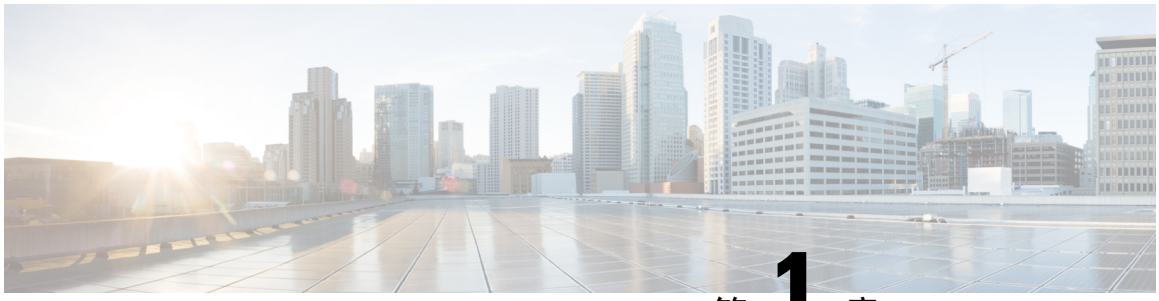
Cisco Secure Firewall 设备管理器配置指南，版本 7.4

首次发布日期: 2023 年 12 月 5 日

上次修改日期: 2024 年 7 月 23 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录



第 1 章

使用入门

以下主题介绍如何开始配置 Cisco Secure Firewall Threat Defense （前称 Firepower Threat Defense）。

本指南适用对象

本指南介绍如何使用威胁防御设备自带的 Secure Firewall 设备管理器 （原名 Firepower 设备管理器）基于 Web 的配置界面配置威胁防御 。

设备管理器可以配置小型或中型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多威胁防御设备的大型网络。

如果要管理大量设备或要使用威胁防御支持的更复杂的功能和配置，请使用 Cisco Secure Firewall Management Center（原名 Firepower 管理中心）而不是集成的设备管理器来配置您的设备。

设备管理器/威胁防御 版本 7.4.1 的新功能

发布日期：2023 年 12 月 13 日

下表列出了在使用 设备管理器进行配置时 威胁防御 7.4.1 中可用的新功能：

特性	说明
平台功能	
Firepower 1010E 支持返回。。	返回对 Firepower 1010E 的支持，该支持在版本 7.2.3 中引入并已在版本 7.3 中暂时弃用。

特性	说明
Cisco Secure Firewall 3130 和 3140 的网络模块。	我们为 Cisco Secure Firewall 3130 和 3140 引入了这些网络模块。 • 2 端口 100G QSFP+ 网络模块 (FPR3K-XNM-2X100G) 请参阅： Cisco Secure Firewall 3110、3120、3130 和 3140 硬件安装指南
VPN 功能	
适用于 Cisco Secure Firewall 3100 的 VTI 环回接口上的 IPsec 流分流。	**升级影响。开始分流符合条件的连接。** 在 Cisco Secure Firewall 3100 上，现在默认通过 VTI 环回接口分流符合条件的 IPsec 连接。以前，此功能仅在物理接口上受支持。此功能在升级时自动启用。 您可以使用 FlexConfig 和 **flow-offload-ipsec** 命令更改配置。
接口功能	
合并的管理接口和诊断接口。	**升级影响。升级后合并接口。** 对于使用 7.4 及更高版本的新设备，您不能使用旧诊断接口。仅合并的管理接口可用。如果已升级到 7.4 或更高版本，并且没有为诊断接口进行任何配置，则接口将自动合并。 如果已升级到 7.4 或更高版本，并且已为诊断接口进行了配置，则可以选择手动合并接口，也可以继续使用单独的诊断接口。请注意，在更高版本中将删除对诊断接口的支持，因此您应计划尽快合并接口。 合并模式还会将 AAA 流量的行为更改为默认使用数据路由表。现在，只有在配置中指定管理专用接口（包括管理接口）时，才可以使用管理专用路由表。 新增/修改的菜单项： • **设备** > **接口** > **管理**接口 • （已移动到接口）**系统设置** > **管理接口** • **设备** > **接口** > **所需的合并接口操作** > **管理接口合并** 新增/经修改的命令： **show management-interface convergence**

特性	说明
不利用 Azure 和 GCP Threat Defense Virtual 的旧版诊断接口。	现在，您可以在没有诊断接口的情况下在 Azure 和 GCP 的 Threat Defense Virtual 上进行部署。Azure 部署仍需要至少两个数据接口，但 GCP 要求您将诊断接口替换为数据接口，新的至少三个接口。（以前，Threat Defense Virtual 部署需要一个管理接口、一个诊断接口和至少两个数据接口。） 限制：此功能仅支持新部署。升级后的设备不支持此功能。 请参阅： Cisco Secure Firewall Threat Defense Virtual 入门指南
适用于 Firepower 1000 系列、Firepower 2100 和 Secure Firewall 3100 的内联集。	您可以在 Firepower 1000 系列、Firepower 2100 和 Secure Firewall 3100 设备上配置内联集。我们在“接口”页面中添加了内联集选项卡。
许可功能	
更改许可证名称并支持运营商许可证。	许可证已被重命名： • 威胁现在更改为 IPS • 恶意软件现在更改为恶意软件防御 • 基本现在更改为基础版 • AnyConnect Apex 现在更改为 Secure Client Premier • AnyConnect Plus 现在更改为 Secure Client Advantage • 仅限 AnyConnect VPN 现在更改为仅限 Secure Client VPN 此外，您现在可以应用运营商许可证，该许可证允许您配置 GTP/GPRS、Diameter、SCTP 和 M3UA 检测。使用 FlexConfig 来配置这些功能。
管理和故障排除功能	
默认 NTP 服务器更新。	**升级影响。系统连接至新源。** 默认 NTP 服务器已从 sourcefire.pool.ntp.org 更改为 time.cisco.com。要使用其他 NTP 服务器，请选择 **设备**，然后点击 **系统设置** 面板中的 **时间服务** 。
用于 HTTPS 管理用户访问的 SAML 服务器。	您可以将 SAML 服务器配置为为 HTTPS 管理访问提供外部身份验证。您可以配置具有以下类型的授权访问的外部用户：管理员、审核管理员、加密管理员、读写用户、只读用户。在使用 SAML 服务器时，您可以使用通用访问卡 (CAC) 登录。 我们更新了 SAML 身份源对象配置和 **系统设置** > **管理访问**页面，以接受这些配置。

特性	说明
检测威胁防御高可用性对中的配置不匹配。	现在，您可以使用 CLI 来检测威胁防御高可用性对中的配置不匹配。 新增/修改的 CLI 命令：**show failover config-sync error**、**show failover config-sync stats** 请参阅： Cisco Secure Firewall Threat Defense 命令参考
使用 Cisco Secure Firewall 3100 捕获丢弃的数据包。	因 MAC 地址表不一致而导致的数据包丢失可能会影响您的调试功能。Cisco Secure Firewall 3100 现在可以捕获这些丢弃的数据包。 新增/修改的CLI 命令：在 **capture** 命令中的 **[drop**{**disable** | **mac-filter**}] 。 请参阅： Cisco Secure Firewall Threat Defense 命令参考
包含在 FXOS 升级中的固件升级。	**机箱/FXOS 升级影响。固件升级会导致设备额外重启一次。** 对于 Firepower 4100/9300，FXOS 升级到 2.14.1+ 版现在包括固件升级。如果设备上的任何固件组件比 FXOS 软件包中的旧，则 FXOS 升级也会更新固件。如果固件已升级，设备会重新启动两次 - 一次是因为 FXOS，另一次是因为固件。 与软件和操作系统升级一样，在固件升级期间不要进行或部署配置更改。即使系统显示为非活动状态，也不要在固件升级过程中手动重新启动或关闭。 请参阅： Cisco Firepower 4100/9300 FXOS 固件升级指南
Firepower 1000/2100 和 Firepower 4100/9300 的数据平面故障后恢复速度更快。	当 Firepower 1000/2100 或 Firepower 4100/9300 上的数据平面进程崩溃时，系统会重新加载进程，而不是重新启动设备。重新加载数据平面还会重新启动其他进程，包括 Snort。如果数据平面在启动期间崩溃，设备将遵循正常的重新加载/重启顺序；这可以避免重新加载循环。 默认情况下，新设备和升级设备均启用此功能。要禁用它，请使用 FlexConfig。 新增/修改的 ASA CLI 命令： **data-plane quick-reload**、**show data-plane quick-reload status** 新增/修改的威胁防御 CLI 命令： **show data-plane quick-reload status** 支持的平台：Firepower 4100/9300、Firepower 4100/9300 请参阅： Cisco Secure Firewall Threat Defense 命令参考 和 Cisco Secure Firewall ASA 系列命令参考。

登录系统

威胁防御设备有两个界面：

设备管理器 网络接口

设备管理器 在 Web 浏览器中运行。使用该界面可配置、管理和监控系统。

命令行界面（CLI、控制台）

可以使用 CLI 进行故障排除。您也可以将其用于初始设置，而不是 设备管理器。

以下主题介绍如何登录这些界面和管理您的用户账户。

用户角色决定用户的访问及操作权限

用户名分配了角色，而角色决定用户能够在 设备管理器中查看哪些内容，或执行哪些操作。本地定义的 **admin** 用户拥有所有权限，但如果使用不同的账户登录，享有的权限可能会减少。

设备管理器 窗口的右上角将显示您的用户名和权限级别。

权限：

- **管理员** - 可以查看和使用所有功能。
- **读写用户**-可以执行只读用户可以执行的任何操作，还可以编辑和部署配置。唯一的限制是无法执行关键系统操作，包括安装升级、创建和恢复备份、查看审核日志以及中止其他 设备管理器用户的会话。
- **只读用户** - 可以查看控制面板和配置，但不能进行任何更改。如果尝试进行更改，错误消息会解释由于缺乏权限出错。
- **加密管理员** - 您可以配置与加密相关的功能（例如证书、解密策略和密钥）。对其他功能的只读权限。
- **审核管理员** - 您可以查看用户登录历史记录和审计日志并执行审核相关操作。对配置功能的只读权限。

这些权限与 CLI 用户可享受的权限不相关。

登录至设备管理器

设备管理器可用于配置、管理和监控系统。配置功能可通过浏览器实现，但无法通过命令行界面 (CLI) 执行，即：必须使用 Web 界面实施安全策略。

使用最新版本的以下浏览器：Firefox、Chrome、Safari、Edge。

注释 如果输入错误的密码且连续 3 次尝试登录失败，账户将锁定 5 分钟。必须待锁定时间结束后方可尝试重新登录。

开始之前

最初，您只能使用 **管理员** 用户名登录 设备管理器 。但是，您可以稍后为外部 AAA 服务器中定义的其他用户配置授权，如管理 设备管理器 和 威胁防御 用户访问 ， 第 785 页中所述。

一次最多可以有 5 个活动登录用户。这包括登录到设备管理器和活动 API 会话（以未过期的 API 令牌表示）的用户。如果超过此限制，则最早的会话（设备管理器登录或 API 令牌）将过期以允许建立新会话。这些限制不适用于 SSH 会话。

过程

步骤 1 使用浏览器打开系统主页，例如 https://ftd.example.com。

您可以使用以下地址中的任何一个。如果配置了 Ipv4 或 IPv6 地址或 DNS 名称，则可以直接使用。

- 管理地址。 默认情况下（在大多数平台上），管理接口是 DHCP 客户端，因此 IP 地址取决于您的 DHCP 服务器。
- 您为 HTTPS 访问打开的数据接口的地址。默认情况下（在大多数平台上），“inside”接口允许 HTTPS 访问，因此可以连接到默认的内部地址 192.168.95.1。有关适用于您型号的内部 IP 地址的详细信息，请参阅进行初始设置之前的默认配置 ， 第 22 页。

  如果更改了 HTTPS 数据端口，则必须在 URL 中包含该自定义端口。例如，如果您已将端口更改为 4443，则 URL 应为：https://ftd.example.com:4443

提示 如果浏览器未配置为识别服务器证书，系统会显示一条有关证书不受信任的警告。将证书作为一种例外接受，或者将证书放到受信任的根证书存储库中。

步骤 2 （仅限本地用户和 RADIUS。）输入为设备定义的用户名和密码，然后点击 **登录**。

您可以使用“**admin**”用户名，这是预定义的用户。默认管理员密码为 Admin123。在 AWS上，除非您在初始部署期间使用用户数据（**高级详细信息** > **用户数据**）定义默认密码，否则默认管理员密码为 AWS 实例 ID。

如果会话连续30分钟处于非活动状态，就会过期，系统将提示您重新登录。从页面右上角的用户图标下拉菜单中选择**注销 (Log Out)**。

步骤 3 （仅限 SAML 服务器。）点击 **登录** 按钮旁边的 **单点登录 (SSO)** 链接。

这会将您引导至 SAML 服务器进行登录。请勿输入凭证，只需点击链接即可。如果输入本地凭证并点击登录，则会使用本地数据库登录。

在 SAML 服务器的登录页面上，像往常一样登录。如果您使用通用访问卡 (CAC) 登录，请点击链接以使用证书登录。设备管理器不直接处理 CAC 身份验证。

登录命令行界面 (CLI)

使用命令行界面 (CLI) 可设置系统以及对系统进行基本的故障排除。无法通过 CLI 会话配置策略。

要登录到 CLI，请执行以下一项操作：

- 使用设备随附的控制台电缆将您的 PC 连接到使用终端仿真器的控制台，终端仿真器的设置为 9600 波特率、8 个数据位、无奇偶校验、1 个停止位、无流量控制。有关控制台电缆的详细信息，请参阅设备的硬件指南。

注释 在 Firepower 和 Secure Firewall 设备型号上，控制台端口上的 CLI 是 Secure Firewall eXtensible 操作系统 (FXOS)。对于某些设备型号，您可以使用 **connect ftd** 命令进入 威胁防御 CLI。对于 Firepower 4100/9300，请参阅连接到应用控制台，第 182 页。仅将 FXOS CLI 用于机箱级故障排除。使用威胁防御 CLI 进行基本配置、监控和正常的系统故障排除。有关 FXOS 命令的信息，请参阅 FXOS 文档。

- 对于 threat defense virtual，请打开虚拟控制台。
- 使用 SSH 客户端连接到管理 IP 地址。如果您为 SSH 连接打开某个数据接口，也可以连接到该接口上的地址（请参阅配置管理访问列表，第 728 页）。默认情况下，SSH 数据接口访问处于禁用状态。使用 **admin** 用户名或其他 CLI 用户账户登录。默认管理员密码为 Admin123。在 AWS上，除非您在初始部署期间使用用户数据（**高级详细信息** > **用户数据**）定义默认密码，否则 threat defense virtual 的默认管理员密码为 AWS 实例 ID。

提示

- 登录后，如需了解 CLI 中可用命令的相关信息，请输入 **help** 或 **?**。有关使用信息，请参阅 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html 中的Cisco Firepower Threat Defense 命令参考。
- 您可以使用 **configure user add** 命令创建可登录 CLI 的本地用户账户。但这些用户只能登录 CLI，他们无法登录设备管理器 Web 界面。
- 您可以在外部服务器中创建可访问 SSH 的用户账户。有关配置 SSH 访问外部身份验证的信息，请参阅配置 威胁防御 CLI (SSH) 用户外部授权 (AAA)，第 787 页。

更改密码

密码应定期更改。以下步骤程序介绍了登录到 设备管理器时如何更改密码。

注释 如果已登录到 CLI，可使用 **configure password** 命令更改密码。您可以使用 **configure user password** *username* 命令为不同的 CLI 用户更改密码。

开始之前

此步骤仅适用于本地用户。如果用户账户是在外部 AAA 服务器上定义的，必须通过该服务器更改密码。

过程

步骤 1 从菜单右上角的用户图标下拉列表中选择**配置文件**。

步骤 2 点击**密码**选项卡。

步骤 3 输入您当前的密码。

步骤 4 输入新密码，然后进行确认。

您可以点击**生成**，为您生成随机的 16 个字符密码。点击“显示密码”() 按钮可查看无掩蔽的密码。然后，点击**复制到剪贴板**链接，以便将密码粘贴到确认字段中。

该页面包括密码的最低要求。您无法更改这些最低要求。密码必须：

- 介于 8 至 128 个字符之间
- 至少有一个小写和一个大写字母
- 至少有一个数字
- 至少有一个特殊字符
- 不包含重复的字母

步骤 5 点击**更改**。

设置用户配置文件首选项

您可以设置用户界面的首选项并更改密码。

过程

步骤 1 从菜单右上角的用户图标下拉列表中选择**配置文件**。

步骤 2 在**配置文件**选项卡中配置以下选项，然后点击**保存**。

- **安排任务的时区** - 选择安排备份和更新等任务要使用的时区。如果此处设置了不同的时区，将对控制面板和事件使用浏览器时区。
- **颜色主题** - 选择用户界面中要使用的颜色主题。

步骤 3 在**密码**选项卡中，可以输入新密码并点击**更改**。

查看英语之外语言的页面

您可以查看以下语言的 GUI 和联机帮助。

- 中文
- 英语（默认）
- 日语
- 韩语

要使用这些语言，您必须在浏览器设置中选择该语言。产品本身没有语言设置。

如果您的浏览器不支持特定语言，则产品不会以该语言显示。例如，仅当您将浏览器配置为使用加拿大法语时，才会显示法语版本。选择其他类型的法语会使产品显示英语。

设置系统

只有完成初始配置，系统才能在网络中正常运行。成功部署包括正确连接电缆和配置将设备插入网络所需的地址，以及将设备连接到互联网或其他上游路由器。以下程序介绍了相关过程。

开始之前

在开始初始设置之前，设备中包括了一些默认设置。有关详细信息，请参阅进行初始设置之前的默认配置，第 22 页。

过程

步骤 1 连接接口，第 10 页

步骤 2 使用设置向导完成初始配置，第 19 页

有关生成的配置的详细信息，请参阅初始设置之后的配置，第 25 页。

连接接口

默认配置假定某些接口用于内部和外部网络。如果基于上述预期将网线连接至接口，初始配置将变得更易于完成。

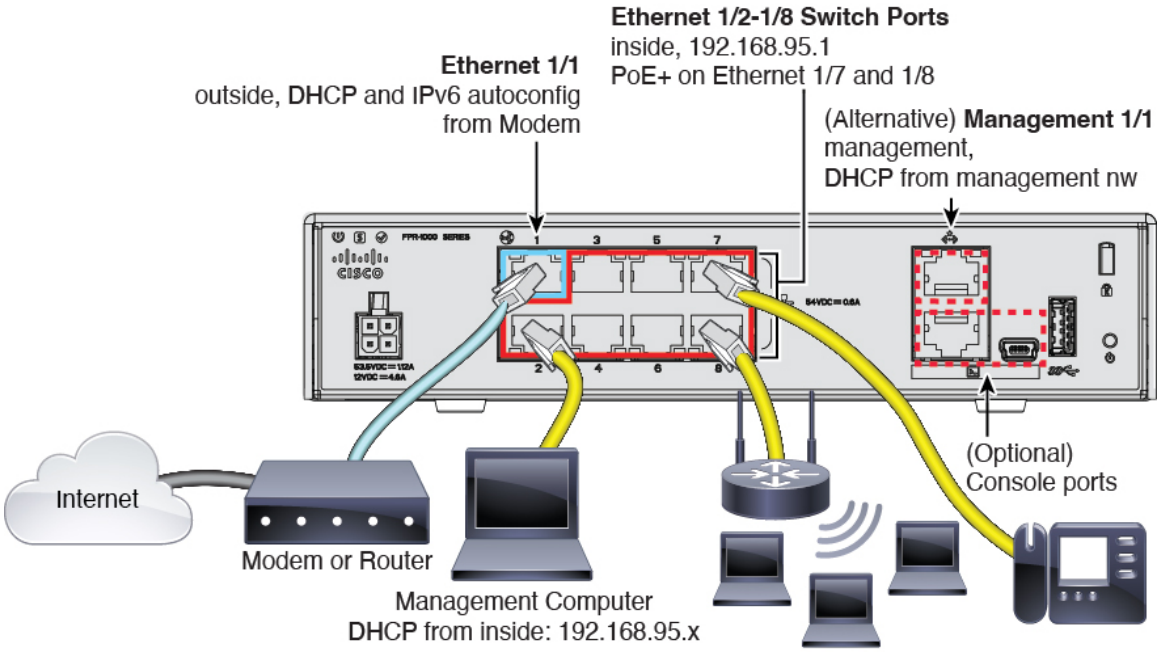
大多数型号的默认配置旨在让您将管理计算机连接至内部接口。或者，您也可以直接将工作站连接到管理端口。接口位于不同的网络上，因此不要尝试将任何内部接口和管理端口连接到同一网络。

不要将任何内部接口连接至具有活动 DHCP 服务器的网络。这将与已在内部接口上运行的 DHCP 服务冲突。如果要为网络使用不同的 DHCP 服务器，请在初始设置后禁用不需要的 DHCP 服务器。

以下主题介绍了在使用内部接口配置设备时，如何为该拓扑进行系统布线。

为 Firepower 1010 布线

图 *1: Firepower 1010* 的布线



- 将您的管理计算机连接至以下接口之一：
  - 以太网 1/2 至 1/8 - 将您的管理计算机直接连接到其中一个内部交换机端口（以太网 1/2 至 1/8），内部网络的默认 IP 地址为 (192.168.95.1)，并运行 DHCP 服务器以向客户端（包括管理计算机）提供 IP 地址，因此请确保这些设置不会与任何现有内部网络设置冲突。
  - 管理接口 1/1 - 将管理计算机连接至管理网络。管理 1/1 接口将从 DHCP 获取 IP 地址，因此请确保您的网络中包含 DHCP 服务器。

    如果需要将管理 1/1 IP 地址从默认值更改为配置静态 IP 地址，还必须将管理计算机连接到控制台端口。请参阅 （可选）在 CLI 中更改管理网络设置，第 18 页。

可稍后从其他接口中配置管理访问权限。

- 将外部网络连接至以太网 1/1 接口。

  默认情况下，使用 IPv4 DHCP 和 IPv6 自动配置获取 IP 地址，但可以在初始配置期间设置静态地址。

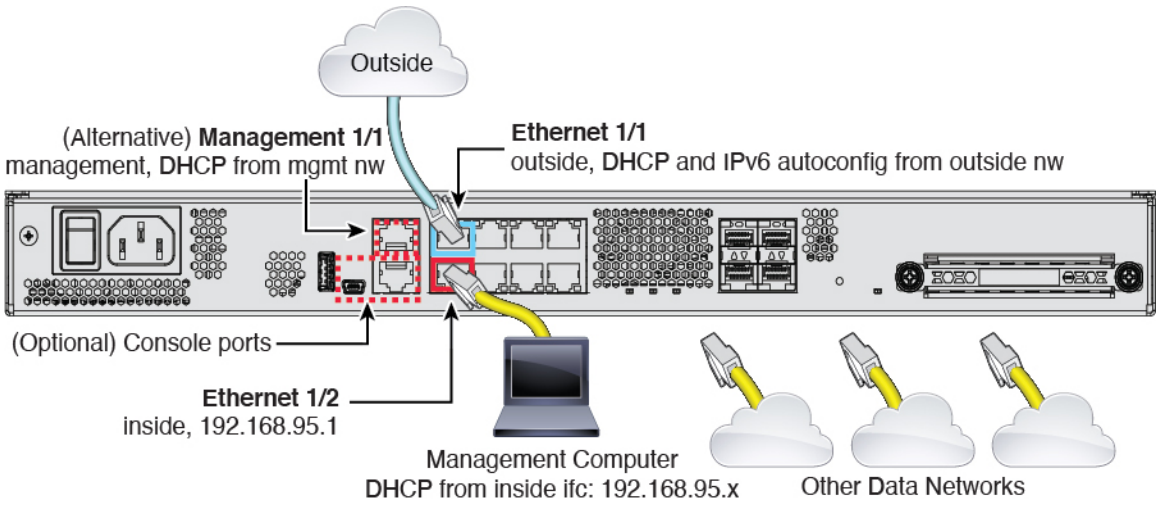
- 将内部设备连接到剩余交换机端口（以太网 1/2 至 1/8）。

  以太网 1/7 和 1/8 是以太网供电+ (PoE+) 端口。

注释 Firepower 1010E 上不支持 PoE。

为 Firepower 1100 布线

图 *2: Firepower 1100* 的布线



- 将您的管理计算机连接至以下任一接口：
  - 以太网 1/2 - 将您的管理计算机直接连接至以太网 1/2 以进行初始配置，或将以太网 1/2 连接至内部网络。以太网 1/2 具有默认 IP 地址 (192.168.95.1)，并运行 DHCP 服务器以向客户端（包括管理计算机）提供 IP 地址，因此请确保这些设置不会与任何现有内部网络设置冲突。
  - 管理接口 1/1（标记为 MGMT）- 将管理计算机连接至管理网络。管理 1/1 接口将从 DHCP 获取 IP 地址，因此请确保您的网络中包含 DHCP 服务器。

    如果需要将管理 1/1 IP 地址从默认值更改为配置静态 IP 地址，还必须将管理计算机连接到控制台端口。请参阅 （可选）在 CLI 中更改管理网络设置，第 18 页。

  可稍后从其他接口中配置管理访问权限。

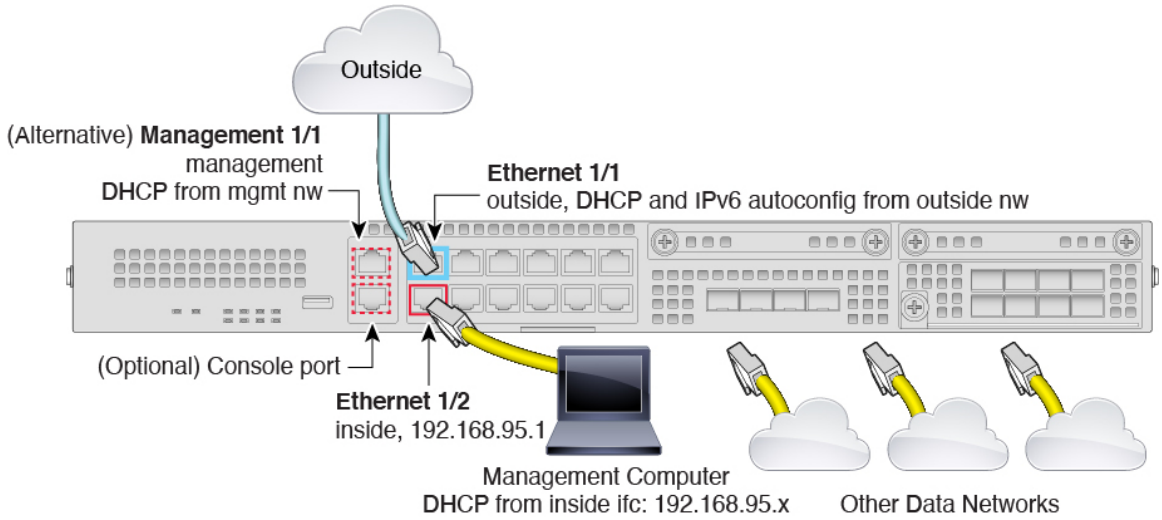
- 将外部网络连接至以太网 1/1 接口（标记为 WAN）。

默认情况下，使用 IPv4 DHCP 和 IPv6 自动配置获取 IP 地址，但可以在初始配置期间设置静态地址。

- 将其他网络连接到其余接口。

为 Firepower 2100 布线

图 *3: Firepower 2100* 的布线



- 将您的管理计算机连接至以下任一接口：
  - 以太网 1/2 - 将您的管理计算机直接连接至以太网 1/2 以进行初始配置，或将以太网 1/2 连接至内部网络。以太网 1/2 具有默认 IP 地址 (192.168.95.1)，并运行 DHCP 服务器以向客户端（包括管理计算机）提供 IP 地址，因此请确保这些设置不会与任何现有内部网络设置冲突
  - 管理接口 1/1（标记为 MGMT）- 将管理计算机连接至管理网络。管理 1/1 接口将从 DHCP 获取 IP 地址，因此请确保您的网络中包含 DHCP 服务器。

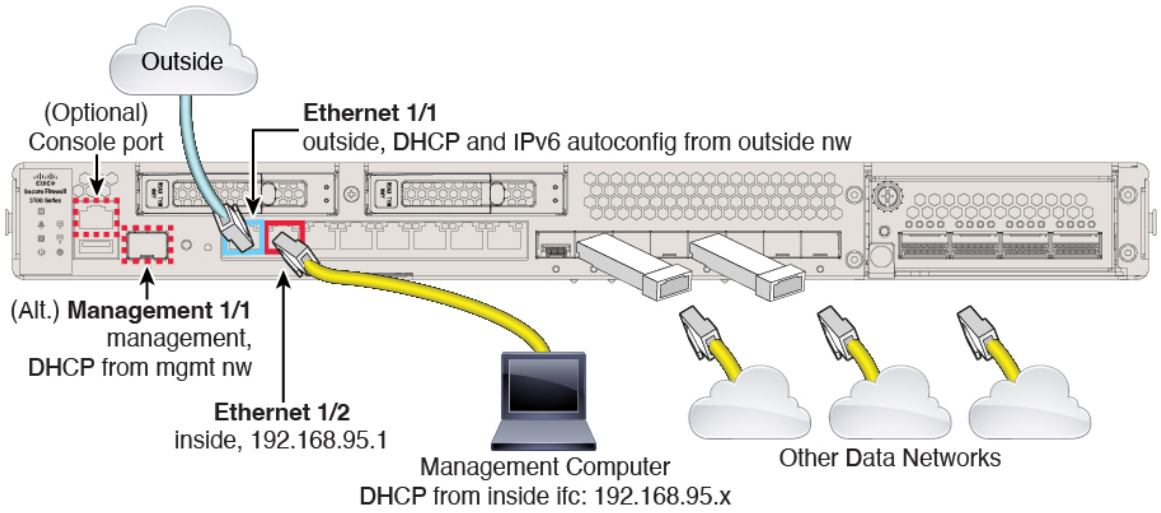
    如果需要将管理 1/1 IP 地址从默认值更改为配置静态 IP 地址，还必须将管理计算机连接到控制台端口。请参阅 （可选）在 CLI 中更改管理网络设置，第 18 页。

  可稍后从其他接口中配置管理访问权限。
- 将外部网络连接至以太网 1/1 接口（标记为 WAN）。

  默认情况下，使用 IPv4 DHCP 和 IPv6 自动配置获取 IP 地址，但可以在初始配置期间设置静态地址。
- 将其他网络连接到其余接口。

为 Secure Firewall 3100 布线

图 *4: Secure Firewall 3100* 的布线



在管理 1/1 或以太网 1/2 上管理 威胁防御 设备。默认配置还会将以太网 1/1 配置为外部接口。

- 将您的管理计算机连接至以下任一接口：
  - 以太网 1/2 - 将您的管理计算机直接连接至以太网 1/2 以进行初始配置，或将以太网 1/2 连接至内部网络。以太网 1/2 具有默认 IP 地址 (192.168.95.1)，并且还会运行 DHCP 服务器以向客户端（包括管理计算机）提供 IP 地址，因此，请确保这些设置不会与任何现有内部网络设置冲突。
  - 管理 1/1 - 将管理 1/1 接口连接到管理网络，并确保管理计算机位于管理网络上，或者可以访问管理网络。管理 1/1 接口从管理网络上的 DHCP 服务器获取 IP 地址；如果使用此接口，则必须确定分配给防火墙的 IP 地址，以便可以从管理计算机连接到 IP 地址。

    如果需要将管理 1/1 IP 地址从默认值更改为配置静态 IP 地址，还必须将管理计算机连接到控制台端口。请参阅 （可选）在 CLI 中更改管理网络设置，第 18 页。

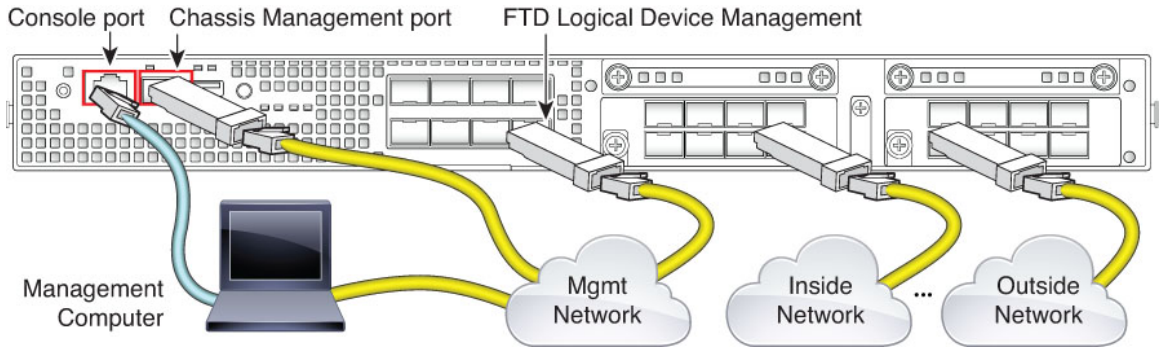
注释 管理 1/1 是需要 SFP 模块的 10 Gb 光纤接口。

- 将外部网络连接到以太网 1/1 接口。

  默认情况下，使用 IPv4 DHCP 和 IPv6 自动配置获取 IP 地址，但可以在初始配置期间设置静态地址。

- 将其他网络连接到其余接口。

为 Firepower 4100 布线



在逻辑设备管理接口上执行初始 威胁防御 配置。可以稍后从任何数据接口启用管理。 威胁防御 设备需连接互联网才可访问许可和更新，且默认行为是将管理流量路由至部署设备时指定的网关 IP 地址。如果希望将管理流量从背板路由至数据接口，则可以稍后在 设备管理器 中配置该设置。

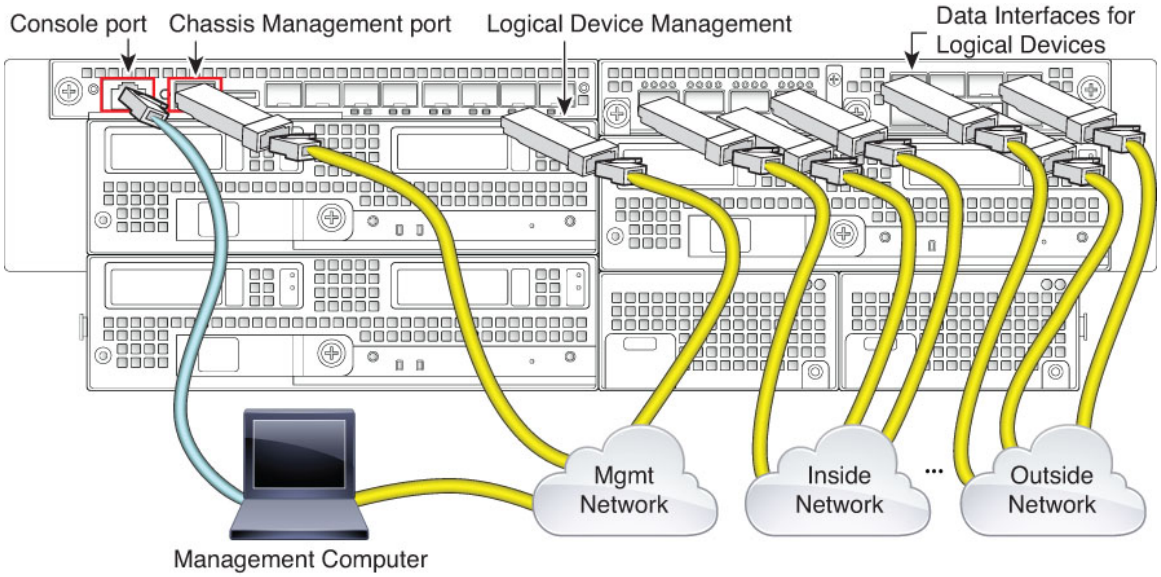
连接以下接口以执行机箱初始设置、持续监控以及使用逻辑设备。

- 控制台端口 - 将管理计算机连接至控制台端口，以执行机箱的初始设置。Firepower 4100 包括 RS-232 转 RJ-45 串行控制台电缆。可能需要使用第三方串口转 USB 电缆建立连接。
- 机箱管理端口 - 将机箱管理端口连接至您的管理网络，以进行配置和持续的机箱管理。
- 威胁防御 逻辑设备管理接口 - 可以选择机箱上用于此目的的任何接口，而不是保留用于 FXOS 管理的机箱管理端口。
- 数据接口 - 将数据接口连接至您的逻辑设备数据网络。可以配置物理接口、Etherchannel 和分支端口，以划分高容量接口。

  对于高可用性配置，请将数据接口用于故障转移/状态链路。

注释 除控制台端口之外的所有接口均需要 SFP/SFP+/QSFP 收发器。请参阅受支持收发器的硬件安装指南。

为 Firepower 9300 布线



在逻辑设备管理接口上执行初始 威胁防御 配置。可以稍后从任何数据接口启用管理。 威胁防御 设备需连接互联网才可访问许可和更新，且默认行为是将管理流量路由至部署设备时指定的网关 IP 地址。如果希望将管理流量从背板路由至数据接口，则可以稍后在 设备管理器 中配置该设置。

连接以下接口以执行机箱初始设置、持续监控以及使用逻辑设备。

- 控制台端口 - 将管理计算机连接至控制台端口，以执行机箱的初始设置。Firepower 9300 包括 RS-232 转 RJ-45 串行控制台电缆。可能需要使用第三方串口转 USB 电缆建立连接。
- 机箱管理端口 - 将机箱管理端口连接至您的管理网络，以进行配置和持续的机箱管理。
- 逻辑设备管理接口 - 使用一个或多个接口管理逻辑设备。可以选择机箱上用于此目的的任何接口，而不是保留用于 FXOS 管理的机箱管理端口。管理接口可以在逻辑设备之间共享，也可以按照逻辑设备使用单独的接口。通常，可以与所有逻辑设备共享管理接口，或者如果使用单独的接口，请将其置于单个管理网络上。但是确切的网络要求可能有所不同。
- 数据接口 - 将数据接口连接至您的逻辑设备数据网络。可以配置物理接口、Etherchannel 和分支端口，以划分高容量接口。可以根据网络要求将多个逻辑设备连接至相同网络或不同网络。所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。

  对于高可用性配置，请将数据接口用于故障转移/状态链路。

注释 除控制台端口之外的所有接口均需要 SFP/SFP+/QSFP 收发器。请参阅受支持收发器的硬件安装指南。

为 Threat Defense Virtual虚拟布线

要安装 threat defense virtual，请前往 http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/products-installation-guides-list.html，参阅用于您的虚拟平台的快速入门指南。以下虚拟平台支持 设备管理器 ： VMware、KVM、Microsoft AzureAmazon Web 服务 (AWS)。

threat defense virtual 默认配置将管理接口和内部接口置于同一子网上。您的管理接口必须具有互联网连接，才能使用智能许可并获取系统数据库的更新。

因此，默认配置的设计使您可以将 Management0/0 和 GigabitEthernet0/1（内部）两个接口都连接到虚拟交换机上的同一网络。默认管理地址使用内部 IP 地址作为网关。因此，管理接口路由通过内部接口，然后通过外部接口连通互联网。

您还可以选择将 Management0/0 连接到与用于内部接口的子网不同的子网，只要使用具有互联网接入的网络即可。确保为网络正确配置管理接口 IP 地址和网关。

VMware 网络适配器和接口如何映射到 威胁防御 物理接口

您可以为 VMware threat defense virtual 设备配置最多 10 个接口。您必须配置至少 4 个接口。

确保 Management0-0 源网络关联到可以访问互联网的 VM 网络。这是必需的，以便系统可以与思科智能软件管理器通信并下载系统数据库更新。

安装 OVF 时分配网络。只要您配置一个接口，稍后便可以通过 VMware 客户端更改虚拟网络。然而，如果需要添加新接口，请务必在列表结尾添加接口；如果在任何其他位置添加或删除接口，则虚拟机监控程序将对接口重新编号，从而使配置中的接口 ID 与错误接口相匹配 中所述。

下表介绍 VMware 网络适配器和源接口如何映射到 threat defense virtual 物理接口名称。对其他接口命名遵循相同的模式，并将相关数字增加一。所有其他接口都是数据接口。有关将虚拟网络分配到虚拟机的详细信息，请参阅 VMware 在线帮助。

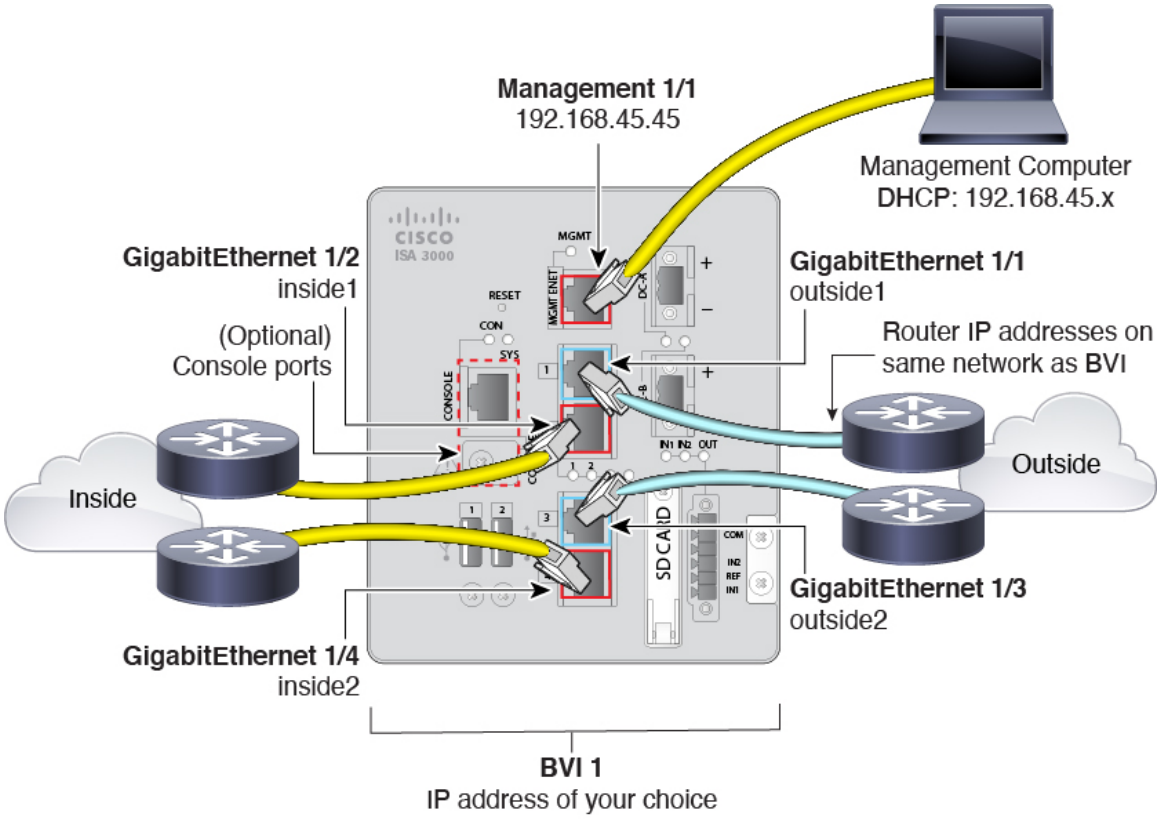
表 *1:* 源网络与目标网络的映射

网络适配器	源网络	目标网络（物理接口名称）	功能
网络适配器 1	Management0-0	Management0/0	管理
网络适配器 2	保留供内部使用。	保留供内部使用。	保留供内部使用。
网络适配器 3	GigabitEthernet0-0	GigabitEthernet0/0	外部数据
网络适配器 4	GigabitEthernet0-1	GigabitEthernet0/1	内部数据
网络适配器 5	GigabitEthernet0-2	GigabitEthernet0/2	数据流量
网络适配器 6	GigabitEthernet0-3	GigabitEthernet0/3	数据流量
网络适配器 7	GigabitEthernet0-4	GigabitEthernet0/4	数据流量
网络适配器 8	GigabitEthernet0-5	GigabitEthernet0/5	数据流量
网络适配器 9	GigabitEthernet0-6	GigabitEthernet0/6	数据流量

网络适配器	源网络	目标网络（物理接口名称）	功能
网络适配器 10	GigabitEthernet0-7	GigabitEthernet0/7	数据流量

ISA 3000 的布线

图 *5: ISA 3000*



- 将 GigabitEthernet 1/1 连接至外部路由器，并将 GigabitEthernet 1/2 连接至内部路由器。

  这些接口构成硬件旁路对。

- 将 GigabitEthernet 1/3 连接至冗余外部路由器，并将 GigabitEthernet 1/4 连接至冗余内部路由器。

  如果您的型号具有铜端口，这些接口形成硬件旁路对；光纤不支持硬件旁路。如果另一对发生故障，这些接口会提供冗余网络路径。这些数据接口中的所有 4 个接口均位于您所选择的同一网络中。您需要将 BVI 1 IP 地址配置为与内部和外部路由器位于同一网络中。

- 将管理接口 1/1 连接至您的管理计算机（或网络）。

  如果需要将管理 1/1 IP 地址从默认值更改为其他值，还必须将管理计算机连接至控制台端口。请参阅 （可选）在 CLI 中更改管理网络设置，第 18 页。

（可选）在 CLI 中更改管理网络设置

如果您无法使用默认管理 IP 地址，可以连接到控制台端口并在 CLI 中执行初始设置，包括设置管理 IP 地址、网关和其他基本网络设置。您只能配置管理接口设置；而无法配置内部或外部接口，稍后可在 GUI 中配置它们。

注释 不需要为 Firepower 4100/9300 使用此过程，因为您已经在部署时手动设置 IP 地址。

注释 除非清除配置，否则无法重复 CLI 设置脚本（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 Cisco Secure Firewall Threat Defense 命令参考。

过程

步骤 1 连接到 威胁防御 控制台端口。有关详细信息，请参阅登录命令行界面 (CLI)，第 7 页。

步骤 2 使用用户名 **admin** 登录。

默认管理员密码为 Admin123。在 AWS上，除非您在初始部署期间使用用户数据（**高级详细信息** > **用户数据**）定义默认密码，否则 threat defense virtual 的默认管理员密码为 AWS 实例 ID。

步骤 3 首次登录威胁防御时，系统会提示您接受“最终用户许可协议”(EULA)并。然后，系统将显示CLI设置脚本。

默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

请参阅以下准则：

- **输入管理接口的 IPv4 默认网关** - 如果您设置手动 IP 地址，则可以输入网关路由器的**数据接口**或 IP 地址。**data-interfaces** 设置将通过背板发送出站管理流量，以退出数据接口。如果您没有可以访问互联网的单独管理网络，则此设置非常有用。源自管理接口的流量包括需要访问互联网的许可证注册和数据库更新。如果您使用 **data-interfaces**，在直接连接到管理网络的情况下，您仍可以在管理接口上使用 设备管理器（或SSH）但是，要对特定网络或主机进行远程管理，则应该使用 **configure network static-routes** 命令添加静态路由。请注意，数据接口上的 设备管理器 管理不受此设置的影响。如果使用 DHCP，则系统使用 DHCP 提供的网关，如果 DHCP 不提供网关，则使用**数据接口**作为回退方法。
- **如果网络信息已更改则需要重新连接** - 如果您已通过 SSH 连接到默认 IP 地址，但在初始设置时更改了 IP 地址，则会断开连接。使用新 IP 地址和密码重新进行连接。控制台连接不会受影响。
- **在本地管理设备？** - 输入**是 (yes)** 以使用 设备管理器。回答**否 (no)** 表示您打算使用本地部署或云端交付管理中心来管理设备。

