。主机还使用邻居发现查找愿意代表自己转发数据包的邻居路由器。此外，节点使用协议主动跟踪哪些邻居可到达及哪些邻居不可达，并检测已更改的链路层地址。当路由器或路由器的路径发生故障时，主机会主动搜索起作用的替代项。

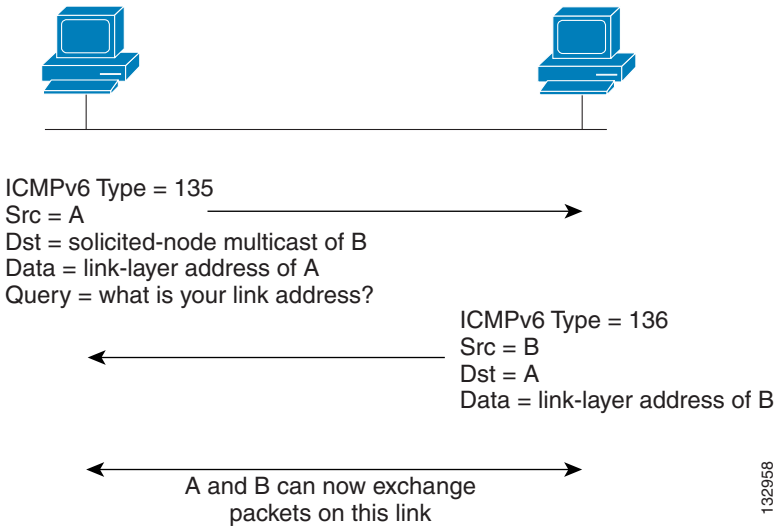
邻居请求消息

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 26-1 显示邻居请求和响应流程。

图 26-1　　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达性。当节点要验证邻居的可达性时，邻居请求消息中的目标地址是邻居的单播地址。

本地链路中一个节点的链路层地址发生变化时，也会发送邻居通告消息。当发生此类变化时，邻居通告的目标地址是所有节点组播地址。

邻居可到达时间

邻居可到达时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快，但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。

重复地址检测

在无状态自动配置过程中，重复地址检测可在新的单播 IPv6 地址被分配给接口之前验证该地址的唯一性 （执行重复地址检测时，新地址保持暂定状态）。重复地址检测首先在新的链路本地地址上执行。当链路本地地址经过验证为唯一时，重复地址检测在接口上所有其他 IPv6 单播地址上执行。

重复地址检测在处于管理性关闭状态的接口上暂停。当接口处于管理性关闭状态时，单播 IPv6 地址将分配给设置为处于挂起状态的接口。恢复管理性打开状态的接口将重新启动对接口上所有单播 IPv6 地址的重复地址检测。

识别出重复地址后，该地址的状态会设置为 DUPLICATE，且不会使用该地址并生成以下错误消息：

```
%ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface
```

如果重复地址是接口的链接本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。但是，地址的状态设置为 DUPLICATE 时，与重复地址关联的所有配置命令均持为已配置。

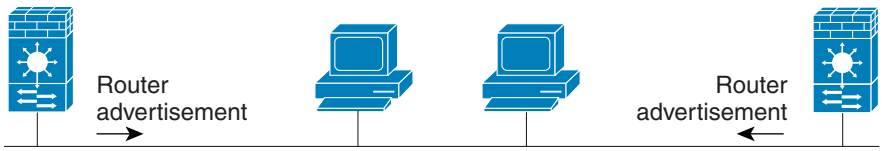
如果接口的链路本地地址发生变化，则会将新的链路本地地址执行重复地址检测，并将重新生成与接口关联的所有其他 IPv6 地址 （重复地址检测仅在新的链路本地地址上执行）。

ASA 使用邻居请求消息执行重复地址检测。默认情况下，接口执行重复地址检测的次数为 1。

路由器通告消息

思科 ASA 可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。路由器通告消息（ICMPv6 类型 134）定期被发送出 ASA 的每个 IPv6 配置接口。路由器通告消息发送到所有节点组播地址。图 26-2 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 26-2　　IPv6 邻居发现 - 路由器通告消息



Router advertisement packet definitions:
ICMPv6 Type = 134
Src = router link-local address
Dst = all-nodes multicast address
Data = options, prefix, lifetime, autoconfig flag

132917

路由器通告消息通常包括以下信息：

- 可供本地链路上节点用于自动配置其 IPv6 地址的一个或多个 IPv6 前缀。
- 通告中包括的每个前缀的有效期信息。
- 标志集，指示可以完成的自动配置的类型 （无状态或有状态）。
- 默认路由器信息 （发送通告的路由器是否应作为默认路由器，以及如果是，路由器应用作默认路由器的持续时间 [秒]）。
- 主机的其他信息，如主机在其发送的数据包中应使用的跳数限制和 MTU。
- 给定链路上邻居请求消息重新传输之间的时间。
- 节点将邻居视为可到达的时间。

也会发送路由器通告，以响应路由器请求消息 （ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。由于路由器请求消息通常由主机在系统启动时发送，而主机没有配置的单播地址，因此，路由器请求消息的源地址通常是未指定的 IPv6 地址 (0:0:0:0:0:0:0:0)。如果主机有一个配置的单播地址，则发送路由器请求消息的接口的单播地址将用作消息的源地址。路由器请求消息的目标地址是链路范围内所有路由器组播地址。当发送路由器通告以响应路由器请求时，路由器通告消息的目标地址是路由器请求消息的源的单播地址。

可以为路由器通告消息配置以下设置：

- 定期路由器通告消息之间的时间间隔。
- 路由器有效期值，指示 IPv6 节点应将 ASA 视为默认路由器的时间。
- 链路中使用的 IPv6 网络前缀。
- 接口是否传输路由器通告消息。

除非另有说明，否则路由器通告消息设置特定于接口并在接口配置模式中输入。

静态 IPv6 邻居

可以在 IPv6 邻居缓存中手动定义一个邻居。如果指定 IPv6 地址的条目在邻居发现缓存中已存在（已通过 IPv6 邻居发现过程获悉），则该条目会自动转换为静态条目。邻居发现过程不会修改 IPv6 邻居发现缓存中的静态条目。

IPv6 邻居发现的许可要求

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

IPv6 邻居发现的先决条件

请根据第 12-12 页的配置 IPv6 寻址配置 IPv6 地址。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

仅在路由模式中受支持。透明模式不受支持。

附加准则和限制

- 时间间隔值包括在发送出该接口的所有 IPv6 路由器通告中。
- 配置的时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快，但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。
- 如果使用 **ipv6 nd ra-lifetime** 命令将 ASA 配置为默认路由器，则传输之间的时间间隔应小于或等于 IPv6 路由器通告的有效期。为防止与其他 IPv6 节点的同步，请将所用的实际值随机调整为指定值的 20% 以内。
- **ipv6 nd prefix** 命令可按前缀控制各个参数，包括是否应该通告前缀。
- 默认情况下，接口上使用 **ipv6 addres** 命令配置为地址的前缀在路由器通告中通告。如果使用 **ipv6 nd prefix** 命令为通告配置前缀，则仅通告这些前缀。
- **default** 关键字可用于为所有前缀设置默认参数。
- 可以设置日期来指定前缀的过期日期。实时倒计时有效有效期和首选有效期。到达过期日期后，将不再会通告前缀。
- 在链路上打开 （默认情况下）时，指定的前缀会分配给该链路。向包含指定前缀的此类地址发送流量的节点会将目标视为在链路上本地可到达。
- 当自动配置启用 （默认情况下）时，它向本地链路上的主机指示可将指定前缀用于 IPv6 自动配置。
- 为使无状态自动配置正常运行，路由器通告消息中通告的前缀长度必须始终为 64 位。
- 路由器有效期值包括在发送出接口的所有 IPv6 路由器通告中。值表示作为该接口上默认路由器的 ASA 用途。
- 将值设置为非零值表示应将 ASA 视为该接口的默认路由器。路由器有效期值的非零值不能小于路由器通告间隔时间。

以下准则和限制适用于配置静态 IPv6 邻居：

- **ipv6 neighbor** 命令类似于 **arp** 命令。如果指定 IPv6 地址的条目在邻居发现缓存中已存在（已通过 IPv6 邻居发现过程获悉），则该条目会自动转换为静态条目。当使用复制命令存储配置时，这些条目存储在配置中。
- 使用 **show ipv6 neighbor** 命令可查看 IPv6 邻居发现缓存中的静态条目。
- **clear ipv6 neighbor** 命令可删除 IPv6 邻居发现缓存中除静态条目之外的所有条目。 **no ipv6 neighbor** 命令可从邻居发现缓存中删除指定的静态条目；该命令不会从缓存中移除动态条目，这些条目从 IPv6 邻居发现过程中获悉。使用 **no ipv6 enabl** 命令在接口上禁用 IPv6 可删除为该接口配置的所有 IPv6 邻居发现缓存条目，静态条目 （条目的状态更改为 INCMP [Incomplete]）之外。
- 邻居发现过程不会修改 IPv6 邻居发现缓存中的静态条目。
- **clear ipv6 neighbor** 命令不会从 IPv6 邻居发现缓存中移除静态条目；仅会清除动态条目。
- IPv6 邻居条目的定期刷新生成了 ICMP 系统日志。 IPv6 邻居条目的 ASA 默认计时器为 30 秒，因此，ASA 将大约每 30 秒生成 ICMPv6 邻居发现和响应数据包。如果 ASA 拥有用 IPv6 地址配置的故障转移 LAN 和状态接口，则 ASA 将每 30 秒为配置的和链路本地的 IPv6 地址生成 ICMPv6 邻居发现和响应数据包。此外，由于每个数据包将生成多个系统日志 （ICMP 连接和本地主机创建或拆卸），因此，似乎一直在不断生成 ICMP 系统日志。可以在常规数据接口上配置 IPv6 邻居条目的刷新时间，但是，不可在故障转移接口上配置。但是，此 ICMP 邻居发现流量对 CPU 的影响最小。

IPv6 邻居发现的默认设置

表 26-1 列出 IPv6 邻居发现的默认设置。

表 26-1 默认的 IPv6 邻居发现参数

参数	默认值
value for the neighbor solicitation transmission message interval	邻居请求传输之间为 1000 秒。
value for the neighbor reachable time	默认值为 0。
value for the router advertisement transmission interval	默认值为 200 秒。
value for the router lifetime	默认值为 1800 秒。
value for the number of consecutive neighbor solicitation messages sent during DAD	默认值为一条消息。
prefix lifetime	默认有效期为 2592000 秒 （30 天），首选有效期为 604800 秒 （7 天）。
on-link flag	该标志已默认打开，表示前缀用于通告接口上。
autoconfig flag	该标志已默认打开，表示前缀用于自动配置。
static IPv6 neighbor	静态条目不在 IPv6 邻居发现缓存中配置。

配置 IPv6 邻居发现

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。

详细步骤

步骤 1　选择 **Configuration > Device Setup > 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。有关详细信息，请参阅第 12-12 页的配置 IPv6 寻址。

步骤 3　点击 **Edit**。系统将显示 Edit Interface 对话框，其中包括三个选项卡：General、 Advanced 和 IPv6。

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。

配置邻居可到达时间

要配置可访问性确认事件发生后远程 IPv6 节点被视为可到达的时间，请执行以下步骤。

详细步骤

步骤 1　选择 **Configuration > Device Setup > 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，请参阅第 12-12 页的配置 IPv6 寻址。

步骤 3　点击 **Edit**。系统将显示 Edit Interface 对话框，其中包括三个选项卡：General、 Advanced 和 IPv6。

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。

详细步骤

步骤 1　选择 **Configuration > Device Setup > 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，请参阅第 12-12 页的配置 IPv6 寻址。

步骤 3　点击 **Edit**。系统将显示 Edit Interface 对话框，其中包括三个选项卡：General、 Advanced 和 IPv6。

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　（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 至 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。

详细步骤

步骤 1　选择 **Configuration > Device Setup > 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，请参阅第 12-12 页的配置 IPv6 寻址。

步骤 3　点击 **Edit**。

系统将显示 Edit Interface 对话框，其中包括三个选项卡：General、 Advanced 和 IPv6。

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。

详细步骤

步骤 1　选择 **Configuration > Device Setup > 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，请参阅第 12-12 页的配置 IPv6 寻址。

步骤 3　点击 **Edit**。

系统将显示 Edit Interface 对话框，其中包括三个选项卡：General、 Advanced 和 IPv6。

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。在不想要 ASA 提供 IPv6 前缀的所有接口（例如，外部接口）上，您可能想要禁用这些消息。

要在接口上抑制 IPv6 路由器通告中路由器有效期值，请执行以下步骤。

详细步骤

步骤 1　选择 **Configuration > Device Setup > Interfaces**。

步骤 2　选择想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，其中包括三个选项卡：General、 Advanced 和 IPv6。

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

可以向 IPv6 路由器通告添加标志，以通知 IPv6 自动配置客户端使用 DHCPv6 来获取 IPv6 地址和 / 或其他信息，如 DNS 服务器地址。

详细步骤

步骤 1　选择 **Configuration > Device Setup > 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，其中包括三个选项卡：General、 Advanced 和 IPv6。

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受管地址配置标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 来获取相关地址以及派生的无状态自动配置地址。

选中 **Hosts should use DHCP for non-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

要配置哪些 IPv6 前缀包括在 IPv6 路由器通告中，请执行以下步骤。

详细步骤

步骤 1　选择 **Configuration > Device Setup > Interfaces**。

步骤 2　选择想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，其中包括三个选项卡：General、 Advanced 和 IPv6。

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到达。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，并指定以下各项：

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。有效值范围为 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 前缀作为首选前缀通告的时间。最大值代表无穷大。有效值范围为 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的月份和日期，然后以 hh:mm 格式输入时间。

步骤 12　点击 **OK** 以保存设置。

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，请参阅第 12-12 页的配置 IPv6 寻址。

要添加 IPv6 静态邻居，请执行以下步骤。

详细步骤

步骤 1　选择 **Configuration > Device Management > Advanced > IPv6 Neighbor Discovery Cache**。

步骤 2　点击 **Add**。

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　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。

查看及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移除。

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　选择 **Monitoring > Interfaces > IPv6 Neighbor Discovery Cache**。

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移除。

注　此操作步骤仅从缓存清除动态发现的邻居；将不清除静态邻居。

附加参考资料

有关实施 IPv6 前缀的其他信息，请参阅以下主题：

- 第 26-12 页的 IPv6 前缀的相关文档
- 第 26-12 页的 IPv6 前缀的 RFC 和文档

IPv6 前缀的相关文档

相关主题	文档标题
ipv6 命令	*命令参考*

IPv6 前缀的 RFC 和文档

RFC	标题
RFC 2373 包含完整文档，显示如何在路由器通告中必须显示 IPv6 网络地址编号。命令参数 *ipv6-prefix* 指示此网络号，其中地址必须以十六进制格式指定，冒号之间使用 16 位值。	IPv6 寻址架构
RFC 3849 指定在文档中使用 IPv6 地址前缀的要求。预留用于文档中的 IPv6 单播地址前缀为 2001:DB8::/32。	预留给文档的 IPv6 地址前缀

IPv6 邻居发现的功能历史记录

表 26-2 列出了各种功能变更以及实施该等功能变更的平台版本。ASDM 向后兼容多个平台版本，因此，未列出已添加支持的特定 ASDM 版本。

表 26-2　　IPv6 邻居发现的功能历史记录

功能名称	版本	功能信息
IPv6 邻居发现	7.0(1)	我们引入了此功能。 我们引入了以下屏幕： Monitoring > Interfaces > IPv6 Neighbor Discovery Cache。 Configuration > Device Management > Advanced > IPv6 Neighbor Discovery Cache。 Configuration > Device Setup > Interfaces > IPv6。
IPv6 DHCP 中继的地址配置标志	9.0(1)	我们修改了以下屏幕：Configuration > Device Device Setup > Interfaces > IPv6。

第 7 部分

AAA 服务器和本地数据库

关于 AAA 的信息

本章介绍身份验证、授权和记帐（AAA，也称为“3A”）。AAA 是一组服务，用于控制对计算机资源的访问、强制实施策略、评估使用情况并提供对服务进行计费所需的信息。这些过程对于高效进行网络管理和安全性而言至关重要。

身份验证

身份验证提供了一种标识用户的方法，这种方法通常先请用户输入有效用户名和有效密码，然后再授予访问权限。AAA 服务器将用户的身份验证凭证与数据库中存储的其他用户凭证进行比较。如果凭证匹配，则允许用户访问网络。如果凭证不匹配，则身份验证失败，并拒绝网络访问。

您可以配置思科 ASA，以便对下列各项进行身份验证：

- 所有与 ASA 建立的管理连接，包括下列会话：
  - Telnet
  - SSH
  - 串行控制台
  - 使用 HTTPS 的 ASDM
  - VPN 管理访问
- **enable** 命令
- 网络访问
- VPN 访问

授权

授权是强制实施策略的过程：确定允许用户访问哪些类型的活动、资源或服务。对用户进行身份验证后，可能会授权该用户执行各种类型的访问或活动。

您可以配置 ASA 以便对下列各项进行授权：

- 管理命令
- 网络访问
- VPN 访问

记帐

记帐用于测量用户在访问期间使用的资源量，这可以包括系统时间长度或者用户在会话期间发送或接收的数据量。记帐是通过记录会话统计信息和使用量信息来执行的，这些信息用于进行授权控制、计费、趋势分析、资源利用和容量规划活动。

身份验证、授权和记帐之间的交互

您可以单独使用身份验证功能，也可以将其与授权和记帐功能配合使用。授权始终要求先对用户进行身份验证。您可以单独使用记帐功能，也可以将其与身份验证和授权功能配合使用。

AAA 服务器

AAA 服务器是用于进行访问控制的网络服务器。身份验证用于标识用户。授权实现策略，这些策略确定经过身份验证的用户能够访问哪些资源和服务。记帐对时间和数据资源进行追踪，这些资源用于计费和分析。

AAA 服务器组

如果要使用外部 AAA 服务器进行身份验证、授权或记帐，您必须先为每种 AAA 协议创建至少一个 AAA 服务器组，并向每个组添加一个或多个服务器。您通过名称来标识 AAA 服务器组。每个服务器组都专门用于一种类型的服务器或服务。

本地数据库支持

ASA 维护一个本地数据库，您可以将用户配置文件填入其中。您可以使用本地数据库代替 AAA 服务器来提供用户身份验证、授权和记帐。

用于 AAA 的本地数据库

本章介绍如何配置用于 AAA 的本地服务器。

关于本地数据库

您可以使用本地数据库实现下列功能：

- ASDM 每用户访问
- 控制台身份验证
- Telnet 和 SSH 身份验证
- **enable** 命令身份验证

  此设置仅适用于 CLI 访问，而不会影响思科 ASDM 登录。
- 命令授权

  如果您使用本地数据库开启命令授权，思科 ASA 将根据用户的权限级别来确定可用的命令。否则，通常不使用权限级别。默认情况下，所有命令的权限级别均为 0 或 15。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，您可以在系统执行空间中配置用户名，以便在 CLI 中使用 **login** 命令提供个人登录；但是，您不能在系统执行空间中配置任何使用本地数据库的 AAA 规则。

注 您不能使用本地数据库进行网络访问授权。

回退支持

本地数据库可以充当多项功能的回退方法。此行为旨在帮助您避免意外被锁定而无法登录 ASA。

用户登录时，将从配置中指定的第一个服务器开始逐个访问组中的服务器，直到有服务器作出响应为止。如果组中的所有服务器都不可用，并且您已将本地数据库配置为回退方法（仅用于管理身份验证和授权），则 ASA 将尝试使用本地数据库。如果未配置任何回退方法，则 ASA 将继续尝试使用 AAA 服务器。

对于需要回退支持的用户，我们建议您确保本地数据库中的用户名和密码与 AAA 服务器上的用户名和密码匹配。这种做法将提供透明的回退支持。由于用户无法确定是 AAA 服务器还是本地数据库正在提供服务，因此，如果 AAA 服务器上使用的用户名和密码与本地数据库中的用户名和密码不同，用户将无法确定应该提供哪个用户名和密码。

本地数据库支持下列回退功能：

- 控制台和启用密码身份验证 - 如果组中的服务器全部不可用，则 ASA 将使用本地数据库对管理访问进行身份验证，这还可以包括启用密码身份验证。
- 命令授权 - 如果组中的 TACACS+ 服务器全部不可用，则使用本地数据库根据权限级别进行命令授权。
- VPN 身份验证和授权 - 支持 VPN 身份验证和授权，以便在通常支持这些 VPN 服务的 AAA 服务器不可用时，启用对 ASA 的远程访问。如果管理员的 VPN 客户端指定了配置为回退到本地数据库的隧道组，只要本地数据库配置了必要的属性，即使 AAA 服务器组不可用，也可以建立 VPN 隧道。

组中存在多个服务器时的回退方式

如果在服务器组中配置了多个服务器，并且对于该服务器组允许回退到本地数据库，则该组中没有任何服务器对来自 ASA 的身份验证请求作出响应时，将会进行回退。为了说明这一点，请考虑以下场景：

您配置了一个 LDAP 服务器组，其中依次包含两个 Active Directory 服务器，即服务器 1 和服务器 2。当远程用户登录时， ASA 将尝试向服务器 1 进行身份验证。

如果服务器 1 作出了身份验证失败响应（例如*找不到用户*），则 ASA 不会尝试向服务器 2 进行身份验证。

如果服务器 1 在超时期限内未作出响应 （或者尝试进行身份验证的次数超过配置的最大值），则 ASA 尝试服务器 2。

如果该组中的两个服务器均未作出响应，并且 ASA 配置为回退到本地数据库，则 ASA 将尝试向本地数据库进行身份验证。

本地数据库准则

在使用本地数据库进行身份验证或授权时，请确保避免被锁定而无法登录 ASA。

相关主题

第 36-25 页的从锁定中恢复

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　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　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，等等。

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　在 **Member of** 字段中输入组名以指定该用户所属的 VPN 组，然后点击 **Add**。

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，以启用管理授权。

选择以下选项之一：

- **Full Access (ASDM, Telnet, SSH and console)** - 如果您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** - 为该用户选择的要用于本地命令授权的权限级别。范围为 0 （最低）到 15 （最高）。
- **CLI login prompt for SSH, Telnet and console (no ASDM access)** - 如果您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。如果还启用了身份验证，则用户无法访问全局配置模式。
- **No ASDM, SSH, Telnet, or console access** - 如果您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。您可以使用任何能够生成 SSH-RSA 原始密钥 （不含证书）的 SSH 密钥生成软件 （例如 ssh keygen）来生成密钥。您查看现有密钥时，该密钥将使用 SHA-256 哈希算法进行加密。如果需要复制并粘贴经过哈希处理的密钥，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** 以删除身份验证密钥，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）。对于由于过长而无法以 Base64 格式粘贴的密钥，请使用此格式。例如，您可以使用 ssh keygen 生成一个 4096 位的密钥，然后将其转换为 PKF 格式，并在此窗格中导入。当您查看现有密钥时，该密钥将使用 SHA-256 哈希算法进行加密。如果需要复制并粘贴经过哈希处理的密钥，请从 **Public Key Athentication** 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** 以删除身份验证密钥，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**。