示例：

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

步骤 4 在新的管理 IP 地址上登录设备管理器 。

使用设置向导完成初始配置

在首次登录设备管理器时，系统会通过设备设置向导指导您完成初始系统配置。

如果您计划在高可用性配置中使用设备，请阅读准备两台用于高可用性的设备 ， 第 196 页。

注释 Firepower 4100/9300 和 ISA 3000 不支持安装向导，因此该流程不适用于这些型号。对于 Firepower 4100/9300，从机箱部署逻辑设备时，设置所有初始配置。对于 ISA 3000，在发货前应用特殊默认配置。

开始之前

确保将数据接口连接到网关设备（例如电缆调制解调器或路由器）。对于边缘部署，网关设备可能是面向互联网的网关。对于数据中心部署，可能是主干路由器。使用您的设备型号的默认“外部”接口（请参阅连接接口 ， 第 10 页和进行初始设置之前的默认配置 ， 第 22 页）。

然后，将管理计算机连接到适用于您的硬件型号的“内部”接口。或者，可以连接到管理接口。对于 threat defense virtual，只需确保连接到管理 IP 地址。

（threat defense virtual 除外，该项需要从管理 IP 地址连接到互联网。）管理接口不需要连接到网络。默认情况下，系统通过连接到互联网的数据接口（通常为外部接口），获取系统许可授权和数据库以及其他更新。如果想使用单独的管理网络，则可以在完成初始设置后，将管理接口连接到网络并配置单独的管理网关。

要在无法访问默认 IP 地址的情况下更改管理接口网络设置，请参阅（可选）在 CLI 中更改管理网络设置，第 18 页。

过程

步骤 1 登录设备管理器。

a) 假定您未在 CLI 中进行初始配置，请在 **https://***ip-address*中打开 设备管理器，其中地址为以下项之一。

- 如果连接到内部接口，则地址为：**https://192.168.95.1**。
- （threat defense virtual 为强制要求）如果您已连接到管理接口：**https://192.168.45.45**。
- （所有其他型号）如果您已连接到管理接口： **https://***dhcp_client_ip*

b) 使用用户名 **admin** 登录。默认管理员密码为 Admin123。在 AWS上，除非您在初始部署期间使用用户数据（**高级详细信息** > **用户数据**）定义默认密码，否则 threat defense virtual 的默认管理员密码为 AWS 实例 ID。。

步骤 2 如果是首次登录系统，而且您未使用过 CLI 安装向导，系统将提示您阅读并接受“最终用户许可协议”以及更改管理员密码。

只有完成这些步骤，才能继续。

步骤 3 为外部接口和管理接口配置以下选项，然后点击**下一步 (Next)**。

注意 点击**下一步 (Next)** 后，您的设置将部署到设备中。该接口将命名为“outside”，并添加到“outside_zone”安全区。请确保您的设置准确无误。

外部接口

- **配置 IPv4** - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择**关**，不配置 IPv4 地址。不管是通过静态方式还是通过 DHCP，都不要在与默认内部地址相同的子网上配置 IP 地址（请参阅进行初始设置之前的默认配置，第 22 页）。 您无法使用安装向导配置 PPPoE。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。您可以在完成向导后配置 PPPoE。请参阅配置物理接口，第 230 页。
- **配置 Ipv6** - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择**关**，不配置 IPv6 地址。

管理接口

- **DNS 服务器** - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器或您从 DHCP 服务器获取的 DNS 服务器。如果您编辑字段并想要恢复默认值，请点击**使用 OpenDNS (Use OpenDNS)** 以重新将合适的 IP 地址载入字段。您的 ISP 可能会要求您使用特定的 DNS 服务器。如果您在完成向导后发现无法进行 DNS 解析，请参阅为管理接口排除 DNS 故障，第 798 页。
- **防火墙主机名** - 系统管理地址的主机名。

步骤 4 配置系统时间设置，然后点击**下一步 (Next)**。

- **时区** - 选择系统时区。
- **NTP 时间服务器** - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

步骤 5 为系统配置智能许可证。

只有具有智能许可证帐户，才能获取和应用系统需要的许可证。最初，可以使用为期90天的评估许可证，以后再设置智能许可。

要立即注册设备，请选择注册设备的选项，点击链接登录您的智能软件管理器账户，生成新的令牌，并将该令牌复制到编辑框。还必须选择服务区域，并决定是否将使用数据发送至 Cisco Success Network。屏幕上的文本更详细地解释了这些设置。

如果您还不想注册设备，请选择评估模式选项。评估期长达90天。若要在以后注册设备并获取智能许可证，请点击**设备**，然后点击**智能许可证 (Smart Licenses)** 组中的链接。

步骤 6 点击**完成 (Finish)**。

下一步做什么

- 如果要使用可选许可证涵盖的功能（例如基于类别的URL过滤、入侵检测或恶意软件防御），请启用所需的许可证。请参阅启用或禁用可选许可证，第 87 页。
- 将其他数据接口连接到不同的网络并配置这些接口。有关配置接口的信息，请参阅如何添加子网，第 66 页和接口，第 225 页。
- 如果通过内部接口管理设备，并且想通过内部接口打开 CLI 会话，请打开用于 SSH 连接的内部接口。请参阅配置管理访问列表，第 728 页。
- 查看使用案例以了解如何使用产品。请参阅最佳实践：威胁防御的使用案例，第 39 页。

如果未获取外部接口的 IP 地址该怎么办

默认设备配置包括一个用于内部接口的静态 Ipv4 地址。此时无法通过初始设备设置向导更改该地址，但随后可以进行更改。

默认的内部 IP 地址可能与连接到设备的其他网络冲突。如果在外部接口上使用 DHCP 从互联网服务提供商 (ISP) 处获取地址，尤其如此。有些 ISP 使用与内部网络相同的子网作为地址池。由于两个数据接口不能使用位于同一子网上的地址，因此无法在外部接口上配置来自 ISP 的冲突地址。

如果内部静态 IP 地址与外部接口上 DHCP 提供的地址存在冲突，则连接图应将外部接口显示为管理 UP，但没有 IPv4 地址。

在这种情况下，设置向导将会成功完成，并且系统将配置所有默认 NAT、访问以及其他策略和设置。只需按照下列程序消除冲突即可。

开始之前

验证ISP连接是否正常。尽管子网冲突会阻碍您获取外部接口上的地址，但如果根本没有连接ISP，也将无法获取地址。

过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接。

步骤 2 将鼠标悬停在内部接口中的**操作**列中，然后点击编辑图标 ( )。

步骤 3 在 **IPv4 地址**选项卡中，输入唯一子网上的静态地址，例如 192.168.2.1/24 或 192.168.46.1/24。请注意，默认管理地址是 192.168.45.45/24，因此不使用该子网。

如果已有 DHCP 服务器在内部网络上运行，那么您还可以选择使用 DHCP。但是，首先必须在**为此接口定义 DHCP 服务器**组中点击**删除**，从接口中删除 DHCP 服务器。

步骤 4 在**为此接口定义 DHCP 服务器**区域中，点击**编辑**并将 DHCP 池更改为新子网上的某个范围（例如 192.168.2.5-192.168.2.254）。

步骤 5 点击**确定**，保存接口更改。

步骤 6 点击菜单中的**部署**按钮以部署更改。

步骤 7 点击**立即部署**。

部署完成后，连接图应显示外部接口此时已有一个 IP 地址。使用内部网络中的客户端验证是否已连接到互联网或其他上游网络。

进行初始设置之前的默认配置

在使用本地管理器（设备管理器）对 威胁防御 设备进行初始配置之前，设备包括以下默认配置。

对于许多型号，此配置假定您通过内部接口打开设备管理器，通常是将计算机直接插入接口，并使用内部接口上定义的DHCP服务器为计算机提供IP地址。或者，也可以将计算机插入管理接口，并通过 DHCP 获取地址。但是，某些型号具有不同的默认配置和管理要求。有关详细信息，请参阅下表。

注释 在使用向导执行设置操作之前，可以使用 CLI 设置（（可选）在 CLI 中更改管理网络设置，第 18 页）预配置其中的许多设置。

默认配置设置

设置	默认	是否可在初始配置期间更改？
管理员用户的密码。	Admin123 Firepower 4100/9300：部署逻辑设备时设置密码。 AWS：除非您在初始部署期间使用用户数据（**高级详细信息** > **用户数据**）定义默认密码，否则默认值为 AWS 实例 ID。	是。必须更改默认密码。
管理 IP 地址。	通过 DHCP 获取。 Threat Defense Virtual192.168.45.45 Firepower 4100/9300：部署逻辑设备时设置管理 IP 地址。	否。 对于 Firepower 4100/9300：选择“是”。
管理网关。	设备上的数据接口。通常外部接口会成为通往互联网的路由。此网关仅适用于关联设备流量。如果设备收到来自 DHCP 服务器的默认网关，则使用该网关。 Firepower 4100/9300：部署逻辑设备时设置网关 IP 地址。 ISA 3000：192.168.45.1。 Threat Defense Virtual：192.168.45.1	否。 对于 Firepower 4100/9300：选择“是”。
管理接口的 DNS 服务器。	OpenDNS 公共 DNS 服务器，IPv4：208.67.220.220 和 208.67.222.222；IPv6：2620:119:35::35。系统从不使用从 DHCP 获取的 DNS 服务器。 Firepower 4100/9300：部署逻辑设备时设置 DNS 服务器。	是
内部接口 IP 地址。	192.168.95.1/24 Firepower 4100/9300：未预配置数据接口。 ISA 3000：BVI1 IP 地址未预配置。BVI1 包括所有内部和外部接口。 Threat Defense Virtual: 192.168.45.1/24	否。

设置	默认	是否可在初始配置期间更改？
内部客户端的 DHCP 服务器。	在内部接口上运行，地址池为 192.168.95.5 - 192.168.95.254。 Firepower 4100/9300：未启用 DHCP 服务器。 ISA 3000：未启用 DHCP 服务器。 Threat Defense Virtual：内部接口上的地址池为 192.168.45.46 - 192.168.45.254。	否。
内部客户端的DHCP 自动配置。（自动配置为客户端提供 WINS 和 DNS 服务器的地址。）	在外部接口上启用。	是的，但属于间接更改。如果为外部接口配置的是静态 IPv4 地址，则禁用 DHCP 服务器自动配置。
外部接口 IP 地址。	IPv4：通过 DHCP 从互联网服务提供商 (ISP) 或上游路由器获取。 IPv6：自动配置。 Firepower 4100/9300：未预配置数据接口。 ISA 3000：BVI1 IP 地址未预配置。BVI1 包括所有内部和外部接口。	是。

各个设备型号的默认接口

在初始配置期间不能选择不同的内部接口和外部接口。若要在配置后更改接口分配，请编辑接口和 DHCP 设置。您必须从网桥组中删除一个接口，然后才能将其配置为非交换接口。

威胁防御设备	外部接口	内部接口
Firepower 1010	以太网接口 1/1	VLAN1（包括除外部接口外的所有其他交换机端口）是个物理防火墙接口。
Firepower 1120、1140 和 1150	以太网接口 1/1	以太网接口 1/2
Firepower 2100 系列	以太网接口 1/1	以太网接口 1/2
Secure Firewall 3100 系列	以太网接口 1/1	以太网接口 1/2
Firepower 4100 系列	未预配置数据接口。	未预配置数据接口。
Firepower 9300 设备	未预配置数据接口。	未预配置数据接口。
Threat Defense Virtual	GigabitEthernet0/0	GigabitEthernet0/1

威胁防御设备	外部接口	内部接口
ISA 3000	GigabitEthernet1/1 和 GigabitEthernet1/3 GigabitEthernet1/1 (outside1) 和 1/2 (inside1) 以及 GigabitEthernet1/3 (outside2) 和 1/4 (inside2)（仅非光纤型号）配置为硬件旁路对。 所有内部和外部接口均是 BVI1 的一部分。	GigabitEthernet1/2 和 GigabitEthernet1/4

初始设置之后的配置

在完成安装向导后，设备配置将包括以下设置。下表显示某项特定设置是否为您显式选择的项目，或者它们是否基于您的其他选项而定义。请验证任何“隐式”配置，如果它们不符合您的需求，对其进行编辑。

注释 Firepower 4100/9300 和 ISA 3000 不支持设置向导。对于 Firepower 4100/9300，从机箱部署逻辑设备时，设置所有初始配置。对于 ISA 3000，在发货前应用特殊默认配置。

设置	配置	显式、隐式或默认配置
管理员用户的密码。	您输入的任何信息。	显式。
管理 IP 地址。	通过 DHCP 获取。 Threat Defense Virtual: 192.168.45.45 Firepower 4100/9300：部署逻辑设备时设置的管理 IP 地址。	默认值。
管理网关。	设备上的数据接口。通常外部接口会成为通往互联网的路由。管理网关仅适用于关联设备流量。如果设备收到来自 DHCP 服务器的默认网关，则使用该网关。 Firepower 4100/9300：部署逻辑设备时设置的网关 IP 地址。 ISA 3000：192.168.45.1 Threat Defense Virtual：192.168.45.1	默认值。
管理接口的 DNS 服务器。	OpenDNS 公共 DNS 服务器，IPv4：208.67.220.220 和 208.67.222.222；IPv6：2620:119:35::35，或您输入的任何内容。系统从不使用从 DHCP 获取的 DNS 服务器。 Firepower 4100/9300：部署逻辑设备时设置的 DNS 服务器。	显式。

设置	配置	显式、隐式或默认配置
管理主机名。	**firepower** 或您输入的任何信息。 Firepower 4100/9300：部署逻辑设备时设置的主机名。	显式。
通过数据接口进行管理访问。	数据接口管理访问列表规则允许通过内部接口进行 HTTPS 访问。不允许 SSH 连接。允许 IPv4 和 IPv6 连接。 Firepower 4100/9300：任何数据接口均无默认管理访问规则。 ISA 3000：任何数据接口均无默认管理访问规则。 Threat Defense Virtual：任何数据接口均无默认管理访问规则。	隐式。
系统时间。	您所选的时区和 NTP 服务器。 Firepower 4100/9300：系统时间继承自机箱。 ISA 3000：思科 NTP 服务器：0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org。	显式。
智能许可证。	注册的基本许可证或激活的评估期，以您的选择为准。 未启用订阅许可证。如需启用它们，请转到智能许可页面。	显式。
内部接口 IP 地址。	192.168.95.1/24 Firepower 4100/9300：未预配置数据接口。 ISA 3000：无。必须手动设置 BVI1 IP 地址。 Threat Defense Virtual: 192.168.45.1/24	默认值。
内部客户端的 DHCP 服务器。	在内部接口上运行，地址池为 192.168.95.5 - 192.168.95.254。 Firepower 4100/9300：未启用 DHCP 服务器。 ISA 3000：未启用 DHCP 服务器。 Threat Defense Virtual：内部接口上的地址池为 192.168.45.46 - 192.168.45.254。	默认值。
内部客户端的 DHCP 自动配置。（自动配置为客户端提供 WINS 和 DNS 服务器的地址。）	如果使用 DHCP 来获取外部接口 IPv4 地址，则在外部接口上启用。 如果使用静态寻址，则禁用 DHCP 自动配置。	显式，但属于间接配置。

设置	配置	显式、隐式或默认配置
数据接口配置。	• Firepower 1010 - 外部接口 Ethernet1/1 是物理防火墙接口。所有其他接口均是已启用的交换机端口，且是内部接口 VLAN1 的一部分。可以将终端或交换机插入这些端口，并从内部接口的 DHCP 服务器获取地址。 • Firepower 4100/9300 - 所有其他数据接口均已禁用。 • ISA 3000 - 所有数据接口均已启用，且是同一网桥组 BVI1 的一部分。GigabitEthernet1/1 和1/3 是外部接口，GigabitEthernet1/2 和1/4 都是内部接口。GigabitEthernet1/1 (outside1) 和 1/2 (inside1) 以及 GigabitEthernet1/3 (outside2) 和 1/4 (inside2)（仅非光纤型号）配置为硬件旁路对。 • 所有其他型号 - 外部和内部接口是唯一配置和启用的接口。所有其他数据接口均已禁用。	默认值。
外部物理接口和 IP 地址。	基于设备型号的默认外部端口。请参阅进行初始设置之前的默认配置，第 22 页。 通过 DHCP 和 IPv6 自动配置获取 IP 地址，或者是输入的静态地址 (IPv4、IPv6 或两者)。 Firepower 4100/9300：未预配置数据接口。 ISA 3000：无。必须手动设置 BVI1 IP 地址。	接口是默认值。 寻址是显式值。
静态路由。	如果为外部接口配置的是静态 IPv4 或 IPv6 地址，则会为 IPv4/IPv6 配置相应的静态默认路由，指向您为该地址类型定义的网关。如果选择 DHCP，则从 DHCP 服务器获取默认路由。 另外，也会为网关和“任何”地址创建网络对象，即为 IPv4 创建 0.0.0.0/0，为 IPv6 创建 ::/0。	隐式。
安全区。	**inside_zone**，包含内部接口。对于 Firepower 4100/9300，需要手动将接口添加至此安全区。 **outside_zone**，包含外部接口。对于 Firepower 4100/9300，需要手动将接口添加至此区域。 （您可以编辑这些区域以添加其他接口，也可以自己创建区域）。	隐式。

设置	配置	显式、隐式或默认配置
访问控制策略。	信任从 inside_zone 到 outside_zone 之间所有流量的规则。此规则允许用户的所有流量从网络内部传至外部，并允许这些连接返回所有流量，无需进行检查。 对于任何其他流量，默认操作是阻止。这样可防止外部发起的任何流量进入网络。 Firepower 4100/9300：无预配置访问规则。 ISA 3000：信任从 inside_zone 到 outside_zone 的所有流量的规则，以及信任从 outside_zone 到 inside_zone 的所有流量的规则。流量受阻止。设备还具有信任 inside_zone 和 outside_zone 中的接口之间所有流量的规则。这使得无需检查内部用户和外部用户之间的所有流量。	隐式。
NAT	接口动态 PAT 规则可将发往外部接口的任何 IPv4 流量的源地址转换为外部接口 IP 地址上的唯一端口。 还有一些隐藏的 PAT 规则，允许通过内部接口进行 HTTPS 访问，并通过管理地址的数据接口进行路由。这些不会显示在 NAT 表中，但如果您在 CLI 中使用 **show nat** 命令，就会看到它们。 Firepower 4100/9300：未预配置 NAT。 ISA 3000：未预配置 NAT。	隐式。

配置基本方法

以下主题介绍配置设备的基本方法。

配置设备

首次登录 设备管理器时，系统将通过安装向导来帮助您配置基本设置。完成该向导后，请使用以下方法来配置其他功能和管理设备配置。

如果难以从视觉上区分项目，请在用户配置文件中选择不同的配色方案。从页面右上角的用户图标下拉菜单中选择**配置文件 (Profile)**。

过程

步骤 1 点击**设备**访问**设备摘要**。

该控制面板直观地显示了设备的状态，包括所启用的接口以及关键设置（绿色）已配置或还需继续配置。有关详细信息，请参阅查看接口状态和管理状态，第 34 页。

状态图像的上方是设备型号、软件版本、VDB（系统和漏洞数据库）版本及入侵规则最后更新时间的摘要。此区域还显示高可用性状态，包括配置该功能的链接；请参阅高可用性（故障转移），第 185 页。它还显示云注册状态，如果您使用云管理，则可以看到设备注册使用的账户；请参阅配置云服务，第 750 页。

图像下方是您可以配置的各种功能分组、每组的配置摘要以及管理系统配置可执行的操作。

步骤 2 点击每组中的链接可配置设置或执行操作。

下面是各组的摘要：

- **接口** - 除了管理接口外，至少应配置两个数据接口。请参阅 接口，第 225 页。
- **路由** - 路由配置。必须定义默认路由。根据您的配置，也可能需要其他路由。请参阅路由，第 299 页。
- **更新** - 地理位置、入侵规则和漏洞数据库更新，以及系统软件升级。如果使用这些功能，请设置定期更新计划，以确保您拥有最新的数据库更新。另外，如需在执行定期计划更新之前下载更新，也可以访问此页面。请参阅更新系统数据库和源，第 765 页。
- **系统设置** - 此组包括多种设置。有些设置是在初始设置设备时配置的基本设置，很少更改。请参阅系统设置，第 727 页。
- **智能许可证** - 显示系统许可证的当前状态。必须安装适当的许可证，才能使用该系统。某些功能需要额外的许可证。请参阅为系统授权许可，第 79 页。
- **备份和恢复** - 备份系统配置或恢复先前的备份。请参阅备份和恢复系统，第 774 页。
- **故障排除** - 应思科技术支持中心的要求生成故障排除文件。请参阅创建故障排除文件，第 803 页。
- **站点间 VPN** - 本设备与远程设备之间的站点间虚拟专用网络 (VPN) 连接。请参阅管理站点间 VPN，第 621 页。
- **远程访问 VPN** - 允许外部客户端连接到内部网络的远程访问虚拟专用网 (VPN) 配置。请参阅配置远程访问 VPN，第 662 页。
- **高级配置** - 使用 FlexConfig 和 Smart CLI 配置使用 设备管理器无法配置的功能。请参阅高级配置，第 811 页。
- **设备管理** - 查看审核日志或导出配置副本。请参阅审核与变更管理，第 779 页。

步骤 3 点击菜单中的**部署**按钮以部署更改。

只有将更改部署至设备，更改才会生效。请参阅部署更改，第 31 页。

下一步做什么

在主菜单中点击**策略**，并为系统配置安全策略。另外，也可以点击**对象**配置这些策略中所需的对象。

配置安全策略

使用安全策略实施组织可接受的使用策略并保护网络免受入侵或其他威胁。

过程

步骤 1 点击**策略 (Policies)**。

“安全策略”(Security Policies) 页面显示通过系统实现连接的常规流程以及安全策略的应用顺序。

步骤 2 点击策略的名称并对其进行配置。

虽然必须始终拥有访问控制策略，但可能不需要配置每个策略类型。以下是策略摘要：

- **SSL 解密 (SSL Decryption)** - 如果要检查加密连接（例如 HTTPS）是否存在入侵、恶意软件等，则必须解密连接。使用 SSL 解密策略确定需要解密的连接。系统检查连接后，会将其重新加密。请参阅配置 SSL 解密策略，第 426 页。
- **身份** - 如果要将网络活动与各个用户相关联，或根据用户或用户组成员身份控制网络访问，请使用身份策略确定与给定源 IP 地址关联的用户。请参阅配置身份策略，第 447 页。
- **安全智能** - 使用安全智能策略快速丢弃进出选定 IP 地址或 URL 的连接。阻止已知恶意站点后，在访问控制策略中便无需考虑这些站点。思科提供定期更新的已知恶意地址和URL源，可使安全智能阻止列表实现动态更新。使用智能源，无需通过编辑策略来添加或删除阻止列表中的项目。请参阅配置安全智能，第 459 页。
- **NAT**（网络地址转换）- 使用 NAT 策略将内部 IP 地址转换为外部可路由地址。请参阅配置 NAT，第 537 页。
- **访问控制 (Access Control)** - 使用访问控制策略确定网络上允许的连接。您可以按安全区域、IP 地址、协议、端口、应用、URL、用户或用户组进行过滤。您还可以使用访问控制规则来应用入侵策略和文件（恶意软件）策略。使用此策略实施 URL 过滤。请参阅配置访问控制策略，第 478 页。
- **入侵 (Intrusion)** - 使用入侵策略检测已知威胁。即使使用访问控制规则应用入侵策略，也仍可以编辑入侵策略，以选择性地启用或禁用特定的入侵规则。请参阅入侵策略，第 497 页。

步骤 3 点击菜单中的**部署**按钮以部署更改。

只有将更改部署至设备，更改才会生效。请参阅部署更改，第 31 页。

搜索规则或对象

您可以在策略规则或对象列表中使用全文本搜索，帮助您找到要编辑的项目。当策略中包含成百上千条规则或数目繁多的对象时，此功能尤为有用。

在任何类型的策略（除入侵策略外）或对象中搜索规则和对象的方法都是相同的：在**搜索**字段中，输入要查找的字符串，然后按 Enter。

此字符串可以位于规则或对象的任何部分，且可以是部分字符串。您可以使用星号 * 作为通配符，匹配零个或多个字符。请勿输入以下字符，因为搜索字符串不支持这些字符：?~!{}<>:%。以下字符将被忽略：;#&。

字符串可以出现在组中的对象内。例如，可以输入 IP 地址并找到具体指定该地址的网络对象或组。

完成后，点击搜索框右侧的 **x** 清空过滤器。

部署更改

在更新策略或设置时，更改不会立即应用到设备中。更改配置的过程分为两步：

1. 进行更改。
2. 部署更改。

通过此过程，您可以执行一组相关的更改，而不必在进行“部分配置”的情况下运行设备。在大多数情况下，仅会部署您做出的更改。但是，如有必要，系统将重新应用整个配置，这可能会造成您的网络中断。此外，有些更改需要重新启动检测引擎，在重启过程中会丢弃流量。因此，当系统中断带来的影响很小时，可以考虑部署更改。

注释 如果部署作业失败，则系统必须回滚对先前配置的任何部分更改。回滚进程包括清除数据平面配置和重新部署以前的版本。这将中断流量，直至回滚进程完成。

完成要进行的更改后，请按照以下程序将它们部署到设备中。

注意 如果检测引擎由于软件资源问题而处于繁忙状态，或由于某个配置要求引擎在配置部署期间重新启动而出现故障，威胁防御设备将丢弃流量。有关需要重新启动的更改的详细信息，请参阅引发检测引擎重启的配置更改，第 32 页。

过程

步骤 1 点击网页右上角的**部署更改 (Deploy Changes)** 图标。

若有未部署的更改，系统会用圆点高亮显示。

“待处理更改”窗口显示配置的部署版本与待处理更改之间的对比信息。这些更改进行了颜色编码，表示出删除、添加或编辑的元素。有关每种颜色的解释，请参阅窗口中的说明。

如果部署要求重新启动检测引擎，则该页面包含一条消息，其中提供要求重新启动的更改的详细信息。如果此时无法接受瞬时流量丢失，请关闭该对话框，等待更好的更改部署时机。

如果图标未高亮显示，仍可以点击图标查看上一个成功部署作业的日期和时间。窗口中还包含显示部署历史记录的链接，点击此链接可访问已经过过滤仅显示部署作业的审核页面。

步骤 2 如果您对所做的更改比较满意，可以点击**立即部署 (Deploy Now)** 立即启动作业。

窗口将显示部署正在进行。您可以关闭窗口，或等待部署完成。如果您在部署过程中关闭窗口，作业不会停止。您可以在任务列表或审核日志中查看结果。如果将窗口保持打开状态，请点击**部署历史记录 (Deployment History)** 链接查看结果。

或者，您现在可以执行以下操作：

- **为作业命名 (Name the Job)** - 要对部署作业命名，请点击**立即部署 (Deploy Now)** 按钮上的下拉箭头，然后选择**为部署作业命名 (Name the Deployment Job)**。输入一个名称，然后点击**部署 (Deploy)**。名称将会连同作业一块显示在审核和部署历史记录中，更便于您查找作业。

  例如，如果将作业命名为“DMZ Interface Configuration”，成功的部署将被命名为“Deployment Completed: DMZ Interface Configuration”。此外，在与部署作业相关的“任务已开始”和“任务已结束”事件中，作业名称将用作事件名称。

- **强制完整部署 (Force a full deployment)** - 如果遇到问题并希望强制系统部署完整配置，而不仅仅是更改，可以点击 **立即部署 (Deploy Now)** 按钮上的下拉箭头，然后选择**应用完整部署 (Apply Full Deployment)**。完整部署会导致流量中断，因此您必须确认要执行此操作，然后才能点击**部署 (Deploy)**。

- **放弃更改 (Discard Changes)** - 要放弃所有待处理更改，请依次点击**更多选项 (More Options)** > **全部放弃 (Discard All)**。系统将要求您进行确认。

- **复制更改 (Copy Changes)** - 要将更改列表复制到剪贴板，请依次点击**更多选项 (More Options)** > **复制到剪贴板 (Copy to Clipboard)**。仅当更改不超过 500 项时，选项才可用。

- **下载更改 (Download Changes)** - 要以文件形式下载更改列表，请依次点击**更多选项 (More Options)** > **以文本形式下载 (Download as Text)**。系统将提示将文件保存到工作站。文件采用 YAML 格式。如果您没有专门支持 YAML 格式的编辑器，可以使用文本编辑器查看。

引发检测引擎重启的配置更改

在部署配置更改时，以下任意配置或操作都会重新启动检测引擎。

⚠

注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。另外，部署某些配置需要检测引擎重新启动，这样会中断流量检测并丢弃流量。

部署

部分更改需要重新启动检测引擎，这将导致瞬时流量丢失。以下更改需要重新启动检测引擎：

- 启用或禁用 SSL 解密策略。
- 更改一个或多个物理接口（但不是子接口）上的 MTU。
- 在访问控制规则上添加或删除文件策略。
- VDB 已更新。
- 创建或中断高可用性配置。

此外，如果 Snort 进程繁忙、总 CPU 使用率超过 60%，部署期间可能会丢弃部分数据包。可以使用 **show asp inspect-dp snort** 命令，检查 Snort 当前的 CPU 使用率。

系统数据库更新

如要将更新下载到规则数据库或VDB，则必须部署该更新，使其处于活动状态。此部署可能会重新启动检测引擎。手动下载更新或计划更新时，可以指明下载完成后是否应自动部署更改。如果没有将系统设置为自动部署更新，则系统将在下一次部署更改时应用更新，此时检测引擎可能会重新启动。

系统更新

安装不重新启动系统和包括二进制更改的系统更新或补丁，需要检测引擎重新启动。二进制更改可能包括对检测引擎、预处理器、漏洞数据库 (VDB) 或共享对象规则的更改。另请注意，不包括二进制更改的补丁有时需要 Snort 重新启动。

强制执行完整部署的配置更改

在大多数情况下，仅会部署您做出的更改。但是，如有必要，系统将重新应用整个配置，这可能会造成您的网络中断。以下是强制执行完整部署的一些更改。

- 最初启用安全情报或身份策略。
- 安全情报和身份策略均已禁用。
- 重复使用数据时创建 EtherChannel。
- 删除以太网通道。
- 修改 EtherChannel 的成员接口关联。
- 删除配置中使用的任何接口。例如，删除属于访问控制规则使用的安全区域的子接口。

- 更改属于 FlexConfig 策略的 FlexConfig 对象，或从策略中删除不包含取消行的对象。省略取消行会强制系统执行完全部署，因为没有特定方法可以删除 FlexConfig 对象生成的配置。您可以通过始终在每个 FlexConfig 对象中包含适当的否定行来避免此问题。

查看接口状态和管理状态

“设备摘要”包括设备的图形视图和管理地址的选定设置。要打开“设备摘要”，请点击**设备**。

此图中要素的颜色根据该要素的状态而变化。将鼠标悬停在要素的上方，有时会显示更多信息。使用此图可监控以下项目。

注释 此图的接口部分（包括接口状态信息）也会显示于**接口 (Interfaces)** 页面和**监控 (Monitoring)** > **系统 (System)** 控制面板中。

接口状态

将鼠标悬停在端口上方可查看其 IP 地址、启用状态和链路状态。IP 地址可静态分配，也可以使用 DHCP 获取。将鼠标悬停于网桥虚拟接口 (BVI) 的上方也会显示成员接口列表。

接口端口使用以下颜色代码：

- 绿色 - 接口已配置和启用，链路为运行状态。
- 灰色 - 接口未启用。
- 橙色/红色 - 接口已配置和启用，但链路中断。如果该接口已连接电缆，则此状态表示有错误需要更正。如果该接口未连接电缆，则此状态为预期状态。

内部、外部网络连接

图中指出了在以下条件下连接到外部（或上游）和内部网络的端口。

- 内部网络 - 仅对名为“内部”的接口显示内部网络的端口。如有其他内部网络，则不显示它们。如果未命名任何接口为“内部”，则不会将任何端口标记为内部端口。
- 外部网络 - 仅对名为“外部”的接口显示外部网络的端口。同内部网络一样，此名称是必需的，否则不会将任何端口标记为外部端口。

管理设置状态

图中显示是否为管理地址配置了网关、DNS 服务器、NTP 服务器和智能许可，以及这些设置是否正常运行。

绿色表示该功能已配置且运行正常，灰色表示未配置或无法正常运行。例如，如果无法连接服务器，则 DNS 框显示灰色。将鼠标悬停在各个要素上可查看详细信息。

如果发现问题，请按以下步骤更正它们：

- 管理端口和网关 - 依次选择**系统设置** > **管理接口**。
- DNS 服务器 - 依次选择**系统设置** > **DNS 服务器**。
- NTP 服务器 - 依次选择**系统设置** > **NTP**。另请参阅NTP 故障排除，第 797 页。
- 智能许可证 - 点击“智能许可证”组下的**查看配置**链接。

查看系统任务状态

系统任务包括无需直接参与而进行的各种操作，例如检索和应用各种数据库更新。您可以查看这些任务的列表及其状态，以确认系统任务是否成功完成。

任务列表将显示系统任务和部署作业的综合状态。审核日志位于**设备** > **设备管理** > **审核日志**下方，其中包含更多详细信息。例如，审核日志将任务开始和任务结束显示为单独的事件，而任务列表将这些事件合并为一个条目。此外，部署作业的审核日志条目包括有关已部署变更的详细信息。

过程

步骤 1 点击主菜单中的**任务列表 (Task List)** 按钮。

此时将打开任务列表，其中显示系统任务的状态和详细信息。

步骤 2 评估任务状态。

如果发现持续性的问题，可能需要修复设备配置。例如，如果一直无法获取数据库更新，则可能是设备的管理 IP 地址无法访问互联网造成。对于任务说明中指出的某些问题，您可能需要联系思科技术支持中心 (TAC)。

针对任务列表可以执行以下操作：

- 点击**成功 (Success)** 或**失败 (Failures)** 按钮，可依据这些状态过滤列表。
- 点击任务的删除图标 ()，可将其从列表中移除。
- 点击**删除所有完成的任务 (Remove All Completed Tasks)** 可清空已结束的所有任务的列表。

使用 CLI 控制台监控和测试配置

威胁防御 设备包括一个可用于监控和故障排除的命令行界面 (CLI)。虽然可以打开 SSH 会话访问所有系统命令，但也可以在 设备管理器 中打开 CLI 控制台使用只读命令，例如各种 **show** 命令以及 **ping**、**traceroute** 和 **packet-tracer**。如果具有管理员权限，还可以输入 **failover**、**reboot** 和 **shutdown** 命令。

从一个页面移动到另一个页面时，可以使 CLI 控制台保持打开状态，并配置和部署功能。例如，在部署新的静态路由之后，可以在 CLI 控制台中使用 **ping** 验证是否可以访问目标网络。

CLI 控制台使用基本的 威胁防御 CLI。不能使用 CLI 控制台进入诊断 CLI、专家模式、FXOS CLI（在使用 FXOS 的型号上）。如果需要进入其他 CLI 模式，请使用 SSH。

有关命令的详细信息，请参阅Cisco Firepower Threat Defense 命令参考，https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html。

注：

- 尽管 CLI 控制台支持 **ping**，但不支持 **ping system** 命令。
- 系统最多可以处理 2 个并发命令。因此，如果其他用户发出命令（例如，使用 REST API），您可能需要等待其他命令完成后才能输入命令。如果此问题持续存在，请使用 SSH 会话，而非 CLI 控制台。
- 命令会根据已部署的配置来返回信息。如果在 设备管理器中更改配置而不进行部署，则不会在命令输出中看到所做更改的结果。例如，如果创建一个新静态路由，但不部署该路由，则该路由不会显示在 **show route** 输出中。

过程

步骤 1 点击网页右上角的 **CLI 控制台**图标。

步骤 2 在出现提示时键入命令，然后按 **Enter** 键。

有些命令需要更长时间生成输出，请耐心等待。如果收到命令执行超时的消息，请重试。如果输入需要交互响应的命令（例如 **show perfstats**），也会出现超时错误。如果问题仍然存在，您可能需要使用 SSH 客户端而不是 CLI 控制台。

以下是有关如何使用该窗口的一些提示。

- 按 **Tab** 键，在键入部分命令时系统会自动补全。此外，此时按 Tab 键，系统还会列出命令中可用的参数。Tab 可列出三级关键字。三级之后，需要使用命令参考来获取更多信息。
- 按 Ctrl+C 可以停止命令执行。
- 要移动窗口，请点击并按住标题中的任意位置，然后将窗口拖到所需位置。
- 点击**展开**（  ）或**收起**（  ）按钮放大或缩小窗口。
- 点击**取消停靠，以独立窗口显示**（  ）按钮，将窗口从网页分离出去，在独立的浏览器窗口中显示。要再次停靠，请点击**停靠到主窗口**（  ）按钮。
- 点击并拖动以突出显示文本，然后按 Ctrl+C 将输出复制到剪贴板。
- 点击**清除 CLI**（  ）按钮，清除所有输出。

- 点击**复制最后一个输出**（  ）按钮，将您输入的最后一个命令的输出内容复制到剪贴板上。

步骤 3 完成后，只需关闭控制台窗口即可。请勿使用 **exit** 命令。

尽管用于登录 设备管理器 的凭证可验证您对 CLI 的访问权限，但使用控制台时，实际上从来无需登录 CLI。

同时使用设备管理器和 REST API

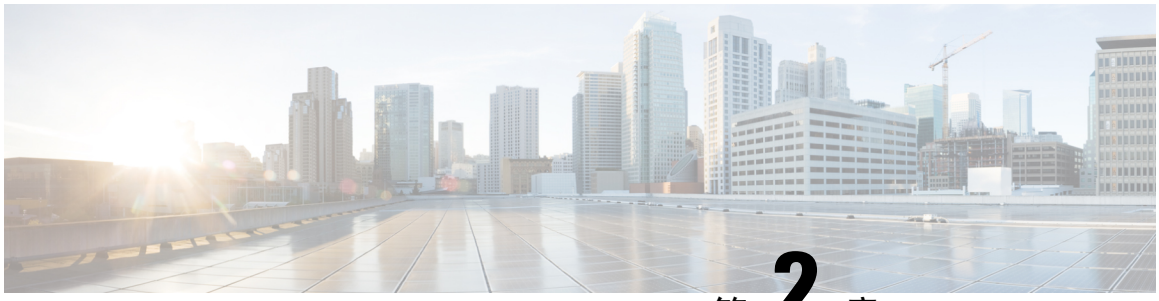
在本地管理模式下设置设备时，您可以使用 设备管理器 和 威胁防御 REST API 配置设备。实际上，设备管理器 使用 REST API 配置设备。

但请注意，REST API 可提供除通过 设备管理器提供的功能之外的其他功能。因此，对于任何给定的功能，您可以使用 REST API 配置通过 设备管理器查看配置时不能显示的设置。

如果配置了在 REST API 中可用、但在 设备管理器中不可用的功能设置，使用 设备管理器更改全局功能（例如远程访问 VPN）时，该设置可能会被撤消。是否保留仅 API 设置可能视情况有所不同，并且在许多情况下，通过 设备管理器 编辑会保留对 设备管理器 中不可用设置的 API 更改。对于任何给定功能，应验证所作更改是否已保留。

一般而言，应避免对任何给定功能同时使用设备管理器和 REST API。相反，配置设备时，应从两者中选择一种方法，逐一配置每项功能。

可以使用 API Explorer 查看和尝试 API 方法。点击“更多选项”按钮 (⋮) 并选择 **API Explorer**。



第 2 章

最佳实践： 威胁防御的使用案例

以下主题介绍了您可能希望使用 设备管理器，通过 威胁防御 完成的一些常见任务。这些使用案例假定您已完成设备配置向导，并保留了此初始配置。即使修改了初始配置，也应该能够使用这些示例了解产品的使用方法。

如何在设备管理器上配置设备

完成设置向导后，您的设备应该会正常工作并应部署了下列基本策略：

- 外部接口和内部接口。其他数据接口则未配置。
- (Firepower 4100/9300) 未预配置任何数据接口。
- (ISA 3000) 网桥组包含 2 个内部接口和 2 个外部接口。要完成设置，需要手动设置 BVI1 IP 地址。
- （除了 Firepower 4100/9300）内部和外部接口的安全区。
- （除了Firepower 4100/9300）信任所有内部到外部流量的访问规则。 对于 ISA 3000，存在允许从内部到外部的所有流量以及从外部到内部的所有流量的访问规则。
- （除了 Firepower 4100/9300 和 ISA 3000） 接口 NAT 规则，用于将所有内部到外部流量转换到外部接口 IP 地址上的唯一端口。
- （除了 Firepower 4100/9300 和 ISA 3000） 在内部接口上运行的 DHCP 服务器。

以下步骤概述了可能需要配置的其他功能。请点击页面上的帮助按钮 (**?**)，获取有关每个步骤的详细信息。

过程

步骤 1 选择**设备**，然后点击**智能许可证**组中的**查看配置**。

对于您想要使用的可选许可证（IPS、恶意软件防御、URL），点击**启用 (Enable)**。如果在安装过程中注册设备，还可启用所需的 RA VPN 许可证。如果不确定是否需要使用某个许可证，请参阅该许可证的说明。

如果尚未注册，可以从该页面执行该操作。点击**注册设备**，并按照说明执行操作。请在评估版许可证到期前进行注册。

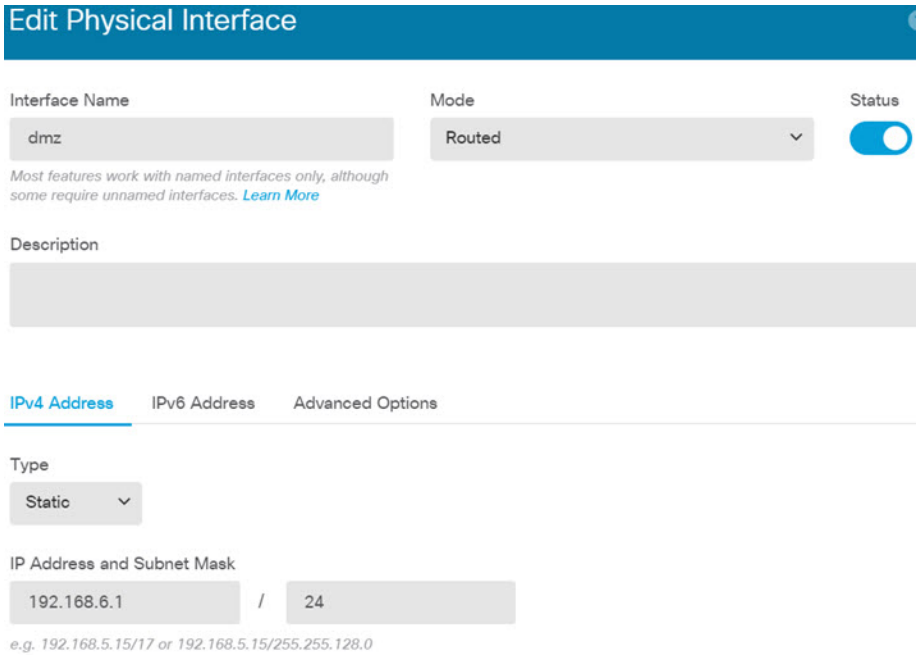
步骤 2 如果连接其他接口，请选择**设备**，然后点击**接口**摘要中的链接，然后点击接口类型以查看接口列表。

- 对于 Firepower 4100/9300，未对任何数据接口进行名称、IP 地址或安全区预配置，因此，您需要启用和配置要使用的任何接口。
- 由于 ISA 3000 预先配置了包含所有数据接口的网桥组，因此无需配置这些接口。但是，必须手动配置 BVI IP 地址。如果要拆分该网桥组，可以对其进行编辑，删除要单独处理的接口。然后，可以将这些接口配置为承载单独的网络。

  对于其他型号，可以为其他接口创建网桥组或配置单独的网络，或同时采用这两种方法。
- 对于 Firepower 1010，除 Ethernet1/1（外部）以外的所有接口均分配给 VLAN1（内部）的访问模式交换机端口。可以将交换机端口更改为防火墙端口；添加新的 VLAN 接口，并为其分配交换机端口；或配置中继模式交换机端口。

点击每个接口的编辑图标 ( )，定义 IP 地址和其他设置。

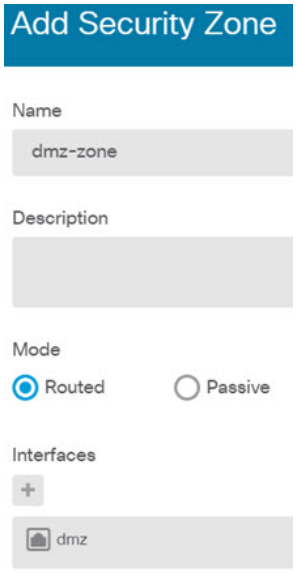
以下示例将一个接口配置为“隔离区”(DMZ)，可以将可公开访问的资产（例如 Web 服务器）放在该区域中。完成后点击**保存 (Save)**。



步骤 3 如果已配置新接口，请选择**对象 (Objects)**，然后从目录中选择**安全区域 (Security Zones)**。

根据需要编辑或创建新区域。每个接口都必须属于一个区域，因为需要根据安全区域而不是接口来配置策略。配置接口时不能将其放在区域中，因此每当创建新接口或更改现有接口的用途之后，都必须编辑区域对象。

以下示例显示如何为 DMZ 接口创建一个新的 DMZ 区域。

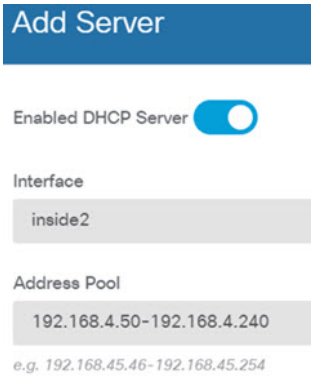


步骤 4 如果希望内部客户端使用DHCP从设备中获取IP地址，请选择**设备**，然后依次选择**系统设置**>**DHCP服务器**。选择 **DHCP 服务器**选项卡。

内部接口已配置了 DHCP 服务器，但可以编辑地址池或甚至将其删除。如果配置了其他内部接口，则在这些接口上设置 DHCP 服务器是非常典型的做法。点击 +，为每个内部接口配置服务器和地址池。

此外，还可以在**配置**选项卡中对为客户端提供的 WINS 和 DNS 列表进行微调。

以下示例显示如何在 inside2 接口（地址池为 192.168.4.50-192.168.4.240）上设置 DHCP 服务器。



步骤 5 选择**设备**，然后点击**路由**组中的**查看配置**，并配置默认路由。

默认路由通常指向位于外部接口之外的上游或 ISP 路由器。默认的 IPv4 路由适用于 any-ipv4 (0.0.0.0/0)，而默认的 IPv6 路由适用于 any-ipv6 (::0/0)。为所使用的每个 IP 版本创建路由。如果使用 DHCP 获取外部接口的地址，则可能已经拥有所需的默认路由。

此页面上定义的路由仅适用于数据接口，而不会影响管理接口。在**系统设置** > **管理接口**上设置管理网关。

以下示例显示 IPv4 的默认路由。在此示例中，isp-gateway 是用于标识 ISP 网关 IP 地址的网络对象（必须从 ISP 中获取地址）。可以通过点击**网关 (Gateway)** 下拉菜单底部的**创建新网络 (Create New Network)**，来创建该对象。

步骤 6 选择**策略 (Policies)**，并为网络配置安全策略。

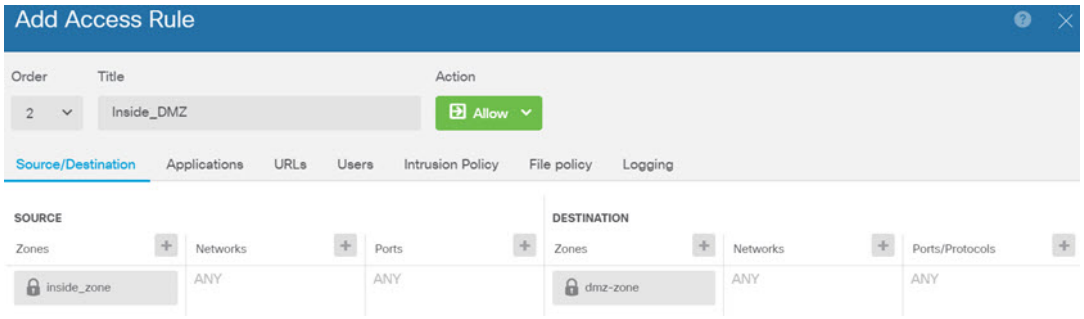
设备安装向导设置允许内部区域与外部区域之间存在流量流动，并对所有接口上流向外部接口的流量启用网络地址转换 (NAT)。即使配置了新接口，如果将其添加到内部区域对象中，访问控制规则也将自动应用于这些接口。

但是，如果有多个内部接口，则需要一条访问控制规则来允许内部区域之间的流量。如要添加其他安全区域，则需要规则来允许这些区域之间的流量。这是您需要进行的最低限度的更改。

此外，您还可配置其他策略以提供附加服务，并对NAT和访问规则进行精细调整，以实现组织需要的结果。您可以配置以下策略：

- **SSL 解密 (SSL Decryption)** - 如果要检查加密连接（例如HTTPS）是否存在入侵、恶意软件等，则必须解密连接。使用 SSL 解密策略确定需要解密的连接。系统检查连接后，会将其重新加密。
- **身份 (Identity)** - 如果要将网络活动与各个用户相关联，或根据用户或用户组成员身份控制网络访问，请使用身份策略确定与给定源 IP 地址关联的用户。
- **安全智能** - 使用安全智能策略快速丢弃进出选定 IP 地址或URL 的连接。阻止已知恶意站点后，在访问控制策略中便无需考虑这些站点。思科提供定期更新的已知恶意地址和URL源，可使安全智能阻止列表实现动态更新。使用智能源，无需通过编辑策略来添加或删除阻止列表中的项目。
- **NAT**（网络地址转换）- 使用 NAT 策略将内部 IP 地址转换为外部可路由地址。
- **访问控制 (Access Control)** - 使用访问控制策略确定网络上允许的连接。您可以按安全区域、IP 地址、协议、端口、应用、URL、用户或用户组进行过滤。您还可以使用访问控制规则来应用入侵策略和文件（恶意软件）策略。使用此策略实施 URL 过滤。
- **入侵 (Intrusion)** - 使用入侵策略检测已知威胁。即使使用访问控制规则应用入侵策略，也仍可以编辑入侵策略，以选择性地启用或禁用特定的入侵规则。

以下示例显示如何在访问控制策略中允许内部区域与 DMZ 区域之间的流量。在此示例中，任何其他选项卡上均未设置任何选项，**日志记录 (Logging)** 除外，其中**在连接结束时 (At End of Connection)** 选项已被选中。



步骤 7 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

如何深入了解您的网络流量

在完成初始设备设置后，您会获得一项访问控制策略，该策略允许所有内部流量访问互联网或其他上游网络，以及一项会阻止所有其他流量的默认操作。在创建其他访问控制规则之前，您可能会发现深入了解网络中实际发生的流量非常有益。

您可以使用 设备管理器 的监控功能来分析网络流量。 设备管理器 报告可帮助您回答以下问题：

- 我的网络的用途是什么？
- 哪些用户使用的网络流量最多？
- 我的用户会访问哪些站点？
- 他们使用的是什么设备？
- 哪些访问控制规则（策略）的使用次数最多？

初始访问规则可提供一些信息帮助您深入了解流量，包括策略、目的和安全区。但要获取用户信息，您需要配置一项要求用户验证自己（身份）的身份策略。要获取网络中所使用应用的信息，您需要进行一些其他调整。

以下步骤程序介绍了如何设置 威胁防御设备以监控流量，并概述了配置和监控策略的端到端流程。

注释 通过此步骤程序无法了解用户所访问站点的网站类别和信誉，因此在URL类别控制面板中看不到有用的信息。只有实施基于类别的 URL 过滤并启用 URL 许可证，才能获取类别和信誉数据。如果只想获取这些信息，可以添加一个新访问控制规则，以允许访问可接受的类别（例如财务），并将其设为访问控制策略的第一个规则。有关实施URL过滤的详细信息，请参阅如何实施可接受使用策略（URL 过滤），第 58 页。

过程

步骤 1 要了解用户行为，您需要配置身份策略以确保可以识别与连接关联的用户。

通过启用身份策略，可以收集有关网络用户以及他们所使用资源的信息。在用户监控控制面板中可获取这些信息。另外，也可以获取事件查看器中所示的连接事件的用户信息。

在本示例中，我们将实施主动身份验证以获取用户身份。使用主动身份验证时，设备将提示用户输入用户名和密码。只有用户使用支持 HTTP 连接的网络浏览器时，才会对他们进行身份验证。

如果用户未通过身份验证，其仍可进行 Web 连接。这仅仅意味着，您不会获取连接的用户身份信息。如果需要，可以创建一项访问控制规则，以丢弃身份验证失败的用户的流量。

a) 在主菜单中点击**策略**，然后点击**身份**。

身份策略最初处于禁用状态。使用主动身份验证时，身份策略使用您的 Active Directory 服务器对用户进行身份验证，并将他们与其使用的工作站的 IP 地址关联。随后，系统会将该 IP 地址的流量标识为该用户的流量。

b) 点击**启用身份策略**。

c) 点击**创建身份规则**按钮或 + 按钮，创建规则以要求进行主动身份验证。

在本示例中，我们假设您要对每个用户都执行身份验证。

d) 为规则输入**名称**，可以是您选择的任何内容，例如 Require_Authentication。

e) 在**源/目标**选项卡上，保留默认设置，此设置应用于任何条件。

您可以根据需要将该策略限制为更具体的流量集。但是，主动身份验证仅适用于 HTTP 流量，因此非 HTTP 流量与源/目标条件匹配并不重要。有关身份策略属性的详细信息，请参阅配置身份规则，第 449 页

f) 对于**操作**，请选择**主动身份验证**。

假设您尚未配置身份策略设置，由于存在一些未定义的设置，系统将打开“身份策略配置”对话框。

g) 配置主动身份验证所需的强制网络门户和 SSL 解密设置。

如果身份规则要求对用户进行主动身份验证，则该用户将被重定向到强制网络门户端口，然后系统会提示他们进行身份验证。强制网络门户需要使用 SSL 解密规则，系统将自动生成这些规则，但您必须选择要用于 SSL 解密规则的证书。

- **服务器证书** - 选择在主动身份验证期间提供给用户的内部证书。您可以选择预定义的自签名 DefaultInternalCertificate，也可以点击**创建新的内部证书**并上传您的浏览器已信任的证书。

  如果用户不上传其浏览器已经信任的证书，则必须接受该证书。

- **重定向到主机名** - 选择定义接口的完全限定主机名的网络对象，该接口应用作主动身份验证请求的强制网络门户。如果该对象尚不存在，请点击**创建新网络**。

  FQDN 必须解析为设备上接口之一的 IP 地址。通过使用 FQDN，您可以为客户端将识别的主动身份验证分配证书，从而避免用户在被重定向到 IP 地址时收到不受信任证书警告。证书可以在证书的使用者备选名称 (SAN) 中指定 FQDN、通配符 FQDN 或多个 FQDN。

  如果身份规则要求对用户进行主动身份验证，但您未指定重定向 FQDN，则用户将被重定向到他们连接的接口上的强制网络门户端口。

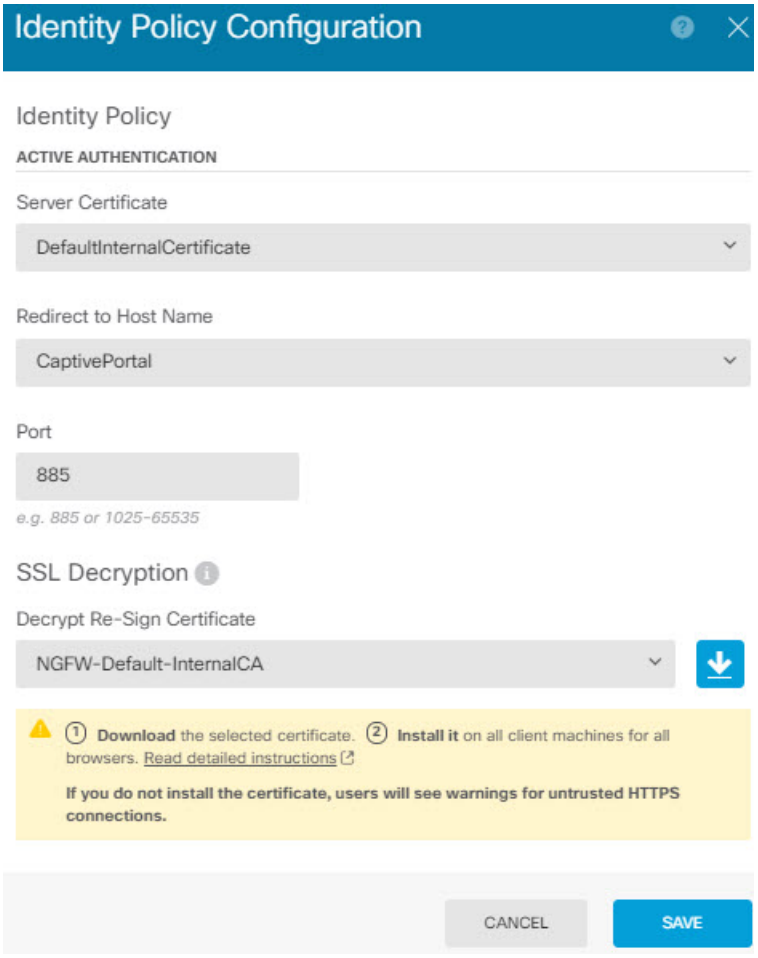
- **端口** - 强制网络门户端口。默认端口是 885 (TCP)。如果配置了其他端口，则该端口必须在 1025-65535 的范围内。

- **解密重签名证书** - 选择内部 CA 证书，以用于使用重签名证书实施解密的规则。您可以使用预定义的 NGFW-Default-InternalCA 证书（默认证书），也可以使用创建或上传的证书。如果尚无证书，请点击**创建内部 CA** 进行创建。（仅当您尚未启用 SSL 解密策略时，系统才会提示您提供解密重签名证书。）

  如果尚未在客户端浏览器中安装证书，请点击下载按钮()获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅为解密重签名规则下载 CA 证书，第 438 页。

示例：

“身份策略配置”对话框现在应如下所示。



h) 点击**保存**以保存主动身份验证设置。

“主动身份验证”选项卡现在显示在“操作”设置下方。

i) 在**主动身份验证**选项卡上，选择 **HTTP 协商**。

此选项允许浏览器和目录服务器按顺序协商最安全的身份验证协议，先是NTLM，然后是HTTP基本验证。

注释 如果您不提供**重定向到主机名** FQDN，HTTP Basic、HTTP 响应页面和 NTLM 身份验证方法会使用接口的 IP 地址将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 *firewall-hostname.AD-domain-name* 进行重定向。如果您想在不提供**重定向到主机名** FQDN 的情况下使用 HTTP 协商，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。建议您始终提供**重定向到主机名** FQDN 以确保行为一致，而无论采用哪种身份验证方法。 如果无法或不想更新 DNS 服务器，请选择其他某种身份验证方法。

j) 对于 **AD 身份源**，请点击**创建新身份领域**。

如果您已创建领域服务器对象，只需选中它并跳过配置服务器的步骤。

填写以下字段，然后点击**确定 (OK)**。

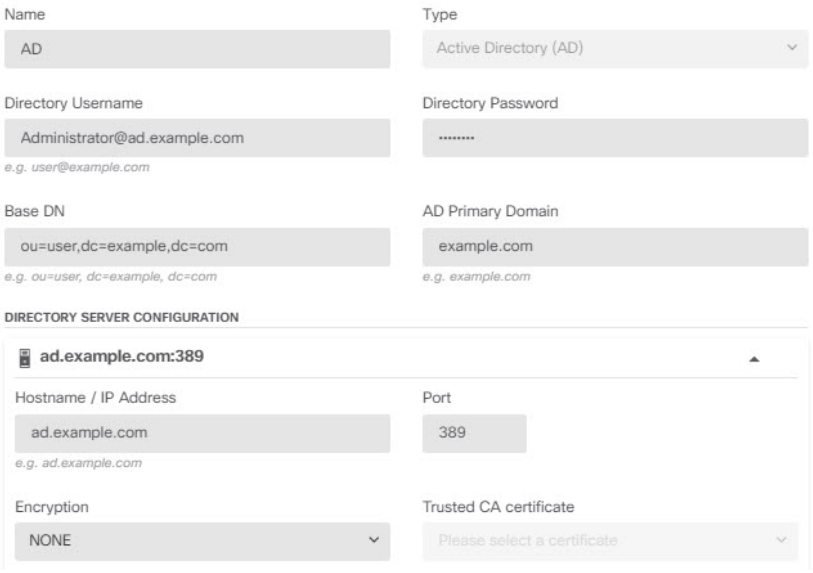
- **名称** - 目录领域的名称。
- **类型** - 目录服务器的类型。Active Directory 是唯一支持的类型，所以无法更改此字段。
- **目录用户名、目录密码** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

  注释 系统使用此信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=adminisntrator、cn=users、dc=example、dc=com。请注意，cn＝users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

- **基准 DN** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如 dc=example,dc=com。有关查找基准 DN 的信息，请参阅确定目录基准标识名，第 154 页。
- **AD 主域** - 设备应加入的 Active Directory 完全限定域名。例如 example.com。
- **主机名/IP 地址** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。
- **端口** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。
- **加密** - 要使用加密连接下载用户和组信息，请选择所需的方法 **STARTTLS** 或 **LDAPS**。系统默认为**无**，也就是说以明文形式下载用户和组信息。
  - **STARTTLS** 将会协商加密方法，并使用目录服务器支持的最强方法。使用端口 389。如果将领域用于远程访问 VPN，则不支持此选项。
  - **LDAPS** 需要基于 SSL 的 LDAP。使用端口 636。
- **受信任的 CA 证书** - 如果选择加密方法，请上传证书颁发机构 (CA) 证书以便在系统和目录服务器之间启用受信任的连接。如果要使用证书进行身份验证，则证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。

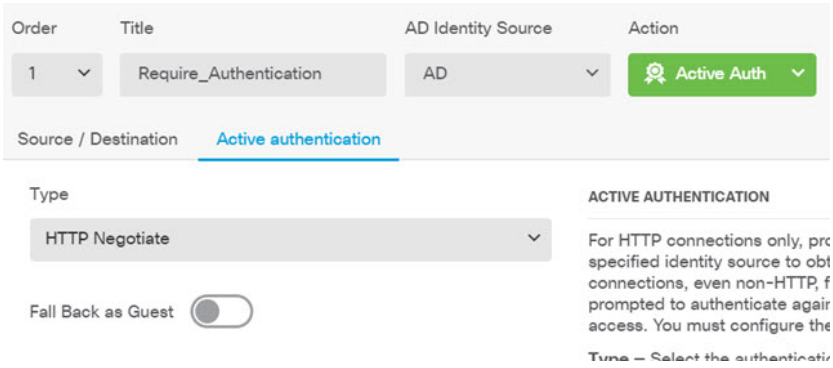
示例：

例如，下图显示了如何为 ad.example.com 服务器创建未加密的连接。主域为 example.com，目录用户名为 Administrator@ad.example.com。所有用户和组信息均位于标识名 (DN) ou=user,dc=example,dc=com 的下方。



k) 对于 **AD 身份源**，请选择您刚刚创建的对象。

规则应类似于以下内容：



l) 点击**确定**以添加规则。

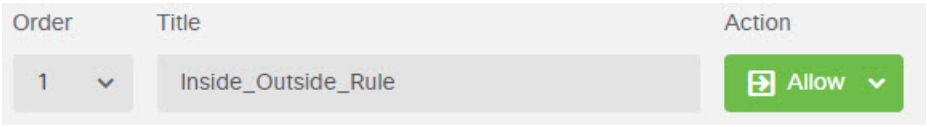
如果查看窗口的右上角，可以看到**部署**图标现在带有一个圆点，表示存在未部署的更改。在用户界面进行更改还不足以获取在设备上配置的更改，还必须部署更改。因此，您可以执行一组相关更改，然后再部署它们，这样就不会出现仅在设备上配置了部分更改的情况。部署更改在此程序的后面步骤执行。

步骤 2 将 Inside_Outside_Rule 访问控制规则上的操作更改为**允许**。

Inside_Outside_Rule访问规则创建为信任规则。但由于不检测受信任的流量，所以在流量匹配条件不含除区域、IP 地址和端口之外的应用或其他条件时，系统无法了解受信任流量（例如应用）的某些特征。如果将该规则更改为允许非受信任的流量，系统会全面检测流量。

注释 （ ISA 3000。）还要考虑将 Outside_Inside_Rule、Inside_Inside_Rule 和 Outside_Outside_Rule 从“信任”更改为“允许”。

a) 点击**策略 (Policies)**页面上的**访问控制 (Access Control)**。
b) 将鼠标悬停在Inside_Outside_Rule行右侧的**操作**单元格上将显示编辑和删除图标，然后点击编辑图标 ( ) 以打开该规则。
c) 在**操作**下选择**允许**。

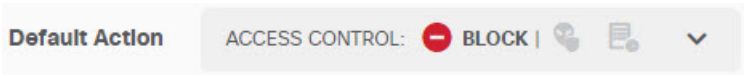


d) 点击**确定**以保存更改。

步骤 3 基于访问控制策略默认操作启用日志记录。

控制面板仅包含与启用连接日志记录的访问控制规则匹配的连接的信息。Inside_Outside_Rule规则启用日志记录，但默认操作为禁用日志记录。因此，控制面板仅显示 Inside_Outside_Rule 的信息，而不反映与任何规则皆不匹配的连接。

a) 点击访问控制策略页面底部默认操作的任意位置。

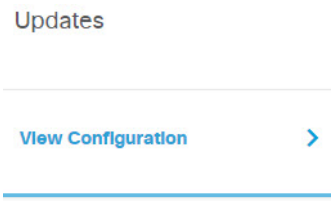


b) 选择**选择日志操作 > 连接开始和结束时**。
c) 点击**确定 (OK)**。

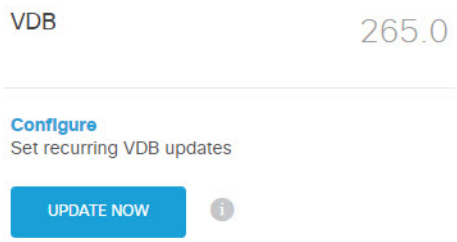
步骤 4 设置漏洞数据库 (VDB) 的更新计划。

思科会定期发布 VDB 更新，其中包括可识别连接中所用应用的应用检测器。您应定期更新 VDB。您可以手动下载更新，也可以设置定期更新计划。以下步骤程序介绍了如何设置计划。默认情况下，VDB 更新处于禁用状态，所以您需要采取措施来获取 VDB 更新。

a) 点击**设备**。
b) 点击“更新”组中的**查看配置**。



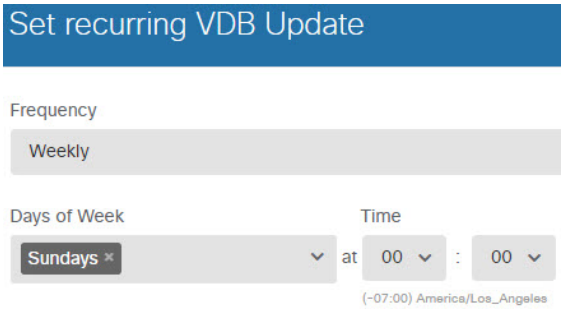
c) 点击 VDB 组中的**配置**。



d) 定义更新计划。

选择不会影响网络的时间和频率。另外，请注意系统在下载更新后会自动执行部署。激活新的检测器需要执行此操作。因此，也会部署您已进行和保存，但尚未部署的任何配置更改。

例如，以下计划会在每周星期日上午 12:00（使用 24 小时制表示法）更新一次 VDB。



e) 点击**保存 (Save)**。

步骤 5 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

这时，监控控制面板和事件应开始显示用户和应用的相关信息。您可以评估这些信息是否存在不需要的模式，并制定新的访问规则来限制不可接受的用途。

如果要开始收集入侵和恶意软件的相关信息，您需要针对一个或多个访问规则启用入侵和文件策略。另外，您还需要对这些功能启用许可证。

如果要开始收集 URL 类别的相关信息，则必须实施 URL 过滤。

如何阻止威胁

通过将入侵策略添加到访问控制规则中，可以实施下一代入侵防御系统(IPS)过滤。入侵策略可分析网络流量，根据已知威胁比较流量内容。如果某个连接与您正在监控的威胁匹配，系统将丢弃该连接，从而阻止攻击。

处理所有其他流量后，才会检验网络流量中是否存在入侵。通过将入侵策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略检测流量。

您只能对**允许**流量的规则配置入侵策略。对于设置为**信任**或**阻止**流量的规则，系统不会执行检测。另外，如果默认操作是**允许**，您可以将入侵策略配置为默认操作的一部分。

这些入侵策略由 思科 Talos 情报小组 (Talos) 设计，其设定了入侵和预处理器规则的状态和高级设置。 如果您使用 Snort 3 作为检测引擎，则可以根据 Talos 策略创建自己的自定义策略。

除了检查允许的流量是否存在潜在入侵之外，您还可以使用安全智能策略来预先阻止所有传送至或来自已知不良 IP 地址，或传送至已知不良 URL 的流量。

过程

步骤 1 如果尚未启用，请启用IPS 许可证。

必须启用IPS许可证，才能使用入侵策略和安全智能。如果您当前使用的是评估许可证，将启用该许可证的评估版本。如果已注册设备，则必须购买所需的许可证，并将其添加到您在 Cisco.com 的智能软件管理器账户。

a) 点击**设备**。
b) 点击“智能许可证”组中的**查看配置**。

c) 点击**IPS** 组中的**启用 (Enable)**。

系统会将该许可证注册到您的账户，或激活相应的评估许可证。该组应指示许可证已启用，且按钮将改为显示“禁用”。

步骤 2 针对一个或多个访问规则选择入侵策略。

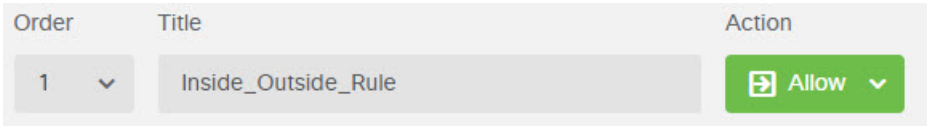
确定哪些规则包括应该扫描威胁的流量。在本示例中，我们会将入侵检测添加到Inside_Outside_Rule中。

a) 在主菜单中点击**策略**。

确保系统显示**访问控制**策略。

b) 将鼠标悬停在Inside_Outside_Rule行右侧的**操作**单元格上将显示编辑和删除图标，然后点击编辑图标 ( ) 以打开该规则。

c) 如果尚未针对**操作**选择**允许**，请进行此选择。

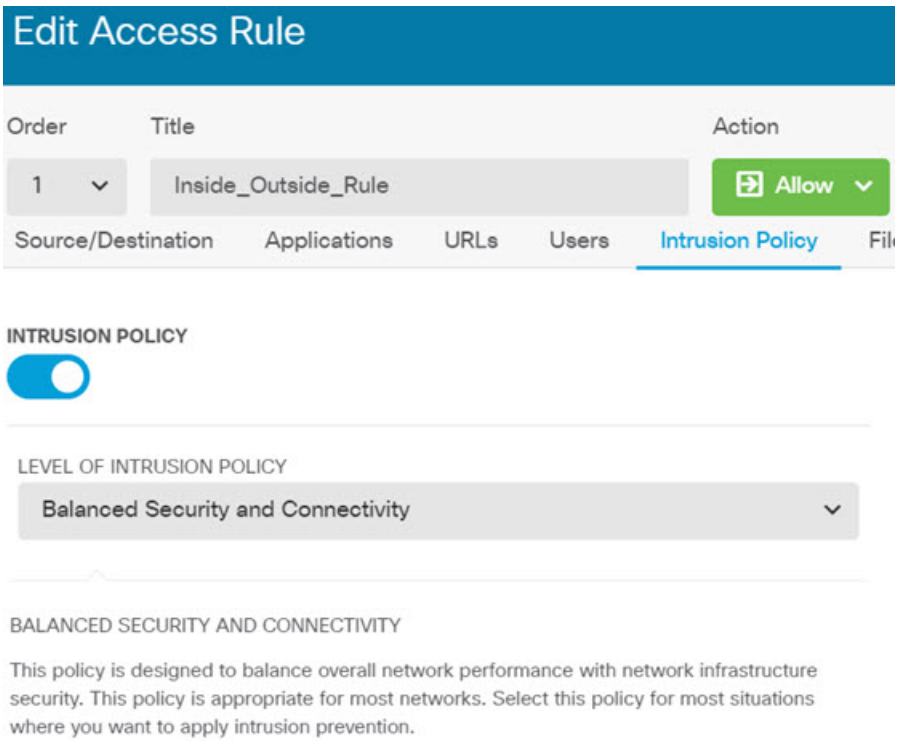


d) 点击**入侵策略**选项卡。

e) 点击**入侵策略**开关启用该选项，然后选择入侵策略。

对于大多数网络，合适的策略是**平衡安全和连接**策略。它提供良好的入侵防御，而不会过度激进，有可能会丢弃可能不想被丢弃的流量。如果您确定要丢弃很多流量，可以选择**连接优先于安全**以放宽策略。

如果您需要积极关注安全性，请尝试**安全优先于连接**策略。**最大检测**策略更加重视网络基础设施的安全性，有可能对操作造成更大的影响。



f) 点击**确定**以保存更改。

步骤 3 （可选。）转到**策略** > **入侵**，点击齿轮图标，然后为入侵策略配置系统日志服务器。

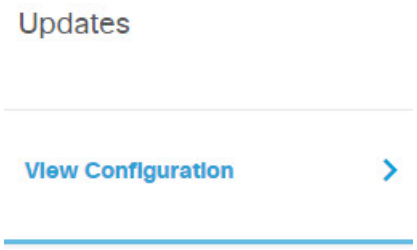
入侵事件不使用为访问控制规则配置的系统日志服务器。

步骤 4 设置入侵规则数据库的更新计划。

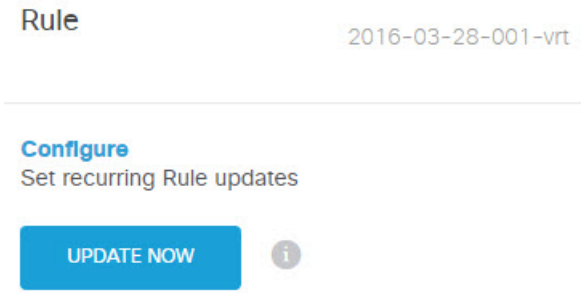
思科会定期发布入侵规则数据库更新，入侵策略使用入侵规则数据库来确定是否应丢弃连接。您应定期更新规则数据库。您可以手动下载更新，也可以设置定期更新计划。以下步骤程序介绍了如何设置计划。默认情况下，数据库更新处于禁用状态，所以您需要采取措施来获取更新的规则。

a) 点击**设备**。

b) 点击“更新”组中的**查看配置**。



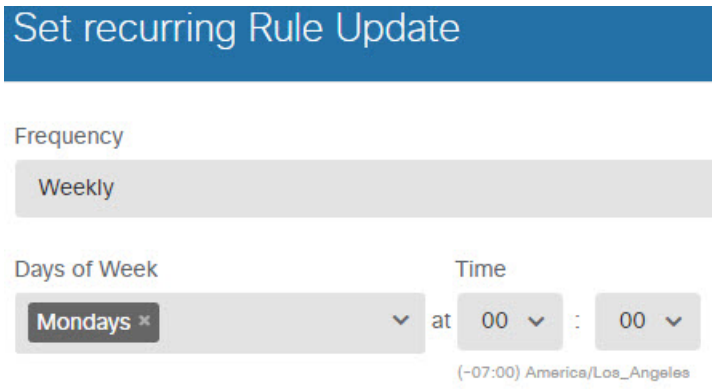
c) 点击“规则”组中的**配置**。



d) 定义更新计划。

选择不会影响网络的时间和频率。另外，请注意系统在下载更新后会自动执行部署。激活新规则需要执行此操作。因此，也会部署您已进行和保存，但尚未部署的任何配置更改。

例如，以下计划会在每周星期一上午 12:00（使用 24 小时制表示法）更新一次规则数据库。



e) 点击**保存 (Save)**。

步骤 5 配置安全智能策略预先丢弃主机和站点已知不良的连接。

通过使用安全智能阻止连接属于已知威胁的主机或站点，为系统节省执行深度数据包检测，以识别每个连接中的威胁所需的时间。安全智能可提早阻止不必要的流量，为系统留出更多的时间来处理您真正关心的流量。

a) 点击**设备**，然后点击**更新**组中的**查看配置**。
b) 点击安全智能源组中的**立即更新**。
c) 此外，点击**配置**为源设置定期更新。默认情况下，**每小时**适合大多数网络，但如有必要，可以降低频率。
d) 点击**策略**，然后点击**安全智能**策略。
e) 点击**启用安全智能**（如果尚未启用该策略）。
f) 在**网络**选项卡上，点击阻止/丢弃列表下的**+**，并选择**网络源**选项卡上的所有源。您可以点击源旁边的 **i** 按钮，阅读每个源的说明。

   如果您看到指出尚不存在任何源的消息，请稍后重试。源下载尚未完成。如果此问题仍然存在，请确保管理 IP 地址和互联网之间存在路径。

g) 点击**确定**添加选定的源。

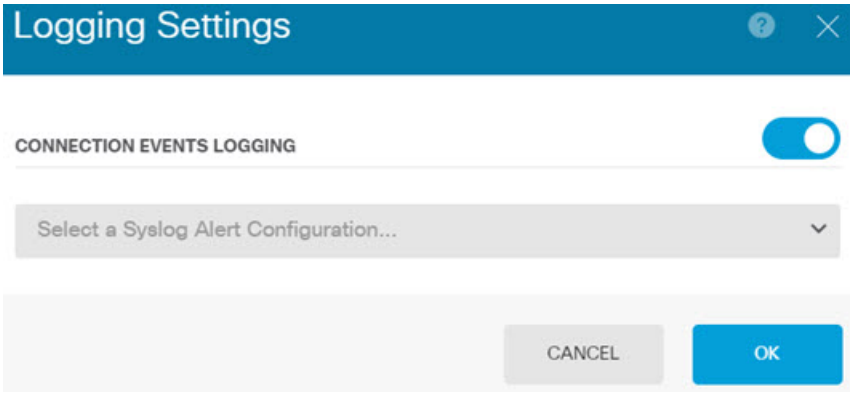
   如果您知道存在其他不良 IP 地址，可以依次点击 **+** > **网络对象**，添加包含这些地址的对象。您可以点击列表底部的**创建新网络对象**立即添加这些对象。

h) 点击 **URL** 选项卡，然后依次点击阻止/丢弃列表中的 **+** > **URL 源**，选择所有 URL 源。点击**确定**以将其添加到列表中。

   与网络列表类似，您可以将自己的URL对象添加到该列表中，以阻止源中不存在的其他站点。依次点击 **+** > **URL 对象**。您可以通过点击列表末尾的**创建新 URL 对象**添加新对象。

i) 点击齿轮图标，并启用**连接事件日志记录**，以便策略能够为匹配的连接生成安全智能事件。点击**确定**，保存更改。

   如果您不启用连接日志记录，您将没有数据来评估策略的表现是否达到预期。如果定义了外部系统日志服务器，现在即可选择此服务器，以便将事件同时发送到该服务器上。



j) 根据需要，您可以在每个选项卡的**不阻止**列表中添加网络或 URL 对象，创建阻止列表例外。

   不阻止列表不是真正的“允许”列表。它们是例外列表。如果例外列表中的地址或 URL 也出现在阻止列表中，系统允许该地址或 URL 的连接传递到访问控制策略。通过这种方式，您可以阻止源，但如果您后期发现所需的地址或站点被阻止，可以使用例外列表来覆盖阻止，而不

需要彻底删除源。注意，这些连接随后由访问控制和入侵策略（如果已配置）评估。因此，如果任何连接包含威胁，这些连接将在入侵检查过程中被识别和阻止。

使用“访问和 SI 规则”控制面板和事件查看器中的“安全智能”视图，判断哪些流量实际上被策略丢弃，以及您是否需要在**不阻止**列表中添加地址或 URL。

步骤 6 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

如果已识别任何入侵，这时监控控制面板和事件应开始显示攻击者、目标和威胁的相关信息。您可以评估这些信息来确定，您的网络是否需要更多安全预防措施，或是否需要降低使用的入侵策略级别。

对于安全智能，您可以在“访问和SI规则”控制面板上查看策略使用情况。您还可以在事件查看器中查看安全智能事件。安全智能数据块不反映在入侵威胁信息中，因为流量在可检测之前已被阻止。

如何阻止恶意软件

用户不断面临着经由互联网站点或其他通信方法（例如邮件）而感染恶意软件的风险。即使受信任的网站，也可能遭受劫持，让信任该网站的用户遭受恶意软件的肆意攻击。网页可能包含来自不同来源的对象。这些对象可能包含图像、可执行文件、JavaScript、广告等等。受感染的网站通常会植入外部源中托管的对象。真正的安全性意味着，逐个查看每个对象，而不只是初始请求。

使用文件策略检测使用恶意软件防御的恶意软件。另外，您还可以使用文件策略执行文件控制，以允许控制特定类型的所有文件，而不考虑文件中是否包含恶意软件。

恶意软件防御使用Cisco Secure Malware Analytics 云为网络流量中检测到的恶意软件检索处置。管理接口必须可连接互联网，以便访问 Cisco Secure Malware Analytics 云 并搜索恶意软件。当设备检测到符合条件的文件时，它将使用该文件的 SHA-256 散列值来查询 Cisco Secure Malware Analytics 云中是否存在该文件的处置。可能的处置可以是**正常**、**恶意软件**或**未知**（没有明确判定）。如果无法连接 Cisco Secure Malware Analytics 云，则处置为**未知**。

通过将文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要检测连接中的任何文件。

您只能对**允许**流量的规则配置文件策略。对于设置为**信任**或**阻止**流量的规则，系统不会执行检测。

过程

步骤 1 如果尚未启用，请启用恶意软件防御和IPS 许可证。

除入侵策略所需的IPS许可证之外，您还必须启用恶意软件防御许可证才能使用文件策略。如果您当前使用的是评估许可证，将启用该许可证的评估版本。如果已注册设备，则必须购买所需的许可证，并将它们添加到您在 Cisco.com 的智能软件管理器账户。

a) 点击**设备**。
b) 点击“智能许可证”组中的**查看配置**。

c) 如果尚未启用，请在**恶意软件防御**组中点击**启用 (Enable)**，如果已经启用，则在**IPS** 组中点击。

系统会将该许可证注册到您的账户，或激活相应的评估许可证。该组应指示许可证已启用，且按钮将改为显示“禁用”。

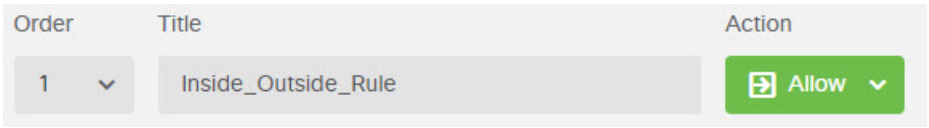
步骤 2 针对一个或多个访问规则选择文件策略。

确定哪些规则包括应该扫描恶意软件的流量。在本示例中，我们会将文件检测添加到 Inside_Outside_Rule 中。

a) 在主菜单中点击**策略**。

确保系统显示**访问控制**策略。

b) 将鼠标悬停在 Inside_Outside_Rule 行右侧的**操作**单元格上将显示编辑和删除图标，然后点击编辑图标 ( ) 以打开该规则。
c) 如果尚未针对**操作**选择**允许**，请进行此选择。

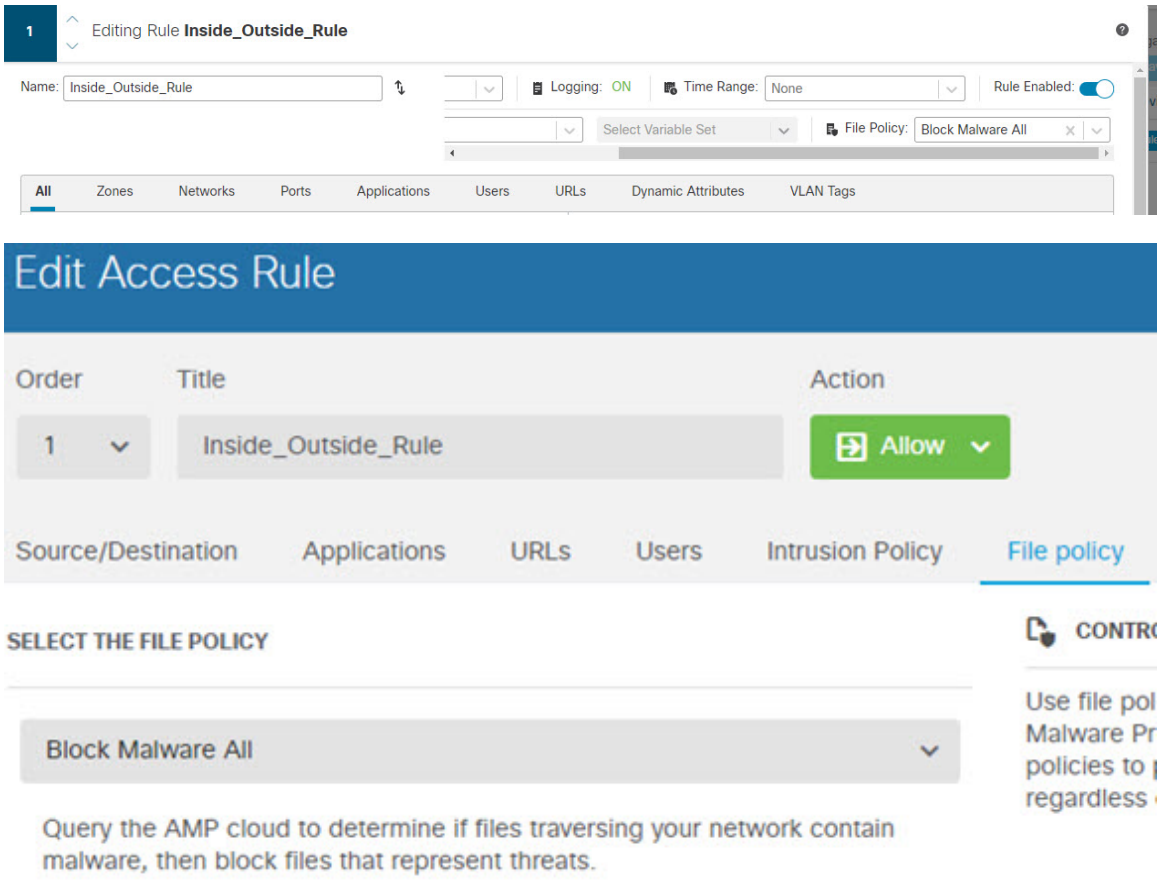


d) 点击**文件策略**选项卡。
e) 点击要使用的文件策略。

您的主要选择为**阻止所有恶意软件**或**全部执行云查找**，前者将丢弃被视为恶意软件的任何文件，后者将查询 Cisco Secure Malware Analytics 云 以确定文件处置，但不执行阻止。如果您想先查看文件评估的方式，请使用云查找。如果对文件的评估方式感到满意，稍后可以切换到阻止策略。

使用其他策略也可以阻止恶意软件。这些策略搭配文件控制，可阻止上传 Microsoft Office（或 Office）和PDF 文档。也就是说，除了阻止恶意软件，这些策略还可阻止用户向其他网络发送这些类型的文件。如果它们符合您的需求，您可以选择这些策略。

对于本示例，请选择**阻止所有恶意软件**。



f) 点击**日志记录**选项卡，并确认是否已选中“文件事件”下的**日志文件**。

默认情况下，无论何时选择文件策略，文件日志记录均已启用。只有启用文件日志记录，才能获得事件和控制面板中的文件和恶意软件信息。

g) 点击**确定**以保存更改。

步骤 3 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

如果已传输任何文件或恶意软件，这时监控控制面板和事件应开始显示文件类型、文件和恶意软件的相关信息。您可以评估这些信息，以确定您的网络在文件传输方面是否需要更多安全预防措施。

如何实施可接受使用策略（URL 过滤）

您的网络可能设有可接受使用策略。可接受使用策略可区分适合您所在组织的网络活动和认为不合适的活动。这些策略通常专注于互联网使用情况，旨在保持工作效率，避免法律责任（例如，维护非敌对工作空间）以及总体控制 Web 网络流量。

您可以使用URL过滤来定义访问策略的可接受使用策略。您可以基于各种类别（例如赌博）过滤，这样就无需识别应阻止的每个单独的网站。对于类别匹配，您还可以指定要允许或阻止的站点的相对信誉。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止。

使用类别和信誉数据还会简化策略创建和管理。此方法可保证系统将按预期控制网络流量。最后，由于思科的威胁智能会不断更新有关新 URL 以及现有 URL 的新类别和新风险的信息，因此可以确保系统使用最新信息来过滤所请求的 URL。代表安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的恶意站点出现和消失的速度可能比您更新和部署新策略的速度要快。

以下程序介绍了如何使用URL过滤实施可接受使用策略。在本例中，我们将阻止某些类别的任何信誉的站点、存在风险的社交网站和未分类站点 badsite.example.com。

过程

步骤 1 如果尚未执行此操作，请启用 **URL** 许可证。

只有启用 URL 许可证，才能使用 URL 类别和信誉信息，或查看控制面板和事件中的信息。如果您当前使用的是评估许可证，将启用该许可证的评估版本。如果已注册设备，则必须购买所需的许可证，并将其添加到您在 Cisco.com 的智能软件管理器账户。

a) 点击**设备**。

b) 点击“智能许可证”组中的**查看配置**。

c) 点击 **URL** 组中的**启用 (Enable)**。

系统会将该许可证注册到您的账户，或激活相应的评估许可证。该组应指示许可证已启用，且按钮将改为显示“禁用”。

步骤 2 创建 URL 过滤访问控制规则。

您可能想要先查看用户访问的站点的类别，再实施阻止规则。对于这种情况，您可以创建一项规则，对可接受的类别（例如财务）执行“允许”操作。由于必须检测所有网络连接来确定URL是否属于此类别，所以即便是非财务站点，您也会收到相关的类别信息。

但是，可能存在您已知要阻止的URL类别。阻止策略还会强制执行检测，所以您会获得非阻止类别连接的类别信息，而不只是受阻止的类别。

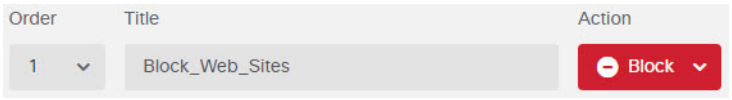
a) 在主菜单中点击**策略**。

确保系统显示**访问控制**策略。

b) 点击 + 可添加新规则。

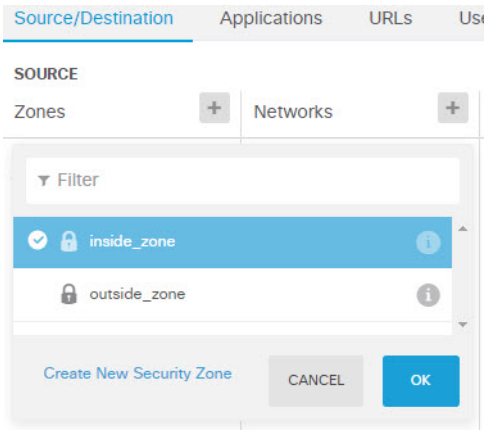
c) 配置顺序、标题和操作。

- **顺序**-默认将新规则添加到访问控制策略的末尾。但是，您必须将此规则放在符合相同源/目的及其他条件的任何规则之前（上方），否则该规则将无法获得匹配（一个连接仅匹配一条规则，即该规则是连接在表中匹配的第一条规则）。对于该规则，我们将使用与初始设备配置期间创建的Inside_Outside_Rule相同的源/目的。您可能也已经创建了其他规则。为了最大限度地提高访问控制效率，最好是尽早设置特定规则，以确保快速决定允许还是丢弃某个连接。对于此示例，请选择 **1** 作为规则顺序。
- **标题** - 为该规则指定一个有意义的名称，例如 Block_Web_Sites。
- **操作** - 选择**阻止**。

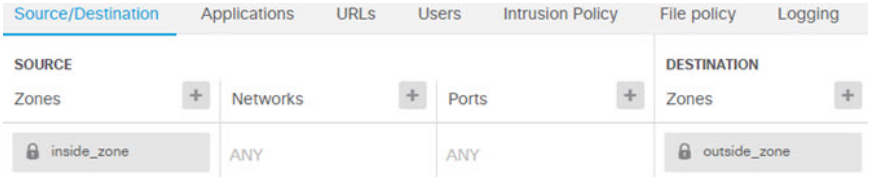


d) 在**源/目的 (Source/Destination)** 选项卡上，点击 + 以打开**源 (Source)** > **区域 (Zones)**，然后选择 **inside_zone**，再在区域对话框中点击**确定 (OK)**。

添加任何条件的方式与此相同。点击+打开一个小对话框，从中点击您要添加的项目。可以点击多个项目，点击已选项目将取消选择该项目（选中标记表示所选项目）。选择项目后，点击**确定**按钮才能将它们添加到策略中，只是选中项目并不能将项目添加到策略中。



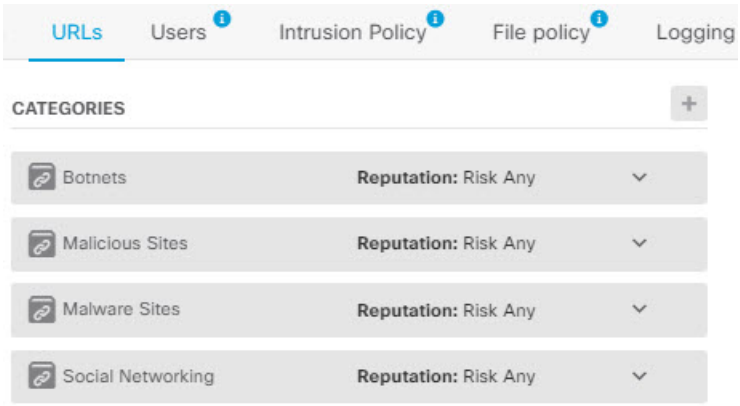
e) 按照相同的方法，为**目的** > **区域**选择 **outside_zone**。