此用户将添加到本地数据库中，并且更改将保存到运行配置中。

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。

以下示例在 Linux 或 Macintosh 系统上生成用于 SSH 的共享密钥，并将其导入到 ASA 中：

步骤 1　在计算机上生成 4096 位的 ssh-rsa 公钥和私钥：

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)?y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + .E         |
|  o o            |
| ooooo           |
+-----------------+
```

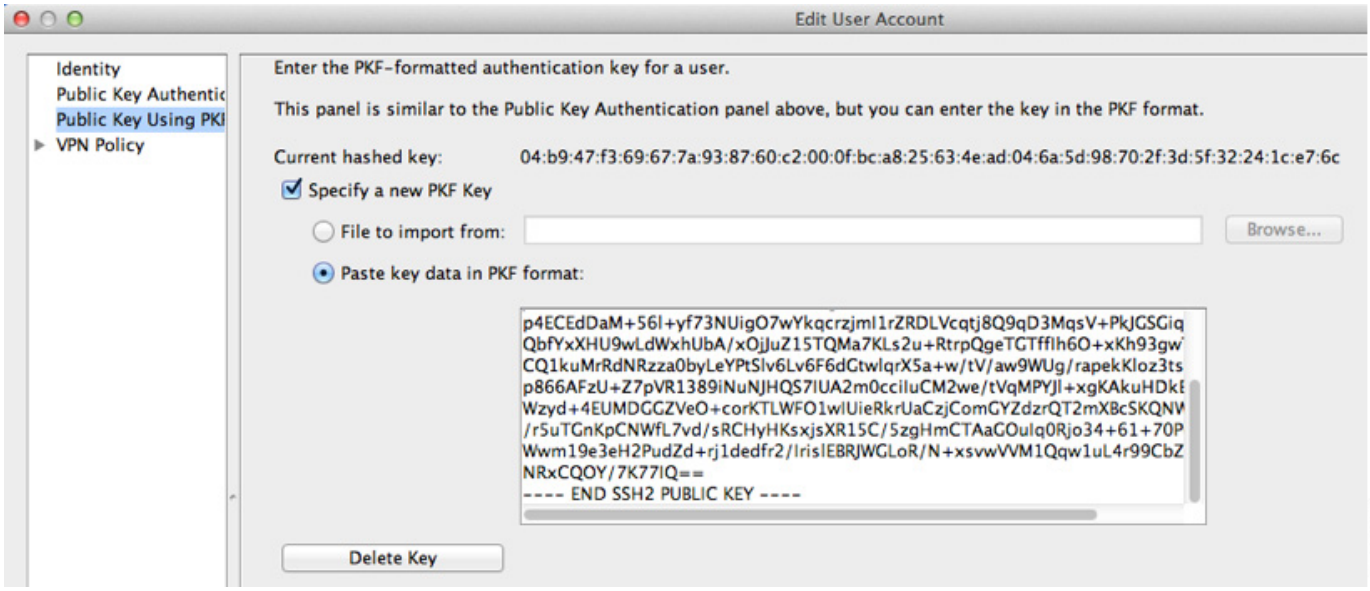
步骤 2　将该密钥转换为 PKF 格式：

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment:"4096-bit RSA, converted by ramona@rboersma-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
```

```
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

步骤 3　将该密钥复制到剪贴板。

步骤 4　在 ASDM 中，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** 并将该密钥粘贴到窗口中：



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　点击您想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

请查看下列屏幕以监控本地数据库：

- **Monitoring > Properties > AAA Servers**

  此窗格显示 AAA 服务器统计信息。

本地数据库的历史

表 28-1　　本地数据库的历史

功能名称	平台版本	功能信息
AAA 的本地数据库配置	7.0(1)	讨论如何配置本地数据库以供 AAA 使用。 我们引入了以下屏幕： Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > User Accounts。
对 SSH 公钥身份验证的支持	9.1(2)	现在，对于与 ASA 的 SSH 连接，您可以按每个用户启用公钥身份验证。您可以指定公钥文件 (PKF) 格式的密钥或 Base64 密钥。PKF 密钥的长度可达 4096 位。对于由于过长而导致 ASA 不支持使用 Base64 格式（限长 2048 位）的密钥，请使用 PKF 格式。 我们引入了以下屏幕： 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。*

AAA RADIUS 服务器

本章介绍如何配置 AAA RADIUS 服务器。

有关 RADIUS 服务器

思科 ASA 支持以下兼容 RFC 的 AAA RADIUS 服务器：

- 思科安全 ACS 3.2、 4.0、 4.1、 4.2 和 5.x
- 思科身份服务引擎 (ISE)
- RSA 身份验证管理器 5.2、 6.1 和 7.x 中的 RSA RADIUS
- Microsoft

支持的身份验证方法

ASA 使用 RADIUS 服务器支持以下身份验证方法：

- PAP - 适用于所有连接类型。
- CHAP 和 MS-CHAPv1 - 适用于 L2TP-over-IPsec 连接。
- MS-CHAPv2 - 适用于 L2TP-over-IPsec 连接和常规 IPsec 远程访问连接（当密码管理功能被启用时）。您也可以通过无客户端连接使用 MS-CHAPv2。
- 身份验证代理模式 - 适用于 RADIUS-to Active-Directory、 RADIUS-to-RSA/SDI、RADIUS-to-Token 服务器和 RSA/SDI-to-RADIUS 连接。

注 为了将 MS-CHAPv2 启用为 ASA 与 RADIUS 服务器之间使用的协议以实现 VPN 连接，您必须在隧道组常规属性里启用密码管理。启用密码管理将生成一个从 ASA 到 RADIUS 服务器的 MS-CHAPv2 身份验证请求。有关详细信息，请参阅 **password-management** 命令说明。

如果在隧道组中使用双重身份验证并启用密码管理，则主要身份验证请求和辅助身份验证请求包含 MS-CHAPv2 请求属性。如果 RADIUS 服务器不支持 MS-CHAPv2，您可以使用 **no mschapv2-capable** 命令，将该服务器配置为发送非 MS CHAPv2 的身份验证请求。

VPN 连接的用户身份验证

ASA 可以使用 RADIUS 服务器进行 VPN 远程访问和防火墙直接转发代理会话的用户验证 （按用户使用动态 ACL 或 ACL 名称）。要实施动态 ACL，您必须将 RADIUS 服务器配置为支持动态 ACL。在用户进行身份验证时，RADIUS 服务器向 ASA 发送可下载的 ACL 或 ACL 名称。ACL 允许或拒绝对指定服务的访问。当身份验证会话超时的时候， ASA 将删除 ACL。

除了 ACL， ASA 还支持许多其他的授权属性和 VPN 远程访问以及防火墙直接转发代理会话的权限设置。

支持的 RADIUS 属性集

ASA 支持以下 RADIUS 属性集：

- RFC 2138 定义的身份验证属性。
- RFC 2139 定义的记账属性。
- RFC 2868 定义的用于隧道协议支持的 RADIUS 属性。
- RADIUS 供应商 ID 9 确定的思科 IOS 供应商特定属性 (VSA)。
- RADIUS 供应商 ID 3076 确定的思科 VPN 相关 VSA。
- RFC 2548 定义的 Microsoft VSA。
- Cisco VSA (Cisco-Priv-Level) 提供 0 至 15 级标准数字权限等级，最低等级 1，最高等级 15。等级 0 表示没有权限。等级 1 （登录）对该等级可用的命令允许执行特权执行模式。等级 2 （启用）允许 CLI 配置权限。

支持的 RADIUS 授权属性

授权指的是实施权限或属性的进程。如果已配置权限或属性，被定义为身份验证服务器的 RADIUS 服务器可以实施权限或属性。这些属性具有供应商 ID 3076。

表 29-1 列出了受支持的 RADIUS 属性，这些属性可用于用户授权。

注 RADIUS 属性名称不包含 cVPN3000 前缀。思科安全 ACS 4.x 支持这一新的命名法，但是， ACS 4.0 之前版本中的属性名仍然包含 cVPN3000 前缀。 ASA 基于属性数字 ID 而非属性名来实施 RADIUS 属性。

表 29-1 列出的所有属性都是从 RADIUS 服务器发送到 ASA 的下行属性，以下编号的属性除外：146、150、151 和 152。这些编号的属性是从 ASA 发送到 RADIUS 服务器的上行属性。RADIUS 属性 146 和 150 是从 ASA 发送到 RADIUS 服务器用于身份验证和授权请求的属性。以上所列的四个属性都是从 ASA 发送到 RADIUS 服务器用于记账开始请求、临时更新请求和停止请求的属性。 8.4(3) 版本引入了上行 RADIUS 属性 146、 150、 151 和 152。

在版本 9.0(1) 中，对于使用 RADIUS 身份验证进行的 IP 地址分配，思科 ACS 5.x 和思科 ISE 不支持 IPv6 框架 IP 地址。

表 29-1　支持的 RADIUS 授权属性

属性名	ASA	属性编号	语法 / 类型	单值或多值	说明或值
Access-Hours	有	1	字符串	单值	时间范围名称，例如工作时间
Access-List-Inbound	有	86	字符串	单值	ACL ID
Access-List-Outbound	有	87	字符串	单值	ACL ID
Address-Pools	有	217	字符串	单值	IP 本地地址池名称
Allow-Network-Extension-Mode	有	64	布尔值	单值	0 = 禁用 1 = 启用
Authenticated-User-Idle-Timeout	有	50	整数	单值	1 - 35791394 分钟
Authorization-DN-Field	有	67	字符串	单值	可能值：UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、 use-entire-name
Authorization-Required		66	整数	单值	0 = 否 1 = 是
Authorization-Type	有	65	整数	单值	0 = 无 1 = RADIUS 2 = LDAP
Banner1	有	15	字符串	单值	为思科 VPN 远程访问会话显示的横幅字符串：IPsec IKEv1、 AnyConnect SSL TLS/DTLS/IKEv2 和 Clientless SSL。
Banner2	有	36	字符串	单值	为思科 VPN 远程访问会话显示的横幅字符串：IPsec IKEv1、 AnyConnect SSL-TLS/DTLS/IKEv2 和 Clientless SSL。如果进行了相应的配置， Banner2 字符串将被与 Banner1 字符串联系在一起。

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名	ASA	属性编号	语法 / 类型	单值或多值	说明或值
Cisco-IP-Phone-Bypass	有	51	整数	单值	0 = 禁用 1 = 启用
Cisco-LEAP-Bypass	有	75	整数	单值	0 = 禁用 1 = 启用
Client Type	有	150	整数	单值	1 = Cisco VPN 客户端 (IKEv1) 2 = AnyConnect 客户端 SSL VPN 3 = 无客户端 SSL VPN 4 = 直接转发代理 5 = L2TP/IPsec SSL VPN 6 = AnyConnect 客户端 IPsec VPN (IKEv2)
Client-Type-Version-Limiting	有	77	字符串	单值	IPsec VPN 版本号字符串
DHCP-Network-Scope	有	61	字符串	单值	IP 地址
Extended-Authentication-On-Rekey	有	122	整数	单值	0 = 禁用 1 = 启用
Group-Policy	有	25	字符串	单值	为远程访问 VPN 会话设置组策略。对于 8.2.x 版本和更高版本，使用该属性而非 IETF-Radius-Class。您可以使用以下任一格式： • *组策略名称* • OU = *组策略名称* • OU = *组策略名称*;
IE-Proxy-Bypass-Local		83	整数	单值	0 = 无 1 = 本地
IE-Proxy-Exception-List		82	字符串	单值	新行 (\n) 分隔 DNS 域列表
IE-Proxy-PAC-URL	有	133	字符串	单值	PAC 地址字符串
IE-Proxy-Server		80	字符串	单值	IP 地址
IE-Proxy-Server-Policy		81	整数	单值	1 = 不修改 2 = 不使用代理服务器 3 = 自动检测 4 = 使用集中器设置
IKE-KeepAlive-Confidence-Interval	有	68	整数	单值	10 - 300 秒
IKE-Keepalive-Retry-Interval	有	84	整数	单值	2 - 10 秒
IKE-Keep-Alives	有	41	布尔值	单值	0 = 禁用 1 = 启用
Intercept-DHCP-Configure-Msg	有	62	布尔值	单值	0 = 禁用 1 = 启用
IPsec-Allow-Passwd-Store	有	16	布尔值	单值	0 = 禁用 1 = 启用

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名	ASA	属性编号	语法 / 类型	单值或多值	说明或值
IPsec-Authentication		13	整数	单值	0 = 无 1 = RADIUS 2 = LDAP （仅限授权） 3 = NT 域 4 = SDI 5 = 内部 6 = 支持有效期的 RADIUS 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	有	42	布尔值	单值	0 = 禁用 1 = 启用
IPsec-Backup-Server-List	有	60	字符串	单值	服务器地址 （空格分隔）
IPsec-Backup-Servers	有	59	字符串	单值	1 = 使用客户端配置的列表 2 = 禁用并清除客户端列表 3 = 使用备份服务器列表
IPsec-Client-Firewall-Filter-Name		57	字符串	单值	指定要被推入客户端 （作为防火墙策略）的过滤器的名称
IPsec-Client-Firewall-Filter-Optional	有	58	整数	单值	0 = 要求 1 = 可选
IPsec-Default-Domain	有	28	字符串	单值	指定要发送到客户端的单个默认域名 （1 - 255 个字符）。
IPsec-IKE-Peer-ID-Check	有	40	整数	单值	1 = 要求 2 = 对等证书是否支持 3 = 不检测
IPsec-IP-Compression	有	39	整数	单值	0 = 禁用 1 = 启用
IPsec-Mode-Config	有	31	布尔值	单值	0 = 禁用 1 = 启用
IPsec-Over-UDP	有	34	布尔值	单值	0 = 禁用 1 = 启用
IPsec-Over-UDP-Port	有	35	整数	单值	4001 - 49151 默认值为 10000。
IPsec-Required-Client-Firewall-Capability	有	56	整数	单值	0 = 无 1 = 远程防火墙 Are-You-There (AYT) 定义的策略 2 = 策略推送的 CPP 4 = 来自服务器的策略
IPsec-Sec-Association		12	字符串	单值	安全关联的名称
IPsec-Split-DNS-Names	有	29	字符串	单值	指定要发送到客户端的辅助域名列表 （1 - 255 个字符）。
IPsec-Split-Tunneling-Policy	有	55	整数	单值	0 = 无分割隧道 1 = 分割隧道 2 = 获准的本地 LAN

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名	ASA	属性编号	语法 / 类型	单值或多值	说明或值
IPsec-Split-Tunnel-List	有	27	字符串	单值	指定描述隧道包含列表的网络或 ACL 名称。
IPsec-Tunnel-Type	有	30	整数	单值	1 = LAN 对 LAN 2 = 远程访问
IPsec-User-Group-Lock		33	布尔值	单值	0 = 禁用 1 = 启用
IPv6-Address-Pools	有	218	字符串	单值	IP 本地地址池 IPv6 的名称
IPv6-VPN-Filter	有	219	字符串	单值	ACL 值
L2TP-Encryption		21	整数	单值	位图： 1 = 要求加密 2 = 40 位 4 = 128 位 8 = 要求无状态 15= 40/128 要求加密 / 无状态
L2TP-MPPC-Compression		38	整数	单值	0 = 禁用 1 = 启用
Member-Of	有	145	字符串	单值	逗号分隔的字符串，例如： `Engineering, Sales` 可在动态访问策略里使用的管理属性。不设置组策略。
MS-Client-Subnet-Mask	有	63	布尔值	单值	IP 地址
NAC-Default-ACL		92	字符串		ACL
NAC-Enable		89	整数	单值	0 = 否 1 = 是
NAC-Revalidation-Timer		91	整数	单值	300 - 86400 秒
NAC-Settings	有	141	字符串	单值	NAC 策略名称
NAC-Status-Query-Timer		90	整数	单值	30 - 1800 秒
Perfect-Forward-Secrecy-Enable	有	88	布尔值	单值	0 = 否 1 = 是
PPTP-Encryption		20	整数	单值	位图： 1 = 要求加密 2 = 40 位 4 = 128 位 8 = 要求无状态 15= 40/128 要求加密 / 无状态
PPTP-MPPC-Compression		37	整数	单值	0 = 禁用 1 = 启用
Primary-DNS	有	5	字符串	单值	IP 地址
Primary-WINS	有	7	字符串	单值	IP 地址
Privilege-Level	有	220	整数	单值	介于 0 和 15 之间的整数。

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名	ASA	属性编号	语法 / 类型	单值或多值	说明或值
Required-Client- Firewall-Vendor-Code	有	45	整数	单值	1 = 思科系统 （带思科集成客户端） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = 思科系统 （带思科入侵防御安全代理）
Required-Client-Firewall-Description	有	47	字符串	单值	字符串
Required-Client-Firewall-Product-Code	有	46	整数	单值	思科系统产品： 1 = 思科入侵防御安全代理或思科集成客户端 (CIC) Zone Labs 产品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 产品： 1 = BlackIce Defender/ 代理 Sygate 产品： 1 = 个人防火墙 2 = 个人防火墙专业版 3 = 安全代理
Required-Individual-User-Auth	有	49	整数	单值	0 = 禁用 1 = 启用
Require-HW-Client-Auth	有	48	布尔值	单值	0 = 禁用 1 = 启用
Secondary-DNS	有	6	字符串	单值	IP 地址
Secondary-WINS	有	8	字符串	单值	IP 地址
SEP-Card-Assignment		9	整数	单值	未使用
Session Subtype	有	152	整数	单值	0 = 无 1 = 无客户端 2 = 客户端 3 = 仅客户端 会话子类型仅限于 Session Type (151) 属性为以下值时：1、 2、 3 和 4。
Session Type	有	151	整数	单值	0 = 无 1 = AnyConnect 客户端 SSL VPN 2 = AnyConnect 客户端 IPSec VPN (IKEv2) 3 = 无客户端 SSL VPN 4 = 无客户端邮件代理 5 = Cisco VPN 客户端 (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN 负载均衡
Simultaneous-Logins	有	2	整数	单值	0 - 2147483647

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名	ASA	属性编号	语法 / 类型	单值或多值	说明或值
Smart-Tunnel	有	136	字符串	单值	智能隧道的名称
Smart-Tunnel-Auto	有	138	整数	单值	0 = 禁用 1 = 启用 2 = 自动启动
Smart-Tunnel-Auto-Signon-Enable	有	139	字符串	单值	域名附加的智能隧道自动登录列表名称
Strip-Realm	有	135	布尔值	单值	0 = 禁用 1 = 启用
SVC-Ask	有	131	字符串	单值	0 = 禁用 1 = 启用 3 = 启用默认服务 5 = 启用默认无客户端 （未使用 2 和 4）
SVC-Ask-Timeout	有	132	整数	单值	5 - 120 秒
SVC-DPD-Interval-Client	有	108	整数	单值	0 = 关闭 5 - 3600 秒
SVC-DPD-Interval-Gateway	有	109	整数	单值	0 = 关闭 5 - 3600 秒
SVC-DTLS	有	123	整数	单值	0 = 假 1 = 真
SVC-Keepalive	有	107	整数	单值	0 = 关闭 15 - 600 秒
SVC-Modules	有	127	字符串	单值	字符串 （模块名）
SVC-MTU	有	125	整数	单值	MTU 值 256 - 1406 个字节
SVC-Profiles	有	128	字符串	单值	字符串 （文件名）
SVC-Rekey-Time	有	110	整数	单值	0 = 禁用 1 - 10080 分钟
Tunnel Group Name	有	146	字符串	单值	(1 - 253 个字符)
Tunnel-Group-Lock	有	85	字符串	单值	隧道组名或 “ 无 ”
Tunneling-Protocols	有	11	整数	单值	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 和 4 相互排斥。 0 - 11、16 - 27、32 - 43、48 - 59 为合法值。
Use-Client-Address		17	布尔值	单值	0 = 禁用 1 = 启用
VLAN	有	140	整数	单值	0 - 4094

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名	ASA	属性编号	语法 / 类型	单值或多值	说明或值
WebVPN-Access-List	有	73	字符串	单值	访问列表名称
WebVPN ACL	有	73	字符串	单值	设备上的 WebVPN ACL 名称
WebVPN-ActiveX-Relay	有	137	整数	单值	0 = 禁用 Otherwise = 启用
WebVPN-Apply-ACL	有	102	整数	单值	0 = 禁用 1 = 启用
WebVPN-Auto-HTTP-Signon	有	124	字符串	单值	保留
WebVPN-Citrix-Metaframe-Enable	有	101	整数	单值	0 = 禁用 1 = 启用
WebVPN-Content-Filter-Parameters	有	69	整数	单值	1 = Java ActiveX 2 = Java 脚本 4 = 映像 8 = 映像内的 Cookie
WebVPN-Customization	有	113	字符串	单值	定制名称
WebVPN-Default-Homepage	有	76	字符串	单值	URL （例如 http://example-example.com）
WebVPN-Deny-Message	有	116	字符串	单值	有效字符串 （500 个字符）
WebVPN-Download_Max-Size	有	157	整数	单值	0x7fffffff
WebVPN-File-Access-Enable	有	94	整数	单值	0 = 禁用 1 = 启用
WebVPN-File-Server-Browsing-Enable	有	96	整数	单值	0 = 禁用 1 = 启用
WebVPN-File-Server-Entry-Enable	有	95	整数	单值	0 = 禁用 1 = 启用
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	有	78	字符串	单值	带可选通配符 (*) 的逗号分隔的 DNS/IP （例如 *.cisco.com, 192.168.1.*, wwwin.cisco.com）
WebVPN-Hidden-Shares	有	126	整数	单值	0 = 无 1 = 可见
WebVPN-Home-Page-Use-Smart-Tunnel	有	228	布尔值	单值	启用 （无客户端主页将通过智能隧道呈现时）。
WebVPN-HTML-Filter	有	69	位图	单值	1 = Java ActiveX 2 = 脚本 4 = 映像 8 = Cookie
WebVPN-HTTP-Compression	有	120	整数	单值	0 = 关闭 1 = 解压压缩
WebVPN-HTTP-Proxy-IP-Address	有	74	字符串	单值	逗号分隔的 DNS/IP: 端口，带 http= 或 https= 前缀 （例如 http=10.10.10.10:80, https=11.11.11.11:443）
WebVPN-Idle-Timeout-Alert-Interval	有	148	整数	单值	0 - 30。 0 = 禁用。
WebVPN-Keepalive-Ignore	有	121	整数	单值	0 - 900

表 29-1　支持的 RADIUS 授权属性 （续）

属性名	ASA	属性编号	语法 / 类型	单值或多值	说明或值
WebVPN-Macro-Substitution	有	223	字符串	单值	无限制。例如，请在以下 URL 中参阅《*SSL VPN 部署指南*》： http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Macro-Substitution	有	224	字符串	单值	无限制。例如，请在以下 URL 中参阅《*SSL VPN 部署指南*》： http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Port-Forwarding-Enable	有	97	整数	单值	0 = 禁用 1 = 启用
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	有	98	整数	单值	0 = 禁用 1 = 启用
WebVPN-Port-Forwarding-HTTP-Proxy	有	99	整数	单值	0 = 禁用 1 = 启用
WebVPN-Port-Forwarding-List	有	72	字符串	单值	端口转发列表名称
WebVPN-Port-Forwarding-Name	有	79	字符串	单值	字符串名称 （例如， Corporate-Apps）。 此文本将取代无客户端门户主页上默认的字符串 “Application Access”。
WebVPN-Post-Max-Size	有	159	整数	单值	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	有	149	整数	单值	0 - 30。 0 = 禁用。
WebVPN Smart-Card-Removal-Disconnect	有	225	布尔值	单值	0 = 禁用 1 = 启用
WebVPN-Smart-Tunnel	有	136	字符串	单值	智能隧道的名称
WebVPN-Smart-Tunnel-Auto-Sign-On	有	139	字符串	单值	域名附加的智能隧道自动登录列表名称
WebVPN-Smart-Tunnel-Auto-Start	有	138	整数	单值	0 = 禁用 1 = 启用 2 = 自动启动
WebVPN-Smart-Tunnel-Tunnel-Policy	有	227	字符串	单值	“e networkname”、“i networkname” 或 “a” 中的某一项，其中 networkname 是指智能隧道网络列表的名称， e 表示不包含的通道， i 表示指定的隧道， a 则表示所有隧道。
WebVPN-SSL-VPN-Client-Enable	有	103	整数	单值	0 = 禁用 1 = 启用
WebVPN-SSL-VPN-Client-Keep-Installation	有	105	整数	单值	0 = 禁用 1 = 启用
WebVPN-SSL-VPN-Client-Required	有	104	整数	单值	0 = 禁用 1 = 启用
WebVPN-SSO-Server-Name	有	114	字符串	单值	有效字符串

表 29-1　　支持的 RADIUS 授权属性 （续）

属性名	ASA	属性编号	语法 / 类型	单值或多值	说明或值
WebVPN-Storage-Key	有	162	字符串	单值	
WebVPN-Storage-Objects	有	161	字符串	单值	
WebVPN-SVC-Keepalive-Frequency	有	107	整数	单值	15 - 600 秒， 0 = 关闭
WebVPN-SVC-Client-DPD-Frequency	有	108	整数	单值	5 - 3600 秒， 0 = 关闭
WebVPN-SVC-DTLS-Enable	有	123	整数	单值	0 = 禁用 1 = 启用
WebVPN-SVC-DTLS-MTU	有	125	整数	单值	MTU 值为 256 - 1406 字节。
WebVPN-SVC-Gateway-DPD-Frequency	有	109	整数	单值	5 - 3600 秒， 0 = 关闭
WebVPN-SVC-Rekey-Time	有	110	整数	单值	4 - 10080 分钟， 0 = 关闭
WebVPN-SVC-Rekey-Method	有	111	整数	单值	0 （关闭）、 1 (SSL)、 2 （新隧道）
WebVPN-SVC-Compression	有	112	整数	单值	0 （关闭）， 1 （解压压缩）
WebVPN-UNIX-Group-ID (GID)	有	222	整数	单值	有效 UNIX 组 ID
WebVPN-UNIX-User-ID (UIDs)	有	221	整数	单值	有效 UNIX 用户 ID
WebVPN-Upload-Max-Size	有	158	整数	单值	0x7fffffff
WebVPN-URL-Entry-Enable	有	93	整数	单值	0 = 禁用 1 = 启用
WebVPN-URL-List	有	71	字符串	单值	URL 列表名称
WebVPN-User-Storage	有	160	字符串	单值	
WebVPN-VDI	有	163	字符串	单值	设置列表

支持的 IETF RADIUS 授权属性

表 29-2 列出了支持的 IETF RADIUS 属性。

表 29-2　　支持的 IETF RADIUS 授权属性

属性名	ASA	属性编号	语法 / 类型	单值或多值	说明或值
IETF-Radius-Class	有	25		单值	对于 8.2.x 版本及更高版本，建议使用表 29-1 中所述的 Group-Policy 属性 (VSA 3076, #25)。 • *组策略名称* • OU = *组策略名称* • OU = *组策略名称*
IETF-Radius-Filter-Id	有	11	字符串	单值	在 ASA 中定义的 ACL 名称，仅适用于全隧道 IPsec 和 SSL VPN 客户端。
IETF-Radius-Framed-IP-Address	有	不适用	字符串	单值	IP 地址

表 29-2　　支持的 IETF RADIUS 授权属性 （续）

IETF-Radius-Framed-IP-Netmask	有	不适用	字符串	单值	IP 地址掩码
IETF-Radius-Idle-Timeout	有	28	整数	单值	秒
IETF-Radius-Service-Type	有	6	整数	单值	秒。业务类型可能值： • .Administrative - 允许用户访问配置提示符。 • .NAS-Prompt - 允许用户访问执行提示符。 • .remote-access - 允许用户访问网络。
IETF-Radius-Session-Timeout	有	27	整数	单值	秒

RADIUS 记账断开原因代码

如果 ASA 在发送数据包时断开，将返回这些代码。

断开原因代码
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

RADIUS 服务器许可要求

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

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

IPv6 准则

支持 IPv6。

附加准则

- 您可以在单情景模式中使用 100 个服务器组或在多情景模式的每个情景中使用 4 个服务器组。
- 单情景模式中每组可支持 16 台服务器，多情景模式中每组可支持 4 台服务器。
- 如果您想要使用本地数据库来配置回退支持，请参阅第 28-2 页的回退支持和第 28-2 页的组中存在多个服务器时的回退方式。
- 为防止使用 RADIUS 身份验证时从 ASA 中锁定，请参阅第 36-25 页的从锁定中恢复。

配置 RADIUS 服务器

配置 RADIUS 服务器任务流程

步骤 1　将 ASA 属性加载到 RADIUS 服务器。加载属性采用的方法取决于您所使用的 RADIUS 服务器类型：

- 思科 ACS：该服务器已集成这些属性。您可以跳过此步骤。
- 来自其他供应商的 RADIUS 服务器（例如， Microsoft 互联网身份验证服务）：您必须手动定义每个 ASA 属性。您可以使用属性名或编号、类型、值和供应商代码 (3076) 来定义属性。

步骤 2　添加 RADIUS 服务器组。请参阅第 29-14 页的配置 RADIUS 服务器组。

步骤 3　对于某个服务器组，将一台服务器添加至该服务器组。请参阅第 29-15 页的将 RADIUS 服务器添加到组。

步骤 4　（可选）指定在 AAA 身份验证质询过程中，将会向用户显示的文本。请参阅第 29-17 页的添加身份验证提示。

配置 RADIUS 服务器组

如果您想要使用一台外部 RADIUS 服务器进行身份验证、授权或记账，则必须首先为每个 AAA 协议创建至少一个 RADIUS 服务器组并为每个组添加一台或多台服务器。您通过名称来标识 AAA 服务器组。

要添加 RADIUS 服务器组，请执行以下操作：

详细步骤

步骤 1　选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**。

步骤 2　在 AAA Server Groups 区域，点击 **Add**。

系统将显示 Add AAA Server Group 对话框。

步骤 3　在 Server Group 字段中，输入一个组名称。

步骤 4　从 Protocol 下拉列表，选择 RADIUS 服务器类型。

步骤 5　在 Accounting Mode 字段中，点击 **Simultaneous** 或 **Single**。

在 Single 模式中， ASA 将记账数据仅发送到一台服务器。

在 Simultaneous 模式中， ASA 将记账数据发送到组中的所有服务器。

步骤 6　在 Reactivation Mode 字段中，点击 **Depletion** 或 **Timed**。

在 Depletion 模式中，只有当组中的所有服务器都处于非活动状态后，故障服务器才被重新激活。

在 Timed 模式中，故障服务器在停机 30 秒后被重新激活。

步骤 7　如果您选择 Depletion 重新激活模式，请在 Dead Time 字段中输入时间间隔。

Dead Time 指从禁用组中最后一台服务器之后到再次启用所有服务器之前的时间，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尝试连接次数。

步骤 9　（可选）如果您正在添加 RADIUS 服务器类型，请执行以下操作：

a. 如果要为无客户端 SSL 和 AnyConnect 会话启用多会话记账，请选中 **Enable interim accounting update** 复选框。

b. 选中 **Enable Active Directory Agent Mode** 复选框，指定 ASA 和 AD 代理之间的共享密钥并指出 RADIUS 服务器组包含不是全功能 RADIUS 服务器的 AD 代理。只有使用该选项进行配置的 RADIUS 服务器组才能够和用户身份相关联。

c. 选中 **Enable dynamic authorization** 复选框，启用 ISE 发送授权更改 (CoA) RADIUS 包。使得可以在 VPN 连接的有效期期间内实施在 ISE 上作出的策略更改。

d. 输入**动态授权端口**。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 authorize only mode** 复选框，为 RADIUS 服务器组启用仅授权模式。如果选中该复选框，则不要求为单台 AAA 服务器配置的通用密码或不需要配置该密码。

f. 选中 **VPN3K Compatibility Option** 向下箭头将列表展开，点击以下任一选项来指定是否合并来自 RADIUS 包的可下载 ACL 和思科 AV pair ACL。

- **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。新服务器组被成功添加到 AAA Server Groups 表。

步骤 11　在 AAA Server Groups 对话框中，点击 **Apply**，将更改保存到运行配置。

将 RADIUS 服务器添加到组

要将 RADIUS 服务器添加到组，请执行以下操作：

详细步骤

步骤 1　选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**，然后在 AAA Server Groups 区域中，点击您想要将服务器添加至的服务器组。

该行会在表中突出显示。

步骤 2　在 Servers in the Selected Group 区域中 （下窗格），点击 **Add**。

系统将为该服务器组显示 Add AAA Server Group 对话框。

步骤 3　从 Interface Name 下拉列表，选择身份验证服务器所在的接口名称。

步骤 4　在 Server Name 或 IP Address 字段中，添加要加入到组的服务器的名称或 IP 地址。

步骤 5　在 Timeout 字段中，添加超时值或保留默认值。超时为在向备用服务器发送请求之前， 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 ACL Netmask Convert 字段中，指定 ASA 如何处理可下载 ACL 中的网络掩码。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， ASA 将其转换为标准的网络掩码表达式。

注　因为这些通配符表达式难以清楚地检测，此设置可能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 假定来自 RADIUS 服务器的可下载 ACL 仅包含标准网络掩码表达式。因而不会对通配符网络掩码表达式进行转换。
- Wildcard - ASA 假定来自 RADIUS 服务器的可下载 ACL 只包含通配符网络掩码表达式，并且在下载 ACL 后会将它们全部转换为标准的网络掩码表达式。

步骤 7　在 Common Password 字段中，指定个问号区分大小写的密码，该密码为通过 ASA 访问 RADIUS 授权服务器的用户的通用密码。请务必将该信息提供给 RADIUS 服务器管理员。

注　对于身份验证 RADIUS 服务器 （而非授权服务器），请勿配置通用密码。

如果将该字段留空，则 RADIUS 授权服务器的访问密码为用户名。

请勿使用 RADIUS 授权服务器进行身份验证。通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，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，则主要身份验证请求和辅助身份验证请求包含 MS-CHAPv2 请求属性。如果 RADIUS 服务器不支持 MS-CHAPv2，则不选中该复选框，将该服务器配置为发送非 MS CHAPv2 的身份验证请求。

步骤 9　在 Retry Interval 字段中，指定 ASA 进行联系服务器尝试之间的等待时间，为 1 至 10 秒。

注　无论您输入了何种重试间隔设置，随后的重试间隔时间始终为 50 或 100 毫秒。这属于预期行为。

步骤 10　在 Accounting Mode 字段中，点击 **Simultaneous** 或 **Single**。

在 Single 模式中， ASA 将记账数据仅发送到一台服务器。

在 Simultaneous 模式中， ASA 将记账数据发送到组中的所有服务器。

步骤 11　在 Server Accounting Port 字段中，指定用于用户记账的服务器端口。默认端口为 1646。

步骤 12　在 Server Accounting Port 字段中，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　在 Server Secret Key 字段中，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该与在 RADIUS 服务器中配置的密钥相匹配。如果您不知道服务器密钥，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。 AAA 服务器被成功添加到 AAA 服务器组。

步骤 15　在 AAA Server Groups 窗格中，点击 **Apply**，将更改保存到运行配置。

添加身份验证提示

当要求 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。该文本主要用于装饰用途，并在用户登录时可以看到的用户名和密码提示上方显示。如果您不指定身份验证提示，当用户通过 RADIUS 服务器进行身份验证时，将看到以下内容：

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：

步骤 1　选择 Configuration > Device Management > Users/AAA，在 Authentication Prompt 窗格中，在 Promptenter 字段中输入文本并添加为消息，该消息在用户登录时可以看到的用户名和密码提示上方显示。

下表显示了身份验证提示的允许字符数限制：

应用	字符限制
Microsoft Internet Explorer	37
Telnet	235
FTP	235

步骤 2　在 Messages 区域，在 User accepted message 和 User rejected message 字段中添加消息。

如果用户从 Telnet 进行身份验证，您可以使用 User accepted message 和 User rejected message 选项来显示不同的状态提示，以说明 RADIUS 服务器是否接受或拒绝身份验证尝试。

如果 RADIUS 服务器对用户进行身份验证， ASA 向用户显示 User accepted message 文本，如果指定的话；否则，ASA 显示 User rejected message 文本，如果指定的话。HTTP 和 FTP 会话的身份验证，仅会在提示符处显示质询文本。不会显示 User accepted message 和 User rejected message 文本。

步骤 3　点击 **Apply**，将更改保存到运行配置。

测试 RADIUS 服务器的身份验证和授权

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。

该行会在表中突出显示。

步骤 2　在 Servers in the Selected Group 表中，点击您想要测试的服务器。

该行会在表中突出显示。

步骤 3　点击 **Test**。

系统将为选定服务器显示 Test AAA Server 对话框。

步骤 4　点击您想要执行的测试的类型 - **Authentication** 或 **Authorization**。

步骤 5　在 Username 字段中，输入用户名。

步骤 6　如果您将测试身份验证，请在 Password 字段中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 RADIUS 服务器

要监控 RADIUS 服务器，请参阅以下窗格：

路径	用途
Monitoring > Properties > AAA Servers	显示已配置 RADIUS 服务器统计信息。
Monitoring > Properties > AAA Servers	显示 RADIUS 服务器运行配置。

附加参考资料

附加参考资料

有关通过 RADIUS 服务器实施 AAA 的附加信息，请参阅第 29-19 页的 RFC。

RFC

RFC	标题
2138	*远程身份验证拨入用户服务 (RADIUS)*
2139	*RADIUS 记帐*
2548	*Microsoft 供应商特定 RADIUS 属性*
2868	*用于隧道协议支持的 RADIUS 属性*

RADIUS 服务器功能历史

台版

表 29-3 列出了各种功能变更以及实施该等功能变更的平台版本。 ASDM 可向后兼容多个平台版本，因此，未列出已添加支持的具体 ASDM 版本。

表 29-1　　RADIUS 服务器功能历史

功能名称	平台版本	功能信息
AAA RADIUS 服务器	7.0(1)	描述如何配置 AAA RADIUS 服务器。 我们引入了以下屏幕： Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > Authentication Prompt。
从 ASA 在 RADIUS 访问请求和记账请求数据包中发送的关键供应商特定属性 (VSA)。	8.4(3)	从 ASA 在 RADIUS 访问请求数据包中发送四个新 VSA - Tunnel Group Name (146) 和 Client Type (150)。从 ASA 在 RADIUS 记账请求数据包中发送 Session Type (151) 和 Session Subtype (152)。为所有类型的记账请求数据包发送所有这四个属性：Start、 Interim-Update 和 Stop。RADIUS 服务器 （例如， ACS 和 ISE）可以实施授权和策略属性或者利用它们进行记账和收费。

用于 AAA 的 TACACS+ 服务器

本章介绍如何配置在 AAA 中使用的 TACACS+ 服务器。

有关 TACACS+ 服务器的信息

ASA 支持使用以下协议执行 TACACS+ 服务器身份验证：ASCII、 PAP、 CHAP 和 MS-CHAPv1。

使用 TACACS+ 属性

思科 ASA 可支持 TACACS+ 属性。 TACACS+ 属性可用于分隔身份验证、授权和记帐功能。该协议支持两种类型的属性：必需和可选。服务器和客户端都必须能够理解必需属性，而且必须将必需属性应用至用户。可选属性是否能被理解，或是否会被使用不作要求。

注 要使用 TACACS+ 属性，请确保您已在 NAS 上启用 AAA 服务。

表 30-1 列出了适用于直通代理连接的受支持的 TACACS+ 授权响应属性。表 30-2 列出了受支持的 TACACS+ 记帐属性。

表 30-1　受支持的 TACACS+ 授权响应属性

属性	说明
acl	确定要应用至连接的本地配置的 ACL。
idletime	指定经过身份验证的用户会话会被终止前，可以有的非活动时长，以分钟为单位。
timeout	指定经过身份验证的用户会话会被终止前，身份验证凭据可以保持活动状态的时长，以分钟为单位。

表 30-2　受支持的 TACACS+ 记帐时间

属性	说明
bytes_in	指定连接过程中，传输的输入字节的数量 （仅停止记录）
bytes_out	指定连接过程中，传输的输出字节的数量 （仅停止记录）
cmd	定义会被执行的命令 （仅命令记帐）。
disc-cause	指定标识断开原因的数值代码 （仅停止记录）。
elapsed_time	定义连接的运行时间 （仅停止记录）。
foreign_ip	指定隧道连接的客户端的 IP 地址。定义用于直通代理连接的最低安全性接口上的地址。
local_ip	指定对于隧道连接，客户端已连接到的 IP 地址。定义用于直通代理连接的最高安全性接口上的地址。
NAS port	包含连接的会话 ID。
packs_in	指定在连接期间传输的输入数据包的数量。
packs_out	指定在连接期间传输的输出数据包的数量。
priv-level	设置为命令记帐请求的用户权限级别，否则设置为 1。
rem_iddr	指定客户端的 IP 地址。
service	指定所使用的服务。对于仅进行命令记帐的情况，始终设置为 “shell”。
task_id	指定记帐事务的唯一任务 ID。
username	指定用户的名称。

TACACS+ 服务器的许可要求

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

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

IPv6 准则

支持 IPv6。

附加准则

- 您可以在单情景模式中使用 100 个服务器组或在多情景模式的每个情景中使用 4 个服务器组。
- 单情景模式中每组可支持 16 台服务器，多情景模式中每组可支持 4 台服务器。
- 如果您想要使用本地数据库来配置回退支持，请参阅第 28-2 页的回退支持和第 28-2 页的组中存在多个服务器时的回退方式。
- 要在使用 TACACS+ 身份验证或授权时，防止来自 ASA 的锁定，请参阅第 36-25 页的从锁定中恢复。

配置 TACACS+ 服务器

配置 TACACS+ 服务器任务流程

步骤 1　添加 TACACS+ 服务器组。请参阅第 30-4 页的配置 TACACS+ 服务器组。

步骤 2　对于某个服务器组，将一台服务器添加至该服务器组。请参阅第 30-4 页的将 TACACS+ 服务器添加至服务器组。

步骤 3　（可选）指定在 AAA 身份验证质询过程中，将会向用户显示的文本。请参阅第 30-5 页的添加身份验证提示。

配置 TACACS+ 服务器组

如果您想要将 TACACS+ 服务器用于身份验证、授权或记帐，必须先创建至少一个 TACACS+ 服务器组，然后向每个服务器组添加一台或多台服务器。您可以通过名称标识 TACACS+ 服务器组。

要添加 TACACS+ 服务器组，请执行以下步骤：

详细步骤

步骤 1　选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**。

步骤 2　在 AAA Server Groups 区域，点击 **Add**。

系统将显示 Add AAA Server Group 对话框。

步骤 3　在 Server Group 字段中，输入一个组名称。

步骤 4　从 Protocol 下拉列表中，选择 TACACS+ 服务器类型：

步骤 5　在 Accounting Mode 字段中，点击 **Simultaneous** 或 **Single**。

在 Single 模式中， ASA 将记账数据仅发送到一台服务器。

在 Simultaneous 模式中， ASA 将记账数据发送到组中的所有服务器。

步骤 6　在 Reactivation Mode 字段中，点击 **Depletion** 或 **Timed**。

在 Depletion 模式中，只有当组中的所有服务器都处于非活动状态后，故障服务器才被重新激活。

在 Timed 模式中，故障服务器在停机 30 秒后被重新激活。

步骤 7　如果您选择 Depletion 重新激活模式，可以在 Dead Time 字段中输入时间间隔。

Dead Time 是以分钟为单位的时段，该时段是禁用组中的最后一台服务器之后，开始所有服务器的后续重新启用之前，会经过的一段时间。

步骤 8　在 Max Failed Attempts 字段中，添加允许的失败尝试次数。

此选项设置在宣告无响应服务器处于非活动状态之前允许的尝试连接失败次数。

步骤 9　点击 **OK**。

系统将关闭 Add AAA Server Group 对话框。新服务器组被成功添加到 AAA Server Groups 表。

步骤 10　在 AAA Server Groups 对话框中，点击 **Apply**，将更改保存到运行配置。

将 TACACS+ 服务器添加至服务器组

要将 TACACS+ 服务器添加至服务器组，请执行以下操作：

详细步骤

步骤 1　选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**，然后在 AAA Server Groups 区域中，点击您想要将服务器添加至的服务器组。

该行会在表中突出显示。

步骤 2　在 Servers in the Selected Group 区域中 （下窗格），点击 **Add**。

系统将为该服务器组显示 Add AAA Server Group 对话框。

步骤 3　从 Interface Name 下拉列表，选择身份验证服务器所在的接口名称。

步骤 4　在 Server Name 或 IP Address 字段中，添加要加入到组的服务器的名称或 IP 地址。

步骤 5　在 Timeout 字段中，添加超时值或保留默认值。超时是 ASA 在向备用服务器发送请求之前等待主服务器响应的持续时间，以秒为单位。

步骤 6　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 7　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 8　点击 **OK**。

系统将关闭 Add AAA Server Group 对话框。 AAA 服务器被成功添加到 AAA 服务器组。

步骤 9　在 AAA Server Groups 窗格中，点击 **Apply**，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。该文本主要用于装饰用途，并在用户登录时可以看到的用户名和密码提示上方显示。

如果您没有指定身份验证提示，用户在使用 TACACS+ 服务器进行身份验证时，会看到以下的默认提示：

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：

步骤 1　选择 **Configuration > Device Management > Users/AAA > Authentication Prompt**。

步骤 2　在 Prompt 字段中输入文本，以便添加为消息，该消息会在用户登录时看到的用户名和密码提示之上显示。

下表显示了身份验证提示的允许字符数限制：

应用	身份验证提示的字符数限制
Microsoft Internet Explorer	37
Telnet	235
FTP	235

步骤 3　在 Messages 区域，在 User accepted message 和 User rejected message 字段中添加消息。

如果用户身份验证通过 Telnet 进行，您可以使用 User accepted message 和 User rejected message 选项来显示不同的状态提示，以便指定 AAA 服务器是接受，还是拒绝身份验证尝试。

如果 AAA 服务器通过用户的身份验证， ASA 会显示 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，仅会在提示符处显示质询文本。不会显示 User accepted message 和 User rejected message 文本。

步骤 4　点击 **Apply**，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 是否可以与 TACACS+ 服务器联系，并对用户进行身份验证或授权，请执行以下操作：

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。

该行会在表中突出显示。

步骤 2　在 Servers in the Selected Group 表中，点击您想要测试的服务器。

该行会在表中突出显示。

步骤 3　点击 **Test**。

系统将会为选定服务器显示 Test AAA Server 对话框。

步骤 4　点击您想要执行的测试的类型 - **Authentication** 或 **Authorization**。

步骤 5　在 Username 字段中，输入用户名。

步骤 6　如果您将测试身份验证，请在 Password 字段中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 TACACS+ 服务器

要监控 TACACS+ 服务器，请参阅以下窗格：

路径	用途
Monitoring > Properties > AAA Servers	显示配置的 TACACS+ 服务器的统计信息。
Monitoring > Properties > AAA Servers	显示 TACACS+ 服务器的运行配置。

TACACS+ 服务器的功能历史记录

表 30-3 列出了各种功能变更以及实施该等功能变更的平台版本。 ASDM 可向后兼容多个平台版本，因此，未列出已添加支持的具体 ASDM 版本。

表 30-3　　TACACS+ 服务器的功能历史记录

功能名称	平台版本	功能信息
TACACS+ 服务器	7.0(1)	介绍如何配置用于 AAA 的 TACACS+ 服务器。 我们引入了以下屏幕： Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > Authentication Prompt。

AAA 中的 LDAP 服务器

本章介绍如何配置 AAA 的 LDAP 服务器。

有关 LDAP 和 ASA 的信息

思科 ASA 兼容于大多数 LDAPv3 目录服务器，包括：

- Sun Microsystems JAVA System Directory Server，现在是 Oracle Directory Server Enterprise Edition 的一部分，以前称为 Sun ONE Directory Server
- Microsoft Active Directory
- Novell
- OpenLDAP

默认情况下， ASA 会自动检测其是否连接到 Microsoft Active Directory、 Sun LDAP、 Novell、 OpenLDAP 或通用 LDAPv3 目录服务器。但是，如果自动检测无法确定 LDAP 服务器类型，则可以手动配置它。

LDAP 服务器准则

配置 LDAP 服务器时，请注意以下准则：

- 为访问 Sun 目录服务器而在 ASA 上配置的 DN 必须能够访问该服务器上的默认密码策略。我们建议将目录管理员或具有目录管理员权限的用户用作 DN。或者，可将 ACL 放在默认密码策略上。
- 您必须通过 SSL 配置 LDAP，以便对 Microsoft Active Directory 和 Sun 服务器启用密码管理。
- ASA 不支持对 Novell、 OpenLDAP 和其他 LDAPv3 目录服务器启用密码管理。
- VPN 3000 集中器和 ASA/PIX 7.0 软件需要思科 LDAP 模式进行授权操作。从 V 7.1.x 开始，ASA 使用本地 LDAP 模式执行身份验证和授权，而不再需要思科模式。

如何用 LDAP 进行身份验证

执行身份验证期间，ASA 将充当用户的 LDAP 服务器的客户端代理，并以纯文本或使用 SASL 协议对 LDAP 服务器执行身份验证。默认情况下，ASA 以纯文本将身份验证参数，通常为用户名和密码传递至 LDAP 服务器。

ASA 支持以下 SASL 机制，按强度递增的顺序列示：

- Digest-MD5 - ASA 以一个由用户名和密码计算的 MD5 值响应 LDAP 服务器。
- Kerberos - ASA 通过使用 GSSAPI Kerberos 机制发送用户名和领域响应 LDAP 服务器。

ASA 和 LDAP 服务器支持这些 SASL 机制的任意组合。如果配置多个机制，则 ASA 将检索服务器上配置的 SASL 机制的列表，并将身份验证机制设置为 ASA 和服务器上配置的最强机制。例如，如果 LDAP 服务器和 ASA 支持这两种机制，则 ASA 将选择两者中的较强者 Kerberos。

对用户成功执行 LDAP 身份验证后，LDAP 服务器将返回已通过身份验证的用户的属性。对于 VPN 身份验证，这些属性通常包括已应用于 VPN 会话的授权数据。在此情况下，使用 LDAP 即可一步完成身份验证和授权。

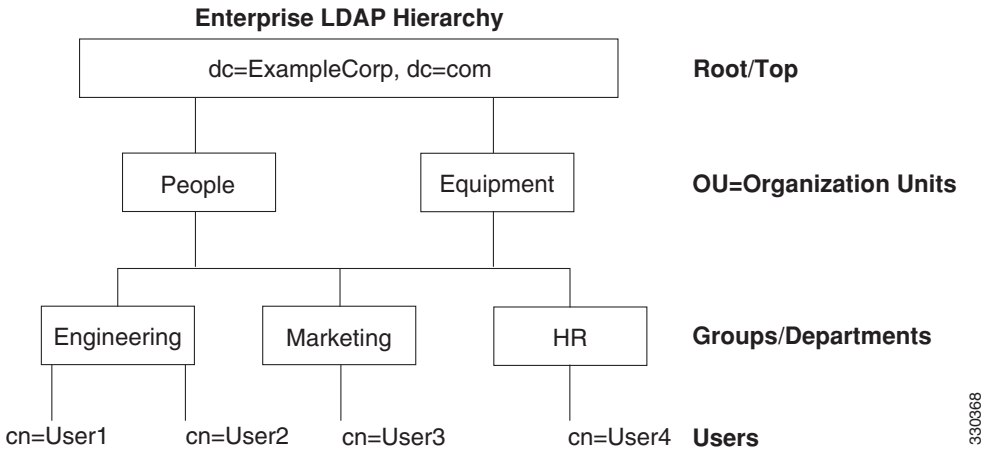
注　有关 LDAP 协议的详细信息，请参阅 RFC 1777、2251 和 2849。

关于 LDAP 层次结构

您的 LDAP 配置应反映贵组织的逻辑层次结构。例如，假设贵公司 Example Corporation 的一名员工叫 Employee1。Employee1 在工程组工作。您的 LDAP 层次结构可能有一个或多个级别。您可能决定设置一个单级别层次结构，在其中 Employee1 被视为 Example Corporation 的一名成员。您也可以设置一个多级别层次结构，在其中 Employee1 被视为工程部门的一名成员，该部门是一个称为 People 的组织单位的成员，而该组织单位则是 Example Corporation 的成员。请参阅图 31-1，了解多级别层次结构的示例。

多级别层次结构的信息比较详细，但是，在单级别层次结构中搜索结果的速度更快。

图 31-1　多级别 LDAP 层次结构



搜索 LDAP 层次结构

ASA 可供您在 LDAP 层次结构中定制搜索。您在 ASA 上配置以下三个字段，定义在 LDAP 层次结构中开始搜索的位置、搜索范围和所搜索信息的类型。这些字段共同将层次结构的搜索仅限于包含用户权限的部分。

- LDAP Base DN 将定义服务器自 ASA 收到授权请求后开始在 LDAP 层次结构中搜索用户信息的位置。
- Search Scope 将定义在 LDAP 层次结构中的搜索范围。搜索继续在层次结构中 LDAP Base DN 下方的多个级别中进行。您可以选择让服务器仅搜索紧接其下方的那个级别，否则，它可能搜索整个子树。单级别搜索比较快，但子树搜索更加广泛。
- Naming Attribute 定义唯一识别 LDAP 服务器中条目的 RDN。常用的命名属性可能包括 cn (Common Name)、 sAMAccountName 和 userPrincipalName。

图 31-1 显示了 Example Corporation 的一个 LDAP 层次结构示例。鉴于该层次结构，您可以不同的方式定义您的搜索。表 31-1 显示了两个搜索配置示例。

在第一个配置示例中，如果 Employee1 用所需 LDAP 授权建立 IPsec 隧道，则 ASA 将向 LDAP 服务器发送一个搜索请求，指明其应在工程组中搜索 Employee1。这种搜索速度很快。

在第二个配置示例中， ASA 发送一个搜索请求，指明服务器应在 Example Corporation 中搜索 Employee1。这种搜索需时较长。

表 31-1　搜索配置示例

编号	LDAP Base DN	搜索范围	命名属性	结果
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	一级	cn=Employee1	搜索速度较快
2	dc=ExampleCorporation,dc=com	子树	cn=Employee1	搜索时间较长

关于绑定到 LDAP 服务器

ASA 使用登录 DN 和登录密码与 LDAP 服务器建立信任（绑定）。执行 Microsoft Active Directory 只读操作 （例如身份验证、授权或组搜索）时， ASA 可绑定登录 DN 与较少权限。例如，登录 DN 可能是 AD “Member Of” 名称为 Domain Users 一部分的用户。对于 VPN 密码管理操作，登录 DN 需要较高的权限，而且必须为 Account Operators AD 组的一部分。

以下是登录 DN 的一个示例：

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA 支持以下身份验证方法：

- 使用未加密密码对端口 389 执行的简单 LDAP 身份验证
- 对端口 636 执行的安全 LDAP (LDAP-S)
- 简单身份验证和安全层 (SASL) MD5
- SASL Kerberos

ASA 不支持匿名身份验证。

注　作为一个 LDAP 客户端， ASA 不支持匿名绑定或请求的传输。

LDAP 服务器许可要求

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

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

IPv6 准则

支持 IPv6。

配置 LDAP 服务器

用于配置 LDAP 服务器的任务流

步骤 1　添加 LDAP 服务器组。请参阅第 31-6 页的配置 LDAP 服务器组　。

步骤 2　将一个服务器添加至组，然后配置服务器参数。请参阅第 31-7 页的将 LDAP 服务器添加到组　。

步骤 3　配置 LDAP 属性映射。请参阅第 31-5 页的配置 LDAP 属性映射。
将 LDAP 服务器添加至 LDAP 服务器组之前，必须添加属性映射。

配置 LDAP 属性映射

ASA 可为以下项使用 LDAP 目录对用户进行身份验证：

- VPN 远程访问用户
- 防火墙网络访问 / 直通代理会话
- 设置策略权限 （也称为授权属性），如 ACL、书签列表、 DNS 或 WINS 设置，以及会话计时器。
- 在本地组策略中设置关键属性

ASA 使用 LDAP 属性映射将本地 LDAP 用户属性转换为思科 ASA 属性。您可以将这些属性映射与 LDAP 服务器进行绑定或删除它们。您还可以显示或清除属性映射。

准则

LDAP 属性映射不支持多值属性。例如，如果用户是多个 AD 组的成员，而且 LDAP 属性映射与多个组匹配，则根据匹配条目的字母顺序选择值。

要正确使用属性映射功能，您需了解 LDAP 属性名称和值，以及用户定义的属性名称和值。

频繁映射的 LDAP 属性的名称以及经常将其映射到的用户定义属性的类型包括：

- IETF-Radius-Class（ASA V 8.2 或更高版本中的 Group_Policy）- 根据目录部门或用户组（例如， Microsoft Active Directory memberOf）属性值设置组策略。组策略属性用 ASDM V 6.2/ASA V 8.2 或更高版本替换 IETF-Radius-Class 属性。
- IETF-Radius-Filter-Id - 将访问控制列表或 ACL 应用于 VPN 客户端、 IPsec 和 SSL。
- IETF-Radius-Framed-IP-Address - 将已分配的静态 IP 地址分配到 VPN 远程访问客户端、IPsec 和 SSL。
- Banner1 - 在 VPN 远程访问用户登录时显示文本标题。
- Tunneling-Protocols - 根据访问类型，允许或拒绝 VPN 远程访问会话。

注　单一 LDAP 属性映射可以包含一个或多个属性。只能从一个特定 LDAP 服务器映射一个 LDAP 属性。

要映射 LDAP 功能，请执行以下步骤：

详细步骤

步骤 1　选择 **Configuration > Remote Access VPN > AAA Local Users > LDAP Attribute Map**（对于本地用户），或者选择 **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，其中的 Map Name 选项卡已激活。

步骤 2　在 Name 字段中，为该属性映射创建一个名称。

步骤 3　在 LDAP Attribute Name 字段中，为要映射的 LDAP 属性之一添加名称。

步骤 4　从 Cisco Attribute Name 下拉列表中，选择一个思科属性。

步骤 5　点击 **Add**。

步骤 6　属性映射成功。要映射更多属性，请重复步骤 1 至 5。

步骤 7　如果想要将任何 LDAP 属性的值映射到已映射思科属性中的新值，请点击 **Map Value** 选项卡。

步骤 8　点击 **Add**。

系统将显示 Add Mapping of Attribute Name 对话框。

步骤 9　从下拉列表中选择 LDAP 属性。

步骤 10　在 LDAP Attribute Value 字段中，输入您希望从 LDAP 服务器返回的该 LDAP 属性的值。

步骤 11　在 Cisco Attribute Value 字段中，输入当该 LDAP 属性包含以前 LDAP Attribute Value 时您希望在思科属性中使用的值。

步骤 12　点击 **Add**。

值映射成功。

步骤 13　要映射更多值，请重复步骤 8 至 12。

步骤 14　点击 **OK** 以返回 Map Value 选项卡，然后再次点击 **OK** 以关闭对话框。

步骤 15　在 LDAP Attribute Value 窗格中，点击 **Apply** 以将值映射保存到运行配置。

配置 LDAP 服务器组

要使用外部 LDAP 服务器执行身份验证、授权和 / 或记帐，首先必须至少创建一个 LDAP 服务器组，且向每个组添加一个或多个服务器。按名称标识 LDAP 服务器组。每个服务器组对应于一个服务器类型。

准则

- 在单模式中，最多可以有 100 个 LDAP 服务器组；在多模式中，每个情景可以有 4 个 LDAP 服务器组。
- 在单模式中，每组最多可以有 16 个 LDAP 服务器；在多模式中，每组可以有 4 个 LDAP 服务器。
- 用户登录时，从您在配置中指定的第一个服务器开始，一次访问一个 LDAP 服务器，直到服务器响应为止。如果该组中的所有服务器均不可用，如将 ASA 配置为回退方法（仅管理身份验证和授权），则其将尝试本地数据库。如果没有回退方法，则 ASA 将继续尝试 LDAP 服务器。

详细步骤

以下步骤说明如何创建和配置 LDAP 服务器组，并将 LDAP 服务器添加到该组。

步骤 1　为 VPN 用户选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**，或 **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**。

步骤 2　在 AAA Server Groups 区域，点击 **Add**。

系统将显示 Add AAA Server Group 对话框。

步骤 3　在 AAA Server Group 字段中，请为该 AAA 服务器组命名。

步骤 4　从 Protocol 下拉列表中，选择 LDAP 服务器类型。

步骤 5　在 Reactivation Mode 字段中，点击与您要使用的模式对应的单选按钮（**Depletion** 或 **Timed**）。

在 Depletion 模式中，只有当组中的所有服务器都处于非活动状态后，故障服务器才被重新激活。

在 Timed 模式中，故障服务器在停机 30 秒后被重新激活。

a. 如果选择 Depletion 重新激活模式，请在 Dead Time 字段输入时间间隔。

Dead Time 是以分钟计量的持续时间，指禁用组内最后一个服务器与随后重新启用所有服务器之间的时间。

步骤 6　在 Max Failed Attempts 字段中，添加在尝试连接到服务器时允许的失败次数。

此选项设置在宣告无响应服务器处于非活动状态之前允许的尝试连接失败次数。

步骤 7　点击 **OK**。

系统将关闭 Add AAA Server Group 对话框。新服务器组被成功添加到 AAA Server Groups 表。

步骤 8　在 AAA Server Groups 对话框中，点击 **Apply** 保存更改。

更改将保存到运行中的配置中。

将 LDAP 服务器添加到组

步骤 1　为 VPN 用户选择 **Configuration > Device Management > Users/AAA > AAA Server Groups**，或 **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**，并在 AAA Server Groups 区域中，选择要将服务器添加到的服务器组。

步骤 2　在 Servers in Selected Group 列表旁边，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　从 Interface Name 下拉列表中，选择连接到 LDAP 服务器的接口名称。

步骤 4　在 Server Name 或 IP Address 字段中，添加 LDAP 服务器的服务器名称或 IP 地址。

步骤 5　在 Timeout 字段中，添加超时值或保留默认值。超时是 ASA 在向备用服务器发送请求之前等待主服务器响应的持续时间，以秒为单位。

步骤 6　在身份验证 / 授权区域的 LDAP 参数中，请配置以下字段：

- **Enable LDAP over SSL**（也称为 secure LDAP 或 LDAP-S） - 如果要使用 SSL 保护 ASA 与 LDAP 服务器之间的通信，请选中此字段。

注　如果未配置 SASL 协议，我们强烈建议您用 SSL 保护 LDAP 通信。

- **Server Port** - 输入 TCP 端口号 389， ASA 将用该端口访问 LDAP 服务器进行简单的 （非安全）身份验证，或访问 TCP 端口 636 进行安全身份验证 (LDAP-S)。所有 LDAP 服务器均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 层次结构中输入基准可分辨名称 (Base Distinguished Name)，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** - 指定服务器在收到源自下拉列表的授权请求时应在 LDAP 层次结构中执行搜索的范围。以下选项可用：
  - One Level - 仅搜索 Base DN 以下的一个级别。此选项速度较快。
  - All Levels - 搜索 Base DN 以下的所有级别 （即搜索整个子树层次结构）。此选项需时较长。
- **Naming Attribute(s)** - 输入唯一识别 LDAP 服务器上的某一条目的 Relative Distinguished Name 属性。常用命名属性为 Common Name (CN)、sAMAccountName、userPrincipalName 和 User 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，该密码用于登录 DN 用户帐户。键入的字符替换为星号。
- **LDAP Attribute Map** - 选择要使用的为该 LDAP 服务器创建的属性映射之一。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** 该选项启用 SASL 的 MD5 机制，对 ASA 与 LDAP 服务器之间的通信进行身份验证。
- **SASL Kerberos authentication** - 启用 SASL 的 Kerberos 机制，保护 ASA 与 LDAP 服务器之间的身份验证通信。只有先定义 Kerberos 服务器，然后才能启用该选项。
- **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 Base DN 执行 AD 组检索。 ASDM 使用已检索 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** - 指定对 AD 服务器查询可用组时等待其做出响应的最长时间。

步骤 7　点击 **OK**。

系统将关闭 Add AAA Server 对话框， AAA 服务器已添加到 AAA 服务器组。

步骤 8　在 AAA Server Groups 窗格中，点击 **Apply**，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：

步骤 1　在 Configuration > Device Management > Users/AAA > AAA Server Groups 窗格中，选择服务器所驻留的服务器组。

步骤 2　在 Selected Group 区域的 Servers 中，选择要测试的服务器。

步骤 3　点击 **Test**。

系统将针对选定服务器显示 Test AAA Server 对话框。

步骤 4　点击您想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 LDAP 服务器

要监控 LDAP 服务器，请执行以下步骤：

步骤 1　在 ASDM 中，选择 **Monitoring > Properties > AAA Servers**。

步骤 2　要更新 LDAP 服务器的状态，请选定它，然后点击 **Update Server Statistics**。

系统将显示 Update AAA Server Status 对话框，已在下拉列表中选定 LDAP 服务器。

步骤 3　点击 **OK**。

步骤 4　要更新当前显示的统计信息，请点击 **Clear Server Statistics**。

LDAP 服务器的功能历史记录

表 31-2 列出了各种功能变更以及实施该等功能变更的平台版本。ASDM 向后兼容多个平台版本，因此，未列出已添加支持的特定 ASDM 版本。

表 31-2　AAA 服务器的功能历史记录

功能名称	平台版本	功能信息
AAA 中的 LDAP 服务器	7.0(1)	LDAP Servers 将介绍对 AAA 的支持以及如何配置 LDAP 服务器。 我们引入了以下屏幕： Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Remote Access VPN > AAA Local Users > LDAP Attribute Map

身份防火墙

本章介绍如何为身份防火墙配置 ASA。

关于身份防火墙的信息

身份防火墙概述

在企业中，用户通常需要访问一个或多个服务器资源。通常，防火墙不知道用户的身份，因此也就无法基于身份应用安全策略。要配置每个用户的访问策略，则您必须配置用户身份验证代理，其要求用户交互 （用户名 / 密码查询）。

ASA 内的身份防火墙基于用户身份提供更细粒度的访问控制。您可以基于用户名和用户组名，而不是通过源 IP 地址配置访问规则和安全策略。ASA 基于 IP 地址与 Windows Active Directory 登录信息的关联应用安全策略，并基于映射的用户名，而不是基于网络 IP 地址报告事件。

身份防火墙与提供实际身份映射的外部 Active Directory (AD) 代理配合，与 Microsoft Active Directory 相集成。ASA 将 Windows Active Directory 用作检索特定 IP 地址的当前用户身份信息的源，并允许 Active Directory 用户的透明身份验证。

通过允许指定用户或组来代替源 IP 地址，基于身份的防火墙服务增强现有访问控制和安全策略机制。基于身份的安全策略可以交错，无传统的基于 IP 地址的规则之间的限制。

身份防火墙的主要优点包括：

- 将网络拓扑从安全策略解耦
- 简化安全策略创建
- 能够轻松识别用户在网络资源上的活动
- 简化用户活动监控

身份防火墙部署的架构

身份防火墙与提供实际身份映射的外部 Active Directory (AD) 代理配合，与 Window Active Directory 相集成。

身份防火墙由三个组件组成：

- ASA
- Microsoft Active Directory

  虽然 Active Directory 是 ASA 中身份防火墙的一部分，但是 Active Directory 管理员对其进行管理。数据可靠性和准确性取决于 Active Directory 中的数据。

  支持的版本包括 Windows Server 2003、 Windows Server 2008 和 Windows Server 2008 R2 服务器。

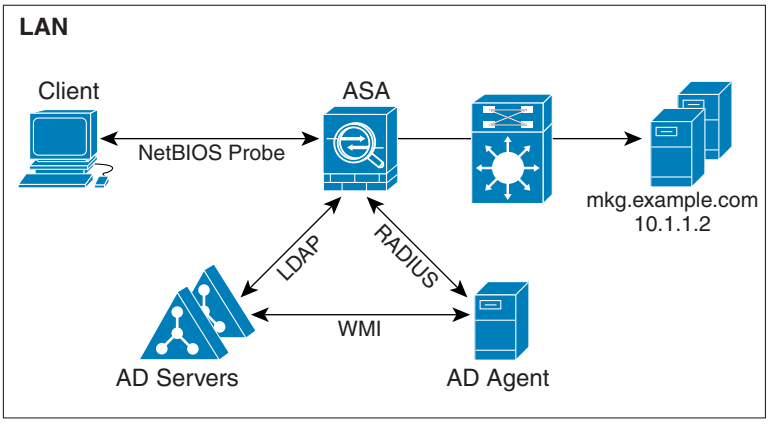
- Active Directory (AD) 代理

  AD 代理在 Windows 服务器上运行。支持的 Windows 服务器包括 Windows 2003、 Windows 2008 和 Windows 2008 R2。

注　对于 AD 代理服务器来说，不支持 Windows 2003 R2。

图 32-1 显示身份防火墙的组件。随后的表格介绍这些组件的角色，以及它们如何互相通信。

图 32-1　身份防火墙组件



1	**在 ASA 上**：管理员配置本地用户组和身份防火墙策略。	4	**客户端 <-> ASA**：客户端通过 Microsoft Active Directory 登录网络。 AD 服务器对用户进行身份验证并生成用户登录安全日志。 或者，客户端可以通过直接转发代理或 VPN 登录网络。
2	**ASA <-> AD 服务器**：ASA 发送对在 AD 服务器上配置的 Active Directory 组的 LDAP 查询。 ASA 整合本地和 Active Directory 组，并基于用户身份应用访问规则和模块化策略框架安全策略。	5	**ASA <-> 客户端**：基于在 ASA 上配置的策略，它许可或拒绝客户端访问。 如果已进行配置， ASA 则探测客户端的 NetBIOS 来通过非活动和无响应用户。
3	**ASA <-> AD 代理**：根据身份防火墙配置，ASA 下载 IP - 用户数据库或向 AD 代理发送 RADIUS 请求来要求提供用户的 IP 地址。 ASA 将从网络身份验证和 VPN 会话所了解到的新映射的条目转发到 AD 代理。	6	**AD 代理 <-> AD 服务器**：AD 代理维护用户 ID 和 IP 地址映射条目的缓存，并将更改通知给 ASA。 AD 代理向系统日志服务器发送日志。

身份防火墙功能

身份防火墙包括以下主要功能。

灵活性

- 通过向 AD 代理查询每个新 IP 地址或通过维护整个用户身份和 IP 地址数据库的本地副本，ASA 可以从 AD 代理检索用户身份和 IP 地址映射。
- 支持用户身份策略目标的主机组、子网或 IP 地址。
- 支持用户身份策略源和目标的完全限定域名 (FQDN)。
- 支持基于 ID 策略的五元组策略组合。基于身份的功能与现有五元组解决方案配套使用。
- 支持使用 IPS 和应用检查策略。
- 从远程访问 VPN、AnyConnect VPN、L2TP VPN 和直接转发代理检索用户身份信息。所有检索到的用户填充到与 AD 代理连接的所有 ASA。

可扩展性

- 每个 AD 代理支持 100 个 ASA。多个 ASA 能够与单个 AD 代理通信，以在更大型网络部署中提供扩展性。
- 假如 IP 地址在所有域中保持唯一，则支持 30 个 Active Directory 服务器。
- 在域中的每个用户身份可以包含多达 8 个 IP 地址。
- 在 ASA 5500 系列型号的有效策略中支持多达 64,000 个用户身份 - IP 地址映射条目。此限制控制应用了策略的用户最大数量。用户总数是在所有不同情景中配置的所有用户合计数量。
- 在有效 ASA 策略中支持多达 256 个用户组。
- 单个访问规则可以包含一个或多个用户组或用户。
- 支持多个域。

可用性

- 当 AD 代理无法将源 IP 地址映射到用户身份时， ASA 从 Active Directory 中检索组信息，回退到 IP 地址网络身份验证。
- 如果任何 Active Directory 服务器或 ASA 不响应， AD 代理会继续运行。
- 支持在 ASA 上配置一个主要 AD 代理和一个辅助 AD 代理。如果主要 AD 代理停止响应，ASA 可以切换到辅助 AD 代理。
- 如果 AD 代理不可用， ASA 可以回退到现有身份源，比如直接转发代理和 VPN 身份验证。
- AD 代理运行监视器进程，在服务关闭时自动重新启动服务。
- 允许在 ASA 之间使用分布式 IP 地址 / 用户映射数据库。

部署方案

根据环境要求，您能够以下列方式部署身份防火墙组件。

图 32-2 显示如何部署身份防火墙组件以允许冗余。方案 1 显示无组件冗余的简单安装。方案 2 也显示无冗余的简单安装。但是，在此部署方案中， Active Directory 服务器和 AD 代理共同位于同一 Windows 服务器上。

图 32-2　　无冗余部署方案

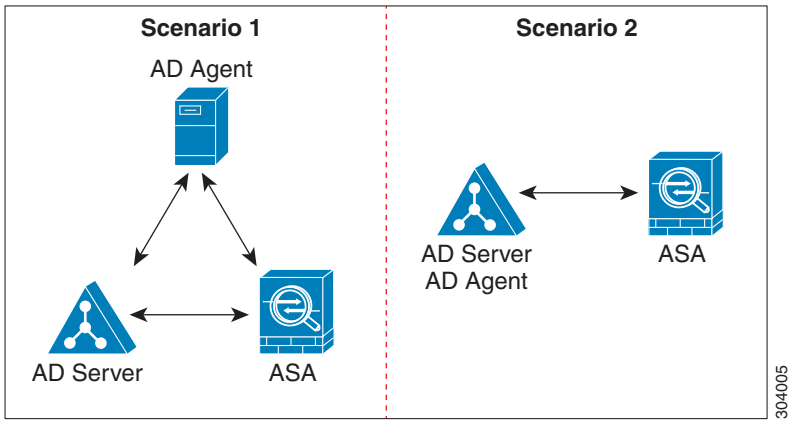


图 32-3 显示如何部署身份防火墙组件以支持冗余。方案 1 显示一种部署，其中有多个 Active Directory 服务器和单个安装在单独 Windows 服务器上的 AD 代理。方案 2 显示一个部署，其中有多个 Active Directory 服务器和多个安装在单独 Windows 服务器上的 AD 代理。

图 32-3　具有冗余组件的部署方案

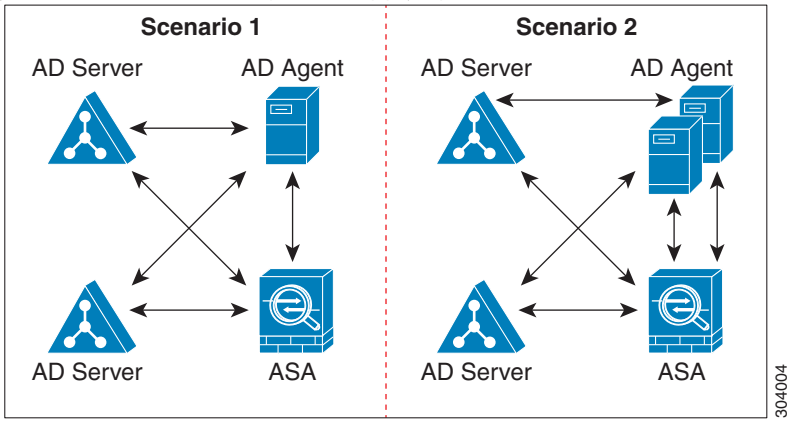


图 32-4 显示所有身份防火墙组件（Active Directory 服务器、AD 代理和客户端）如何进行安装以及如何在局域网上进行通信。

图 32-4　基于局域网的部署

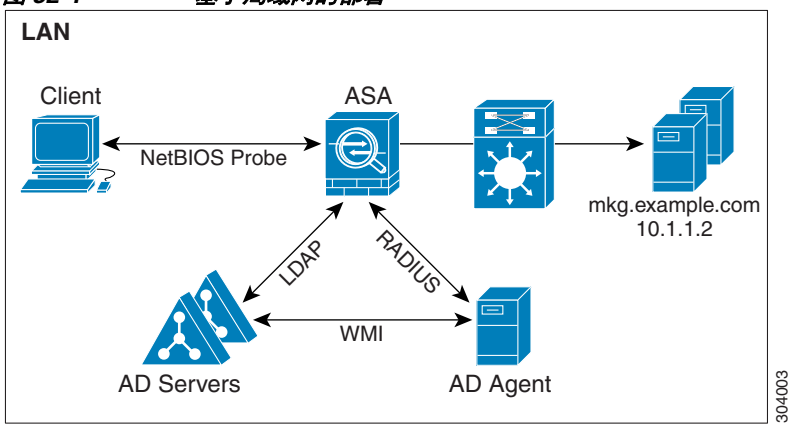


图 32-5 显示支持远程站点的基于广域网的部署。Active Directory 服务器和 AD 代理安装在主站点局域网中。客户端位于远程站点，并通过广域网连接至身份防火墙组件。

图 32-5　基于广域网的部署

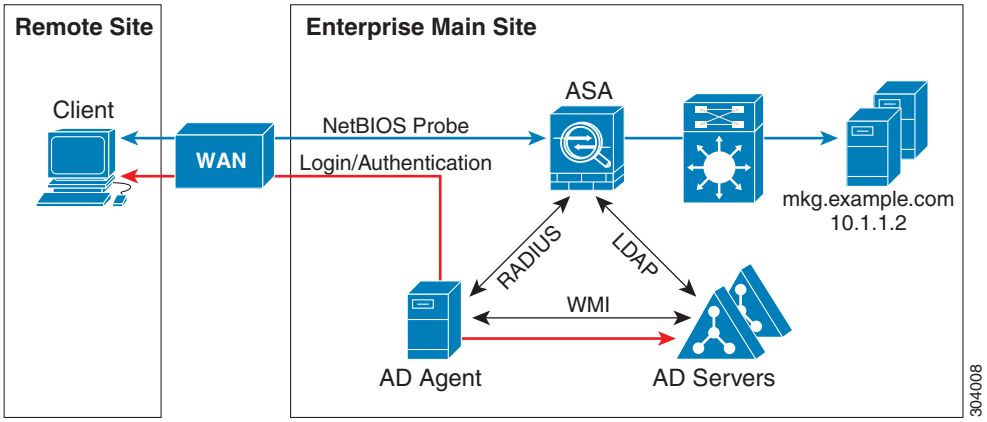


图 32-6 也显示支持远程站点的基于广域网的部署。 Active Directory 服务器安装在主站点局域网中。但是， AD 代理通过远程站点的客户端进行安装和访问。远程客户端通过广域网连接至主站点的 Active Directory 服务器。

图 32-6　具有远程 AD 代理的基于广域网的部署

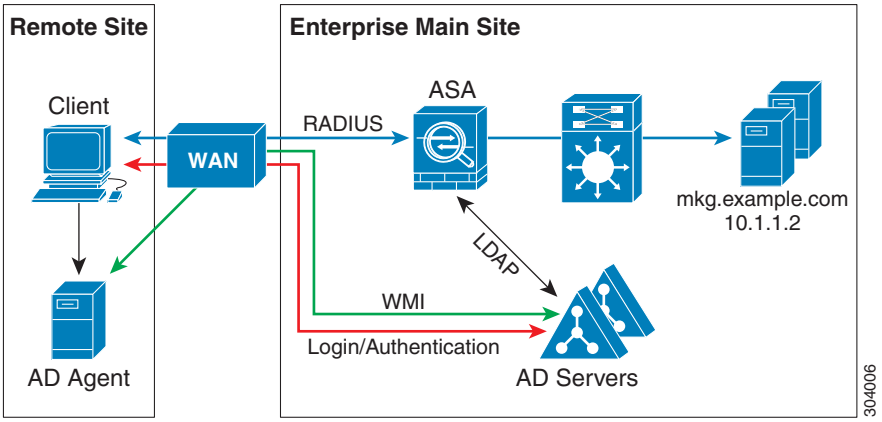
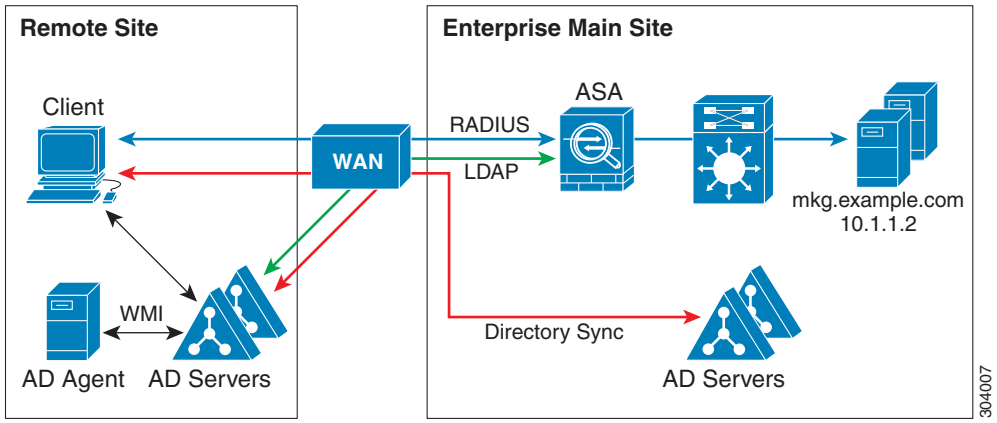


图 32-7 显示扩展的远程站点安装。AD 代理和 Active Directory 服务器安装在远程站点。客户端登录位于主站点的网络资源时，在本地访问这些组件。远程 Active Directory 服务器必须与位于主站点的中央 Active Directory 服务器同步其数据。

图 32-7　具有远程 AD 代理和 AD 服务器的基于广域网的部署



身份防火墙许可

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

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

故障转移准则

- 当启用状态故障转移时，身份防火墙支持从主用设备到备用设备的用户身份 - IP 地址映射和 AD 代理状态复制。但是，仅复制用户身份 - IP 地址映射、 AD 代理状态和域状态。用户和用户组记录不会复制到备用 ASA。
- 配置故障转移后，也必须配置备用 ASA 以直接连接至 AD 代理来检索用户组。即使当已为身份防火墙配置 NetBIOS 探测选项，备用 ASA 也不会向客户端发送 NetBIOS 数据包。
- 当主用 ASA 确定客户端处于非活动状态时，信息传播到备用 ASA。用户统计信息不会传播到备用 ASA。
- 配置故障转移后，必须将 AD 代理配置为与主用和备用 ASA 通信。有关在 AD 代理服务器上配置 ASA 的步骤，请参阅 《*Active Directory 代理安装和设置指南*》。

IPv6 准则

- 支持 IPv6。
- AD 代理支持具有 IPv6 地址的终端。它可以接收日志事件中的 IPv6 地址，将其置于缓存中，并通过 RADIUS 消息进行发送。
- 不支持 IPv6 上的 NetBIOS。

附加准则和限制

- 不支持将完整 URL 用作目标地址。
- 对于要运行的 NetBIOS 探测，在 ASA、 AD 代理和客户端之间的网络必须支持 UDP 封装的 NetBIOS 流量。
- 当存在干预路由器时，身份防火墙的 MAC 地址检查不起作用。登录同一路由器之后的客户端的用户具有相同的 MAC 地址。通过使用此实现，来自同一路由器的所有数据包都可以通过检查，这是因为 ASA 无法确定路由器之后的实际 MAC 地址。
- 以下 ASA 功能不支持在扩展 ACL 中使用基于身份的对象和 FQDN：
  - 路由映射
  - 加密映射
  - WCCP
  - NAT
  - 组策略 （除 VPN 过滤器外）
  - DAP

- 您可以使用 **user-identity update active-user-database** 命令主动发起从 AD 代理进行的用户 - IP 地址下载。

  根据设计，如果以前的下载会话已完成， ASA 将不允许再次发出此命令。

  因此，如果用户 - IP 数据库非常大，以前的下载会话仍未完成，并且，您发出另一个 **user-identity update active-user-database** 命令，系统将显示以下错误消息：