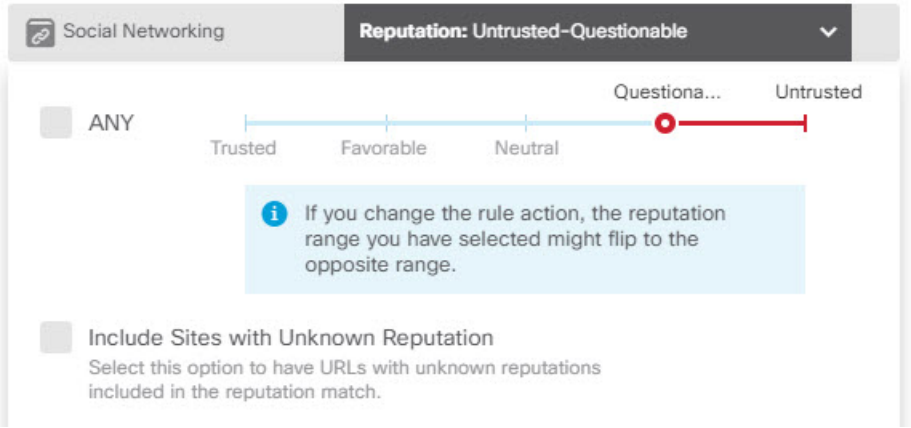
f) 点击 **URL** 选项卡。

g) 点击**类别**的 **+**，然后选择要完全或部分阻止的类别。

在本示例中，请选择僵尸网络、恶意网站、恶意软件站点和社交网络。您可能还希望阻止其他类别。如果您知道要阻止的站点，但不确定类别，请在**待检查 URL** 字段输入 URL，然后点击**前往**。您将转至显示查询结果的网站。



h) 要对“社交网络”类别按信誉敏感性实施阻止，请点击该类别的**信誉：任何风险**，取消选择**任何**，然后将滑块移到**可疑**。点击远离滑块的位置将其关闭。



信誉滑块的左侧指示要允许的站点，右侧是要阻止的站点。在这种情况下，只会阻止信誉属于“可疑”和“不受信任”范围的社交网站。因此，您的用户应该能够访问风险较低的常用社交网站。

选择**包含信誉未知的站点**选项，可使具有未知信誉的 URL 包括在信誉匹配项中。新站点通常未评级，并且站点的信誉可能会由于其他原因而未知或无法确定。

使用信誉，您可以选择性地阻止要允许的某个类别内的某些站点。

i) 点击类别列表左侧 **URL** 列表旁边的 **+**。

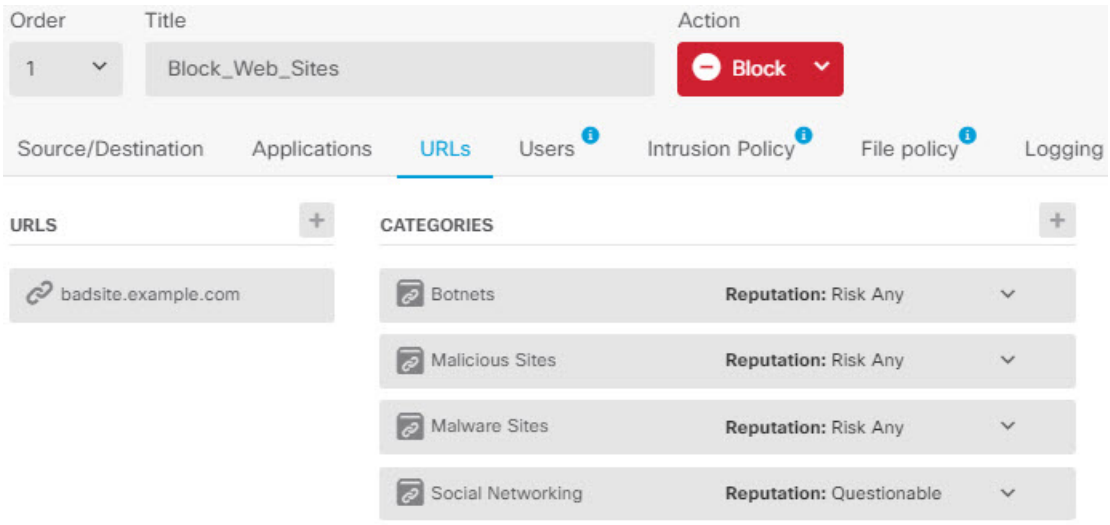
j) 在弹出对话框的底部，点击**创建新 URL** 链接。

k) 对于名称和 URL，请输入 **badsite.example.com**，然后点击**确定**以创建对象。

您可以为该对象指定与 URL 相同的名称，也可以为其指定不同的名称。对于 URL，请勿包含 URL 的协议部分，只添加服务器名称。

l) 选择该新对象，然后点击**确定 (OK)**。

在编辑策略时添加该新对象，即可方便地将该对象添加到列表中。新对象不会自动选中。



m) 点击**日志记录**选项卡，然后依次选择**选择日志操作** > **连接开始和结束时**。

只有启用日志记录才能将类别和信誉信息记入 Web 类别控制面板和连接事件。

n) 点击**确定**以保存该规则。

步骤 3 （可选。）设置 URL 过滤的首选项。

在启用 URL 许可证时，系统会自动启用对 Web 类别数据库的更新。系统每 30 分钟检查一次更新，不过数据通常每天更新一次。如果您由于某种原因不想更新，可以关闭这些更新。

a) 点击**设备**。

b) 依次点击**系统设置** > **流量设置** > **URL 过滤首选项**。

c) 在 **URL 查询源**下，选择建议的选项： **本地数据库和 Cisco 云**。

如果安装的URL数据库没有进行站点分类，Cisco云可能会进行分类。云返回类别和信誉，基于类别的规则随后可以正确应用至URL请求。对因内存限制而安装较小URL数据库的低端系统而言，选择此选项非常重要。

或者，您可以将查找限制为本地数据库或 Cisco 云。

d) 选择合理的 **URL 生存时间**，例如 24 小时。

e) 点击**保存 (Save)**。

步骤 4 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

此时，监控控制面板和事件应开始显示URL类别和信誉及被丢弃连接的相关信息。您可以评估此信息以确定您的 URL 过滤要丢弃这些不符合条件的站点，还是您需要针对特定类别降低信誉设置。

请考虑事先通知用户，您会基于网站的分类和信誉阻止对网站的访问。

如何控制应用的使用

Web 已成为企业交付应用（无论是基于浏览器的应用平台，还是使用 Web 协议传入和传出企业网络的富媒体应用）普遍使用的平台。

威胁防御通过检查连接确定使用的应用。这样即可写入针对应用的访问控制规则，而不只是针对特定的 TCP/UDP 端口。因此，即使使用相同的端口，也可以选择性地阻止或允许基于 Web 的应用。

虽然可以选择要允许或阻止的特定应用，但也可以基于类型、类别、标记、风险或业务相关性写入规则。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

思科会通过系统和漏洞数据库 (VDB) 更新频繁更改并添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

在此使用案例中，我们将阻止属于**匿名程序/代理**类别的任何应用。

开始之前

此使用案例假定您已完成使用案例如何深入了解您的网络流量，第 44 页。该使用案例介绍了如何收集应用使用信息，您可以在“应用”控制面板中分析这些信息。了解实际使用的应用可帮助您基于应用设计有效的规则。另外，该使用案例还介绍了如何安排 VDB 更新，我们在此不再重复。请务必要定期更新 VDB，以便可正确识别应用。

过程

步骤 1 创建基于应用的访问控制规则。

a) 在主菜单中点击**策略**。

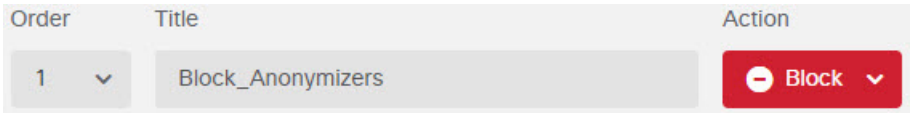
确保系统显示**访问控制**策略。

b) 点击 + 可添加新规则。

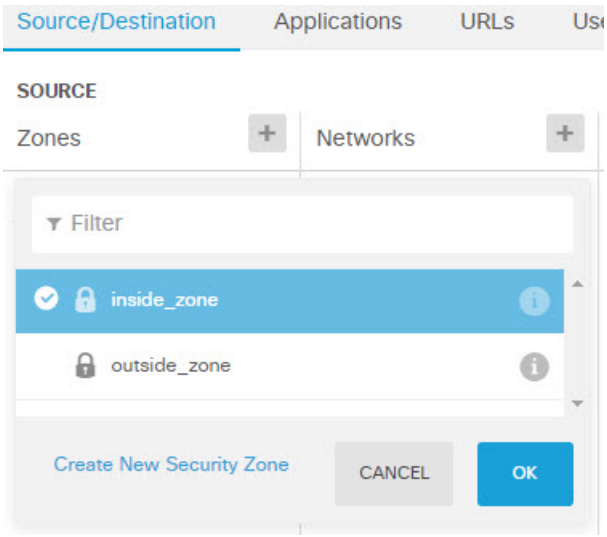
c) 配置顺序、标题和操作。

- **顺序** - 默认将新规则添加到访问控制策略的末尾。但是，您必须将此规则放在符合相同源/目的及其他条件的任何规则之前（上方），否则该规则将无法获得匹配（一个连接仅匹配一条规则，即该规则是连接在表中匹配的第一条规则）。对于该规则，我们将使用与初始设备配置期间创建的 Inside_Outside_Rule 相同的源/目的。您可能也已经创建了其他规则。为了最大限度地提高访问控制效率，最好是尽早设置特定规则，以确保快速决定允许还是丢弃某个连接。对于此示例，请选择 **1** 作为规则顺序。
- **标题** - 为该规则指定一个有意义的名称，例如 Block_Anonymizers。

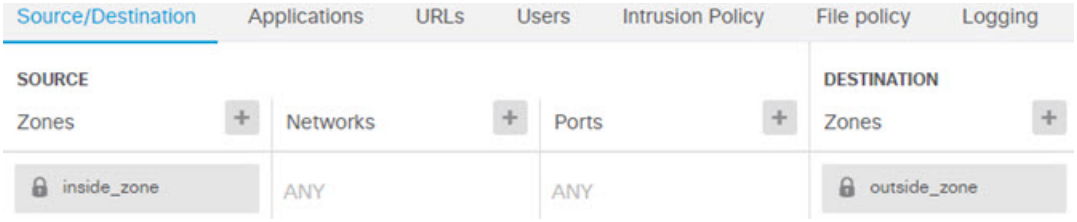
- **操作** - 选择**阻止**。



d) 在**源/目的 (Source/Destination)** 选项卡上，点击 **+** 以打开**源 (Source)** > **区域 (Zones)**，然后选择 **inside_zone**，再在区域对话框中点击**确定 (OK)**。



e) 按照相同的方法，为**目的** > **区域**选择 **outside_zone**。



f) 点击**应用**选项卡。

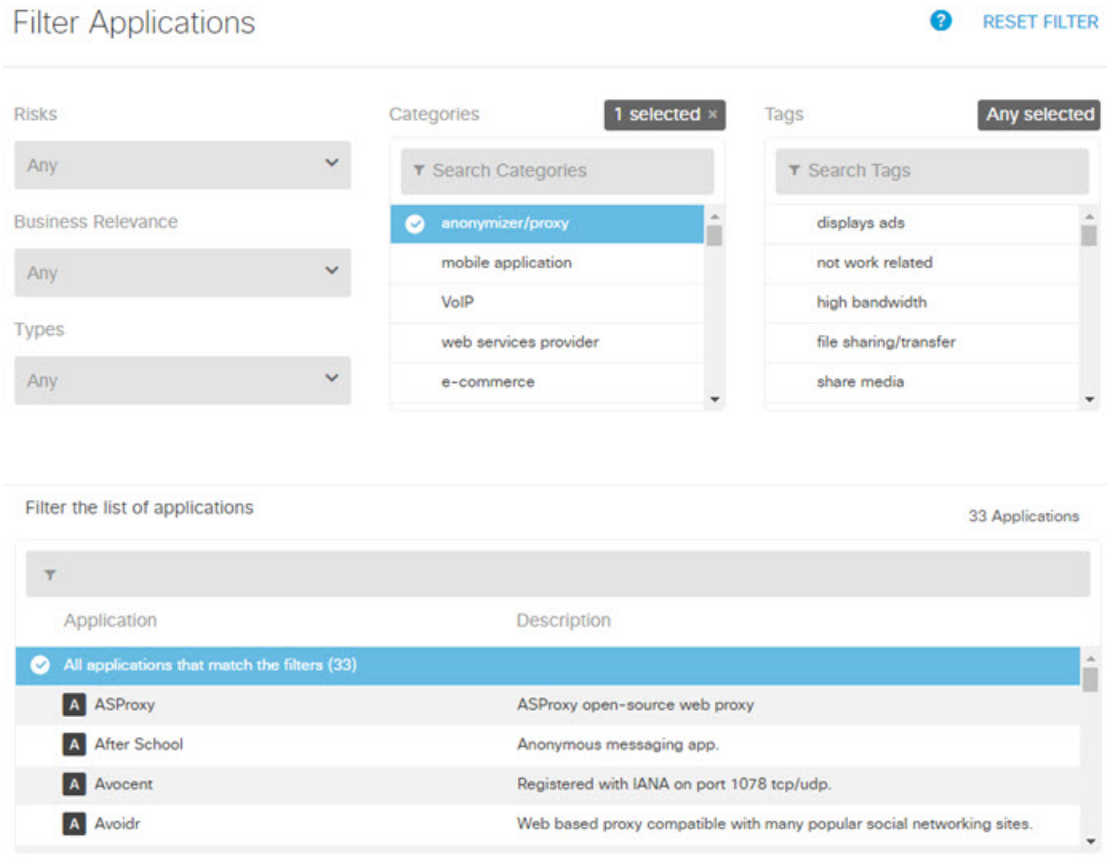
g) 针对**应用**点击 **+**，然后点击弹出对话框底部的**高级过滤器**链接。

虽然可以事先创建应用过滤器对象，再在此处从“应用过滤器”列表中选择它们，但也可以直接在访问控制规则中指定条件，再选择将该条件另存为过滤器对象。除非为单个应用写入规则，否则使用“高级过滤器”对话框查找应用和构建适当的条件更方便。

在选择条件时，对话框底部的“应用”列表将准确显示符合条件的应用。您要编写的规则将应用到这些应用中。

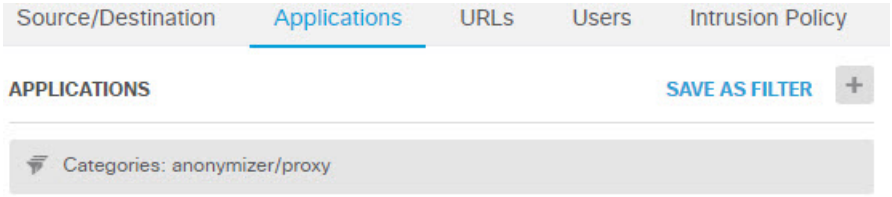
仔细查看此列表。例如，您可能会希望阻止风险极高的所有应用。但是，截至本文撰写之时，TFPT 被归为风险极高类别。而大多数组织不想阻止该应用。请花些时间测试各种过滤条件，以查看哪些应用符合您的选择。请注意，这些列表可能随着每次 VDB 更新而变化。

在本例中，从“类别”列表中选择“匿名程序/代理”。



h) 在“高级过滤器”对话框中点击 **添加 (Add)**。

“应用”选项卡中将添加并显示该过滤器。



i) 点击**日志记录**选项卡，然后依次选择**选择日志操作** > **连接开始和结束时**。

您必须启用日志记录选项卡才能获取与此规则阻止的任何连接相关的信息。

j) 点击**确定**以保存该规则。

步骤 2 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 3 点击**监控**并评估结果。

现在，您可能会在**网络概况**控制面板中看到“应用”构件中丢弃的连接。使用**所有/已拒绝/已允许**下拉选项可仅关注被丢弃的应用。

此外，还可以在**Web 应用**控制面板上查找应用的相关信息。**应用**控制面板显示与协议相关的结果。假定您启用了身份策略并要求身份验证，当有人尝试使用这些应用时，您应该能够将应用与尝试连接的用户相关联。

如何添加子网

如果您的设备有一个可用接口，则可以将其连接到交换机（或其他路由器）为其他子网提供服务。

添加子网的潜在原因很多。对于此使用案例，我们将处理以下典型场景。

- 子网是内部网络，使用专用网络 192.168.2.0/24。
- 该网络的接口使用静态地址 192.168.2.1。在本例中，网络使用的是物理接口。另一种选项是使用已连线的接口，并为新网络创建一个子接口。
- 设备将使用 DHCP 为网络中的工作站提供地址，使用的地址池为 192.168.2.2 - 192.168.2.254。
- 允许网络访问其他内部网络和外部网络。传至外部网络的流量将使用 NAT 获取公共地址。

注释 此示例假定未使用的接口不是网桥组的一部分。如果它当前是网桥组成员，则必须首先将其从网桥组中删除，然后再执行此步骤过程。

开始之前

将网络电缆物理连接到新子网的接口和交换机。

过程

步骤 1 配置接口。

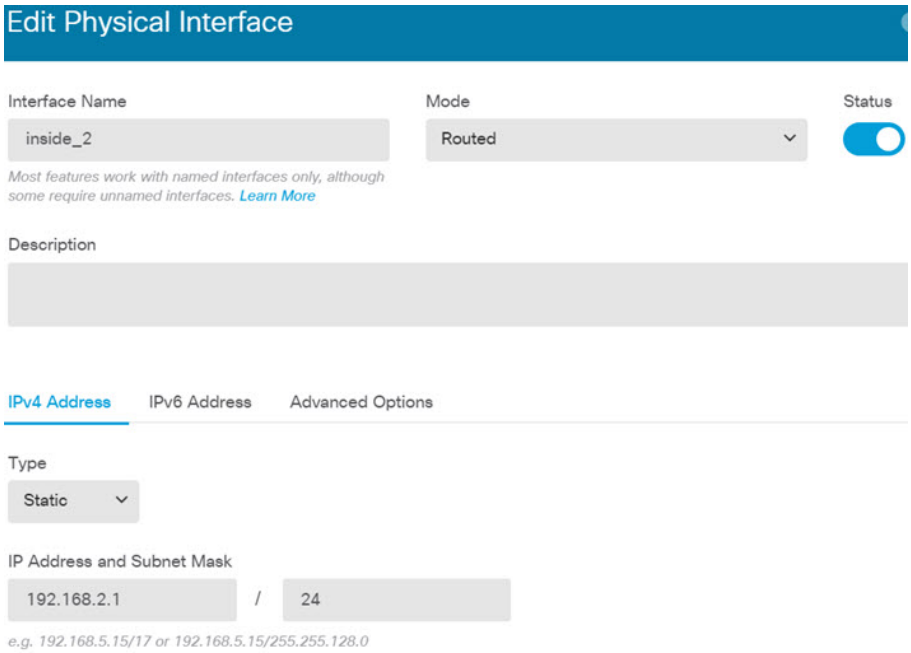
a) 点击**设备**，点击**接口**摘要中的链接，然后点击接口类型以查看接口列表。

b) 将鼠标悬停在您连线的接口行右侧的**操作**单元格上方，然后点击编辑图标 ( )。

c) 配置基本接口属性。

- **名称** - 接口的名称。在本例中为 **inside_2**。
- **模式** - 选择**路由**。

- **状态** - 点击状态开关启用该接口。
- **IPv4 地址**选项卡 - 针对**类型**选择**静态**，然后输入 **192.168.2.1/24**。



d) 点击**保存 (Save)**。

接口列表将显示更新的接口状态和配置的 IP 地址。

步骤 2 针对该接口配置 DHCP 服务器。

a) 点击**设备**。

b) 点击**系统设置** > **DHCP 服务器**。

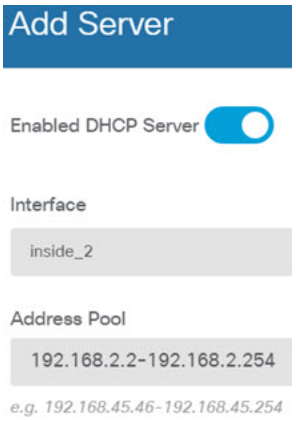
c) 点击 **DHCP 服务器**选项卡。

下表列出了所有现有 DHCP 服务器。如果使用默认配置，列表中包含内部接口的一个 DHCP 服务器。

d) 点击表格上方的 **+**。

e) 配置服务器属性。

- **启用 DHCP 服务器** - 点击此开关启用该服务器。
- **接口** - 选择您提供 DHCP 服务所使用的接口。在本例中，选择 inside_2。
- **地址池** - 服务器可以为网络中设备提供的地址。输入 192.168.2.2-192.168.2.254。确保未包含网络地址 (.0)、接口地址 (.1) 或广播地址 (.255)。另外，如果网络中的任何设备需要使用静态地址，请从池中排除这些地址。池必须是一系列连续地址，所以请从该范围的开头或末尾选择静态地址。



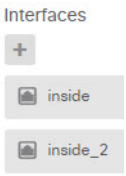
f) 点击 **添加 (Add)**。

#	INTERFACE	ENABLED DHCP SERVER	ADDRESS POOL
1	**inside**	Enabled	192.168.1.5-192.168.1.254
2	**inside_2**	Enabled	192.168.2.2-192.168.2.254

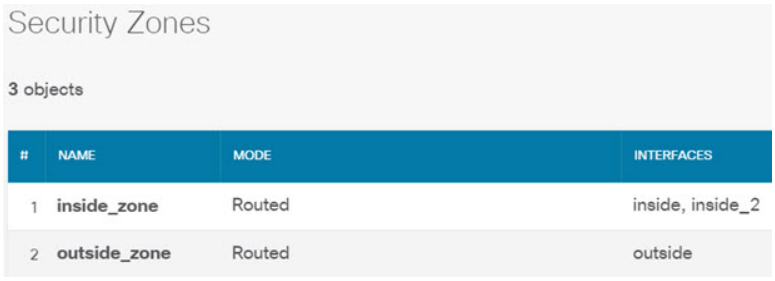
步骤 3 将该接口添加到内部安全区。

要在接口上编写策略，该接口必须属于安全区。您需要针对安全区编写策略。因此，您在区域中添加和删除接口时，会自动更改应用于接口的策略。

a) 在主菜单中点击**对象**。
b) 从对象目录中选择**安全区**。
c) 将鼠标悬停在 **inside_zone** 对象行右侧的**操作**单元格上方，然后点击编辑图标 ( )。
d) 点击**接口**下的 **+**，选择 inside_2 接口，然后点击接口列表中的**确定**。



e) 点击**保存 (Save)**。



步骤 4 创建一条允许在内部网络之间传输流量的访问控制规则。

不会自动允许任何接口之间的流量。必须创建访问控制规则，才能允许所需的流量。唯一例外情况是，允许访问控制规则默认操作中的流量。在本例中，我们假定您保留了设备安装向导配置的阻止默认操作。因此，您需要创建一条规则，以允许内部接口之间的流量。如果已经创建这样的规则，请跳过此步骤。

a) 在主菜单中点击**策略**。

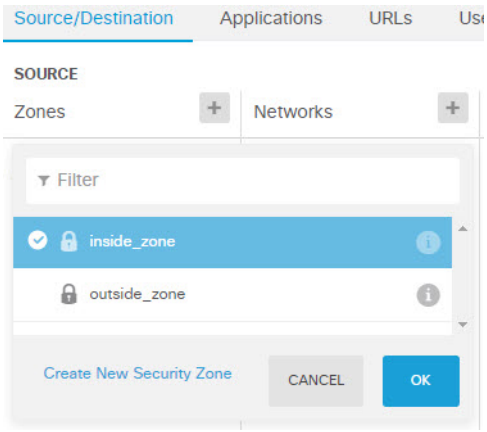
确保系统显示**访问控制**策略。

b) 点击 + 可添加新规则。

c) 配置顺序、标题和操作。

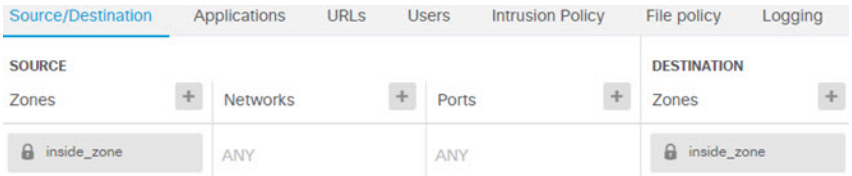
- **顺序** - 默认将新规则添加到访问控制策略的末尾。但是，您必须将此规则放在符合相同源/目的及其他条件的任何规则之前（上方），否则该规则将无法获得匹配（一个连接仅匹配一条规则，即该规则是连接在表中匹配的第一条规则）。对于该规则，我们将使用唯一“源/目的”条件，所以可以将该规则添加到列表的末尾。
- **标题** - 为该规则指定一个有意义的名称，例如 Allow_Inside_Inside。
- **操作** - 选择**允许**。

d) 在**源/目的 (Source/Destination)** 选项卡上，点击 + 以打开**源 (Source)** > **区域 (Zones)**，然后选择 **inside_zone**，再在区域对话框中点击**确定 (OK)**。



e) 按照相同的方法，为**目的** > **区域**选择 **inside_zone**。

安全区必须至少包含两个接口，以便为源和目标选择同一区域。



f) （可选。）配置入侵和恶意软件检测。

虽然内部接口位于受信任区域，但用户通常会将笔记本电脑连接到网络。因此，用户可能不知道会将外部网络或Wi-Fi热点的威胁带入网络内部。因此，您可能希望扫描内部网络之间的流量中是否存在入侵和恶意软件。

请考虑执行以下操作。

- 点击**入侵策略**选项卡，启用入侵策略，并使用滑块选择“平衡安全和连接”策略。
- 点击**文件策略**选项卡，然后选择“阻止所有恶意软件”策略。

g) 点击**日志记录**选项卡，然后依次选择**选择日志操作** > **连接开始和结束时**。

只有启用日志记录，才能获得符合该规则的任何连接的相关信息。日志记录会向控制面板中添加统计信息，并会显示事件查看器中的事件。

h) 点击**确定**以保存该规则。

步骤 5 确认是否已为新子网定义所需的策略。

通过将该接口添加到 inside_zone 安全区，inside_zone 的任何现有策略将自动应用到新子网。但是，请花些时间来检查您的策略，确保未遗漏任何其他策略。

如果已完成初始配置，即可应用以下策略。

- **访问控制** - Inside_Outside_Rule 应允许新子网和外部网络之间的所有流量。如果您按照前面的使用案例执行了操作，该策略还会提供入侵和恶意软件检测。必须有一条规则允许新网络和外部网络之间的某些流量，否则用户将无法访问互联网或其他外部网络。
- **NAT** - InsideOutsideNATrule 适用于传至外部接口的任何接口，并会应用于接口 PAT。如果保留了此规则，则从新网络传至外部网络的流量会将IP地址转换为外部接口IP地址上的唯一端口。如果在传至外部接口时没有应用于所有接口或 inside_zone 接口的规则，则可能需要立即创建一条规则。
- **身份** - 没有默认的身份策略。但是，如果您按照前面的使用案例执行了操作，则可能已有需要对新网络进行身份验证的身份策略。如果没有适用的身份策略，但希望掌握新网络的用户信息，请立即创建一条策略。

步骤 6 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

确认新子网中的工作站是否使用 DHCP 获取 IP 地址，以及它们是否可访问其他内部网络和外部网络。使用监控控制面板和事件查看器评估网络使用情况。

如何被动监控网络上的流量

威胁防御设备通常部署为主动防火墙和IPS（入侵防御系统）安全设备。设备的核心功能是提供主动网络保护，丢弃不需要的连接和威胁。

但是，您还可以在被动模式下部署系统，使设备只分析受监控交换机端口上的流量。此模式主要用于演示或测试目的，以便您可以在将设备部署为主动防火墙之前熟悉设备。使用被动部署，您可以监控网络上的各种威胁、用户浏览的 URL 类别，等等。

虽然被动模式通常用于演示或测试目的，但也可以在生产环境中使用，前提是它可提供所需的服务，例如 IDS（入侵检测系统，而无需防御）。您可以搭配使用被动接口和主动防火墙路由接口，以提供组织所需的确切服务组合。

以下过程介绍如何被动部署系统来分析通过有限数量的交换机端口传递的流量。

注释 本示例适用于硬件 威胁防御设备。您还可以对 threat defense virtual 使用被动模式，但网络设置是不同的。有关详细信息，请参阅为 Threat Defense Virtual 被动接口配置 VLAN，第 267 页。否则，此程序也适用 threat defense virtual。

开始之前

此过程假定您已连接内部和外部接口，并完成初始设备设置向导。即使在被动部署中，您也需要连接到互联网下载系统数据库更新。您还需要能够连接到管理接口以打开 设备管理器（可通过到内部或管理端口的直接连接实现）。

该示例还假设您已在**策略 (Policies)** > **入侵 (Intrusion)** 页面上为入侵策略启用系统日志。

过程

步骤 1 将交换机端口配置为 SPAN（交换端口分析器）端口，并为源接口配置监控会话。

以下示例为 Cisco Nexus 5000 系列交换机上的两个源接口设置 SPAN 端口和监控会话。如果您使用不同类型的交换机，所需的命令可能会有所不同。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
```

```
switch(config-monitor)# no shut
```

验证：

```
switch# show monitor session 1 brief
   session 1
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

步骤 2 将 威胁防御接口连接到交换机的 SPAN 端口。

最好选择 威胁防御设备上当前未使用的端口。根据示例交换机配置，将电缆连接到交换机的以太网 1/48。这是监控会话的目标接口。

步骤 3 将 威胁防御接口配置为被动模式。

a) 点击**设备**，然后点击**接口**摘要中的链接，再点击**接口**或 **EtherChannel**。

b) 点击要编辑的物理接口或 EtherChannel 的编辑图标 ( )。

选择当前未使用的接口。如果您要将使用中的接口转换为被动接口，需要先从任何安全区中删除该接口，并删除使用该接口的所有其他配置。

c) 将**状态**滑块设置为已启用设置 ( )。

d) 进行以下配置：

- **接口名称** - 接口名称，最多 48 个字符。字母字符必须为小写。例如，**monitor**。
- **模式** - 选择**被动**。

e) 点击**确定 (OK)**。

步骤 4 为接口创建被动安全区。

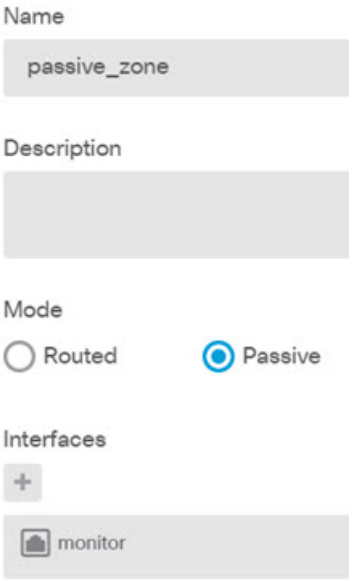
a) 选择**对象**，然后从目录中选择**安全区**。

b) 点击 + 按钮。

c) 输入对象的**名称**和说明（后者为可选项）。例如，**passive_zone**。

d) 对于**模式**，请选择**被动**。

e) 点击 +，然后选择被动接口。



f) 点击**确定 (OK)**。

步骤 5 为被动安全区配置一个或多个访问控制规则。

创建的规则数量和类型取决于您想要收集的信息。例如，如果您要将系统配置为 IDS（入侵检测系统），需要至少一个分配有入侵策略的允许规则。如果您想要收集URL类别数据，需要至少一个具有 URL 类别规范的规则。

您可以创建阻止规则，以确定系统本可阻止主动路由接口上的哪些连接。这些连接实际上并没有被阻止，因为接口是被动接口，但您将清楚地看到系统会如何整理网络上的流量。

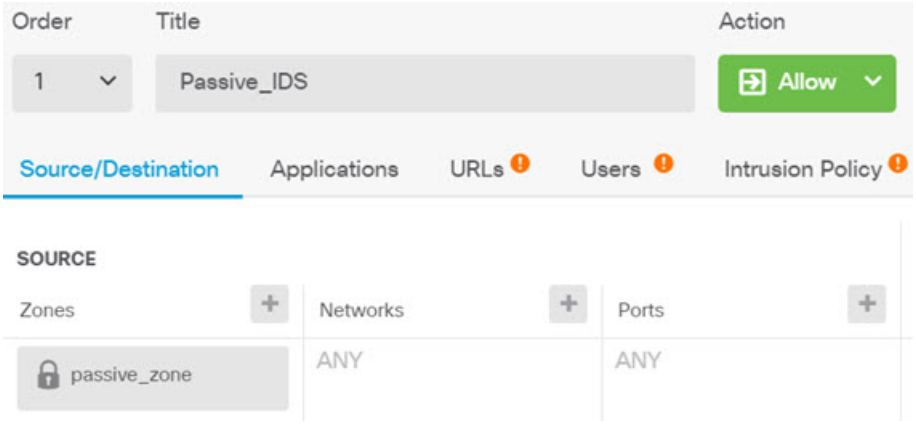
以下使用案例介绍访问控制规则的主要用途。这些规则也适用于被动接口。只需选择被动安全区作为所创建规则的源区域。

- 如何阻止威胁，第 51 页
- 如何阻止恶意软件，第 55 页
- 如何实施可接受使用策略（URL 过滤），第 58 页
- 如何控制应用的使用，第 63 页

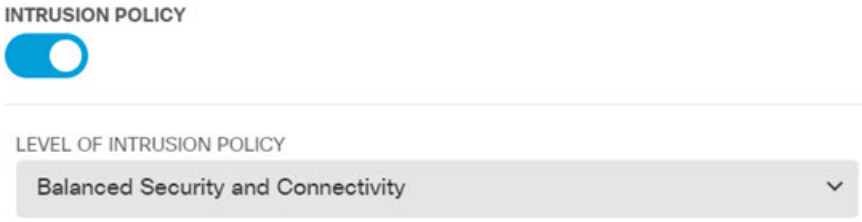
以下过程创建两条允许规则来应用入侵策略并收集 URL 类别数据。

a) 依次选择**策略** > **访问控制**。
b) 点击 **+** 添加允许所有流量、但应用入侵策略的规则。
c) 选择 **1** 作为规则顺序。此规则比默认规则更具体，但并不与之重叠。如果您已有自定义规则，请为这些规则选择适当的位置，以便传递到被动接口的流量不匹配这些规则。
d) 输入规则的名称，例如 **Passive_IDS**。
e) 对**操作**选择**允许**。
f) 在**源/目标**选项卡上，选择**源** > **区域**下的被动区。不要配置选项卡上的任何其他选项。

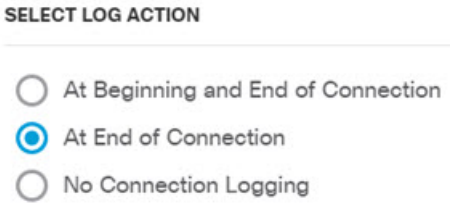
在评估模式运行时，此阶段的规则应为：



g) 点击**入侵策略**选项卡，将滑块滑动至**打开**，并选择**平衡安全和连接**入侵策略（建议将此策略应用于大多数网络）。



h) 点击**日志记录**选项卡，并选择**在连接结束时**作为日志记录选项。



i) 点击**确定 (OK)**。

j) 点击 **+** 添加要求系统执行深度检测以确定所有 HTTP 请求的 URL 和类别的规则。

通过此规则，您可以在控制面板中查看 URL 类别信息。为节省处理时间并提高性能，系统仅在至少有一个指定 URL 类别条件的访问控制规则时确定 URL 类别。

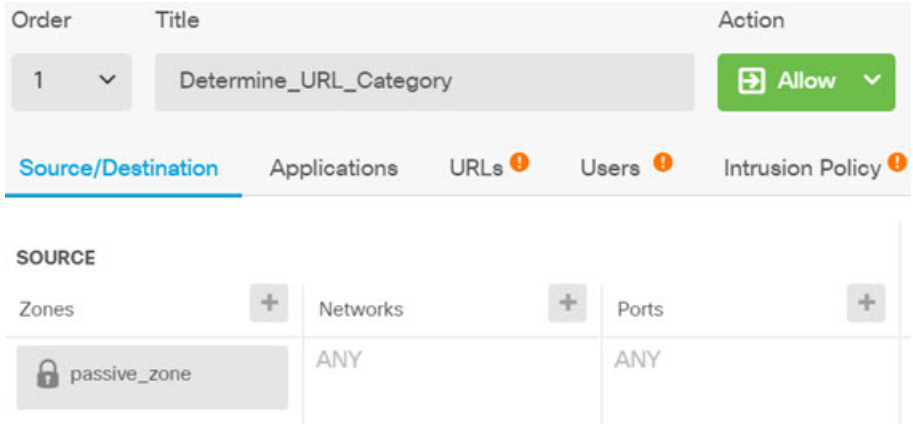
k) 选择**1**作为规则顺序。这样可将规则放置在上一个规则(Passive_IDS)上方。如果您将其放置在该规则（适用于所有流量）后面，流量将永远不会匹配您现在创建的规则。

l) 输入规则的名称，例如 **Determine_URL_Category**。

m) 对**操作**选择**允许**。

或者，您可以选择**阻止**。上述任一操作都可以实现此规则的目的。

n) 在**源/目标**选项卡上，选择**源** > **区域**下的被动区。不要配置选项卡上的任何其他选项。



o) 点击 **URL** 选项卡，点击**类别**标题旁边的 +，然后选择任何类别。例如，**搜索引擎和门户**。或者，可以选择信誉级别，或保留默认值“任何”。

p) 点击**入侵策略**选项卡，将滑块滑动至**打开**，并选择您为第一个规则选择的同一入侵策略。

q) 点击**日志记录**选项卡，并选择**在连接结束时**作为日志记录选项。

但是，如果您选择**阻止**操作，请选择**在连接开始和结束时**。由于被阻止的连接不会自行终止，只能在连接开始时获取日志信息。

r) 点击**确定 (OK)**。

步骤 6 （可选。）配置其他安全策略。

您还可以配置以下安全策略，了解它们对流量的影响：

- **身份** - 收集用户信息。您可以在身份策略中配置规则，以确保识别与源 IP 地址关联的用户。为被动接口实施身份策略的过程与为路由接口实施身份策略的过程相同。请按照如何深入了解您的网络流量，第 44 页所述的使用案例操作。
- **安全智能** - 阻止已知不良 IP 地址和 URL。有关详细信息，请参阅如何阻止威胁，第 51 页。

注释 被动接口上的所有加密流量均划分为无法解密类别，因此 SSL 解密规则无效，不会应用于被动接口。

步骤 7 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 8 使用监控控制面板分析来自整个网络的流量和威胁类型。如果您确定要让 威胁防御设备主动丢弃不需要的连接，请重新部署设备，以便您可以配置用于为监控网络提供防火墙保护的主动路由接口。

更多示例

除了使用案例一章中的示例之外，某些解释特定服务的章节中还包括示例配置。您可能对下面的示例感兴趣。

访问控制

- 如何使用 TrustSec 安全组标记控制网络访问， 第 491 页

网络地址转换 (NAT)

IPv4 地址的 NAT

- 提供对内部 Web 服务器的访问权限（静态自动 NAT）， 第 577 页
- FTP、HTTP 和 SMTP 的单个地址（具有端口转换的静态自动 NAT）， 第 579 页
- 转换因目标而异（动态手动 PAT）， 第 585 页
- 转换因目标地址和端口而异（动态手动 PAT）， 第 591 页
- DNS 回复修改、外部接口上的 DNS 服务器， 第 603 页
- DNS 回复修改、主机网络上的 DNS 服务器， 第 606 页
- 使站点间 VPN 流量豁免 NAT， 第 636 页

IPv6 地址的 NAT

- NAT64/46 示例：内部 IPv6 网络与外部 IPv4 互联网， 第 563 页
- NAT64/46 示例：包含外部 IPv4 互联网和 DNS 转换的内部 IPv6 网络， 第 565 页
- NAT66 示例：网络间的静态转换， 第 570 页
- NAT66 示例：简单 IPv6 接口 PAT， 第 573 页
- DNS 64 回复修改， 第 597 页

远程访问虚拟专用网络 (RA VPN)

- 如何实施 RADIUS 授权更改， 第 683 页
- 如何使用 Duo LDAP 配置双因素身份验证， 第 691 页
- 如何在外部接口上为远程访问 VPN 用户提供互联网访问权限（发夹方法）， 第 697 页
- 如何通过远程访问 VPN 使用外部网络上的目录服务器， 第 701 页
- 如何通过组控制 RA VPN 访问， 第 714 页

- 如何对不同虚拟路由器中的内部网络进行 RA VPN 访问， 第 718 页
- 如何自定义 Secure Client 图标和徽标， 第 721 页

站点间虚拟专用网络 (VPN)

- 使站点间 VPN 流量豁免 NAT， 第 636 页
- 如何在外部接口上为外部站点间 VPN 用户提供互联网访问（发夹方法）， 第 642 页
- 如何通过站点间 VPN 保护来自多个虚拟路由器的网络流量， 第 649 页

SSL/TLS 解密

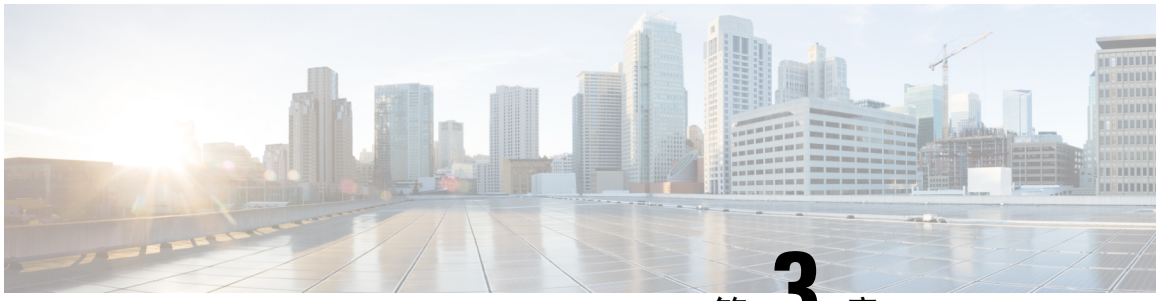
- 示例：从网络阻止较旧的 SSL/TLS 版本， 第 439 页

FlexConfig 策略

- 如何启用和禁用默认全局检测， 第 833 页
- 如何撤消 FlexConfig 更改， 第 839 页
- 如何启用唯一流量类检测， 第 840 页

虚拟路由

- 如何提供对包含重叠地址空间的多个虚拟路由器的互联网访问权限 ， 第 331 页
- 如何通过多个虚拟路由器路由到远程服务器， 第 325 页
- 如何对不同虚拟路由器中的内部网络进行 RA VPN 访问， 第 718 页
- 如何通过站点间 VPN 保护来自多个虚拟路由器的网络流量， 第 649 页



第 3 章

为系统授权许可

以下主题介绍如何向 威胁防御设备授予许可证。

防火墙系统的智能许可

思科智能许可是一种灵活的许可模式，为您提供一种更简便、更快速、更一致的方式来购买和管理整个思科产品组合和整个组织中的软件。此外它很安全，您可以控制用户可访问的内容。借助智能许可，您可以：

- **轻松激活：** 智能许可建立了可在整个组织中使用的软件许可证池，不再需要产品激活密钥 (PAK)。
- **统一管理：** 利用 My Cisco Entitlements (MCE)，您可以在一个易于使用的门户中全面了解您的所有 Cisco 产品和服务，始终了解您拥有以及正在使用的产品和服务。
- **许可证灵活性：** 您的软件没有与硬件节点锁定，因此您可以根据需要轻松使用和传输许可证。

要使用智能许可，您必须先在 Cisco Software Central (software.cisco.com) 上创建智能帐户。

有关思科许可的更详细概述，请访问 cisco.com/go/licensingguide

思科智能软件管理器

在为 威胁防御设备购买一个或多个许可证时，可以在思科智能软件管理器中对其进行管理：https://software.cisco.com/#SmartLicensing-Inventory。通过思科智能软件管理器，您可以为组织创建一个主账户。

默认情况下，许可证分配给主账户下的默认虚拟帐户。作为账户管理员，您可以创建其他虚拟帐户；例如，为区域、部门或子公司创建账户。使用多个虚拟帐户有助于管理大量许可证和设备。

许可证和设备按虚拟帐户进行管理；只有该虚拟帐户的设备可以使用分配给该账户的许可证。如果您需要其他许可证，则可以从另一个虚拟帐户传输未使用的许可证。您还可以在虚拟帐户之间传输设备。

当您向思科智能软件管理器注册某个设备时，会在管理器中创建一个产品实例注册令牌，然后将其输入 设备管理器。注册的设备将基于使用的令牌与某个虚拟帐户相关联。

有关思科智能软件管理器的详细信息，请参阅该管理器的在线帮助。

与许可证颁发机构的定期通信

使用产品实例注册令牌注册 威胁防御 设备时，设备会向思科许可证颁发机构注册。许可证颁发机构会为该设备与许可证颁发机构之间的通信颁发 ID 证书。此证书有效期为 1 年，但需要每 6 个月续签一次。如果 ID 证书到期（通常在九个月或一年内未通信），设备将恢复撤销注册状态，许可的功能将被暂停使用。

设备定期与许可证颁发机构进行通信。如果您在思科智能软件管理器中进行更改，则可以刷新设备上的授权，以使更改立即生效。另外，也可以等待设备按计划通信。常规许可证通信每 12 小时进行一次，但如果设备具有宽限期，则会最多运行 90 天，而不会进行自动通报。您必须在 90 天截止前与许可证颁发机构联系。

智能许可证类型

下表介绍了 威胁防御设备可用的许可证。

购买 威胁防御设备会自动附带基础版许可证。其他所有许可证均是可选的。

表 *2:* 智能许可证类型

许可证	持续时间	授予的功能
基础版	永久	可选期限的许可证中未包括的所有功能。 注册时，基础版许可证会自动添加到您的帐户。Cisco Secure Firewall 3100 是个例外。购买防火墙时，您将获得基础许可证，并且该许可证的管理方式与您账户中的其他许可证一样。例如，您需要在注册时确保许可证位于正确的虚拟帐户中。 您还必须指定是否**在使用此令牌注册的产品上允许出口控制功能**。仅在您的国家/地区满足出口控制标准时，才可以选择此选项。此选项控制您对高级加密和需要高级加密的功能的使用。

许可证	持续时间	授予的功能
IPS	基于期限	需要使用以下策略： • 入侵 • 文件（还需要恶意软件防御） • 安全智能
恶意软件防御	基于期限	文件策略（还需要IPS ）。
URL	基于期限	URL 策略 - 基于类别和信誉的 URL 过滤或 DNS 查找请求过滤。 您可以对单个 URL 执行 URL 过滤，而不使用此许可证。
RA VPN： • Secure Client Advantage • Secure Client Premier • 仅限 Secure Client VPN	基于期限或永久，取决于许可证类型。	远程接入 VPN 配置。您的基础许可证必须允许出口控制功能，以便配置远程访问 RA VPN。在注册设备时，您需要选择是否满足出口要求。 设备管理器 可以使用任何有效 Secure Client 许可证。可用功能不因许可证类型不同而不同。如果尚未购买，请参阅远程访问 VPN 的许可要求，第 661 页。 另请参阅《思科 *AnyConnect* 订购指南》http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf。
运营商	基于期限	移动网络协议检测。您需要此许可证来配置 GTP/GPRS、Diameter、SCTP 和 M3UA 检测。使用 FlexConfig 配置这些检测。