  ```
  "ERROR: one update active-user-database is already in progress."
  ```

  您需要等到上次会话完全结束，然后才可以发出另一个 **user-identity update active-user-database** 命令。

  此行为另一个示例的发生是由于从 AD 代理到 ASA 的数据包丢失。

  当发出 **user-identity update active-user-database** 命令时，ASA 要求提供要下载的用户 - IP 映射条目的总数。然后， AD 代理发起与 ASA 的 UDP 连接，并发送授权请求数据包的更改信息。

  如果由于某种原因导致数据包丢失，ASA 也就无法识别这一点。因此，ASA 会保持会话 4 到 5 分钟。在此期间，如果您已发出 **user-identity update active-user-database** 命令，系统将继续显示错误消息。

- 将 Cisco Context Directory Agent (CDA) 与 ASA 或 Cisco Ironport Web Security Appliance (WSA) 配合时，请确保打开以下端口：
  - UDP 身份验证端口 - 1645
  - UDP 记帐端口 - 1646
  - UDP 侦听端口 - 3799

    侦听端口用于从 CDA 向 ASA 或 WSA 发送授权更改请求。
- 对于域名，以下字符无效：\:*?"<>|。有关命名约定，请参阅 http://support.microsoft.com/kb/909264。
- 对于用户名，以下字符无效：\[]:;=,+*?"<>|@。
- 对于用户组名，以下字符无效：\[]:;=,+*?"<>|。

先决条件

在 ASA 中配置身份防火墙之前，必须满足 AD 代理和 Microsoft Active Directory 的先决条件。

AD 代理

- AD 代理必须安装在可通过 ASA 访问的 Windows 服务器上。此外，您必须将 AD 代理配置为从 Active Directory 服务器获取信息并与 ASA 通信。
- 支持的 Windows 服务器包括 Windows 2003、 Windows 2008 和 Windows 2008 R2。

注　对于 AD 代理服务器来说，不支持 Windows 2003 R2。

- 关于安装和配置 AD 代理的步骤，请参阅 《*Active Directory 代理安装和设置指南*》。
- 在 ASA 中配置 AD 代理之前，请获取 AD 代理和 ASA 用于通信的密钥值。该值必须在 AD 代理和 ASA 上均匹配。

Microsoft Active Directory

- Microsoft Active Directory 必须安装在 Windows 服务器上，并且可通过 ASA 访问。支持的版本包括 Windows 2003、 2008 和 2008 R2 服务器。
- 在 ASA 上配置 Active Directory 服务器之前，请在 Active Directory 中创建用于 ASA 的用户帐户。
- 此外，ASA 通过使用在 LDAP 上启用的 SSL 向 Active Directory 服务器发送加密的登录信息。在 Active Directory 服务器上必须启用 SSL。有关如何启用 Active Directory 的 SSL，请参阅 Microsoft Active Directory 的文档。

注　在运行 AD 代理安装程序之前，必须在 AD 代理监控的每个 Microsoft Active Directory 服务器上安装 *README First for the Cisco Active Directory Agent* 中列出的补丁。即使当 AD 代理直接安装在域控制器服务器上时，这些补丁也是必需的。

配置身份防火墙

本节包含以下：

配置身份防火墙任务流程

要配置身份防火墙，请执行以下任务：

步骤 1　在 ASA 中配置 Active Directory 域。

请参阅第 32-10 页的配置 Active Directory 域和第 32-10 页的配置 Active Directory 服务器组。

关于部署 Active Directory 服务器以满足环境要求的方式，另请参阅第 32-4 页的部署方案。

步骤 2　在 ASA 中配置 AD 代理。

请参阅第 32-10 页的配置 Active Directory 服务器组和第 32-11 页的配置 Active Directory 代理组。

关于部署 AD 代理以满足环境要求的方式，另请参阅第 32-4 页的部署方案。

步骤 3　配置身份选项。

请参阅第 32-12 页的配置身份选项。

步骤 4　配置基于身份的安全策略。在配置 AD 域和 AD 代理后，您可以创建将用在许多功能中的基于身份的对象组和 ACL。

请参阅第 32-14 页的配置基于身份的安全策略。

配置 Active Directory 域

为使 ASA 在从 AD 代理接收 IP - 用户映射时可以从特定域下载 Active Directory 组和接受用户身份，在 ASA 上的 Active Directory 域配置是必需的。

先决条件

- Active Directory 服务器 IP 地址
- LDAP 基础 DN 的可分辨名称
- 身份防火墙用于连接 Active Directory 域控制器的 Active Directory 用户的可分辨名称和密码

要配置 Active Directory 域，请执行以下步骤：

步骤 1　选择 **Configuration > Firewall > Identity Options**。

步骤 2　如有必要，请选中 **Enable User Identity** 复选框启用用户身份。

步骤 3　在 Domains 部分，请点击 **Add**，或从列表中选择一个域，并点击 **Edit**。

系统将显示 Domain 对话框。

步骤 4　在 Domain NETBIOS Name 字段中，输入一个名称 （最多 32 个字符，由 [a-z]、 [A-Z]、 [0-9]、 [!@#$%^&()-_=+[]{};,.] 组成，第一个字符不能为 . 和空格）。如果域名包含空格，则必须用引号将该空格字符引起来。域名不区分大小写。

在编辑现有域名时，与现有用户和用户组相关的域名不会更改。

步骤 5　从 AD 服务器组列表中，选择与该域相关联的 Active Directory 服务器或点击 **Manage** 以将新服务器组添加到列表中。请参阅第 32-10 页的配置 Active Directory 服务器组。

步骤 6　点击 **OK** 保存域设置并关闭该对话框。

后续操作

请参阅第 32-10 页的配置 Active Directory 服务器组和第 32-11 页的配置 Active Directory 代理组。

配置 Active Directory 服务器组

要配置 Active Directory 服务器组，请执行以下步骤：

步骤 1　选择 **Configuration > Firewall > Identity Options > Add > Manage**。

系统将显示 Configure Active Directory Server Groups 对话框。

步骤 2　要为身份防火墙添加 Active Directory 服务器组，请点击 **Add**。

系统将显示 Add Active Directory Server Group 对话框。

步骤 3　要将服务器添加到 Active Directory 服务器组，请从 Active Directory 服务器组列表中选择该组，然后点击 **Add**。

系统将显示 Add Active Directory Server 对话框。

步骤 4　点击 **OK** 保存设置并关闭该对话框。

后续操作

请参阅第 32-11 页的配置 Active Directory 代理和第 32-11 页的配置 Active Directory 代理组。

配置 Active Directory 代理

先决条件

确保在配置 AD 代理之前具备以下信息：

- AD 代理 IP 地址
- ASA 和 AD 代理之间的共享密钥

要配置 AD 代理，请执行以下步骤：

步骤 1　选择 **Configuration > Firewall > Identity Options**。

步骤 2　如有必要，请选中 **Enable User Identity** 复选框启用此功能。

步骤 3　在 Active Directory Agent 部分，点击 **Manage**。

系统将显示 Configure Active Directory Agents 对话框。

步骤 4　要添加 AD 代理，请点击 **Add** 按钮。或者，从列表中选择代理组，然后点击 **Edit**。

要继续，请参阅第 32-11 页的配置 Active Directory 代理组。

步骤 5　点击 **OK**，保存更改。

后续操作

配置 AD 代理组。请参阅第 32-11 页的配置 Active Directory 代理组。

配置身份防火墙的访问规则。请参阅第 32-14 页的配置基于身份的安全策略。

配置 Active Directory 代理组

为 AD 代理服务器组配置主要和辅助 AD 代理。当 ASA 检测到主要 AD 代理不响应，并已指定辅助代理，ASA 将切换到辅助 AD 代理。AD 代理的 Active Directory 服务器将 RADIUS 用作通信协议；因此，您应该指定 ASA 和 AD 代理之间的共享密钥的关键属性。

要配置 AD 代理组，请执行以下步骤：

步骤 1　从 Configure Active Directory Agents 对话框中点击 **Add**。

系统将显示 Add Active Directory Agent Group 对话框。

步骤 2　输入 AD 代理组名称。

步骤 3　从 Primary Active Directory Agent 部分指定 ASA 在其上侦听来自 AD 代理服务器的流量的接口，然后输入服务器或 IP 地址的 FQDN。

步骤 4　在 Primary Active Directory Agent 部分，请输入超时间隔和在 AD 代理不响应时 ASA 将继续尝试联系 AD 代理的重试间隔。

步骤 5　输入主要 AD 代理和 ASA 之间使用的共享密钥。

步骤 6　从 Secondary Active Directory Agent 部分指定 ASA 在其上侦听来自 AD 代理服务器的流量的接口，然后输入服务器的 FQDN 或 IP 地址。

步骤 7　在 Secondary Active Directory Agent 部分，请输入超时间隔和在 AD 代理不响应时 ASA 将继续尝试联系 AD 代理的重试间隔。

步骤 8　输入辅助 AD 代理和 ASA 之间使用的共享密钥。

步骤 9　点击 **OK** 保存更改并关闭该对话框。

后续操作

配置身份防火墙的访问规则。请参阅第 32-14 页的配置基于身份的安全策略。

配置身份选项

使用此窗格来添加或编辑身份防火墙功能；选中 **Enable** 复选框启用此功能。默认情况下，身份防火墙功能被禁用。

先决条件

在为身份防火墙配置身份选项之前，满足 AD 代理和 Microsoft Active Directory 的先决条件。有关 AD 代理和 Microsoft Active Directory 安装的要求，请参阅第 32-8 页的先决条件。

要配置身份防火墙的身份选项，请执行以下步骤：

步骤 1　选择 **Configuration > Firewall > Identity Options**。

步骤 2　如有必要，请选中 **Enable User Identity** 复选框启用此功能。

步骤 3　要为身份防火墙添加一个域，请点击 **Add** 显示 Add Domain 对话框。

步骤 4　要继续，请参阅第 32-10 页的配置 Active Directory 域。

步骤 5　对于已添加到 Domains 列表中的域，选中当域因为 Active Directory 域控制器未响应而关闭时是否禁用规则。

当域关闭且为该域选中此选项时， ASA 禁用与该域中的用户关联的用户身份规则。此外，该域内所有用户 IP 地址的状态在 Monitoring > Properties > Identity > Users 窗格中都标记为禁用。

步骤 6　从 Default Domain 下拉列表中选择用于身份防火墙的默认域。

当没有为所有用户或用户组明确配置域时，所有用户和用户组都使用默认域。当未指定默认域时，用户和组的默认域是 LOCAL。

此外，身份防火墙为所有本地定义的用户组或本地定义的用户 （通过使用 VPN 或网络门户登录和进行身份验证的用户）使用 LOCAL 域。

注　选择的默认域名必须与在 Active Directory 域控制器上配置的 NetBIOS 域名相匹配。如果域名不匹配， AD 代理会错误地将用户 - IP 映射与在配置 ASA 时输入的域名相关联。要查看 NetBIOS 域名，请在任意文本编辑器中打开 Active Directory 用户事件安全日志。

对于多情景模式，您可以为每个情景以及在系统执行空间中设置一个默认域名。

步骤 7　在 Active Directory Agent 部分，请从下拉列表中选择 AD 代理组。要添加 AD 代理组，请点击 **Manage**。有关详细信息，请参阅第 32-11 页的配置 Active Directory 代理。

步骤 8　在 Hello Timer 字段中输入秒数，范围从 10 到 65535。

在 ASA 与 AD 代理之间的 hello 计时器定义 ASA 交换 Hello 数据包的频率。ASA 使用 hello 数据包来获取 ASA 复制状态 （保持同步或失去同步）和域状态 （运行或关闭）。如果 ASA 未收到来自 AD 代理的响应，则会在指定的时间间隔后重新发送 hello 数据包。

指定 ASA 将继续发送 hello 数据包到 AD 代理的次数。默认情况下，秒数设置为 30 秒，重试次数设置为 5 次。

步骤 9　选中 **Enable Event Timestamp** 复选框使 ASA 能够持续跟踪它收到的用于每个标识符的上一个事件时间戳，并能够在事件时间戳晚于 ASA 的时钟至少 5 分钟的情况下，或者，如果其时间戳早于上一个事件时间戳时，丢弃任何消息。

对于最近启动的不知道上一个事件时间戳的 ASA，ASA 会将事件时间戳与自己的时钟进行比较。如果事件至少是在 5 分钟之前， ASA 将不接受该消息。

我们建议您将 ASA、Active Directory 和 Active Directory 代理配置为使用 NTP 来同步它们之间的时钟。

步骤 10　在 Poll Group Timer 字段中，请输入 ASA 用于查询 DNS 服务器解析完全限定域名 (FQDN) 的小时数。默认情况下，轮询计时器设置为 4 小时。

步骤 11　在 Retrieve User Information 中，请从列表中选择一个选项：

- On Demand - 指定当 ASA 接收到要求新连接的数据包并且其源 IP 地址的用户没有位于用户身份数据库中时， ASA 将从 AD 代理检索 IP 地址的用户映射信息。
- Full-download - 指定 ASA 向 AD 代理发送请求以在 ASA 开始时下载整个 IP - 用户映射表，然后在用户登录和注销时接收递增的 IP - 用户映射信息。

注　选择 On Demand 的优点是使用较少的内存，因为只查询和存储接收到的数据包的用户。

步骤 12　在 Error Conditions 部分，选择如果 AD 代理没有响应是否禁用规则。

当 AD 代理关闭，并且已选择此选项时， ASA 将禁用与该域中用户关联的用户身份规则。此外，该域内所有用户 IP 地址的状态在 Monitoring > Properties > Identity > Users 窗格中都标记为禁用。

步骤 13　在 Error Conditions 部分，选择在 NetBIOS 探测失败时是否移除用户的 IP 地址。

选择此选项可指定当到用户的 NetBIOS 探测阻塞 （例如，用户客户端不响应 NetBIOS 探测）时的操作。到该客户端的网络连接可能阻塞或客户端处于非活动状态。选择此选项时， ASA 禁用与该用户 IP 地址关联的身份规则。

步骤 14　在 Error Conditions 部分，选择当用户的 MAC 地址与 ASA 当前已映射到该 MAC 地址的 IP 地址不一致时是否移除用户的 MAC 地址。选中此选项时， ASA 禁用与特定用户关联的用户身份规则。

步骤 15　在 Error Conditions 部分，选择是否跟踪未找到的用户。

步骤 16　在 Users 部分，选择 Idle Timeout 选项并输入一个时间 （以分钟为单位，范围从 1 到 65535 分钟）。默认情况下，空闲超时设置为 60 分钟。

启用此选项配置在活动用户被认为空闲时的计时器，这意味着 ASA 在超过指定时间后不会接收到来自该用户 IP 地址的流量。在计时器到期后，用户的 IP 地址标记为非活动状态，并从本地缓存的 IP - 用户数据库中移除， ASA 不再通知有关该 IP 地址的 AD 代理。仍然允许现有流量通过。当启用 Idle Timeout 选项后，即使当 NetBIOS Logout Probe 已配置时， ASA 也运行非活动计时器。

注　Idle Timeout 选项不适用于 VPN 或直接转发代理用户。

步骤 17　在 NetBIOS Logout Probe 部分，启用 NetBIOS 探测并设置探测到用户 IP 地址前的探测计时器（1 到 65535 分钟）和重试探测之间的重试间隔 （1 到 256 次重试）。

启用此选项配置 ASA 探测用户主机以确定用户客户端是否仍旧处于活动状态的频率。为了最小化 NetBIOS 数据包，当用户已空闲超过 Idle Timeout 分钟字段中指定的分钟数时，ASA 仅向客户端发送一个 NetBIOS 探测。

步骤 18　在 NetBIOS Logout Probe 部分，请从 User Name 列表中选择一个选项：

- Match Any - 只要来自主机的 NetBIOS 响应包含分配到 IP 地址的用户的用户名，用户身份就被视为有效。指定此选项要求主机启用 Messenger 服务并配置 WINS 服务器。
- Exact Match - 分配到 IP 地址的用户的用户名在 NetBIOS 响应中必须唯一。否则，该 IP 地址的用户身份就被视为无效。指定此选项要求主机启用 Messenger 服务并配置 WINS 服务器。
- User Not Needed - 只要 ASA 接收到来自主机的 NetBIOS 响应，用户身份就被视为有效。

步骤 19　点击 **Apply** 保存身份防火墙配置。

后续操作

配置 Active Directory 域和服务器组。请参阅第 32-10 页的配置 Active Directory 域和第 32-10 页的配置 Active Directory 服务器组。

配置 AD 代理。请参阅第 32-10 页的配置 Active Directory 服务器组。

配置基于身份的安全策略

您可以在许多 ASA 功能中纳入基于身份的策略。任何使用扩展 ACL 的功能（除了在第 32-7 页的准则和限制中列为不支持的 ACL）都可以利用身份防火墙。现在，您可以将用户身份参数添加到扩展 ACL 中，并添加基于网络的参数。

可以使用身份的功能包括以下内容：

- 访问规则 - 访问规则利用网络信息允许或拒绝接口上的流量。借助身份防火墙，您可以基于用户身份控制访问。请参阅防火墙配置指南。
- AAA 规则 - 身份验证规则 （也称为直接转发代理）基于用户控制网络访问。由于此功能非常类似于访问规则加上身份防火墙，因此 AAA 规则现在可以用作用户 AD 登录超时情况下的身份验证备份方法。例如，对于无有效登录的任何用户，您可以触发 AAA 规则。要确保 AAA 规则仅对无有效登录的用户触发，您可以在用于访问规则和 AAA 规则的扩展 ACL 中指定特殊用户名：None （无有效登录的用户）和 Any （有有效登录的用户）。在访问规则中，请照常为用户和组配置策略，但是，包括允许所有 None 用户的 AAA 规则；必须允许这些用户，以便他们以后可以触发 AAA 规则。然后，配置拒绝 Any 用户的 AAA 规则（这些用户将不受 AAA 规则的限制，并已由访问规则处理），但是 AAA 规则允许所有 None 用户。例如：

```
access-list 100 ex permit ip user CISCO\xyz any any
access-list 100 ex deny ip user CISCO\abc any any
access-list 100 ex permit ip user NONE any any
access-list 100 ex deny any any
access-group 100 in interface inside

access-list 200 ex deny ip user ANY any any
access-list 200 ex permit user NONE any any
aaa authenticate match 200 inside user-identity
```

有关详细信息，请参阅旧版功能指南。

- 云网络安全 - 可以控制将哪些用户发送给云网络安全代理服务器。此外，您可以在基于用户组（包含在发送到云网络安全的 ASA 流量报头中）的云网络安全 ScanCenter 上配置策略。请参阅防火墙配置指南。
- VPN 过滤器 - 虽然 VPN 一般不支持身份防火墙 ACL，但您可以将 ASA 配置为在 VPN 流量上执行基于身份的访问规则。默认情况下， VPN 流量不受访问规则限制。您可以强制 VPN 客户端遵守使用身份防火墙 ACL 的访问规则（使用 **no sysopt connection permit-vpn** 命令）。还可以使用具有 VPN 过滤器功能的身份防火墙 ACL； VPN 过滤器一般实现与访问规则相似的效果。

监控身份防火墙

监控 AD 代理

要监控身份防火墙的 AD 代理组件，请执行以下步骤：

步骤 1　选择 **Monitoring > Properties > Identity > AD Agent**。

步骤 2　点击 **Refresh** 更新窗格中的数据。

此窗格显示有关主要和辅助 AD 代理的以下信息：

- AD 代理状态
- 域状态
- AD 代理统计信息

监控组

要监控为身份防火墙配置的用户组，请执行以下步骤：

步骤 1　选择 **Monitoring > Properties > Identity > Group**。

步骤 2　要显示使用选定组的访问规则的列表，请点击 **Where used**。

步骤 3　点击 **Refresh** 更新窗格中的数据。

此窗格以 *domain\group_name* 格式显示用户组列表。

监控身份防火墙的内存使用情况

要监控身份防火墙在 ASA 消耗的内存使用情况，请执行以下步骤：

步骤 1　选择 **Monitoring > Properties > Identity > Memory Usage**。

步骤 2　点击 **Refresh** 更新窗格中的数据。

此窗格显示身份防火墙中各种模块的内存使用情况 （以字节为单位）：

- 用户
- 组
- 用户状态
- LDAP

  ASA 发送对在 Active Directory 服务器中配置的 Active Directory 组的 LDAP 查询。 Active Directory 服务器对用户进行身份验证并生成用户登录安全日志。
- AD 代理
- 其他
- 总内存使用情况

注　如何配置身份防火墙以从 AD 代理检索用户信息会影响功能所使用的内存量。您可以指定 ASA 是使用按需检索还是全部下载检索。选择按需检索的优点是使用较少的内存，因为只查询和存储接收到的数据包的用户。有关详细信息，请参阅第 32-12 页的配置身份选项。

监控身份防火墙用户

要显示有关包含在身份防火墙所使用的用户 IP - 用户映射数据库中包含的所有用户的信息，请执行以下步骤：

步骤 1　选择 **Monitoring > Properties > Identity > User**。

注　活动用户以绿色突出显示。

步骤 2　要显示有关活动用户的其他信息，请从列表中选择用户并点击 **Details**。Details 按钮仅对活动用户启用。

步骤 3　要使用选定的用户显示访问规则的列表，请点击 **Where used**。

步骤 4　点击 **Refresh** 更新窗格中的数据。

此窗格显示用户的以下信息：

domain\user_name　状态 （活动或非活动）　连接数　空闲分钟数

默认域名可以是实时域名、特殊保留词或 LOCAL。对于所有本地定义的用户组或本地定义的用户 （通过使用 VPN 或网络门户登录和进行身份验证的用户），身份防火墙使用 LOCAL 域名。当未指定默认域时，默认域名为 LOCAL。

基于每个用户而不是使用用户的 IP 地址存储空闲时间。

如果在 Active Directory 服务器关闭或域关闭时禁用规则的选项，或者在 AD 代理中的禁用规则选项无效而且 AD 代理关闭，则所有已登录用户都处于禁用状态。您可以在 Identity Options 窗格中配置这些选项。

或者，您可以通过访问 Firewall Dashboard 窗格查看用户的统计信息。 Firewall Dashboard 选项卡可用于查看有关通过 ASA 的流量的重要信息。选择 **Home > Firewall Dashboard > Top Usage Statistics > Top 10 Users** 选项卡。

只有当在 ASA 中配置了身份防火墙功能时，其中包括配置这些其他组件 - Microsoft Active Directory 和 Cisco Active Directory (AD) 代理， Top 10 Users 选项卡才显示数据。有关详细信息，请参阅第 32-9 页的配置身份防火墙。

根据选择的选项，Top 10 Users 选项卡显示有关前 10 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。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　Top Usage Status 区域的前三个选项卡显示威胁检测数据，与身份防火墙功能无关。

身份防火墙的功能历史记录

表 32-1 列出了此功能的版本历史记录。 ASDM 可向后兼容多个平台版本，因此，未列出已添加支持的具体 ASDM 版本。

表 32-1　身份防火墙的功能历史记录

功能名称	版本	功能信息
身份防火墙	8.4(2)	我们引入了身份防火墙功能。 我们引入或修改了以下屏幕： Configuration > Firewall > Identity Options Configuration > Firewall > Objects > Local User Groups Monitoring > Properties > Identity.

ASA 和思科 TrustSec

关于集成思科 TrustSec 的 ASA

关于思科 TrustSec

通常，防火墙等安全功能根据预定义的 IP 地址、子网和协议执行访问控制。然而，随着企业不断向无边界网络过渡，用于连接人员和公司的技术以及对数据和网络保护的安全要求有了长足的发展。同时，终端变得越来越具流动性，而且用户通常利用各种终端 （例如，笔记本电脑 （而非台式机）、智能手机或平板电脑），这样用户属性结合终端属性一起提供了关键特征 （除了现有的基于 6 元组的规则以外），带防火墙功能的交换机和路由器或专用防火墙等实施设备能够可靠地利用这些关键特征制定访问控制决策。

因此，对于支持跨客户网络、在网络的接入层、分发层和核心层以及在数据中心实现安全性，终端属性或客户端身份属性的可用性和传送性已经成为越来越重要的要求。

思科 TrustSec 可以提供基于现有的身份感知基础设施的访问控制，确保网络设备之间的数据保密性，并集成平台上的安全访问服务。在思科 TrustSec 功能中，实施设备结合用户属性和终端属性制定基于角色和基于身份的访问控制决策。此信息的可用性和传送性支持在网络的接入层、分发层和核心层实现跨网络安全性。

在环境中实施思科 TrustSec 具备以下优势：

- 支持越来越具移动性和复杂的劳动力可以从任意设备进行适当并更安全的访问
- 针对正在连接有线或无线网络的人员和设备提供全面的可视性，降低安全风险
- 针对访问物理或云计算型的 IT 资源的网络用户的活动提供优越控制
- 通过集中化、高度安全的访问策略管理和可扩展的实施机制降低总体拥有成本

有关在各种思科产品上使用思科 TrustSec 功能的详细信息，请参阅第 33-22 页的附加参考资料。

思科 TrustSec 中的 SGT 和 SXP 支持

在思科 TrustSec 功能中，安全组访问可以将拓扑感知网络转换为基于角色的网络，支持在基于角色的访问控制 (RBAC) 的基础上实施端到端策略。在身份验证期间获得的设备和用户凭证用于按安全组对数据包进行分类。每个进入思科 TrustSec 云的数据包被标记有安全组标记 (SGT)。这种标记有助于可信的中间设备识别数据包的源身份，沿着数据路径实施安全策略。当 SGT 被用于定义安全组 ACL 时， SGT 可以指明域上的权限级别。

SGT 通过 IEEE 802.1X 身份验证、网络身份验证或 MAC 身份验证旁路 (MAB) 被分配到设备，被分配的同时带有 RADIUS 供应商特定属性。SGT 可以被静态地分配给特定 IP 地址或交换机接口。在成功进行身份验证之后， SGT 可以被动态地传送到交换机或访问点。

安全组交换协议 (SXP) 一种为思科 TrustSec 开发的协议，用以在不具有 （支持 SGT 的）硬件支持的网络设备上将 IP--to-SGT 映射数据库传送到支持 SGT 和安全组 ACL 的硬件。SXP 为一种控制层面协议，可以将 IP-SGT 映射从身份验证点 （例如，旧版接入层交换机）传送到网络中的上游设备。

SXP 连接为点到点的连接，使用 TCP 作为底层传输协议。 SXP 使用众所周知的 TCP 端口号 64999 发起连接。此外， SXP 连接唯一可通过源 IP 地址和目标 IP 地址被识别。

思科 TrustSec 功能中的角色

为了提供基于身份和策略的访问实施，思科 TrustSec 功能包含以下角色：

- 访问请求者 (AR) - 访问请求者指的是请求访问网络中受保护资源的终端设备。它们是架构的主要主体，其访问权限视身份凭证而定。

  访问请求者包括终端设备，例如 计算机、笔记本电脑、移动电话、打印机、摄像机和支持 MACsec 功能的 IP 电话。

- 策略决定点 (PDP) - 策略决定点负责制定访问控制决策。PDP 可以提供 802.1x、MAB 和网络身份验证等功能。 PDP 通过 VLAN、 DACL 和安全组访问 (SGACL/SXP/SGT) 支持身份验证和实施。

  在思科 TrustSec 功能中，思科身份服务引擎 (ISE) 可充当 PDP。思科 ISE 提供身份和访问控制策略功能。

- 策略信息点 (PIP) - 策略信息点是向策略决策点提供外部信息 （例如，信誉、位置和 LDAP 属性）的源。

  策略信息点包括 Session Directory、 Sensor IPS 和 通信管理器等设备。

- 策略管理点 (PAP) - 策略管理点定义策略并将策略插入授权系统。PAP 提供思科 TrustSec 标记到用户身份映射和思科 TrustSec 标记到服务器资源映射，充当一个身份资源库。

  在思科 TrustSec 功能中，思科安全访问控制系统 （带集成式 802.1x 和 SGT 支持的策略服务器）充当 PAP。

- 策略实施点 (PEP) - 策略实施点是实施 PDP 为每个 AR 制定的决策 （策略规则和操作）的实体。 PEP 设备通过网络上的主要通信路径获悉身份信息。 PEP 设备从多个来源获悉每个 AR 的身份属性，例如终端代理、授权服务器、对等实施设备和网络流量。反过来， PEP 设备使用 SXP 将 IP-SGT 映射传送到网络上相互信任的对等设备。

  策略实施点包括多种网络设备，例如 Catalyst 交换机、路由器、防火墙 （具体是指 ASA）、服务器、 VPN 设备和 SAN 设备。

思科 ASA 在身份架构中为 PEP 角色提供服务。ASA 采用 SXP 直接从身份验证点获悉身份信息，并利用这些信息实施基于身份的策略。

安全组策略实施

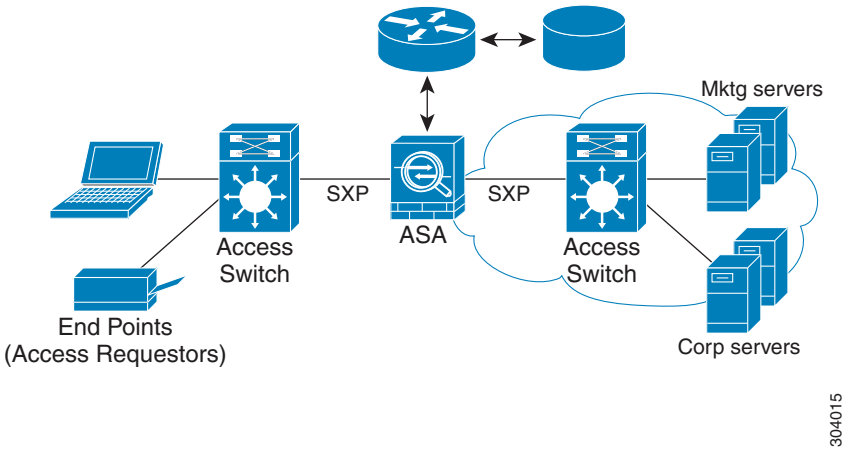
安全策略实施基于安全组名称进行。终端设备尝试访问数据中心中的资源。与在防火墙上配置的基于 IP 的传统策略相比，基于身份的策略基于用户和设备身份配置。例如，允许市场营销承包商访问市场营销服务器；允许市场营销公司用户访问市场营销服务器和公司服务器。

此类部署的优点包括：

- 使用单一对象 (SGT) 简化策略管理定义和实施用户组与资源。
- 在支持思科 TrustSec 的交换机基础设施中保留用户身份和资源身份。

图 33-1 显示了基于安全组名称的策略实施部署。

图 33-1　　基于安全组名称的策略实施部署



通过实施思科 TrustSec，您可以配置支持服务器分类的安全策略，并且实现以下功能：

- 可以将 SGT 分配给服务器池，以简化策略管理。
- SGT 信息保留在支持思科 TrustSec 的交换机的基础设施中。
- ASA 可以使用 IP-SGT 映射，在思科 TrustSec 域上实施策略。
- 服务器强制要求 802.1x 授权，由此可能简化部署。

ASA 如何实施基于安全组的策略

注　ASA 上同时允许基于用户的安全策略和基于安全组的策略。网络属性、基于用户的属性和基于安全组的属性的任意组合都能够在安全策略中配置。有关配置基于用户的安全策略的详细信息，请参阅第 32 章，“身份防火墙”。

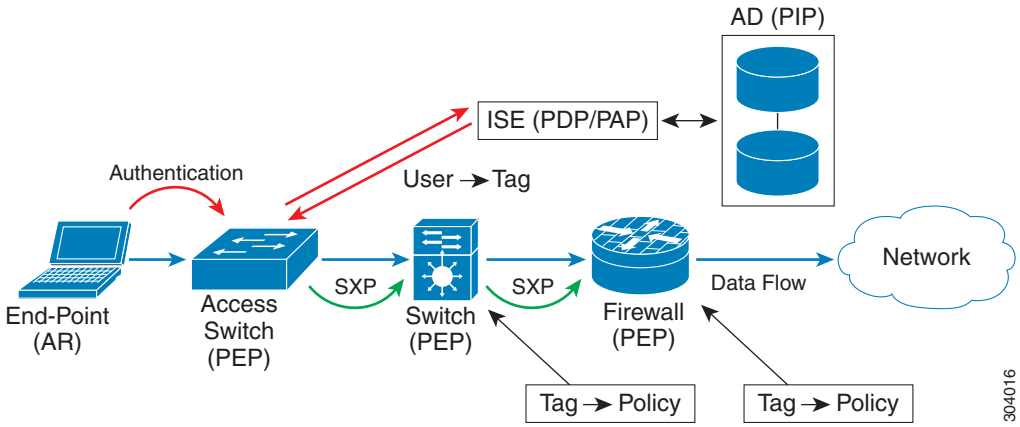
要配置 ASA 与思科 TrustSec 配合使用，您必须从 ISE 导入受保护访问凭证 (PAC) 文件。有关详细信息，请参阅第 33-14 页的导入 PAC 文件。

将 PAC 文件导入 ASA，在 ASA 与 ISE 之间建立安全的通信信道。信道建立之后， ASA 发起与 ISE 之间的 PAC 安全 RADIUS 事务，下载思科 TrustSec 环境数据（即安全组表）。此安全组表将 SGT 映射到安全组名称。安全组名称在 ISE 上创建，为安全组提供用户友好的名称。

首次下载安全组表时， ASA 会浏览表中的所有条目，解析已在 ASA 上配置的安全策略包含的所有安全组名称；然后， ASA 在本地激活这些安全策略。如果无法解析安全组名称， ASA 会为未知安全组名称生成一条系统日志消息。

图 33-2 显示如何在思科 TrustSec 中实施安全策略。

图 33-2　　安全策略实施



1. 终端设备直接或通过远程访问连接到接入层设备，并使用思科 TrustSec 进行身份验证。
2. 通过使用 802.1X 或网络身份验证等身份验证方法，接入层设备可以利用 ISE 对终端设备进行身份验证。终端设备传送角色和组成员信息，将此设备划分至相应的安全组。
3. 接入层设备使用 SXP，将 IP-SGT 映射传送到上游设备。
4. ASA 接收数据包，并利用 SXP 传送的 IP -SGT 映射在 SGT 中查找源 IP 地址和目标 IP 地址。

   如果映射是新映射， ASA 则将其记录在本地 IP-SGT 管理器数据库中。IP-SGT 管理器数据库在控制层面中运行，为每个 IPv4 或 IPv6 地址跟踪 IP-SGT 映射。此数据库记录映射被获悉的源。 SXP 连接的对等 IP 地址可用作映射源。每个 IP-SGT 映射条目都可以有多个源。

   如果 ASA 被配置为 Speaker， ASA 则将所有 IP-SGT 映射条目传输到其 SXP 对等体。有关详细信息，请参阅第 33-6 页的关于 ASA 上的 Speaker 和 Listener 角色。
5. 如果在 ASA 上使用此 SGT 或安全组名称配置安全策略， ASA 则实施此策略。（您可以在 ASA 上创建包含 SGT 或安全组名称的安全策略。为了基于安全组名称实施策略， ASA 需要一个安全组表，以将安全组名称映射到 SGT。）

   如果 ASA 在安全组表中找不到安全组名称，并且安全组名称包含在安全策略中， ASA 则认为此安全组名未知，并生成一条系统日志消息。在 ASA 刷新来自 ISE 的安全组表并获悉安全组名称之后， ASA 会生成一条系统日志消息，指明安全组名称已知。

安全组更改对 ISE 产生的影响

通过从 ISE 下载更新的表， ASA 定期刷新安全组表。在不同的下载之间， ISE 上的安全组会发生更改。直到 ASA 刷新安全组表，这些更改才会在 ASA 上体现出来。

提示　我们建议您在维护窗口期间安排 ISE 上的策略配置更改，然后在 ASA 上手动刷新安全组表，确保安全组更改包含在内。

按这种方式处理策略配置更改，可以最大限度增加安全组名称获得解析和安全策略立即进入活动状态的几率。

当环境数据计时器过期时，系统会自动刷新安全组表。您也可以按需触发安全组表刷新。

如果安全组在 ISE 上发生更改，当 ASA 刷新安全组表时，会发生以下事件：

- 只有使用安全组名称配置的安全组策略才需要通过安全组表进行解析。包含策略组标记的策略始终处于活动状态。
- 当安全组表首次可用时，浏览所有包含安全组名称的策略，解析安全组名称，激活策略。浏览所有包含标记的策略，并为未知标记生成系统日志。
- 如果安全组表已过期，将继续根据最新下载的安全组表实施策略，直到您清楚此表有新表变得可用为止。
- 当解析的安全组名称在 ASA 上变成未知时，它会停用安全策略；然而，此安全策略依然存在于 ASA 运行配置中。
- 如果在 PAP 上删除某个现有安全组，以前已知的安全组标记会变成未知，但在 ASA 上不会发生策略状态更改。以前已知的安全组名称会变成未解析，然后策略被停用。如果安全组名称被重用，则使用新标记重新编译策略。
- 如果在 PAP 上添加新安全组，以前未知的安全组标记会变成已知，会生成系统日志消息，但策略状态不会发生更改。以前未知的安全组名称变成已解析，然后相关联的策略被激活。
- 如果已在 PAP 上重命名标记，使用标记配置的策略会显示新的标记名称，策略状态不会发生更改。使用此新标记值重新编译使用安全组名称配置的策略。

关于 ASA 上的 Speaker 和 Listener 角色

ASA 支持 SXP 向其他网络设备发送和从这些设备接收 IP-SGT 映射条目。 SXP 允许安全设备和防火墙从访问交换机获悉身份信息，无需硬件升级或更改。 SXP 还能够用来将上游设备 （例如，数据中心设备）的 IP-SGT 映射条目重新传送到下游设备。ASA 能够接收来自上游和下游方向的信息。

当在 ASA 上配置到 SXP 对等体的 SXP 连接时，您必须将 ASA 指定为此连接的说话者或收听者，以便它能够交换身份信息：

- 说话者模式 - 配置 ASA，以便它能够将在 ASA 上收集的所有活动 IP-SGT 映射条目转发给上游设备，进行策略实施。
- 收听者模式 - 配置 ASA，以便可以从下游设备 （具备 SGT 功能的交换机）接收 IP-SGT 映射条目，并使用这些信息创建策略定义。

如果将 SXP 连接的一端配置为说话者，必须将另一端配置为 收听者，反之亦然。如果 SXP 连接的两端设备都配置同一角色 （说话者或收听者）， SXP 连接将失败，同时 ASA 将生成一条系统日志消息。

多个 SXP 连接能够获悉已从 IP-SGT 映射数据库下载的 IP-SGT 映射条目。在 ASA 上建立到 SXP 对等体的 SXP 连接后，收听者从说话者下载整个 IP-SGT 映射数据库。此后发生的所有更改仅在网络上出现新设备时被发送。因此， SXP 信息流速率与终端主机对网络进行身份验证的速率成比例。

已通过 SXP 连接获悉的 IP-SGT 映射条目在 SXP IP-SGT 映射数据库中进行维护。可以通过不同 SXP 连接获悉相同映射条目。此映射数据库为每个已获悉的映射条目维护一个副本。同一 IP-SGT 映射值的多个映射条目按获悉映射的连接的对等 IP 地址进行识别。SXP 请求 IP-SGT 管理器在首次获悉新映射时添加映射条目，并在移除 SXP 数据库中的最后副本时移除映射条目。

无论 SXP 连接何时被配置为说话者， SXP 都请求 IP-SGT 管理器将在设备上收集的所有映射条目转发给对等体。当在本地获悉新映射时， IP-SGT 管理器请求 SXP 通过已配置为说话者的连接转发此映射。

将 ASA 配置为 SXP 连接的说话者和收听者会形成 SXP 环路，这意味着，SXP 数据能够被最初传输它的 SXP 对等体接收。

SXP 通信速率

SXP 信息流速率与终端主机对网络进行身份验证的速率成比例。建立 SXP 对等之后，收听者设备从说话者设备下载整个 IP-SGT 数据库。之后，所有更改仅在新设备出现在网络中或者离开网络时被增量发送。另请注意，只有挂接到新设备的访问设备才能对上游设备发起这种增量更新。

换句话说， SXP 协议的通信速率不会高于受限于身份验证服务器能力的身份验证速率。因此，SXP 通信速率不是主要问题。

SXP 计时器

- 重试打开计时器 - 如果设备上有一个 SXP 连接未建立，则触发重试打开计时器。在重试打开计时器过期后，设备浏览整个连接数据库，如果有任何连接处于关闭或 “ 待定 ” 状态，重试打开计时器将重新启动。计时器默认值为 120 秒。 0 值意味着重试计时器不会启动。重试打开计时器继续，直到所有 SXP 连接都建立或重试打开计时器值已被设为 0 为止。
- 删除抑制计时器 - 当收听者上的某个连接被中断时，触发连接特定删除抑制计时器。已获悉的映射条目不会被立即删除，而是一直保留到删除抑制计时器过期。此计时器过期后，这些映射条目将被删除。删除抑制计时器的值被设为 120 秒，该值不可配置。
- 协调计时器 - 如果在删除抑制计时器期间建立 SXP 连接，则对此连接实施批量更新。这意味着，最新映射条目已被获悉，并且被关联到新的连接实例化标识符。定期的连接特定协调计时器在后台启动。当此协调计时器过期时，它将扫描整个 SXP 映射数据库，识别当前连接会话中所有未被获悉的映射条目 （即带有不匹配连接实例化标识符的映射条目），并对这些条目进行标记，以便将它们删除。这些条目在后续协调审核中被删除。协调计时器默认值为 120 秒。 ASA 上不允许设为 0 值，以防止过时条目的停留时间超出指定范围，给策略实施造成意外结果。
- HA 协调计时器 - 启用 HA 时，主用和备用装置的 SXP 映射数据库保持同步。新的主用装置尝试建立到其所有对等体的新 SXP 连接，并获取最新映射条目。 HA 协调计时器可以提供一种识别和移除旧映射条目的方法。该计时器在故障转移后启动，使 ASA 有时间获取最新映射条目。在 HA 协调计时器过期后， ASA 将扫描整个 SXP 映射数据库，识别当前连接会话中所有未被获悉的映射条目。标记有不匹配实例化标识符的映射条目以便删除。此协调机制与协调计时器的协调机制相同。时间值与协调计时器的时间值相同，并且可配置。

在 SXP 对等体终止其 SXP 连接后， ASA 启动删除抑制计时器。只有被指定为收听者的 SXP 对等体才能够终止连接。如果 SXP 对等体在删除抑制计时器运行期间连接， ASA 将启动协调计时器；然后， ASA 更新 IP-SGT 映射数据库，以获悉最新映射。

IP-SGT 管理器数据库

IP-SGT 管理器数据库不会将任何条目从主用装置同步到备用装置。 IP-SGT 管理器数据库接收 IP-SGT 映射条目的每个源都会将其数据库从主用装置同步到备用装置，然后向备用装置上的 IP-SGT 管理器提供最终 IP-SGT 映射。

对于 9.0(1) 版本， IP-SGT 管理器数据库仅从 SXP 源接收 IP-SGT 映射更新。

ASA- 思科 TrustSec 集成的功能

ASA 将思科 TrustSec 作为其基于身份的防火墙功能的一部分。思科 TrustSec 可以提供以下功能：

灵活性

- ASA 可被配置为 SXP 说话者或收听者，或两者。
- ASA 支持将 SXP 用于 IPv6 和支持 IPv6 的网络设备。
- SXP 能够为 IPv4 和 IPv6 地址更改映射条目。
- SXP 终端支持 IPv4 和 IPv6 地址。
- ASA 仅支持 SXP 第 2 版本。
- ASA 可以与支持 SXP 的不同网络设备协商 SXP 版本。 SXP 版本协商消除了对静态版本配置的需求。
- 您可以配置 ASA，使其在 SXP 协调计时器过期时刷新安全组表，您也可以按需下载安全组表。从 ISE 更新 ASA 上的安全组表时，更改将在相应的安全策略中体现出来。
- ASA 根据源字段或目标字段或两者中的安全组名称支持安全策略。您可以根据安全组、 IP 地址、 Active Directory 组 / 用户名和 FQDN 构成的组合，在 ASA 上配置安全策略。

可用性

- 在 ASA 上，您可以在主用 / 主用和主用 / 备用配置中配置基于安全组的策略。
- ASA 可以与专为实现高可用性 (HA) 配置的 ISE 进行通信。
- 您可以在 ASA 上配置多台 ISE 服务器，如果第一台服务器无法访问，它将继续访问第二台服务器，以此类推。然而，如果服务器列表被下载为思科 TrustSec 环境数据的一部分，它将被忽略。
- 如果 ASA 上从 ISE 下载的 PAC 文件过期，并且它无法下载更新的安全组表， ASA 将继续根据最后下载的安全组表实施安全策略，直到 ASA 下载更新的安全组表为止。

集群

- 对于第 2 层网络，所有装置共享同一 IP 地址。当您更改接口地址时，更改的配置将被发送到所有其他装置。当 IP 地址从特定装置的接口更新时，系统会发送一份通知，以更新此装置上的 IP-SGT 本地数据库。
- 对于第 3 层网络，为主装置上的每个接口配置地址池，并将此配置同步到从装置。在主装置上，发送表示 IP 地址已分配给接口的通知，并且更新 IP-SGT 本地数据库。通过利用已同步到从装置的地址池配置 （池中每个接口的第一个地址始终属于主装置），每个从装置上的 IP-SGT 数据库可以使用主装置的 IP 地址来更新。

  当从装置启动时，它会通知主装置。然后，主装置浏览每个接口上的地址池，为向其发送通知的新从装置计算 IP 地址，并更新主装置上的 IP-SGT 本地数据库。此外，主装置还将有关新从装置的信息通知其他从装置。在通知处理过程中，每个从装置都会为新从装置计算 IP 地址，并将此条目添加到每个从装置上的 IP-SGT 本地数据库。所有从装置都具有地址池配置，以此确定 IP 地址值。对于每个接口，按以下方法确定值：

  Master IP + (M-N)，其中：

  M - 最大装置数量 （最多允许 8 个）

  N - 发送通知的从装置号

  当任何接口上的 IP 地址池发生更改时，需要在主装置以及每个其他从装置上的 IP-SGT 本地数据库中重新计算和更新所有从装置和主装置的 IP 地址。需要删除旧 IP 地址，并添加新 IP 地址。

当发生更改的地址池配置被同步到从装置时，在配置更改处理过程中，每个从装置为主装置和每个其他 IP 地址已更改的从装置重新计算 IP 地址，然后删除旧 IP 地址的条目，并添加新 IP 地址。

可扩展性

表 33-1 显示 ASA 支持的 IP-SGT 映射条目数。

表 33-1　IP-SGT 映射条目的容量数

ASA 型号	IP-SGT 映射条目数
带 SSP-10 的 5585-X	18,750
带 SSP-20 的 5585-X	25,000
带 SSP-40 的 5585-X	50,000
带 SSP-60 的 5585-X	100,000

表 33-2 显示 ASA 支持的 SXP 连接数。

表 33-2　SXP 连接

ASA 型号	SXP TCP 连接数
带 SSP-10 的 5585-X	150
带 SSP-20 的 5585-X	250
带 SSP-40 的 5585-X	500
带 SSP-60 的 5585-X	1000

思科 TrustSec 的许可要求

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

使用思科 TrustSec 的先决条件

配置 ASA 使用思科 TrustSec 之前，您必须执行以下任务：

- 第 33-10 页的通过 ISE 注册 ASA
- 第 33-10 页的在 ISE 上创建安全组
- 第 33-10 页的生成 PAC 文件

通过 ISE 注册 ASA

在 ASA 能够成功导入 PAC 文件之前，您必须将 ASA 配置为 ISE 中可识别的思科 TrustSec 网络设备。要通过 ISE 注册 ASA，请执行以下步骤：

1. 登录 ISE。
2. 选择 **Administration > Network Devices > Network Devices**。
3. 点击 **Add**。
4. 输入 ASA 的 IP 地址。
5. 当 ISE 被用于进行用户身份验证时，请在 Authentication Settings 区域输入一个共享密钥。

   在 ASA 上配置 AAA 服务器时，请提供您在 ISE 上创建的共享密钥。 ASA 上的 AAA 服务器使用此共享密钥与 ISE 进行通信。
6. 指定 ASA 的设备名、设备 ID、密码和下载时间间隔。有关如何执行这些任务的详细信息，请参阅 ISE 文档。

在 ISE 上创建安全组

配置 ASA 与 ISE 进行通信时，您需指定 AAA 服务器。在 ASA 上配置 AAA 服务器时，您必须指定服务器组。必须配置安全组，使其使用 RADIUS 协议。要在 ISE 上创建安全组，请执行以下步骤：

1. 登录 ISE。
2. 选择 **Policy > Policy Elements > Results > Security Group Access > Security Group**。
3. 为 ASA 添加安全组。（安全组是全局性的，而非特定于 ASA。）

   ISE 在 Security Groups 下创建带有标记的条目。
4. 在 Security Group Access 区域，为 ASA 配置设备 ID 凭证和密码。

生成 PAC 文件

生成 PAC 文件之前，您必须已通过 ISE 注册 ASA。要生成 PAC 文件，请执行以下步骤：

1. 登录 ISE。
2. 选择 **Administration > Network Resources > Network Devices**。
3. 从设备列表中，选择 ASA。
4. 在 Security Group Access (SGA) 下方，点击 **Generate PAC**。
5. 要加密 PAC 文件，请输入密码。

   为加密 PAC 文件而输入的密码（或加密密钥）独立于在 ISE 上被配置为设备凭证的一部分的密码。

ISE 生成 PAC 文件。ASA 能够通过 TFTP、FTP、HTTP、HTTPS 或 SMB，从闪存或远程服务器导入 PAC 文件。（导入之前， PAC 文件不必驻留在 ASA 闪存上。）

有关 PAC 文件的详细信息，请参阅第 33-14 页的导入 PAC 文件。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

IPv6 准则

支持 IPv6 用于 SXP 终端。

集群准则

支持集群环境中的主装置和从装置。

故障转移准则

通过配置支持服务器列表。如果第一台服务器无法访问， ASA 则尝试连接列表中的第二台服务器，以此类推。然而，被下载为思科 TrustSec 环境数据的一部分的服务器列表将被忽略。

支持主用 / 备用和主用 / 主用情境。接管之后，所有 SXP 数据将被从主用装置复制到备用装置。

附加准则

思科 TrustSec 在单一情景和多情景模式中支持智能报障服务功能，但在系统情景模式中不支持此功能。

限制

- ASA 只能配置为在单一思科 TrustSec 域中进行互操作。
- ASA 不支持设备上的静态 SGT 名称映射配置。
- SXP 消息不支持 NAT。
- SXP 在网络中将 IP-SGT 映射传送到实施点。如果接入层交换机与实施点分属不同的 NAT 域，它上传的 IP-SGT 映射则无效，而且在实施设备上进行的 IP-SGT 映射数据库查找不会显示有效的结果。因此， ASA 无法在实施设备上应用安全组感知安全策略。
- 您可以为 ASA 配置用于 SXP 连接的默认密码，或者选择不使用密码；然而，不支持将连接特定密码用于 SXP 对等体。配置的默认 SXP 密码应当在部署网络中保持一致。如果配置连接特定密码，连接可能会失败，并且显示警告消息。如果使用默认密码配置连接，但未配置默认密码，则结果与不使用密码配置连接时的结果相同。
- 当设备拥有到对等体的双向连接，或者设备是单向连接设备链的一部分时，会形成 SXP 连接环路。（ASA 可以从数据中心的接入层为资源获悉 IP-SGT 映射。 ASA 可能需要将这些标记传送到下游设备。）SXP 连接环路会导致 SXP 消息传输出现意外行为。在 ASA 配置为说话者和收听者的情况下，会发生 SXP 连接回路，使 SXP 数据会被最初传输它的对等体接收。
- 更改 ASA 本地 IP 地址时，您必须确保所有 SXP 对等体已更新其对等体列表。此外，如果 SXP 对等体更改其 IP 地址，您必须确保这些更改在 ASA 上体现出来。
- 不支持自动 PAC 文件配置。 ASA 管理员必须从 ISE 管理界面请求 PAC 文件，并将其导入 ASA。有关 PAC 文件的详细信息，请参阅第 33-10 页的生成 PAC 文件和第 33-14 页的导入 PAC 文件。
- PAC 文件有过期日期。您必须在当前 PAC 文件过期之前导入更新的 PAC 文件；否则， ASA 将无法检索环境数据更新。

- 当安全组在 ISE 上发生更改（例如，被重命名或删除）时， ASA 不会更改任何包含与已更改安全组相关联的 SGT 或安全组名称的 ASA 安全组策略的状态；然而， ASA 会生成系统日志消息，指明这些安全策略已更改。

  请参阅，有关在 ASA 上手动更新安全组表以包含来自 ISE 的更改的详细信息，请参阅第 33-17 页的刷新环境数据。
- 在 ISE 1.0 中不支持组播类型。
- SXP 连接在两个被 ASA 互联的 SXP 对等体之间保持正在初始化状态，如以下示例所示。

  （SXP 对等体 A）- - - - (ASA) - - - （SXP 对等体 B）

  因此，当配置 ASA 与思科 TrustSec 集成时，您必须在 ASA 上启用 no-NAT、no-SEQ-RAND 和 MD5-AUTHENTICATION TCP 选项，配置 SXP 连接。为 SXP 对等体之间以 SXP 端口 TCP 64999 为目标的流量创建 TCP 状态旁路策略。然后，在相应的接口上应用该策略。

  例如，以下命令集显示如何为 TCP 状态旁路策略配置 ASA：