Threat Defense Virtual 许可

本部分描述可用于 threat defense virtual 的性能分级许可授权。

可以在任何受支持的 threat defense virtual vCPU/内存配置中使用任何 threat defense virtual 许可证。这可让 threat defense virtual 客户在各种各样的 VM 资源占用空间中运行。这还会增加受支持的 AWS 和 Azure 实例类型的数量。配置 threat defense virtual VM 时，支持的 vCPU 最大核数为 16（对于 VMware 和 KVM 上的 FTDv；支持的最大内存为 32GB RAM 。

Threat Defense Virtual 智能许可的性能级别

RA VPN 的会话限制由安装的 threat defense virtual 平台授权级别确定，并通过速率限制器强制执行。下表总结了基于授权层和速率限制器的会话限制。

表 *3:* 基于授权的 ***Threat Defense Virtual*** 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv100，16Gbps	16 核/32 GB	16Gbps	10,000

Threat Defense Virtual 性能级许可准则和限制

许可 threat defense virtual 设备时，请时刻注意以下准则和限制。

- threat defense virtual 支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。
- 可以在任何受支持的 threat defense virtual 核心/内存配置中使用任何 threat defense virtual 许可证。这可让 threat defense virtual 客户在各种各样的 VM 资源占用空间中运行。
- 无论您的设备是处于评估模式还是已注册到思科智能软件管理器，您都可以在部署 threat defense virtual时选择性能级别。

注释 确保智能许可账户包含所需的可用许可证。选择与您账户中的许可证相匹配的级别很重要。如果要将 threat defense virtual 升级到 7.0 版，可以选择 **FTDv - 变量**来保持当前的许可证合规性。threat defense virtual 会根据您的设备功能（内核数/RAM）继续执行会话限制。

- 部署新 threat defense virtual 设备或使用 REST API 调配 threat defense virtual 时，默认性能级别为 FTDv50。
- 基础版许可证以订用为基础，并映射到性能级别。您的虚拟帐户需要具有 threat defense virtual 设备的 基础版 许可证授权，以及 IPS 、恶意软件防御和 URL 过滤 许可证的授权。
- 每个 HA 对等体使用一个授权，并且每个 HA 对等体上的授权必须匹配，包括基础版许可证。
- 高可用性对的性能级别更改应应用于主对等体。
- 通用 PLR 许可单独应用于高可用性对中的每台设备。辅助设备不会自动镜像主设备的性能级别，而是必须手动更新。

出口控制设置对加密功能的影响

注册设备时，您还必须指定是否**在使用此令牌注册的产品上允许出口控制功能**。仅在您的国家/地区满足出口控制标准时，才可以选择此选项。此选项控制您对高级加密和需要高级加密的功能的使用。

评估模式被视为与使用非出口合规账户进行注册相同。这意味着在评估模式下运行时，无法配置远程访问 VPN 或使用高级加密算法。

最特别的是，DES 标准仅在评估或非出口合规模式下可用。

因此，如果您配置加密功能（例如站点间 VPN），或加密高可用性组中的故障转移连接，可能会在注册出口合规账户后最终出现连接问题。如果该功能在评估模式下使用 DES，则在您注册账户后该配置将被破坏。

考虑以下建议来避免与加密相关的问题：

- 在注册设备之前，避免配置加密功能，例如站点间 VPN 和加密的故障转移连接。
- 使用出口合规账户注册设备后，编辑您在评估模式下配置的所有加密功能，并选择更安全的加密算法。测试并验证这些功能中的每项功能，以确保它们正常运行。

注释 如果您在评估模式下配置了 HA 故障转移加密，还需要重新启动 HA 组中的两台设备，才能开始使用更强的加密。建议您先删除加密，以避免两台设备将自己视为主用设备的“脑裂”情况。

可选许可证过期或被禁用的影响

如果以下任一可选许可证过期，您可以继续使用需要该许可证的功能。但是，该许可证将被标记为不合规，您需要购买许可证并将其添加到您的账户，才能使该许可证恢复合规状态。

如果禁用了某个可选许可证，系统将做出如下反应：

- 恶意软件防御 - 系统会停止查询安全恶意软件分析云，并且还会停止确认从安全恶意软件分析云发送的追溯性事件。如果现有访问控制策略包含文件策略，则您无法重新部署这些策略。请注意，在禁用恶意软件防御许可证后的很短时间内，系统可以使用现有缓存文件处置情况。在时间窗过期后，系统将向这些文件分配不可用的处置情况。
- IPS - 系统将不再应用入侵或文件策略。对于安全智能策略，系统不再应用策略并停止下载智能源更新。您无法重新部署需要该许可证的现有策略。
- URL - 带有 URL 类别条件的访问控制规则会立即停止过滤 URL 或 DNS 查找请求，且系统不会再下载对 URL 数据的更新。如果现有访问控制策略包含的规则带有基于类别和信誉的 URL 标准，则不能重新部署现有的访问控制策略。
- RA VPN - 您不能编辑远程访问 VPN 配置，但可以将其删除。用户仍可使用 RA VPN 配置进行连接。但是，如果您更改设备注册，致使系统不再符合导出规定，则远程访问VPN配置会立即停止，且所有远程用户都无法通过 VPN 进行连接。

管理智能许可证

使用“智能许可证”(Smart License) 页面可查看系统当前的许可证状态。系统必须获得许可。

该页面显示您使用的是90天评估许可证，还是已注册到思科智能软件管理器。注册后，您可以查看与思科智能软件管理器的连接状态，以及各类许可证的状态。

使用授权标识智能许可证代理状态：

- 已授权（“已连接”、“足够的许可证”）- 设备已成功联系许可证颁发机构并向其注册，该机构已向设备授予许可证授权。设备现在处于合规状态。
- 不合规 - 设备没有可用的许可证授权。许可功能可继续工作。但您必须购买或释放其他授权，才能变为合规状态。
- 授权已过期 - 设备已连续 90 天或更长时间未与许可颁发机构通信。许可功能可继续工作。在此状态下，智能许可证代理将重试其授权申请。如果重试成功，代理将进入“不合规”或“已授权”状态，并开始新的授权期限。尝试手动同步设备。

注释 点击智能许可证状态旁边的 **i** 按钮，可查看虚拟帐户、出口控制功能，并可获链接来打开思科智能软件管理器。出口控制功能可控制受国家安全、外交政策和反恐怖主义法律和法规约束的软件。

以下步骤程序概述了如何管理系统的许可证。

开始之前

如果您没有系统互联网路径，则无法使用智能许可，而将切换到永久许可证预留 (PLR) 模式。有关详细信息，请参阅在气隙网络中应用永久许可证，第 88 页。

过程

步骤 1 点击**设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 2 注册该设备。

只有注册到思科智能软件管理器，才能分配可选许可证。在评估期结束前进行注册。

请参阅注册设备，第 85 页。

注释 注册时，选择是否向思科发送使用数据。可以通过点击齿轮图标旁边的**转到 Cisco Success Network** 链接更改选择。

步骤 3 申请和管理可选功能许可证。

只有注册可选许可证后，才能使用该许可证控制的功能。请参阅启用或禁用可选许可证，第87页。

步骤 4 维护系统许可。

您可以执行以下任务：

- 与思科智能软件管理器同步，第 87 页
- 取消注册设备，第 88 页

注册设备

购买 威胁防御 设备会自动附带 基础版 许可证。基础版 许可证涵盖可选许可证未覆盖的所有功能。它是一种永久许可证。

在初始系统设置期间，系统会提示您将设备注册到思科智能软件管理器。如果您选择使用90天的评估许可证，必须在评估期结束前注册设备。

注册设备时，您的虚拟帐户会向设备分配许可证。注册设备也会注册已启用的任何可选许可证。

开始之前

注册设备时，仅该设备被注册。如果设备已配置为高可用性，您必须登录到高可用性对的另一台设备注册该设备。

过程

步骤 1 点击**设备**，然后点击“智能许可证”(the Smart License) 摘要中的**查看配置 (View Configuration)**。

步骤 2 点击**注册设备 (Register Device)**，并按照说明执行操作。

a) 点击链接以打开思科智能软件管理器 (Cisco Smart Software Manager)，然后登录您的账户或创建一个新账户（如果需要）。

b) 生成新的令牌。

在创建令牌时，指定该令牌的有效使用期限。建议的过期期限为 30 天。此期限定义令牌本身的过期日期，不会影响您使用该令牌注册的设备。如果令牌在使用前过期，只需生成一个新令牌即可。

您还必须指定是否**在使用此令牌注册的产品上允许出口控制功能**。仅在您的国家/地区满足出口控制标准时，才可以选择此选项。此选项控制您对高级加密和需要高级加密的功能的使用。

c) 复制该令牌，并将其粘贴到“智能许可证注册”对话框的编辑框中。

d) （**仅限 Threat Defense Virtual**）为您的 threat defense virtual 设备选择性能级别，或保留默认选择。

未选择性能级别时，您的threat defense virtual设备将在传统模式下运行，默认设置为4核/8 GB；有关详细信息，请参阅更改 Threat Defense Virtual 性能级别，第 86 页。

e) 选择用于思科云服务注册的区域。

注册后，如果需要更改此区域，则必须取消注册该设备，然后重新注册，并选择新区域。

f) 决定是否向思科发送使用数据。

阅读“Cisco Success Network”步骤中的信息，点击**样本数据 (Sample Data)** 链接查看收集到的实际数据，然后决定是否选中**启用 Cisco Success Network (Enable Cisco Success Network)** 选项。

g) 点击**注册设备 (Register Device)**。

更改 Threat Defense Virtual 性能级别

threat defense virtual 支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。可以在任何受支持的 threat defense virtual 核心/内存配置中使用任何 threat defense virtual 许可证。这可让 threat defense virtual 客户在各种各样的 VM 资源占用空间中运行；请参阅Threat Defense Virtual 智能许可的性能级别，第 81 页。

当您将 threat defense virtual 升级到 7.0 以上版本时，设备会自动改为“FTDv 变量”级别状态，并继续使用非分级授权，直到您选择授权级别。

请注意以下事项：

- 您可以根据吞吐量或 RA VPN 要求更改性能级别以满足部署需求。请记住，threat defense virtual 部署时内核和内存资源可调。您选择的性能级别不应超过设备规格。
- AWS 不支持更改性能层。

过程

步骤 1 点击**设备**，然后点击“智能许可证”(the Smart License) 摘要中的**查看配置 (View Configuration)**。

步骤 2 从**性能级别**下拉列表中选择所需选项。

- FTDv5（4 核/8 GB）
- FTDv10（8 核/8 GB）
- FTDv20（8 核/8 GB）
- FTDv30（8 核/16 GB）
- FTDv50（12 核/24 GB）
- FTDv100（16 核/24 GB）

注释 系统根据当前设备规格突出显示最佳级别。

步骤 3 查看您的选择和设备规格。

注释 配置 threat defense virtual VM 时，支持的 vCPU 最大核心数为 12（对于 VMware 和 KVM 上的 FTDv100，最大为 16）；支持的最大内存为 24 GB RAM。您选择的性能级别不应超过设备规格。

步骤 4 点击**是**更改性能级别。

启用或禁用可选许可证

您可以启用（注册）或禁用（解除）可选许可证。只有启用许可证后，才能使用该许可证控制的功能。

如果您不想再使用某个可选期限许可证包含的功能，可以禁用该许可证。禁用许可证会在思科智能软件管理器账户中将其释放，以便可将其应用到其他设备。

另外，在评估模式下运行时，还可启用这些许可证的评估版本。在评估模式下，只有注册设备，许可证才会注册到思科智能软件管理器。但是，您不能在评估模式下启用远程访问 RA VPN 或运营商许可证。

开始之前

在禁用许可证之前，请确保它不在使用中。重写或删除需要该许可证的任何策略。

对于在高可用性配置中运行的设备，只需在主用设备上上启用或禁用许可证。备用设备请求（或释放）必要许可证时，更改会在下一次部署配置时反映在备用设备上。启用许可证时，必须确保思科智能软件管理器账户具有足够的许可证，否则可能会造成一台设备合规，而另一台设备不合规。

过程

步骤 1 点击**设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 2 根据需要，点击每个可选许可证的**启用/禁用**控件。

- **启用** - 将许可证注册到您的思科智能软件管理器帐户，并启用控制的功能。现在，您可以配置和部署该许可证控制的策略了。
- **禁用** - 取消许可证向思科智能软件管理器帐户的注册，并禁用控制的功能。新策略中无法配置这些功能，也不能再部署使用该功能的策略。

步骤 3 如果启用 **RA VPN** 许可证，请选择您账户中可用的许可证类型。

与思科智能软件管理器同步

系统定期与思科智能软件管理器同步许可证信息。常规许可证通信每30天进行一次，但如果设备具有宽限期，则最多运行 90 天，而不会进行自动通报。

不过，如果您在思科智能软件管理器中进行更改，可以刷新设备上的授权，以使更改立即生效。

同步可获取许可证的当前状态，并更新授权和 ID 证书。

过程

步骤 1 点击**设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 2 从齿轮下拉列表中选择**重新同步连接**。

取消注册设备

如果您不想再使用设备，可以从思科智能软件管理器中将其取消注册。取消注册后，您的虚拟帐户将释放与该设备关联的基础版许可证和所有可选许可证。可选许可证可以分配给其他设备。此外，从云和云服务中取消注册该设备。

取消注册设备后，该设备中的当前配置和策略将继续按原样运行，但无法进行或部署任何更改。

开始之前

当取消注册一台设备时，只有该设备被取消注册。如果该设备已配置高可用性，那么您必须登录到高可用性对的另一台设备才能取消注册该设备。

过程

步骤 1 点击**设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 2 从齿轮下拉列表中选择**取消注册设备**。

步骤 3 如果确实要取消注册设备，请阅读警告并点击**取消注册**。

在气隙网络中应用永久许可证

气隙网络是指内部没有通往互联网的路径的网络。这些网络是高安全性网络，您希望在其中消除任何外部进入和攻击的可能性。由于没有通往互联网的路径，因此您无法直接在思科智能软件管理器中注册设备。但是，您可以使用永久许可证预留 (PLR) 模式来获取可应用于设备的许可证。

如果需要使用 PLR 模式，请注意以下几点：

- 需要接入互联网的功能（例如文件策略、URL 查找或对公共网站的上下文交叉启动）将无法工作。
- 即使您启用了网络分析和 Cisco Success Network，思科也不会由于缺少互联网访问权限而收集相关数据。
- 您需要手动上传地理位置数据库、入侵规则和漏洞数据库 (VDB) 的更新。例如，可以将更新下载到闪存，然后将闪存放入您的安全建筑物中，并从受保护的工作站上传更新。

注释 思科智能软件管理器使用设备序列号来分配永久许可证。如果您需要取消注册设备，并且正常的取消注册或取消过程无法删除许可证分配，则需要联系思科技术支持部门，以从思科智能软件管理器中删除注册。重新映像设备不会删除许可证注册。

以下主题详细介绍不同类型的永久许可证及其应用方式，以及如何取消注册或取消注册设备。

通用永久与特定许可证预留

有两种不同类型的许可证预留：

- 通用永久许可证预留（通用 PLR 或 UPLR）- 通用永久许可证允许永久无限制地使用受支持防火墙产品，其中包括所有可选许可证。在您购买并应用通用永久许可证后，任何已应用的功能许可证（通常是基于时间的许可证）都将永久适用。但是，智能许可证账户中的替换许可证到期时，您仍需购买替换许可证。
- 特定许可证预留-特定许可证预留需要与标准智能许可相同数量和类型的许可证。当您获取此许可证时，可以选择除基本许可证外的所需可选功能许可证。必须在许可证到期时定期更新许可证。

设备管理器 仅支持通用 PLR。

您必须与思科代表协作，在自己的思科智能软件管理器 (CSSM) 账户中启用“通用永久许可证预留”(PLR) 模式。

验证您的智能账户是否可以提供通用许可证

要验证您是否可以获取和应用永久许可证，请登录 CSSM 账户并转至**智能软件许可 (Smart Software Licensing)** > **清单 (Inventory)**页面，然后点击**许可证 (Licenses)** 选项卡。如果您可以看到**许可证预留**按钮，则表明您有权获取永久许可证预留。

但是，此按钮会启动一个同时适用于通用和特定永久许可证的向导。

您还必须完整查看可用许可证列表，以验证是否存在适用于设备的通用许可证。此许可证将在由**许可证预留**按钮启动的向导的第 2 步中显示为可选项。

如果您可以看到**许可证预留**按钮，并且可以获取通用许可证，则可以继续转换系统以使用永久许可证。如果未显示此按钮，或者您只能预留特定许可证，请致电您的思科代表，并请求为您的账户启用通用 PLR 模式。

切换到 PLR 模式并应用通用许可证

如验证您的智能账户是否可以提供通用许可证，第 89 页中所述，一旦您确认自己可以获取永久许可证并已购买所需的通用许可证，就可以切换到永久许可证预留 (PLR) 模式并应用许可证。

⚠

注意 如果您当前处于评估模式，则在切换到 PLR 模式后无法切换回评估模式。

开始之前

如果设备配置为具有高可用性，则必须为高可用性组中的两个设备单独完成此任务。

过程

步骤 1 点击**设备**，然后点击智能许可证摘要中的**查看配置**。

步骤 2 如果您已使用智能许可功能注册设备，请从齿轮⚙下拉列表中选择**取消注册设备**，然后确认取消注册。等待注销任务完成，然后再继续操作。

步骤 3 从齿轮⚙下拉列表中选择**切换到通用 PLR**，以切换到“通用永久许可证预留”(PLR) 模式。

阅读警告信息，然后点击**是**确认切换。

系统将转换为 PLR 模式，然后开始 PLR 注册过程。

步骤 4 完成 PLR 注册。

a) 当系统打开“通用永久许可证预留”对话框时，第一步中包括您将需要的请求代码。您可以点击**另存为 TXT** 将其保存在文本文件中，或点击**打印**将其打印出来。您还可以突出显示字符串，然后按 Ctrl+C 将字符串复制到剪贴板。

如果您在切换模式后取消进程，可以点击“许可”(Licensing) 页面上的**继续预留 (Continue Reservation)** 按钮来重启。

b) 登录您的 CSSM 账户，转到**智能软件许可 (Smart Software Licensing)** > **清单 (Inventory)**页面，然后点击**许可证 (Licenses)**选项卡。

c) 点击**许可证预留**按钮，然后按照向导中的说明进行操作。系统将提示输入您生成的请求代码，然后，您将获得授权码。

该向导包括以下步骤：

1. 输入许可证请求代码，或上传含代码的文本文件，然后点击**下一步**。
2. 在第 2 步中，系统将显示您将许可的系统的产品详细信息，以及可用许可证的项目符号列表。为本地管理的 威胁防御 设备选择通用许可证，然后点击 **下一步**。
3. 在第 3 步中，验证您是否选择了正确的许可证，然后点击**生成授权码**。
4. 在第 4 步中，系统将显示授权码。点击**下载为文件**或**复制到剪贴板**，以保存代码。
5. 点击**关闭**以退出向导。

d) 返回 设备管理器，将授权码粘贴到相应的字段中。

通用许可证的有效授权码的格式为 XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXX，其中 X 是字母数字字符。如果您的授权码是 XML 文件，则表示您具有特定许可证，并且不能在

此系统上使用该许可证。请如取消 PLR 注册，第 91 页中所述取消注册，以确保在 CSSM 中发布预留许可证。然后，与思科代表合作，将您的智能账户转换为通用 PLR。

e) 点击**注册**。

系统将开始注册过程。刷新“许可”(Licensing) 页面以检查注册状态。

步骤 5 根据需要启用可选功能许可证。

通用许可证仅为设备注册 基础版 许可证。现在，您可以为每个所需功能许可证点击**启用**。

取消 PLR 注册

在完成前，您可以取消“通用永久许可证预留 (PLR)”请求。例如，如果您启动 PLR 注册流程，并发现您的智能软件管理器账户未设置 PLR，则您可以在获得 PLR 模式的授权和适当设置智能许可证账户时取消此流程。

如果已完成 PLR 注册流程，则无法取消此流程。请参阅在 PLR 模式下取消注册设备，第 92 页。

过程

步骤 1 点击**设备**，然后点击智能许可证摘要中的**查看配置**。

步骤 2 从齿轮 下拉列表中选择**取消 PLR**，以开始取消流程。

步骤 3 选择适用于您的选项：

- **我在 CSSM 中有许可证** - 如果您已通过思科智能软件管理器 (CSSM) 中的许可证注册向导，并且已获得授权码，请使用此选项。此时，CSSM 中预留有许可证，您需要释放这些许可证。
- **我在 CSSM 中没有许可证** - 如果您在获取授权码时尚未完成 CSSM 向导，则使用此选项。例如，如果您在 设备管理器 中启动 PLR 注册，但随后发现您的智能账户中没有显示 **许可证预留** 按钮。

步骤 4 （如果已选择**我在 CSSM 中有许可证**。）您需要从 CSSM 获取释放码，以确保您的许可证不再被标记为正在使用。否则，其他设备将无法使用这些许可证。

a) 将您从 CSSM 获取的授权码（在注册时）粘贴到取消对话框，然后点击**生成释放码**。

b) 当**释放许可证代码**字段中有代码时，点击**另存为 TXT** 将其保存到文本文件，或点击**打印**进行打印。您还可以选择代码，然后按 Ctrl+C 将其复制到剪贴板。

c) 在 CSSM 中，在**智能软件许可 (Smart Software Licensing)** > **清单 (Inventory)** 页面中找到设备（名称是设备序列号），点击**操作 (Action)** > **删除 (Remove)**，然后输入释放码。

等待 CSSM 指示产品已成功删除。

步骤 5 点击**确定**完成取消流程。

系统将返回到“智能许可证”模式。但是，设备将被取消注册，并且您无法重启评估模式。此时，您必须使用智能许可证来注册设备，或切换回 PLR 模式并重新注册，才能使用该设备。

在 PLR 模式下取消注册设备

如果不再需要对设备进行许可（例如，因为要停用设备或将其移至另一个需单独许可的设备），则可以取消注册该设备。

取消注册设备时会将许可证恢复为未使用状态。如果不取消注册设备，许可证仍将标记为正在使用中，并且不能用于其他用途。

过程

步骤 1 点击**设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 2 从齿轮 下拉列表中选择**取消注册通用 PLR**，阅读警告信息，然后点击**是**开始此流程。

步骤 3 当“取消注册通用永久许可证预留”对话框打开时，系统将在**发布许可证代码**字段中填充您在发布 CSSM 账户中当前已分配许可证所需的代码。点击**另存为 TXT**，或点击**打印**以保留此代码的副本。您也可以选择此项并使用 Ctrl+C 将其复制到剪贴板。

步骤 4 转到您的 CSSM 账户，在**智能软件许可 (Smart Software Licensing)** > **清单 (Inventory)**页面中找到设备（“名称”(Name) 是设备序列号），点击**操作 (Action)** > **删除 (Remove)**，然后输入释放码。

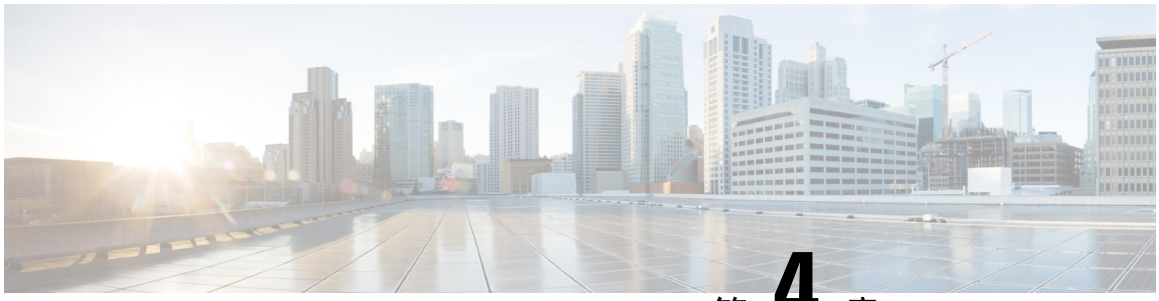
等待 CSSM 指示产品已成功删除。

步骤 5 返回 设备管理器，在“取消注册设备”对话框中点击 **取消注册** 。

由此，此过程便已完成。此时，CSSM 中的许可证可分配给其他设备，并且 威胁防御 设备未经许可。

第 部分

系统监控



第 4 章

监控设备

系统包括控制面板和事件查看器，通过它们可监控设备和通过设备传递的流量。

启用日志记录以获取流量统计信息

使用监控控制面板和事件查看器，可以监控各种流量统计信息。但是，必须启用日志记录才能告诉系统要收集哪些统计信息。日志记录生成各种类型的事件，有助于深入了解通过系统的连接。

以下主题详细介绍事件及其提供的信息，并特别强调连接日志记录。

事件类型

系统可以生成以下类型的事件。只有生成这些事件，才能在监控控制面板中查看相关统计信息。

连接事件

您可以在用户生成通过系统传递的流量时生成连接事件。启用访问规则连接日志记录以生成这些事件。还可启用安全智能策略和 SSL 解密规则日志记录，以生成连接事件。

连接事件包括有关连接的各种信息，包括源和目标 IP 地址及端口、使用的 URL 和应用，以及传输的字节数或数据包数。另外，还包括执行的操作（例如，允许或阻止连接）和应用于连接的策略的信息。

入侵事件

系统检查网络上传输的数据包是否存在可能影响主机及其数据的可用性、完整性和机密性的恶意活动。如果系统识别出潜在的入侵，会生成入侵事件；入侵事件是有关攻击源和攻击目标的日期、时间、攻击程序类型以及情境信息的记录。无论调用访问控制规则的日志记录配置如何，系统均会生成设为阻止或提醒的入侵规则的入侵事件。

文件事件

文件事件表示系统基于文件策略在网络流量中检测到或者被阻止的文件。只有在应用文件策略的访问规则中启用文件日志记录，才能生成这些事件。

无论调用访问控制规则采用何种日志记录配置，在系统生成文件事件时，都会记录相关连接的终止。

恶意软件事件

作为整体访问控制配置的一部分，系统可在网络流量内检测恶意软件。恶意软件防护可以生成恶意软件事件，其中包含生成事件的处置，有关检测该恶意软件的方式、位置和时间的情境数据。只有在应用文件策略的访问规则中启用文件日志记录，才能生成这些事件。

文件的处置可能发生变化，例如，从安全变为恶意软件或从恶意软件变为安全。如果 恶意软件防护 向 Cisco Secure Malware Analytics 云 查询文件，且云决定在查询一周内更改处置，系统即会生成追溯性恶意软件事件。

安全智能事件

安全智能事件是由安全智能策略为该策略阻止或监控的每个连接生成的一种连接事件。所有安全智能事件都有一个由系统填充的“安全智能类别”字段。

对于各事件，都有一个相应的“常规”连接事件。由于评估安全智能策略后才会评估许多其他安全策略（包括访问控制），所以当安全智能阻止连接时，所生成事件不含系统从后续评估中收集的信息（如用户身份）。

可配置的连接日志记录

您应该根据您组织的安全和合规性需求记录连接。如果您的目标是限制所生成事件的数量和提高性能，则只能启用对分析至关重要的连接的日志记录。然而，如果出于分析目的，您想要广泛了解网络流量，则可启用其他连接的日志记录。

由于系统可能会因为多种原因记录连接，因此禁用某一处的日志记录不能确保匹配连接不会被记录。

可在以下位置配置连接日志记录。

- 访问控制规则和默认操作 - 连接结束时的日志记录可提供有关连接的大多数信息。另外，您还可以记录连接开始信息，但这些事件的信息不完整。连接日志记录默认处于禁用状态，因此必须针对所要跟踪的流量的每个规则（和默认操作）启用该日志记录。
- 安全智能策略 - 可启用日志记录，为已阻止的各连接生成安全智能连接事件。当系统由于安全智能过滤而记录连接事件时，它也会记录匹配的安全智能事件（这是一种您可以单独查看和分析的特殊类型连接事件）。
- SSL 解密规则和默认操作 - 可在连接结束时配置日志记录。对于受阻连接，系统会立即结束会话并生成事件。对于受监控连接以及您将其传递到访问控制规则的连接，系统会在会话结束时生成事件。

自动连接日志记录

系统自动保存以下连接结束事件，而不管其他日志记录配置如何。

- 除非通过访问控制策略的默认操作来处理连接，否则系统会自动记录与入侵事件关联的连接。您必须在默认操作上启用日志记录以获取匹配流量的入侵事件。
- 系统会自动记录与文件和恶意软件事件关联的连接。这仅适用于连接操作：您可以选择禁止生成文件和恶意软件事件。

连接日志记录的提示

在考虑日志记录配置和评估相关统计信息时，请记住以下提示：

- 当您通过访问控制规则允许流量时，可以使用关联的入侵或文件策略（或同时使用这两种策略），在流量到达其最终目标前进一步检测流量并阻止入侵、禁止文件和恶意软件。不过请注意，对于加密负载，文件和入侵检测已默认禁用。如果入侵或文件策略需要阻止连接，系统将立即记录连接结束事件，而不考虑连接日志设置。允许日志记录的连接提供有关网络流量的大多数统计信息。
- 受信任连接是由信任访问控制规则或访问控制策略中的默认操作所处理的连接。但是，不会检测受信任连接中是否存在发现数据、入侵、禁止文件和恶意软件。因此，受信任连接的连接事件包含的信息有限。
- 对于阻止流量的访问控制规则和访问控制策略默认操作，系统将记录连接开始事件。匹配流量会被拒绝，无需进一步检测。
- 在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件使数据库不堪重负。在对“阻止”规则启用日志记录之前，请考虑该规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口上的流量。
- 如果在配置远程访问 VPN 连接配置文件时选择**为已解密的流量 (sysopt permit-vpn) 绕过访问控制策略**选项，或以其他方式启用 **sysopt connection permit-vpn** 命令，则所有的站点间或远程访问 VPN 流量将绕过检测和访问控制策略。因此，您将不会收到有关此流量的任何连接事件，且此流量也不会反映在任何统计控制面板中。

将事件发送至外部系统日志服务器

除了通过 设备管理器（其事件存储容量有限）查看事件外，还可以选择配置规则和策略以将事件发送至外部系统日志服务器。然后，可使用所选系统日志服务器平台的功能和附加存储查看和分析事件数据。

要将事件发送至外部系统日志服务器，请编辑启用连接日志记录的各规则、默认操作或策略，并在日志设置中选择系统日志服务器对象。要将入侵事件发送到系统日志服务器，请在入侵策略设置中配置服务器。要将文件/恶意软件事件发送到系统日志服务器，请在**设备** > **系统设置** > **日志记录设置**中配置服务器。

有关更多信息，请参阅各规则和策略类型的帮助，另请参阅配置系统日志服务器，第 138 页。

使用思科基于云的服务来评估事件

除了使用事件查看器和自身的系统日志服务器，还可以向思科基于云的服务器发送连接事件、高优先级入侵、文件和恶意软件事件。思科基于云的服务（例如威胁响应）可以从该云服务器提取事件，然后可以使用这些服务来评估这些事件。

这些基于云的服务独立于 威胁防御 设备和 设备管理器。如果选择使用要求将这些事件发送至 Cisco 云的服务，则必须在 **设备 (Device)** > **系统设置 (System Settings)** > **云服务 (Cloud Services)** 页面上启用该连接。请参阅将事件发送至思科云，第 752 页。

监控流量和系统控制面板

系统包括多个控制面板，它们可用来分析通过设备传递的流量和安全策略的结果。使用这些信息可评估您的配置的总体效率，识别和解决网络问题。

高可用性组中设备的控制面板仅显示该设备的统计信息。统计信息不会在设备之间同步。

注释 流量相关的控制面板中使用的数据基于访问控制规则进行收集，该规则实现连接或文件日志记录以及允许日志记录的其他安全策略。控制面板不会反映匹配未启用日志记录的规则的流量。请确保配置规则以记录对您重要的信息。另外，只有配置了身份规则来收集用户身份，才能获得用户信息。最后，只有拥有入侵、文件、恶意软件和URL类别功能的许可证，并配置了使用这些功能的规则，才能获得这些功能的相关信息。

过程

步骤 1 在主菜单中点击**监控 (Monitoring)**，打开“控制面板”(Dashboards) 页面。

您可以选择预定义的时间范围（例如前一小时或上周），也可以使用特定开始和结束时间自定义时间范围，以便控制控制面板图形和表格中所示的数据。

流量相关的控制面板包括以下显示类型：

- 前 5 个条形图 - 这些图形显示在**网络概况**控制面板中，以及点击控制面板表中的项目时看到的各项目的摘要控制面板中。您可以在**事务**数或**数据使用量**（收发的总字节数）之间切换信息。另外，还可以切换显示屏以显示所有事务、允许的事务或拒绝的事务。点击**查看更多**链接可查看与该图相关的表格。
- 表格 - 表格显示特定类型的项目（例如，应用或 URL 类别）及该项目的事务总数、允许的事务、阻止的事务、数据使用量和收发的字节数。您可以在原始**值**和**百分比**之间切换数字，并显示前 10、100 或 1000 个条目。如果项目是链接，点击该链接可查看摘要控制面板及更多详细信息。

步骤 2 点击目录中的**控制面板**链接，可查看以下数据的控制面板：

- **网络概况** - 显示有关网络流量的摘要信息，包括匹配的访问规则（策略）、发起流量的用户、连接中使用的应用、匹配的入侵威胁（签名）、所访问 URL 的 URL 类别和连接最常访问的目标。
- **用户** - 显示网络的热门用户。只有配置身份策略，才能查看用户信息。如果没有用户身份，则包含源 IP 地址。您可能会看到以下特殊实体：
  - **身份验证失败** - 系统提示用户进行身份验证，但用户未在允许的最大尝试次数内输入有效的用户名/密码对。身份验证失败本身不会阻止用户访问网络，但您可以写入访问规则来限制这些用户访问网络。
  - **访客** - “访客”用户与“身份验证失败”用户类似，只是您的身份规则配置为将这些用户称为“访客”。系统提示“访客”用户进行身份验证，但他们在最大尝试次数内未成功通过身份验证。
  - **无需身份验证** - 系统不提示用户进行身份验证，因为该类用户的连接与指定不进行身份验证的身份规则匹配。
  - **未知** - 没有用户的 IP 地址映射，也没有身份验证失败的记录。通常，这意味着尚无来自该地址的 HTTP 流量。
- **应用** - 显示网络中使用的热门应用，例如 Facebook。只有检测连接，才能获得这些信息。只有连接匹配“允许”规则或使用区域、地址和端口之外条件的“阻止”规则时，才会对它们进行检测。因此，在触发需要检测的任何规则之前，如果该连接受信任或被阻止，则无法获得应用信息。
- **Web 应用** - 显示网络中使用的热门 Web 应用，例如 Google。收集 Web 应用信息的条件与“应用”控制面板的条件相同。
- **URL 类别** - 基于所访问网站的分类，显示网络中使用的热门网站类别，例如博彩或教育机构。要获得这些信息，必须至少设置一条以URL类别为流量匹配条件的访问控制规则。对于匹配该规则的流量，或必须检测以确定是否匹配该规则的流量，可以获得此方面的相关信息。而对于匹配第一个 Web 类别访问控制规则之前规则的连接，则不会看到它们的类别（或信誉）信息。
- **访问和 SI 规则** - 显示热门访问规则和安全智能规则（与网络流量匹配的对应项目）。
- **区域** - 显示用于进出设备的流量的热门安全区对。
- **目的** - 显示网络流量排名靠前的目的。
- **攻击者** - 显示排名靠前的攻击者，即触发入侵事件的连接源。只有在访问规则中配置入侵策略，才能查看这些信息。
- **目标** - 显示入侵事件排名靠前的目标，即攻击的受害者。只有在访问规则中配置入侵策略，才能查看这些信息。
- **威胁** - 显示已触发的排名靠前的入侵规则。只有在访问规则中配置入侵策略，才能查看这些信息。
- **文件日志** - 显示网络流量中发现的排名靠前的文件类型。只有在访问规则中配置文件策略，才能查看这些信息。

- **恶意软件** - 显示热门恶意软件操作和处置组合。您可以详细了解相关文件类型的信息。只有在访问规则中配置文件策略，才能查看这些信息。
  - 可能的操作包括：恶意软件云查找、阻止、存档阻止（加密）、检测、自定义检测、云查找超时、恶意软件阻止、存档阻止（已超出深度）、自定义检测阻止、TID 阻止、存档阻止（检测失败）。
  - 可能的处置包括：恶意软件、未知、安全、自定义检测、不可用。
- **SSL 解密** - 显示通过设备的加密与纯文本流量的细分以及根据 SSL 解密规则解密加密流量方法的细分。
- **系统** - 显示整个系统视图，包括接口及其状态（将鼠标悬停在接口上，查看其 IP 地址）、总平均系统吞吐量（一小时内的时间以 5 分钟存储桶为单位，一小时以上的时间以一小时存储桶为单位）、有关系统事件以及 CPU、内存和磁盘的使用情况的摘要信息。您可以将吞吐量图形限制为显示特定接口（而非所有接口）的吞吐量。

  注释 “系统”控制面板所示的信息为整个系统的相关信息。如果登录到设备 CLI，您可以使用各种命令来查看更多详细信息。例如，**show cpu** 和 **show memory** 命令包括用于显示其他详细信息的参数，而这些控制面板显示来自 **show cpu system** 和 **show memory system** 命令的数据。

步骤 3 另外，您还可以点击目录中的这些链接：

- **事件** - 查看发生的事件。只有在各个访问规则中启用连接日志记录，才能查看与这些规则相关的连接事件。此外，在安全智能策略和 SSL 解密规则中启用日志记录，以查看安全智能事件和其他连接事件数据。这些事件可以帮助您解决用户的连接问题。
- **会话**- 查看和管理 设备管理器 用户会话。有关详细信息，请参阅 管理设备管理器用户会话，第 789 页。

使用命令行监控更多统计信息

设备管理器 控制面板提供与通过设备的流量和一般系统使用情况相关的各种统计信息。但是，您可以使用 CLI 控制面板或登录设备 CLI 获取控制面板未涵盖方面的其他信息（请参阅登录命令行界面 (CLI)，第 7 页）。

CLI 包含各种 **show** 命令，可用来提供这些统计信息。您还可以使用 CLI 进行常规故障排除，包括 **ping** 和 **traceroute** 等命令。大多数 **show** 命令都与 **clear** 命令结合使用，用于将统计信息重置为 0。（无法从 CLI 控制台清除统计信息。）

您可以在Cisco Firepower Threat Defense 命令参考(http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html) 中查找有关这些命令的文档。

例如，您会发现以下较常用的命令。

- **show nat** 显示您的 NAT 规则的命中计数。
- **show xlate** 显示处于活动状态的实际 NAT 转换。
- **show conn** 提供当前通过设备的连接的相关信息。
- **show dhcpd** 提供您在接口上配置的 DHCP 服务器的相关信息。
- **show interface** 提供每个接口的使用统计信息。

查看事件

您可以查看启用日志记录的安全策略中生成的事件。另外，也可为触发的入侵策略和文件策略生成事件。

事件查看器表格可实时显示生成的事件。有新事件生成时，旧事件将退出表格。

开始之前

除了连接匹配相关策略外，是否会生成特定类型的事件还取决于以下事件：

- 连接事件 - 访问规则必须启用连接日志记录。此外还可以在安全智能策略和 SSL 解密规则中启用连接日志记录。
- 入侵事件 - 访问规则必须应用入侵策略。
- 文件和恶意软件事件 - 访问规则必须执行文件策略并启用文件日志记录。
- 安全智能事件 - 必须启用和配置安全智能策略，并启用日志记录。

过程

步骤 1 点击主菜单中的**监控**。

步骤 2 从目录中选择**事件**。

事件查看器将基于事件类型在选项卡中组织事件。有关详细信息，请参阅事件类型，第 95 页。

步骤 3 点击显示您要查看的事件类型的选项卡。

您可以对事件列表执行以下操作：

- 点击**暂停**以停止添加新事件，这样即可更加轻松地查找和分析事件。点击**继续**以允许显示新事件。
- 选择不同的刷新率（5 秒、10 秒、20 秒或 60 秒）以控制新事件的显示速度。
- 创建包含所需列的自定义视图。要创建自定义视图，请点击选项卡栏中的 + 按钮，或点击**添加/删除列**。无法更改预设的选项卡，所以添加或删除列将会创建新视图。有关详细信息，请参阅配置自定义视图，第 102 页。

- 要更改列的宽度，请点击列标题并将列标题分隔符拖动至所需的宽度。
- 将鼠标悬停在某个事件上方，点击**查看详细信息**可查看该事件的完整信息。有关事件中各个字段的描述，请参阅事件字段说明，第 104 页。

步骤 4 如果需要，对表格应用过滤器，以协助您基于各种事件属性找到所需的事件。

要创建新过滤器，请通过从下拉列表中选择原子元素，手动键入过滤器；也可以点击事件表格中包括要基于其过滤的值的单元格，构建一个过滤器。您可以点击同一列中的多个单元格，在这些值之间创建 OR 条件；也可以点击不同列的单元格，在列之间创建 AND 条件。如果通过点击单元格构建过滤器，还可以编辑生成的过滤器对其微调。有关创建过滤器规则的详细信息，请参阅过滤事件，第 103 页。

在构建过滤器后，执行以下任一操作：

- 要应用过滤器和更新表格以仅显示匹配过滤器的事件，请点击**过滤器**按钮。
- 要清除您应用的整个过滤器并使表返回未过滤状态，请点击**过滤器**框中的**重置过滤器**。
- 要清除过滤器中的某个原子元素，请将鼠标悬停在该元素上方，并点击该元素的 **X**。然后，点击**过滤器**按钮。

配置自定义视图

您可以创建自己的自定义视图，这样即可在查看事件时轻松地查看所需的列。另外，还可以编辑或删除自定义视图，但无法编辑或删除预定义的视图。

过程

步骤 1 依次选择**监控** > **事件**。

步骤 2 执行以下操作之一：

- 要基于现有自定义（或预定义）视图创建新视图，请点击该视图的选项卡，然后点击选项卡左侧的 + 按钮。
- 要编辑现有的自定义视图，请点击该视图的选项卡。

注释 要删除自定义视图，只需点击该视图选项卡中的 **X** 即可。删除无法撤消。

步骤 3 点击右侧事件表上方的**添加/删除列 (Add/Remove Columns)** 链接，选择或取消选择列，直到选定列表中仅包含要包含在视图中的列为止。

点击列，并在可用（但未使用）列表和选定列表之间拖动它们。另外，您还可以点击和拖动选定列表中的列，以更改表格中从左至右的列顺序。有关列的描述，请参阅事件字段说明，第 104 页。

完成后，点击**确定 (OK)** 以保存列更改。

注释 如果在查看预定义视图时更改列选项，将会创建一个新视图。

步骤 4 如果需要，点击和拖动列分隔符可更改列宽。

过滤事件

您可以创建复杂过滤器，将事件表格限制为您当前感兴趣的事件。您可以单独或组合使用以下方法来构建过滤器：

点击列

要构建过滤器，最简单的方法就是点击事件表格中包含要基于其过滤的值的单元格。点击单元格会用为该值和字段组合正确设定的规则更新**过滤器**字段。但是，使用此方法要求现有的事件列表中包含所需的值。

不能基于所有列执行过滤。如果可基于某个单元格的内容过滤，将鼠标悬停在该单元格上方时，它将显示下划线。

选择原子元素

另外，您还可以构建过滤器，具体方法为：点击**过滤器**字段，从下拉列表中选择所需的原子元素，然后再键入匹配值。这些元素包括在事件表格中未作为列显示的事件字段。另外，还包括定义您键入的值和要显示的事件之间关系的操作符。而点击列总会生成“equals (=)”过滤器，在选择元素时，还可以对数值字段选择“大于 (>)”或“小于 (<)”。

无论采用何种方式在**过滤器**字段中添加元素，均可通过在该字段中键入信息来调整操作符或值。点击**过滤器**可将过滤器应用于表格。

事件过滤器的操作符

在事件过滤器中可以使用以下操作符：

=	等于。该事件与指定值匹配。不能使用通配符。
!=	不等于。该事件与指定值不匹配。要构建不等表达式，必须键入！（感叹号）。
>	大于。该事件包含大于指定值的值。此操作符仅可用于数值，例如端口和IP地址。
<	小于。该事件包含小于指定值的值。此操作符仅可用于数值。

复杂事件过滤器的规则

在构建包含多个原子元素的复杂过滤器时，请记住以下规则：

- 相同类型的元素在该类型的所有值之间具有 OR 关系。例如，“包括发起方 IP=10.100.10.10”和“发起方 IP=10.100.10.11”与包含其中任一地址作为流量源的事件匹配。
- 不同类型的元素之间为 AND 关系。例如，“包括发起方 IP=10.100.10.10”和“目标端口/ICMP 类型=80”与仅包含此源地址 AND 目标端口的事件匹配。不显示从 10.100.10.10 传至不同目标端口的事件。

- 数值元素（包括IPv4和IPv6地址）可以指定范围。例如，您可以指定“目标端口=50-80”，以捕获此范围内端口的所有流量。使用连字符分隔开始和结束编号。并不是所有数值字段均可使用范围，例如在源元素中无法指定 IP 地址范围。
- 不能使用通配符或正则表达式。

事件字段说明

事件可包含以下信息。在查看事件详细信息时可以看到这些信息。另外，您还可以向事件查看器表格中添加列，以显示您最感兴趣的信息。

下面是可用字段的完整列表。并不是每个字段都适用于每种事件类型。请记住，任何单独事件的可用信息视系统记录连接的方式、原因和时间而异。

操作

对于连接或安全智能事件，与记录连接的访问控制规则关联的操作或默认操作：

允许

明确允许的连接。

信任

受信任的连接。信任规则在第一个数据包上检测到的TCP连接仅生成连接结束事件。系统将在最终会话数据包发送完毕 1 小时后生成事件。

阻止

阻止的连接。在以下条件下，**阻止**操作可与“允许”访问规则相关联：

- 某个攻击程序漏洞被入侵策略阻止的连接。
- 某个文件被文件策略阻止的连接。
- 被安全智能阻止的连接。
- 被 SSL 策略阻止的连接。

默认操作

连接按默认操作处理。

对于文件或恶意文件事件，与文件所匹配规则的规则操作相关联的文件规则操作，以及任何关联的文件规则操作选项。

允许的连接

系统是否允许事件的流量通过。

应用

在连接中检测到的应用。

应用业务相关性

与连接中检测到的应用流量关联的业务相关性：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类应用都有相关业务相关性；该字段显示级别最低的业务相关性。

应用类别、应用标记

展示了应用特征的条件条件，协助您了解应用功能。

应用风险

与连接中检测到的应用流量关联的风险：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类应用都有一个相关风险；该字段显示最高风险。

阻止类型

在与事件中的流量匹配的访问控制规则中指定的与事件中的流量匹配的阻止类型：阻止或交互式阻止。

客户端应用、客户端版本

在连接中检测到的客户端应用及版本。

客户端业务相关性

与连接中检测到的客户端流量关联的业务相关性：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类客户端都有相关的业务相关性；该字段显示级别最低（最不相关）的业务相关性。

客户端类别、客户端标记

展示了应用特征的条件条件，协助您了解应用功能。

客户端风险

与连接中检测到的客户端流量关联的风险：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类客户端都有一个相关风险；该字段显示最高风险。

连接

内部产生的流量的唯一 ID。

连接阻止类型指示器

在与事件中的流量匹配的访问控制规则中指定的与事件中的流量匹配的阻止类型：阻止或交互式阻止。

连接字节数

连接的总字节数。

连接时间

连接开始的时间。

连接时间戳

检测到连接的时间。

拒绝的连接

系统是否已拒绝事件的流量通过。

目标国家/地区和大洲

接收主机所在的国家/地区和大洲。

目标 IP

入侵、文件或恶意软件事件中的接收主机使用的 IP 地址。

目标端口/ICMP 代码；目标端口；目标 Icode

会话响应方使用的端口或 ICMP 代码。

目标安全组标记、目标安全组标记名称

与目标关联的 TrustSec 安全组标记编号和名称（如有）。

方向

文件传输的方向。

处置

文件的处置：

恶意软件

表示 Cisco Secure Malware Analytics 云 将文件归类为恶意软件，或文件威胁评分超过文件策略定义的恶意软件阈值。本地恶意软件分析也可以将文件标记为恶意软件。

干净

表示 Cisco Secure Malware Analytics 云 将文件分类为干净，或用户将文件添加到干净列表。

未知

表示系统已查询 Cisco Secure Malware Analytics 云，但文件尚未被分配处置情况；换句话说， Cisco Secure Malware Analytics 云 尚未对文件进行分类。

自定义检测

表示用户将文件添加到自定义检测列表。

不可用

表示系统无法查询 Cisco Secure Malware Analytics 云。您可能看到很少一部分事件为此处置；这是预期行为。

不适用

表示“检测文件”或“阻止文件”规则处理了文件，系统未查询 Cisco Secure Malware Analytics 云。

传出接口、传出安全区

连接离开设备所通过的接口和区域。

出口虚拟路由器

目标接口所属的虚拟路由器（如有）名称。

事件、事件类型

事件的类型。

事件秒数、事件微秒数

检测到事件的时间（秒或微秒）。

文件类别

文件类型的一般类别，例如：Office 文档、存档、多媒体、可执行文件、PDF 文件、编码文件、图形或系统文件。

文件事件时间戳

文件或恶意软件文件的创建时间和日期。

文件名

文件名称。

文件规则操作

检测文件的文件策略规则的相关操作以及任何相关文件规则操作选项。

文件 SHA-256

文件的 SHA-256 散列值。

文件大小 (KB)

文件大小（千字节）。如果文件在完全接收前被系统阻止，文件大小可能为空。

文件类型

文件类型，例如 HTML 或 MSEXE。

文件/恶意软件策略

与事件生成相关的文件策略。

文件日志阻止类型指示器

在与事件中的流量匹配的文件规则中指定的与事件中的流量匹配的阻止类型：阻止或交互式阻止。

防火墙策略规则、防火墙规则

处理连接的访问控制规则或默认操作。

首个数据包

查看会话的第一个数据包的日期和时间。

HTTP 来源地址

HTTP 来源地址，表示在连接中检测到的 HTTP 流量的请求 URL 来源地址（例如提供到另一个 URL 的链接或从其导入链接的网站）。

HTTP 响应

发送的 HTTP 状态代码用于响应客户端通过连接的 HTTP 请求。

IDS 分类

生成事件的规则所属的分类。

传入接口、传入安全区

连接进入设备所通过的接口和区域。

入口虚拟路由器

源接口所属的虚拟路由器（如有）名称。

发起方字节、发起方数据包

会话发起方发送的总字节数或数据包总数。

发起方国家/地区和大洲

发起会话的主机所在的国家/地区和大洲。只有发起方的 IP 地址可路由，方可用。

发起方 IP

在连接或安全智能事件中发起会话的主机 IP 地址（以及主机名，如果已启用 DNS 解析）。

内联结果

系统是否丢弃或本可丢弃触发入侵事件的数据包（如果在内联模式下操作）。空白表示触发的规则未被设置为“丢弃并生成事件”

入侵策略

启用了生成事件的规则的入侵策略。

IPS 阻止类型指示器

与事件中的流量匹配的入侵规则的操作。

最后一个数据包

查看会话的最后一个数据包的日期和时间。

MPLS 标记

与触发此入侵事件的数据包相关的多协议标记交换标记。

恶意软件阻止类型指示器

在与事件中的流量匹配的文件规则中指定的与事件中的流量匹配的阻止类型：阻止或交互式阻止。

消息

对于入侵事件，事件的解释性文本。对于恶意软件或文件事件而言，与恶意软件事件相关的任何其他信息。

NAT 目标 IP

对于接受网络地址转换 (NAT) 的数据包，为转换后的目标 IP 地址。

NAT 目标端口

对于接受网络地址转换 (NAT) 的数据包，为转换后的目标端口。

NAT 源 IP

对于接受网络地址转换 (NAT) 的数据包，为转换后的源 IP 地址。

NAT 源端口

对于接受网络地址转换 (NAT) 的数据包，为转换后的源端口。

NetBIOS 域

会话中使用的 NetBIOS 域。

原始客户端国家/地区和大洲

发起会话的原始客户端所在的国家/地区和大洲。只有原始客户端的 IP 地址可路由，方可用。

原始客户端 IP

发起 HTTP 连接的客户端的原始 IP 地址。此地址由 X-Forwarded-For (XFF) 或 True-Client-IP HTTP 报头字段或其对应项目派生。

策略、策略版本

访问控制策略及其版本，包括与事件相关的访问（防火墙）规则。

优先级

由 思科 Talos 情报小组 (Talos) 确定的事件优先级：高、中或低。

协议

连接中使用的传输协议。

原因

各种情况下的连接记录原因如下表所述。否则该字段为空。

原因	说明
DNS 阻止	系统未经检查就根据域名和安全情报数据拒绝连接。“DNS 阻止”原因与“阻止”、“找不到域”或 Sinkhole 操作匹配，具体取决于 DNS 规则操作。
DNS 监控	系统将根据域名和安全情报数据拒绝连接，但您将系统配置为监控而不是拒绝连接。

原因	说明
大象流	连接速率大到足以被认为是大象流，这种流的大小足以影响整体系统性能。默认情况下，大象流是速率大于每 10 秒 1GB 的流。您可以使用 **system support elephant-flow-detection** 命令调整字节和时间阈值，以在设备 CLI 中识别大象流。
文件阻止	连接中包含系统禁止传输的文件或恶意软件文件。“文件阻止”原因始终与“阻止”操作匹配。
文件自定义检测	连接中包含自定义检测列表上系统禁止传输的文件。
文件监控	系统在连接中检测到特定类型的文件。
允许继续传输文件	文件传输最初被“阻止文件”或“阻止恶意软件”文件规则阻止。在部署允许该文件的新访问控制策略之后，将自动继续 HTTP 会话。
阻止继续传输文件	“检测文件”或“恶意软件云查找”文件规则最初允许文件传输。在新访问控制策略阻止文件部署之后，会自动停止 HTTP 会话。
入侵阻止	系统阻止或本可阻止在连接中检测到的漏洞（入侵策略违规）。“入侵阻止”原因与用于阻止漏洞的“阻止”操作和用于本可阻止漏洞的“允许”操作匹配。
入侵监控	系统检测到但并未阻止连接中检测到的漏洞。当触发的入侵规则状态设置为“生成事件”时，即会发生这种情况。
IP 阻止	系统未经检查就根据 IP 地址和安全情报数据拒绝连接。“IP 阻止”原因始终与“阻止”操作匹配。
SSL 阻止	系统基于 SSL 检查配置阻止加密连接。“SSL 阻止”原因始终与“阻止”操作匹配。
URL 阻止	系统未经检查就根据 URL 和安全情报数据拒绝连接。“URL 阻止”原因始终与“阻止”操作匹配。

接收时间

事件生成的日期和时间。

引用的主机

如果连接中的协议是 HTTP 或 HTTPS，此字段显示各自协议使用的主机名。

响应方字节、响应方数据包

会话响应方发送的总字节数或数据包总数。

响应方国家/地区和大洲

响应会话的主机所在的国家/地区和大洲。只有响应方的 IP 地址可路由，方可用。

响应方 IP

连接或安全智能事件中的会话响应者主机 IP 地址（以及主机名，如果已启用 DNS 解析）。

SI 类别 ID（安全智能类别）

包含被阻止项的对象的名称，例如网络或 URL 对象名称，或智能源类别名称。

签名

文件/恶意软件事件的签名 ID。

源国家/地区和大洲

发送主机所在的国家/地区和大洲。只有源 IP 地址可路由，方可用。

源 IP

入侵、文件或恶意软件事件中的发送主机使用的 IP 地址。

源端口/ICMP 类型；源端口；源端口 Itype

会话发起方使用的端口或 ICMP 类型。

源安全组标记、源安全组标记名称

与源关联的 TrustSec 安全组标记编号和名称（如有）。

SSL 实际操作

系统应用于连接的实际操作。此操作可能与预期操作不同。例如，连接可能与应用解密的规则匹配，但出于某些原因不能被解密。

操作	说明
阻止/阻止并重置	表示阻止的加密连接。
解密（重新签名）	表示使用重新签名的服务器证书解密的传出连接。
解密（替换密钥）	表示使用具有替代公钥的自签名服务器证书解密的传出连接。
解密（已知密钥）	表示使用已知私钥解密的传入连接。
默认操作	表示连接采用默认操作处理。
不解密	表示系统未解密的连接。

SSL 证书指纹

用于验证证书的 SHA 散列值。

SSL 证书状态

仅在配置了证书状态规则条件时，此字段才适用。如果加密流量与 SSL 规则匹配，则此字段显示以下一个或多个服务器证书状态值：

- 自签名
- 有效
- 无效签名
- 无效颁发者
- 已到期
- 未知
- 无效
- 已撤销

如果无法解密的流量与 SSL 规则相匹配，则此字段显示“未检查”。

SSL 加密套件

连接中使用的加密套件。

SSL 预期操作

连接匹配的 SSL 规则中指定的操作。

SSL 流标志

已加密连接的前十大调试级别标记。

SSL 流信息

在 SSL 握手期间客户端与服务器之间交换的 SSL/TLS 消息，例如 HELLO_REQUEST 和 CLIENT_HELLO。有关 TLS 连接中交换的消息的详细信息，请参阅 http://tools.ietf.org/html/rfc5246。

SSL 策略

应用于连接的 SSL 解密策略的名称。

SSL 规则

应用于连接的 SSL 解密规则的名称。

SSL 会话 ID

在 SSL 握手期间，在客户端与服务器之间协商的十六进制会话 ID。

SSL 通知单 ID

在 SSL 握手期间发送的会话单信息的一个十六进制散列值。

SSL URL 类别

SSL 解密处理过程中确定的目标 Web 服务器的 URL 类别。

SSL 版本

连接中使用的 SSL/TLS 版本。

TCP 标志

在连接中检测到的 TCP 标记。

数据包总数

在连接中传输的数据包总数，即**发起方数据包** + **响应方数据包**。

URL、**URL 类别**、**URL 信誉**、**URL 信誉评分**

会话期间受控主机请求的 URL 以及 URL 类别、信誉和信誉评分（如有）。

对于 DNS 查找请求过滤，类别和信誉用于 DNS 查询字段中显示的 FQDN。URL 字段将为空，因为正在为 DNS 请求而不是 Web 请求执行类别/信誉查找。

如果系统识别或阻止 SSL 应用，而请求的 URL 位于加密流量中，系统会基于 SSL 证书识别流量。因此，对于 SSL 应用，URL 表示包含在证书中的通用名称。

用户

与发起方 IP 地址关联的用户。

VLAN

与触发事件的数据包相关的最内部的 VLAN ID。

Web 应用业务相关性

与连接中检测到的 Web 应用流量相关的业务相关性：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类网络应用都有相关的业务相关性；该字段显示级别最低（最不相关）的业务相关性。

Web 应用类别、**Web 应用标记**

展示了 Web 应用特征的条件条件，协助您了解 Web 应用功能。

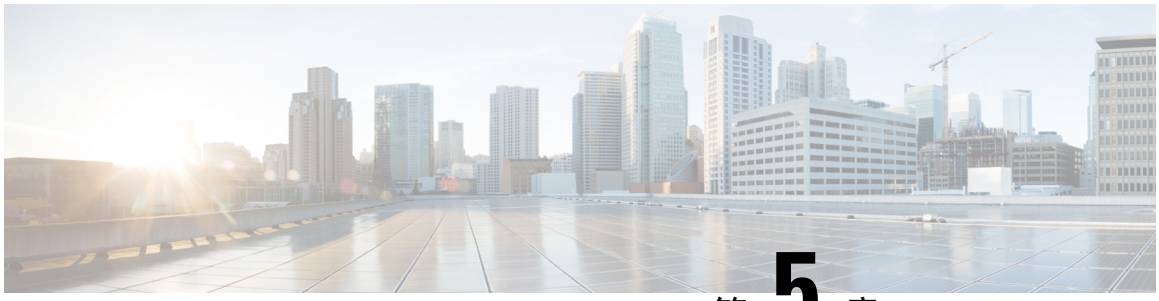
Web 应用风险

与连接中检测到的 Web 应用流量关联的风险：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类 Web 应用都有一个相关风险；该字段显示最高风险。

Web 应用

表示连接中检测到的 HTTP 流量内容或请求的 URL 的 Web 应用。

如果 Web 应用不匹配事件的 URL，该流量大概是推荐流量，例如广告流量。如果系统检测到推荐流量，则会存储该推荐应用（如有），并将该应用列为 Web 应用。



第 5 章

思科 ISA 3000 的报警

您可以配置思科 ISA 3000 设备上的报警系统，以便在出现不正常情况时发出警告。

关于报警

您可以将 ISA 3000 配置为在多种条件下发出报警。如果有任何条件与配置的设置不匹配，系统会触发报警，报警的报告方式为 LED、系统日志消息、SNMP 陷阱以及连接到报警输出接口的外部设备。默认情况下，触发的报警仅会发出系统日志消息。

您可以将报警系统配置为监控以下对象：

- 电源。
- 主温度传感器和辅助温度传感器。
- 报警输入接口。

ISA 3000 具有内部传感器、2 个报警输入接口以及 1 个报警输出接口。您可以将外部传感器（如门禁传感器）连接到报警输入接口，将外部报警设备（如蜂鸣器或指示灯）连接到报警输出接口。

报警输出接口是一个中继装置。根据报警条件，中继处于连接或断开状态。当处于连接状态时，连接至该接口的任何设备都将被激活。当中继处于断开状态时，会导致连接的任何设备都处于非活动状态。只要触发了报警，中继就会保持连接状态。

有关连接外部传感器和报警中继装置的信息，请参阅思科 ISA 3000 工业安全设备硬件安装指南。

报警输入接口

您可以将报警输入接口（或触点）连接到外部传感器，例如检测门是否打开的传感器。

每个报警输入接口都有一个对应的LED。这些LED负责传达每个报警输入的报警状态。您可以为每个报警输入配置触发器和严重性。除了 LED，您还可以配置触点来触发输出中继（用于激活外部报警），以发送系统日志消息和 SNMP 陷阱。

下表介绍与报警输入的报警条件所对应的LED状态。表中还介绍了启用这些报警输入响应时输出中继、系统日志消息和 SNMP 陷阱的行为。

报警状态	LED	输出中继	系统日志	SNMP 陷阱
未配置报警	关闭	—	—	—
未触发任何报警	绿灯常亮	—	—	—
已激活报警	次要报警 - 红色长亮 重大报警 - 红色闪烁	中继已通电	生成系统日志	发送 SNMP 陷阱
报警结束	绿灯常亮	继电器断电	生成系统日志	—

报警输出接口

您可以将外部报警（如蜂鸣器或灯光）连接到报警输出接口。

报警输出接口充当一个中继，并且还有一个对应的 LED，用于传达连接到输入接口的外部传感器以及内部传感器（例如双电源和温度传感器）的报警状态。请配置哪些报警应该激活输出中继（如果有）。

下表介绍与报警条件对应的LED和输出中继的状态。表中还介绍了启用这些报警响应时系统日志消息和 SNMP 陷阱的行为。

报警状态	LED	输出中继	系统日志	SNMP 陷阱
未配置报警	关闭	—	—	—
未触发任何报警	绿灯常亮	—	—	—
已激活报警	红色常亮	中继已通电	生成系统日志	发送 SNMP 陷阱
报警结束	绿灯常亮	继电器断电	生成系统日志	—

系统日志报警

默认情况下，触发任何报警时，系统都会发送系统日志消息。如果您不希望收到这些消息，可以禁用系统日志消息传递。

要使系统日志报警正常工作，您还必须在**设备** > **系统设置** > **日志记录设置**上启用诊断日志记录。配置系统日志服务器、控制台日志记录或内部缓冲区日志记录。

如果未启用诊断日志记录的目标，报警系统不清楚向何处发送系统日志消息。

SNMP 陷阱报警

您可以选择配置报警，将 SNMP 陷阱发送到 SNMP 服务器。要让 SNMP 陷阱报警正常使用，您还必须配置 SNMP 设置。

使用 威胁防御 API 配置 SNMP。点击“更多选项”按钮 (⋮) 并选择 API Explorer。然后，查找 SNMP 资源并查看型号文档，了解有关如何配置此功能的信息。您可以使用 SNMP 版本 2c 或 3；不支持版本 1。有关配置 SNMP 的完整信息，请参阅最新版本 ASA 软件的《*CLI* 手册 *1*：思科 *ASA* 系列常规操作 *CLI* 配置指南》中的 SNMP 章节。指南位置为 https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html。

报警默认值

下表指定了报警输入接口（触点）、冗余电源和温度的默认值。

	警报	触发	严重性	SNMP 陷阱	输出中继	系统日志消息
报警触点 1	启用	关闭状态	次要	Disabled	已禁用	已启用
报警触点 2	启用	关闭状态	次要	Disabled	已禁用	已启用
冗余电源（在启用时）	启用	—	—	Disabled	已禁用	已启用
温度	为主温度报警启用（高阈值和低阈值的默认值分别为 92°C 和 -40°C） 为辅助报警禁用。	—	—	为主温度报警启用	为主温度报警启用	为主温度报警启用

为 ISA 3000 配置报警

请使用 FlexConfig 为 ISA 3000 配置报警。以下主题介绍如何配置不同类型的报警。

配置报警输入触点

如果您将报警输入触点（接口）连接到外部传感器，可以将触点配置为基于传感器的输入发出报警。事实上，如果触点关闭，即电流停止流经触点，系统会默认启用触点来发送系统日志消息。只有当默认设置不符合您的要求时，才需要配置触点。

报警触点的编号分别是 1 和 2，您需要了解如何连接物理引脚以配置正确的设置。单独配置每个触点。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。

步骤 3 点击 **+** 按钮以创建新的对象。

步骤 4 为对象输入名称。例如，**Enable_Alarm_Contact**。

步骤 5 在**模板**编辑器中，输入配置触点所需的命令。

a) 配置报警触点的说明。

alarm contact {**1** | **2**} **description** *string*

例如，要将触点 1 的说明设置为“Door Open”，请输入以下命令：

```
alarm contact 1 description Door Open
```

b) 配置报警触点的严重性。

alarm contact {**1** | **2** | **any**} **severity** {**major** | **minor** | **none**}

您可以指定 **any** 更改所有触点的严重性，而不是配置一个触点。严重性控制与触点关联的 LED 指示灯的行为。

- **major**- LED 指示灯红色闪烁。
- **minor**- LED 指示灯红色长亮。这是默认值。
- **none**- LED 指示灯熄灭。

例如，要将触点 1 的严重级别设置为“Major”，请输入以下命令：

```
alarm contact 1 severity major
```

c) 配置报警触点的触发器。

alarm contact {**1** | **2** | **any**} **trigger** {**open** | **closed**}

您可以指定 **any** 更改所有触点的触发器，而不是配置一个触点。触发器决定发出报警信号的电气条件。

- **open**- 触点的正常状态为闭合，即电流流经触点。如果触点变成打开状态，即电流停止流动，会触发警报。

- **closed**- 触点的正常状态为打开，即电流不通过触点。如果触点变成闭合状态，即电流开始流经触点，会触发警报。这是默认值。

例如，将门禁传感器连接到报警输入触点1，该触点的正常状态为没有电流流经报警触点（即打开）。如果门被打开，触点会变成闭合状态，电流将流经报警触点。您应将报警触发器设为关闭，以便当电流开始流动时，警报响起。

```
alarm contact 1 trigger closed
```

d) 配置触发报警触点时采取的操作。

alarm facility input-alarm {**1** | **2**} {**relay** | **syslog** | **notifies**}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。默认情况下，此选项已启用。
- **通知** - 发送 SNMP 陷阱。

例如，要启用报警输入触点 1 的所有操作，请输入以下命令：

```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

步骤 6 在**取消模板**编辑器中，输入撤消此配置所需的命令。

所有这些命令采用**no**形式来将其禁用并恢复默认设置。例如，如果您的模板包含此过程中所示的所有命令示例，取消模板如下：

```
no alarm contact 1 description Door Open
no alarm contact 1 severity major
no alarm contact 1 trigger closed
no alarm facility input-alarm 1 relay
no alarm facility input-alarm 1 syslog
no alarm facility input-alarm 1 notifies
```

步骤 7 点击**确定**保存对象。

步骤 8 将对象添加到 FlexConfig 策略中。

a) 点击目录中的 **FlexConfig 策略**。

b) 在组列表中点击 **+**。

c) 选择 Enable_Alarm_Contact 对象，然后点击**确定**。

系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。

d) 点击**保存**。

您现在可以部署策略。

步骤 9 部署完成后，在 CLI 控制台或 SSH 会话中使用 **show running-config** 命令，验证对运行配置的更改是否正确。测试外部传感器，验证是否可以触发警报。

配置电源报警

ISA 3000 包含两个电源。默认情况下，系统在单电源模式下运行。但是，您可以配置系统在双电源模式下运行，其中第二个电源会在主电源发生故障时自动供电。启用双电源模式时，自动启用电源报警来发送系统日志警报，但您可以完全禁用警报，或同时启用 SNMP 陷阱或报警硬件中继。

以下过程说明如何启用双电源模式下，以及如何配置电源报警。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。

步骤 3 点击 **+** 按钮以创建新的对象。

步骤 4 为对象输入名称。例如，**Enable_Power_Supply_Alarm**。

步骤 5 在**模板**编辑器中，输入配置电源报警所需的命令。

a) 启用双电源模式。

power-supply dual

例如：

```
power-supply dual
```

b) 配置触发电源报警时要采取的操作。

alarm facility power-supply rps {**relay** | **syslog** | **notifies** | **disable**}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。默认情况下，此选项已启用。
- **通知** - 发送 SNMP 陷阱。
- **禁用** - 禁用电源报警。为电源报警配置的任何其他操作都无法运行。

例如，要启用电源报警的所有操作，请输入以下命令：

```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

步骤 6 在**取消模板**编辑器中，输入撤消此配置所需的命令。

所有这些命令采用**no**形式来将其禁用并恢复默认设置。例如，如果您的模板包含此过程中所示的所有命令示例，取消模板如下：

```
no power-supply dual
no alarm facility power-supply rps relay
no alarm facility power-supply rps syslog
no alarm facility power-supply rps notifies
```

步骤 7 点击**确定**保存对象。

步骤 8 将对象添加到 FlexConfig 策略中。

a) 点击目录中的 **FlexConfig 策略**。

b) 在组列表中点击 **+**。

c) 选择 Enable_Power_Supply_Alarm 对象，然后点击**确定**。

系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。

d) 点击**保存**。

您现在可以部署策略。

步骤 9 部署完成后，在 CLI 控制台或 SSH 会话中使用 **show running-config** 命令，验证对运行配置的更改是否正确。

配置温度报警

您可以配置基于设备中 CPU 卡温度的警报。

您可以设置主要和辅助温度范围。如果温度低于低阈值，或超过高阈值，则触发报警。

默认对所有报警操作启用主温度报警：输出中继、系统日志和 SNMP。主要温度范围的默认设置为 -40°C 至 92°C。

默认情况下，禁用辅助温度报警。您可以将辅助温度范围设置为 -35°C 至 85°C。

由于辅助温度范围比主范围更严格，如果您设置辅助低温度或高温度，该设置将禁用对应的主要设置，即使您为主设置配置非默认值。您不能启用两个单独的高温度报警和两个单独的低温度报警。

因此，在实践中，您应为高温度和低温度仅配置主要设置或仅配置辅助设置。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。

步骤 3 点击 **+** 按钮以创建新的对象。

步骤 4 为对象输入名称。例如，**Enable_Temperature_Alarm**。

步骤 5 在**模板**编辑器中，输入配置温度报警所需的命令。

a) 配置可接受的温度范围。

alarm facility temperature {**primary** | **secondary**} {**low** | **high**} *temperature*

温度单位为摄氏度。主要报警的允许范围为 -40 至 92，这也是默认的范围。辅助报警的允许范围是 -35 到 85。低值必须小于高值。

例如，要设置更严格的 -20 至 80 温度范围（在辅助报警的允许范围内），请按如下所示配置辅助报警：

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

b) 配置触发温度报警时要采取的操作。

alarm facility temperature {**primary** | **secondary**} {**relay** | **syslog** | **notifies**}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。
- **通知** - 发送 SNMP 陷阱。

例如，要启用辅助温度报警的所有操作，请输入以下命令：

```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

步骤 6 在**取消模板**编辑器中，输入撤消此配置所需的命令。

所有这些命令采用 **no** 形式来恢复默认设置（针对主要报警）或将其禁用（针对辅助报警）。例如，如果您的模板包含此过程中所示的所有命令示例，取消模板如下：

```
no alarm facility temperature secondary low -20
no alarm facility temperature secondary high 80
no alarm facility temperature secondary relay
no alarm facility temperature secondary syslog
no alarm facility temperature secondary notifies
```

步骤 7 点击**确定**保存对象。

步骤 8 将对象添加到 FlexConfig 策略中。

a) 点击目录中的 **FlexConfig 策略**。

b) 在组列表中点击 **+**。

c) 选择 Enable_Temperature_Alarm 对象，然后点击**确定**。

系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。

d) 点击**保存**。

您现在可以部署策略。

步骤 9 部署完成后，在 CLI 控制台或 SSH 会话中使用 **show running-config** 命令，验证对运行配置的更改是否正确。

监控报警

以下主题介绍如何监控和管理报警。

监控报警状态

您可以在 CLI 中使用以下命令监控报警。

- **show alarm settings**

  显示每个可能的报警的当前配置。

- **show environment alarm-contact**

  显示输入报警触点的物理状态信息。

- **show facility-alarm relay**

  显示有关已触发输出中继的报警信息。

- **show facility-alarm status** [**info** | **major** | **minor**]

  显示所有已触发报警的信息。您可以通过过滤 **major** 或 **minor** 状态来限制视图。**info** 关键字提供与不使用关键字时相同的视图。

监控报警系统日志消息

根据您配置的报警类型，您可能会看到以下系统日志消息。

双电源报警

- %FTD-1-735005：电源设备冗余正常
- %FTD-1-735006：电源设备冗余丢失

温度报警

在这些报警中，*Celsius* 将替换为设备上检测到的温度，以摄氏为单位。

- %FTD-6-806001：主要报警 CPU 温度高 *Celsius*
- %FTD-6-806002：CPU 高温主要报警已清除
- %FTD-6-806003：主要报警 CPU 温度低 *Celsius*

- %FTD-6-806004：CPU 低温主要报警已清除
- %FTD-6-806005：辅助报警 CPU 温度高 *Celsius*
- %FTD-6-806006：CPU 高温辅助报警已清除
- %FTD-6-806007：辅助报警 CPU 温度低 *Celsius*
- %FTD-6-806008：CPU 低温辅助报警已清除

报警输入触点报警

在这些报警中，*description* 是您所配置触点的说明。

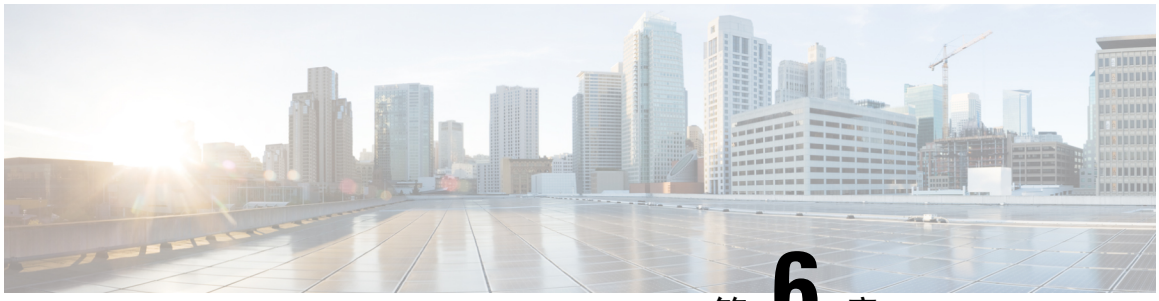
- %FTD-6-806009：与 ALARM_IN_1 *alarm_1_description* 对应的报警已确定
- %FTD-6-806010：与 ALARM_IN_1 *alarm_1_description* 对应的报警已清除
- %FTD-6-806011：与 ALARM_IN_2 *alarm_2_description* 对应的警报已确定
- %FTD-6-806012：与 ALARM_IN_2 *alarm_2_description* 对应的报警已清除

关闭外部报警

如果您使用连接到报警输出的外部报警，并触发了报警，可以使用 **clear facility-alarm output** 命令从设备 CLI 关闭外部报警。此命令会断开输出引脚，同时关闭输出 LED。

第 II 部分

可重用对象



第 6 章

对象

对象是可重用容器，用于定义在策略或其他设置中要使用的条件。例如，网络对象定义主机和子网地址。

对象允许您定义条件，这样即可在不同策略中重新使用相同的条件。在更新对象时，将自动更新使用该对象的所有策略。

- 对象类型，第 127 页
- 管理对象，第 130 页

对象类型

可以创建以下类型的对象。在大多数情况下，如果策略或设置允许使用对象，则必须使用对象。

对象类型	主要用途	说明
Secure Client 配置文件	远程访问 VPN。	Secure Client 配置文件随 Secure Client 软件一起下载到客户端。这些配置文件定义与客户端相关的诸多选项，例如启动时自动连接和自动重新连接，以及是否允许最终用户更改 Secure Client 首选项和高级设置中的选项。 请参阅 配置并上传客户端配置文件，第 663 页。
应用过滤器	访问控制规则。	应用过滤器对象定义 IP 连接中使用的应用，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。您可以在策略中使用这些对象而不是使用端口规格来控制流量。 请参阅配置应用过滤器对象，第 134 页。
证书	身份策略。 远程访问 VPN。 SSL 解密规则。 管理 Web 服务器。	数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。 请参阅配置证书，第 144 页。

对象类型	主要用途	说明
DNS 组	管理和数据接口的 DNS 设置。	DNS 组定义 DNS 服务器列表和某些相关联的属性。需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 www.example.com。 请参阅配置 DNS 组，第 742 页。
事件列表过滤器	选定日志记录目标的系统日志记录设置。	事件列表过滤器创建用于系统日志消息的过滤器列表。您可以使用它们来限制发送到特定日志记录位置（例如系统日志服务器或内部日志缓冲区）的消息。 请参阅配置事件列表过滤器，第 734 页。
地理位置	安全策略。	地理位置对象定义托管设备（流量的源或目的）的国家/地区和大洲。您可以在策略中使用这些对象而不是使用 IP 地址来控制流量。 请参阅配置地理位置对象，第 137 页。
身份源	身份策略。 远程访问 VPN。 设备管理器访问。	身份源是定义用户账户的服务器和数据库。身份源信息具有多种用途，例如提供与 IP 地址关联的用户身份，或是对远程访问 VPN 连接或到设备管理器的访问进行身份验证。 请参阅身份源，第 151 页。
IKE 策略	VPN。	互联网密钥交换 (IKE) 策略对象定义用于对 IPsec 对等体进行身份验证、协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的 IKE 提议。IKEv1 和 IKEv2 有单独的对象。 请参阅配置全局 IKE 策略，第 626 页。
IPsec 提议	VPN。	IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。 请参阅配置 IPsec 提议，第 630 页。
网络	安全策略和各种设备设置。	网络组和网络对象（统称为“网络对象”）定义主机或网络的地址。 请参阅配置网络对象和组，第 130 页。
端口	安全策略。	端口组和端口对象（统称为“端口对象”）定义流量的协议、端口或 ICMP 服务。 请参阅配置端口对象和组，第 132 页。
密钥	Smart CLI 和 FlexConfig 策略。	密钥对象定义要加密和隐藏的密码或其他身份验证字符串。 请参阅配置密钥对象，第 831 页。

对象类型	主要用途	说明
安全区	安全策略。	安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。 请参阅配置安全区，第 133 页。
SGT 组	访问控制策略。	Trustsec 安全组标记 (SGT) 定义思科身份服务引擎 (ISE) 中定义的流量标记。您必须先配置ISE，然后才能创建这些对象。接下来，您可以将对象用作访问控制规则中的源/目的地匹配条件。 请参阅配置安全组标记 (SGT) 组，第 139 页。
SLA 监控器	静态路由。	SLA 监控器定义用于监控静态路由的目标 IP 地址。如果监控器确定无法再访问目标 IP 地址，则系统可安装备用静态路由。 请参阅配置 SLA 监控器对象，第 311 页。
SSL 密码	SSL 设置。	SSL 密码对象定义在建立与 威胁防御的 SSL 连接时可以使用的安全级别、TLS/DTLS 协议版本和加密算法的组合。在系统设置中使用这些对象为与设备建立 TLS/SSL 连接的用户定义安全要求。 请参阅配置 TLS/SSL 密码设置，第 761 页。
系统日志服务器	访问控制规则。 诊断日志记录。 安全智能策略。 SSL 解密规则。 入侵策略。 文件/恶意软件策略	系统日志服务器对象标识可接收面向连接的消息或诊断系统日志（系统日志）消息的服务器。 请参阅配置系统日志服务器，第 138 页。
URL	访问控制规则。 安全智能策略。	URL 对象和组（统称为“URL 对象”）定义网络请求的 URL 或 IP 地址。 请参阅配置 URL 对象和组，第 136 页。
用户	远程访问 VPN。	您可以直接在设备上创建与远程访问 VPN 搭配使用的用户账户。您可以使用本地用户账户代替外部身份验证源，或与后者搭配使用。 请参阅配置本地用户，第 168 页。

管理对象

您可以直接通过“对象”(Objects) 页面配置对象，也可以在编辑策略时进行配置。两种方法得到的结果相同：新对象或更新的对象，所以请使用当下符合您需求的方法。

以下程序介绍如何直接通过“对象”(Objects) 页面创建和管理对象。

注释 在编辑策略或设置时，如果属性需要对象，系统将会为您显示已定义的对象列表，从中您可以选择适当的对象。如果所需的对象不存在，只需点击列表中所示的**创建新对象 (Create New Object)** 链接即可。

过程

步骤 1 选择**对象**。

“对象”(Objects) 页面有一个目录，其中列出了可用的对象类型。在选择对象类型时，您会看到现有对象的列表，并可在此处创建新对象。另外，还可看到对象内容和类型。

步骤 2 从目录中选择对象类型，并执行以下任一操作：

- 要创建对象，请点击 **+** 按钮。对象的内容视类型而异；有关每个对象类型的具体信息，请参阅配置主题。
- 要创建组对象，请点击**添加组** () 按钮。组对象包含多个项目。
- 要编辑对象，请点击该对象的编辑图标 ()。无法编辑预定义对象的内容。
- 要删除对象，请点击该对象的删除图标 ()。如果某个策略或其他对象目前正在使用对象，或者对象为预定义对象，则无法将其删除。

配置网络对象和组

使用网络组和网络对象（统称为“网络对象”）可定义主机或网络的地址。然后，您可以在安全策略中使用这些对象来定义流量匹配条件，或在设置中使用它们来定义服务器或其他资源的地址。

网络对象定义单个主机或网络地址，而网络组对象可以定义多个地址。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑地址属性时，点击对象列表中所示的**创建新网络 (Create New Network)** 链接来创建网络对象。

过程

步骤 1 选择**对象**，然后从目录中选择**网络**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要创建组，请点击**添加组** () 按钮。
- 要编辑某个对象或组，请点击该对象的编辑图标 ()。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ()。

步骤 3 输入对象的名称和说明（后者为可选项），并定义对象内容。

我们建议不要单独使用 IP 地址作为名称，以便您可以轻松地从对象内容或独立 IP 地址中识别对象名称。如果您想要在名称中使用 IP 地址，请添加一个有意义的前缀，例如 host-192.168.1.2 或 network-192.168.1.0。如果您使用 IP 地址作为名称，系统会添加一条竖线作为前缀，例如 |192.168.1.2. 设备管理器 不会在对象选择器中显示这条竖线，但如果您在 CLI 中使用 **show running-config** 命令检查运行配置，您将看到此命名标准。

步骤 4 配置对象的内容。

网络对象

选择对象**类型**并配置内容：

- **网络** - 使用以下格式之一输入网络地址：
  - IPv4 网络（包含子网掩码），例如 10.100.10.0/24 或 10.100.10.0/255.255.255.0。
  - IPv6 网络（包括前缀），例如 2001:DB8:0:CD30::/60。
- **主机** - 使用以下格式之一输入主机 IP 地址：
  - IPv4 主机地址，例如 10.100.10.10。
  - IPv6 主机地址，例如 2001:DB8::0DB8:800:200C:417A 或 2001:DB8:0:0:0DB8:800:200C:417A。
- **范围** - 地址范围，起始地址和终止地址用连字符分隔。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。例如，192.168.1.10-192.168.1.250 或 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100。
- **FQDN** - 输入完全限定域名，例如 www.example.com。不能使用通配符。此外，请选择 **DNS 解析**确定是否要将 IPv4 地址、IPv6 地址，或这两个地址与 FQDN 关联。默认值为 IPv4 和 IPv6 这两个地址。只能在访问控制规则中使用这些对象。规则匹配通过 DNS 查找获取的 FQDN IP 地址。

网络组

点击 + 按钮，以选择要添加到组中的网络对象或组。另外，也可以创建新对象。

步骤 5 点击**确定 (OK)**，保存更改。

配置端口对象和组

使用端口组和端口对象（统称为“端口对象”）可定义流量的协议、端口或 ICMP 服务。然后，可以在安全策略中使用这些对象来定义流量匹配条件，例如使用访问规则来允许流量传送至特定 TCP 端口。

端口对象定义单一协议、TCP/UDP 端口、端口范围或 ICMP 服务，而端口组对象可定义多项服务。

该系统中包括多个针对通用服务的预定义对象。您可以在策略中使用这些对象，但无法编辑或删除系统定义的对象。

注释 在创建端口组对象时，请确保合理组合对象。例如，如果在访问规则中使用某个对象指定源端口和目标端口，则不能在该对象中混合使用多个协议。在编辑已使用的对象时请务必小心，否则可能导致使用该对象的策略无效（和被禁用）。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑服务属性时，点击对象列表中所示的**创建新端口**链接来创建端口对象。

过程

步骤 1 选择**对象**，然后从目录中选择**端口**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要创建组，请点击**添加组** () 按钮。
- 要编辑某个对象或组，请点击该对象的编辑图标 ()。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ()。

步骤 3 输入对象的名称和说明（后者为可选项），并定义对象内容。

端口对象

选择**协议**，然后按以下所示配置该协议：

- **TCP**、**UDP** - 输入单一端口或端口范围编号，例如 80（适用于 HTTP）或 1-65535（涵盖所有端口）。
- **ICMP**、**IPv6-ICMP** - 选择 ICMP **类型**和**代码**（可选）。选择 **Any** 类型可应用于所有 ICMP 消息。有关类型和代码的信息，请参阅以下页面：
  - ICMP -http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6 -http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- **其他** - 选择所需协议。

端口组

点击 + 按钮，以选择要添加至该组的端口对象。另外，也可以创建新对象。

步骤 4 点击**确定 (OK)**，保存更改。

配置安全区

安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。您可以定义多个区域，但一个给定接口只能位于一个区域中。

系统将在初始配置期间创建以下区域。您可以编辑这些区域以添加或移除接口；如果不再使用这些区域，也可以删除它们。

- **inside_zone** - 包括内部接口。如果内部接口为网桥组，则此区域包括所有网桥组成员接口，而不是内部网桥虚拟接口 (BVI)。此区域用于表示内部网络。
- **outside_zone** - 包括外部接口。此区域用于表示在您控制之外的网络，例如互联网。

通常，按接口在网络中扮演的角色对它们分组。例如，可将连接至互联网的接口放在 **outside_zone** 安全区，并将内部网络的所有接口放在 **inside_zone** 安全区。然后，可以对来自外部区域和传至内部区域的流量应用访问控制规则。

在创建区域之前，请考虑要应用至网络的访问规则和其他策略。例如，无需将所有内部接口都放到同一个区域。如果您有 4 个内部网络，并希望将其中一个与另外三个区别对待，则可以创建两个区域（而不是一个区域）。如果有一个接口需允许外部访问公共 Web 服务器，您可能希望对该接口使用单独的区域。

以下步骤程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑安全区属性时，点击对象列表中所示的**创建新安全区**链接来创建安全区。

过程

步骤 1 选择**对象**，然后从目录中选择**安全区**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 输入对象的名称和说明（后者为可选项）。

步骤 4 选择区域的**模式**。

模式与接口模式直接关联。区域可以包含一种类型的接口。

- **路由 (Routed)** - 路由接口是可应用安全策略的直通流量的正常接口。

- **被动 (Passive)** - 被动接口不影响流经设备的流量。
- **内联 (Inline)** - 内联接口是用于 IPS 处理的内联集的成员。

步骤 5 在**接口**列表中，点击 **+** 并选择要添加到该区域的接口。

列表中将显示当前不在该区域的所有已命名接口。只有配置接口并为其指定了名称，才能将其添加到该区域。

如果所有已命名接口均已在该区域内，则列表为空。如果要尝试将某个接口移到其他区域，则首先必须将其从当前区域中删除。

注释 您不能将网桥组接口 (BVI) 添加到某个区域，而只能添加成员接口。您可以将成员接口放到不同的区域中。

步骤 6 点击**确定 (OK)**，保存更改。

配置应用过滤器对象

应用过滤器对象定义 IP 连接中使用的应用，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。您可以在策略中使用这些对象而不是使用端口规格来控制流量。

虽然您可以指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

您可以直接在策略中选择应用和应用过滤器，而不使用应用过滤器对象。但是，如果要为同一组应用或过滤器创建多个策略，使用对象则非常方便。该系统包括多个预定义的应用过滤器，您不能编辑或删除它们。

注释 思科会通过系统和漏洞数据库 (VDB) 更新频繁更改并添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑访问控制规则时，在向“应用”(Applications) 选项卡中添加应用条件后点击**另存为过滤器 (Save As Filter)** 链接来创建应用过滤器对象。

开始之前

编辑过滤器时，如果所选应用已由 VDB 更新删除，则会在应用名称后显示“（已弃用）”。必须从过滤器中删除这些应用，否则将阻止后续部署和系统软件升级。

过程

步骤 1 选择**对象**，然后从目录中选择**应用过滤器**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ()。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ()。

步骤 3 输入对象的名称和说明（后者为可选项）。

步骤 4 在**应用 (Applications)** 列表中，点击**添加 +** 并选择要添加到该对象的应用和过滤器。

初始列表将在连续滚动的列表中显示应用。点击**高级过滤器 (Advanced Filter)** 可查看过滤器选项，可更加方便地查看和选择应用。完成选择后，点击**添加 (Add)**。您可以重复该过程，以添加更多应用或过滤器。

注释 单个过滤器条件中的多个选项具有 OR 关系。例如，风险高 OR 非常高。过滤器之间的关系是 AND，因此是风险高 OR 非常高，AND 业务相关性低 OR 非常低。在选择过滤器时，显示屏中的应用列表更新，只显示符合条件的应用。您可以使用这些过滤器来帮助查找要单独添加的应用，或确认是否要选择所需的过滤器以添加到规则中。

风险

应用所用的用途可能违反组织安全策略的可能性，从非常低到非常高。

业务相关性

在组织的业务运营环境（非娱乐性）下使用应用的可能性，从非常低到非常高。

类型

应用类型：

- **应用协议** - 应用协议（例如 HTTP 和 SSH），代表主机之间的通信。
- **客户端协议** - 客户端（例如 Web 浏览器和邮件客户端），代表主机上运行的软件。
- **Web 应用** - Web 应用（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL。

类别

说明应用的最基本功能的应用通用分类。

标记

关于应用的其他信息，与类别类似。

对于加密流量，系统可以仅使用标记有 **SSL 协议**的应用识别和过滤流量。只有在未加密或已解密的流量中才能检测到没有此标记的应用。此外，系统仅将**已解密的流量**标记分配给可在已解密的流量中检测到的应用，而不会将它们分配给加密或未加密的流量中检测到的应用。

应用列表（显示屏底部）

在从列表上方的选项中选择过滤器时，此列表将进行更新，所以您可查看当前符合过滤器的应用。在计划将过滤器条件添加到规则中时，使用此列表可确认您的过滤器是否针对所需的应用。如果您计划添加特定应用，请从此列表中选择它们。

步骤 5 点击**确定 (OK)**，保存更改。

配置 URL 对象和组

使用 URL 对象和组（统称为“URL 对象”）可定义 Web 请求的 URL 或 IP 地址。可以使用这些对象在访问控制策略中执行手动 URL 过滤，或在安全智能策略中进行阻止。

URL 对象定义单个 URL 或 IP 地址，而 URL 组对象可以定义多个 URL 或地址。

在创建 URL 对象时，请记住以下要点：

- 如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配。然后，如果满足以下任一条件，则 URL 被视为匹配项：
  - 字符串位于 URL 的开头。
  - 字符串后面有一个点。
  - 字符串开头包含一个点。
  - 字符串后面跟有 :// 字符。

  例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。

注释 我们建议您不要使用手动URL过滤阻止或允许个别网页或部分网站（即，带有 / 字符的 URL），因为这样可能会重组服务器并将页面移至新路径。

- 系统忽略加密协议（HTTP 与 HTTPS）。换句话说，如果阻止网站，系统将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个应用条件指定特定协议。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 example.com 而不是 http://example.com。
- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公钥中的使用者公用名创建该对象。此外，系统会忽略使用者公用名中的子域，因此，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

  但请注意，证书中的使用者公用名可能与网站的域名完全无关。例如，youtube.com证书中的使用者公用名是 *.google.com（当然，这可能会随时更改）。如果使用 SSL 解密策略解密 HTTPS 流量以便 URL 过滤规则可用于解密策略，则可能获得更一致的结果。

注释 如果由于证书信息不再可用，浏览器恢复 TLS 会话，则 URL 对象将不匹配 HTTPS 流量。因此，即使精心配置 URL 对象，也可能会得到不一致的 HTTPS 连接结果。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑 URL 属性时，点击对象列表中所示的**创建新 URL** 链接来创建 URL 对象。

过程

步骤 1 选择**对象**，然后从目录中选择 **URL**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要创建组，请点击**添加组** () 按钮。
- 要编辑某个对象或组，请点击该对象的编辑图标 ()。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ()。

步骤 3 输入对象的名称和说明（后者为可选项）。

步骤 4 定义对象内容。

URL 对象

在 **URL** 框中输入 URL 或 IP 地址。在 URL 中不能使用通配符。

URL 组

点击 + 按钮选择要添加到组中的 URL 对象。另外，也可以创建新对象。

步骤 5 点击**确定 (OK)**，保存更改。

配置地理位置对象

地理位置对象定义托管设备（流量的源或目的）的国家/地区和大洲。您可以在策略中使用这些对象而不是使用 IP 地址来控制流量。例如，使用地理位置可以很容易地将访问权限限制为特定国家/地区，而无需知道此处使用的所有潜在 IP 地址。

通常，可以直接在策略中选择地理位置，而无需使用地理位置对象。但是，如果要为同一组国家/地区或大洲创建多个策略，使用对象则非常方便。

注释 为了确保使用最新的地理位置数据来过滤流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑网络属性时，点击对象列表中所示的**创建新地理位置 (Create New Geolocation)** 链接来创建地理位置对象。

过程

步骤 1 选择**对象**，然后从目录中选择**地理位置**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 输入对象的名称和说明（后者为可选项）。

步骤 4 在**大洲/国家/地区 (Continents/Countries)** 列表中，点击**添加 + (Add +)** 并选择要添加到该对象的大洲和国家/地区。

选择大洲将会选择该大洲内的所有国家/地区。

步骤 5 点击**确定 (OK)**，保存更改。

配置系统日志服务器

系统日志服务器对象标识可接收面向连接的消息或诊断系统日志（系统日志）消息的服务器。如果已为日志收集和分析设置一台系统日志服务器，请创建对象以进行定义并在相关策略中使用这些对象。

可以将下列类型的事件发送至系统日志服务器：

- 连接事件。根据下列策略类型配置系统日志服务器对象：访问控制规则和默认操作、SSL 解密规则和默认操作、安全智能策略。
- 入侵事件。根据入侵策略配置系统日志服务器对象。
- 诊断事件。请参阅配置系统将日志记录发送到远程系统日志服务器，第 732 页。
- 文件/恶意软件事件。在**设备** > **系统设置** > **日志记录设置**中配置系统日志服务器。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑系统日志服务器属性时，点击对象列表中所示的**添加系统日志服务器**链接来创建系统日志服务器对象。

过程

步骤 1 选择**对象**，然后从目录中选择**系统日志服务器**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。

- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置系统日志服务器的属性：

- **IP 地址** - 输入系统日志服务器的 IP 地址。
- **协议类型、端口号** - 选择用于系统日志的协议并输入端口号。默认值为 UDP/514。如果您选择 **TCP**，系统可以识别何时系统日志服务器不可用，并停止发送事件，直至服务器再次可用。默认 UDP 端口为 514，默认 TCP 端口为 1470。如果您更改默认值，端口范围必须介于 1025 至 65535 之间。

  注释 如果您使用 TCP 作为传输协议，系统会打开与系统日志服务器的 4 个连接，以确保消息不会丢失。如果您使用系统日志服务器从大量设备收集消息，并且合并的连接开销对该服务器来说太大，请改用 UDP。

- **用于设备日志的接口** - 选择应使用哪个接口发送诊断系统日志消息。以下类型的事件始终使用管理接口：连接、入侵、文件和恶意软件。接口选择决定与系统日志消息关联的 IP 地址。选择以下选项之一：
  - **数据接口** - 选择用于诊断系统日志消息的数据接口。如果可以通过网桥组成员接口访问该服务器，请改而选择该网桥组接口 (BVI)。您不能选择被动接口。

    对于连接、入侵、文件和恶意软件系统日志消息，源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。请注意，路由表中必须有适当的路由，以便将流量从选定接口引导至系统日志服务器，以获取这些事件类型。
  - **管理接口** - 对所有类型的系统日志消息使用管理接口。源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。

步骤 4 点击**确定 (OK)**，保存更改。

配置安全组标记 (SGT) 组

使用安全组标记 (SGT) 组对象以根据身份服务引擎 (ISE) 分配的 SGT 识别源或目标地址。然后，可以将访问控制规则中的对象用于定义流量匹配条件。

您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

有关如何使用 SGT 进行访问控制的详细信息，请参阅如何使用 TrustSec 安全组标记控制网络访问，第 491 页。

开始之前

在创建 SGT 组之前，必须配置 ISE 身份源以订用 SXP 映射并部署更改。然后，系统从 ISE 服务器检索 SGT 信息。只有在下载 SGT 后，您才能创建 SGT 组。

过程

步骤 1 选择**对象**，然后从目录中选择 **SGT 组**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 为对象输入**名称**和说明（后者为可选项）。

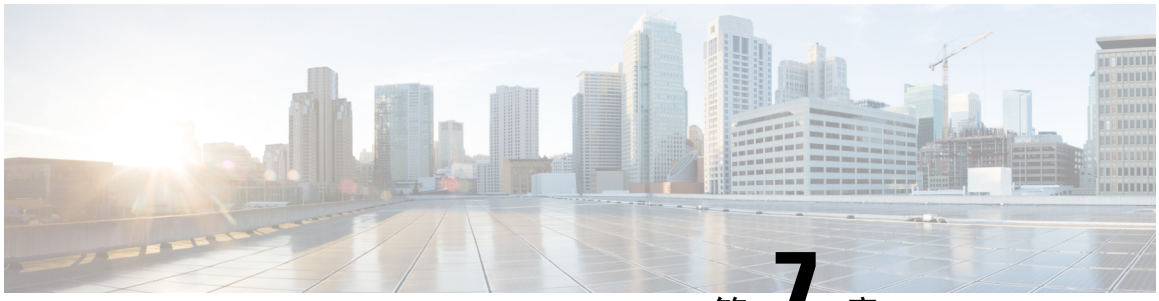
步骤 4 在**标记**下，点击 + 并选择要包含在对象中的已下载 SGT。

要删除 SGT，请点击标记名称右侧的 **x**。

如果列表为空，则系统无法下载任何 SGT 映射。如果发生这种情况，请采取以下措施：

- 确保 ISE 身份对象订用 SXP 主题。您必须订用 SXP，才能获取映射。
- 验证 ISE 中是否定义了静态映射，以及 ISE 是否配置为发布这些映射。如果不存在任何映射，就没有任何内容可供下载。请参阅在 ISE 中配置安全组和 SXP 发布 ， 第 494 页。

步骤 5 点击**确定 (OK)**。



第 7 章

证书

数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。以下主题介绍如何创建和管理证书。

关于证书

数字证书是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、序列号、公司、部门或 IP 地址。数字证书还包括用户或设备的公钥副本。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。

您可以创建以下类型的证书：

- 内部证书 - 内部身份证书是用于特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。当内部证书因任何原因到期或无效时，您可以通过以下 CLISH CLI 命令重新生成证书：