```
access-list SXP-MD5-ACL extended permit tcp h支持路由和透明防火墙模式。ost peerA host
peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

- ASA 5585-X 的硬件架构专门用于以最佳方式加载平衡正则数据包，但采用第 2 层安全组标记实施的内联已标记数据包例外。当 ASA 5585-X 处理传入的内联已标记数据包时，可能会出现明显的性能降级。其他 ASA 平台上的内联已标记数据包以及 ASA 5585-X 上的未标记数据包不会出现这种问题。一种解决方法是卸载访问策略，最大限度地减少进入 ASA 5585-X 的内联已标记数据包，允许交换机处理已标记策略实施。另一种解决方法是使用 SXP，使 ASA 5585-X 能够将 IP 地址映射到安全组标记，无需接收已标记数据包。
- ASASM 不支持第 2 层安全组标记实施。

为思科 TrustSec 集成配置 ASA

为思科 TrustSec 集成配置 AAA 服务器

在配置 ASA 集成思科 TrustSec 的过程中，您必须配置 ASA，使其能够与 ISE 进行通信。

先决条件

- 必须配置参考服务器组，使其使用 RADIUS 协议。如果您将非 RADIUS 服务器组添加到 ASA，配置将失败。
- 如果 ISE 也用于进行用户身份验证，则获取您在通过 ISE 注册 ASA 时在 ISE 上输入的共享密钥。请联系 ISE 管理员，以获取此信息。

要为思科 TrustSec 集成配置 ASA 与 ISE 进行通信，请执行以下步骤：

步骤 1　在 ASDM 主应用窗口中，选择 **Configuration > Firewall > Identity By TrustSec**。

步骤 2　要将服务器组添加到 ASA，请在 Server Group Setup 区域点击 **Manage**，系统将显示 Configure AAA Server Group 对话框。

步骤 3　在 AAA Server Group 字段中，输入在 ISE 上为 ASA 创建的安全组名称。

您在这里指定的服务器组名称必须匹配在 ISE 上为 ASA 创建的安全组名称。如果这两个组名称不匹配， ASA 将无法与 ISE 进行通信。请联系 ISE 管理员，以获取此信息。

步骤 4　从 Protocol 下拉列表中选择 RADIUS。

有关设置 AAA Server Group 对话框中剩余字段的详细信息，请参阅第 29-14 页的配置 RADIUS 服务器组。

步骤 5　点击 **OK**。 ASA 将该组添加到 AAA Server Groups 列表中。

步骤 6　要将服务器添加到组中，请选择您刚刚创建的 AAA 服务器组，在 Servers in the Selected Group 区域（下面的窗格）点击 **Add**。系统将显示 Add AAA Server 对话框。

步骤 7　在 Interface Name 字段中，选择 ISE 服务器驻留的网络接口。

步骤 8　在 Server Name or IP Address 字段中，输入 ISE 服务器的 IP 地址。

有关设置 AAA Server 对话框中剩余字段的详细信息，请参阅第 29-15 页的将 RADIUS 服务器添加到组。

步骤 9　点击 **OK**。 ASA 将 ISE 服务器添加到 AAA 服务器列表中。

步骤 10　点击 **Apply**，保存添加的 ISE 服务器和服务器组，以便与思科 TrustSec 集成。

更改将保存到运行中的配置中。

导入 PAC 文件

将受保护的访问凭证 (PAC) 文件导入 ASA，与 ISE 建立连接。信道建立之后，ASA 发起与 ISE 之间的安全 RADIUS 事务，下载思科 TrustSec 环境数据 （即安全组表）。此安全组表将 SGT 映射到安全组名称。安全组名称在 ISE 上创建，为安全组提供用户友好的名称。

更具体地说，在 RADIUS 事务之前没有建立信道。 ASA 使用 PAC 文件进行身份验证，通过 ISE 发起 RADIUS 事务。

提示　PAC 文件包含一个共享密钥，允许 ASA 和 ISE 保证它们之间的 RADIUS 事务安全可靠。考虑到此密钥的敏感性质，您必须将其安全地存储在 ASA 上。

导入时， PAC 文件被转化为 ASCII HEX 格式，并被发送到处于非交互模式的 ASA 中。成功导入此文件后， ASA 从 ISE 下载思科 TrustSec 环境数据，无需在 ISE 中配置的设备密码。

先决条件

- 在 ASA 能够成功生成 PAC 文件之前，您必须将 ASA 配置为 ISE 中可识别的思科 TrustSec 网络设备。虽然 ASA 能够导入任何 PAC 文件，但 PAC 文件只在被正确配置的 ISE 生成时才能在 ASA 上运行。有关详细信息，请参阅第 33-10 页的通过 ISE 注册 ASA。
- 在 ISE 上生成 PAC 文件时，请获取用于加密此文件的密码。

  ASA 要求此密码，以导入并解密 PAC 文件。
- 访问 ISE 生成的 PAC 文件。ASA 能够通过 TFTP、FTP、HTTP、HTTPS 或 SMB，从闪存或远程服务器导入 PAC 文件。（导入之前， PAC 文件不必驻留在 ASA 闪存上。）
- 已为 ASA 配置了服务器组。

限制

- 当 ASA 成为故障转移配置的一部分时，您必须将 PAC 文件导入主 ASA 设备。
- 当 ASA 成为集群配置的一部分时，您必须将 PAC 文件导入主设备。

要导入 PAC 文件，请执行以下步骤：

步骤 1　在 ASDM 主应用窗口中，选择 **Configuration > Firewall > Identity By TrustSec**。

步骤 2　选中 **Enable Security Exchange Protocol** 复选框，以启用 SXP。

步骤 3　在 Server Group Setup 区域，点击 **Import PAC**。系统将显示 Import PAC 对话框。

步骤 4　在 Filename 字段中，按以下格式之一输入 PAC 文件的路径和文件名：

- disk0：disk0 上的路径和文件名
- disk1：disk1 上的路径和文件名
- flash：闪存上的路径和文件名

步骤 5　在 Password 字段中，输入用于加密 PAC 文件的密码。此密码独立于在 ISE 上配置为设备凭证的一部分的密码。

步骤 6　在 Confirm Password 字段中，重新输入此密码进行确认。

步骤 7　点击 **Import**。

步骤 8　点击 **Apply**，保存更改。

更改将保存到运行中的配置中。

配置安全交换协议

配置安全交换协议 (SXP) 包括在 ASA 中启用此协议，并为 SXP 设置以下默认值：

- SXP 连接的源 IP 地址
- SXP 对等体之间的身份验证密码
- SXP 连接的重试间隔
- 思科 TrustSec SXP 协调期

注　要让 SXP 在 ASA 上运行，至少要有一个接口处于 UP/UP 状态。

目前，当 SXP 已启用且所有接口都关闭时， ASA 不会显示一条指明 SXP 未工作或无法启用的消息。如果您通过输入 **show running-config** 命令来检查配置，此命令输出则显示以下消息：
`"WARNING: SXP configuration in process, please wait for a few moments and try again."`

此消息是通用的，不会指出 SXP 不运行的原因。

要为 ASA 与思科 TrustSec 集成配置默认值，请执行以下步骤：

步骤 1　在 ASDM 主应用窗口中，选择 **Configuration > Firewall > Identity By TrustSec**。

步骤 2　选中 **Enable Security Exchange Protocol** 复选框，以启用 SXP。默认情况下， SXP 被禁用。

在多情景模式中，在用户情景中启用 SXP。

步骤 3　在 Default Source 字段中，输入 SXP 连接的默认本地 IP 地址。此 IP 地址可以是一个 IPv4 或 IPv6 地址。

注　ASA 将 SXP 连接的本地 IP 地址确定为对等体 IP 地址可以访问的传出接口 IP 地址。如果配置的本地地址与传出接口 IP 地址不同，ASA 将无法连接到 SXP 对等体并会生成系统日志消息。

步骤 4　在 Default Password 字段中，输入用于对 SXP 对等体进行 TCP MD5 身份验证的默认密码。默认情况下，不为 SXP 连接设置密码。

您可以将此密码指定为最多 162 个字符的加密字符串，或最多 80 个字符的 ASCII 密钥字符串。配置密码的加密级别为可选操作。如果配置加密级别，您只能设置一个级别：

- Level 0 - 未加密纯文本
- Level 8 - 已加密文本

步骤 5　在 Retry Timer 字段中，输入 ASA 尝试在 SXP 对等体之间建立新 SXP 连接的默认时间间隔。

ASA 继续尝试连接到新 SXP 对等体，直到连接成功为止。只要 ASA 上有一个未建立的 SXP 连接，就会触发重试计时器。

输入重试计时器值，范围为 0 至 64000 秒。如果指定为 0 秒，该计时器永远不会过期， ASA 也不会尝试连接 SXP 对等体。默认情况下， *timer value* 为 120 秒。

当重试计时器过期时， ASA 会浏览连接数据库，如果数据库包含任何已关闭或处于 “ 待处理 ” 状态的连接， ASA 会重新启动重试计时器。

步骤 6　在 Reconcile Timer 字段中，输入协调计时器的默认值。

在 SXP 对等体终止其 SXP 连接后，ASA 启动抑制计时器。如果 SXP 对等体在抑制计时器运行期间连接， ASA 将启动协调计时器；然后， ASA 更新 SXP 映射数据库，以获悉最新映射。

当协调计时器过期时， ASA 将扫描 SXP 映射数据库，以识别旧映射条目 （在上一连接会话中获悉的条目）。 ASA 将这些连接标记为过时条目。当协调计时器过期时， ASA 从 SXP 映射数据库移除这些过时条目。

输入协调计时器值，范围为 1 至 64000 秒。默认情况下， *timer value* 为 120 秒。

注　您无法将计时器值指定为 0 秒，因为该值会阻止协调计时器启动。不允许协调计时器运行的话，会使旧条目保留时间不确定，导致策略实施出现意外结果。

步骤 7　点击 **Apply**，保存默认设置。

更改将保存到运行中的配置中。

添加 SXP 连接对等体

对等体间的 SXP 连接为点到点的连接，使用 TCP 作为底层传输协议。

要添加 SXP 连接对等体，请执行以下步骤：

步骤 1　在 ASDM 主应用窗口中，选择 **Configuration > Firewall > Identity By TrustSec**。

步骤 2　需要的话，选中 **Enable Security Exchange Protocol** 复选框，以启用 SXP。

步骤 3　点击 **Add**。系统将显示 Add Connection 对话框。

步骤 4　在 Peer IP Address 字段中，输入 SXP 对等体的 IPv4 或 IPv6 地址。对等体 IP 地址必须可从 ASA 传出接口进行访问。

步骤 5　（可选）在 Source IP Address 字段中，输入 SXP 连接的本地 IPv4 或 IPv6 地址。指定源 IP 地址为可选操作，然而，指定源 IP 地址可以防止错误配置。

步骤 6　从 Password 下拉列表中，选择下列值之一，指定是否使用 SXP 连接的身份验证密钥：

- default - 使用为 SXP 连接配置的默认密码。

  请参阅第 33-15 页的配置安全交换协议。
- none - 不使用 SXP 连接的密码。

步骤 7　（可选）从 Mode 下拉列表中，选择下列值之一，指定 SXP 连接模式：

- local - 使用本地 SXP 设备。
- peer - 使用对等 SXP 设备。

步骤 8　从 Role 下拉列表中，将 ASA 指定为 SXP 连接的说话者或收听者：

- 说话者 - ASA 可以将 IP-SGT 映射转发到上游设备。
- 收听者 - ASA 可以从下游设备接收 IP-SGT 映射。

请参阅第 33-6 页的关于 ASA 上的 Speaker 和 Listener 角色。

步骤 9　点击 **OK**。对等体将出现在 Connection Peers 列表中。

步骤 10　点击 **Apply** 以保存设置。

更改将保存到运行中的配置中。

刷新环境数据

ASA 可以从 ISE 下载环境数据，其中包括安全组标记 (SGT) 名称表。当您在 ASA 上完成以下任务时， ASA 会自动刷新从 ISE 获取的环境数据。

- 配置 AAA 服务器与 ISE 进行通信。
- 从 ISE 导入 PAC 文件。
- 识别 ASA 将用于检索思科 TrustSec 环境数据的 AAA 服务器组。

通常，您无需手动刷新来自 ISE 的环境数据；然而，安全组会在 ISE 上发生更改。这些更改不会在 ASA 上体现出来，直到您刷新 ASA 安全组表中的数据，所以您需要刷新 ASA 上的数据，以确保在 ISE 上所做的任何安全组更改都能在 ASA 上体现出来。

提示　我们建议您在维护窗口期间在 ISE 上安排策略配置更改，并在 ASA 上安排手动刷新数据。按这种方式处理策略配置更改，可以最大限度增加安全组名称获得解析和安全策略在 ASA 上立即进入活动状态的几率。

先决条件

必须将 ASA 配置为 ISE 中可识别的思科 TrustSec 网络设备，而且 ASA 必须已成功导入 PAC 文件，确保对思科 TrustSec 所做的更改已应用到 ASA。

限制

- 当 ASA 成为 HA 配置的一部分时，您必须刷新主 ASA 设备上的环境数据。
- 当 ASA 成为集群配置的一部分时，您必须刷新主设备上的环境数据。

要刷新环境数据，请执行以下步骤：：

步骤 1　在 ASDM 主应用窗口中，选择 **Configuration > Firewall > Identity By TrustSec**。

步骤 2　在 Server Group Setup 区域，点击 **Refresh Environment Data**。

ASA 刷新来自 ISE 的思科 TrustSec 环境数据，将协调计时器重置为已配置的默认值。

配置安全策略

您可以将思科 TrustSec 策略纳入多项 ASA 功能中。任何使用扩展 ACL （除非在本章节被列为不支持）的功能都能够利用思科 TrustSec。现在，您可以将安全组参数添加到扩展 ACL 以及基于网络的传统参数中。

- 要配置 访问规则，请参阅防火墙配置指南。
- 要配置可在 ACL 中使用的安全组对象组，请参阅第 17-5 页的配置安全组对象组。

例如，访问规则通过网络信息允许或拒绝接口上的流量。通过思科 TrustSec，您可以根据安全组控制访问。例如，您可以为 sample_securitygroup1 10.0.0.0 255.0.0.0 创建访问规则，这意味着，安全组可以拥有 10.0.0.0/8 子网上的任何 IP 地址。

您可以根据安全组名称 （服务器、用户、非受管设备等等）、基于用户的属性和基于 IP 地址的传统对象 （IP 地址、Active Directory 对象和 FQDN）构成的组合配置安全策略。安全组成员能够扩展到角色以外，将设备和位置属性包含在内，并且不受用户组成员约束。

配置第 2 层安全组标记实施

思科 TrustSec 可以对每个网络用户和资源进行识别和身份验证，并分配一个称为安全组标记 (SGT) 的 16 位数字。反过来，此标识符可以在网络跳段之间传送，允许任何中间设备 （例如 ASA、交换机和路由器）根据此身份标记实施策略。

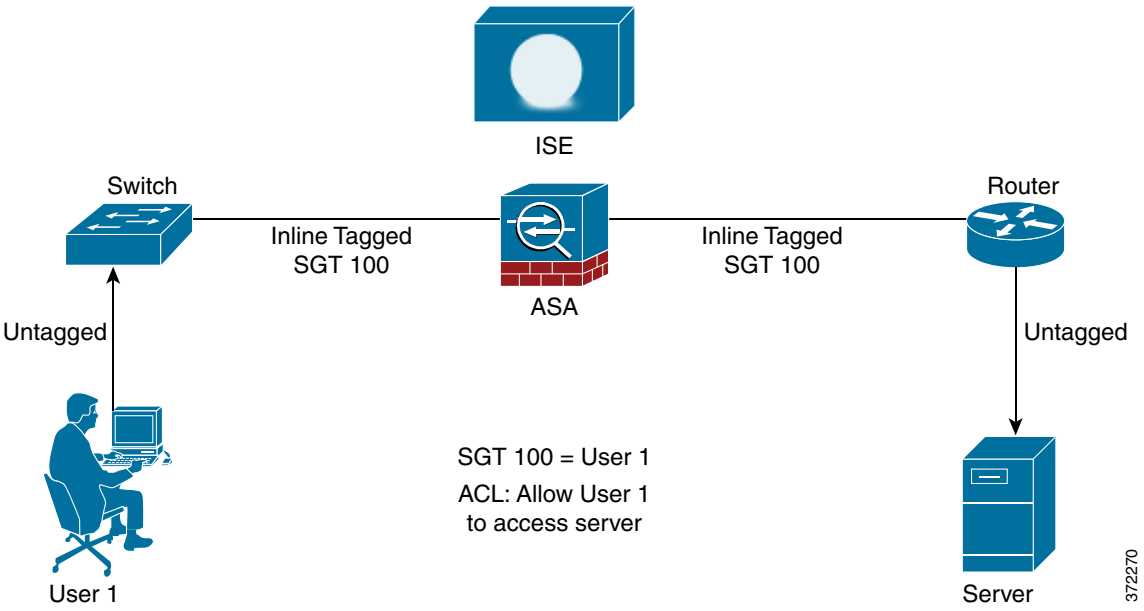
SGT plus Ethernet Tagging，也称作第 2 层 SGT 实施，使 ASA 能够使用思科专有以太网帧 (EtherType 0x8909) 在以太网接口上发送和接收安全组标记，其允许将源安全组标记插入纯文本以太网帧。 ASA 可以根据手动每接口配置，在传出数据包上插入安全组标记并在传入数据包上处理安全组标记。此功能允许跨网络设备对终端身份进行内联逐跳传送，在每个跳段之间提供无缝的第 2 层 SGT 实施。

限制

- 仅支持物理接口、 VLAN 接口、端口通道接口和冗余接口。
- 不支持逻辑接口或虚拟接口，例如 BVI。
- 不支持采用 SAP 协商和 MACsec 的链路加密。
- 不支持故障转移链路。
- 不支持集群控制链路。
- 如果 SGT 已更改， ASA 不会对现有流量进行重新分类。任何根据以前 SGT 指定的策略决定对流量寿命依然有效。然而， ASA 能够立即体现出口数据包上的 SGT 更改，即使这些数据包属于根据以前 SGT 进行分类的流量。

图 33-3 显示了典型的第 2 层 SGT 实施示例。

图 33-3　　第 2 层 SGT 实施



使用情境

表 33-3 描述了配置此功能时进口流量的预期行为。

表 33-3　进口流量

接口配置	收到的已标记数据包	收到的未标记数据包
未发布命令。	数据包被丢弃。	SGT 值来自 IP-SGT 管理器。
cts manual 命令被发布。	SGT 值来自 IP-SGT 管理器。	SGT 值来自 IP-SGT 管理器。
cts manual 命令和 **policy static sgt** *sgt_number* 命令都被发布。	SGT 值来自 **policy static sgt** *sgt_number* 命令。	SGT 值来自 **policy static sgt** *sgt_number* 命令。
cts manual 命令和 **policy static sgt** *sgt_number* **trusted** 命令都被发布。	SGT 值来自数据包中的内联 SGT。	SGT 值来自 **policy static sgt** *sgt_number* 命令。

注　如果没有来自 IP-SGT 管理器的匹配 IP-SGT 映射，则为 “Unknown” 使用预留 SGT 值 “0x0”。

表 33-4 描述了配置此功能时出口流量的预期行为。

表 33-4　出口流量

接口配置	发送的已标记或未标记数据包
未发布命令。	未标记
cts manual 命令被发布。	已标记
cts manual 命令和 **propagate sgt** 命令都被发布。	已标记
The **cts manual** 命令和 **no propagate sgt** 命令都被发布。	未标记

表 33-5 描述了配置此功能时流向设备的流量和流出设备的流量的预期行为。

表 33-5　流向设备的流量和流出设备的流量

接口配置	接收的已标记或未标记数据包
未在进口接口上为流向设备的流量发布命令。	数据包被丢弃。
在进口接口上为流向设备的流量发布了 **cts manual** 命令。	数据包已被接受，但没有策略实施或 SGT 传送。
未发布 **cts manual** 命令，或者在出口接口上为流出设备的流量发布了 **cts manual** 命令和 **no propagate sgt** 命令。	未标记数据包被发送，但没有策略实施。 SGT 号来自 IP-SGT 管理器。
发布了 **cts manual** 命令，或者在出口接口上为流出设备的流量发布了 **cts manual** 命令和 **propagate sgt** 命令。	已标记数据包被发送。 SGT 号来自 IP-SGT 管理器。

注　如果没有来自 IP-SGT 管理器的匹配 IP-SGT 映射，则为 “Unknown” 使用预留 SGT 值 “0x0”。

启用 SGT plus Ethernet Tagging

要启用 SGT plus Ethernet Tagging，执行以下步骤：

步骤 1　在 ASDM 中，选择以下选项之一：

- **Configuration > Device Setup > Interfaces > Add Interface > Advanced**
- **Configuration > Device Setup > Interfaces > Add Redundant Interface > Advanced**
- **Configuration > Device Setup > Interfaces > Add Ethernet Interface > Advanced**

步骤 2　在 Secure Group Tagging 区域，选中 **Enable secure group tagging for Cisco TrustSec** 复选框。

在接口上传送安全组标记

要在接口上启用或禁用安全标记传送，请执行以下步骤：

步骤 1　在 ASDM 中，选择以下选项之一：

- **Configuration > Device Setup > Interfaces > Add Interface > Advanced**
- **Configuration > Device Setup > Interfaces > Add Redundant Interface > Advanced**
- **Configuration > Device Setup > Interfaces > Add Ethernet Interface > Advanced**

步骤 2　在 Secure Group Tagging 区域，选中 **Enable secure group tagging for Cisco TrustSec** 复选框。

步骤 3　选中 **Tag egress packets with service group tags** 复选框。

将策略应用到手动配置的思科 TrustSec 链路

要将策略应用到手动配置的 CTS 链路，请执行以下步骤：

步骤 1　在 ASDM 中，选择以下选项之一：

- **Configuration > Device Setup > Interfaces > Add Interface > Advanced**
- **Configuration > Device Setup > Interfaces > Add Redundant Interface > Advanced**
- **Configuration > Device Setup > Interfaces > Add Ethernet Interface > Advanced**

步骤 2　在 Secure Group Tagging 区域，选中 **Enable secure group tagging for Cisco TrustSec** 复选框。

步骤 3　选中 **Tag egress packets with service group tags** 复选框。

步骤 4　选中 **Add a static secure group tag to all ingress packets** 复选框。

步骤 5　输入安全组标记号。有效值范围为 2 至 65519。

步骤 6　选中 **This is a trusted interface.Do not override existing secure group tags** 复选框。

步骤 7　点击 **OK**，保存设置并关闭 Advanced 选项卡。

手动配置 IP-SGT 绑定

要手动配置 IP-SGT 绑定，执行以下步骤：

步骤 1　选择 **Configuration > Firewall Identity by TrustSec**。

步骤 2　在 SGT Map Setup 区域，点击 **Add**。（要修改现有 IP-SGT 绑定，请将其选中，并点击 **Edit**。要移除现有 IP-SGT 绑定，请将其选中，并点击 **Delete**。）

系统将显示 Add SGT Map 对话框。

步骤 3　在相应的字段中输入 SGT 映射 IP 地址和 SGT 值。 SGT 号的有效值为 2 至 65519。

步骤 4　点击 **OK**，然后点击 **Apply**。

新配置的 IP-SGT 绑定将显示在 SGT Map Setup 区域中。

面向思科 TrustSec 的 AnyConnect VPN 支持

ASA 9.3(1) 版本完全支持 VPN 会话的安全组标记。可以使用外部 AAA 服务器或者通过配置本地用户数据库，向 VPN 会话分配安全组标记 (SGT)。然后，可以在第 2 层以太网上通过思科 TrustSec 系统传送此标记。当 AAA 服务器无法提供 SGT 时，安全组标记对于组策略和本地用户非常有用。

如果 AAA 服务器属性中没有用以分配给 VPN 用户的 SGT， ASA 则使用默认组策略中的 SGT。如果组策略中没有 SGT，则分配标记 0x0。

远程用户连接到服务器的典型步骤

1. 用户连接到 ASA。
2. ASA 从 ISE 请求 AAA 信息，其中可能包含 SGT。 ASA 还为用户的隧道流量分配 IP 地址。
3. ASA 使用 AAA 信息进行身份验证并创建隧道。
4. ASA 使用来自 AAA 信息的 SGT 和已分配的 IP 地址，在第 2 层标头中添加 SGT。
5. 包含 SGT 的数据包被传送到思科 TrustSec 网络中的下一个对等设备。

将 SGT 添加到本地用户和组

通过 ASDM 中的以下对话，您可以添加 SGT 标记：

- Configuration > Remote Access VPN > AAA/Local Users > Local Users。 Add 或者 Edit 用户，选择 VPN Policy 面板，为 Security Group Tag (STG) 输入一个值。
- Configuration > Remote Access VPN > Network (Client) Access > Group Policies，在 General 选项卡上，展开 More Options，并在 Security Group Tag (SGT) 中输入一个值。

监控思科 TrustSec

要在 ASA 上监控思科 TrustSec，在 ASDM 中选择以下路径之一：

路径	用途
Monitoring > Properties > Identity By TrustSec > SXP Connections	显示为思科 TrustSec 基础设施和 SXP 命令配置的默认值。
Monitoring > Properties > Connections	显示所有 SXP 连接的数据。过滤 IP 地址安全组表映射条目，以便您能够按安全组表值、安全组名称或 IP 地址查看数据。
Monitoring > Properties > Identity By TrustSec > Environment Data	显示包含在 ASA 上的安全组表中的思科 TrustSec 环境信息。
Monitoring > Properties > Identity By TrustSec > IP Mapping	显示在数据路径中维护的 IP 地址安全组表映射数据库中的 IP 地址安全组表映射条目。过滤 IP 地址安全组表映射条目，以便您能够按安全组表值、安全组名称或 IP 地址查看数据。 **提示**　点击 **Where Used**，显示已选中安全组对象在 ACL 中的使用位置，或者嵌入到另一个安全组对象中的位置。
Monitoring > Properties > Identity By TrustSec > PAC	显示有关从 ISE 导入 ASA 的 PAC 文件的信息。当 PAC 文件已过期或将 30 天内过期时，显示一条警告消息。

附加参考资料

参考网站	说明
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html	介绍面向企业的思科 TrustSec 系统和架构。
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_DesignZone_TrustSec.html	提供有关在企业中部署思科 TrustSec 解决方案的指导说明，包含到组件设计指南的链接。
http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/solution_overview_c22-591771.pdf	提供有关与 ASA、交换机、无线 LAN (WLAN) 控制器和路由器配合使用的思科 TrustSec 解决方案的概述。
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html	提供思科 TrustSec 平台支持矩阵，其中列出了支持思科 TrustSec 解决方案的思科产品。

思科 TrustSec 集成的功能历史

表 33-6 列出了各种功能变更以及实施该等功能变更的平台版本。 ASDM 可向后兼容多个平台版本，因此，未列出已添加支持的具体 ASDM 版本。

表 33-6　　思科 TrustSec 集成的功能历史

功能名称	平台版本	功能信息
思科 TrustSec 集成	9.0(1)	思科 TrustSec 可以提供基于现有的身份感知基础设施的访问控制，确保网络设备之间的数据保密性，并集成平台上的安全访问服务。在思科 TrustSec 功能中，实施设备结合用户属性和终端属性制定基于角色和基于身份的访问控制决策。 在此版本中，ASA 与思科 TrustSec 集成以提供基于安全组的策略实施。思科 TrustSec 域中的访问策略不受拓扑影响，基于源和目标设备的角色，而非基于网络 IP 地址。 ASA 可以将此项思科 TrustSec 功能用于其他类型的基于安全组的策略 （例如应用检查）；例如，您可以根据安全组配置包含访问策略的类映射。 我们引入或修改了以下屏幕： Configuration > Firewall > Identity By TrustSec Configuration > Firewall > Objects > Security Groups Object Groups Configuration > Firewall > Access Rules > Add Access Rules Monitoring > Properties > Identity By Tag.
第 2 层安全组标记施加	9.3(1)	现在，您可以使用结合了以太网标记的安全组标记来实施策略。 SGT plus Ethernet Tagging，也称作第 2 层 SGT 实施，使 ASA 能够使用思科专有以太网帧 (EtherType 0x8909) 在以太网接口上发送和接收安全组标记，其允许将源安全组标记插入纯文本以太网帧。 我们修改了以下屏幕： Configuration > Device Setup > Interfaces > Add Interface > Advanced Configuration > Device Setup > Interfaces > Add Redundant Interface > Advanced Configuration > Device Setup > Add Ethernet Interface > Advanced.

ASA 和思科移动支持

关于 ASA 和思科移动支持

思科 ASA 是边缘设备，可对受思科移动支持 (ME) （思科身份服务引擎 (ISE) 的一个组件）管理的移动设备提供对于公司网络的外部访问权限。作为适用于 ISE ME 的网络访问设备 (NAD)，ASA 可用作移动设备授权、注册和定期登记的代理。它在外部远程移动设备 （AnyConnect 设备管理客户端）与移动设备管理器 （ISE 移动支持服务器）之间提供安全通信路径。这样一来，运行 AnyConnect 客户端应用的外部移动设备就可以完全像内部移动设备一样参与移动设备管理。

本节仅介绍 ASA 特定配置及行为。

可通过指定以下各项在 ASA 上配置 ME 代理功能：

- AnyConnect ME 客户端用于注册和登记请求的 ASA 接口和端口。
- 用于对客户端进行身份验证的 AAA 服务器。通常是 Radius 服务器 （该服务器是 ISE 移动支持解决方案的一个组成部分）。
- 用于向移动支持服务器对 ASA 进行识别和身份验证的信任点

ASA MDM 代理准则和限制

- ME 代理功能仅在单情景路由器模式中受支持。
- ME 代理没有 ASA 许可要求。 ME 的许可在 ISE 上执行。
- 在移动设备上运行的 AnyConnect ME 客户端使用同一个 URI 与 ME 服务器通信，无论用户是在内部 （位于公司网络上）还是在外部 （位于公用网络上）。要支持这一行为，网络的 DNS 配置必须将 ME URI 解析到 ASA 网关（以实现外部支持）和 ISE 策略服务器节点 (PSN)（以实现内部支持）。

- 对于 AnyConnect ME 客户端与 ASA 之间的身份验证以及 ASA 与 ISE ME 服务器之间的身份验证，需要数字证书。为纳入了 ASA ME 代理的移动支持解决方案计划和配置证书时，请注意以下几点：
  - 对 ISE 策略服务节点进行 ASA 身份验证的证书必须允许同时代表多个代理设备。
  - 对于注册期间作为 SCEP 的结果而在移动设备上接收的 AnyConnect 客户端证书，应将其定义为在外部时对 ASA 进行身份验证，在内部时对 ISE 进行身份验证。同样，以相同的方式在 Apple iOS 移动设备上接收的其他 Applie iOS 客户端证书也应具有这种行为。
  - 可如下定义单一证书：在 Subject Alternative Name (SAN) 字段中指定两个服务器的 FQDN，从而将证书定义为会向移动设备上的客户端进行 ASA 和 ISE 身份验证。
- 外部受管移动设备不能访问 “ISE 我的设备 ” 门户。要访问此门户，移动设备用户必须是内部用户。

将 ASA 配置为 MDM 代理

准备工作

- 必须配置 Radius 服务器组，使其能够访问 ISE AAA Radius 服务器以进行授权和记帐。
- 必须配置信任点，用于代表 AnyConnect 客户端向 ISE MDM 服务器进行 ASA 身份验证。

操作步骤

步骤 1　转至 **Configuration > Remote Access VPN > AAA/Local Users > MDM Proxy**。

步骤 2　设置 **Access Interface** 字段：

- **MDM Server Access Interface(s)** - 选择用于处理来自客户端的 MDM 代理请求的接口。
- **Enrollment Port** - 指定用于所选接口上的 MDM 客户端身份验证和注册请求的端口。默认端口是 443。
- **Check-in Port** - （可选）指定用于所选接口上的 MDM 登记请求的端口 （1 到 65535）。此端口不得用于任何其他服务。

步骤 3　设置 **Radius Server Groups** 字段：

- **Authentication Server Group** - 指定用于 MDM 客户端身份验证的身份验证服务器组。可选择预配置的服务器组，或者指定一个新的服务器组。
- **Accounting Server Group** - 指定用于记录各种 MDM 客户端操作的记帐服务器组。可选择预配置的服务器组，或者指定一个新的服务器组。

步骤 4　设置 **MDM Server Authentication** 字段：

- **Device Certificate** - 指定 ASA 用于向 MDM 服务器 （位于 ISE 上）进行自我身份验证的信任点。可选择预配置的服务器组，或者选择 **New** 以打开 **Create Radius Server Group for MDM Proxy** 对话框，并配置 ISE MDM Radius 服务器。
- **Password Expiration** - 指定在密码到期之前多少天发出警告。

步骤 5　点击 **OK**。

监控 Mobile Enablement Proxy 活动

要查看 ASA 的移动支持统计信息，请在 ASDM 中选择以下路径：

Monitoring > VPN > VPN Statistics > MDM Proxy Statistics

ASA Mobile Enablement Proxy 的功能历史记录

功能名称	平台版本	功能信息
Mobile Enablement Proxy	9.3(1)	Mobile Enablement Proxy 是 ISE Mobile Enablement 解决方案的组件，允许外部移动设备以与内部移动设备完全相同的方式参与移动设备管理。 我们引入了以下屏幕：**Configuration > Remote Access VPN > AAA/Local Users > MDM Proxy**。

第 35 章

数字证书

本章介绍了如何配置数字证书。

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。数字证书包括识别设备或用户的信息，如名称、序列号、公司、部门或 IP 地址。 CA 是 “ 签署 ” 证书以验证其真实性，从而确保设备或用户的身份的可信颁发机构。 CA 在 PKI （使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。

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 的证书。此配置允许多个身份、根和证书层次结构。 ASA 根据 CRL （也称为权限撤销列表）评估第三方证书，从身份证书一直到从属证书颁发机构链。

几种不同类型的可用数字证书的说明如下：

- *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，通过签署的代码透露证书来源。

本地 CA 在 ASA 上集成了一项独立的证书授权功能，并且会部署证书，对已颁发的证书提供安全的撤销检查。本地 CA 凭借通过网站登录页面进行的用户注册提供了一个安全、可配置的内部机构进行证书身份验证。

注　CA 证书和身份证书适用于站点到站点 VPN 连接和远程访问 VPN 连接。本文档中的操作步骤是指在 ASDM GUI 中使用远程访问 VPN。

数字证书是一种用于身份验证的数字识别方式。数字证书包括识别设备或用户的信息，如名称、序列号、公司、部门或 IP 地址。 CA 是 “ 签署 ” 证书以验证其真实性，从而确保设备或用户的身份的可信颁发机构。 CA 在 PKI （使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。

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 的证书。此配置允许多个身份、根和证书层次结构。几种不同类型的可用数字证书的说明如下：

- *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。数字证书包括识别用户或的设备信息，如名称、序列号、公司、部门或 IP 地址。数字证书还包括用户或设备的公钥副本。 CA 可以是可信的第三方，如 VeriSign，或公司内建立的私有 （内部） CA。

提示　有关包括证书配置和负载均衡的情景示例，请参阅以下 URL：https://supportforums.cisco.com/docs/DOC-5964。

公钥加密

由公钥加密支持的数字签名提供了一种验证设备和用户身份的方法。在 RSA 加密系统等公钥加密中，每个用户都具有一个包含公钥和私钥的密钥对。密钥对互为补充，采用其中一个密钥加密的任何东西均可使用另一个密钥解密。

简单来说，使用私钥加密数据时，将形成签名。签名附于数据中并发送给接收方。接收方将发送方的公钥应用于数据。如果随数据一起发送的签名与将公钥应用于数据的结果相匹配，则验证了消息的有效性。

此过程依赖于，接收方具有发送方公钥的副本，且高度肯定此密钥属于发送方，而非冒充发送方的其他人。

获取发送方公钥通常是在外部处理或通过安装时执行的操作处理。例如，默认情况下，大多数网络浏览器都是使用几个 CA 的根证书进行配置。对于 VPN，作为 IPsec 一部分的 IKE 协议可使用数字签名在设置安全关联之前验证对等设备身份。

证书可扩展性

在没有数字证书的情况下，必须手动为每个与其通信的对等体配置各自的 IPSec 对等体；因此，每个添加到网络的新对等体都会要求对需要与其安全通信的每个对等体进行配置更改。

使用数字证书时，系统将向 CA 注册每个对等体。两个对等体试图进行通信时，它们将交换证书并以数字方式签署数据以进行相互身份验证。新对等体添加到网络时，向 CA 注册该对等体，其他任何对等体都不需要修改。新对等体尝试进行 IPSec 连接时，证书将自动交换并且对等体可进行身份验证。

通过 CA，对等体可将证书发送到远程对等体并进行一些公钥加密，从而自行向远程对等体进行身份验证。每个对等体将发送由 CA 颁发的唯一证书。之所以执行此过程，是因为每个证书会封装关联对等体的公钥，每个证书由 CA 进行身份验证，且所有参与对等体都将 CA 视为身份验证机构。此过程称为带 RSA 签名的 IKE。

对等体可继续为多个 IPsec 会话发送其证书，并可向多个 IPSec 对等体发送证书，直到证书过期。证书过期后，对等体管理员必须从 CA 获取新的证书。

CA 还可以为不再参与 IPsec 的对等体撤销证书。撤销的证书无法被其他对等体识别为有效证书。撤销的证书列于 CRL 中，每个对等体都可能会在从其他对等体接受证书之前检查这些证书。

有些 CA 会在实施过程中使用 RA。RA 是一种用作 CA 的代理的服务器，因此，CA 功能可以在 CA 不可用时继续使用。

密钥对

密钥对是 RSA 密钥，具有以下特征：

- RSA 密钥可用于 SSH 或 SSL。
- SCEP 注册支持 RSA 密钥的认证。
- 为了生成密钥，RSA 密钥的最大密钥模值为 2048 位。默认长度为 1024 位。许多使用含超过 1024 位 RSA 密钥对的身份证书的 SSL 连接可能会导致 ASA 上的 CPU 使用率较高，并导致无客户端登录被拒绝。
- 对于签名操作，支持的最大密钥长度为 4096 位。我们建议使用至少为 2048 位的密钥长度。
- 您可以生成一个通用 RSA 密钥对，用于签名和加密，也可以为每种用途生成单独的 RSA 密钥对。单独的签名和加密密钥有助于减少密钥泄露的机会，因为 SSL 使用密钥进行加密，但不签名。但是，IKE 使用密钥进行签名，但不加密。通过为每种用途使用单独的密钥，泄露密钥的风险降至最低。

信任点

信任点可让您管理和跟踪 CA 与证书。信任点是一种 CA 或身份对的表现。信任点包括 CA 的身份、CA 特定配置参数，以及与一个注册的身份证书的关联。

定义信任点之后，可以在要求指定 CA 的命令中根据名称来引用它。您可以配置多个信任点。

注　如果 Cisco ASA 具有多个共享相同 CA 的信任点，则只有其中一个共享 CA 的信任点可用于验证用户证书。要控制将哪个共享 CA 的信任点用于验证由该 CA 颁发的用户证书，请使用 **support-user-cert-validation** 命令。

对于自动注册，信任点必须使用注册 URL 进行配置，并且信任点代表的 CA 必须在网络中可用且必须支持 SCEP。

您可以 PKCS12 格式导出和导入密钥对，以及与某个信任点关联的已颁发证书。此格式有助于在不同的 ASA 上手动复制信任点配置。

证书注册

ASA 需要每个信任点都有一个 CA 证书，它自己也需要一个或两个证书，具体取决于信任点使用的密钥的配置。如果信任点使用单独的 RSA 密钥进行签名和加密，则 ASA 需要两个证书，每种用途一个。在其他密钥配置中，只需要一个证书。

ASA 支持使用 SCEP 自动注册和手动注册，这样可将 base-64 编码的证书直接粘贴到终端。对于站点到站点 VPN，必须注册每个 ASA。对于远程访问 VPN，必须注册每个 ASA 和每个远程访问 VPN 客户端。

SCEP 请求的代理

ASA 可代理 AnyConnect 和第三方 CA 之间的 SCEP 请求。如果 ASA 用作代理，则 CA 只需要允许它访问。如果要 ASA 提供此服务，用户必须在 ASA 发送注册请求之前使用任意受 AAA 支持的方法进行身份验证。您还可以使用主机扫描和动态访问策略强制注册资格规则。

ASA 只在 AnyConnect SSL 或 IKEv2 VPN 会话中支持此功能。它支持所有符合 SCEP 的 CA，包括 Cisco IOS CS、 Windows Server 2003 CA 和 Windows Server 2008 CA。

无客户端 （基于浏览器）访问不支持 SCEP 代理，但 WebLaunch （无客户端启动 AnyConnect）支持它。

ASA 不支持证书的轮询。

ASA 支持此功能的负载均衡。

撤销检查

证书颁发后，在固定时期内有效。有时， CA 会在此时期到期前撤销证书，例如，因为安全问题或名称变化或关联等原因而撤销。 CA 会定期发布签署的撤销证书列表。启用撤销检查可强制 ASA CA 在每次使用证书进行身份验证时检查并确定其未撤销该证书。

启用撤销检查后，ASA 会在 PKI 证书验证过程中使用 CRL 检查、OCSP 或同时使用两者检查证书撤销状态。只有在第一种方法返回错误时 （例如，指示服务器不可用时）才使用 OCSP。

通过 CRL 检查， ASA 可检索、分析、缓存 CRL，从而提供完整的撤销 （和未撤销）证书及其证书序列号列表。 ASA 根据 CRL （也称为权限撤销列表）评估证书，从身份证书一直到从属证书颁发机构链。

OCSP 提供了一种更具可扩展性的撤销状态检查方法。此方法通过验证机构对证书状态进行本地化，验证机构会查询特定证书的状态。

支持的 CA 服务器

ASA 支持以下 CA 服务器：

Cisco IOS CS、 ASA 本地 CA 和符合 X.509 的第三方 CA 供应商，包括但不限于：

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

CRL 为 ASA 提供了一种方法来确定某个有效期内的证书是否已被证书颁发机构 (CA) 撤销。CRL 配置是信任点配置的一部分。

进行证书身份验证时，可使用 **revocation-check crl** 命令配置 ASA 以将 CRL 检查设为强制性检查。也可以使用 **revocation-check crl none** 命令将 CRL 检查设为可选检查，这种情况下，在 CA 无法提供更新的 CRL 数据时，证书身份验证也会成功。

ASA 可使用 HTTP、SCEP 或 LDAP 从 CA 检索 CRL。为每个信任点检索的 CRL 会在为每个信任点配置的时间内一直缓存。

当 ASA 缓存 CRL 的时间长于配置用于缓存 CRL 的时间时，ASA 会认为 CRL 太陈旧（因而也就不太可靠）或 “ 过时 ”。ASA 会在下一次证书身份验证需要检查过时 CRL 时尝试检索更新版本的 CRL。

ASA 缓存 CRL 的时间由以下两个因素决定：

- 使用 **cache-time** 命令指定的分钟数。默认值为 60 分钟。
- 检索的 CRL 中的 NextUpdate 字段，CRL 中可能没有该字段。可使用 **enforcenextupdate** 命令控制 ASA 是否需要和使用 NextUpdate 字段。

ASA 通过以下方式利用这两个因素：

- 如果不需要 NextUpdate 字段，ASA 会在由 **cache-time** 命令定义的时间过后将 CRL 标记为 “ 过时 ”。
- 如果需要 NextUpdate 字段， ASA 会在由 **cache-time** 命令和 NextUpdate 字段指定的两个时间中较早的那个时间点将 CRL 标记为 “ 过时 ”。例如，如果 **cache-time** 命令设置为 100 分钟，而 NextUpdate 字段指定下一次更新是在 70 分钟后，则 ASA 会将 CRL 标记为 “ 在 70 分钟后过时 ”。

如果 ASA 的内存不足以存储为给定信任点缓存的所有 CRL，它将删除最近最少使用的 CRL 以为新检索的 CRL 腾出空间。

OCSP

OCSP 为 ASA 提供了一种方法来确定某个有效期内的证书是否已被证书颁发机构 (CA) 撤销。OCSP 配置是信任点配置的一部分。

OCSP 在验证机构（一种 OCSP 服务器，也称为*响应方*）上对证书状态进行本地化，这样 ASA 就可查询特定证书的状态。相比 CRL 检查，此方法可提供更好的可扩展性和更新的撤销状态，并且可帮助装有大型 PKI 的公司部署和扩展安全网络。

注　ASA 允许 OCSP 响应有五秒钟的时间偏差。

在进行证书身份验证时，可使用 **revocation-check ocsp** 命令配置 ASA 以将 OCSP 检查设为强制性检查。也可以使用 **revocation-check ocsp none** 命令将 OCSP 检查设为可选检查，这种情况下，在验证机构无法提供更新的 OCSP 数据时，证书身份验证也会成功。

OCSP 提供三种定义 OCSP 服务器 URL 的方法。 ASA 按以下顺序使用这些服务器：

1. 使用 **match certificate** 命令在匹配证书覆盖规则中定义的 OCSP URL。
2. 使用 **ocsp url** 命令配置的 OCSP URL。
3. 客户端证书的 AIA 字段。

注　要将信任点配置为验证自签名 OCSP 响应方证书，请将自签名响应方证书作为可信 CA 证书导入其自己的信任点。之后，在客户端证书验证信任点配置 **match certificate** 命令以使用包括自签名 OCSP 响应方证书的信任点验证响应方证书。使用相同操作步骤在客户端证书的验证路径外部配置验证响应方证书。

OCSP 服务器（响应方）证书通常会签署 OCSP 响应。在收到响应后，ASA 将尝试验证响应方证书。CA 通常会将 OCSP 响应方证书的有效期设置为相对较短的时间以将受危害的可能性降至最低。CA 通常还会在响应方证书中包含 ocsp-no-check 扩展，表明此证书不需要进行撤销状态检查。但是，如果此扩展不存在，ASA 将尝试使用信任点中指定的同一方法检查撤销状态。如果响应方证书无法验证，则撤销检查失败。要避免这种可能性，请使用 **revocation-check none** 命令配置响应方证书验证信任点，并使用 **revocation-check ocsp** 命令配置客户端证书。

本地 CA

本地 CA 执行以下任务：

- 在 ASA 上集成基本证书授权操作。
- 部署证书。
- 为已颁发的证书提供安全的撤销检查。
- 在 ASA 上提供一个证书授权功能以便与基于浏览器和基于客户端的 SSL VPN 连接配合使用。
- 为用户提供可信数字证书，而无需依赖于外部证书授权。
- 提供安全的内部机构进行证书身份验证，并提供通过网站登录进行的直接用户注册。

本地 CA 文件的存储

ASA 可使用本地 CA 数据库访问和实施用户信息、已颁发的证书和撤销列表。默认情况下，此数据库驻留在本地闪存中，也可以配置为驻留在已安装且允许 ASA 访问的外部文件系统上。

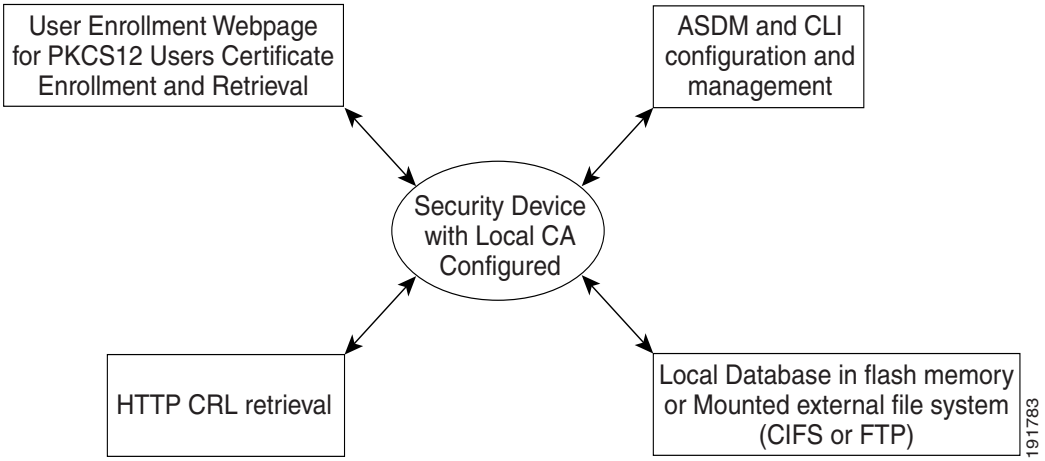
可存储在本地 CA 用户数据库中的用户数量不受限制；但是，如果出现闪存存储问题，将生成系统日志以提示管理员采取行动，并且本地 CA 可能会被禁用，直到存储问题得到解决。闪存可存储不超过 3500 个用户的数据库；但是，超过 3500 个用户的数据库需要外部存储器。

本地 CA 服务器

在 ASA 上配置本地 CA 服务器后，用户可为每个证书进行注册，方法如下：登录网站并输入用户名及由本地 CA 管理员提供的一次性密码以验证其注册资格。

图 35-1 显示本地 CA 服务器驻留在 ASA 上并处理来自网站用户的注册请求，以及来自其他证书验证设备和 ASA 的 CRL 查询。本地 CA 数据库和配置文件保存在 ASA 闪存（默认存储器）或单独的存储设备上。

图 35-1　　本地 CA



证书和用户登录凭证

下一节介绍了使用证书和用户登录凭证 （用户名和密码）进行身份验证和授权的不同方法。这些方法适用于 IPsec、 AnyConnect 和无客户端 SSL VPN。

在任何情况下， LDAP 授权都不会使用密码作为凭证。 RADIUS 授权对所有用户使用公用密码或使用用户名作为密码。

用户登录凭证

身份验证和授权的默认方法是使用用户登录凭证。

- 身份验证
  - 通过隧道组 （也称为 ASDM 连接配置文件）中的身份验证服务器组设置启用
  - 使用用户名和密码作为凭证
- 授权
  - 通过隧道组 （也称为 ASDM 连接配置文件）中的授权服务器组设置启用
  - 使用用户名作为凭证

证书

如果已配置用户数字证书， ASA 会先验证证书。但是，它不会使用证书的任意 DN 作为用户名进行身份验证。

如果身份验证和授权均已启用， ASA 将使用用户登录凭证同时进行用户身份验证和授权。

- 身份验证
  - 通过身份验证服务器组设置启用
  - 使用用户名和密码作为凭证

- 授权
  - 通过授权服务器组设置启用
  - 使用用户名作为凭证

如果身份验证禁用，而授权启用， ASA 将使用主要 DN 字段进行授权。

- 身份验证
  - 通过身份验证服务器组设置禁用 （设置为 None）
  - 未使用凭证
- 授权
  - 通过授权服务器组设置启用
  - 使用证书主要 DN 字段的用户名作为凭证

注　如果证书中不存在主要 DN 字段， ASA 将使用次要 DN 字段值作为授权请求的用户名。

以包含以下 Subject DN 字段和值的用户证书为例：

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

如果主要 DN = EA（邮件地址）并且次要 DN = CN（公用名称），则授权请求中使用的用户名是 anyuser@example.com。

本地证书的先决条件

本地证书有以下先决条件要求：

- 确保正确配置 ASA 以支持证书。配置不正确的 ASA 可能会导致注册失败或请求包含不准确信息的证书。
- 确保正确配置 ASA 的主机名和域名。要查看当前配置的主机名和域名，请输入 **show running - config** 命令。
- 确保在配置 CA 之前准确设置 ASA 时钟。证书具有有效和到期的日期和时间。当 ASA 向 CA 注册并获取证书时， ASA 会检查当前时间是否在证书的有效范围内。如果超出范围，注册失败。

SCEP 代理支持的先决条件

将 ASA 配置为代理以提交对第三方证书的请求时，具有以下要求：

- 终端中必须运行的是 AnyConnect 安全移动客户端 3.0 或更高版本。
- 在组策略的连接配置文件中配置的身份验证方法必须设置为同时使用 AAA 和证书身份验证。
- 对于 IKEv2 VPN 连接， SSL 端口必须处于打开状态。
- CA 必须处于自动授予模式。

数字证书准则

情景模式准则

- 对于第三方 CA，只在单情景模式中受支持。

故障转移准则

- 在带状态的故障转移中不支持复制会话。
- 对于本地 CA，不支持故障转移。

IPv6 准则

不支持 IPv6。

附加准则

- 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。
- 启用故障转移时，无法配置本地 CA。您只能为无故障转移的独立 ASA 配置本地 CA 服务器。有关详细信息，请参阅 CSCty43366。
- 证书注册完成后，ASA 将存储包含用户的密钥对和证书链的 PKCS12 文件，每次注册需要约 2 KB 的闪存或磁盘空间。实际的磁盘空间容量取决于已配置的 RSA 密钥长度和证书字段。在可用闪存容量有限的 ASA 上添加大量待处理的证书注册时，请记住此准则，因为这些 PKCS12 文件在配置的注册检索超时期间存储在闪存中。我们建议使用至少为 2048 位的密钥长度。
- 本地 CA 服务器证书第一次生成时 （即，最初配置本地 CA 服务器并发出 **no shutdown** 命令时），**lifetime ca-certificate** 命令生效。CA 证书到期时，配置的有效期值用于生成新的 CA 证书。您不能更改现有 CA 证书的有效期值，
- 而应配置 ASA 以使用身份证书保护流向管理接口的 ASDM 流量和 HTTPS 流量。使用 SCEP 自动生成的身份证书会在每次重新启动后重新生成，因此请确保手动安装您自己的身份证书。本操作步骤仅适用于 SSL，有关示例，请参阅以下 URL：http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml。
- ASA 和 AnyConnect 客户端只可验证其中 X520Serialnumber 字段 （使用者名称中的序列号）使用 PrintableString 格式的证书。如果序列号格式使用编码 （如 UTF8），证书授权将失败。
- 如果在 ASA 上导入证书参数时，只对证书参数使用有效的字符和值。
- 要使用通配符 (*) 符号，请确保在允许在字符串值中使用此字符的 CA 服务器上使用编码。虽然 RFC 5280 建议使用 UTF8String 或 PrintableString，但您应使用 UTF8String，因为 PrintableString 无法将通配符识别为有效字符。如果在导入过程中发现无效的字符或值，ASA 将拒绝导入的证书。例如：

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read
162*H÷ytes as CA certificate:0U0= \Ivr"phÕV°3é¼þ0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

配置数字证书

本节介绍了如何配置本地 CA 证书。确保按照所列任务的顺序正确配置此类型的数字证书。

配置 CA 证书身份验证

CA Certificates 窗格显示可用的证书（通过颁发和接受颁发的 CA 服务器进行标识）、证书到期日期、关联的信任点，以及证书用法或用途。在 CA Certificates 窗格中，您可以执行以下任务：

- 对自签名或从属 CA 证书进行身份验证。
- 在 ASA 上安装 CA 证书。
- 创建新证书配置。
- 编辑现有的证书配置。
- 手动获取 CA 证书并将其导入。
- 让 ASA 使用 SCEP 联系 CA，然后自动获取并安装证书。
- 显示选定证书的详细信息和颁发者信息。
- 访问现有 CA 证书的 CRL。
- 移除现有 CA 证书的配置。
- 保存新的或修改的 CA 证书配置。
- 放弃所有更改并将身份验证配置恢复原始设置。

添加或安装 CA 证书

您可以使用 PEM 格式手动粘贴证书，或通过使用 SCEP 自动注册，从现有文件中添加新证书配置。 SCEP 是一种安全的消息传递协议，它需要的用户干预最少，可让您仅使用 VPN Concentrator Manager 即可注册和安装证书。

要添加或安装 CA 证书，请执行以下步骤：

步骤 1　在 ASDM 主应用窗口中，选择 **Configuration > Remote Access VPN > Certificate Management > CA Certificates**。

步骤 2　点击 **Add**。

系统将显示 Install Certificate 对话框。系统将以只读格式显示选定信任点名称。

步骤 3　要从现有文件添加证书配置，请点击 **Install from a file** 单选按钮 （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　要手动注册，请点击 **Paste certificate in PEM format** 单选按钮。

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，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　要自动注册，点击 **Use SCEP** 单选按钮。 ASA 将使用 SCEP 联系 CA，获取证书并在设备上安装证书。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 自动注册要求您提供以下信息：

- 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。

注　选择使用 SCEP 方法安装证书时，请参阅 SCEP 代理支持的先决条件。

步骤 10　要显示新证书和现有证书的其他配置选项，请点击 **More Options**。

系统将显示 Configuration Options for CA Certificates 窗格。

步骤 11　要继续，请参阅第 35-11 页的编辑或移除 CA 证书配置。

编辑或移除 CA 证书配置

要更改或移除现有 CA 证书配置，请执行以下步骤：

步骤 1　要更改现有 CA 证书配置，请选择该配置，然后点击 **Edit**。

系统将显示 Edit Options for CA Certificates 窗格。要更改其中的任意设置，请参阅以下节中的操作步骤：

- 第 35-12 页的配置 CRL 检索策略
- 第 35-13 页的配置 CRL 检索方法
- 第 35-13 页的配置 OCSP 规则
- 第 35-14 页的配置高级 CRL 和 OCSP 设置

步骤 2　要移除 CA 证书配置，请选择该配置，然后点击 **Delete**。

注　删除证书配置后，它将无法恢复。要重新创建删除的证书，请点击 **Add** 以重新输入所有证书配置信息。

显示 CA 证书详细信息

要显示有关选定 CA 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*只显示*选项卡：

- General 选项卡显示类型、序列号、状态、用途、公钥类型、 CRL 分发点、证书有效期和关联的信任点等值。这些值适用于可用和挂起状态。
- 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 证书撤销

要配置 CA 证书撤销，请以单情景或多情景模式执行以下站点到站点的任务：

步骤 1　在 ASDM 应用窗口中，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　在 Configuration Options for CA Certificates 窗格中，点击 **Revocation Check** 选项卡。

步骤 3　要禁用证书的撤销检查，请点击 **Do not check certificates for revocation** 单选按钮。

步骤 4　要选择一个或多个撤销检查方法（CRL 或 OCSP），请点击 **Check certificates for revocation** 单选按钮。

步骤 5　在 Revocation Methods 区域，可用的方法显示在左侧。点击 **Add** 可将某个方法移至右侧，将其变为可用。点击 **Move Up** 或 **Move Down** 可更改方法顺序。

您选择的方法将按照它们的添加顺序进行实施。如果某个方法返回错误，则下一个撤销检查方法将激活。

步骤 6　选中 **Consider certificate valid if revocation checking returns errors** 复选框以忽略证书验证过程中的撤销检查错误。

步骤 7　点击 **OK** 以关闭 Revocation Check 选项卡。或者，要继续，请参阅第 35-12 页的配置 CRL 检索策略。

配置 CRL 检索策略

要配置 CRL 检索策略，请执行以下步骤：

步骤 1　在 ASDM 应用窗口中，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** 复选框以将撤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 将按照它们的添加顺序进行实施。如果指定 URL 出现错误，则按照该顺序采用下一个 URL。

步骤 4　在 Static Configuration 区域，点击 **Add**。

系统将显示 Add Static URL 对话框。

步骤 5　在 URL 字段中，输入要用于分发 URL 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　要更改静态 URL，请选择 URL，然后点击 **Edit**。

步骤 7　要移除现有的静态 URL，请选择 URL，然后点击 **Delete**。

步骤 8　要更改静态 URL 显示的顺序，请点击 **Move Up** 或 **Move Down**。

步骤 9　点击 **OK** 以关闭此选项卡。或者，要继续，请参阅第 35-13 页的配置 CRL 检索方法。

配置 CRL 检索方法

要配置 CRL 检索方法，请执行以下步骤：

步骤 1　在 ASDM 应用窗口中，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　在 Configuration Options for CA Certificates 窗格中，点击 **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 将通过连接到使用密码访问的已命名 LDAP 服务器来启动一个 LDAP 会话。默认情况下，连接是在 TCP 端口 389 上。输入以下所需参数：
  - 姓名
  - 密码
  - 确认密码
  - 默认服务器 （服务器名称）
  - 默认端口 (389)
- 要启用 HTTP 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。或者，要继续，请参阅第 35-13 页的配置 OCSP 规则。

配置 OCSP 规则

ASA 按优先级顺序检查 OCSP 规则，并应用第一个匹配的规则。 X.509 数字证书可代替使用 CRL。

注　确保您已在尝试添加 OCSP 规则之前配置证书映射。如果未配置证书映射，系统将显示错误消息。要配置证书映射，请选择 **Configuration > Site-to-Site VPN > Advanced > Certificate to Connection Profile Maps > Rules > Add**。

要配置 OCSP 规则以获取 X.509 数字证书的撤销状态，请执行以下步骤：

步骤 1　在 ASDM 应用窗口中，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　在 Configuration Options for CA Certificates 窗格中，点击 **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。规则的优先级序号显示在 Index 字段中。此证书的 OCSP 服务器的 URL 显示在 URL 字段中。

步骤 4　要添加新的 OCSP 规则，请点击 **Add**。

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　输入规则的优先级序号。

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　要编辑现有的 OCSP 规则，请选择规则，然后点击 **Edit**。

步骤 11　要删除 OCSP 规则，请选择规则，然后点击 **Delete**。

步骤 12　点击 **OK** 以关闭此选项卡。或者，要继续，请参阅第 35-14 页的配置高级 CRL 和 OCSP 设置。

配置高级 CRL 和 OCSP 设置

证书颁发后，在固定时期内有效。有时， CA 会在此时期到期前撤销证书，例如，因为安全问题或名称变化或关联等原因而撤销。 CA 会定期发布签署的撤销证书列表。启用撤销检查可强制 ASA 检查 CA 是否未撤销正在验证的证书。 ASA 支持两种检查撤销状态的方法：CRL 和 OCSP。

要配置其他 CRL 和 OCSP 设置，请执行以下步骤：

步骤 1　在 ASDM 应用窗口中，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　在 Configuration Options for CA Certificates 窗格中，点击 **Advanced** 选项卡。

步骤 3　在 CRL Options 区域，以分钟为单位输入两次缓存刷新之间的时间。默认时间为 60 分钟。范围为 1-1440 分钟。为避免必须从 CA 重复检索相同的 CRL， ASA 可将检索的 CRL 存储在本地，这称为 CRL 缓存。 CRL 缓存容量根据平台而异，是所有情景的累计容量。如果尝试缓存新检索的 CRL 超出了其容量限制， ASA 将移除最近最少使用的 CRL，直到有更多的可用空间。

步骤 4　选中 **Enforce next CRL update** 复选框可要求有效的 CRL 具有未过期的 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 值或具有已过期的 Next Update 值。

步骤 5　在 OCSP Options 区域，输入 OCSP 服务器的 URL。 ASA 按照以下顺序使用 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，以加密方式将请求与响应绑定在一起以避免重放攻击。此过程的处理方式是，将请求中的扩展与响应中的扩展进行匹配，确保它们是相同的。如果您所使用的 OCSP 服务器发送不包含此匹配的 nonce 扩展的预生成响应，则取消选中 **Disable nonce extension** 复选框。

步骤 7　在 Other Options 区域，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 应从指定 CA 接受证书。
- 选中 **Accept certificates issued by the subordinate CAs of this CA** 复选框以指示 ASA 应从从属 CA 接受证书。

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。

后续操作

请参阅第 35-28 页的监控 CRL。

配置身份证书身份验证

身份证书可用于通过 ASA 对 VPN 访问进行身份验证。您还可以将身份证书用于使用 ASDM Launcher 访问 ASDM。请参阅 ASDM Identity Certificate Wizard 和 http://www.cisco.com/go/asdm-certificate 中的说明。

在 Identity Certificates Authentication 窗格中，可以执行以下任务：

- 添加或导入新的身份证书。
- 显示身份证书的详细信息。
- 删除现有的身份证书。
- 导出现有的身份证书。
- 导入现有的身份证书。
- 向 Entrust 注册身份证书。

- 第 35-16 页的添加或导入身份证书
- 第 35-17 页的显示身份证书详细信息
- 第 35-18 页的删除身份证书
- 第 35-18 页的导出身份证书
- 第 35-18 页的生成证书签名请求
- 第 35-19 页的安装身份证书

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：

步骤 1　在 ASDM 主应用窗口中，选择 **Configuration > Remote Access VPN > Certificate Management > Identity Certificates**。

步骤 2　点击 **Add**。

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　要从现有文件导入身份证书，请点击 **Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)** 单选按钮。

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　要添加新身份证书，请点击 **Add a new identity certificate** 单选按钮。

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　要使用默认密钥对名称，请点击 **Use default keypair name** 单选按钮。

步骤 10　要使用新密钥对名称，请点击 **Enter a new key pair name** 单选按钮，并键入新名称。ASA 支持多个密钥对。

步骤 11　从下拉列表中选择模值。如果不确定模值，请向 Entrust 查询。

步骤 12　点击 **General purpose** 单选按钮 （默认）或 **Special** 单选按钮，选择密钥对用途。如果选择 **Special** 单选按钮， ASA 将生成两个密钥对，一个用于签名，一个用于加密。这种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*只显示*信息：

- 要认证其公钥的密钥对的名称。
- 生成密钥的时间和日期。
- RSA 密钥对的用途。
- 密钥对的模值 （以位为单位）： 512、 768、 1024 和 2048。默认值为 1024。
- 密钥数据，它包含文本格式的特定密钥数据。

步骤 14　完成后点击 **OK** 以关闭 Key Pair Details 对话框。

步骤 15　选择要组成身份证书中的 DN 的证书使用者 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 属性如下所示：

- 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** 以关闭 Certificate Subject DN 对话框。

步骤 18　要创建自签名证书，请选中 **Generate self-signed certificate** 复选框。

步骤 19　要让身份证书充当本地 CA，请选中 **Act as local certificate authority and issue dynamic certificates to TLS proxy** 复选框。

步骤 20　要建立其他身份证书设置，请点击 **Advanced**。

系统将显示 Advanced Options 对话框，其中显示以下三个选项卡：Certificate Parameters、Enrollment Mode 和 SCEP Challenge Password。

注　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，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。
- 以点分十进制符号表示、由四部分组成的网络中的 ASA IP 地址。
- 要将 ASA 序列号添加到证书参数中，请选中 **Include serial number of the device** 复选框。

步骤 22　点击 **Enrollment Mode** 选项卡，然后输入以下信息：

- 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** 以关闭 Advanced Options 对话框。

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。

显示身份证书详细信息

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*只显示*选项卡：

- General 选项卡显示类型、序列号、状态、用途、公钥类型、 CRL 分发点、证书有效期和关联的信任点等值。这些值适用于可用和挂起状态。
- 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。

删除身份证书

要移除身份证书配置，请选择该配置，然后点击 **Delete**。

注　删除证书配置后，它将无法恢复。要重新创建删除的证书，请点击 **Add** 以重新输入所有证书配置信息。

导出身份证书

您可以 PKCS12 格式（这是公钥加密标准，可以是 base64 编码或十六进制格式）导出带所有关联密钥和证书的证书配置。完整配置包括整个链（根 CA 证书、身份证书、密钥对），而不是注册设置（使用者名称、FQDN 等）。此功能常用于故障转移或负载均衡配置以在一组 ASA 上复制证书；例如，呼叫中心组织（具有多个应答呼叫的单元）的远程访问客户端。这些单元必须具有等效的证书配置。在这种情况下，管理员可以导出证书配置，然后在一组 ASA 上将其导入。

要导出身份证书，请执行以下步骤：

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，以便查找要向其中导出证书配置的文件。

步骤 3　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

要生成发送到 Entrust 的证书签名请求，请执行以下步骤：

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，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，它将提供有关选定密钥对的信息，包括生成的日期和时间、用途（通用或特殊用途）、模值和密钥数据。

c. 完成后点击 **OK** 以关闭 Key Details 对话框。

d. 点击 **New** 以显示 Add Key Pair 对话框。要继续，请转至第 35-16 页的添加或导入身份证书的第 8 步。生成密钥对后，可将其发送到 ASA 或将其保存到文件中。

步骤 3　在 Certificate Subject DN 区域，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，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** 以从属性表中移除属性。

e. 完成后点击 **OK** 以关闭 Additional DN Attributes 对话框。

添加的属性将显示在 Additional DN Attributes 字段中。

步骤 5　如果 CA 需要，可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，之后您可将其发送**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　要完成注册过程，请点击 **request a certificate from Entrust** 链接，复制粘贴提供的 CSR 并通过 Entrust 网页表单 （在 http://www.entrust.net/cisco/ 上提供）进行提交。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** 链接以完成注册过程。

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。之后，您需要通过在 Identity Certificate 窗格中选择待处理的请求并点击 **Install**，安装证书。点击 **Close** 以关闭 Enroll with Entrust 对话框。

安装身份证书

除非某项注册处于待处理状态，否则 Identity Certificates 窗格上的 Install 按钮将显示为灰色。当 ASA 收到 CSR 时，Identity Certificates 窗格将显示待处理的 ID 证书。选择待处理的身份证书时，Install 按钮将激活。

将待处理的请求传输到 CA 时， CA 将注册该请求并将证书返回到 ASA。您收到证书之后，请点击 **Install** 并突出显示相应的身份证书以完成操作。

要安装待处理的身份证书，请执行以下步骤：

步骤 1　在 Identity Certificates 窗格中，请点击 **Add** 以显示 Add Identity Certificate 对话框。

步骤 2　在 Add Identity Certificate 对话框中，点击 **Add a new identity certificate** 单选按钮。

步骤 3　（可选）更改密钥对或创建新的密钥对。密钥对是必要的。

步骤 4　输入 Certificate Subject 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，请参阅第 35-15 页的配置身份证书身份验证中的第 17 至 23 步。

步骤 8　在 Add Identity Certificate 对话框中，点击 **Add Certificate**。

系统显示 Identity Certificate Request 对话框。

步骤 9　输入 CSR 文件的类型名称，文本，例如 c:\verisign-csr.txt，然后点击 **OK**。

步骤 10　将 CSR 文本文件发送给 CA。或者，您也可以将该文本文件粘贴到 CA 网站的 CSR 注册页面。

步骤 11　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　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。

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。

后续操作

请参阅第 35-20 页的配置代码签名证书。

配置代码签名证书

代码签名将数字签名附加到实际的可执行代码上。此数字签名提供了足够的信息来验证签名者身份，并确保代码在签名后未进行修改。

代码签名证书是其关联私钥用于创建数字签名的特殊证书。用于签署代码的证书从 CA 获取，其中的签名代码透露了证书来源。您可以在 Code Signer 窗格上导入代码签名证书，或选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Java Code Signer**。

在 Code Signer 窗格中，您可以执行以下任务：

- 显示代码签名证书的详细信息。
- 删除现有的代码签名证书。
- 导入现有的代码签名证书。
- 导出现有的代码签名证书。
- 向 Entrust 注册代码签名证书。

显示代码签名证书详细信息

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*只显示*选项卡：

- General 选项卡显示类型、序列号、状态、用途、公钥类型、 CRL 分发点、证书有效期和关联的信任点等值。这些值适用于可用和挂起状态。
- 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。

删除代码签名证书

要移除代码签名证书配置，请选择该配置，然后点击 **Delete**。

注　删除证书配置后，它将无法恢复。要重新创建删除的证书，请点击 **Import** 以重新输入所有证书配置信息。

导入代码签名证书

要导入代码签名证书，请执行以下步骤：

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证书配置。

导出代码签名证书

要导出代码签名证书，请执行以下步骤：

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，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，以便查找要向其中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。

后续操作

请参阅第 35-22 页的使用本地 CA 进行身份验证。

使用本地 CA 进行身份验证

本地 CA 提供了一种安全、可配置的内部机构进行证书身份验证，该机构驻留在 ASA 上，可与基于浏览器和基于客户端的 SSL VPN 连接配合使用。

用户通过登录指定网站进行注册。本地 CA 在 ASA 上集成了基本的证书授权操作，并且会部署证书，对已颁发的证书提供安全的撤销检查。

本地 CA 让您可以执行以下任务：

- 配置本地 CA 服务器。
- 撤销和取消撤销本地 CA 证书。
- 更新 CRL。
- 添加、编辑和删除本地 CA 用户。

- 第 35-22 页的配置本地 CA 服务器
- 第 35-25 页的删除本地 CA 服务器

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：

步骤 1　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（取消选中）。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　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。

自签名证书密钥用途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，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，并防止本地 CA 服务器被擅自关闭或意外关闭。如果本地 CA 证书或密钥对丢失且必须恢复，则需要使用该密码解锁 PKCS12 档案。

注　需要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的位置。

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，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仍在存储器中并且注册处于禁用状态。

配置的本地 CA 启用后，以下两个设置将处于*只显示*状态：

- Issuer Name 字段，列出颁发者的使用者名称和域名，由 username 和 subject-name-default DN 设置 cn=FQDN 组成。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，该值指定了 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 窗格中将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　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所需的设备上。

步骤 8　输入客户端证书有效期值，该值指定了由 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)。

在 SMTP Server & Email Settings 区域，通过指定以下设置为本地 CA 服务器设置邮件地址：

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** 以关闭 Browse Server Name/IP Address 对话框。

b.　使用 “adminname@hostname.com” 格式输入要用于向本地 CA 用户发送邮件的发件人地址。自动邮件会将一次性密码传送给新注册的用户并在证书需要续订或更新时发出邮件。

c.　输入主题，它指定了本地 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，默认主题为 “Certificate Enrollment Invitation”。

步骤 9　要配置其他选项，请点击 **More Options** 下拉箭头。

步骤 10　输入 CRL 分发点，即 ASA 上的 CRL 位置。默认位置为 http://hostname.domain/+CSCOCA+/asa_ca.crl。

步骤 11　要让 CRL 可用于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 1-65535 之间的任意端口号。默认端口号为 TCP 端口 80。

注　您无法重命名 CRL；它的名称始终为 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，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 12　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 将在每次撤销或取消撤销用户证书时更新和重新颁发 CRL，但如果未发生撤销变更，则会在每个 CRL 有效期后自动重新颁发一次 CRL。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 13　输入数据库存储位置以为本地 CA 配置和数据文件指定存储区域。ASA 可使用本地 CA 数据库访问和实施用户信息、已颁发的证书和撤销列表。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 14　从显示的文件夹列表中选择存储位置，然后点击 **OK**。

注　闪存可存储不超过 3500 个用户的数据库；超过 3500 个用户的数据库需要外部存储器。

步骤 15　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。允许的 DN 属性如以下列表所示：

- CN（公用名称）
- 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（州 / 省）
- T（标题）

步骤 16　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 OTP 有效期无关。默认值为 24 小时。

注　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 的网络浏览器进行。

步骤 17　输入电邮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。

步骤 18　输入向用户发送提醒邮件时距到期的天数。默认值为 14 天。

步骤 19　点击 **Apply** 以保存新的或修改的 CA 证书配置。或者，点击 **Reset** 以清除所有更改并返回原始设置。

删除本地 CA 服务器

要从 ASA 移除本地 CA 服务器，请执行以下步骤：

步骤 1　在 CA Server 窗格中，点击 **Delete Certificate Authority Server**。

系统将显示 Delete Certificate Authority 对话框。

步骤 2　要删除 CA 服务器，请点击 **OK**。要保留 CA 服务器，请点击 **Cancel**。

注　删除本地 CA 服务器后，将无法恢复或还原。要重新创建删除的 CA 服务器配置，必须重新输入所有 CA 服务器配置信息。

后续操作

请参阅第 35-25 页的管理用户数据库。

管理用户数据库

本地 CA 用户数据库包含用户识别信息和用户状态 （已注册、已允许、已撤销等）。在 Manage User Database 窗格中，您可以执行以下任务：

- 将用户添加到本地 CA 数据库。
- 更改现有的用户识别信息。
- 从本地 CA 数据库中移除用户。
- 注册用户。
- 更新 CRL。
- 将 OTP 电邮给用户。
- 查看或重新生成 （更换） OTP。

添加本地 CA 用户

要添加本地 CA 用户，请执行以下步骤：

步骤 1　要将新用户输入本地 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　输入现有的有效邮件地址。

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 属性如下所示：

- 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** 以关闭 Certificate Subject DN 对话框。

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。

发送初始 OTP 或更换 OTP

要自动向新添加的用户发送含唯一 OTP 和本地 CA 注册 URL 的注册许可通知邮件，请点击 **Email OTP**。

系统将显示一个信息对话框，指示 OTP 已发送给新用户。

要自动重新颁发新的 OTP 并将含新密码的通知邮件发送给现有用户或新用户，请点击 **Replace OTP**。

编辑本地 CA 用户

要修改有关数据库中现有的本地 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　输入现有的有效邮件地址。

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**。Certificate Subject DN 的可用 X.500 属性如下所示：

- 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** 以关闭 Certificate Subject DN 对话框。

步骤 7　选中 **Allow enrollment** 复选框以重新注册用户，然后点击 **Edit User**。

更新的用户详细信息将显示在 Manage User Database 窗格中。

删除本地 CA 用户

要从数据库中移除用户并从本地 CA 数据库中移除任何颁发给该用户的证书，请选择该用户，然后点击 **Delete**。

注　删除的用户无法恢复。要重新创建删除的用户记录，请点击 **Add** 以重新输入所有用户信息。

允许用户注册

要注册选定用户，请点击 A**llow Enrollment**。

在 Manage User Database 窗格中，用户状态更改为 “enrolled”。

注　如果用户已注册，系统会显示一条错误消息。

查看或重新生成 OTP

要查看或重新生成选定用户的 OTP，请执行以下步骤：

步骤 1　点击 **View/Regenerate OTP** 以显示 View & Regenerate OTP 对话框。

系统将显示当前的 OTP。

步骤 2　完成后，点击 **OK** 以关闭 View & Regenerate OTP 对话框。

步骤 3　要重新生成 OTP，请点击 **Regenerate OTP**。

系统将显示新生成的 OTP。

步骤 4　点击 **OK** 以关闭 View & Regenerate OTP 对话框。

后续操作

请参阅第 35-28 页的管理用户证书。

管理用户证书

要更改证书状态，请执行以下步骤：

步骤 1　在 Manage User Certificates 窗格中，按用户名或证书序列号选择特定证书。

步骤 2　选择以下选项之一：

- 如果要在用户证书有效期到期时删除用户访问权限，请点击 **Revoke**。本地 CA 还会在证书数据库中将证书标记为 “ 已撤销 ”，自动更新信息并重新颁发 CRL。
- 要恢复访问权限，请选择撤销的证书并点击 **Unrevoke**。本地 CA 还会在证书数据库中将证书标记为 “ 已取消撤销 ”，自动更新信息并重新颁发 CRL。

步骤 3　完成后点击 **Apply** 以保存更改。

后续操作

请参阅第 35-28 页的监控 CRL。

监控 CRL

要监控 CRL，请执行以下步骤：

步骤 1　在 ASDM 主应用窗口中，选择 **Monitoring > Properties > CRL**。

步骤 2　在 CRL 区域，从下拉列表中选择 CA 证书名称。

步骤 3　要显示 CRL 详细信息，请点击 **View CRL**。例如：

```
CRL Issuer Name:
    cn=asa4.cisco.com
    LastUpdate: 09:58:34 UTC Nov 11 2010
    NextUpdate: 15:58:34 UTC Nov 11 2010
    Cached Until: 15:58:34 UTC Nov 11 2010
    Retrieved from CRL Distribution Point:
      ** CDP Not Published - Retrieved via SCEP
    Size (bytes): 224
    Associated Trustpoints: LOCAL-CA-SERVER
```

步骤 4　完成后，点击 **Clear CRL** 以删除 CRL 详细信息并选择其他要查看的 CA 证书。

证书管理的功能历史

表 35-1　　证书管理的功能历史

功能名称	平台版本	功能信息
证书管理	7.0(1)	数字证书（包括 CA 证书、身份证书和代码签名证书）是一种用于身份验证的数字识别方式。数字证书包括识别设备或用户的信息，如名称、序列号、公司、部门或 IP 地址。CA 是“签署”证书以验证其真实性，从而确保设备或用户的身份的可信颁发机构。CA 在 PKI（使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。 我们引入了以下屏幕： Configuration > Remote Access VPN > Certificate Management Configuration > Site-to-Site VPN > Certificate Management。 我们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)	我们引入此此功能，可从第三方 CA 对设备证书进行安全部署。

第 8 部分

系统管理

第 36 章

管理访问

本章介绍如何通过 Telnet、 SSH 和 HTTPS （使用 ASDM）访问思科 ASA 进行系统管理、如何对用户进行身份验证和授权以及如何创建登录横幅。

注 要访问 ASA 接口进行管理访问，您也不需要允许主机 IP 地址的访问规则，只需根据本章内各节配置管理访问。

配置 ASDM、 Telnet 或 SSH 的 ASA 访问

本节介绍如何使客户端使用 ASDM、 Telnet 或 SSH 访问 ASA。

ASDM、 Telnet 或 SSH 的 ASA 访问许可要求

下表显示此功能的许可要求：

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

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

IPv6 准则

支持 IPv6。

型号准则

对于 ASASM，从交换机到 ASASM 的会话是 Telnet 会话，但是，不要求根据本节进行 Telnet 访问配置。

附加准则

- 除非使用 VPN 隧道中的 Telnet，否则，无法使用 Telnet 登录到最低安全接口。
- 不支持对进入 ASA 时所经由的接口以外的接口进行管理访问。例如，如果管理主机位于外部接口上，则只能发起直接到外部接口的管理连接。此规则的唯一例外是通过 VPN 连接。请参阅第 36-7 页的配置 VPN 隧道上的管理访问。
- ASA 允许：
  - 每个情景最多 5 个并发 Telnet 连接，在所有情景中最多分为 100 个连接 （如果有）。
  - 每个情景最多 5 个并发 SSH 连接，在所有情景中最多分为 100 个连接 （如果有）。
  - 每个情景最多 5 个并发 ASDM 连接，在所有情景中最多分为 32 个 ASDM 实例（如果有）。
- ASA 支持 SSH 第 1 版和第 2 版中提供的 SSH 远程外壳程序功能，并支持 DES 和 3DES 加密。
- 不支持通过 SSL 和 SSH 进行 XML 管理。
- （8.4 及更高版本）不再支持 SSH 默认用户名。使用 SSH 以及 **pix** 或 **asa** 用户名和登录密码 无法再连接至 ASA。要使用 SSH，则必须使用 命令 Configuration > Device Management > Users/AAA > AAA Access > Authentication 配置 AAA 身份验证；然后通过选择 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，我们建议也将本地身份验证配置为备用方法。
- （9.1(2) 及更高版本）已移除默认 Telnet 登录密码；使用 Telnet 前必须手动设置密码。请参阅第 14-1 页的设置主机名、域名及启用和 Telnet 密码。
- 如果无法建立到 ASA 接口的 Telnet 或 SSH 连接，请确保已根据第 36-1 页的配置 ASDM、Telnet 或 SSH 的 ASA 访问中的说明启用到 ASA 的 Telnet 或 SSH。

配置管理访问

要识别允许使用 Telnet、 SSH 或 ASDM 连接 ASA 的客户端 IP 地址，请执行以下步骤。

先决条件

在多情景模式中，请在情景执行空间中完成此操作步骤。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。

操作步骤

步骤 1　在 ASDM 中，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，此功能已启用。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) 密钥交换组 1 或组 14。用于密钥交换的 DH 组 1 和组 14 密钥交换方法在 ASA 上均受支持。如果未指定 DH 组密钥交换方法，则将使用 DH 组 1 密钥交换方法。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。

步骤 7　点击 **Apply**。

更改将保存到运行中的配置中。

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. 选择 **Configuration > Device Setup > Device Name/Password**。

b. 在 **Telnet Password** 区域，选中 **Change the password to access the console of the security appliance** 复选框。

c. 输入旧密码 （对于新 ASA，请将此字段留空）、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. 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，可以使用 AAA 服务器配置身份验证。

d. 点击 **Apply**。

e. 添加本地用户。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，用户可以进入 http://10.1.1.4/admin/ 或 https://10.1.8.4/admin/，同时到达在 HTTPS 地址的 ASDM 启动页面。

如果要启用重定向，为您支持进行 ASDM 访问的各个接口执行此操作步骤。

提示　在管理接口上的访问规则必须允许 HTTP 连接和 HTTPS 连接；这些协议通常分别使用端口 80 和 443。

步骤 1　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，请配置以下选项：

- Redirect HTTP to HTTPS - 是否将 HTTP 请求重定向至 HTTPS。
- HTTP Port - 识别接口从其重定向 HTTP 连接的端口。默认端口为 80。

步骤 4　点击 OK。

使用 Telnet 客户端

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。请参阅第 14-1 页的设置主机名、域名及启用和 Telnet 密码。

如果配置 Telnet 身份验证 （请参阅第 36-13 页的配置 CLI、和 enable 命令访问的身份验证），则请输入通过 AAA 服务器或本地数据库定义的用户名和密码。

使用 SSH 客户端

在管理主机上的 SSH 客户端中输入用户名和密码。当启动 SSH 会话时，系统将在 ASA 控制台上显示圆点 (.)，然后显示以下 SSH 用户身份验证提示符：

```
ciscoasa(config)#.
```

显示这个圆点不会影响 SSH 的功能。在用户身份验证发生之前的 SSH 密钥交换过程中，正在生成服务器密钥或正在使用私有密钥解密消息时，系统在控制台上显示这个圆点。完成这些任务可能需要两分钟或更长的时间。圆点是验证 ASA 繁忙和未暂停的进度指示器。

或者，可以配置公用密钥而不是使用密码。请参阅第 28-3 页的向本地数据库添加用户帐户。

配置 CLI 参数

CLI 参数许可要求

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

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单一和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

配置登录横幅

您可以配置在用户连接至 ASA 时、在用户登录之前或在用户进入特权 EXEC 模式之前将显示的消息。

限制

在添加横幅后，如果有以下情况，可能关闭至 ASA 的 Telnet 或 SSH 会话：

- 没有足够的系统内存可用来处理横幅消息。
- 在尝试显示横幅消息时发生 TCP 写入错误。

准则

- 从安全角度来看，重要的是横幅阻止未经授权的访问。请勿使用 “ 欢迎 ” 或 “ 请 ”，因为它们看起来似乎是在邀请入侵者进入。以下横幅设置对未经授权访问的正确语调：

  您已登录到安全设备。如果您无权访问此设备，请立即注销，否则可能有犯罪的风险。

- 有关横幅消息的准则，请参阅 RFC 2196。

要配置登录横幅，请执行以下步骤：

详细步骤

步骤 1　选择 **Configuration > Device Management > Management Access > Command Line (CLI) > Banner**, ，然后将横幅文本添加到将为 CLI 创建的横幅类型字段中：

- 当用户在 CLI 上访问特权 EXEC 模式时，系统将显示会话 (exec) 横幅。
- 当用户登录 CLI 时，系统将显示登录横幅。
- 当用户首次连接 CLI 时，系统将显示 message-of-the-day (motd) 横幅。
- 当用户通过用户身份验证并连接 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。
- 仅允许 ASCII 字符，包括换行符 （Enter，计为两个字符）。
- 请勿在横幅内使用制表符，因为它们没有保留在 CLI 版本内。
- 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 2　点击 **Apply**。

新的横幅保存到运行配置中。

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。在多情景模式中，提示符还显示情景名称。在 CLI 提示符中可以显示以下项目：

cluster-unit	（单模式和多模式）显示集群设备名称。集群中的每个设备都有一个唯一的名称。
context	（仅多模式）显示当前情景的名称。
domain	显示域名。
hostname	显示主机名。
priority	显示故障转移优先级为 pri （主要）或 sec （辅助）。
state	显示设备的流量传输状态。系统显示以下状态值： • act - 故障转移已启用，并且设备正在主动传输流量。 • stby - 故障转移已启用，并且设备当前没有传输流量，正处于备用、故障或其他非活动状态。 • actNoFailover - 故障转移未启用，并且设备正在主动传输流量。 • stbyNoFailover - 故障转移未启用，并且设备当前没有传输流量。在备用设备上存在高于阈值的接口故障时，可能出现这种情况。 显示集群内设备的角色 （主或从）。例如，在提示符 ciscoasa/cl2/slave 中，主机名为 ciscoasa，设备名称为 cl2，状态名称为 slave。

详细步骤

要自定义 CLI 提示符，执行以下步骤：

步骤 1　选择 **Configuration > Device Management > Management Access > Command Line (CLI) > CLI Prompt**，然后执行以下操作之一自定义提示符：

- 要向提示符添加属性，请点击 Available Prompts 列表内的属性，然后点击 **Add**。可以将多个属性添加到提示符中。属性从 Available Prompts 列表移到 Selected Prompts 列表中。
- 要从提示符移除属性，请点击 Selected Prompts 列表内的属性，然后点击 **Delete**。属性从 Selected Prompts 列表移到 Available Prompts 列表。
- 要更改属性在命令提示符中显示的顺序，请点击 Selected Prompts 列表中的属性并点击 **Move Up** 或 **Move Down** 更改该顺序。

提示符将更改并显示在 CLI Prompt Preview 区域。

步骤 2　点击 **Apply**。

新提示符保存到运行配置中。

更改控制台超时

控制台超时设置在特权 EXEC 模式或配置模式中连接可以保持的时间；达到超时的情况下，会话进入到用户 EXEC 模式。默认情况下，会话不会超时。此设置不会影响可保持控制台端口连接的时间，该连接永不超时。

要更改控制台超时，请执行以下步骤：

详细步骤

步骤 1　要定义以分钟为单位的新超时值，请选择 **Configuration > Device Management > Management Access > Command Line (CLI) > Console Timeout**。

步骤 2　要指定无限制时间，请输入 **0**。默认值为 0。

步骤 3　点击 **Apply**。

超时值更改并保存到运行配置中。

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，则可以将该接口识别为管理访问接口。例如，如果从外部接口进入 ASA，通过此功能可以使用 ASDM、 SSH、 Telnet 或 SNMP 连接内部接口；或者，当从外部接口进入时，可以 ping 内部接口。通过以下 VPN 隧道类型可以实现管理访问：IPsec 客户端、 IPsec 站到站和 AnyConnect SSL VPN 客户端。

- 第 36-8 页的管理接口的许可要求
- 第 36-2 页的准则和限制
- 第 36-8 页的配置管理接口

管理接口的许可要求

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

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单模式中受支持。

防火墙模式准则

在路由模式中受支持。

IPv6 准则

支持 IPv6。

附加准则

仅可以定义一个管理访问接口。

注　对于下面的配置，192.168.10.0/24 是 AnyConnect 或 IPsec VPN 客户端的 VPN 池。每个配置允许 VPN 客户端用户使用管理接口 IP 地址将 ASDM 或 SSH 连接至 ASA。

要仅允许 VPN 客户端用户访问 ASDM 或 HTTP（以及拒绝访问所有其他用户），请输入以下命令：

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.10.0 255.255.255.0 management_interface
```

要仅允许 VPN 客户端用户使用 SSH 访问 ASA （以及拒绝访问所有其他用户），请输入以下命令：