```
> system support regenerate-security-keyring
  String  Certificate to be regenerated, default or fdm
```

- 内部证书颁发机构 (CA) 证书 - 内部 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名的内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。

- 可信证书颁发机构 (CA) 证书 - 可信的 CA 证书可用于签署其他证书。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。

证书颁发机构 (CA) 是指“签署”证书以确认其真实性，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。CA 可以是可信的第三方（例如 VeriSign），也可以是组织内建立的私有（内部）CA。CA 负责管理证书请求和颁发数字证书。有关详细信息，请参阅 公钥加密，第 142 页。

公钥加密

在 RSA 加密系统等公钥加密中，每位用户都有一个包含公钥和私钥的密钥对。这一对密钥相互补充，用其中一个密钥加密的任何内容都可用另一个密钥解密。

简言之，使用私钥加密数据时会形成一个签名。此签名附加在数据中并发送给接收者。接收者对数据应用发送者的公钥。如果随数据一起发送的签名与对数据应用公钥的结果一致，就会确立消息的有效性。

此过程的前提是接收者拥有发送者的公钥副本而且非常确定此密钥属于发送者，而不是伪装成发送者的其他人。

获取发送方公钥通常是在外部处理或通过安装时执行的操作处理。例如，默认情况下，大多数 Web 浏览器都使用若干 CA 的根证书进行配置。

您可以通过 openssl.org、维基百科或其他来源了解有关数字证书和公钥加密的更多信息。充分了解 SSL/TLS 加密有助于您为自己的设备建立安全连接。

功能使用的证书类型

您需要为每个功能创建正确类型的证书。以下功能需要证书。

身份策略（强制网络门户）- 内部证书

（可选。）强制网络门户用于身份策略中。在向设备进行身份验证时，为了标识自己的身份并获得与其用户名关联的 IP 地址，用户必须接受此证书。如果不提供证书，设备将使用自动生成的证书。

身份领域（身份策略和远程访问 VPN）- 受信任的 CA 证书

（可选。）如果对目录服务器进行加密连接，则必须接受证书才能在目录服务器上执行身份验证。当系统按身份和远程访问 VPN 策略提示用户进行身份验证时，用户必须进行身份验证。如果不对目录服务器使用加密，则不需要证书。

管理 Web 服务器（管理访问系统设置）- 内部证书

（可选） 设备管理器 是基于 Web 的应用，所以在 Web 服务器上运行。您可以上传您的浏览器视为有效的证书，以避免出现“不受信任的颁发机构”警告。

远程访问 VPN - 内部证书

（必需。）内部证书用于外部接口，在 Secure Client 与设备进行连接时确定客户端的设备身份。客户端必须接受此证书。

站点间 VPN - 内部和受信任 CA 证书

如果对站点间 VPN 连接使用证书身份验证，您需要选择用于对连接中的本地对等体进行身份验证的内部身份证书。虽然这并不是 VPN 连接定义的一部分，但您还需要上传用于签署本地和远程对等体身份证书的受信任 CA 证书，以便系统可以对对等体进行身份验证。

SSL 解密策略 - 内部、内部 CA 和受信任 CA 证书 以及证书组

（必需。）SSL 解密策略将证书用于以下目的：

- 内部证书用于已知的密钥解密规则。
- 在客户端和 威胁防御 设备之间创建会话时，内部 CA 证书用于解密重签名规则。
- 在 威胁防御 设备和服务器之间创建会话时，受信任 CA 证书直接用于解密重签名规则。受信任 CA 证书用于验证服务器证书的签名机构。您可以直接配置这些证书或在策略设置的证书组中进行配置。系统包括大量受信任 CA 证书（集中放置于 Cisco-Trusted-Authorities 组中），因此您可能无需上传任何其他证书。

示例：使用 OpenSSL 生成内部证书

以下示例使用 OpenSSL 命令生成内部服务器证书。您可以从 openssl.org 获取 OpenSSL。有关具体信息，请查阅 OpenSSL 文档。此示例中使用的命令可能会更改，您还可以使用其他您可能想要使用的可用选项。

此程序旨在让您了解如何获取要上传到 威胁防御 的证书。

注释 这里显示的 OpenSSL 命令仅作为示例。调整参数以满足您的安全要求。

过程

步骤 1 生成密钥。

```
openssl genrsa -out server.key 4096
```

步骤 2 生成证书签名请求 (CSR)。

```
openssl req -new -key server.key -out server.csr
```

步骤 3 使用密钥和 CSR 生成自签证书。

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

由于 设备管理器 不支持加密的密钥，请尝试在生成自签证书时按回车键跳过质询密码。

步骤 4 在 设备管理器中创建内部证书对象时，将文件上传到相应的字段。

您还可以复制/粘贴文件内容。示例命令创建以下文件：

- server.crt - 将内容上传或粘贴到“服务器证书”字段中。
- server.key - 将内容上传或粘贴到“证书密钥”字段中。如果您在生成密钥时提供了密码，则可以使用以下命令对其进行解密。输出发送到 stdout，您可以从其中复制它。

```
openssl rsa -in server.key -check
```

配置证书

威胁防御 支持 PEM 或 DER 格式的 X509 证书。如果需要，可使用 OpenSSL 生成证书、从受信任的证书颁发机构获取证书或创建自签名证书。

有关证书的详细信息，请参阅关于证书，第 141 页。

有关每项功能所用证书类型的信息，请参阅功能使用的证书类型，第 142 页。

以下步骤程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑证书属性时，点击对象列表中所示的**创建新证书**链接来创建证书对象。

过程

步骤 1 选择**对象**，然后从目录中选择**证书**。

系统提供以下预定义证书（您可以按原样使用或替换它们）。

- DefaultInternalCertificate
- DefaultWebserverCertificate
- NGFW-Default-InternalCA

此外，系统还包括许多从第三方证书颁发机构获取的受信任的 CA 证书。SSL 解密策略可使用这些证书执行解密重新签署操作。Cisco-Trusted-Authorities 组包括所有这些证书，并且是 SSL 解密策略使用的默认组。

可以点击预定义的搜索过滤器，将列表限制为仅**系统定义**或**用户定义**的证书。您还可以使用**弱密钥**过滤器来查找密钥短于建议最小长度的证书。建议您将这些证书替换为具有更长密钥的证书。

步骤 2 执行以下操作之一：

- 要创建新的证书对象，请使用 + 菜单中适合证书类型的命令。
- 要创建新证书组，请点击 并选择**添加证书组**。
- 要查看或编辑证书或组，请点击证书的编辑图标 () 或查看图标 ()。
- 要删除未引用的证书或组，请点击证书的垃圾桶图标 ()。

有关创建或编辑证书的详细信息，请参阅下列主题：

- 上传内部证书和内部 CA 证书，第 145 页

- 生成自签名的内部证书和内部 CA 证书，第 146 页
- 上传受信任的 CA 证书，第 148 页
- 配置受信任 CA 证书组，第 149 页

上传内部证书和内部 CA 证书

内部身份证书是特定系统或主机的证书。

内部 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。

您可以使用 OpenSSL 工具包自行生成这些证书，也可以从证书颁发机构获取证书，然后再按照以下步骤程序上传证书。有关生成密钥的示例，请参阅示例：使用 OpenSSL 生成内部证书，第 143 页。

此外，您还可以生成自签名的内部身份和内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。有关创建自签名证书的信息，请参阅生成自签名的内部证书和内部 CA 证书，第 146 页。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型，第 142 页。

过程

步骤 1 选择**对象**，然后从目录中选择**证书**。

步骤 2 执行以下操作之一：

- 依次点击 + > **添加内部证书**，然后点击**上传证书和密钥**。
- 依次点击 + > **添加内部 CA 证书**，然后点击**上传证书和密钥**。
- 要编辑或查看证书，请点击信息图标( )。对话框中将显示证书主题、颁发者和有效时间范围。点击“替换证书”即可上传新的证书和密钥。此外，您还可以在对话框中粘贴证书和密钥。

步骤 3 键入证书的**名称**。

该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 4 点击**上传证书**（或在编辑时点击**替换证书**），并选择证书文件（例如 *.crt）。允许的文件扩展名有 .pem、.cert、.cer、.crt 和 .der。或者，粘贴证书。

该证书必须为 PEM 或 DER 格式的 X509 证书。

您粘贴的证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行。例如：

```
-----BEGIN CERTIFICATE-----
MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
```

```
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

步骤 5 点击**上传密钥**（或在编辑时点击**替换密钥**），并选择证书文件（例如 *.key）。文件扩展名必须为.key。或者，粘贴证书的密钥。

该密钥无法加密，且必须是 RSA 密钥。

例如：

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQClSu1BknrMjzw/5FZ9YgdMLDUGJlbYgkjN7mVrkjyLQx2TYsem
r8iTiKB6iyTKbuS4iPeyEYkNF5FglCqKWEdmthNZkBhOsPs1A8e60r5mImeDrtw+
Cc0O5cSfnlTAw5CgcGkcxTCaGIZmXMkzwGlfYmzbJDeazfSmvys76A8I8wIDAQAB
AoGAUVDgEX8vXE0m9cOubPZ54pZo64KW/OJzUKP0TwxdLqGw/h39XFpkEXiIgmDL
(...5 lines removed...)
DSWvzekRDH83dmP66+MIbWePhbhty+D1OxbiuVuHV0/ZhxOhCG8tig3R8QJBAJmj
fId05+1dNI4tGbWv6hHh/H/dTP2STlZ3jERMZd29fjIRuJ9jpFC2lIDjvs8YGeAe
0YHkfSOULJn8/jOCf6kCQQDIJiHfGF/31Dk/8/5MGrg+3zau6oKXiuv6db8Rh+7l
MUOx09tvbBUy9REJq1YJWTKpeKD+E0QL+FX0bqvz4tHA
-----END RSA PRIVATE KEY-----
```

步骤 6 点击**确定 (OK)**。

如果密钥大小小于生成的自签名证书所允许的最小大小，则系统会警告您该证书不符合建议的最低要求。点击**继续**可继续上传证书，但建议您创建更强的新证书。

生成自签名的内部证书和内部 CA 证书

内部身份证书是特定系统或主机的证书。

内部 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。

您可以生成自签名的内部身份和内部 CA 证书，即这些证书由设备自身签署。如果配置自签名的内部 CA 证书，该 CA 将在设备上运行。系统会生成证书和密钥。

此外，还可以使用 OpenSSL 创建证书或从受信任的 CA 获取证书，再上传它们。有关详细信息，请参阅上传内部证书和内部 CA 证书，第 145 页。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型，第 142 页。

过程

步骤 1 选择**对象**，然后从目录中选择**证书**。

步骤 2 执行以下操作之一：

- 依次点击 + > **添加内部证书**，然后点击**自签名证书**。
- 依次点击 + > **添加内部 CA 证书**，然后点击**自签名证书**。

注释 要编辑或查看证书，请点击信息图标 ( )。对话框中将显示证书主题、颁发者和有效时间范围。点击**替换证书**，可上传新的证书和密钥。替换证书后，不能重新执行以下步骤中介绍的自签名特性设置。相反，您必须粘贴或上传新的证书，如上传内部证书和内部 CA 证书，第 145 页中所述。其余步骤仅适用于新的自签名证书。

步骤 3 键入证书的**名称**。

该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 4 为证书主题和颁发者信息至少配置以下一项。

- **国家/地区** (C) - 证书中包括的双字符 ISO 3166 国家/地区代码。例如，美国的国家/地区代码是 US。从下拉列表中选择国家/地区代码。
- **州或省** (ST) - 证书中包括的州或省。
- **地区或城市** (L) - 证书中包括的地区，例如城市名称。
- **组织** (O) - 证书中包括的组织或公司名称。
- **组织单位（部门）** (OU) - 证书中包含的组织单位名称（例如部门名称）。
- **通用名称** (CN) - 证书中包括的 X.500 通用名称。它们可能是设备、网站或其他文本字符串的名称。通常需要有此元素，才能成功进行连接。例如，用于远程访问 VPN 的内部证书中必须包括 CN。
- **密钥类型** - 要为此证书生成的密钥的类型：RSA、ECDSA（椭圆曲线数字签名算法）或 EDDSA（爱德华兹曲线数字签名算法）。
- **密钥大小** - 要生成的密钥的大小。通常，较长的密钥更安全。但是，生成模数较大的密钥需要更长的时间，而且交换时的处理时间也更长。允许的大小因密钥类型而异。
  - RSA 密钥可以是 2048、3072 或 4096 位。
  - ECDSA 密钥可以是 256、384 或 521 位。

    EDDSA 密钥可以是 256 位。
- **有效期** - 证书将被视为有效的时间段。无论您如何设置到期日期，默认设置为 825 天（从今天起）。点击**设置默认值**可恢复为默认值。您可以通过以下任一方法配置该时间段。请务必在证书过期前进行更换。
  - **按日期** - 点击**到期日期**，然后选择证书应被视为有效的最后一天。
  - **按天数** - 输入从今天起证书应被视为有效的天数。输入数字后，您可以点击**按日期**查看计算得出的到期日期。

步骤 5 点击**保存 (Save)**。

上传受信任的 CA 证书

受信任证书颁发机构 (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。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型，第 142 页。

受信任 CA 证书可从外部证书颁发机构获取，也可以使用自己的内部 CA 创建（例如通过 OpenSSL 工具生成证书）。然后，使用以下步骤程序上传证书。

开始之前

系统会每天联系思科一次，以确定是否有新的或更新的受信任 CA 证书，并在可用时下载更新后的证书。这一日常检查可确保预安装的证书都保持最新。您可以使用 **show cert-update** 命令在 CLI 中监控此自动检查。您可以使用 **configure cert-update auto-update disable** 命令来禁用日常检查，并可以使用 **configure cert-update run-now** 命令来手动下载更新。

过程

步骤 1 选择**对象**，然后从目录中选择**证书**。

步骤 2 执行以下操作之一：

- 依次点击 + > **添加受信任 CA 证书**。
- 要编辑证书，请点击证书的编辑图标 ( )。

步骤 3 键入证书的**名称**。

该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 4 点击**上传证书**（或在编辑时点击**替换证书**），然后选择受信任CA证书文件（例如*.pem）。允许的文件扩展名有 .pem、.cert、.cer、.crt 和 .der。或者，粘贴到受信任 CA 证书中。

证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。

该证书必须为 PEM 或 DER 格式的 X509 证书。

您粘贴的证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行。例如：

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
```

```
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

步骤 5 如果此证书不是由证书颁发机构颁发，请选择**跳过 CA 证书检查 (Skip CA Certificate Check)**。

如果需要将本地 CA 证书安装为受信任的 CA 证书，请跳过此复选框。

步骤 6 设置**验证使用**以限制证书的使用。

某些功能允许您选择是否可以根据特定证书验证连接。您必须在证书中指出这些功能可以有效使用证书，否则连接将被拒绝。

这些选项中未包含的任何功能都可以根据此证书进行验证，而无需明确的使用许可。例如，SSL 解密策略和托管 设备管理器的 Web 服务器会忽略“验证使用”选项。如果您在此字段中选择任何选项，证书将下载到使用 **show running-config** 命令显示的运行配置。

这些选项的主要目的是阻止您建立 VPN 连接，因为它们可以根据特定证书进行验证。

- **SSL 服务器** - 验证远程 SSL 服务器上的证书。用于动态 DNS。
- **SSL 客户端** - 验证远程访问 VPN 传入连接的证书。
- **IPsec 客户端** - 验证 IPsec 站点间 VPN 传入连接的证书。
- **其他** - 验证 LDAPS 等不受 Snort 检测引擎管理的功能。仅当特定功能存在问题时，才选择此选项。**其他**与所有其他选项只能二选其一：您必须先取消选择**其他**，然后才能选择任何其他选项，而且必须先取消选择所有选项，然后才能选择**其他**。

步骤 7 点击**确定 (OK)**。

配置受信任 CA 证书组

使用 SSL 解密策略设置中的外部受信任 CA 证书组指定 SSL 解密策略应信任哪些证书。如果最终用户尝试连接到证书颁发机构的证书不在受信任证书中的站点，则用户会收到一条消息，要求信任该证书。因此，不将证书放在受信任列表中会给最终用户带来不便，但这本身并不能阻止连接（您可以使用访问控制规则来完成连接）。

默认组为 Cisco-Trusted-Authorities。仅在以下情况下，您才需要创建自己的组：

- 您希望信任不在默认组中的证书。然后，您可以在 SSL 解密策略设置中选择默认组和新组。
- 您希望信任的证书列表比默认组限制更严格。然后，您将创建一个具有受信任证书的完整列表（而不只是您所增加的受信任证书）的组，并将其选择为 SSL 解密策略设置中的唯一组。

开始之前

上传您将添加到组中的所有受信任 CA 证书（如果它们尚未进入系统中）。

过程

步骤 1 选择**对象**，然后从目录中选择**证书**。

步骤 2 执行以下操作之一：

- 要创建新证书组，请点击 并选择**添加证书组**。
- 要编辑证书组，请点击该组的编辑图标 ( )。

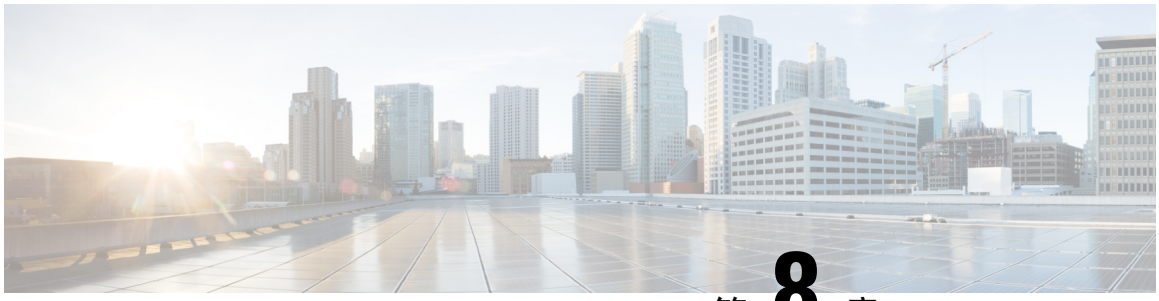
步骤 3 为证书组输入**名称**和说明（后者为可选项）。

步骤 4 点击 + 将证书添加到组。

在组中添加您需要的所有证书。在构建组时，您可以点击**创建新的受信任 CA 证书**以上传新证书。

如果您不再需要组中的证书，请点击证书的 X 图标（右侧）。

步骤 5 点击**确定 (OK)**。



第 8 章

身份源

身份源是定义用户账户的服务器和数据库。身份源信息具有多种用途，例如提供与IP地址关联的用户身份，或是对远程访问 VPN 连接或到 设备管理器的访问进行身份验证。

以下主题介绍如何定义身份源。后期配置需要使用身份源的服务时，可以使用这些对象。

关于身份源

身份源是为组织内的人员定义用户账户的AAA服务器和数据库。身份源信息具有多种用途，例如提供与 IP 地址关联的用户身份，或是对远程访问 VPN 连接或到 设备管理器的访问进行身份验证。

使用**对象 (Objects)** > **身份源 (Identity Sources)** 页面可以创建和管理您的源。后期在配置需要身份源的服务时，会用到这些对象。

以下是受支持的身份源及其用途：

Active Directory (AD) 身份领域

Active Directory 可提供用户账户和身份验证信息。请参阅 Active Directory (AD) 身份领域， 第 153 页。

您可以将此源用于以下目的：

- 远程访问 VPN，作为主要身份源。您可以配合使用 AD 和 RADIUS 服务器。
- 身份策略，用于主动身份验证，并作为用户身份源用于被动身份验证。

Active Directory (AD) 领域序列

AD 领域序列是 AD 领域对象的有序列表。如果您在网络中管理多个 AD 域，则领域序列将非常有用。请参阅 配置 AD 领域序列， 第 157 页。

您可以将此源用于以下目的：

- 身份策略，作为用户身份源用于被动身份验证。序列中的领域顺序决定了在存在冲突的极少数情况下系统确定用户身份的方式。

思科身份服务引擎 (ISE) 或思科身份服务引擎被动身份连接器 (ISE-PIC)

如果使用 ISE，可以将 威胁防御设备与您的 ISE 部署集成。请参阅 身份服务引擎 (ISE)，第 162 页。

您可以将此源用于以下目的：

- 身份策略，作为被动身份源来从 ISE 收集用户身份信息。

RADIUS 服务器、RADIUS 服务器组

如果您使用的是 RADIUS 服务器，还可以将其与 设备管理器配合使用。必须将每个服务器定义为单独的对象，然后将其归入服务器组（其中，指定组中的服务器是彼此的副本）。为服务器组分配功能，但不为单个服务器分配功能。请参阅 RADIUS 服务器和组，第 158 页。

您可以将此源用于以下目的：

- 远程访问 VPN 用作身份验证、授权和记账的身份源。您可以配合使用 AD 和 RADIUS 服务器。
- 身份策略，作为被动身份源来从远程访问 VPN 登录收集用户身份信息。
- 对 设备管理器 或 威胁防御 CLI 管理用户进行外部身份验证。可以支持具有不同授权级别的多个管理用户。这些用户可以登录到系统进行设备配置和监控。

SAML 服务器

安全断言标记语言 2.0 (SAML 2.0) 是一种开放标准，用于在各方（尤其是身份提供程序 [IdP] 和运营商 [SP]）之间交换身份验证和授权数据。

您可以将此源用于以下目的：

- 远程访问 VPN，作为单点登录 (SSO) 身份验证源。
- 对 设备管理器用户进行外部身份验证。可以支持具有不同授权级别的多个管理用户。这些用户可以登录到系统进行设备配置和监控。

LocalIdentitySource

这是本地用户数据库，其中包括您在 设备管理器中定义的用户。选择 **对象** > **用户** 管理此数据库中的用户账户。请参阅本地用户，第 168 页。

注释 本地身份源数据库不包含您在 CLI 中配置（使用 **configure user add** 命令）以进行 CLI 访问的用户。CLI 用户与您在 设备管理器中创建的用户是完全独立的。

您可以将此源用于以下目的：

- 远程访问 VPN，作为主要身份源或回退身份源。
- 身份策略，作为被动身份源来从远程访问 VPN 登录收集用户身份信息。

Active Directory (AD) 身份领域

Microsoft Active Directory (AD) 定义用户账户。您可以为 Active Directory 域创建 AD 身份领域。以下主题介绍如何定义 AD 身份领域。

支持的目录服务器

可以使用 Windows Server 2012、2016 和 2019 上的 Microsoft Active Directory (AD)。

请注意以下有关服务器配置的信息：

- 如果要对用户组或组内用户执行用户控制，则必须在目录服务器上配置用户组。如果服务器按照基本对象层次结构组织用户，系统无法执行用户组控制。
- 目录服务器必须使用下表中列出的字段名称，以便系统从该域的服务器中检索用户元数据。

元数据	**Active Directory** 字段
LDAP 用户名	samaccountname
名字	givenname
姓氏	sn
邮箱地址	mail Userprincipalname（如果 mail 没有值）
部门	department distinguishedname（如果 department 没有值）
电话号码	telephonenumber

对用户数量的限制

设备管理器 可以从目录服务器下载多达 50,000 个用户的信息。

如果您的目录服务器上有超过 50,000 个用户账户，则在访问规则中选择用户时或查看基于用户的控制面板信息时，您不会看到所有可能的名称。您仅可以对已下载的名称编写规则。

此限制也适用于与组相关联的名称。如果组成员超过 50,000 个，则只能将下载的 50,000 个名称与组成员身份进行匹配。

确定目录基准标识名

配置目录属性时，需要为用户和组指定公共基准标识名(DN)。基准在您的目录服务器中定义，并且会因网络而不同。您必须输入正确的基准，身份策略才能正常使用。如果基准错误，则系统无法确定用户名或组名，进而导致基于身份的策略无法使用。

提示 要获得正确的基准，请咨询目录服务器的管理员。

对于 Active Directory，您可以用域管理员的身份登录 Active Directory 服务器，并按照如下所示在命令提示符后输入 **dsquery** 命令来确定正确的基准：

用户搜索库

输入 **dsquery user** 命令时加上已知用户名（部分或完整），以确定基准标识名。例如，以下命令使用部分名称“John*”返回以“John.”开头的所有用户的信息。

```
C:\Users\Administrator>dsquery user -name “John*”
“CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com”
```

基准 DN 为 “DC=csc-lab,DC=example,DC=com”。

组搜索基准

输入 **dsquery group** 命令时加上已知用户名，以确定基准标识名。例如，以下命令使用组名称 Employees 返回标识名：

```
C:\>dsquery group -name “Employees”
“CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com”
```

组基准 DN 为 “DC=csc-lab,DC=example,DC=com”。

此外，还可以使用 ADSI Edit 程序浏览 Active Directory 结构（**开始** > **运行** > **adsiedit.msc**）。在“ADSI 编辑”(ADSI Edit) 中，右键点击任意对象，例如组织单位 (OU)、组或用户，然后选择**属性 (Properties)** 查看标识名。然后，可以复制 DC 值的字符串作为基准。

要验证您是否获得了正确的基准，请执行以下操作：

1. 点击目录属性中的“测试连接”(Test Connection) 按钮验证连接。解决所有问题后，保存目录属性。
2. 提交对设备的更改。
3. 创建访问规则，选择**用户**选项卡，并尝试从目录添加已知的用户和组名称。在您键入内容时，系统会自动填充建议，以匹配包含该目录的领域中的用户和组。如果这些建议显示在一个下拉列表中，则说明系统可以成功查询目录。如果您没有看到建议，而且确定您键入的字符串应显示在用户或组名称中，则需要更正相应的搜索基准。

配置 AD 身份领域

身份领域是目录服务器加上提供身份验证服务所需的其他属性。目录服务器包含有权访问您网络的用户和用户组的相关信息。

对于 Active Directory，领域就等于 Active Directory 域。为需要支持的各个 AD 域创建单独的领域。

领域用于以下策略中：

- 身份 - 领域提供用户身份和组成员身份信息，然后您可将这些信息用于访问控制规则。系统每天都会在当天的最后一个小时 (UTC) 下载有关所有用户和组更新后的信息。必须能够从管理接口访问目录服务器。
- 远程访问 VPN - 领域提供身份验证服务，用于确定是否允许接入某个连接。必须能够从 RA VPN 外部接口访问目录服务器。
- 访问控制和 SSL 解密 - 您可以在规则的用户条件中选择领域，以便对此领域内的所有用户应用此规则。

与您的目录管理员一起获取配置目录服务器属性所需的值。

注释 如果目录服务器不在相连的网络中或无法通过默认路由使用，请为该服务器创建静态路由。依次选择**设备** > **路由** > **查看配置**，创建静态路由。或者，在定义服务器时选择适当的接口。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑领域属性时，点击对象列表中所示的**创建新身份领域**链接来创建身份领域对象。

开始之前

确保目录服务器、威胁防御设备和客户端之间的时间设置一致。这些设备间的时间偏差可能会导致用户身份验证操作失败。“一致”说明您可以使用不同的时区，但时间相对于这些时区应是相同的；例如，10 AM PST = 1 PM EST。

过程

步骤 1 选择**对象**，然后从目录中选择**身份源**。

步骤 2 执行以下操作之一：

- 要创建 AD 领域，请点击 + > **AD**。
- 要编辑领域，请点击此领域的编辑图标 ( )。

要删除未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置基本领域属性。

- **名称** - 目录领域的名称。

- **类型** - 目录服务器的类型。Active Directory 是唯一支持的类型，所以无法更改此字段。
- **目录用户名、目录密码** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

  注释　系统使用此信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=administrator,cn=users,dc=example,dc=com。请注意，cn＝users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

- **基准 DN** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如，cn=users,dc=example,dc=com。有关查找基准 DN 的信息，请参阅确定目录基准标识名，第 154 页。
- **AD 主域** - 设备应加入的 Active Directory 完全限定域名。例如 example.com。

步骤 4 配置目录服务器属性。

- **主机名/IP 地址** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。
- **接口** - 应通过其访问 AD 服务器的接口。如果不选择接口，系统会使用数据路由表查找合适的接口。如果您要使用某个管理专用接口，则必须明确选择该接口；不能在管理专用路由表中使用路由查找。
- **端口** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。
- **加密** - 要使用加密连接下载用户和组信息，请选择所需的方法 **STARTTLS** 或 **LDAPS**。系统默认为**无**，也就是说以明文形式下载用户和组信息。
  - **STARTTLS** 将会协商加密方法，并使用目录服务器支持的最强方法。使用端口 389。如果将领域用于远程访问 VPN，则不支持此选项。
  - **LDAPS** 需要基于 SSL 的 LDAP。使用端口 636。
- **受信任的 CA 证书** - 如果选择加密方法，请上传证书颁发机构 (CA) 证书以便在系统和目录服务器之间启用受信任的连接。如果要使用证书进行身份验证，则证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。

步骤 5 如果领域有多个服务器，请点击**添加其他配置**，并输入每个额外服务器的属性。

您可以将最多 10 个 AD 服务器添加到领域。这些服务器需要彼此复制并支持相同的 AD 域。

为方便起见，您可以折叠和展开每个服务器条目。用主机名/IP 地址和端口标记各个部分。

步骤 6 点击**测试**按钮验证系统是否可以与服务器通信。

系统使用单独的进程和接口访问服务器，因此您可能会收到错误通知，指出连接适用于一种用途而不适用于另一种用途，例如可用于身份策略，但不可用于远程访问 VPN。如果无法访问服务器，请确认IP地址和主机名正确、DNS服务器具有该主机名的条目等。您可能需要为该服务器配置静态路由。有关详细信息，请参阅目录服务器连接故障排除，第 157 页。

步骤 7 点击**确定 (OK)**。

配置 AD 领域序列

您可以在被动身份规则中使用 AD 领域序列，以便系统可以尝试匹配多个 AD 服务器中的用户。在领域序列中，配置 AD 领域的有序列表，其中每个 AD 服务器管理不同的领域或域，例如 engineering.example.com 和 marketing.example.com。

仅当您支持多个 AD 域且来自不同域的用户可能通过 威胁防御 设备发送流量时，领域序列才有用。这些领域可用于为使用被动身份验证的用户会话查找身份。在极少数可能发生冲突的情况下，可以使用领域顺序解决身份冲突。

过程

步骤 1 选择**对象**，然后从目录中选择**身份源**。

步骤 2 执行以下操作之一：

- 要创建 AD 领域序列，请依次点击 + > **AD 领域序列**。
- 要编辑 AD 领域序列，请点击该对象的编辑图标 ( )。

要删除未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置领域序列属性：

- **名称** - 对象的名称。
- **说明** - 对象的可选说明。
- **AD 领域** - 点击 + 将 AD 领域对象添加到序列中。添加领域后，点击并将领域拖放到所需的有序序列中。

步骤 4 点击**确定**。

现在，您可以在被动身份规则中选择 AD 领域序列。

目录服务器连接故障排除

系统使用不同的进程与您的目录服务器通信，具体取决于服务器的功能。因此，身份策略的连接可以正常工作，而远程访问 VPN 的连接则失败。

这些进程使用不同的接口与目录服务器进行通信。您必须确保这些接口的连接性。

- 管理接口，用途：身份策略。
- 数据接口，用途：远程访问 VPN（外部接口）。

配置身份领域时，请使用**测试**按钮验证连接是否可以正常工作。失败消息应指示该功能存在连接问题。根据身份验证属性和路由/接口配置，以下是您可能会遇到的常规问题。

目录用户身份验证问题。

如果问题是系统因用户名或密码而无法登录目录服务器，请确保用户名和密码正确并在目录服务器上有效。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

此外，系统还会根据用户名和密码信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=administrator,cn=users,dc=example,dc=com。请注意，cn = users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

目录服务器可通过数据接口进行访问。

如果目录服务器所在的网络直接连接到数据接口（例如千兆以太网接口）或是可从直连网络路由，那么您必须确保虚拟管理接口与目录服务器之间存在路由。

- 使用 **data-interfaces** 作为管理网关应该能够确保路由成功。
- 如果管理接口上有显式网关，则该网关路由器需要与目录服务器之间建立路由。
- 如果直连网络与托管目录服务器的网络之间存在路由器，则为目录服务器配置静态路由(**设备** > **路由**)。
- 验证数据接口的 IP 地址和子网掩码是否正确。

目录服务器位于外部网络上。

如果目录服务器位于外部（上行链路）接口另一端的网络，您可能需要配置站点间VPN连接。有关详细程序，请参阅如何通过远程访问 VPN 使用外部网络上的目录服务器，第 701 页。

RADIUS 服务器和组

您可以使用 RADIUS 服务器对 远程访问 VPN 连接以及 设备管理器 和 威胁防御 CLI 管理用户进行身份验证和授权。例如，如果您还使用 Cisco Identity Services Engine (ISE) 及其 RADIUS 服务器，可以将该服务器与 设备管理器 搭配使用。

配置要使用 RADIUS 服务器的功能时，您应选择 RADIUS 组而不是单个服务器。RADIUS 组所含 RADIUS 服务器是彼此副本的集合。如果一个组具有多个服务器，这些服务器可构成备份服务器链，在其中一台服务器不可用时提供冗余。但即使只有一台服务器，也必须创建包含一个成员的组，以配置功能的 RADIUS 支持。

以下主题介绍如何配置 RADIUS 服务器和组，以便它们可用于支持的功能。

配置 RADIUS 服务器

RADIUS 服务器提供 AAA（身份验证、授权和记账）服务。如果您使用 RADIUS 服务器进行用户身份验证和授权，可以将这些服务器与 设备管理器搭配使用。

为每个 RADIUS 服务器创建对象后，创建 RADIUS 服务器组，以包含每个重复服务器组。

开始之前

如果您想要为 RA VPN 配置重定向 ACL，在创建和编辑服务器对象之前，您必须使用 Smart CLI 创建扩展 ACL。在编辑对象时，您无法创建 ACL。

过程

步骤 1 选择**对象**，然后从目录中选择**身份源**。

步骤 2 执行以下操作之一：

- 要创建对象，请依次点击 **+** > **RADIUS 服务器**。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置以下属性：

- **名称** - 对象的名称。这不需要与服务器上配置的任何内容匹配。
- **服务器名称或 IP 地址** - 服务器的完全限定主机名 (FQDN) 或 IP 地址。例如，radius.example.com 或 10.100.10.10.
- **身份验证端口** - 在其上执行 RADIUS 身份验证和授权的端口。默认值为 1812。
- **超时** - 系统将请求发送至下一服务器之前等待服务器响应的时长，此为 1-300 秒之间的数值。默认值为 10 秒。如果您将此服务器用作远程访问 VPN 的辅助身份验证源，例如用于提示输入身份验证令牌，请将超时时间至少延长到 60 秒，以便让用户有时间获取和输入令牌。
- **服务器密钥** -（可选。）用于加密 威胁防御设备和 RADIUS 服务器之间数据的共享密钥。该密钥是一个区分大小写的字母数字字符串，最多 64 个字符，且不含空格。密钥必须以字母数字字符或下划线开头，它可以包含特殊字符：$ & - _ . + @。字符串必须匹配 RADIUS 服务器上配置的字符串。如果不配置密钥，则不加密连接。

步骤 4 （可选。）如果您使用服务器进行远程访问 VPN 授权更改配置，您可以点击**仅限于 RA VPN** 链接并配置以下选项。

- **重定向 ACL** - 选择要用于 RA VPN 重定向 ACL 的扩展 ACL。在**设备 (Device)** > **高级配置 (Advanced Configuration)** > **智能 CLI (Smart CLI)** > **对象 (Objects)**页面上使用 Smart CLI **扩展访问列表 (Extended Access List)**创建扩展 ACL。

重定向 ACL 的目的是将初始流量发送到思科身份服务引擎 (ISE)，以便 ISE 可以评估客户端安全状况。ACL 应向 ISE 发送 HTTPS 流量，而非已设定发往 ISE 的流量或被定向到域名解析 DNS 服务器的流量。有关示例，请参阅在 威胁防御 设备上配置授权更改，第 685 页。

- **用于连接 RADIUS 服务器的接口** - 与该服务器通信时要使用的接口。如果您选择**通过路由查找解决**，系统将始终使用数据路由表来确定要使用的接口。如果您选择**手动选择接口**，系统将始终使用您选择的接口。如果您要使用某个管理专用接口，则必须明确选择该接口；不能对管理专用路由表使用路由查找。

  如果您在配置授权更改，则必须选择特定接口，以便系统可以在该接口上正确启用 CoA 侦听程序。

  如果此服务器还用于 设备管理器 管理访问，则此接口将被忽略。系统始终通过管理 IP 地址对管理访问尝试进行身份验证。

步骤 5 （可选，仅编辑对象时）点击**测试**检查系统是否可以连接到服务器。

系统会提示输入用户名和密码。测试确认是否可以连接服务器，如果可以连接，则确认是否可以对用户名进行身份验证。

步骤 6 点击**确定 (OK)**。

配置 RADIUS 服务器组

RADIUS 服务器组中包含一个或多个 RADIUS 服务器对象。组中的服务器必须是彼此的备份。这些服务器构成备份服务器链，因此，如果第一台服务器不可用，系统可以尝试列表中的下一个服务器。

在一项功能中配置 RADIUS 支持时，必须选择服务器组。因此，即使只有一台 RADIUS 服务器，也必须创建包含该服务器的组。

过程

步骤 1 选择**对象**，然后从目录中选择**身份源**。

步骤 2 执行以下操作之一：

- 要创建对象，请依次点击 + > **RADIUS 服务器组 (RADIUS Server Group)**。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置以下属性：

- **名称** - 对象的名称。这不需要与服务器上配置内容匹配。
- **断路时间** - 只有当所有服务器均发生故障时，才会重新激活故障服务器。断路时间是指最后一台服务器发生故障后，在重新激活所有服务器之前所等待的时间，其值为 0-1440 分钟。仅当配

置回退到本地数据库时，失效时间时间才适用；身份验证将在本地尝试，直到失效时间结束。默认值为 10 分钟。

- **最大失败尝试次数** - 尝试组中下一个服务器之前发送到 RADIUS 服务器的失败 AAA 事务（即，未收到响应的请求）的数量。您可以指定 1 到 5 之间的数字，默认值为 3。超过最大失败尝试次数时，系统会将服务器标记为故障。

  对于给定功能，如果您使用本地数据库配置回退方法，并且组中的所有服务器都无法响应，则会将该组视为无法响应，并将尝试回退方法。该服务器组会在断路时间内保持标记为无响应，以确保该时段内其他 AAA 请求不会尝试联系该服务器组，而是立即使用回退方法。

- **动态授权（仅限于 RA VPN）**、**端口** - 如果为此 RADIUS 服务器组启用 RADIUS 动态授权或授权更改 (CoA) 服务，该组会注册 CoA 通知并侦听指定的端口，以便使 CoA 策略从思科身份服务引擎 (ISE) 进行更新。默认侦听端口为 1700，也可以指定 1024 到 65535 范围内的其他端口。仅当您在远程访问 VPN 中结合 ISE 使用此服务器组时，才能启用动态授权

- **支持 RADIUS 服务器的领域** - 如果 RADIUS 服务器配置为使用 AD 服务器对用户进行身份验证，请选择指定了与此 RADIUS 服务器结合使用的 AD 服务器的 AD 领域。如果尚不存在此领域，请点击列表底部的**创建新身份领域 (Create New Identity Realm)** 立即配置。

- **RADIUS 服务器列表** - 选择为该组定义服务器的最多 16 个 RADIUS 服务器对象。按优先级顺序添加这些对象。使用列表中的第一个服务器，直至此服务器无法响应。添加对象后，您可以通过拖放重新排列对象。如果所需的对象尚不存在，请点击**创建新的 RADIUS 服务器 (Create New RADIUS Server)** 立即添加对象。

  您也可以点击**测试 (Test)** 链接，验证系统是否可以连接到服务器。系统会提示输入用户名和密码。测试确认是否可以连接服务器，如果可以连接，则确认是否可以对用户名进行身份验证。

步骤 4 （可选。）点击**测试所有服务器 (Test All Servers)** 按钮，检查到组中每台服务器的连接。

系统会提示输入用户名和密码。系统会检查是否可以连接每个服务器，以及用户名是否可在每台服务器上进行身份验证。

步骤 5 点击**确定 (OK)**。

RADIUS 服务器和组故障排除

当外部授权无法使用时，您可以检查以下事项。

- 使用 RADIUS 服务器和服务器组对象中的**测试**按钮，验证是否可以从设备连接到服务器。务必在测试之前保存对象。如果测试失败：
  - 请注意，测试会忽略为服务器配置的接口，且始终使用管理接口。如果未将 RADIUS 身份验证代理配置为响应来自管理 IP 地址的请求，则测试预期失败。
  - 验证您在测试期间是否输入了正确的用户名/密码组合。如果用户名/密码组合不正确，您将收到凭证错误消息。

- 验证服务器的加密密钥、端口和 IP 地址。如果使用主机名，验证是否为管理接口配置了 DNS。考虑在 RADIUS 服务器上更改了密钥，但未在设备配置中更改的可能性。
- 如果测试仍然失败，您可能需要配置到 RADIUS 服务器的静态路由。请尝试从 CLI 控制台或 SSH 会话对服务器执行 ping 操作，检查是否可以访问服务器。

- 如果外部身份验证一直都在工作，却停止了工作，请考虑是否会出现所有服务器均处于空载时间的情况。如果配置回退到本地身份验证，在组内的所有 RADIUS 服务器都发生故障时，空载时间是系统在再次尝试连接第一个服务器之前等待的分钟数。在停滞时间内会使用本地身份验证，因此给定用户的用户名和密码将是本地用户名/密码。默认时间为 10 分钟，不过您可以配置最长 1440 分钟。
- 如果 HTTPS 外部身份验证对一部分用户适用，对另一部分用户不适用，请评估 RADIUS 服务器中为每个用户账户定义的 cisco-av-pair 属性。此属性可能未正确配置。属性缺失或不正确将阻止对该用户账户的所有 HTTS 访问。
- 如果 SSH 外部身份验证对一部分用户适用，对另一部分用户不适用，请评估 RADIUS 服务器中为每个用户账户定义的 Service-Type 属性。此属性可能未正确配置。属性缺失或不正确将阻止对该用户账户的所有 SSH 访问。

身份服务引擎 (ISE)

您可以将思科身份服务引擎 (ISE) 或 ISE 被动身份连接器 (ISE-PIC) 部署与 威胁防御设备相集成，以使用 ISE/ISE-PIC 进行被动身份验证。

ISE/ISE-PIC 是一个授权身份源，并为使用 Active Directory (AD)、LDAP、RADIUS 或 RSA 进行身份验证的用户提供用户感知数据。但是，对于 威胁防御，您只能将 ISE 与 AD 配合使用，以获悉用户身份。除查看各种监控控制面板和事件中的用户信息之外，还可以将用户身份用作访问控制和SSL解密策略中的匹配条件。

有关 Cisco ISE/ISE-PIC 的更多信息，请参阅《思科身份服务引擎管理员指南》(https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html) 和《身份服务引擎被动身份连接器 *(ISE-PIC)* 安装和管理员指南》(https://www.cisco.com/c/en/us/support/security/ise-passive-identity-connector/tsd-products-support-series-home.html)。

ISE 的准则和限制

- 由于系统不将设备身份验证与用户关联，因此防火墙系统不支持与 Active Directory 身份验证同时进行 802.1x 设备身份验证。如果使用 802.1x 主动登录，则将 ISE 配置为仅报告 802.1x 主动登录（设备和用户）。这样，仅向系统报告一次设备登录。
- ISE/ISE-PIC 不报告 ISE 访客服务用户的活动。
- 同步 ISE/ISE-PIC 服务器和设备上的时间。否则，系统可能会以意外间隔执行用户超时。
- 如果将 ISE/ISE-PIC 配置为监控大量用户组，则由于内存限制，系统可能会根据组丢弃用户映射。因此，带有领域或用户条件的规则可能不会按预期执行。

- 有关与此版本的系统兼容的 ISE/ISE-PIC 的特定版本，请参阅 *Cisco Secure Firewall* 兼容性指南，https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-device-support-tables-list.html。
- 使用 ISE 服务器的 IPv4 地址，除非您确认您的 ISE 版本支持 IPv6。

配置身份服务引擎

要使用思科身份服务引擎 (ISE) 或思科身份服务引擎被动身份连接器 (ISE PIC) 作为被动身份源，您必须配置与 ISE 平台交换网格 (pxGrid) 服务器的连接。

开始之前

- 从 ISE 中导出 pxGrid 和 MNT 服务器证书。例如，在 ISE PIC 2.2 上，可在**证书 (Certificates)** > **证书管理 (Certificate Management)** > **系统证书 (System Certificates)** 页面找到这些证书。MNT（监控和故障排除节点）在证书列表的“使用者”列中显示为 Admin。您可以在**对象 (Objects)** > **证书 (Certificates)**页面将它们上传为受信任的 CA 证书，也可以在以下过程中上传这些证书。这些节点可能使用相同的证书。
- 您还必须配置 AD 身份领域。系统从 AD 获取用户列表，从 ISE 获取用户到 IP 地址映射的信息。
- 如果您将使用安全组标记 (SGT) 进行访问控制（无论是否具有静态安全组标记映射），并侦听 SXP 主题，则还需要在 ISE 中配置 SXP 和这些映射。请参阅在 ISE 中配置安全组和 SXP 发布，第 494 页。

过程

步骤 1 选择**对象**，然后从目录中选择**身份源**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + > **身份服务引擎 (Identity Services Engine)**。可创建最多一个 ISE 对象。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置以下属性：

- **名称** - 对象的名称。
- **状态 (Status)** - 点击开关以启用或禁用对象。禁用对象时，您不能将 ISE 用作身份规则中的身份源。
- **说明** - 对象的可选说明。
- **主节点主机名/IP 地址** - 主要 pxGrid ISE 服务器的主机名或 IP 地址。不要指定 IPv6 地址，除非确认您的 ISE 版本支持 IPv6。

- **辅助节点主机名/IP 地址 (Secondary Node Hostname/IP Address)** - 如果您设置辅助 ISE 服务器以实现高可用性，请点击**添加辅助节点主机名/IP 地址 (Add Secondary Node Hostname/IP Address)** 并输入辅助 pxGrid ISE 服务器的主机名或 IP 地址。
- **pxGrid 服务器 CA 证书** - 受信任的 pxGrid 框架证书颁发机构证书。如果部署包括主要和辅助 pxGrid 节点，则两个节点的证书必须由同一证书颁发机构签署。
- **MNT 服务器 CA 证书** - 执行批量下载时 ISE 证书的受信任的证书颁发机构证书。如果您的 MNT（监控和故障排除）服务器不是单独的服务器，此证书可能与 pxGrid 服务器证书相同。如果部署包括主要和辅助 MNT 节点，则两个节点的证书必须由同一证书颁发机构签署。
- **服务器证书** - 连接 ISE 或执行批量下载时，威胁防御设备必须向 ISE 提供的内部身份证书。
- **订用** - 选择应订用哪个 ISE pxGrid 主题。订用主题意味着您将下载与该主题相关的数据。
  - **会话目录主题** - 是否获取有关用户会话的信息，包括用户会话的 SGT 映射。默认情况下，此选项已启用。如果要获取被动用户身份以在安全策略中使用并在监控控制面板中实现可视化，则应选择此选项。
  - **SXP 主题** - 是否获取静态“SGT 到 IP”地址映射。如果要基于安全组标记 (SGT) 编写访问控制规则，请选择此主题。
- **ISE 网络过滤器** - 可设置用来限制 ISE 向系统报告的数据的可选过滤器。如果提供网络过滤器，ISE 会仅报告网络上符合过滤器要求的数据。点击 **+**，选择标识网络的网络对象，然后点击**确定 (OK)**。如果您需要创建对象，点击**创建新网络 (Create New Network)**。仅配置 IPv4 网络对象。

步骤 4 点击**测试 (Test)** 按钮，验证系统是否可以连接到 ISE 服务器。

如果测试失败，请点击**查看日志 (See Logs)** 链接了解详细的错误消息。例如，以下消息表示系统无法在规定端口连接到服务器。存在的问题可能是，没有路由到主机（即 ISE 服务器未使用预期端口），或访问控制规则阻止这类连接。

```
Captured Jabberwerx log:2018-05-11T16:10:30 [   ERROR]: connection timed out while
trying to test connection to host=10.88.127.142:ip=10.88.127.142:port=5222
```

步骤 5 点击**确定 (OK)** 保存对象。

下一步做什么

配置 ISE 后，启用身份策略，配置被动身份验证规则，并部署配置。然后，您必须转到 ISE/ISE PIC 并接受设备作为订阅方。如果您配置 ISE/ISE PIC 自动接受订阅方，无需手动接受订用。

ISE/ISE-PIC 身份源故障排除

ISE/ISE-PIC 连接

如果您遇到 ISE 或 ISE-PIC 连接问题，请检查以下事项：

- 必须启用 ISE 中的 pxGrid 身份映射功能，才能将 ISE 与 威胁防御设备成功集成。
- 在 ISE 服务器与 威胁防御设备成功建立连接之前，您必须手动在 ISE 中批准客户端。

  或者，您可以在ISE中启用**自动审批新账户**，具体操作请参照《思科身份服务引擎管理员指南》中有关管理用户和外部身份源的章节。
- 威胁防御设备（服务器）证书必须包含 **clientAuth** 扩展密钥用法值，否则不能包含任何扩展密钥用法值。如果设置了 clientAuth 扩展密钥用法，还必须选择不设置密钥用法，或设置数字签名密钥用法值。使用 设备管理器 创建的自签名身份证书满足这些要求。
- ISE 服务器上的时间必须与 威胁防御上的时间同步。如果设备不同步，系统可能会以非预期时间间隔执行用户超时。

ISE/ISE-PIC 用户数据

如果您遇到 ISE 或 ISE-PIC 报告的用户数据问题，请注意以下事项：

- 系统检测到其数据尚未在数据库中的 ISE 用户的活动后，会从服务器检索其相关信息。ISE 用户发现的活动并非由访问控制规则处理，而且在系统于用户下载中成功检索到这些活动的相关信息之前，活动不会显示在控制面板中。
- 不能对由 LDAP、RADIUS 或 RSA 域控制器进行身份验证的 ISE 用户执行用户控制。
- 系统不会收到 ISE 访客服务用户的用户数据。

SAML 服务器

您可以将安全断言标记语言 2.0 (SAML 2.0) 服务器配置为远程访问 VPN 连接 和设备管理器用户的单点登录 (SSO) 身份验证源。SAML 是用于在各方（尤其是身份提供程序 [IdP] 和服务提供商 [SP]）之间交换身份验证和授权数据的开放标准。

配置 SAML 服务器

您可以将安全断言标记语言 2.0 (SAML 2.0) 服务器配置为远程访问 VPN 连接 和设备管理器用户的单点登录 (SSO) 身份验证源。例如，Duo 接入网关 (DAG) 是 SAML 服务器。

当您使用 SAML 服务器作为身份验证方法时，SAML 服务器充当身份提供程序 (IdP)，而 威胁防御设备充当服务提供商 (SP)。

对于 RA VPN，您可以使用 SAML 服务器作为主要身份验证源，但不能配置辅助身份验证源，也不能配置回退源。

对于设备管理器登录，如果配置 SAML 服务器以支持通用访问卡 (CAC)，则可以在使用 SAML 服务器时使用该卡登录。

开始之前

从 SAML 服务器身份提供程序获取以下信息：如果可能，请以 XML 文件形式下载用户信息，以便轻松上传。

- 实体 ID URL，其提供 SAML 服务器元数据。
- 登录 URL。
- 注销 URL。
- 身份提供程序证书。

过程

步骤 1 执行以下任一项操作即可转到“SAML 服务器”(SAML Servers) 页面：

- 选择**对象**，然后从目录中选择**身份源**。
- 依次选择**设备** > **远程访问 VPN** > **SAML 服务器**。

步骤 2 执行以下操作之一：

- 要创建对象，请依次点击 **+** > **SAML 服务器**。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置以下属性：

- **名称** - 对象的名称。
- **说明** - 对象的可选说明。
- **身份提供程序 (IDP) 实体 ID URL** - 这是用于提供元数据 XML 的页面的 URL（元数据 XML 说明 SAML 颁发者将如何响应请求）。有些 SAML 服务器产品称之为实体 ID，有些称之为元数据 URL。此 URL 必须为 4-256 个字符，包括协议 https://。例如 https://191.168.2.21/dag/saml2/idp/metadata.php。

  注释 如果以 XML 文件形式从 SAML 服务器下载信息，请点击**从 XML 文件填充 (Populate from XML file)** 并选择该文件。可以从 XML 文件中填充此字段以及**登录 URL (Sign-In URL)** 和**身份提供程序证书 (Identity Provider Certificate)**。

- **登录 URL** - 用于登录到身份提供程序 SAML 服务器的 URL。此 URL 必须介于 4-500 个字符之间，包括协议。允许使用 http:// 和 https://。例如 https://191.168.2.21/dag/saml2/idp/SSOService.php。
- **注销 URL** - 用于注销身份提供程序 SAML 服务器的 URL。此 URL 必须介于 4-500 个字符之间，包括协议。允许使用 http:// 和 https://。例如 https://191.168.2.21/dag/saml2/idp/SingleLogoutService.php。

- **服务提供商证书**- 用于 威胁防御 设备的内部证书。理想情况下，您已上传由获认可的第三方签名的证书，现在可以选择该证书。您还可以使用内置的DefaultInternalCertificate，或点击**创建新内部证书**并立即上传签名证书。SAML 服务器身份提供程序必须信任此证书，因此您可能需要将其上传到 SAML 服务器。有关如何上传证书或以其他方式启用与服务提供商的信任关系的信息，请参阅 SAML 服务器文档。
- **身份提供程序证书** - SAML 服务器身份提供程序的受信任 CA 证书。从 SAML 服务器下载此证书。如果尚未上传，请点击**创建新的受信任 CA 证书**并立即上传。
- **请求签名** - 为登录请求签名时使用的加密算法。选择“无”可禁用加密。否则，请选择以下一个选项（按从弱到强的顺序排序）：SHA1、SHA256、SHA384、SHA512。
- **请求超时** - SAML 断言具有有效时间段：用户必须在此有效时间段内完成单点登录请求。您可以设置超时时间值（以秒为单位）以更改此有效时间段。如果设置的超时时间长于断言的NotOnOrAfter条件，系统将忽略您设置的超时时间值，并且NotOnOrAfter条件将生效。范围为1-7200 秒。默认值为 300 秒。
- **此 SAML 身份提供程序 (IDP) 位于内部网络上** - SAML 服务器是否在内部网络上运行，而不是在受保护网络外部运行。
- **在登录时请求重新执行 IDP 身份验证** - 选择此选项可使用户在每次登录时重新进行身份验证，而不是让 SAML 服务器重新使用以前的身份验证会话。默认情况下，此选项已启用。

步骤 4 点击 **用户角色** 并为外部用户配置 RBAC 授权角色。

- **默认用户角色**-分配用户的授权角色（如果无法通过此页面上的设置确定）。
- **组成员属性**-SAML 服务器中定义用户的 RBAC 授权角色的用户属性。
- **角色映射**-对于每个角色，键入将在SAML用户记录的组成员属性中显示的字符串，该字符串应与该角色对应。
  - **管理员**-对应用的所有方面具有完全读写访问权限的用户。
  - **加密管理员 (Cryptographic Admin)** - 可以配置与加密相关的功能（例如证书、解密策略和密钥）的用户。对其他功能的只读权限。
  - **审核管理员 (Audit Admin)** - 可以查看用户登录历史记录和审计日志并执行审核相关操作的用户。对配置功能的只读权限。
  - **读写**-用户可以执行只读用户可以执行的任何操作，但还可以编辑和部署配置。唯一的限制是无法执行关键系统操作，包括安装升级、创建和恢复备份、查看审核日志以及中止其他设备管理器 用户的会话。
  - **只读**-用户可以查看控制面板和配置，但不能进行任何更改。如果尝试进行更改，错误消息会解释由于缺乏权限出错。

步骤 5 点击**确定 (OK)**。

下一步做什么

如果启用了**请求签名 (Request Signature)** 来加密通信，则需要将设备管理器信息上传到 SAML 服务器。从身份源列表中，点击服务器的**下载 (Download)** ( ) 按钮，然后保存 XML 文件。然后，登录 SAML 服务器并上传信息。有关详细信息，请参阅 SAML 提供商文档。

如果使用服务器进行设备管理器登录，但无法正常工作，请验证 SAML 服务器配置。

- 登录 SAML IdP 并验证设备管理器 SAML 响应使用者是否已正确配置。值应为：https://<FDM_URL>/api/fdm/latest/fdm/token
- 如果在 SAML 服务器对象中启用了签名，请确保将设备管理器公共证书上载到 SAML 应用中，然后启用加密。上传设备管理器 XML 文件应会将证书添加到 SAML 服务器。您也可以通过 FDM API 来检索设备管理器证书：https://<FDM_URL>/saml/metadata

本地用户

本地用户数据库 (LocalIdentitySource) 包括您在 设备管理器中定义的用户。

您可以将本地定义的用户用于以下目的：

- 远程访问 VPN，作为主要身份源或回退身份源。
- 管理访问权限，作为 设备管理器 用户的主要或辅助源。

  admin 用户是系统定义的本地用户。但是，管理员用户无法登录远程访问 VPN。您不能创建额外的本地管理用户。

  如果您定义管理访问的外部身份验证，登录到设备的外部用户将显示在本地用户列表中。
- 身份策略，作为被动身份源间接从远程访问 VPN 登录收集用户身份。

以下主题介绍如何配置本地用户。

配置本地用户

您可以直接在设备上创建与远程访问VPN搭配使用的用户账户。您可以使用本地用户账户代替外部身份验证源，或与后者搭配使用。

如果您使用本地用户数据库作为远程访问VPN的回退身份验证方式，请确保在本地数据库中配置与外部数据库中的名称相同的用户名/密码。否则，回退机制将无效。

此处定义的用户无法登录设备 CLI。

过程

步骤 1 依次选择**对象** > **用户**。

列表将显示用户名和服务类型，可以是：

- MGMT - 针对可以登录到 设备管理器的管理用户。始终定义管理员用户，并且无法将其删除。也不能配置其他MGMT用户。但是，如果您定义管理访问的外部身份验证，登录到设备的外部用户将作为 MGMT 用户显示在本地用户列表中。
- 远程访问 VPN - 针对可以登录到设备上配置的远程访问 VPN 的用户。您还必须选择主要或辅助（回退）源的本地数据库。

步骤 2 执行以下操作之一：

- 要添加用户，请点击 +。
- 要编辑用户，请点击该用户的编辑图标 ()。

如果您不再需要特定用户账户，请点击该用户的删除图标 ()。

步骤 3 配置用户属性：

用户名和密码可以包含除空格和问号之外的任何可打印 ASCII 字母数字或特殊字符。可打印的字符为 ASCII 代码 33-126。

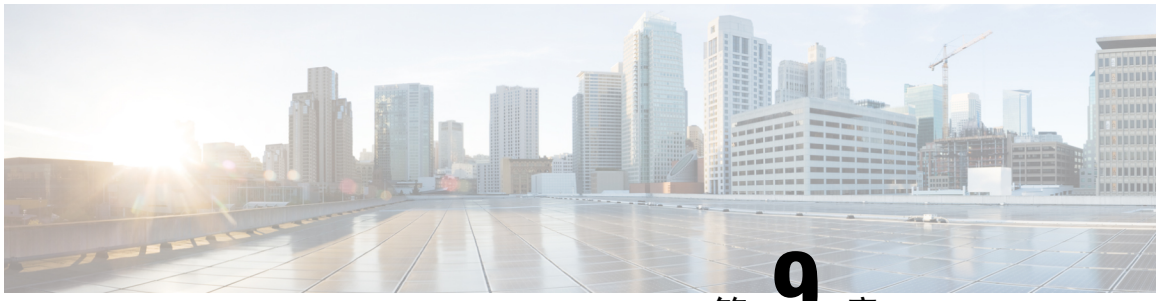
- **名称** - 用于登录远程访问 VPN 的用户名。名称可以是 4 至 64 个字符，但不能包含空格。例如，johndoe。
- **密码**、**确认密码** - 输入账户的密码。密码长度必须介于 8 到 16 个字符之间。它不能包含相同的连续字母。它还必须至少包含以下各项中的一项：数字、大写和小写字符，以及特殊字符。

注释 用户无法更改其密码。告诉他们密码，需要更改密码时，必须编辑用户账户。此外，不要更新外部 MGMT 用户的密码：密码由外部 AAA 服务器控制。

步骤 4 点击**确定 (OK)**。

第 III 部分

基本操作



第 9 章

Firepower 4100/9300 上的逻辑设备

Firepower 4100/9300 是具有灵活性的安全平台，可在其中安装一个或多个逻辑设备。

必须配置机箱接口，添加逻辑设备，并使用 Cisco Secure Firewall 机箱管理器或 FXOS CLI 将接口分配到 Firepower 4100/9300 机箱上的设备。您无法在 设备管理器中执行这些任务。

本章介绍基本的接口配置以及如何使用 机箱管理器添加独立或高可用性逻辑设备。要使用 FXOS CLI，请参阅 FXOS CLI 配置指南。有关更多高级 FXOS 程序和故障排除，请参阅 FXOS 配置指南。

关于接口

Firepower 4100/9300 机箱支持物理接口和 EtherChannel（端口通道）接口。EtherChannel 接口最多可以包含同一类型的 16 个成员接口。

机箱管理接口

机箱管理接口用于通过 SSH 或 机箱管理器来管理 FXOS 机箱。此接口独立于分配给应用管理用逻辑设备的 MGMT 型接口。

要配置此接口参数，必须从 CLI 进行配置。要在 FXOS CLI 中查看此接口，请连接到本地管理并显示管理端口：

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

请注意，即使将物理电缆或小型封装热插拔模块拔下，或者执行了 **mgmt-port shut** 命令，机箱管理接口仍会保持正常运行状态。

注释 机箱管理接口不支持巨型帧。

接口类型

物理接口 和 EtherChannel（端口通道）接口可以是下列类型之一：

- 数据 - 用于常规数据。不能在逻辑设备之间共享数据接口，且逻辑设备无法通过背板与其他逻辑设备通信。对于数据接口上的流量，所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。
- 数据共享 - 用于常规数据。仅容器实例支持这些数据接口，可由一个或多个逻辑设备/容器实例（仅限威胁防御-使用-管理中心 ）共享。
- 管理 - 用于管理应用程序实例。这些接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。只能为每个逻辑设备分配一个管理接口。根据您的应用和管理器，您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。有关独立机箱管理接口的信息，请参阅机箱管理接口 ，第 173 页。

注释 管理接口更改会导致逻辑设备重新启动，例如将管理接口从 e1/1 更改为 e1/2 会导致逻辑设备重新启动以应用新的管理接口。

- 事件 - 用作 威胁防御-using-管理中心 设备的辅助管理接口。

注释 安装每个应用实例时，会分配一个虚拟以太网接口。如果应用不使用事件接口，则虚拟接口将处于管理员关闭状态。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- 集群 - 用作集群逻辑设备的集群控制链路。默认情况下，系统会在端口通道 48 上自动创建集群控制链路。“集群”类型仅在 EtherChannel 接口上受支持。设备管理器 和 CDO 不支持集群。

FXOS 接口与应用接口

Firepower 4100/9300 管理物理接口和 EtherChannel（端口通道）接口的基本以太网设置。在应用中，您可以配置更高级别的设置。例如，您只能在 FXOS 中创建 EtherChannel；但是，您可以为应用中的 EtherChannel 分配 IP 地址。

下文将介绍 FXOS 接口与应用接口之间的交互。

VLAN 子接口

对于所有逻辑设备，您可以在应用内创建 VLAN 子接口。

机箱和应用中的独立接口状态

您可以从管理上启用和禁用机箱和应用中的接口。必须在两个操作系统中都启用能够正常运行的接口。由于接口状态可独立控制，因此机箱与应用之间可能出现不匹配的情况。

Firepower 9300 硬件和软件组合的要求与前提条件

Firepower 9300 包括 3 个安全模块插槽和多种类型的安全模块。请参阅以下要求：

- 安全模块类型 - 您可以在 Firepower 9300 中安装不同类型的模块。例如，您可以将 SM-48 作为模块 1、SM-40 作为模块 2、SM-56 作为模块 3 安装。
- 本地和容器实例 - 在安全模块上安装容器实例时，该模块只能支持其他容器实例。本地实例将使用模块的所有资源，因此只能在模块上安装一个本地实例。可以在某些模块上使用本地实例，在其他模块上使用容器实例。例如，您可以在模块 1 和模块 2 上安装本地实例，但在模块 3 上安装容器实例。
- 高可用性 - 仅在 Firepower 9300 上的同类模块间支持高可用性。 但是，这两个机箱可以包含混合模块。例如，每个机箱都设有 SM-40、SM-48 和 SM-56。可以在 SM-40 模块之间、SM-48 模块之间和 SM-56 模块之间创建高可用性对。
- ASA 和 威胁防御 应用类型-您可以在机箱中的独立模块上安装不同类型的应用。例如，您可以在模块 1 和模块 2 上安装 ASA，在模块 3 上安装 威胁防御 。
- ASA 或 威胁防御 版本 - 您可以在单独的模块上运行不同版本的应用实例类型，或在同一模块上运行单独的容器实例。例如，您可以在模块 1 上安装 威胁防御 6.3，在模块 2 上安装 威胁防御 6.4，在模块 3 上安装 威胁防御 6.5。

逻辑设备的准则和限制

有关准则和限制，请参阅以下章节。

接口的准则和限制

默认 MAC 地址

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。

- EtherChannel - 对于 EtherChannel，属于通道组的所有接口共用同一个 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员身份不影响 MAC 地址。

一般准则和限制

高可用性

- 在应用配置中配置高可用性。
- 可以将任何数据接口用作故障转移和状态链路。
- 高可用性故障转移配置中的两个设备必须：
  - 型号相同。
  - 将同一接口分配至高可用性逻辑设备。
  - 拥有相同数量和类型的接口。启用高可用性之前，所有接口必须在 FXOS 中进行相同的预配置。
- 有关详细信息，请参阅 高可用性的系统要求，第 193 页。

配置接口

默认情况下，物理接口处于禁用状态。可以启用接口，添加 Etherchannel，编辑接口属性。

启用或禁用接口

可以将每个接口的**管理状态**更改为启用或禁用。默认情况下，物理接口处于禁用状态。

过程

步骤 1 选择**接口 (Interfaces)** 打开接口页面。

“接口 (Interfaces)”页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 要启用接口，请点击已禁用**滑块已禁用**（  ），使其更改为已启用**滑块已启用**（  ）。

点击**是**，确认更改。以直观展示图表现的对应接口从灰色变为绿色。

步骤 3 要禁用接口，请点击已启用**滑块已启用**（  ），使其更改为已禁用**滑块已禁用**（  ）。

点击**是**，确认更改。以直观展示图表现的对应接口从绿色变为灰色。

配置物理接口

您可以通过物理方式启用和禁用接口，并设置接口速度和双工。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在应用中以逻辑方式启用它。

注释 对于 QSFPH40G-CUxM，默认情况下自动协商会始终处于启用状态，并且您无法将其禁用。

开始之前

- 不能单独修改已经是 EtherChannel 成员的接口。务必在将接口添加到 EtherChannel 之前为其配置设置。

添加 **EtherChannel**（端口通道）

EtherChannel（也称为端口通道）最多可以包含 16 个同一介质类型和容量的成员接口，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。链路聚合控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

您可以将 EtherChannel 中的每个物理数据接口配置为：

- Active - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- 开启 - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

注释 如果将其模式从打开更改为主用或从主用更改为打开状态，则可能需要多达三分钟的时间才能使 EtherChannel 进入运行状态。

Firepower 4100/9300 机箱仅支持主用 LACP 模式下的 Etherchannel，以便每个成员接口发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。 如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

Firepower 4100/9300 机箱 创建 EtherChannel 时，EtherChannel 将处于**挂起**状态（对于主动 LACP 模式）或**关闭**状态（对于打开 LACP 模式），直到将其分配给逻辑设备，即使物理链路是连通的。EtherChannel 在以下情况下将退出**挂起**状态：

- 将 EtherChannel 添加为独立逻辑设备的数据或管理端口
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的管理接口或集群控制链路
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的数据端口，并且至少有一个单元已加入该集群

请注意，EtherChannel 在您将它分配到逻辑设备前不会正常工作。如果从逻辑设备移除 EtherChannel 或删除逻辑设备，EtherChannel 将恢复为**挂起**或**关闭**状态。

配置逻辑设备

在 Firepower 4100/9300 机箱上添加独立逻辑设备或高可用性对。

为 设备管理器 添加独立的 威胁防御

可以将 设备管理器 与本地实例结合使用。不支持容器实例。独立逻辑设备可单独使用，也可在高可用性对中使用。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像到 Firepower 4100/9300 机箱。
- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口不同于仅用于机箱管理的机箱管理端口 。
- 您还必须至少配置一个数据类型的接口。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址
  - DNS 服务器 IP 地址
  - 威胁防御 主机名和域名

过程

请参阅《 设备管理器 配置指南》，以开始配置安全策略。

添加高可用性对

威胁防御 高可用性（也称为故障转移）是在应用中配置，而不是在 FXOS 中配置。但为了让您的机箱做好配置高可用性的准备，请参阅以下步骤。

开始之前

请参阅高可用性的系统要求，第 193 页。

过程

步骤 1 将相同的接口分配给各个逻辑设备。

步骤 2 为故障转移和状态链路分配 1 个或 2 个数据接口。

这些接口用于交换 2 个机箱之间的高可用性流量。我们建议您将一个 10 GB 数据接口用于组合的故障转移和状态链路。如果您有可用的接口，可以使用单独的故障转移和状态链路；状态链路需要的带宽最多。不能将管理类型的接口用于故障转移或状态链路。我们建议您在机箱之间使用一个交换机，并且不将同一网段中的其他任何设备作为故障转移接口。

步骤 3 在逻辑设备上启用高可用性。请参阅高可用性（故障转移），第 185 页。

步骤 4 如果您在启用高可用性后需要更改接口，请先在备用设备上执行更改，然后再在主用设备上执行更改。

更改威胁防御逻辑设备上的接口

可以在 威胁防御 逻辑设备上分配或取消分配接口。然后，您可以在 设备管理器中同步接口配置。

添加新接口或删除未使用接口对 威胁防御 配置的影响最小。但是，删除安全策略中使用的接口会影响配置。可以直接在 威胁防御 配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。引用安全区的策略不受影响。还可以编辑已分配的 EtherChannel 的成员关系，而不影响逻辑设备或要求在设备管理器上进行同步。

可以在删除旧接口前，将配置从一个接口迁移至另一个接口。

开始之前

- 根据配置物理接口，第 177 页和添加 EtherChannel（端口通道），第 177 页配置您的接口，并添加任何 EtherChannel。

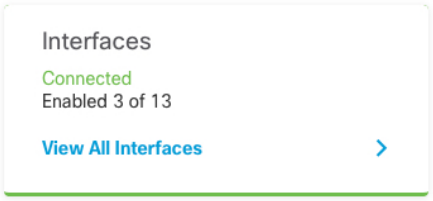
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到EtherChannel。对于新的EtherChannel，您可以随后将 EtherChannel 分配到设备。
- 对于高可用性，请确保在所有设备上添加或删除该接口，然后在设备管理器 中同步配置。我们建议先在备用设备上更改接口，然后再在主用设备上更改接口。请注意，新的接口在管理权限关闭的状态下添加，因此，它们不会影响接口监控。
- 在多实例模式下，要更改具有相同 vlan 标记的另一个子接口的子接口，必须先删除该接口的所有配置（包括nameifconfig），然后从机箱管理器取消分配该接口。取消分配后，添加新接口，然后使用 管理中心中的同步接口。

过程

步骤 1 同步和迁移 设备管理器 中的接口。

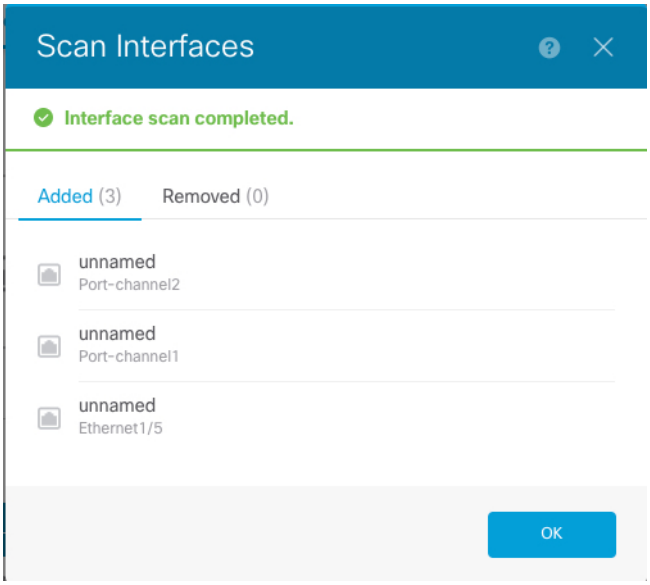
a) 登录至设备管理器。

b) 点击**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的**查看所有接口 (View All Interfaces)** 链路。



c) 点击**扫描接口图标**。

d) 等待接口扫描，然后点击**确定**。



e) 使用名称、IP 地址等配置新接口。

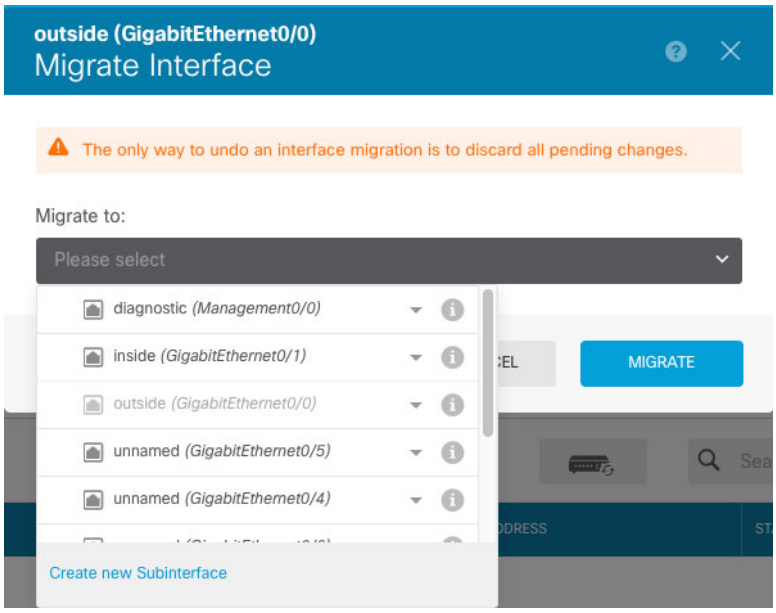
如果要使用待删除接口的现有 IP 地址和名称，则需要使用虚拟名称和 IP 地址重新配置旧接口，以便可以在新接口上使用这些设置。

f) 要将旧接口替换为新接口，请点击旧接口的“替换”图标。

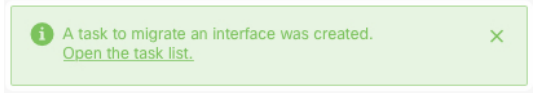
替换图标

此过程会将旧接口替换为引用该接口的所有配置设置中的新接口。

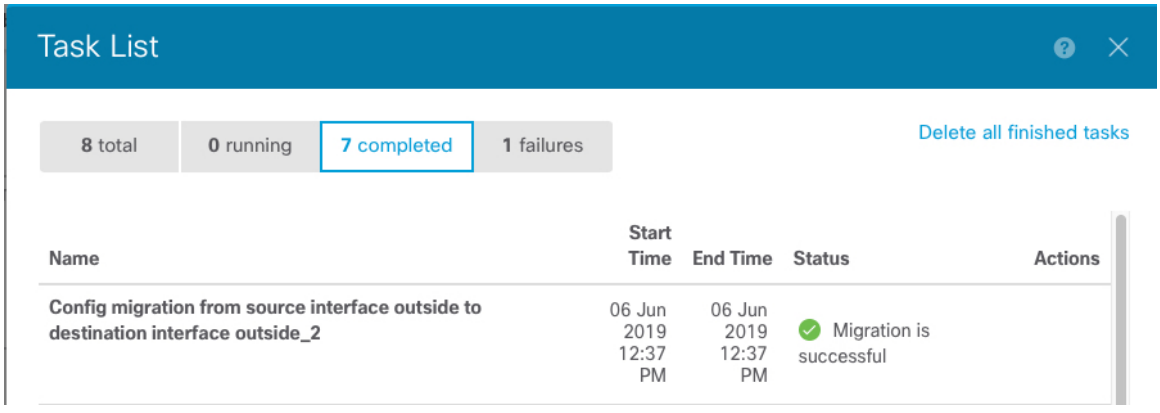
g) 从**替换接口**下拉列表中选择新接口。



h) 一则消息将显示在**接口 (Interfaces)** 页面上。点击消息中的链接。

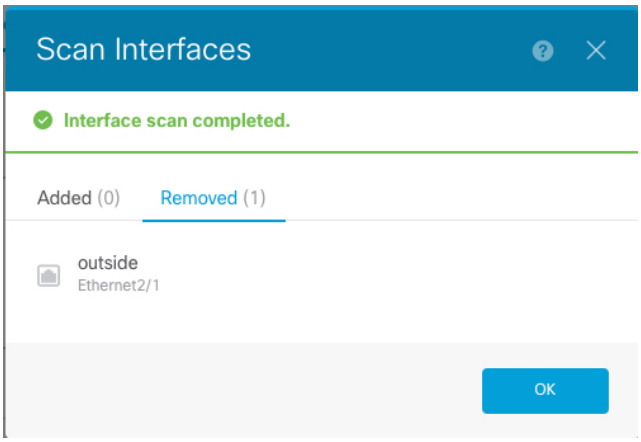


i) 检查**任务列表**，以确保迁移成功。



步骤 2 再次在 设备管理器 中同步接口。

图 *6:* 设备管理器扫描接口



连接到应用控制台

使用以下程序连接至应用的控制台。

过程

步骤 1 使用控制台连接或 Telnet 连接来连接至模块 CLI。

connect module *slot_number* {**console** | **telnet**}

要连接至不支持多个安全模块的设备的安全引擎，请使用 **1** 作为 *slot_number*。

使用 Telnet 连接的优点在于，您可以同时对模块开展多个会话，并且连接速度更快。

示例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

步骤 2 连接到应用控制台。

connect ftd *name*

要查看实例名称，请输入不含名称的命令。

示例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

步骤 3 退出应用控制台到 FXOS 模块 CLI。

- 威胁防御 - 输入 **exit**

步骤 4 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 **~**

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 Telnet 会话：

a) 输入 **Ctrl-],**。

Firepower 4100/9300 逻辑设备的历史记录

特性	Version	详细信息
支持 Firepower 4100/9300 上的 设备管理器	6.5.0	现在，您可以将 设备管理器 与 Firepower 4100/9300上的 威胁防御 逻辑设备配合使用。 设备管理器 不支持多实例功能；仅支持本地实例。 **注释** 需要 FXOS 2.7.1。

第 10 章

高可用性（故障转移）

以下主题介绍如何配置和管理主用/备用设备故障转移，以实现 威胁防御系统的高可用性。

关于高可用性（故障转移）

高可用性或故障转移设置可以将两台设备相关联，这样，当主设备发生故障时，辅助设备可以接管其任务。这有助于您在设备发生故障时保持网络运行。

配置高可用性需要两台相同的 威胁防御设备，二者之间通过专用故障转移链路和（可选）状态链路彼此互连。这两台设备不断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并同步已部署的配置更改。系统使用状态链路将连接状态信息传递到备用设备，因此如果发生故障转移，用户连接将得以保留。

这两台设备构成一对主用/备用设备，其中一台设备是主用设备并传递流量。备用设备不会主动传递流量，但会使配置和其他状态信息与主用设备同步。

系统会对主用设备的运行状况（硬件、接口、软件以及环境状态）进行监控，以便确定是否符合特定的故障转移条件。如果符合条件，主用设备将故障转移至备用设备，届时备用设备将变成主用设备。

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 威胁防御设备来接管故障设备的功能。当主用设备发生故障时，备用设备将变为主用设备。

主/辅助角色和主用/备用状态

在故障转移对中这两台设备之间的主要区别是哪台是主用设备，哪台是备用设备，即要使用哪些 IP 地址以及哪台设备积极传递流量。

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

- 如果两台设备同一时间启动（并且运行状况相同），则主设备总是会成为主用设备。
- 主设备 MAC 地址始终与主用 IP 地址相匹配。此规则的例外是，当辅助设备成为主用设备并且无法通过故障转移链路获取主设备 MAC 时。在这种情况下，会使用辅助设备的 MAC 地址。

启动时的主用设备确定

主用设备按以下方式确定：

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

故障转移事件

在主用/备用故障转移中，故障转移会在设备级别进行。

下表显示了每个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（故障转移或禁用故障转移）、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 *4:* 故障转移事件

故障事件	策略	主用设备操作	备用设备操作	说明
主用设备发生故障（电源或硬件）	故障转移	不适用	成为主用设备 将主用设备标记为发生故障	在任何受监控接口或故障转移链路上，均未收到 Hello 消息。
以前的主用设备恢复	禁用故障转移	成为备用设备	无需操作	无。
备用设备发生故障（电源或硬件）	禁用故障转移	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过程中发生故障	禁用故障转移	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	您应尽快恢复故障转移链路，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。

故障事件	策略	主用设备操作	备用设备操作	说明
故障转移链路在启动时发生故障	禁用故障转移	成为主用设备 将故障转移链路标记为发生故障	成为主用设备 将故障转移链路标记为发生故障	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。
状态链路发生故障	禁用故障转移	无需操作	无需操作	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	成为主用设备	无。
备用设备上的接口故障超过阈值	禁用故障转移	无需操作	将备用设备标记为发生故障	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。

故障转移和状态故障转移链路

故障转移链路是两台设备之间的专用连接。状态故障转移链路也是专用连接，不过，您可以使用一个故障转移链路作为组合的故障转移/状态链路，也可以创建单独的专用状态链路。如果仅使用故障转移链路，状态信息也会通过该链路：状态故障转移功能不会受到影响。

默认情况下，故障转移和状态故障转移链路上的通信是纯文本通信（不加密）。为了增强安全性，您可以通过配置 IPsec 加密密钥对通信加密。

以下主题更加详细地介绍了这些接口，并就如何连接设备以获得最佳效果给出了建议。

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，以确定每台设备的运行状态和同步配置更改。

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 (keep-alives)。
- 网络链路状态。
- MAC 地址交换。
- 配置复制和同步。
- 系统数据库更新，包括VDB和规则，但不包括地理位置和安全智能数据库。每个系统会单独下载地理位置和安全智能更新。如果您创建更新计划，这些更新应保持同步。但是，如果您在主用设备上执行手动地理位置或安全智能更新，那么也应在备用设备上执行同样的操作。

注释 事件、报告和审核日志数据不会同步。事件查看器和控制面板仅显示与特定设备相关的数据。此外，部署历史记录、任务历史记录和其他审核日志事件不会同步。

状态故障转移链路

系统使用状态链路将连接状态信息传送到备用设备。此信息可在发生故障转移时帮助备用设备保留现有连接。

对故障转移和状态故障转移链路使用一条链路能够最大程度地节省接口。但是，如果您有一个大型配置和高流量网络，必须考虑对状态链路和故障转移链路使用专用接口。

用于故障转移和状态链路的接口

可以使用未使用但已启用的数据接口（物理接口或 EtherChannel 接口）作为故障转移链路；但无法指定当前配置了名称的接口。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。该接口只能用于故障转移链路（还用于状态链路）。无法使用管理接口、子接口、VLAN 接口或交换机端口进行故障转移。

威胁防御 设备用户数据和故障转移链路之间共享接口。

请参阅下列有关调整故障转移和状态链路大小的准则：

- Firepower 4100/9300 - 我们建议您将一个 10 GB 的数据接口用于组合的故障转移和状态链路。
- 所有其他型号 - 1 GB 接口对于组合的故障转移和状态链路而言已足够大。

使用 EtherChannel 接口作为故障转移链路或状态链路时，必须在建立高可用性之前，确认具有相同 ID 和成员接口的同一 EtherChannel 在两台设备上都存在。如果 EtherChannel 不匹配，您需要先禁用 HA 并更正辅助设备的配置。要阻止无序数据包，仅使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。您不能在 EtherChannel 配置用作故障转移链路时对其进行修改。

连接故障转移和状态故障转移接口

您可以将任何未使用的数据物理接口用作故障转移链路和可选的专用状态链路。但是，您不能选择当前已配置名称或具有子接口的接口。故障转移和状态故障转移链路接口不会被配置为通常的网络接口。这些接口只是为了进行故障转移通信，不能用于直通流量或管理访问。

此配置在设备之间是同步的，因此您必须为链路的两端选择相同的端口号。例如，用于故障转移链路的两台设备都使用 GigabitEthernet1/3。

使用以下两种方法中的一种连接故障转移链路和专用状态链路（如已使用）：

- 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 威胁防御设备的故障转移接口。专用状态链路的要求与故障转移链路相同，只是必须与故障转移链路位于不同的网段上。

注释 使用交换机的优点是，如果设备的其中一个接口发生故障，可以轻松确定哪一个接口出现故障。如果使用直连电缆连接，那么当一个接口发生故障时，链路将在两个对等体上断开，这样将难以确定哪台设备出现故障。

- 使用以太网电缆直接连接设备，无需外部交换机。威胁防御 在其铜缆以太网端口上支持自动 MDI/MDIX，因此您可以使用交叉电缆或直通电缆。如果使用的是直通电缆，接口会自动检测该电缆，并将其中一个发送/接收对交换为 MDIX。

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

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，威胁防御设备可使用数据接口来确定是否需要进行故障转移。随后，故障转移操作会被暂停，直到故障转移链路恢复正常。

请参阅以下连接情景，以设计具有弹性的故障转移网络。

情景 1 - 不推荐

如果单台交换机或一组交换机用于连接两台 威胁防御设备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 威胁防御设备都将处于主用状态。因此，建议**不要**使用下图中显示的 2 种连接方法。

图 *7:* 使用单交换机连接 - 不推荐

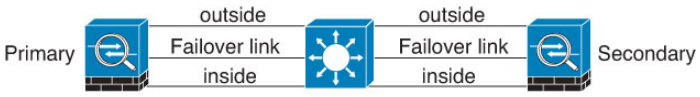
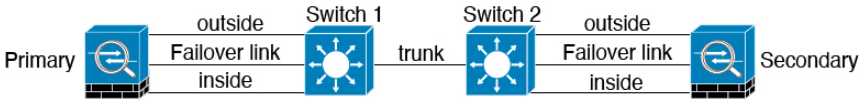


图 *8:* 使用双交换机连接 - 不推荐



情景 2 - 推荐

我们建议不要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，如下图所示。

图 *9:* 使用其他交换机连接

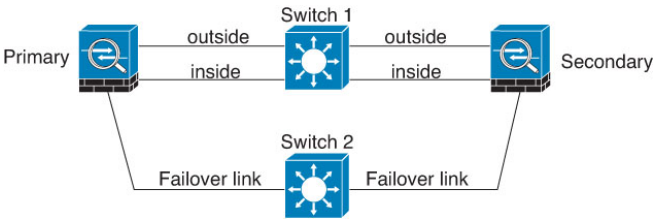
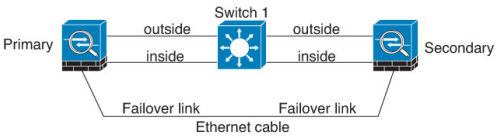


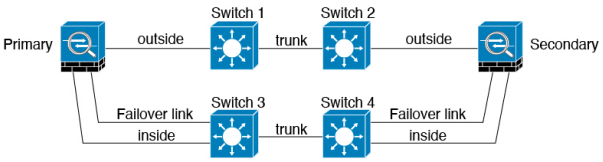
图 *10:* 通过电缆连接



情景 3 - 推荐

如果 威胁防御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，如下图所示。

图 *11:* 使用安全交换机连接



状态故障转移如何影响用户连接

主用设备与备用设备共享连接状态信息。这意味着，备用设备可以保持某些类型的连接，而不会影响用户。

但是，有一些类型的连接不支持状态故障转移。对于这些连接，如果发生故障转移，用户需要重新建立连接。通常，连接会根据连接中所用协议的行为自动进行。

以下主题介绍状态故障转移支持或不支持的功能。

支持的功能

对于状态故障转移，以下状态信息会传送至备用 威胁防御设备：

- NAT 转换表。
- TCP 和 UDP 连接和状态，包括 