```
ciscoasa(config)# ssh 192.168.10.0 255.255.255.0 management_interface
```

配置管理接口

要配置管理接口，请执行以下操作：

详细步骤

步骤 1　在 Configuration > Device Management > Management Access > Management Interface 窗格中，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 2　点击 **Apply**。

分配管理接口并将更改保存到运行配置中。

配置系统管理员 AAA

本节介绍如何启用系统管理员的身份验证和命令授权。

有关系统管理员 AAA 的信息

本节介绍系统管理员 AAA。

有关管理身份验证的信息

本节介绍管理访问的身份验证。

比较有无身份验证的 CLI 访问

如何登录 ASA 取决于是否启用身份验证：

- No Authentication - 如果不启用 Telnet 的任何身份验证，则不输入用户名；请输入登录密码。（无身份验证时， SSH 不可用）。将访问用户 EXEC 模式。
- Authentication - 如果根据此节启用 Telnet 或 SSH 身份验证，请输入如 AAA 服务器或本地用户数据库所定义的用户名和密码。将访问用户 EXEC 模式。

要在登录后进入特权 EXEC 模式，请输入 **enable** 命令。 **enable** 如何使用取决于是否启用身份验证：

- No Authentication - 如果不配置启用身份验证，请在输入 **enable**。但是，如果不使用启用身份验证，在输入 **enable** 命令后，则不再以特定用户身份登录。为了保留用户名，请使用启用身份验证。
- Authentication - 如果配置启用身份验证， ASA 将再次提示您输入用户名和密码。当执行命令授权时此功能特别有用，因为用户名在确定用户可以输入的命令时非常重要。

对于使用本地数据库的启用身份验证，可以使用 **login** 命令，而不是 **enable** 命令。**login** 保留用户名，但不需要配置开启身份验证。

比较有无身份验证的 ASDM 访问

默认情况下，可以使用空的用户名和启用密码登录到 ASDM。请注意，如果在登录屏幕输入用户名和密码 （而不是将用户名留空），则 ASDM 将检查本地数据库是否有匹配项。

如果配置 HTTP 身份验证，则无法再使用空的用户名和启用密码来使用 ASDM。

对从交换机到 ASA 服务模块的会话进行身份验证

对于从交换机到 ASASM 的会话 （使用 **session** 命令），您可以配置 Telnet 身份验证。对于从交换机到 ASASM 的虚拟控制台连接 （使用 **service-module session** 命令），您可以配置串行端口身份验证。

在多情景模式中，您无法在系统配置中配置任何 AAA 命令。但是，如果在管理员情景中配置 Telnet 或串行身份验证，则身份验证也适用于从交换机到 ASASM 的会话。在此实例中使用管理员情景 AAA 服务器或本地用户数据库。

有关命令授权的信息

本节介绍命令授权。

- 第 36-10 页的支持的命令授权方法
- 第 36-11 页的关于用户凭证保留
- 第 36-11 页的安全情境和命令授权

支持的命令授权方法

您可以使用以下两种命令授权方法之一：

- 本地权限级别 - 在 ASA 上配置命令权限级别。当本地、RADIUS 或 LDAP（如果将 LDAP 属性映射到 RADIUS 属性）用户对 CLI 访问进行身份验证时， ASA 将该用户置于由本地数据库、 RADIUS 或 LDAP 服务器定义的权限级别中。用户可以访问分配的权限级别及此级别以下的命令。请注意，当所有用户首次登录时，他们都访问用户 EXEC 模式 （0 级或 1 级命令）。用户需要使用 **enable** 命令重新进行身份验证以进入特权 EXEC 模式 （2 级或更高级别命令），或者可以使用 **login** 命令登录 （仅适用于本地数据库）。

注　您可以使用本地命令授权，无需作为本地数据库的任何用户，也无需 CLI 或 **enable** 身份验证。在输入 **enable** 命令时，您却输入系统启用密码，从而 ASA 将您置于 15 级。然后您可以创建每个级别的启用密码，从而当输入 **enable** *n* （范围为 2 到 15）时， ASA 将您置于 *n* 级。除非启用本地命令授权 （请参阅第 36-19 页的配置本地命令授权），否则，不使用这些级别。（有关 **enable** 命令的详细信息，请参阅命令参考。）

- TACACS+ 服务器权限级别 - 在 TACACS+ 服务器上，配置用户或组在对 CLI 访问进行身份验证后可以使用的命令。用户在 CLI 输入的每个命令都使用 TACACS+ 服务器进行验证。

关于用户凭证保留

当用户登录到 ASA 时，该用户需要提供进行身份验证的用户名和密码。 ASA 保留这些会话凭证，以防以后在会话中需要进一步身份验证。

在以下配置就绪后，用户只需使用本地服务器进行登录的身份验证。随后的串行授权使用保存的凭证。系统还会提示用户输入 15 级权限的密码。当退出特权模式时，用户再次进行身份验证。在特权模式中不会保留用户凭据。

- 本地服务器配置为对用户访问进行身份验证。
- 15 级权限命令访问配置为需要密码才能实现。
- 用户帐户配置为仅串行授权 （无法访问控制台或 ASDM）。
- 用户帐户配置为 15 级权限命令访问。

下表显示在此情况下 ASA 如何使用凭证。

所需凭证	用户名和密码身份验证	串行 授权	特权模式命令授权	特权 模式退出授权
用户名	是	否	否	是
密码	是	否	否	是
特权模式密码	否	否	是	否

安全情境和命令授权

以下是在多个安全情境中实施命令授权时要考虑的重点：

- AAA 设置按每个情景分立，在情景中没有共享。

  在配置命令授权时，必须单独配置每个安全情境。此配置能够实现对不同安全情境执行不同的命令授权。

  在安全情境之间切换时，管理员应该清楚，在他们登录时指定的用户名所允许的命令在新的情景会话中可能不同，或者可能根本没有在新的情景中配置该命令授权。如果不知道安全情境之间的命令授权可能不同，这可能会使管理员感到困惑。该行为在下一点更为复杂。

- 无论在以前的情景会话中使用了哪个用户名，以 **changeto** 命令开始的新情景会话始终将默认 enable_15 用户名用作管理员身份。如果没有为 enable_15 用户配置命令授权，或者如果对 enable_15 用户的授权不同于对以前情景会话中的用户的授权，则此行为可能导致混淆。

  此行为也影响命令记帐，这只有在可以将发出的每个命令与特定管理员准确关联时才有用。由于有权限使用 **changeto** 命令的所有管理员都可以在其他情景中使用 enable_15 用户名，因此命令记帐记录可能不容易识别谁曾经以 enable_15 用户名登录系统。如果对每个情景都使用不同的记帐服务器，则跟踪谁曾经使用 enable_15 用户名需要从多个服务器关联数据。

  在配置命令授权时，请考虑以下事项：

  - 有权限使用 **changeto** 命令的管理员实际上有权限在每一个其他情景中使用 enable_15 用户可以使用的所有命令。
  - 如果要对每个情景授权不同命令，请确保在每个情景中拒绝 enable_15 用户名使用对有权使用 **changeto** 命令的管理员也拒绝的命令。

  在安全情境之间切换时，管理员可以退出特权 EXEC 模式并再次输入 **enable** 命令以使用所需的用户名。

注　系统执行空间不支持 AAA 命令；因此，命令授权在系统执行空间不可用。

系统管理员的 AAA 许可要求

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

先决条件

AAA 服务器或本地数据库的先决条件

您必须在 AAA 服务器或本地数据库中配置用户。对于 AAA 服务器，则需要配置 ASA 与其通信。请参阅以下各章：

- AAA 服务器 - 请参阅适用的 AAA 服务器类型一章。
- 本地数据库 - 请参阅第 28-3 页的向本地数据库添加用户帐户。

管理身份验证的先决条件

在 ASA 可以对 Telnet、SSH 或 HTTP 用户进行身份验证之前，必须识别允许与 ASA 通信的 IP 地址。对于 ASASM，在多情景模式中对系统进行访问是一个例外情况；从交换机到 ASASM 的会话是 Telnet 会话，但是无需进行 Telnet 访问配置。有关详细信息，请参阅第 36-1 页的配置 ASDM、 Telnet 或 SSH 的 ASA 访问。

本地命令授权的先决条件

- 配置 **enable** 身份验证。（请参阅第 36-13 页的配置 CLI、和 enable 命令访问的身份验证。）

  enable 身份验证对于在用户访问 **enable** 命令后保持用户名是很有必要的。

  或者，您可以使用 **login** 命令 （身份验证时与 **enable** 命令相同；仅适用于本地数据库），无需配置。因为它不如 **enable** 身份验证安全，所以不建议您使用此选项。

  您也可以使用 CLI 身份验证，但不是必需的。
- 请参阅每个用户类型的以下先决条件：
  - 本地数据库用户 - 在本地数据库中为每个用户配置 0 到 15 级权限。
  - RADIUS 用户 - 为用户配置思科 VSA CVPN3000 权限级别 0 到 15 之间的值。
  - LDAP 用户 - 为用户配置值在 0 到 15 之间的权限级别，然后根据第 31-5 页的配置 LDAP 属性映射将 LDAP 属性映射到思科 VSA CVPN3000 权限级别。

TACACS+ 命令授权的先决条件

- 配置 CLI 和 **enable** 身份验证（请参阅第 36-13 页的配置 CLI、和 enable 命令访问的身份验证）。

管理记帐的先决条件

- 配置 CLI 和 **enable** 身份验证（请参阅第 36-13 页的配置 CLI、和 enable 命令访问的身份验证）。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

在单情景和多情景模式中受支持。

防火墙模式准则

在路由和透明防火墙模式中均受支持。

IPv6 准则

支持 IPv6。

默认设置

默认命令权限级别

默认情况下，以下命令会分配到 0 级权限。所有其他命令会分配到 15 级权限。

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

如果将任何配置模式命令移到低于 15 的级别，请确保也将 **configure** 命令移到该级别，否则，用户将无法进入配置模式。

要查看所有权限级别，请参阅第 36-20 页的查看本地命令的权限级别。

配置 CLI、和 enable 命令访问的身份验证

您可以要求进行 CLI、 ASDM 和 enable 命令访问的身份验证。

先决条件

- 根据第 36-1 页的配置 ASDM、 Telnet 或 SSH 的 ASA 访问配置 Telnet、 SSH 或 HTTP 访问。
- 对于 SSH 访问，必须配置 SSH 身份验证；无默认用户名。

详细步骤

步骤 1　要对使用 **enable** 命令的用户进行身份验证，请选择 **Configuration > Device Management > Users/AAA > AAA Access > Authentication**，并配置以下设置：

a. 选中 **Enable** 复选框。

b. 从 Server Group 下拉列表中选择服务器组名称或 LOCAL 数据库。

c. （可选）如果选择 AAA 服务器，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。点击 **Use LOCAL when server group fails** 复选框。我们建议您在本地数据库中使用与 AAA 服务器相同的用户名和密码，因为 ASA 提示符不会给出使用何种方法的任何指示。

步骤 2　要对访问 CLI 或 ASDM 的用户进行身份验证，请选择 **Configuration > Device Management > Users/AAA > AAA Access > Authentication**，并配置以下设置：

a. 选中一个或多个以下复选框：

- **HTTP/ASDM** - ASDM 对使用 HTTPS 访问 ASA 的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。对于多模式访问，请参阅第 36-10 页的对从交换机到 ASA 服务模块的会话进行身份验证。
- **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。对于多模式访问，请参阅第 36-10 页的对从交换机到 ASA 服务模块的会话进行身份验证。

b. 对于选中的每个服务，请从 Server Group 下拉列表中选择服务器组名称或 LOCAL 数据库。

c. （可选）如果选择 AAA 服务器，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。点击 **Use LOCAL when server group fails** 复选框。我们建议您在本地数据库中使用与 AAA 服务器相同的用户名和密码，因为 ASA 提示符不会给出使用何种方法的任何指示。

步骤 3　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。用户角色差异化可防止远程访问 VPN 和网络访问用户建立到 ASA 的管理连接。

注　串行访问未包含在管理授权内，因此，如果您配置 命令启用 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。

详细步骤

步骤 1　选择以下选项之一：

- 要启用管理授权，请选择 **Configuration > Device Management > Users/AAA > AAA Access > Authorization**，然后选中 **Perform authorization for exec shell access > Enable** 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。

  此选项也启用通过 RADIUS 对管理用户权限级别提供的支持，这些权限级别可与本地命令权限级别配合使用进行命令授权。有关详细信息，请参阅第 36-19 页的配置本地命令授权。

  当配置 **authentication-server** 选项时，可使用同一服务器进行身份验证和授权。

- 要启用管理授权，请选择 **Configuration > Device Management > Users/AAA > AAA Access > Authorization**，然后选中 **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 模式必须的 Service-Type 和 Privilege-Level 属性决定。要进入特权 EXEC 模式，用户必须具有 Administrative 的 Service-Type 属性和分配给这些用户的大于 1 的 Privilege Level 属性。

  在系统情景中不支持此选项。但是，如果在管理员情景中配置 Telnet 或串行身份验证，则身份验证也适用于从交换机到 ASASM 的会话。

  如果单独输入 **aaa authorization exec** 命令，则没有影响。

  在管理授权中使用串行身份验证时，不包括 **auto-enable** 选项。

  auto-enable 选项不会影响 **aaa authentication http** 命令。

  在配置 **auto-enable** 选项之前，我们建议您同时配置协议登录和启用身份验证，使所有身份验证请求都转至相同的 AAA 服务器组，如以下示例所示：

  ```
  ciscoasa (config)# aaa authentication ssh console RADIUS
  ciscoasa (config)# aaa authentication enable console RADIUS
  ciscoasa (config)# aaa authorization exec authentication-server auto-enable
  ```

  我们*不*建议您使用其他类型的配置。

步骤 2　要配置用户进行管理授权，请参阅每个 AAA 服务器类型或本地用户的以下要求：

RADIUS 或 LDAP （已映射）用户

当用户通过 LDAP 进行身份验证时，本地 LDAP 属性及其值可以映射到思科 ASA 属性以提供特定授权功能。为思科 VSA CVPN3000 权限级别配置 0 到 15 之间的值。然后，将 LDAP 属性映射到思科 VAS CVPN3000 权限级别。有关详细信息，请参阅第 31-5 页的配置 LDAP 属性映射。

当 RADIUS IETF **service-type** 属性作为 RADIUS 身份验证和授权请求的结果在访问接受消息中进行发送时，其用于表示授予通过身份验证的用户的服务类型：

- Service-Type 6 (Administrative) - 允许对通过 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 身份验证选项时对 CLI 进行访问，但是，如果配置 HTTP 选项，则拒绝 ASDM 配置访问。允许进行 ASDM 监控访问。如果使用 **aaa authentication enable console** 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）用户仍然可以进行身份验证并终止其远程访问会话。所有其他类型 （Voice、 FAX 等）按同一方式处理。

在访问接受消息中发送 RADIUS Cisco VSA **privilege-level** 属性 (Vendor ID 3076, sub-ID 220) 时，该属性用于表示用户的权限级别。

当通过身份验证的用户尝试通过 ASDM、 SSH 或 Telnet 对 ASA 进行管理访问，但没有相应的权限级别实现此操作时，则 ASA 将生成系统日志消息 113021。此消息会通知用户，由于不适当的管理权限，尝试登录失败。

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 and higher - 允许在配置 Telnet 或 SSH 身份验证选项时对 CLI 进行访问，但是，如果配置 HTTP 选项，则拒绝 ASDM 配置访问。允许进行 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。您无法使用由 Authentication 选项卡选项指定的任何服务 （不包括 Serial 选项；允许进行串行访问）。

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。有关详细信息，请参阅第 28-3 页的向本地数据库添加用户帐户。

为本地数据库用户配置密码策略

您使用本地数据库配置身份验证进行 CLI 或 ASDM 访问时，可以配置密码策略，该策略要求用户在指定的时间后更改其密码，还规定密码标准，例如最短长度和更改后的最小字符数。

密码策略仅适用于使用本地数据库的管理用户，而不适用于可以使用本地数据库的其他流量类型，例如网络访问的 VPN 或 AAA，也不适用于通过 AAA 服务器进行身份验证的用户。

- 第 36-16 页的配置密码策略
- 第 36-18 页的更改密码

配置密码策略

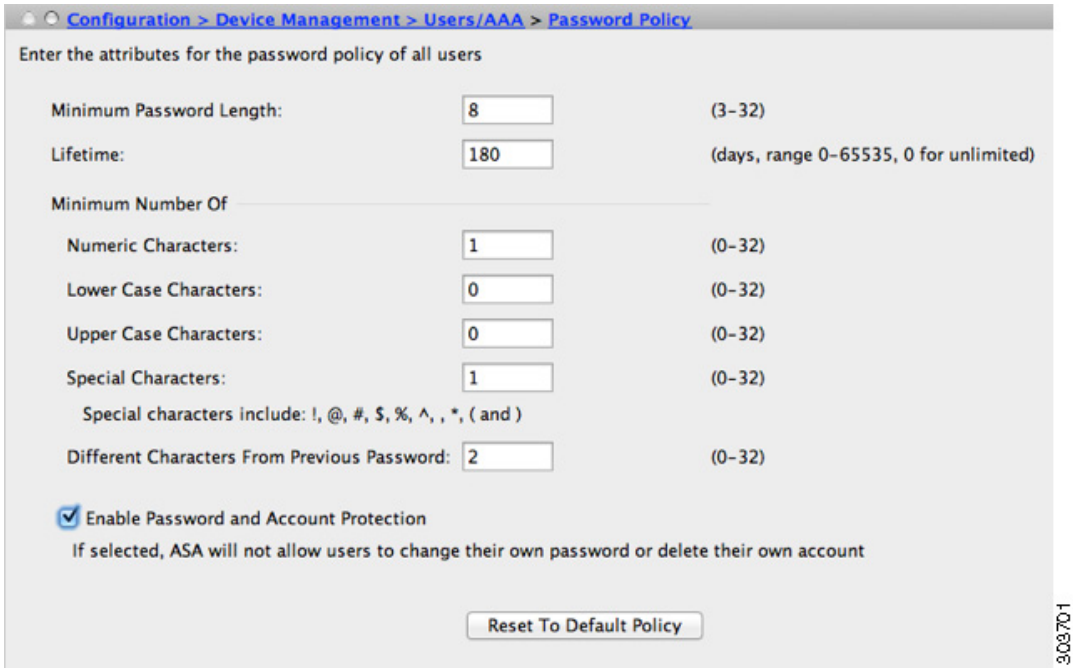
配置密码策略后，当您更改密码 （自己本人的或其他用户的）时，密码策略将应用于新密码。任何现有密码都受新策略约束。使用 User Accounts 窗格更改密码时，以及使用 Change My Password 窗格 更改密码时，将应用新策略。

先决条件

- 根据第 36-13 页的配置 CLI、和 enable 命令访问的身份验证配置 CLI/ASDM 和 enable 身份验证。请确保指定本地数据库。

详细步骤

步骤 1　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）密码到期前的天数间隔；控制台端口的用户不会由于密码到期而锁定。有效值为 0 和 65536 天之间。默认值为 0 天，表示密码不会到期。

  在密码到期前 7 天，系统会显示警告消息。在密码到期后，拒绝远程用户访问系统。要在到期后访问，请执行以下步骤：

  - 让另一个管理员更改密码。
  - 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 和 64 个字符之间。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：！、@、#、$、%、^、&、*、'(‘ 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 和 64 个字符之间。默认值为 0。字符匹配与位置无关，意味着只有新密码字符不在当前密码的任何地方出现时才视为被更改。

步骤 3　（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。默认设置被禁用：用户可以使用任何一种方法更改密码。

如果启用此功能，当尝试在 User Accounts 窗格中更改密码时，系统会生成以下错误消息：

```
ERROR: Changing your own password is prohibited
```

步骤 4　要将密码策略重置为默认值，请点击 **Reset to Default**。

步骤 5　点击 **Apply** 以应用配置设置。

更改密码

如果在密码策略内配置密码有效期，则需要在旧密码到期时将 密码更改为新密码。如果启用密码策略身份验证，此密码更改方法是必需的。如果未启用密码策略身份验证，则可以使用此方法，或者直接使用 User Accounts 窗格更改用户帐户。

详细步骤

步骤 1　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，在其中可以确定对用户可用的命令。默认情况下，当登录时，可以访问用户 EXEC 模式，此模式仅提供最小数量的命令。当输入 **enable** 命令 （或在使用本地数据库时输入 **login** 命令），则可以访问特权 EXEC 模式和高级命令（包括配置命令）。

您可以使用以下两种命令授权方法之一：

- 本地权限级别
- TACACS+ 服务器权限级别

有关命令授权的详细信息，请参阅第 36-10 页的有关命令授权的信息。

- 第 36-19 页的配置本地命令授权
- 第 36-20 页的查看本地命令的权限级别
- 第 36-20 页的在 Commands TACACS+ 服务器上配置命令
- 第 36-23 页的配置 TACACS+ 命令授权

配置本地命令授权

通过本地命令授权可以为 16 个权限级别 （0 到 15）之一分配命令。默认情况下，会向每个命令分配 0 级或 15 级权限。您可以将每个用户定义在特定权限级别，并且，每个用户可以输入在分配权限级别或以下的任何命令。 ASA 支持在本地数据库、 RADIUS 服务器或 LDAP 服务器 （如果将 LDAP 属性映射到 RADIUS 属性）中定义的用户权限级别。有关详细信息，请参阅以下各节：

- 第 28-3 页的向本地数据库添加用户帐户
- 第 29-2 页的支持的身份验证方法
- 第 31-5 页的配置 LDAP 属性映射

要配置本地命令授权，请执行以下步骤：

详细步骤

步骤 1　要启用命令授权，请选择 **Configuration > Device Management > Users/AAA > AAA Access > Authorization**，然后选中 **Enable authorization for command access > Enable** 复选框。

步骤 2　从 Server Group 下拉列表中选择 LOCAL。

步骤 3　当启用本地命令授权时，您可以选择手动向单个命令或命令组分配权限级别，或者启用预定义的用户帐户权限。

- 要使用预定义的用户帐户权限，请点击 **Set ASDM Defined User Roles**。

  ASDM Defined User Roles Setup 对话框中将显示这些命令及其级别。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，仅访问监控部分）。

- 要手动配置命令级别，请点击 **Configure Command Privileges**。

  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，或者也可以选择配置模式以查看该模式中可用的命令。例如，如果选择情景，则可以查看该情景配置模式中的所有可用命令。如果可以在用户 EXEC 或特权 EXEC 模式中以及配置模式中输入命令，并且命令在各个模式中执行不同的操作，则您可以分别设置这些模式的权限级别。

Variant 列显示 show、 clear 或 cmd。您可以仅为命令的显示、清除或配置形式设置权限。命令的配置形式通常是导致配置更改的形式，或者是以未修改的命令形式（无 **show** 或 **clear** 前缀），或者是以 **no** 形式。

要更改命令级别，请双击此命令或点击 **Edit**。您可以将级别设置在 0 和 15 之间。您只能配置主命令的权限级别。例如，可以配置所有 aaa 命令的级别，但是不可以单独配置 **aaa authentication** 命令和 **aaa authorization** 命令的级别。

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 4　为了支持来自 RADIUS 的管理用户权限级别，请选中 **Perform authorization for exec shell access > Enable** 复选框。

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。

此选项还启用本地、 RADIUS、已映射 LDAP 和 TACACS+ 用户的管理授权。有关详细信息，请参阅第 36-14 页的使用管理授权限制用户的 CLI 和 ASDM 访问。

步骤 5　点击 **Apply**。

系统成功分配授权设置，并且将更改保存到运行配置中。

查看本地命令的权限级别

在 Tools > Command Line Interface 工具中输入以下命令后，可以查看命令的权限级别。

在 Commands TACACS+ 服务器上配置命令

您可以在思科安全访问控制服务器 (ACS) TACACS+ 服务器上，为组或为单个用户将命令配置为共享配置文件组件。对于第三方 TACACS+ 服务器，有关命令授权支持的详细信息，请参阅服务器文档。

请参阅以下在思科安全 ACS 3.1 版本中配置命令的准则；许多这些准则也适用于第三方服务器。

- ASA 将待授权的命令作为外壳命令发送，因此请在 TACACS+ 服务器上将命令配置为外壳命令。

注　思科安全 ACS 可能包括称为“pix-shell”的命令类型。请勿将此类型用于 ASA 命令授权。

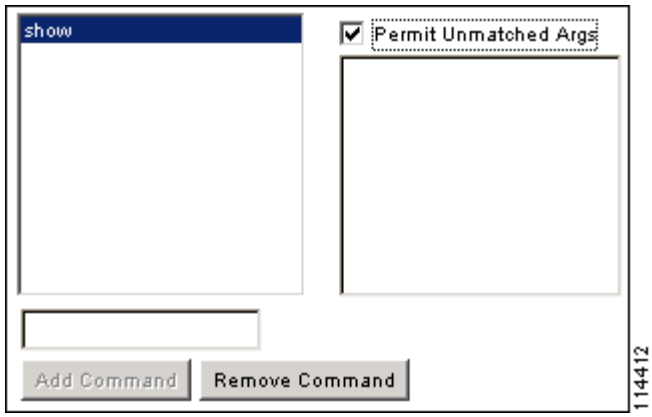
- 命令的第一个词被视为主命令。所有附加的单词都被视为参数，需要在其前面放置 **permit** 或 **deny**。

  例如，要允许 **show running-configuration aaa-server** 命令，请向命令字段添加 **show running-configuration**，然后在参数字段键入 **permit aaa-server**。

- 您可以通过选中 **Permit Unmatched Args** 复选框，允许不会明确拒绝的命令的所有参数。

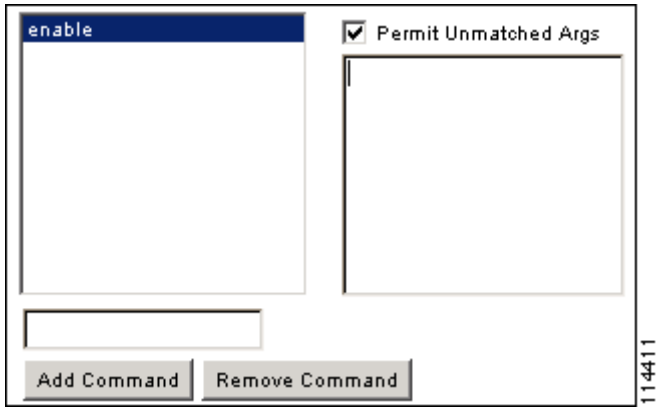
  例如，您可以仅配置 **show** 命令，那么将允许所有 **show** 命令。我们建议使用此方法，这样您就无需预测命令的每个变量（包括缩写和问号），其显示 CLI 的使用情况（请参阅图 36-1）。

图 36-1　　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**（请参阅图 36-2）。

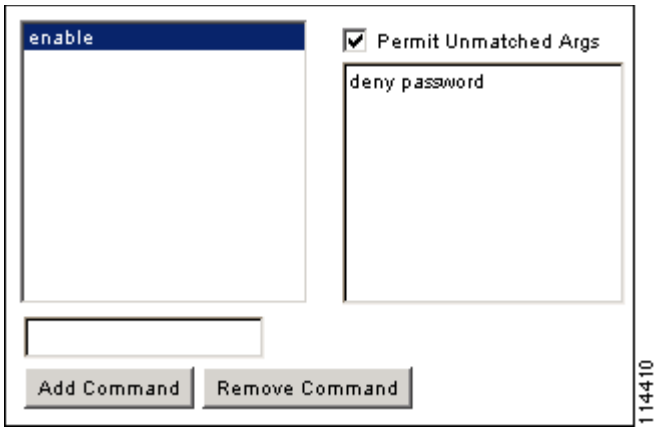
图 36-2　　允许单个单词命令



- 要禁止某些参数，请输入参数并在前面放置 **deny**。

  例如，要允许 **enable**，但不允许 **enable password**，请在命令字段中输入 **enable**，在参数字段内输入 **deny password**。确保选中 **Permit Unmatched Args** 复选框，这样仍能单独允许 **enable**（请参阅图 36-3）。

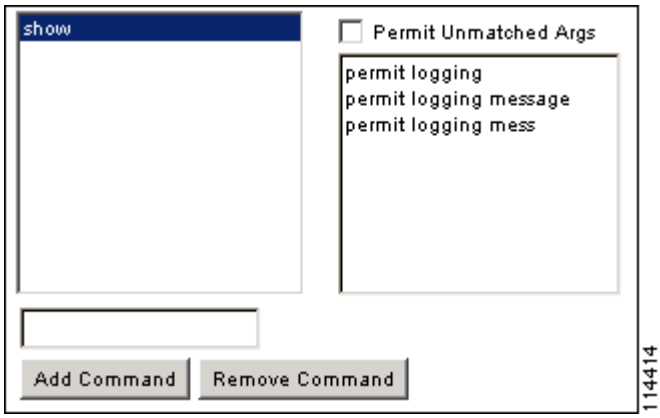
图 36-3　　禁止参数



- 当缩写命令行中的命令时， ASA 将前缀和主 命令扩展为全文本，但是您输入过程中，它将附加参数发送到 TACACS+ 服务器。

  例如，如果您输入 **sh log**，那么 ASA 将整个 **show logging** 命令发送到 TACACS+ 服务器。但是，如果您输入 **sh log mess**，那么 ASA 将 **show logging mess** 命令发送到 TACACS+ 服务器，而不是发送扩展的 **show logging message** 命令。您可以将同一参数的多种拼写配置为预期缩写 （请参阅图 36-4）。

图 36-4　　指定缩写



- 我们建议您允许所有用户使用以下基本命令：
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**
  - **logout**
  - **pager**
  - **show pager**

- **clear pager**
- **quit**
- **show version**

配置 TACACS+ 命令授权

如果启用 TACACS+ 命令授权，且用户在 CLI 输入命令，则 ASA 将向 TACACS+ 服务器发送命令和用户名以确定命令是否经过授权。

在启用 TACACS+ 命令授权之前，请确保您已经以在 TACACS+ 服务器上定义的用户身份登录 ASA，并且具有必要的命令授权来继续配置 ASA。例如，您应该以授权所有命令的管理员用户身份登录。否则，可能会意外锁定。

请勿保存配置，直到您确定配置会以所需的方式发挥作用。如果由于错误发生锁定，通常您可以通过重新启动 ASA 恢复访问。如果仍然锁定，请参阅第 36-25 页的从锁定中恢复。

请确保 TACACS+ 系统完全稳定且可靠。必要的可靠性级别通常需要完全冗余的 TACACS+ 服务器系统和完全冗余的 ASA 连接性。例如，在 TACACS+ 服务器池中，包括一个连接至接口 1 的服务器 和另一个连接至接口 2 的服务器。如果 TACACS+ 服务器不可用，您也可以将本地命令授权配置为回退方法。在这种情况下，您需要根据第 36-19 页的配置命令授权中列出的操作步骤配置本地用户和命令权限级别。

要配置 TACACS+ 命令授权，执行以下步骤：

详细步骤

步骤 1　要使用 TACACS+ 服务器执行命令授权，请选择 **Configuration > Device Management > Users/AAA > AAA Access > Authorization**，然后选中 **Enable authorization for command access > Enable** 复选框。

步骤 2　从 Server Group 下拉列表中选择 AAA 服务器组名称。

步骤 3　（可选）如果 AAA 服务器不可用，则您可以配置 ASA 使用本地数据库作为回退方法。要执行此操作，请选中 **Use LOCAL when server group fails** 复选框。我们建议您在本地数据库中使用与 AAA 服务器相同的用户名和密码，因为 ASA 提示符不会给出使用何种方法的任何指示。请确保在本地数据库 （请参阅第 28-3 页的向本地数据库添加用户帐户）和命令权限级别 （请参阅第 36-19 页的配置本地命令授权）中配置用户。

步骤 4　点击 **Apply**。

系统成功分配命令授权设置，并且将更改保存到运行配置中。

配置管理访问记帐

在 CLI 中输入 **show** 命令之外的任何命令时，您可以将记帐消息发送到 TACACS+ 记帐服务器。您可以在用户登录时、输入 **enable** 命令时或者发出命令时配置记帐。

对于命令记帐，您只可以使用 TACACS+ 服务器。

要配置管理访问和 enable 命令记帐，请执行以下步骤：

详细步骤

步骤 1　要在用户输入 **enable** 命令时启用用户记帐，请执行以下步骤：

a. 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. 从 Server Group 下拉列表中选择 RADIUS 或 TACACS+ 服务器组名称。

步骤 2　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 区域下，选中 Serial、 SSH 和 / 或 Telnet 复选框。

b. 对于每种连接类型，从 Server Group 下拉列表中选择 RADIUS 或 TACACS+ 服务器组的名称。

步骤 3　要配置命令记帐，请执行以下步骤：

a. 在 Require command accounting 区域下，选中 **Enable** 复选框。

b. 从 Server Group 下拉列表中选择 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，您可以将记帐消息发送到 TACACS+ 记帐服务器。

c. 如果您使用 Command Privilege Setup 对话框自定义命令权限级别，则可以通过在权限级别下拉列表中指定最小权限级别来限定 ASA 对哪些命令进行记帐。 ASA 不对在最小权限级别以下的命令进行记帐。

步骤 4　点击 **Apply**。

系统成功分配记帐设置，并且将更改保存到运行配置中。

查看当前登录用户

要查看当前登录用户，请在 Tools > Command Line Interface tool 中：

```
ciscoasa# show curpriv
```

示例

以下是 **show curpriv** 命令的输出示例：

```
ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

表 36-1 介绍 **show curpriv** 命令输出。

表 36-1　　show curpriv 命令输出说明

字段	说明
Username	用户名。如果您以默认用户身份登录，则名称是 enable_1 （用户 EXEC）或 enable_15 （特权 EXEC）。
Current privilege level	级别范围为 0 到 15。除非您配置本地命令授权并为中间权限级别分配命令，否则只能使用 0 级和 15 级。
Current Modes	可用的访问模式如下： • P_UNPR - 用户 EXEC 模式 （0 级和 1 级） • P_PRIV - 特权 EXEC 模式 （2 级到 15 级） • P_CONF - 配置模式

设置管理会话配额

您可以建立同步管理会话的最大数量。如果达到最大值，则不允许其他会话，并生成系统日志消息。要防止系统锁定，则管理会话配额机制无法阻止控制台会话。

要设置管理会话配额，执行以下步骤：

步骤 1　选择 **Configuration > Device Management > Management Access > Management Session Quota**。

步骤 2　输入在 ASA 上允许的同步 ASDM、 SSH 和 Telnet 会话的最大数量。有效值范围为 0 到 10000。

注　如果超过管理配额会话数量，则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。表 36-2 列出常见锁定条件以及如何从中恢复：

表 36-2　　CLI 身份验证和命令授权锁定场景

功能	锁定条件	说明	解决方法：单模	解决方法：多模
本地 CLI 身份验证	未在本地数据库中配置用户。	如果本地数据库中没有用户，则您无法登录，并且无法添加任何用户。	登录并重置密码和 **aaa** 命令。	从交换机会话到 ASA。从系统执行空间，您可以变更到情景并添加用户。
TACACS+ 命令授权 TACACS+ CLI 身份验证 RADIUS CLI 身份验证	服务器关闭或无法访问，且没有配置回退方法。	如果服务器无法访问，则您无法登录或无法输入任何命令。	1. 登录并重置密码和 AAA 命令。 2. 将本地数据库配置为回退方法，这样服务器关闭时不会锁定。	1. 如果服务器由于 ASA 上的网络配置不正确而无法访问，则请从交换机会话到 ASA。从系统执行空间，您可以变更到情景并重新配置网络设置。 2. 将本地数据库配置为回退方法，这样服务器关闭时不会锁定。
TACACS+ 命令授权	您以没有足够权限的用户或不存在的用户身份登录。	启用命令授权，但是然后发现用户无法再输入任何命令。	修复 TACACS+ 服务器用户帐户。 如果无法访问 TACACS+ 服务器，并且需要立即配置 ASA，则请登录维护分区并重置密码和 **aaa** 命令。	从交换机会话到 ASA。从系统执行空间，您可以变更到情景并完成配置更改。您也可以禁用命令授权，直到修复 TACACS+ 配置。
本地命令授权	您以没有足够权限的用户登录。	启用命令授权，但是然后发现用户无法再输入任何命令。	登录并重置密码和 **aaa** 命令。	从交换机会话到 ASA。从系统执行空间，您可以变更到情景并更改用户级别。

监控设备访问

要监控设备访问，请参阅以下窗格：

路径	用途
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。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、基于时间重新生成密钥和上次重新生成密钥的时间。要断开特定会话，请点击 **Disconnect**。
Monitoring > Properties > Device Access > Authenticated Users	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	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。要清除锁定的特定用户，请点击 **Clear Selected Lockout**。要清除锁定的所有用户，请点击 **Clear All Lockouts**。

管理访问的功能历史记录

表 36-3 列出了各种功能变更以及实施该等功能变更的平台版本。 ASDM 可向后兼容多个平台版本，因此，未列出已添加支持的具体 ASDM 版本。

表 36-3　　管理访问的功能历史记录

功能名称	平台版本	功能信息
管理访问	7.0(1)	我们引入了此功能。 我们引入了以下屏幕： 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。要使用 SSH，您必须使用 **aaa authentication ssh console LOCAL** 命令 (CLI) 或 Configuration > Device Management > Users/AAA > AAA Access > Authentication 配置 AAA 身份验证；然后通过输入 **username** 命令 (CLI) 或选择 Configuration > Device Management > Users/AAA > User Accounts (ASDM) 定义本地用户。如果要使用 AAA 服务器而不是本地数据库进行身份验证，我们建议也将本地身份验证配置为备用方法。
使用本地数据库时，支持管理员密码策略。	8.4(4.1)、9.1(2)	您使用本地数据库配置身份验证进行 CLI 或 ASDM 访问时，可以配置密码策略，该策略要求用户在指定的时间后更改其密码，还规定密码标准，例如最短长度和更改后的最小字符数。 我们引入了以下屏幕：Configuration > Device Management > Users/AAA > Password Policy。

表 36-3　　管理访问的功能历史记录 （续）

功能名称	平台版本	功能信息
对 SSH 公钥身份验证的支持	8.4(4.1)、9.1(2)	您可以基于每个用户启用到 ASA 的 SSH 连接的公钥身份验证。您可以指定公钥文件 (PKF) 格式的密钥或 Base64 密钥。 PKF 密钥的长度可达 4096 位。对于由于过长而导致 ASA 不支持使用 Base64 格式 （限长 2048 位）的密钥，请使用 PKF 格式。 我们引入了以下屏幕： 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 SSH 密钥交换的 Diffie-Hellman 群 14	8.4(4.1)、9.1(2)	已添加支持 Diffie-Hellman 群 14 进行 SSH 密钥交换 以前，只支持组 1。 我们修改了以下屏幕：Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH。
支持最大数量的管理会话	8.4(4.1)、9.1(2)	您可以设置同步 ASDM、SSH 和 Telnet 会话的最大数量。 我们引入了以下屏幕：Configuration > Device Management > Management Access > Management Session Quota。
对于在多情景模式中的 ASASM，支持从交换机进行 Telnet 和虚拟控制台身份验证。	8.5(1)	虽然从多情景模式中的交换机连接至 ASASM 也连接至系统执行空间，但是您可以在管理员情景中配置身份验证以监管这些连接。
SSH 的 AES-CTR 加密	9.1(2)	ASA 中的 SSH 服务器实施现在支持 AES - CTR 模式加密。
改进的 SSH 重新生成密钥间隔		在连接时间达到 60 分钟后或数据流量达到 1 GB 后，SSH 连接重新生成密钥。
改进的一次性密码身份验证	9.2(1)	有足够授权权限的管理员可以通过输入自己的身份验证凭证一次进入特权 EXEC 模式。 **auto-enable** 选项已添加到 **aaa authorization exec** 命令中。 我们修改了以下屏幕：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

升级路径和迁移

- 如果您从 9.0 之前的版本升级，由于 ACL 迁移，您以后可能无法执行降级；如果您想要降级，请务必备份您的配置文件。有关详细信息，请参阅 9.0 升级指南中的 ACL 迁移章节。
- 要将 9.1(2.8) 之前的版本升级至 9.1(2.8) 或更高版本，您必须正在运行以下任一版本：
  - 8.4(5) 或更高版本
  - 9.0(2) 或更高版本
  - 9.1(2)

如果您运行任意*早期*版本，则必须*先*升级至以上任一版本，否则无法直接升级至 9.1(2.8) 或更高版本。例如：

9.1(2.8) 之前的 ASA 版本	首先升级到：	然后升级到：
8.2(1)	8.4(7)	9.3(1) 或更高版本
8.4(4)	8.4(7)	9.3(1) 或更高版本
9.0(1)	9.0(4)	9.3(1) 或更高版本
9.1(1)	9.1(2)	9.3(1) 或更高版本

- 如果您将从 8.3 之前的版本升级：
  - 有关迁移配置的重要信息，请参阅 *《至 8.3 版本的思科 ASA 5500 迁移指南》*。
  - 您无法直接升级到 9.0 或更高版本。要成功迁移，您必须先升级至 8.4 版本。
- 零停机时间升级的软件版本要求：

  故障转移配置或 ASA 集群中的设备应具有相同的主要 （第一个编号数字）和次要 （第二个编号）软件版本。然而，在升级过程中，您不需要使设备保持版本相同；您可在每台设备上运行不同版本的软件，并且仍然保持故障转移支持。为确保长期的兼容性和稳定性，我们建议尽可能地将所有设备升级至相同版本。

  表 37-1 展示了执行零停机时间升级的受支持方案。

表 37-1　　零停机时间升级支持

升级类型	支持
维护版本	您可以在次要版本中从任何维护版本升级到任何其他维护版本。 例如，您可以从 9.1(1) 升级至 9.1(5)，而无需先安装两者之间的维护版本。
次要版本	您可以从一个次要版本升级至下一个次要版本。您无法跳过某个次要版本。 例如，您可以从 9.0 升级到 9.1。从 9.0 直接升级到 9.2 不支持零停机升级；您必须首先升级到 9.1。 **注**　即使功能配置已迁移，但仍有可能实现零停机升级。
主要版本	您可以从上一个版本的最后一个次要版本，升级至下一个主要版本。 例如，假设 8.6 是您的型号的 8.x 版本系列的最后一个次要版本，则您可以从 8.6 升级至 9.0。从 8.6 直接升级到 9.1 不支持零停机升级；您必须首先升级到 9.0。对于次要版本不支持的型号，您可以跳过次要版本；例如，对于 ASA 5585-X，您可以从 8.4 升级到 9.0（8.5 或 8.6 不支持该型号）。 **注**　即使功能配置已迁移，但仍有可能实现零停机升级。

查看当前版本

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

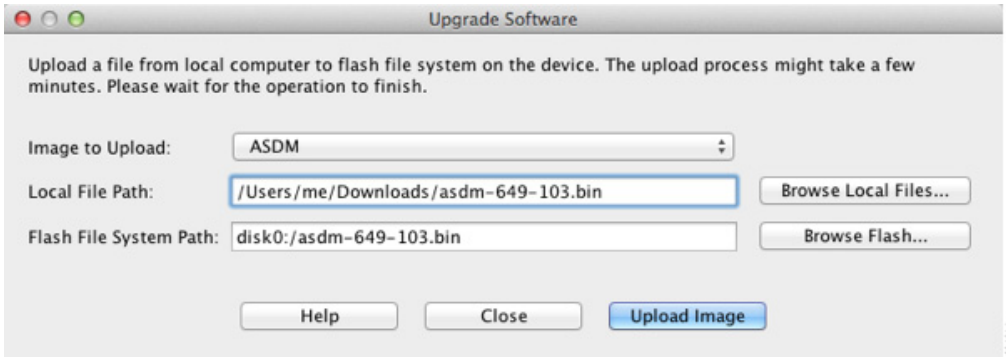
Upgrade Software from Local Computer 工具允许您将映像文件从您的计算机上传至闪存文件系统，以便升级 ASA。

操作步骤

步骤 1　（如果要进行配置迁移）在 ASDM 中，请使用 **Tools > Backup Configurations** 工具备份现有配置。

步骤 2　在 ASDM 主应用程序窗口中，选择 **Tools > Upgrade Software from Local Computer**。

系统将显示 **Upgrade Software** 对话框。



步骤 3　从 **Image to Upload** 下拉列表中选择 **ASDM**。

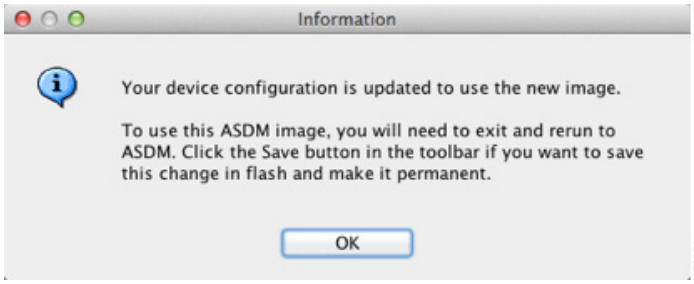
步骤 4　在 **Local File Path** 字段中，输入该文件在您计算机上的本地路径，或者点击 **Browse Local Files** 在您计算机上查找文件。

步骤 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。

步骤 6　点击 **Upload Image**。上传过程可能需要数分钟。

步骤 7　系统会提示您将此映像设置为 ASDM 映像。点击 **Yes**。

步骤 8　系统会提醒您退出 ASDM 并保存配置。点击 **OK**。您会退出升级工具。**注意：**在升级 ASA 软件*之后*，您将保存配置并重新加载 ASDM。



步骤 9　重复步骤 2 到步骤 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。

步骤 10　选择 **Tools > System Reload**，重新加载 ASA。

系统将显示一个新窗口，要求您验证该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 （默认选项）。

b. 选择重新加载的时间 （例如，默认设置 **Now**）。

c. 点击 **Schedule Reload**。

一旦开始重新加载，系统将显示 Reload Status 窗口，该窗口表明正在执行重新加载。系统还提供了退出 ASDM 的选项。

步骤 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　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 9.2(1)，实际下载的可能为 9.2(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

步骤 1　（如果要进行配置迁移）在 ASDM 中，请使用 **Tools > Backup Configurations** 工具备份现有配置。

步骤 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。

步骤 3　输入您的 Cisco.com 用户名和密码，然后点击 **Login**。

系统将显示 **Cisco.com Upgrade Wizard**。

注　如果无可用升级，系统将显示对话框。点击 **OK** 退出向导。

步骤 4　点击 **Next** 显示 **Select Software** 屏幕。

系统将会显示当前的 ASA 版本和 ASDM 版本。

步骤 5　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。

步骤 6　点击 **Next**，显示 **Review Changes** 屏幕。

步骤 7　请验证以下项：

- 已下载正确的 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。

步骤 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，其中提供有详细信息，如升级安装状态 （成功或失败）。

步骤 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。

步骤 10　点击 **Finish**，退出向导，保存对配置的更改。

注　要升级到下一个较高版本 （如可用），您必须重新启动向导。

升级故障转移对或 ASA 集群

升级主用 / 备用故障转移对

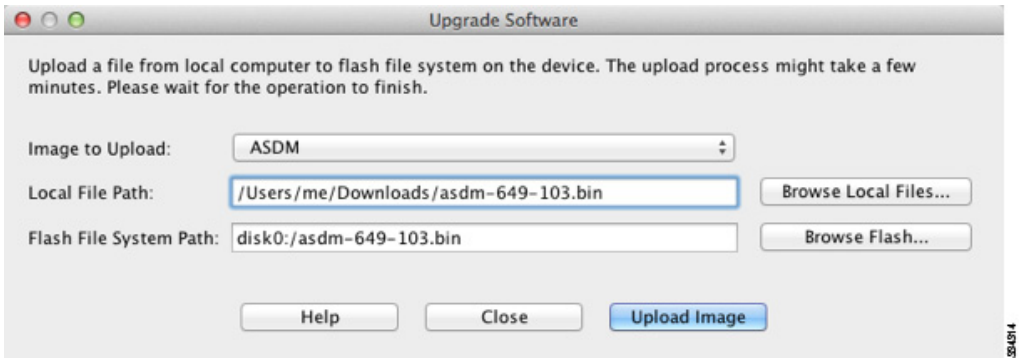
要升级主用 / 备用故障转移对，请执行以下步骤。

操作步骤

步骤 1　（如果要进行配置迁移）在 ASDM 中，请使用 **Tools > Backup Configurations** 工具备份现有配置。

步骤 2　在主用设备上的 ASDM 主应用程序窗口中，选择 **Tools > Upgrade Software from Local Computer**。

系统将显示 Upgrade Software 对话框。



步骤 3　从 Image to Upload 下拉列表中选择 **ASDM**。

步骤 4　在 Local File Path 字段中，输入该文件在您计算机上的本地路径，或者点击 **Browse Local Files** 在您计算机上查找文件。

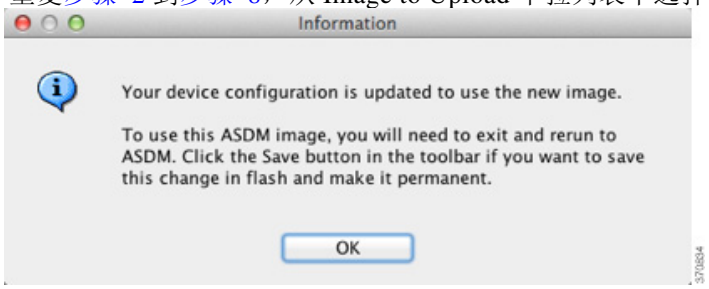
步骤 5　在 Flash File System Path 字段中，输入闪存文件系统的路径，或者点击 **Browse Flash** 在闪存文件系统中查找目录或文件。

步骤 6　点击 **Upload Image**。上传过程可能需要数分钟。

步骤 7　系统会提示您将此映像设置为 ASDM 映像。点击 **Yes**。

步骤 8　系统会提醒您退出 ASDM 并保存配置。点击 **OK**。您会退出升级工具。**注意：**在升级 ASA 软件*之后*，您将保存配置并重新加载 ASDM。

步骤 9　重复步骤 2 到步骤 8，从 Image to Upload 下拉列表中选择 **ASA**。



步骤 10　点击工具栏上的 **Save** 图标，保存配置更改。

步骤 11　将 ASDM 连接至*备用*设备，并根据步骤 2 到步骤 9，使用在主用设备上使用的相同位置，上传 ASA 和 ASDM 软件。

步骤 12　选择 **Tools > System Reload**，以便重新加载备用 ASA。

系统将显示一个新窗口，要求您验证该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 （默认选项）。

b. 选择重新加载的时间 （例如，默认设置 **Now**）。

c. 点击 **Schedule Reload**。

一旦开始重新加载，系统将显示 Reload Status 窗口，该窗口表明正在执行重新加载。系统还提供了退出 ASDM 的选项。

步骤 13　在备用 ASA 重新加载后，请重新启动 ASDM 并连接至备用设备以确保其运行。

步骤 14　再次将 ASDM 连接至*主用*设备。

步骤 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。

步骤 16　选择 **Tools > System Reload**，以便重新加载 （以前的）主用 ASA。

系统将显示一个新窗口，要求您验证该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 （默认选项）。

b. 选择重新加载的时间 （例如，默认设置 **Now**）。

c. 点击 **Schedule Reload**。

一旦开始重新加载，系统将显示 Reload Status 窗口，该窗口表明正在执行重新加载。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

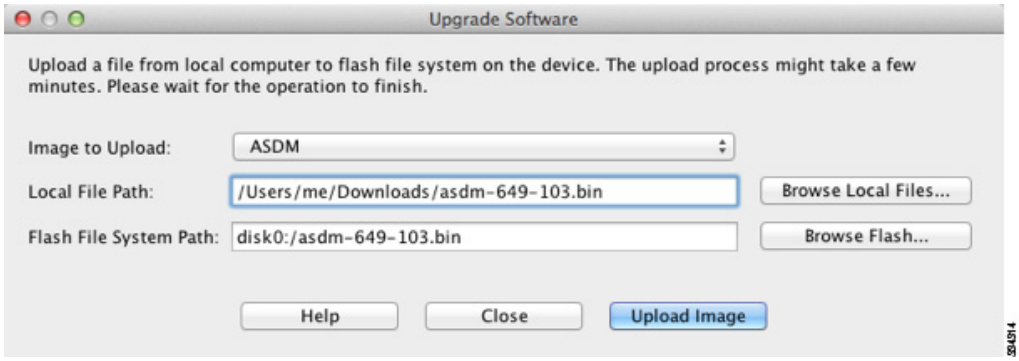
在系统执行空间中执行以下步骤。上执行这些步骤。

操作步骤

步骤 1　（如果要进行配置迁移）在 ASDM 中，请使用 **Tools > Backup Configurations** 工具备份现有配置。

步骤 2　在主设备上的 ASDM 主应用程序窗口中，选择 **Tools > Upgrade Software from Local Computer**。

系统将显示 Upgrade Software 对话框。



步骤 3　从 Image to Upload 下拉列表中选择 **ASDM**。

步骤 4　在 Local File Path 字段中，输入该文件在您计算机上的本地路径，或者点击 **Browse Local Files** 在您计算机上查找文件。

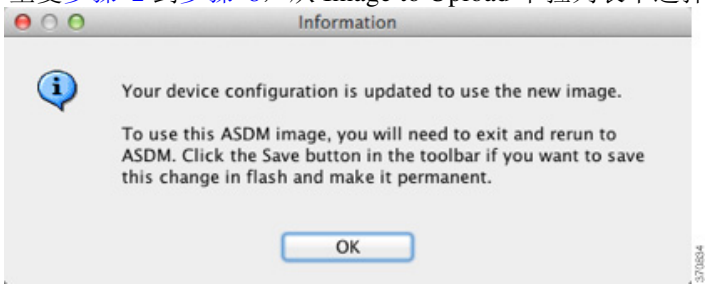
步骤 5　在 Flash File System Path 字段中，输入闪存文件系统的路径，或者点击 **Browse Flash** 在闪存文件系统中查找目录或文件。

步骤 6　点击 **Upload Image**。上传过程可能需要数分钟。

步骤 7　系统会提示您将此映像设置为 ASDM 映像。点击 **Yes**。

步骤 8　系统会提醒您退出 ASDM 并保存配置。点击 **OK**。您会退出升级工具。**注意：**在升级 ASA 软件*之后*，您将保存配置并重新加载 ASDM。

步骤 9　重复步骤 2 到步骤 8，从 Image to Upload 下拉列表中选择 **ASA**。



步骤 10　点击工具栏上的 **Save** 图标，保存配置更改。

步骤 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。

步骤 12　将 ASDM 连接至*辅助*设备，并根据步骤 2 到步骤 9，使用在主用设备上使用的相同位置，上传 ASA 和 ASDM 软件。

步骤 13　选择 **Tools > System Reload**，以便重新加载辅助 ASA。

系统将显示一个新窗口，要求您验证该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 （默认选项）。

b. 选择重新加载的时间 （例如，默认设置 **Now**）。

c. 点击 **Schedule Reload**。

一旦开始重新加载，系统将显示 Reload Status 窗口，该窗口表明正在执行重新加载。系统还提供了退出 ASDM 的选项。

步骤 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。

步骤 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。

步骤 16　选择 **Tools > System Reload**，以便重新加载 （以前的）主用 ASA。

系统将显示一个新窗口，要求您验证该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 （默认选项）。

b. 选择重新加载的时间 （例如，默认设置 **Now**）。

c. 点击 **Schedule Reload**。

一旦开始重新加载，系统将显示 Reload Status 窗口，该窗口表明正在执行重新加载。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

步骤 1　在主设备上启动 ASDM：

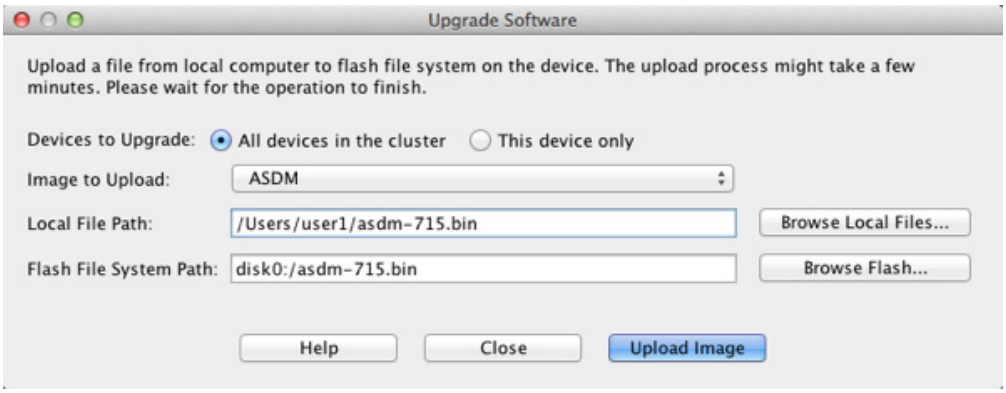
步骤 2　（如果要进行配置迁移）在 ASDM 中，请使用 **Tools > Backup Configurations** 工具备份现有配置。

步骤 3　在 ASDM 主应用程序窗口中，选择 **Tools > Upgrade Software from Local Computer**。

系统将显示 Upgrade Software from Local Computer 对话框。

步骤 4　点击 **All devices in the cluster** 单选按钮。

系统将显示 Upgrade Software 对话框。



步骤 5　从 Image to Upload 下拉列表中选择 **ASDM**。

步骤 6　在 Local File Path 字段中，输入该文件在您计算机上的本地路径，或者点击 **Browse Local Files** 在您计算机上查找文件。

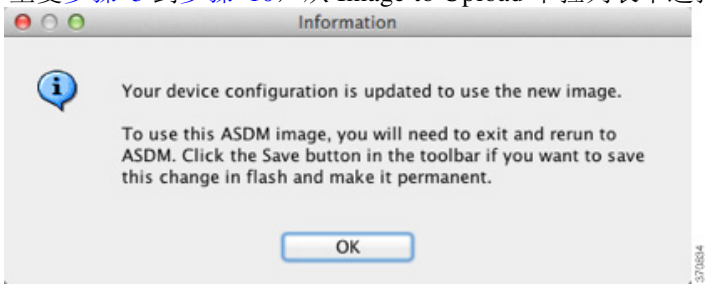
步骤 7　在 Flash File System Path 字段中，输入闪存文件系统的路径，或者点击 **Browse Flash** 在闪存文件系统中查找目录或文件。

步骤 8　点击 **Upload Image**。上传过程可能需要数分钟。

步骤 9　系统会提示您将此映像设置为 ASDM 映像。点击 **Yes**。

步骤 10　系统会提醒您退出 ASDM 并保存配置。点击 **OK**。您会退出升级工具。**注意：**在升级 ASA 软件*之后*，您将保存配置并重新加载 ASDM。

步骤 11　重复步骤 3 到步骤 10，从 Image to Upload 下拉列表中选择 **ASA**。

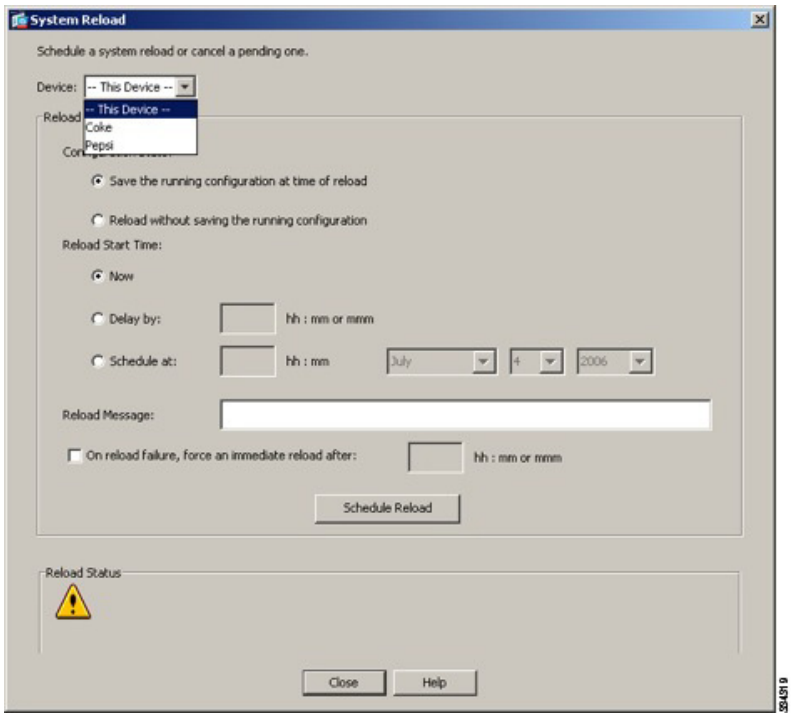


步骤 12　点击工具栏上的 **Save** 图标，保存配置更改。

步骤 13　选择 **Tools > System Reload**。

系统将显示 System Reload 对话框。

步骤 14　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）。



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。

步骤 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。

步骤 16　选择 **Tools > System Reload**，并在 System Reload 对话框中从 Device 下拉列表中选择 **--This Device--**，从而重新加载主设备。

步骤 17　退出并重新启动 ASDM；您将重新连接至新的主设备。

管理文件

ASDM 提供了一套文件管理工具来帮助您执行基本的文件管理任务。文件管理工具可用来查看、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（装入点）上的文件。

注　在多情景模式中，此工具仅适用于系统安全情景。

配置文件访问

配置 FTP 客户端模式

ASA 可使用 FTP，向 FTP 服务器上传映像文件或配置文件，或者从中下载这些文件。在被动 FTP 模式中，客户端发起控制连接和数据连接。服务器是被动模式中的数据连接的接收方，会响应其针对特定连接而侦听的端口号。

详细步骤

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**。

FTP 客户端配置会被将更改，并保存至运行配置。

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。只有被允许使用 SSH 访问 ASA 的客户端，可以建立安全复制连接。

限制

- 该服务器没有目录支持。目录支持的缺乏，会限制远程客户端访问 ASA 的内部文件。
- 该服务器不支持欢迎信息。
- 该服务器不支持通配符。

先决条件

- 根据 第 36-3 页的配置管理访问，在 ASA 上启用 SSH。
- ASA 许可证必须具有强加密 (3DES/AES) 许可证，才能支持 SSH V2 连接。

详细步骤

步骤 1　选择 **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server**，然后选中 **Enable secure copy server** 复选框。

步骤 2　点击 **Apply**。

示例

在外部主机上的客户端中，执行 SCP 文件传输。例如，在 Linux 中输入以下命令：

```
scp -v -pw password source_filename username@asa_address:{disk0|disk1}:/dest_filename
```

-v 表示详细，如果您未指定 **-pw**，会收到输入密码的提示。

自定义 ASA 安全复制客户端

您可以使用板载 SCP 客户端，将文件复制至 ASA，或者从中复制文件 （请参阅第 37-16 页的访问文件管理工具）。此部分允许您自定义 SCP 客户端操作。

先决条件

对于多情景模式，请在系统执行空间中完成本操作步骤。如果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**。

详细步骤

步骤 1　视情景模式而定：

- 对于单模式，请选择 **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP)**。
- 对于系统中的多模式，请选择 **Configuration > Device Management > Device Administration > Secure Copy**。

步骤 2　ASA 会存储其所连接至的每个 SCP 服务器的 SSH 主机密钥。您可以在 ASA 数据库中，视需要手动添加或删除服务器及其密钥。

要添加密钥，请执行以下操作：

a. 对于新服务器，请点击 **Add**，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. 指定以下任一密钥：

- Fingerprint - 输入已经过哈希处理的密钥；例如，您从 **show** 命令输出复制的密钥。
- Key - 输入 SSH 主机的公钥或经过哈希处理的值。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 对其进行哈希处理。

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 3　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。启用此选项时，如果主机密钥尚未存储在 ASA 上，系统会提示您选择接受或拒绝主机密钥。禁用此选项时，如果以前没有存储主机密钥，ASA 会自动接受主机密钥。

步骤 4　点击 **Apply**。

配置 ASA TFTP 客户端路径

TFTP 是一种简单的客户端 / 服务器文件传输协议， RFC 783 和 RFC 1350 修订版对其进行了描述。2. 您可以将 ASA 配置为 TFTP *客户端*，以便其可以将文件复制至 TFTP *服务器*，或者从中复制文件 （请参阅第 37-17 页的传输文件。这样，您可以备份配置文件，并将其传播至多台 ASA。

此部分允许您预定义到 TFTP 服务器的路径，这样您就无需在诸如 **copy** 和 **configure net** 的命令中，输入该路径。

详细步骤

步骤 1　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，输入将在其上保存配置文件的 TFTP 服务器的 IP 地址。

步骤 4　在 Path 字段中，输入将在其上保存配置文件的 TFTP 服务器的路径。

例如：/tftpboot/asa/config3

步骤 5　点击 **Apply**。

添加装入点

添加 CIFS 装入点

要定义通用互联网文件系统 (CIFS) 装入点，请执行以下步骤：

步骤 1　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 文件系统附加至 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 or IP Address 字段中，输入装入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 CIFS 服务器所在的 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入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入文件系统的用户的密码。

步骤 9　在 Confirm Password 字段中，再次输入密码。

步骤 10　点击 **OK**。

系统将会关闭 Add CIFS Mount Point 对话框。

步骤 11　点击 **Apply**。

添加 FTP 装入点

注　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。

步骤 1　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 文件系统附加至 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 or IP Address 字段中，输入装入点所在服务器的名称或 IP 地址。

步骤 5　在 Mode 字段中，点击 FTP 模式的单选按钮 （**Active** 或 **Passive**）。当您选择 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入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入文件系统的用户的密码。

步骤 9　在 Confirm Password 字段中，再次输入密码。

步骤 10　点击 **OK**。

系统将会关闭 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：

步骤 1　在 ASDM 主应用程序窗口中，选择 **Tools > File Management**。

系统将显示 File Management 对话框。

- Folders 窗格会显示磁盘上的可用文件夹。
- Flash Space 会显示闪存总容量，以及可用的内存容量。
- Files 区域会显示选定文件夹中的文件的以下相关信息：
  - 路径
  - 文件名
  - 大小（字节）
  - 修改时间
  - 状态，表明选定文件是被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**，以便在浏览器中显示选定文件。

步骤 3　点击 **Cut**，以便剪切选定文件，从而将其粘贴至另一目录。

步骤 4　点击 **Copy**，以便复制选定文件，从而将其粘贴至另一目录。

步骤 5　点击 **Paste**，以便将复制的文件粘贴至选定目标。

步骤 6　点击 **Delete**，以便将从选定文件从闪存中删除。

步骤 7　点击 **Rename**，以便重命名文件。

步骤 8　点击 **New Directory**，以便创建用于存储文件的新目录。

步骤 9　点击 **File Transfer**，以便打开 File Transfer 对话框。有关详细信息，请参阅第 37-17 页的传输文件。

步骤 10　点击 **Mount Points**，以便打开 Manage Mount Points 对话框。有关详细信息，请参阅第 37-15 页的添加装入点 。

传输文件

文件传输工具允许您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至 ASA，也可以从中传出文件。您可以使用 HTTP、 HTTPS、 TFTP、 FTP 或 SMB，将远程文件传输至 ASA，也可以从中传出文件。

注　对于 IPS SSP 软件模块，在您将 IPS 软件下载至 disk0 之前，请确保至少 50% 的闪存可用。当您安装 IPS 时， IPS 会为其文件系统保留 50% 的内部闪存。

在本地计算机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：

步骤 1　在 ASDM 主应用程序窗口中，选择 **Tools > File Management**。

系统将显示 File Management 对话框。

步骤 2　点击 **File Transfer** 旁的向下箭头，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*您想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，选择您想要上传或下载的文件，然后点击向右箭头或向左箭头，以便将文件传输至所需位置。

步骤 4　在您完成操作后，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：

步骤 1　在 ASDM 主应用程序窗口中，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　要传输来自远程服务器的文件，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　文件传输可以支持 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 类型如下所示：
   - ap - 被动模式中的 ASCII 文件
   - an - 非被动模式中的 ASCII 文件
   - ip - 被动模式中的二进制映像文件
   - in - 非被动模式中的二进制映像文件

步骤 5　要传输来自闪存文件系统的文件，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** 找到文件所在的位置。

步骤 7　此外，您可以通过 CLI 复制来自启动配置、运行配置或 SMB 文件系统的文件。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. 要将文件传输至闪存文件系统，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** 找到文件所在的位置。

步骤 9　要将文件传输至远程服务器，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。有效的类型如下所示：
   - ap - 被动模式中的 ASCII 文件
   - an - 非被动模式中的 ASCII 文件
   - ip - 被动模式中的二进制映像文件
   - in - 非被动模式中的二进制映像文件

步骤 10　点击 **Transfer** 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 （如有必要）。

步骤 12　点击 **OK** 继续文件传输。

文件传输过程可能需要几分钟的时间；请务必等待其完成。

步骤 13　文件传输完成后，请点击 **Close**。

配置要使用的映像和启动配置

如果您有多台 ASA 或多个 ASDM 映像，应指定想要启动的映像。如果您不设置映像，则会使用默认启动映像，并且该映像可能不是想要使用的映像。对于启动配置，您或者可以指定配置文件。

默认设置

ASA Image

- Physical ASA - 启动其在内部闪存中找到的第一个应用映像。
- ASAv - 启动您在首次部署时创建的只读 boot:/ 分区中的映像。您可以升级闪存中的映像，并配置 ASAv，以便从该映像启动。请注意，如果您随后清除您的配置 ，则 ASAv 将还原为加载原始部署映像。

ASDM Image

All ASA - 启动其在内部闪存中 （或者，如果此位置不存在映像，则在外部闪存中）找到的第一个 ASDM 映像。

Startup Configuration

默认情况下， ASA 会从是隐藏文件的启动配置启动。

详细步骤

步骤 1　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 服务器之上，用于设备从其启动的映像。如果您指定位于 TFTP 服务器上的映像，则该映像在列表中必须是第一个映像。如果设备无法访问 TFTP 服务器以便加载映像，则它会尝试加载列表中位于闪存中的下一个映像文件。

步骤 2　在 Boot Image/Configuration 窗格中，点击 **Add**。

步骤 3　浏览至您想要从其启动的映像。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 按钮安排映像顺序。

步骤 5　（可选）在 Boot Configuration File Path 字段中，点击 **Browse Flash** 并选择配置，从而指定启动配置文件。点击 **OK**。

步骤 6　在 ASDM Image File Path 字段中，点击 **Browse Flash** 并选择映像，从而指定 ASDM 映像。点击 **OK**。

步骤 7　点击 **Apply**。

备份和还原 配置或其他文件

Tools 菜单上的 Backup and Restore 选项允许您，备份和还原 ASA 运行配置、启动配置、已安装的附加映像以及 SSL VPN 客户端映像与配置文件。

ASDM 上的 Backup Configurations 屏幕允许您，选择要备份的文件类型，将要备份的文件压缩为单个 zip 文件，然后将该 zip 文件传输至您在计算机上选择的目录。类似地，要还原文件，您可以选择计算机上的源 zip 文件，然后选择要还原的文件类型。

- 第 37-22 页的备份本地 CA 服务器
- 第 37-22 页的备份本地 CA 服务器
- 第 37-23 页的将运行配置保存至 TFTP 服务器

执行全面系统备份或还原

以下操作步骤说明，如何将配置和映像备份至 zip 文件，通过该文件还原配置和映像，以及如何将该文件传输至您的本地计算机。

- 第 37-20 页的准备工作
- 第 37-21 页的备份系统
- 第 37-22 页的还原备份

准备工作

- ASA 必须处于单情景模式中。
- 如果您在备份过程中，或者在备份完成后，进行了任何配置更改，这些更改不会包含在备份中。如果您在备份完成后更改了配置，并然后执行还原，则此配置将会被覆盖。因此， ASA 的行为可能会不同。
- 您一次仅可启动一个备份或还原。
- 您仅能将配置还原至与执行原始备份时相同的 ASA 版本。您不能使用还原工具来将配置从一个 ASA 版本，迁移至另一版本。如果需要进行配置迁移， ASA 在其加载新的 ASA 操作系统时，会自动升级驻留的启动配置。
- 如果您使用集群，您仅可以在主设备上备份或还原启动配置、运行配置和身份证书。
- 如果您使用故障转移，您必须为主用和备用设备单独创建和还原备份。
- 如果您为 ASA 设置主密码，则您需要该密码才能还原使用此操作步骤创建的备份配置。如果您不知道 ASA 的主密码，请参阅第 14-8 页的配置主密码，以便了解如何在继续备份之前，重置该密码。
- 如果您导入 PKCS12 数据（使用 **crypto ca trustpoint** 命令），且信任点使用 RSA 密钥，系统将为导入的密钥对分配与信任点相同的名称。由于这一限制，如果您在还原 ASDM 配置后，为信任点及其密钥对指定不同的名称，启动配置将与原始配置相同，但运行配置将包含不同的密钥对名称。这意味着，如果您将不同的名称用于密钥对和信任点，将无法还原原始配置。为了解决此问题，请确保将相同的名称用于信任点及其密钥对。
- 每个备份文件包括以下内容：
  - 运行配置
  - 启动配置
  - 所有安全映像

    思科安全桌面和端口扫描映像

    思科安全桌面和端口扫描设置

    AnyConnect (SVC) 客户端映像和配置文件

    AnyConnect (SVC) 自定义和转换
  - 身份证书 （包括绑定至身份证书的 RSA 密钥；不包括独立密钥）
  - 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
  - 连接配置文件的预先填充脚本
  - 代理自动配置
  - 转换表
  - 网络内容
  - 版本信息

备份系统

此操作步骤说明，如何执行全面系统备份。

操作步骤

步骤 1　在您的计算机上创建用于存储备份文件的文件夹，这样，以后需要还原这些文件时，您可以很轻松地找到它们。

步骤 2　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，以便查看 SSL VPN 配置的备份选项。默认情况下，所有配置文件都会被选中和备份 （如可用）。如果您要备份列表中的所有文件，请转至步骤 5。

步骤 3　如果您想选择要备份的配置，请取消选中 **Backup All** 复选框。

步骤 4　选中要备份的选项旁的复选框。

步骤 5　点击 **Browse Local，以便指定备份 .zip 文件的目录和文件名。**

步骤 6　在 Select 对话框中，选择您想要在其中存储备份文件的目录。

步骤 7　点击 **Select**。该路径将会显示在 Backup File 字段中。

步骤 8　在目录路径之后，输入目标备份文件的名称。备份文件名的长度必须介于 3 至 232 个字符。

步骤 9　点击 **Backup**。除非您要备份证书或者 ASA 在使用主密码，否则将立即进行备份。

步骤 10　如果您在 ASA 上配置并启用了主密码，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，建议您更改主密码。如果您知道主密码，请点击 **Yes**，以便继续进行备份。除非您要备份身份证书，否则将立即进行备份。

步骤 11　如果您要备份身份证书，系统会要求您输入一个单独的密码，该密码将用于对采用 PKCS12 格式的证书进行编码。您可以输入密码，或者跳过此步骤。

注　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，请参阅第 37-22 页的备份本地 CA 服务器。

- 要加密证书，请在 Certificate Passphrase 对话框中输入并确认您的证书密码，然后点击 **OK**。还原证书时，您将需要记得您在此对话框中输入的密码。
- 点击 **Cancel** 跳过此步骤，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，以便提供成功或失败消息。

注　备份 “ 失败消息 ” 最有可能是缺少指定类型的现有配置而导致的。

步骤 13　点击 **OK** 关闭 Backup Statistics 对话框。

还原备份

您可以指定通过您本地计算机上的 zip 文件还原配置和映像。

操作步骤

步骤 1　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还原的配置的 zip 文件，然后点击 **Select**。路径和 zip 文件名会显示在 **Local File** 字段中。

必须通过选择 **Tools > Backup Configurations** 选项，创建要还原的 zip 文件。

步骤 3　点击 **Next**。系统将会显示第二个 Restore Configuration 对话框。选中您想要还原的配置旁的复选框。所有可用的 SSL VPN 配置都会被默认选中。

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密码， ASDM 会提示您输入密码。

步骤 6　如果您选择还原运行配置，系统会询问您是想要合并运行配置，替换运行配置，还是想要跳过还原过程的这一部分。

- 合并配置会整合当前运行配置和备份的运行配置。
- 替换运行配置仅使用备份的运行配置。
- 跳过此步骤将不会还原备份的运行配置。

ASDM 会显示状态对话框，直到还原操作完成。

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。如果您没有还原运行配置，请刷新 ASDM 会话以使更改生效。

备份本地 CA 服务器

当您执行 ASDM 备份时，备份不会包括本地 CA 服务器数据库，因此您不会备份存储在该服务器上的 CA 证书。如果您要备份本地 CA 服务器，请使用采用 ASA CLI 的以下手动过程：

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，以便创建 LOCAL-CA-SERVER 信任点和还原密钥对。

```
crypto ca import LOCAL-CA-SERVER pkcs12 <passphrase> (paste the pkcs12
base64 data here)
```

注　对于此步骤，请务必使用确切名称 “LOCAL-CA-SERVER”。

步骤 3　如果 LOCAL-CA-SERVER 目录不存在，您需要通过输入 **mkdir LOCAL-CA-SERVER** 来创建该目录。

步骤 4　将本地 CA 文件复制至 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，以便启用本地 CA 服务器

```
crypto ca server
 no shutdown
```

步骤 6　输入 **show crypto ca server** 命令，以便检查本地 CA 服务器是否正在正常运行。

步骤 7　保存配置。

将运行配置保存至 TFTP 服务器

此功能可以在 TFTP 服务器上存储当前运行配置文件的副本。

要将运行配置保存至 TFTP 服务器，请执行以下步骤：

步骤 1　在 ASDM 主应用程序窗口中，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　要配置默认 TFTP 设置，请选择 **Configuration > Device Management > Management Access > File Access > TFTP Client**。在您配置此设置后，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

System Reload 工具允许您计划系统重新启动，或者取消挂起的重新启动。

要计划系统重新启动，请执行以下步骤：

步骤 1　在 ASDM 主应用程序窗口中，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，在以下选项中进行选择：

- 点击 **Now** 立即执行重新启动。
- 点击 **Delay by**，以便将重新启动延迟指定的时长。以小时数和分钟数或仅有分钟数的形式，输入开始重新启动之前的时间。
- 点击 **Schedule at**，以便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，请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，以便以小时数和分钟数或仅有分钟数的形式，显示多长时间之后再次尝试重新启动。

e. 点击 **Schedule Reload**，以便按配置计划重新启动。

Reload Status 区域会显示重新启动的状态。

步骤 3　选择以下任一选项：

- 点击 **Cancel Reload** 停止计划的重新启动。
- 点击 **Refresh**，以便在计划的重新启动完成后，刷新 Reload Status 显示。
- 点击 **Details**，以便显示计划的重新启动的结果。

将您的软件降级

当您升级至 8.3 版本时，您的配置会被迁移。旧的配置会自动存储在闪存中。例如，当您从 8.2(1) 版本升级至 8.3(1) 版本时，旧的 8.2(1) 配置会被将存储在闪存中名为 8_2_1_0_startup_cfg.sav 的文件中。

注　在降级前，您必须手动还原旧的配置。

本部分介绍如何执行降级。

- 第 37-25 页的激活密钥兼容性的相关信息
- 第 37-25 页的执行降级

激活密钥兼容性的相关信息

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

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

执行降级

有关配置迁移的详细信息，请参阅第 37-19 页的 Tools 菜单上的 Backup and Restore 选项允许您，备份和还原 ASA 运行配置、启动配置、已安装的附加映像以及 SSL VPN 客户端映像与配置文件。

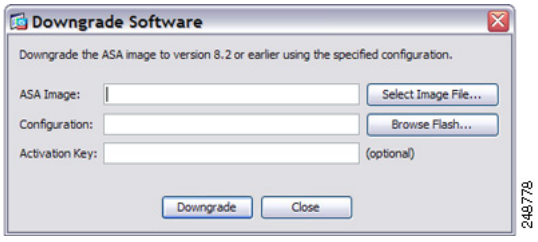
要从 8.3 版本降级，请执行以下步骤：

详细步骤

步骤 1　选择 **Tools > Downgrade Software**。

系统将显示 Downgrade Software 对话框。

图 37-1　　降级软件



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　点击以下任一单选按钮：

- **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**，以便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** 选择预迁移配置文件。（默认情况下，此配置文件会保存在 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 之前的激活密钥）。

有关详细信息，请参阅第 37-25 页的激活密钥兼容性的相关信息。

步骤 6　点击 **Downgrade**。

此工具是完成以下功能的快捷方式：

1. 清除启动映像配置 (**clear configure boot**)。
2. 将启动映像设置为旧映像 (**boot system**)。
3. （可选）输入新的激活密钥 (**activation-key**)。
4. 将运行配置保存至启动 (**write memory**)。这会将 BOOT 环境变量设置为旧映像，因此，当您重新加载时，将会加载旧映像。
5. 将旧配置复制至启动配置 (**copy** *old_config_url* **startup-config**)。
6. 重新加载 (**reload**)。

配置自动更新

有关自动更新的信息

自动更新是一种协议规范，它允许自动更新服务器将配置和软件映像下载至许多 ASA，并可提供从中央位置对 ASA 的基本监控。

自动更新客户端或服务器

ASA 可以被配置为客户端或服务器。作为自动更新客户端，它会定期轮询自动更新服务器，以便获取软件映像和配置文件的更新。作为自动更新服务器，它会向配置为自动更新客户端的 ASA 发送更新。

自动更新的优势

在解决管理 ASA 的管理员所面临的许多问题方面，自动更新十分有用，例如：

- 解决动态寻址和 NAT 挑战。
- 执行一次操作即可提交配置更改。
- 提供更新软件的可靠方法。

- 利用易于理解的方法来实现高可用性 （故障转移）。
- 通过开放接口提供灵活性。
- 简化了用于服务提供商环境的安全解决方案。

自动更新规范提供了远程管理应用所需的基础设施，以便下载 ASA 配置、软件映像和从一个中心位置或多个位置执行基本监控。

自动更新规范允许自动更新服务器向 ASA 推送配置信息或向其发送信息请求，或者通过让 ASA 定期轮询自动更新服务器来拉取配置信息。自动更新服务器也可以向 ASA 发送命令，以便随时发出即时的轮询请求。自动更新服务器与 ASA 之间的通信需要每个 ASA 上的通信路径和本地 CLI 配置。

故障转移配置中的自动更新服务器支持

您可以使用自动更新服务器，将软件映像和配置文件部署至主用 / 备用故障转移配置下的 ASA。要在主用 / 备用故障转移配置上启用自动更新，请在故障转移对中的主设备上输入自动更新服务器配置。

以下限制和行为适用于故障转移配置下的自动更新服务器支持：

- 仅支持单模式、主用 / 备用配置。
- 加载新的平台软件映像时，故障转移对会停止传输流量。
- 使用基于局域网的故障转移时，新的配置不得更改故障转移链路配置。如果新的配置更改了故障转移链路配置，设备之间的通信将会失败。
- 仅主设备将会自动通报自动更新服务器。主设备必须处于主用状态才能进行自动通报。如果主设备不处于主用状态， ASA 会自动故障转移至主设备。
- 仅主设备会下载软件映像或配置文件。软件映像或配置随后会被复制至辅助设备。
- 接口 MAC 地址和硬件串行 ID 均来自主设备。
- 存储在自动更新服务器或 HTTP 服务器上的配置文件仅用于主设备。

自动更新过程概述

以下是故障转移配置下的自动更新过程的概述。此过程假设故障转移已启用且正常运行。如果设备正在同步配置，备用设备由于 SSM 卡故障以外的原因处于故障状态，或者故障转移链路发生故障，则无法进行自动更新。

1. 两台设备会交换平台和 ASDM 软件校验和以及版本信息。
2. 主设备会联系自动更新服务器。如果主设备不处于主用状态， ASA 会先故障转移至主设备，然后与自动更新服务器联系。
3. 自动更新服务器会使用软件校验和与 URL 信息进行回复。
4. 如果主设备确定主用设备或备用设备的平台映像文件需要更新，将会进行以下操作：
   a. 主设备使用来自自动更新服务器的 URL，从 HTTP 服务器检索适当的文件。
   b. 主设备将映像复制至备用设备，然后更新自身的映像。
   c. 如果两台设备都有新映像，则辅助 （备用）设备会先重新加载。
   – 如果在辅助设备启动时可以执行无中断升级，则辅助设备成为主用设备，并且主设备将重新加载。主设备在完成加载后将成为主用单元。
   – 如果在备用设备启动时无法执行无中断升级，则两台设备会同时重新加载。

d. 如果仅辅助 （备用）设备有新映像，则只有辅助设备会重新加载。主设备会进行等待，直到辅助设备完成重新加载。

e. 如果仅主 （主用）设备有新映像，则辅助设备会成为主用设备，并且主设备将重新加载。

f. 更新过程会再次从步骤 1 开始。

5. 如果 ASA 确定主设备或辅助设备的 ASDM 文件需要更新，将会进行以下操作：

a. 主设备使用自动更新服务器提供的 URL，从 HTTP 服务器检索 ASDM 映像文件。

b. 主设备将会视需要，将 ASDM 映像复制至备用设备。

c. 主设备会更新自身的 ASDM 映像。

d. 更新过程会再次从步骤 1 开始。

6. 如果主设备确定需要更新配置，将会进行以下操作：

a. 主设备会从指定 URL 检索配置文件。

b. 新配置会同时替换两台设备上的旧配置。

c. 更新过程会再次从步骤 1 开始。

7. 如果所有映像和配置文件的校验和匹配，则无需更新。更新过程结束，直到下一次轮询时间。

监控自动更新过程

您可以使用 **debug auto-update client** 或 **debug fover cmd-exe** 命令，以便显示在自动更新过程中执行的操作。以下内容是 **debug auto-update client** 命令的示例输出。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”，具体取决于哪一更新失败。 *version* 是更新的版本号。 *reason* 是更新失败的原因。

准则和限制

- 如果 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 **File > Refresh ASDM with the Running Configuration on the Device**，以便获取最新配置，在 ASDM 中所做的所有配置更改都将会丢失。
- 如果 HTTPS 被选为用于与自动更新服务器进行通信的协议， ASA 将会使用 SSL，这要求 ASA 具有 DES 或 3DES 许可证。
- 自动更新仅在单情景模式中受支持。

配置与自动更新服务器的通信

详细步骤

要配置自动更新功能，请选择 **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。

Auto Update Servers 表允许您查看以前配置的自动更新服务器的参数。 ASA 会先轮询在该表顶部列出的服务器。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。

双击 Auto Update Server 表中的任意行可以打开 Edit Auto Update Server 对话框，在该对话框中，您可以修改自动更新服务器参数。这些更改会立即反映在表中，但您必须点击 **Apply**，以便将其保存至配置。

Timeout 区域允许您设置 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，以便允许 ASA 在未接收到自动更新服务器的响应时超时。
- Timeout Period (Minutes) - 输入如果没有收到自动更新服务器的响应，ASA 在超时前将会等待的分钟数。

Polling 区域允许您配置 ASA 将从自动更新服务器轮询信息的频率。 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，在该对话框中，您可以配置轮询自动更新服务器的日期和时间。
- Retry Period (minutes) - 如果轮询服务器的尝试失败，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，以便获取新信息的次数。

添加或编辑自动更新服务器

Add/Edit Auto Update Server 对话框包含以下字段：

- URL - 自动更新服务器用于与 ASA 进行通信的协议（HTTP 或 HTTPS）以及到自动更新服务器的路径。
- Interface - 向自动更新服务器发送请求时使用的接口。
- Do not verify server's SSL certificate - 选中该字段，以便禁用使用 CA 根证书，对自动更新服务器返回的证书进行的验证。自动更新服务器和 ASA 必须使用相同的 CA。

User 区域包含以下字段：

- User Name (Optional) - 输入访问自动更新服务器所需的用户名。
- Password - 输入自动更新服务器的用户密码。
- Confirm Password - 重新输入自动更新服务器的用户密码。
- Use Device ID to uniquely identify the ASA - 启用使用设备 ID 的身份验证。设备 ID 用于向自动更新服务器唯一地标识 ASA。
- Device ID - 要使用的设备 ID 的类型。
  - Hostname - 主机的名称。
  - Serial Number - 设备序列号。
  - IP Address on interface - 选定接口的 IP 地址，该地址将用于向自动更新服务器唯一地标识 ASA。
  - MAC Address on interface - 选定接口的 MAC 地址，该地址将用于向自动更新服务器唯一地标识 ASA。
  - User-defined value - 唯一的用户 ID。

设置轮询计划

Set Polling Schedule 对话框允许您配置， 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。

Daily Update 窗格组允许您配置，您想要 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，以便允许 ASA 随机地选择轮询自动更新服务器的时间。

软件和配置的功能历史记录

表 37-2 列出了各种功能变更以及实施该等功能变更的平台版本。 ASDM 可向后兼容多个平台版本，因此，未列出已添加支持的具体 ASDM 版本。

表 37-2　　软件和配置的功能历史记录

功能名称	平台版本	功能信息
安全复制客户端	9.1(5)/9.2(1)	ASA 现在支持安全复制 (SCP) 客户端，以便将文件传输至 SCP 服务器，或从中传出文件。 我们修改了以下屏幕： Tools > File Management > File Transfer > Between Remote Server and Flash **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server**
默认启用的自动更新服务器证书验证	9.2(1)	现在，自动更新服务器证书验证会默认启用；对于新的配置，您必须显式禁用证书验证。如果您从早期版本升级，而且您没有启用证书验证，则证书验证不会被启用，并且，您会看到以下警告： `WARNING: The certificate provided by the auto-update servers will not be verified.In order to verify this certificate please use the verify-certificate option.` 配置将会被迁移为显式配置的无验证。 我们修改了以下屏幕：Configuration > Device Management > System/Image Configuration > Auto Update > Add Auto Update Server。

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。可以配置多个事件管理器小程序来响应不同的事件和执行不同的操作。

受支持的事件

EEM 支持以下事件：

- 系统日志 - ASA 使用系统日志消息 ID 来识别触发事件管理器小程序的系统日志消息。您可以配置多个系统日志事件，但系统日志消息 ID 可能不会在一个事件管理器小程序内重叠。
- 计时器 - 可以使用计时器触发事件。对于每个事件管理器小程序，每个计时器只能配置一次。每个事件管理器小程序最多可以有三个计时器。计时器的三种类型如下：
  - 看门狗 （定期）计时器在小程序操作完成后的指定时间段后触发事件管理器小程序，并会自动重新启动。
  - 倒数 （一次性）计时器在指定时间段后立即触发事件管理器小程序，且通常不会重新启动，除非移除并重新添加它们。
  - 绝对 （一天一次）计时器促使事件在每天的指定时间发生一次，并会自动重新启动。时间格式为 hh:mm:ss。

  对于上述类型的每个事件管理器小程序，只能配置一个计时器事件。
- 无 - 当您使用 CLI 或 ASDM 手动运行事件管理器小程序时，会触发 None 事件。
- 崩溃 - 如果 ASA 崩溃，会触发崩溃事件。无论 **output** 命令的值是什么，**action** 命令都会指向 crashinfo 文件。输出在 **show tech** 命令之前生成。

事件管理器小程序上的操作

当事件管理器小程序被触发时，会执行事件管理器小程序上的操作。每个操作都具有用于指定操作序列的编号。该序列号在事件管理器小程序中必须是唯一的。可以为一个事件管理器小程序配置多个操作。命令是典型的 CLI 命令，例如 **show blocks**。

输出目标

可以使用 **output** 命令将操作输出发送到指定的位置。一次只能启用一个输出值。默认值为 **output none**。此值丢弃 **action** 命令的任何输出。此命令在全局配置模式中作为权限级别为 15（最高）的用户运行。此命令可能不接受任何输入，因为它处于禁用状态。您可以将 **action** CLI 命令的输出发送到以下三个位置之一：

- **None** - 这是默认位置，会丢弃输出
- **Console** - 此位置将输出发送到 ASA 控制台
- **File** - 此位置将输出发送到文件。以下四个文件选项可用：
  - **Create a unique file** - 每次调用事件管理器小程序时，此选项会创建具有唯一名称的新文件
  - **Create/overwrite a file** - 每次调用事件管理器小程序时，此选项会覆盖指定的文件。
  - **Create/append to a file** - 每次调用事件管理器小程序时，此选项会附加到指定的文件。如果指定的文件不存在，则会创建文件。
  - **Create a set of files** - 此选项会创建一组具有唯一名称的文件，每次调用事件管理器小程序时，都会轮换这些文件。

EEM 准则

情景模式准则

多情景模式不支持 EEM。

附加准则

- 在发生崩溃期间， ASA 的状态一般是未知的。在这种情况下运行某些命令可能不安全。
- 事件管理器小程序的名称不能包含空格。
- 不能修改 None 事件和 Crashinfo 事件参数。
- 因为系统日志消息会发送到 EEM 中进行处理，因此可能会影响性能。
- 每个事件管理器小程序的默认输出均为 **output none**。要更改此设置，必须输入其他输出值。
- 只能为每个事件管理器小程序定义一个输出选项。

配置 EEM

EEM 的配置由以下任务组成：

步骤 1　创建事件管理器小程序，然后配置各种事件。请参阅第 38-3 页的创建事件管理器小程序并配置事件。

步骤 2　在事件管理器小程序上配置操作，然后配置操作输出的目标。请参阅第 38-4 页的配置操作和操作输出的目标。

步骤 3　运行事件管理器小程序。请参阅第 38-5 页的运行事件管理器小程序。

创建事件管理器小程序并配置事件

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，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）并对其进行描述。描述最多可包含 256 个字符。如果用引号将描述文本引起来，描述文本可包含空格。

步骤 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。 0 表示未定义时间段。
- **Periodic**：输入以秒为单位的时间段。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**：输入以秒为单位的时间段。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）并对其进行描述。描述最多可包含 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。有效的序列号范围是 0 到 4294967295。

步骤 5　在 **CLI Command** 字段中输入 CLI 命令。此命令在全局配置模式中作为权限级别为 15 （最高）的用户运行。此命令可能不接受任何输入，因为它处于禁用状态。

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，这样将会丢弃 **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，这样会将 **action** 命令的输出发送到控制台。

注　运行此命令会影响性能。

- 从 **Output Location** 下拉列表中选择 **File** 选项，这样会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，这样将会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，这样会将 **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，这样会将 **action** 命令输出写入到一个文件中，每次写入时都会附加到原有文件。

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**。

EEM 示例

以下示例显示这样的事件管理器小程序：每小时记录一次有关阻止泄露情况信息，并将输出写入到一组会轮换的日志文件中，从而保存一天的日志：

```
ciscoasa(config)# event manager applet blockcheck
ciscoasa(config-applet)# description "Log block usage"
ciscoasa(config-applet)# event timer watchdog time 3600
ciscoasa(config-applet)# output rotate 24
ciscoasa(config-applet)# action 1 cli command "show blocks old"
```

以下示例显示这样的事件管理器小程序：在每天凌晨 1 点重新启动 ASA，并根据需要保存配置：

```
ciscoasa(config)# event manager applet dailyreboot
ciscoasa(config-applet)# description "Reboot every night"
ciscoasa(config-applet)# event timer absolute time 1:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "reload save-config noconfirm"
```

以下示例显示在午夜与凌晨 3 点之间禁用给定接口的事件管理器小程序。

```
ciscoasa(config)# event manager applet disableintf
ciscoasa(config-applet)# description "Disable the interface at midnight"
ciscoasa(config-applet)# event timer absolute time 0:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"

ciscoasa(config)# event manager applet enableintf
ciscoasa(config-applet)# description "Enable the interface at 3am"
ciscoasa(config-applet)# event timer absolute time 3:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "no shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"
```

监控 EEM

可使用以下屏幕监控 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 的历史记录

表 38-1　　EEM 的历史记录

功能名称	平台版本	说明
嵌入式事件管理器 (EEM)	9.2(1)	EEM 服务使您可以调试问题并提供用于故障排除的通用日志记录。这项服务由两个部分组成：EEM 响应或侦听的事件，以及定义操作和 EEM 所响应事件的事件管理器小程序。可以配置多个事件管理器小程序来响应不同的事件和执行不同的操作。 引入了以下屏幕：Configuration > Device Management > Advanced > Embedded Event Manager, Monitoring > Properties > EEM Applets。

第 39 章

故障排除

本章介绍了如何对思科 ASA 进行故障排除。

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。该向导在每个入口和传出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。

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 选择 **Wizards > Packet Capture Wizard**。

系统将显示 **Overview of Packet Capture** 屏幕，其中列出了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** 区域执行以下任一操作：

- 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，请参阅第 39-3 页的入口流量选择器。

步骤 7　点击 **Next** 以显示 **Egress Traffic Selector** 屏幕。要继续，请参阅第 39-4 页的出口流量选择器。

注　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，请参阅第 39-4 页的缓冲区。

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。有效大小的范围为 1534-33554432 个字节。
c. 选中 **Use circular buffer** 复选框以存储捕获的数据包。

注　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，请参阅第 39-4 页的摘要。

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，请参阅第 39-4 页的运行捕获。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** 以移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摘要，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** 以移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，请参阅第 39-5 页的保存捕获。

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记编号以为 Cisco TrustSec 服务启用数据包捕获。有效的安全组标记编号范围为 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。

摘要

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 使用率 ” 和 “%CPU 利用率 ” 表示不同的东西：

- CPU 利用率提供了物理 CPU 的统计信息。
- CPU 使用率提供了基于 CPU 超线程的逻辑 CPU 统计信息。但是，由于只使用一个 vCPU，因此超线程未打开。

vCenter 按如下方式计算 CPU 使用率 (%)：

当前使用的虚拟 CPU 的用量，以总可用 CPU 的百分比表示

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式如下：

以 MHz 为单位的使用率 / 虚拟 CPU 数量 x 核心频率

当比较以 MHz 为单位的使用率时， vCenter 和 ASAv 值是一致的。根据 vCenter 图表， MHz % CPU 使用率计算方式如下：

60/(2499 x 1 vCPU) = 2.4

第 9 部分

记录、 SNMP 和 Smart Call Home

日志记录

本章描述如何记录系统消息并将其用于故障排除。

关于日志记录

系统日志记录是将来自设备的消息收集到运行系统日志守护程序的服务器的方法。记录到中央系统日志服务器有助于汇聚日志和警报。思科设备可以将其日志消息发送到 UNIX 样式系统日志服务。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件将其打印。此形式的日志记录为日志提供受保护的长期存储。日志在例程故障排除和事件处理方面均有帮助。

思科 ASA 系统日志提供有关对 ASA 进行监控和故障排除的信息。通过日志记录功能，可以执行以下操作：

- 指定应记录哪些系统日志消息。
- 禁用或更改系统日志消息的严重性级别。
- 指定一个或多个应发送系统日志消息的位置，包括内部缓冲区、一个或多个系统日志服务器、 ASDM、 SNMP 管理站、指定的邮件地址或 Telnet 和 SSH 会话。
- 以组形式 （例如，按严重性级别或消息类）配置和管理系统日志消息。
- 指定是否对系统日志生成应用速率限制。
- 指出在内部日志缓冲区已满时如何处理其内容，将缓冲区内容发送到 FTP 服务器，或者将内容保存到内部闪存。
- 按位置、严重性级别、类或自定义消息列表过滤系统日志消息。

多情景模式中的日志记录

每个安全情景包含其自己的日志记录配置并生成其自己的消息。如果登录到系统或管理情景，然后更改为其他情景，则在会话中查看的消息只是与当前情景相关的消息。

在系统执行空间中生成的系统日志消息（包括故障转移消息）连同在管理情景中生成的消息在管理情景中进行查看。无法在系统执行空间中配置日志记录或查看任何日志记录信息。

可以配置 ASA 和 ASASM 来将情景名称随附于各消息，从而帮助区分发送到单个系统日志服务器的情景消息。此功能还帮助确定哪些消息来自管理情景，哪些消息来自系统；源于系统执行空间的消息使用设备 ID **system**，源于管理情景的消息使用管理情景的名称作为设备 ID。

系统日志消息分析

以下是可以从各种系统日志消息审阅中获取的信息类型的一些示例：

- ASA 和 ASASM 安全策略允许的连接。这些消息帮助确定安全策略中仍然存在的漏洞。
- ASA 和 ASASM 安全策略拒绝的连接。这些消息显示将哪些类型的活动定向到受保护内部网络。
- 使用 ACE 拒绝速率日志记录功能将显示在 ASA 或 ASA 服务模块 上发生的攻击。
- IDS 活动消息可以显示已发生的攻击。
- 用户身份验证和命令使用情况提供安全策略更改的审计线索。
- 带宽使用情况消息显示已构建和中断的各连接以及使用的持续时间和流量。
- 协议使用情况消息显示用于各连接的协议和端口号。
- 地址转换审计线索消息记录构建或中断的 NAT 或 PAT 连接，在接收到从网络内部到外部环境的恶意活动报告的情况下，这些消息可有所帮助。

系统日志消息格式

系统日志消息以百分比符号 (%) 开头并构造如下：

```
%ASA Level Message_number: Message_text
```

字段描述如下：

ASA	由 ASA 和 ASASM 生成的消息的系统日志消息设备代码。该值始终为 ASA。
Level	1 至 7。级别反映系统日志消息描述的情况的严重性 - 数字越低，情况越严重。
Message_number	用于标识系统日志消息的六位数编号。
Message_text	用于描述情况的文本字符串。系统日志消息的此部分有时包含 IP 地址、端口号或用户名。

严重性级别

表 40-1 列出系统日志消息严重性级别。可以将自定义颜色分配给各严重性级别，从而更轻松地在 ASDM 日志查看器中对其进行区分。要配置系统日志消息颜色设置，请选择 **Tools > Preferences > Syslog** 选项卡，或者在日志查看器本身中，点击工具栏上的 **Color Settings**。

表 40-1　　系统日志消息严重性级别

级别号	严重性级别	说明
0	**emergencies**	系统不可用。
1	**alert**	需要立即采取措施。
2	**critical**	严重情况。
3	**error**	错误情况。
4	**warning**	警告情况。
5	**notification**	正常但重大的情况。
6	**informational**	消息仅供参考。
7	**debugging**	消息仅供调试。

注　ASA 和 ASASM 不会生成严重性级别为零 (emergencies) 的系统日志消息。此级别在 **logging** 命令中提供用于与 UNIX 系统日志功能兼容，但是不由 ASA 使用。

消息类和系统日志 ID 范围

有关系统日志消息类以及与每个类关联的系统日志消息 ID 范围的列表，请参阅系统日志消息指南。

系统日志消息过滤

您可以过滤生成的系统日志消息，以便仅将某些系统日志消息发送到特定输出目标。例如，可以将 ASA 和 ASASM 配置为将所有系统日志消息发送到一个输出目标，并将这些系统日志消息的子集发送到其他输出目标。

具体而言，可以配置 ASA 和 ASASM，以便根据以下条件将系统日志消息定向到输出目标：

- 系统日志消息 ID 号
- 系统日志消息严重性级别
- 系统日志消息类 （相当于 ASA 和 ASASM 的功能区域）

通过创建在设置输出目标时可以指定的消息列表来定制这些条件。或者，可以将 ASA 或 ASASM 配置为独立于消息列表将特定消息类发送到各类型的输出目标。

可以通过两种方法使用系统日志消息类：

- 使用 **logging class** 命令指定整个类别的系统日志消息的输出位置。
- 使用 **logging list** 命令创建指定消息类的消息列表。

系统日志消息类提供按类型将系统日志消息分类的方法，相当于 ASA 和 ASASM 的特性或功能。例如， vpnc 类表示 VPN 客户端。

特定类中的所有系统日志消息都共享其系统日志消息 ID 号中相同的前三位数字。例如，所有以数字 611 开头的系统日志消息 ID 都与 vpnc（VPN 客户端）类相关联。系统日志消息与从 611101 至 611323 的 VPN 客户端功能范围相关联。

此外，大多数 ISAKMP 系统日志消息都具有公用预置对象集来帮助识别隧道。这些对象在适用时前置于系统日志消息的描述性文本。如果在生成了系统日志消息时对象未知，则不显示特定的*标题 = 值*组合。

对象的前缀如下：

Group = *groupname*, Username = *user*, IP = *IP_address*

其中组是隧道组，用户名是来自本地数据库或 AAA 服务器的用户名， IP 地址是远程访问客户端或第 2 层对等体的公用 IP 地址。

将日志查看器中的消息排序

您可以将所有 ASDM 日志查看器 （也就是说， Real-Time Log Viewer、 Log Buffer Viewer 和 Latest ASDM Syslog Events Viewer）中的消息排序。要按多列将表排序，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。要按时间顺序将消息排序，请同时选择日期和时间列；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 和在 Latest ASDM Syslog Events Viewer 中将消息排序时，传入的新消息按照已排序的顺序显示，而非按其通常情况显示在顶部。也就是说，它们与其余消息混合。

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，使用以下任何或所有条件指定系统日志消息组：严重性级别、消息 ID、范围日志消息 ID 范围或消息类。

例如，可以使用消息列表执行以下操作：

- 选择严重性级别为 1 和 2 的系统日志消息，然后将其发送到一个或多个邮件地址。
- 选择与消息类 （例如 ha）关联的所有系统日志消息，然后将其保存到内部缓冲区。

消息列表可以包含多个消息选择条件。但是，必须与新命令条目一起添加各消息选择条件。可以创建包含重叠消息选择条件的消息列表。如果消息列表中的两个条件选择同一消息，则仅记录一次消息。

集群

系统日志消息是用于在集群环境中记帐、监控和故障排除的一种实用工具。集群中的每个 ASA 设备 （最多允许八台设备）独立生成系统日志消息；然后，通过某些 **logging** 命令可以控制报头字段，包括时间戳和设备 ID。系统日志服务器使用设备 ID 标识系统日志生成器。您可以使用 **logging device-id** 命令生成具有相同或不同设备 ID 的系统日志消息，使消息看似来自集群中的相同或不同设备。

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

IPv6 准则

不支持 IPv6。

附加准则

- 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，必须从其他供应商获取 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。
- 在备用 ASA 上不支持通过 TCP 发送系统日志。
- ASA 支持在单情景模式中使用 **logging host** 命令配置 16 个系统日志服务器。在多情景模式中，限制为每个情景 4 个服务器。
- 应该可以通过 ASA 和 ASASM 到达系统日志服务器。应该将 ASASM 配置为拒绝可以从其到达系统日志服务器的接口上的 ICMP 不可达消息，并将系统日志发送到同一服务器。请确保已对所有严重性级别启用日志记录。要防止系统日志服务器崩溃，请抑制生成系统日志 313001、 313004 和 313005。
- 使用自定义消息列表仅与访问列表命中相匹配时，对于已将其日志记录严重性级别提高至调试 （级别 7）的访问列表不会生成访问列表日志。对于 **logging list** 命令，默认日志记录严重性级别设置为 6。此默认行为是故意的。将访问列表配置的日志记录严重性级别显式更改为调试时，还必须更改日志记录配置本身。

  以下是来自 **show running-config logging** 命令的不含访问列表命中的样本输出，因为其日志记录严重性级别已更改为调试：

  ```
  ciscoasa# show running-config logging
  logging enable
  logging timestamp
  logging list test message 106100
  logging buffered test
  ```

  以下是来自 **show running-config logging** 命令的包含访问列表命中的样本输出：

  ```
  ciscoasa# show running-config logging
  logging enable
  logging timestamp
  logging buffered debugging
  ```

  在此情况下，访问列表配置不更改并会显示访问列表命中数，如下例所示：

  ```
  ciscoasa(config)# access-list global line 1 extended permit icmp any host 4.2.2.2 log
  debugging interval 1 (hitcnt=7) 0xf36b5386
  ciscoasa(config)# access-list global line 2 extended permit tcp host 10.1.1.2 any eq
  www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
  ciscoasa(config)# access-list global line 3 extended permit ip any any (hitcnt=543)
  0x25f9e609
  ```

配置日志记录

本节描述如何配置日志记录。

步骤 1　启用日志记录 请参阅第 40-6 页的启用日志记录。

步骤 2　配置系统日志消息的输出目标。请参阅第 40-6 页的配置输出目标。

注　最低配置取决于要执行的操作，以及在 ASA 和 ASASM 中处理系统日志消息的要求。

启用日志记录

要启用日志记录，请执行以下步骤：

操作步骤

步骤 1　在 ASDM 中，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该发送系统日志消息的位置，包括内部日志缓冲区、一个或多个外部系统日志服务器、 ASDM、 SNMP 管理站、控制台端口、指定的邮件地址或 Telnet 和 SSH 会话。

将系统日志消息发送到外部系统日志服务器

可以根据外部系统日志服务器上的可用磁盘空间将消息存档，并在保存日志记录数据后对其进行处理。例如，可以指定在记录特定类型的系统日志消息后要执行的操作，从日志提取数据并将记录保存到其他文件以进行报告，或者使用特定于站点的脚本跟踪统计信息。

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　选择 **Configuration > Device Management > Logging > Logging Setup**。

步骤 2　选中 **Enable logging** 复选框来为 ASA 开启日志记录。

步骤 3　选中 **Enable logging on the failover standby unit** 复选框来为备用 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。当缓冲区充满时，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 至 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** 以标识 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** 复选框以在覆盖缓冲区内容之前将其保存到 内部闪存。

注　此选项仅在路由模式或透明单一模式中可用。

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　此选项仅在单一路由模式或透明模式中可用。

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的日志缓冲区内容的 FTP 服务器上的目录路径。

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　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，因此可能需要更改系统日志的该值。

步骤 3　选中 **Include timestamp in syslogs** 复选框以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** 表应该显示整个系统日志消息 ID 列表。
- 选择 **Show disabled syslog IDs** 以指定 **Syslog ID** 表应该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** 表应该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** 表应该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：

注　**Syslog ID** 字段仅供显示。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　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　要指定使用哪个作为设备 ID，请选择以下选项之一：

- 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。

  如果使用的是集群，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　选择以下选项之一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　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　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，请选择以下选项之一：

- 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　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和复制已记录的条目，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　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　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　选择 **Configuration > Device Management > Logging > E-Mail Setup**。

步骤 2　指定用作作为邮件消息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　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　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　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** 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警报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　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** 保存对运行配置所做的更改。

在 ASDM 中查看系统日志消息

步骤 1　选择 **Home > Latest ASDM Syslog Messages** 来查看已发送到 ASDM 的最新系统日志消息。

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　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
- 邮件
- 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，请参阅第 40-13 页的应用日志记录过滤器。

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，请参阅第 40-15 页的创建自定义事件列表。

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　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　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，请参阅第 40-8 页的编辑系统日志 ID 设置。

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 **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　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　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　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　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　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。任一协议的有效端口值为 1025 至 65535。默认 UDP 端口为 514。默认 TCP 端口为 1470。

注　在备用 ASA 上不支持通过 TCP 发送系统日志。

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　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　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，请执行下列操作：

操作步骤

步骤 1　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** 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　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　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　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　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　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　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** 以保存更改。

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　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　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**。

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　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	严重性级别
Emergency	0 - 系统不可用
Alert	1 - 需要立即采取措施
Critical	2 - 严重情况
Error	3 - 错误情况
Warning	4 - 警告情况
Notification	5 - 正常但重大的情况
Informational	6 - 消息仅供参考
Debugging	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，请参阅第 40-21 页的指定或更改单独系统日志消息的速率限制。

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，请参阅第 40-22 页的添加或编辑系统日志消息的速率限制。

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，请参阅第 40-22 页的编辑系统日志严重性级别的速率限制。

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　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　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**
- **Monitoring > Logging > Real-Time Log Viewer > View**
- **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。单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**。单击 **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**。单击 **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**。单击 **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。单击 **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**。单击 **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。多个条目必须以逗号分隔。

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
源 IP = 192.168.1.1 或 0.0.0.0 源端口 = 67	FILTER: srcIP=192.168.1.1,0.0.0.0;srcPort=67;
严重性 = Informational 目标 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;
源 IP = 1.1.1.1 描述 = 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　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** 以移除当前过滤器设置并输入新设置。否则，更改显示的设置，然后点击 **OK**。

  注　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，可以右键单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** 以移除输出，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。在您完成操作后，点击 Close。

日志记录的历史记录

表 40-2　　日志记录的历史记录

功能名称	平台版本	说明
日志记录	7.0(1)	通过各种输出目标提供 ASA 网络日志记录信息，并且包含用于查看和保存日志文件的选项。 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。
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。

表 40-2　　日志记录的历史记录 （续）

功能名称	平台版本	说明
日志记录类和已保存的日志记录缓冲区	8.2(1)	添加了对日志记录消息的 dap 事件类的支持。 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。 我们未修改任何 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。 我们修改了以下屏幕： 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。
集群	9.0(1)	添加了对于在 ASA 5580 和 5585-X 上的集群环境中生成系统日志消息的支持。 修改了以下屏幕：Configuration > Logging > Syslog Setup > Advanced > Advanced Syslog Configuration。

SNMP

本章描述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，并且支持同时使用全部三个版本。利用在 ASA 接口上运行的 SNMP 代理，可以通过诸如 HP OpenView 之类的网络管理系统 (NMS) 监控 ASA 和 ASASM。ASA、ASAv 和 ASASM 通过发出 GET 请求来支持 SNMP 只读访问。不允许 SNMP 写访问，因此，无法对 SNMP 进行更改。此外，不支持 SNMP SET 请求。

可以将 ASA、 ASAv 和 ASASM 配置为发送陷阱，它们是指向 NMS 的特定事件 （事件通知）的从受管设备到管理站的未经请求的消息，也可以使用 NMS 在 ASA 上浏览管理信息库 (MIB)。MIB 是定义的集合，ASA、ASAv 和 ASASM 维护由每个定义的值组成的数据库。浏览 MIB 意味着从 NMS 发出 MIB 树的一系列 GET-NEXT 或 GET-BULKGET 请求以确定值。

ASA、 ASAv 和 ASASM 具有 SNMP 代理，用于在发生预定义为需要通知 （例如，当网络中的链路开启或关闭时）的事件的情况下通知指定的管理站。它发送的通知包括用于向管理站表明其自身身份 SNMP OID。 ASA、 ASAv 或 ASASM SNMP 代理还会在管理站请求信息时进行应答。

SNMP 术语

表 41-1 列出在使用 SNMP 时常用的术语。

表 41-1 SNMP 术语

术语	说明
代理	在 ASA 上运行的 SNMP 服务器。 SNMP 代理具有以下功能： • 对来自网络管理站的信息和操作请求作出响应。 • 控制对其管理信息库 （即 SNMP 可以查看或更改的对象的集合）的访问。 • 不允许 SET 操作。
浏览	通过从设备上的 SNMP 代理轮询所需信息来从网络管理站监控该设备的运行状况。此活动可能包括从网络管理站发出 MIB 树的一系列 GET-NEXT 或 GET-BULK 请求以确定值。
管理信息库 (MIB)	用于收集有关数据包、连接、缓冲区、故障转移等的信息的标准化数据结构。 MIB 由大多数网络设备使用的产品、协议和硬件标准来定义。 SNMP 网络管理站可以浏览 MIB，并请求在出现特定数据或事件时将其发送。
网络管理站 (NMS)	PC 或工作站设置为监控 SNMP 事件和管理设备，例如 ASA、 ASAv 和 ASASM。
对象标识符 (OID)	用于向设备的 NMS 表明该设备的身份并向用户指示监控和显示的信息源的系统。
陷阱	用于生成从 SNMP 代理到 NMS 的消息的预定义事件。事件包括警报条件，例如链路开启、链路关闭、冷启动、热启动、身份验证或系统日志消息。

SNMP 第 3 版概述

SNMP 第 3 版提供第 1 或 2c 版中没有的安全增强功能。SNMP 第 1 和 2c 版以明文形式在 SNMP 服务器和 SNMP 代理之间传输数据。 SNMP 第 3 版向安全协议操作中添加了身份验证和隐私选项。此外，该版本通过基于用户的安全模型 (USM) 和基于视图的访问控制模型 (VACM) 控制对 SNMP 代理和 MIB 对象的访问。 ASA 和 ASASM 还支持创建 SNMP 组和用户，以及为安全 SNMP 通信启用传输身份验证和加密所需的主机。

安全模型

为进行配置，身份验证和隐私选项会共同组成安全模型。安全模型适用于用户和组，分为以下三种类型：

- NoAuthPriv - 无身份验证且无隐私，意味着未对消息应用安全性。
- AuthNoPriv - 有身份验证但无隐私，意味着消息会进行身份验证。
- AuthPriv - 有身份验证并有隐私，意味着消息会进行身份验证并加密。

SNMP 组

SNMP 组是可以将用户添加到的访问控制策略。每个 SNMP 组配置有安全模型，并与 SNMP 视图关联。SNMP 组内的用户必须与 SNMP 组的安全模型匹配。这些参数指定 SNMP 组内的用户使用的身份验证和隐私类型。每个 SNMP 组名称 / 安全模型对必须唯一。

SNMP 用户

SNMP 用户具有指定的用户名、用户所属的组、身份验证密码、加密密码，以及要使用的身份验证和加密算法。身份验证算法选项为 MD5 和 SHA。加密算法选项为 DES、 3DES 和 AES （在 128、 192 和 256 版中可用）。创建用户时，必须将其与 SNMP 组相关联。然后，用户将继承该组的安全模型。

SNMP 主机

SNMP 主机是 SNMP 通知和陷阱发送到的 IP 地址。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。
- 必须使用正确的安全模型创建用户和组。
- 必须按正确的顺序移除用户、组和主机。
- 使用 **snmp - server host** 命令创建 ASA、 ASAv 或 ASASM 规则以允许传入 SNMP 流量。

SNMP 系统日志消息传递

SNMP 生成编号为 212*nnn* 的详细系统日志消息。系统日志消息向指定接口上的指定主机表明 SNMP 请求、 SNMP 陷阱、 SNMP 信道和来自 ASA 或 ASASM 的 SNMP 响应的状态。

有关系统日志消息的详细信息，请参阅系统日志消息指南。

注　如果 SNMP 系统日志消息超过较高的速率 （约 4000 条 / 秒），则 SNMP 轮询将失败。

应用服务和第三方工具

有关 SNMP 支持的信息，请参阅以下 URL：

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

有关使用第三方工具处理 SNMP 第 3 版 MIB 的信息，请参阅以下 URL：

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP 准则

故障转移准则

每个 ASA、 ASAv 或 ASASM 中的 SNMP 客户端与其对等体共享引擎数据。引擎数据包括 SNMP-FRAMEWORK-MIB 的 engineID、 engineBoots 和 engineTime 对象。引擎数据作为二进制文件写入到 flash:/snmp/*contextname*。

IPv6 准则

不支持 IPv6。

附加准则

- 您必须具有 Cisco Works for Windows 或其他 SNMP MIB-II 兼容浏览器才能接收 SNMP 陷阱或浏览 MIB。
- 不支持基于视图的访问控制，但是 VACM MIB 可供浏览来确定默认视图设置。
- ENTITY-MIB 在非管理情景中不可用。在非管理情景中改用 IF-MIB 执行查询。
- 对于 AIP SSM 或 AIP SSC 不支持 SNMP 第 3 版。
- 不支持 SNMP 调试。
- 不支持 ARP 信息检索。
- 不支持 SNMP SET 命令。
- 使用 NET-SNMP 第 5.4.2.1 版时，仅支持 AES128 加密算法版本。不支持 AES256 或 AES192 加密算法版本。
- 如果结果导致 SNMP 处于不一致状态，则会对现有配置进行更改。
- 对于 SNMP 第 3 版，必须按以下顺序进行配置：组、用户、主机。
- 在删除组之前，必须确保删除与该组关联的所有用户。
- 在删除用户之前，必须确保未配置与该用户名关联的主机。
- 如果已使用特定安全模型将用户配置为属于特定组，并且，如果该组的安全级别进行了更改，则必须按此顺序执行以下操作：
  - 从该组中移除用户。
  - 更改组安全级别。
  - 添加属于新组的用户。
- 不支持创建自定义视图来限制对 MIB 对象子集的用户访问。
- 所有的请求和陷阱只能在默认的 Read/Notify View 中获取。
- 在管理情景中生成 connection-limit-reached 陷阱。要生成此陷阱，必须在已达到连接限制的用户情景中配置至少一个 SNMP 服务器主机。
- 不能在 ASA 5585 SSP-40 (NPE) 上查询机箱温度。
- 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。选择 **Wizards > Packet Capture Wizard**，然后遵循屏幕上的说明执行操作。
- 最多可以添加 4000 台主机。不过，其中仅 128 台可用于陷阱。
- 支持的活动轮询目标总数为 128。
- 可以指定网络对象来表示要添加为主机组的单个主机。

- 可以将多个用户与一台主机关联。
- 可以在不同的 **host-group** 命令中指定重叠网络对象。为最后一个主机组指定的值对于不同网络对象中的公用主机集合生效。
- 如果删除主机组或与其他主机组重叠的主机，则会使用所配置的主机组中已指定的值再次设置主机。
- 主机获取的值取决于用于运行命令的指定序列。
- SNMP 发送的消息大小的限制为 1472 字节。
- 集群成员不同步其 SNMPv3 引擎 ID。因此，集群中的每个设备应具有唯一的 SNMPv3 用户配置。

配置 SNMP

本节描述如何配置 SNMP。

步骤 1　启用 SNMP 代理和 SNMP 服务器。请参阅第 41-5 页的启用 SNMP 代理和 SNMP 服务器。

步骤 2　将 SNMP 管理站配置为接收来自 ASA 的请求。请参阅第 41-5 页的配置 SNMP 管理站。

步骤 3　配置 SNMP 陷阱。请参阅第 41-6 页的配置 SNMP 陷阱。

步骤 4　配置 SNMP 第 1 和 2c 版参数或 SNMP 第 3 版参数。请参阅第 41-7 页的配置 SNMP 第 1 或 2c 版的参数或第 41-7 页的配置 SNMP 第 3 版的参数。

启用 SNMP 代理和 SNMP 服务器

要启用 SNMP 代理和 SNMP 服务器，请执行以下步骤：

操作步骤

步骤 1　选择 **Configuration > Device Management > Management Access > SNMP**。默认情况下，已启用 SNMP 服务器。

步骤 2　要继续，请参阅第 41-5 页的配置 SNMP 管理站。

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　选择 **Configuration > Device Management > Management Access > SNMP**。

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 主机驻留所在的接口。

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 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 或 2c 版的参数

要配置 SNMP 第 1 或 2c 版的参数，请执行以下步骤：

操作步骤

步骤 1　选择 **Configuration > Device Management > Management Access > SNMP**。

步骤 2　如果使用的是 SNMP 第 1 或 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 和受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，但是多个空格会缩短为单个空格。

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，但是多个空格会缩短为单个空格。

步骤 5　进入侦听来自 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，必须输入社区字符串。如果选择第 3 版，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。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。

在 **SNMP Host Access List** 窗格中将显示新主机。

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　选择 **Configuration > Device Management > Management Access > SNMP**。

步骤 2　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。移除组中的最后一个用户时， ASDM 会删除该组。

注　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　不能更改组名。

步骤 4　点击 **USM Model** 选项卡以使用用户安全模型 (USM) 组。

步骤 5　点击 **Add**。

系统将显示 **Add SNMP USM Entry** 对话框。

步骤 6　输入组名。

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　选择 **Configuration > Device Management > Management Access > SNMP**。

步骤 2　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。移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

有关监控 SNMP 的信息，请参阅以下屏幕。

- **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 41-2 SNMP 历史记录

功能名称	平台版本	说明
SNMP 第 1 和 2c 版	7.0(1)	通过明文社区字符串在 SNMP 服务器与 SNMP 代理之间传输数据来提供 ASA、ASAv 和 ASASM 网络监控及事件信息。 我们修改了以下屏幕：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型 SNMP 第 3 版提供 3DES 或 AES 加密和支持。通过使用 USM，此版本允许配置用户、组和主机以及身份验证特性。此外，该版本还允许对代理和 MIB 对象进行访问控制，并且包含其他 MIB 支持。 我们修改了以下屏幕：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。 我们修改了以下屏幕：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 将设置为已为接口描述设置的值。

表 41-2　　SNMP 历史记录 （续）

功能名称	平台版本	说明
ASA 服务模块 (ASASM)	8.5(1)	ASASM 支持 8.4(1) 中存在的所有 MIB 和陷阱，但以下除外： 8.5(1) 中不受支持的 MIB： • CISCO-ENTITY-SENSOR-EXT-MIB （仅支持 entPhySensorTable 组下的对象）。 • ENTITY-SENSOR-MIB （仅支持 entPhySensorTable 组中的对象）。 • DISMAN-EXPRESSION-MIB （仅支持 expExpressionTable、expObjectTable 和 expValueTable 组中的对象）。 8.5(1) 中不受支持的陷阱： • ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)。此陷阱仅用于电源故障、风扇故障和高 CPU 温度事件。 • InterfacesBandwidthUtilization.
SNMP 陷阱	8.6(1)	支持 ASA 5512-X、 5515-X, 5525-X、 5545-X 和 5555-X 的以下其他关键字：**entity power-supply-presence**、 **entity power-supply-failure**、 **entity chassis-temperature**、 **entity chassis-fan-failure**、 **entity power-supply-temperature**。 我们修改了以下命令：**snmp-server enable traps**。
VPN 相关 MIB	9.0(1)	已实施更新版本的 CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB 来支持下一代加密功能。 已为 ASASM 启用下列 MIB： • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	添加了对以下 MIB 的支持：CISCO-TRUSTSEC-SXP-MIB。
SNMP OID	9.1(1)	已添加五个新的 SNMP 物理供应商类型 OID 来支持 ASA 5512-X、 5515-X、5525-X、 5545-X 和 5555-X。
NAT MIB	9.1(2)	添加了 cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 来支持 xlate_count 和 max_xlate_count 条目，相当于允许使用 **show xlate count** 命令进行轮询。
SNMP 主机、主机组和用户列表	9.1(5)	现在最多可以添加 4000 台主机。支持的活动轮询目标数为 128。可以指定网络对象来表示要添加为主机组的单个主机。可以将多个用户与一台主机关联。 我们修改了以下屏幕：Configuration > Device Management > Management Access > SNMP。

表 41-2 SNMP 历史记录 （续）

功能名称	平台版本	说明
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 MIB 和陷阱	9.3(2)	CISCO-PRODUCTS-MIB 和 CISCO-ENTITY-VENDORTYPE-OID-MIB 已更新为支持新的 ASA 5506-X、 ASA 5506W-X 和 ASA 5508-X。 ASA 5506-X 和 ASA 5508-X 已作为新产品添加到 SNMP sysObjectID OID 和 entPhysicalVendorType OID 表中。 现在， ASA 支持 CISCO-CONFIG-MAN-MIB，这使您可以执行以下操作： • 了解已为特定配置输入了哪些命令。 • 在运行配置发生更改后通知 NMS。 • 跟踪与上一次更改或保存运行配置相关的时间戳。 • 跟踪命令的其他更改，例如，终端详细信息和命令源。 我们修改了以下屏幕：Configuration > Device Management > Management Access > SNMP > Configure Traps > SNMP Trap Configuration。

第 42 章

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

您可以通过启用 Anonymous Reporting 服务来帮助改进思科 ASA 平台，此服务使思科能够安全地接收来自设备的最少量错误和运行状况信息。启用此功能后，客户身份将保持匿名，而不会发送任何识别信息。

启用 Anonymous Reporting 将会创建信任点并安装证书。 ASA 需要 CA 证书以验证 Smart Call Home 网络服务器上存在的服务器证书并构造 HTTPS 会话，以使 ASA 能够安全地发送消息。思科将导入软件中预定义的证书。如果您决定启用 Anonymous Reporting，则 ASA 上将会安装一个证书，其硬编码的信任点名称为 _SmartCallHome_ServerCA。当您启用 Anonymous Reporting 时，系统将会创建此信任点，安装相应的证书，并且您将接收到有关此操作的消息。然后，该证书将出现在您的配置中。

如果启用 Anonymous Reporting 时相应的证书已存在于配置中，则不会创建信任点，并且不会安装任何证书。

注 启用 Anonymous Reporting 即表示您同意将指定的数据传输至思科或代表思科运营的供应商 （包括美国以外的国家 / 地区）。
思科将保护所有客户的隐私。有关思科对个人信息的处置的详细信息，请参阅以下 URL 中提供的思科隐私声明：
http://www.cisco.com/web/siteassets/legal/privacy.html

DNS 需求

必须正确配置 DNS 服务器，ASA 才能访问思科 Smart Call Home 服务器并向思科发送消息。由于 ASA 可能位于专用网络中，而未接入公用网络，因此思科将验证 DNS 配置，并在必要时通过执行下列任务来配置 DNS：

1. 为所有已配置的 DNS 服务器执行 DNS 查找。
2. 通过在最高安全级别的接口上发送 DHCPINFORM 消息，从 DHCP 服务器获取 DNS 服务器。
3. 使用思科 DNS 服务器进行查找。
4. 将静态 IP 地址随机用于 tools.cisco.com。

执行这些任务并不会更改当前配置。（例如，从 DHCP 获取的 DNS 服务器不会添加到配置中。）

如果未配置任何 DNS 服务器，并且 ASA 无法访问 Cisco Smart Call Home 服务器，则对于发送的每条 Smart Call Home 消息，思科都将生成一条严重性级别为 “ 警告 ” 的系统日志消息，以提醒您正确配置 DNS。

有关系统日志消息的详细信息，请参阅系统日志消息指南。

关于 Smart Call Home

对 Smart Call Home 服务进行全面配置后，此服务可以检测到站点中的问题，并且通常在您知道这些问题存在之前，向思科报告这些问题或者通过用户定义的其他渠道进行报告 （例如通过邮件报告或者直接向您报告）。根据这些问题的严重性，思科将通过提供下列服务，对您的系统配置问题、产品寿命终止声明以及安全公告问题等等作出回应：

- 通过持续进行监控、发出实时的主动警报以及进行详细诊断，迅速确定问题。
- 通过 Smart Call Home 通知使您知晓潜在的问题，在这些通知中，已提交服务请求，并随附了所有诊断数据。
- 自动直接联系思科 TAC 专家，更迅速地解决紧急问题。
- 缩短故障排除时间，从而更高效地利用员工资源。
- 自动生成发往思科 TAC 的服务请求 （如果您签订了服务合同），这些请求将发送给适当的支持团队，该支持团队将提供可以加快解决问题的详细诊断信息。

您可以通过 Smart Call Home 门户快速访问使您能够执行下列活动的必需信息：

- 在一个位置查看所有 Smart Call Home 消息、诊断信息和建议。
- 检查服务请求状态。
- 查看所有已启用 Smart Call Home 的设备的最新清单和配置信息。

Anonymous Reporting 和 Smart Call Home 指南

Anonymous Reporting

- 必须配置 DNS。
- 如果首次尝试无法发送 Anonymous Reporting 消息，则 ASA 将再重试两次，然后丢弃该消息。
- Anonymous Reporting 可以与其他 Smart Call Home 配置共存，而不会更改现有配置。例如，如果启用 Anonymous Reporting 之前 Smart Call Home 处于禁用状态，那么它将保持处于禁用状态，即使在 Anonymous Reporting 启用后也是如此。
- 如果 Anonymous Reporting 处于启用状态，您将无法删除信任点，并且禁用 Anonymous Reporting 时，信任点仍保留。如果 Anonymous Reporting 处于禁用状态，则您可以删除信任点，但禁用 Anonymous Reporting 不会导致删除信任点。
- 如果您使用的是多情景模式配置，则 **dns**、**interface** 和 **trustpoint** 命令处于管理员情景中，而 **call-home** 命令处于系统情景中。

Smart Call Home

- 在多情景模式中， **subscribe-to-alert-group snapshot periodic** 命令划分成两个命令：一个命令用于从系统配置中获取信息，另一个命令用于从用户情景中获取信息。
- Smart Call Home 后端服务器只能接受 XML 格式的消息。
- 如果已启用集群功能，并且已将 Smart Call Home 配置为订用安全级别为 “ 紧急 ” 的诊断警报组，那么将向思科发送 Smart Call Home 消息以报告重要的集群事件。仅对于下列事件，才会发送 Smart Call Home 集群消息：
  - 当装置加入集群时
  - 当装置离开集群时
  - 当集群装置变成集群主装置时
  - 当集群中的辅助装置发生故障时

  发送的每条消息都包含以下信息：
  - 处于活动状态的集群成员的计数
  - 对集群主装置运行的 **show cluster info** 命令和 **show cluster history** 命令的输出

相关主题

- 第 42-2 页的 DNS 需求
- 第 14-10 页的配置 DNS 服务器

配置 Anonymous Reporting 和 Smart Call Home

虽然 Anonymous Reporting 是 Smart Call Home 服务的组成部分，并且使思科能够以匿名方式接收来自设备的最少量错误和运行状况信息，但是 Smart Call Home 服务提供了对系统运行状况的自定义支持，从而使思科 TAC 能够监控您的设备，并且在存在问题时 （通常在您知道问题已发生之前）提交个案。

可以在系统上同时配置这两个服务，尽管配置 Smart Call Home 服务将会提供与 Anonymous Reporting 相同的功能以及自定义服务。

配置 Anonymous Reporting

要配置 Anonymous Reporting，请执行下列步骤：

操作步骤

步骤 1　选择 **Configuration > Device Management > Smart Call Home**。

步骤 2　选择 **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，请执行下列步骤。

操作步骤

步骤 1　选择 **Configuration > Device Management > Smart Call Home**。

步骤 2　选择 **Enable Registered Smart Call Home** 复选框，以启用 Smart Call Home 并向思科 TAC 注册您的 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. 您可以在 **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. 您可以在 **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。

- 清单警报组。
- 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**，您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. 选择 **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. 选择 **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网络地址。

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、清单、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. 您可以在 **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星期几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分派警报的事件严重性，然后点击 **OK**。

步骤 9　对于基于时间的清单警报，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分派警报的频率，然后点击 **OK**。

步骤 11　对于基于时间的快照警报，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星期几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　对于基于事件的系统日志警报，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. 选择 **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. 选择 **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分派警报的系统日志消息 ID。

d. 点击 **OK** 以保存配置。

步骤 13　对于基于事件的遥测警报，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星期几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

表 42-1　Anonymous Reporting 和 Smart Call Home 的历史

功能名称	平台版本	说明
Smart Call Home	8.2(2)	Smart Call Home 服务用于在 ASA 上提供主动诊断和实时警报，并提供更高的网络可用性和运行效率。 我们引入了以下屏幕： Configuration > Device Management > Smart Call Home。
Anonymous Reporting	9.0(1)	您可以通过启用 Anonymous Reporting 服务来帮助改进 ASA 平台，此服务使思科能够安全地接收来自设备的最少量错误和运行状况信息。 我们修改了以下屏幕：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 配置为订用安全级别为 “ 紧急 ” 的诊断警报组，那么将向思科发送 Smart Call Home 消息以报告重要的集群事件。仅对于以下三个事件，才会发送 Smart Call Home 集群消息： • 当装置加入集群时 • 当装置离开集群时 • 当集群装置变成集群主装置时 发送的每条消息都包含以下信息： • 处于活动状态的集群成员的计数 • 对集群主装置运行的 **show cluster info** 命令和 **show cluster history** 命令的输出

第 10 部分

参考网站

地址、协议和端口

本章提供 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（八位元），字段之间用点分隔。 IP 地址的第一个部分识别主机所在的网络，第二个部分识别给定网络上的特定主机。网络号字段称为网络前缀。给定网络上的所有主机共享同一个网络前缀，但必须有唯一的主机号。对于有类 IP，地址类确定网络前缀与主机号之间的边界。

类

IP 主机地址分为三种不同的地址类：A 类、 B 类和 C 类。每一类在 32 位地址内的不同点固定网络前缀与主机号码之间的边界。 D 类地址保留用于组播 IP。

- A 类地址 （1.xxx.xxx.xxx 到 126.xxx.xxx.xxx）仅将第一个八位元用作网络前缀。
- B 类地址 （128.0.xxx.xxx 到 191.255.xxx.xxx）将前两个八位元用作网络前缀。
- C 类地址 （192.0.0.xxx 到 223.255.255.xxx）将前三个八位元用作网络前缀。

由于 A 类地址具有 16,777,214 个主机地址，B 类地址具有 65,534 台主机，因此，可以使用子网掩码将这些庞大的网络分割成较小的子网。

专用网络

如果需要在网络上使用大量地址，但不需要在互联网上路由这些地址，可以使用互联网编号分配机构 (IANA) 推荐的专用 IP 地址 （请参阅 RFC 1918）。以下地址范围被指定为不应通告的专用网络：

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

子网掩码

通过子网掩码，可以将一个 A 类、B 类或 C 类网络转换为多个网络。利用子网掩码，可以创建扩展网络前缀，从而将主机号中的位添加到网络前缀中。例如，C 类网络前缀始终包含 IP 地址的前三个八位元。但是， C 类扩展网络前缀还部分使用第四个八位元。

如果使用二进制记法而不是点分十进制记法，将会有助于理解子网掩码。子网掩码中的位与互联网地址一一对应：

- 如果 IP 地址中的对应位是扩展网络前缀的一部分，该位将被设置为 1。
- 如果该位是主机号的一部分，将被设置为 0。

示例 1：如果有 B 类地址 129.10.0.0，并想将第三个八位元全部用作扩展网络前缀而不是主机号的一部分，则必须将子网掩码指定为 11111111.11111111.11111111.00000000。该子网掩码将这个 B 类地址转换为等效的 C 类地址，其中的主机号仅包含最后一个八位元。

示例 2：如果只想将第三个八位元的一部分用于扩展网络前缀，必须将子网掩码指定为类似 11111111.11111111.11111000.00000000 的形式，这种形式的子网掩码仅将第三个八位元中的 5 位用于扩展网络前缀。

可以将子网掩码写成点分十进制掩码或 */ 位数*（“ 斜杠 *位数* ”）掩码。在示例 1 中，对于点分十进制掩码，可以将每个二进制八位元转换为十进制数：255.255.255.0。对于 */ 位数*掩码，可以添加数字 1s: /24。在示例 2 中，十进制数为 255.255.248.0， / 位数为 /21。

还可以将第三个八位元的一部分用于扩展网络前缀，从而将多个 C 类网络构建成一个较大的超网。例如， 192.168.0.0/20。

确定子网掩码

请参阅表 43-1，以根据您希望拥有的主机数来确定子网掩码。

注　子网的第一个和最后一个数字已保留，但 /32 除外，该数字用于识别单个主机。

表 43-1　　主机、位掩码和点分十进制掩码

主机	/ 位掩码	点分十进制掩码
16,777,216	/8	255.0.0.0 A 类网络
65,536	/16	255.255.0.0 B 类网络
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0

表 43-1　主机、位掩码和点分十进制掩码 （续）

主机	/ 位掩码	点分十进制掩码
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	255.255.255.0 C 类网络
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
不使用	/31	255.255.255.254
1	/32	255.255.255.255 单个主机地址

确定要与子网掩码配合使用的地址

以下各节介绍如何确定要与 C 类和 B 类网络的子网掩码配合使用的网络地址。

C 类网络地址

对于主机数在 2 与 254 之间的网络，第四个八位元是主机地址数量的倍数，从 0 开始。例如，表 43-2 显示了 8 主机子网 (/29) 为 192.168.0.x。

注　子网的第一个和最后一个地址已保留。在第一个子网示例中，不能使用 192.168.0.0 或 192.168.0.7。

表 43-2　C 类网络地址

掩码为 /29 (255.255.255.248) 的子网	地址范围
192.168.0.0	192.168.0.0 到 192.168.0.7
192.168.0.8	192.168.0.8 到 192.168.0.15
192.168.0.16	192.168.0.16 到 192.168.0.31
-	-
192.168.0.248	192.168.0.248 到 192.168.0.255

B 类网络地址

要确定与主机数在 254 与 65,534 之间的网络的子网掩码配合使用的网络地址，需要确定每个可能的扩展网络前缀的第三个八位元的值。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，前两个八位元是固定的，因为它们用于扩展网络前缀中，第四个八位元是 0，因为所有位都用于主机号。

要确定第三个八位元的值，请按照以下步骤操作：

步骤 1　用 65,536 （使用第三个和第四个八位元的地址的总数）除以您想要的主机地址数量，以计算出可从网络构建的子网数量。

例如， 65,536 除以 4096 个主机等于 16。

因此， 4096 个地址有 16 个子网，每个都位于 B 类网络上。

步骤 2　用 256 （第三个八字元值的数量）除以子网数量，以确定第三个八字元值的倍数：

在本示例中， 256/16 = 16。

第三个八字元是 16 的倍数，从 0 开始。

表 43-3 显示了网络 10.1 的 16 个子网。

注　子网的第一个和最后一个地址已保留。在第一个子网示例中，不能使用 10.1.0.0 或 10.1.15.255。

表 43-3　　网络的子网

掩码为 /20 (255.255.240.0) 的子网	地址范围
10.1.0.0	10.1.0.0 到 10.1.15.255
10.1.16.0	10.1.16.0 到 10.1.31.255
10.1.32.0	10.1.32.0 到 10.1.47.255
-	-
10.1.240.0	10.1.240.0 到 10.1.255.255

IPv6 地址

IPv6 是继 IPv4 之后的下一代互联网协议。它提供经过扩展的地址空间、简化的报头格式、经过改进的扩展和选项支持、流标签功能以及身份验证和隐私功能。有关 IPv6 的介绍，请参阅 RFC 2460。有关 IPv6 寻址架构的介绍，请参阅 RFC 3513。

本节介绍 IPv6 地址的格式和架构。

相关主题

第 12-12 页的配置 IPv6 寻址

IPv6 地址格式

IPv6 地址以一系列八个 16 位十六进制字段表示，字段之间用冒号 (:) 分隔，格式为：x:x:x:x:x:x:x:x。下面是 IPv6 地址的两个示例：

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

注　IPv6 地址中的十六进制字母不区分大小写。

不需要将前导零包含在地址的各个字段中，但每个字段必须至少包含一位数。因此，示例地址 2001:0DB8:0000:0000:0008:0800:200C:417A 从左侧数起的第三到第六个字段中的前导零可移除，从而缩短为 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移除了三个前导零，仅留下了一个 8，从左侧数起的第六个字段移除了一个前导零，留下了 800。

对 IPv6 地址来说，包含几个连续的十六进制零字段很常见。可以使用两个冒号 (::) 压缩 IPv6 地址开始、中间或结尾位置的连续零字段 （冒号表示连续的十六进制零字段）。表 43-4 显示了不同类型 IPv6 地址的几个地址压缩示例。

表 43-4　　IPv6 地址压缩示例

地址类型	标准形式	压缩形式
单播	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
组播	FF01:0:0:0:0:0:0:101	FF01::101
环回	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

注　两个冒号 (::) 在 IPv6 地址中只能用一次，用以表示连续的零字段。

在同时包含 IPv4 和 IPv6 地址的环境中，通常使用 IPv6 的替代格式。此替代格式为 x:x:x:x:x:x:y.y.y.y，其中，x 表示 IPv6 地址六个高位部分的十六进制值，y 表示该地址 32 位 IPv4 部分的十进制值（该部分代替 IPv6 地址的剩余两个 16 位部分）。例如，IPv4 地址 192.168.1.1 可表示为 IPv6 地址 0:0:0:0:0:0:FFFF:192.168.1.1 或 ::FFFF:192.168.1.1。

IPv6 地址类型

以下是 IPv6 地址的三种主要类型：

- **Unicast** - 单播地址是单个接口的标识符。发送到单播地址的数据包将会传输到通过该地址识别的接口。一个接口可能分配有多个单播地址。
- **Multicast** - 组播地址是一组接口的标识符。发送到某个组播地址的数据包将会传输到通过该地址识别的所有地址。
- **Anycast** - 任播地址是一组接口的标识符。与组播地址不同的是，发送到任播地址的数据包仅传输到 “ 最近 ” 的接口 （以路由协议的距离为测量标准）。

注　IPv6 中没有广播地址。组播地址提供广播功能。

单播地址

本节介绍 IPv6 单播地址。单播地址识别网络节点上的接口。

全局地址

IPv6 全局单播地址的通用格式为全局路由前缀，其后跟的是子网 ID，然后是接口 ID。全局路由前缀可以是未被其他 IPv6 地址类型保留的任何前缀。

所有的全局单播地址 （以二进制 000 开头的除外）都具有改良 EUI-64 格式的 64 位接口 ID。

以二进制 000 作为开头的全局单播地址在地址的接口 ID 部分的大小或结构上没有任何限制。具有嵌入式 IPv4 地址的 IPv6 地址就是属于此类型的地址。

相关主题

- 第 43-9 页的 IPv6 地址前缀
- 第 43-7 页的接口标识符
- 第 43-6 页的与 IPv4 兼容的 IPv6 地址

站点本地地址

站点本地地址用于在一个站点内寻址。此类地址可在不使用全局唯一前缀的情况下用于对整个站点进行寻址。站点本地地址具有前缀 FEC0::/10，后跟 54 位子网 ID，并以改良 EUI-64 格式的 64 位接口 ID 结尾。

站点本地路由器不将具有源或目标站点本地地址的任何数据包转发到站点外。因此，站点本地地址可被视为专用地址。

链路本地地址

所有接口均需要有至少一个链路本地地址。可以根据接口配置多个 IPv6 地址，但只能配置一个链路本地地址。

链路本地地址是一个 IPv6 单播地址，通过使用链路本地前缀 FE80::/10 和改良 EUI-64 格式接口标识符，可在任意接口上自动配置此类地址。链路本地地址用于邻居发现协议和无状态自动配置过程。使用链路本地地址的节点可进行通信；它们不需要站点本地地址或全局唯一地址即可进行通信。

路由器不会转发具有源或目标链路本地地址的任何数据包。因此，链路本地地址可被视为专用地址。

与 IPv4 兼容的 IPv6 地址

有两种类型的 IPv6 地址可包含 IPv4 地址。

第一种类型是与 IPv4 兼容的 IPv6 地址。IPv6 过渡机制包括通过 IPv4 路由基础设施用隧道动态传输 IPv6 数据包的主机和路由器技术。使用此技术的 IPv6 节点分配有特殊的 IPv6 单播地址，从而可传送低位 32 位的全局 IPv4 地址。此类地址被称为与 IPv4 兼容的 IPv6 地址，其格式为 ::y.y.y.y，其中， y.y.y.y 是 IPv4 单播地址。

注　在与 IPv4 兼容的 IPv6 地址中使用的 IPv4 地址必须为全局唯一的 IPv4 单播地址。

第二种类型的 IPv6 地址具有嵌入式 IPv4 地址，被称为 IPv4 映射 IPv6 地址。此类地址用于将 IPv4 节点的地址表示为 IPv6 地址。此类地址的格式为 ::FFFF:y.y.y.y，其中， y.y.y.y 是 IPv4 单播地址。

未指定地址

未指定地址 0:0:0:0:0:0:0:0 表示没有 IPv6 地址。例如，IPv6 网络上新初始化的节点可能将未指定地址用作其数据包的源地址，直至它接收到 IPv6 地址。

注　未指定 IPv6 地址不能分配给接口。未指定 IPv6 地址不得用作 IPv6 数据包或 IPv6 路由报头中的目标地址。

环回地址

环回地址 0:0:0:0:0:0:0:1 可被节点用于向其自身发送 IPv6 数据包。 IPv6 中的环回地址与 IPv4 (127.0.0.1) 中的环回地址功能相同。

注　IPv6 环回地址不能分配给物理接口。将 IPv6 环回地址用作其源地址或目标地址的数据包必须留在创建该数据包的节点内。 IPv6 路由器不转发将 IPv6 环回地址用作其源地址或目标地址的数据包。

接口标识符

IPv6 单播地址中的接口标识符用于标识链路上的接口。接口标识符在子网前缀内需要是唯一的。很多情况下，接口标识符来源于接口链路层地址。可以将同一个接口标识符用在一个节点的多个接口上，前提是，这些接口连接到不同的子网。

对于所有单播地址，除了以二进制 000 开头的之外，接口标识符的长度需要是 64 位，且以改良 EUI-64 格式构造。改良 EUI-64 格式以 48 位 MAC 地址为基础，通过颠倒 MAC 地址中的通用 / 本地位并在 MAC 地址的上三个字节与下三个字节之间插入十六进制数 FFFE 创建而成。

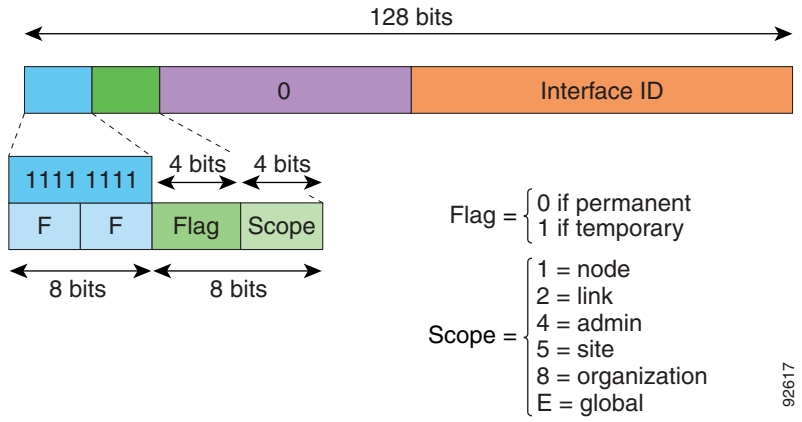
例如，具有 MAC 地址 00E0.b601.3B7A 的接口有一个 64 位接口 ID 02E0:B6FF:FE01:3B7A。

组播地址

IPv6 组播地址是一组接口的标识符，组中的标识符通常位于不同的节点上。发送到某个组播地址的数据包将会传输到通过组播该地址识别的所有接口。一个接口可属于任意数量的组播组。

IPv6 组播地址具有前缀 FF00::/8 (1111 1111)。紧跟前缀的八位元定义组播地址的类型和范围。永久分配（已知）的组播地址具有一个等于 0 的标志参数；临时（瞬时）组播地址具有一个等于 1 的标志参数。有节点范围、链路范围、站点范围、组织范围或全局范围的组播地址分别具有范围参数 1、 2、 5、 8 或 E。例如，前缀为 FF02::/16 的组播地址是具有链路范围的永久组播地址。图 43-1 显示了 IPv6 组播地址的格式。

图 43-1　　IPv6 组播地址格式



IPv6 节点 （主机和路由器）需要加入到以下组播组：

- 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　请求节点地址用于邻居请求消息中。

IPv6 路由器需要加入到以下组播组：

- FF01::2 （接口本地）
- FF02::2 （链路本地）
- FF05::2 （站点本地）

组播地址不得用作 IPv6 数据包中的源地址。

注　IPv6 中没有广播地址。 IPv6 组播地址取代了广播地址。

任播地址

IPv6 任播地址是分配给多个接口的单播地址 （通常属于不同的节点）。路由至一个任播地址的数据包会路由至具有该地址的最近接口，接近度由所用的路由协议确定。

任播地址从单播地址空间中进行分配。任播地址是分配给多于一个接口的单播地址，这些接口必须配置为将该地址识别为任播地址。

以下限制适用于任播地址：

- 任播地址不能用作 IPv6 数据包的源地址。
- 任播地址不能分配给 IPv6 主机，而只能分配给 IPv6 路由器。

注　任播地址在 ASA 上不受支持。

必需地址

IPv6 主机必须至少配置有以下地址 （自动或手动）：

- 用于每个接口的链路本地地址
- 环回地址
- 全节点组播地址
- 用于每个单播或任播地址的请求节点地址

IPv6 路由器必须至少配置有以下地址 （自动或手动）：

- 必需的主机地址
- 用于被配置为用作路由器的所有接口的子网路由器任播地址
- 全路由器组播地址

IPv6 地址前缀

IPv6 地址前缀 （其格式为 ipv6-prefix/prefix-length）可用于表示整个地址空间的连续比特块。IPv6 前缀必须采用 RFC 2373 规定的格式，在这种格式中，地址用十六进制的 16 位值指定，各个值之间用冒号分隔。前缀长度是十进制值，表示组成前缀 （地址的网络部分）的地址高位连续位有多少。例如， 2001:0DB8:8086:6502::/32 是有效的 IPv6 前缀。

IPv6 前缀识别 IPv6 地址的类型。表 43-5 显示了各种 IPv6 地址类型的前缀。

表 43-5　IPv6 地址类型前缀

地址类型	二进制前缀	IPv6 记法
未指定	000...0 （128 位）	::/128
环回	000...1 （128 位）	::1/128
组播	11111111	FF00::/8
链路本地 （单播）	1111111010	FE80::/10
站点本地 （单播）	1111111111	FEC0::/10
全局 （单播）	所有其他地址。	
任播	取自单播地址空间。	

协议和应用

表 43-6 列出了协议的文字值和端口号；两者均可在 ASA 命令中输入。

表 43-6　　协议文字值

文字	值	说明
ah	51	IPv6 的身份验证报头， RFC 1826。
eigrp	88	增强型内部网关路由协议。
esp	50	IPv6 的封装安全负载， RFC 1827。
gre	47	通用路由封装。
icmp	1	互联网控制消息协议， RFC 792。
icmp6	58	IPv6 的互联网控制消息协议， RFC 2463。
igmp	2	互联网组管理协议， RFC 1112。
igrp	9	内部网关路由协议。
IP	0	互联网协议。
ipinip	4	IP-in-IP 封装。
ipsec	50	IP 安全。输入 ipsec 协议文字相当于输入 esp 协议文字。
nos	94	网络操作系统 (Novell's NetWare)。
ospf	89	开放式最短路径优先路由协议， RFC 1247。
pcp	108	负载压缩协议。
pim	103	协议无关组播。
pptp	47	点对点隧道协议。输入 pptp 协议文字相当于输入 gre 协议文字。
snp	109	Sitara 网络协议。
tcp	6	传输控制协议， RFC 793。
udp	17	用户数据报协议， RFC 768。

可以在 IANA 网站上联机查看协议号：

http://www.iana.org/assignments/protocol-numbers

TCP 和 UDP 端口

表 43-7 列出了端口的文字值和端口号；两者均可在 ASA 命令中输入。请参阅以下说明：

- ASA 将端口 1521 用于 SQL*Net。这是 Oracle for SQL*Net 所用的默认端口。但是，此值与 IANA 端口分配不一致。
- ASA 侦听端口 1645 和 1646 上的 RADIUS。如果 RADIUS 服务器使用标准端口 1812 和 1813，可以将 ASA 配置为使用 **authentication-port** 和 **accounting-port** 命令侦听这些端口。
- 要分配 DNS 访问的端口，请使用 **domain** 文字值，而不是 **dns**。如果使用 **dns**，则 ASA 会假设您打算使用 **dnsix** 文字值。

可以在 IANA 网站上联机查看端口号：
http://www.iana.org/assignments/port-numbers

表 43-7　　端口文字值

文字	TCP 还是 UDP？	值	说明
aol	TCP	5190	美国在线
bgp	TCP	179	边界网关协议， RFC 1163
biff	UDP	512	供邮件系统用于通知用户新邮件已收到
bootpc	UDP	68	引导协议客户端
bootps	UDP	67	引导协议服务器
chargen	TCP	19	字符生成器
citrix-ica	TCP	1494	Citrix 独立计算结构 (ICA) 协议
cmd	TCP	514	与 **exec** 类似，但 **cmd** 还具有自动身份验证
ctiqbe	TCP	2748	计算机电话接口快速缓冲区编码
daytime	TCP	13	白天， RFC 867
discard	TCP、 UDP	9	丢弃
domain	TCP、 UDP	53	DNS
dnsix	UDP	195	DNSIX 会话管理模块审核重定向器
echo	TCP、 UDP	7	回显
exec	TCP	512	远程进程执行
finger	TCP	79	Finger
ftp	TCP	21	文件传输协议 （控制端口）
ftp-data	TCP	20	文件传输协议 （数据端口）
gopher	TCP	70	Gopher
https	TCP	443	使用 SSL 的 HTTP
h323	TCP	1720	H.323 呼叫信令
hostname	TCP	101	NIC 主机名服务器
ident	TCP	113	身份验证服务
imap4	TCP	143	互联网消息访问协议，版本 4
irc	TCP	194	互联网中继聊天协议
isakmp	UDP	500	互联网安全关联和密钥管理协议
kerberos	TCP、 UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn Shell
ldap	TCP	389	轻量级目录访问协议
ldaps	TCP	636	轻量级目录访问协议 (SSL)
lpd	TCP	515	行式打印机后台守护程序 - 打印机后台打印程序
login	TCP	513	远程登录

表 43-7　　端口文字值 （续）

文字	TCP 还是 UDP？	值	说明
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
nntp	TCP	119	网络新闻传输协议
ntp	UDP	123	网络时间协议
pcanywhere-status	UDP	5632	pcAnywhere 状态
pcanywhere-data	TCP	5631	pcAnywhere 数据
pim-auto-rp	TCP、 UDP	496	协议无关组播，反向路径泛洪，密集模式
pop2	TCP	109	邮局协议 - 版本 2
POP3	TCP	110	邮局协议 - 版本 3
pptp	TCP	1723	点对点隧道协议
radius	UDP	1645	远程身份验证拨入用户服务
radius-acct	UDP	1646	远程身份验证拨入用户服务 （计帐）
rip	UDP	520	路由信息协议
secureid-udp	UDP	5510	使用 UDP 的 SecureID
smtp	TCP	25	简单邮件传输协议
snmp	UDP	161	简单网络管理协议
snmptrap	UDP	162	简单网络管理协议 - 陷阱
sqlnet	TCP	1521	结构化查询语言网络
ssh	TCP	22	安全外壳
sunrpc (rpc)	TCP、 UDP	111	Sun 远程过程调用
syslog	UDP	514	系统日志
tacacs	TCP、 UDP	49	增强型终端访问控制器访问控制系统
talk	TCP、 UDP	517	通话
telnet	TCP	23	RFC 854 Telnet
tftp	UDP	69	简单文件传输协议
time	UDP	37	时间
uucp	TCP	540	UNIX 对 UNIX 复制程序
who	UDP	513	谁
whois	TCP	43	是谁
www	TCP	80	万维网
xdmcp	UDP	177	X 显示管理器控制协议

本地端口和协议

表 43-8 列出了 ASA 为了处理流向 ASA 的流量而打开的协议、 TCP 端口和 UDP 端口。除非启用了表 43-8 中所列的功能和服务，否则，ASA *不会*打开任何本地协议或任何 TCP 或 UDP 端口。打开默认的侦听协议或端口，必须配置 ASA 的功能或服务。很多情况下，启用功能或服务后，可以配置除默认端口以外的端口。

表 43-8　　按功能和服务打开的协议和端口

功能或服务	协议	端口号	备注
DHCP	UDP	67,68	-
故障转移控制	105	不适用	-
HTTP	TCP	80	-
HTTPS	TCP	443	-
ICMP	1	不适用	-
IGMP	2	不适用	协议只能在目标 IP 地址 224.0.0.1 上打开
ISAKMP/IKE	UDP	500	可配置。
IPsec (ESP)	50	不适用	-
通过 UDP 的 IPsec (NAT-T)	UDP	4500	-
通过 UDP 的 IPsec（兼容思科 VPN 3000 系列）	UDP	10000	可配置。
通过 TCP 的 IPsec (CTCP)	TCP	-	未使用默认端口。配置通过 TCP 的 IPsec 时，必须指定端口号。
NTP	UDP	123	-
OSPF	89	不适用	协议只能在目标 IP 地址 224.0.0.5 和 224.0.0.6 上打开
PIM	103	不适用	协议只能在目标 IP 地址 224.0.0.13 上打开
RIP	UDP	520	-
RIPv2	UDP	520	端口只能在目标 IP 地址 224.0.0.9 上打开
SNMP	UDP	161	可配置。
SSH	TCP	22	-
状态更新	8（非安全）9（安全）	不适用	-
Telnet	TCP	23	-
VPN 负载均衡	UDP	9023	可配置。
VPN 个人用户身份验证代理	UDP	1645、 1646	端口只能通过 VPN 隧道访问。

ICMP 类型

表 43-9 列出了 ICMP 类型的编号和名称 （可以在 ASA 命令中输入这些信息）。

表 43-9　　ICMP 类型

ICMP 编号	ICMP 名称
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect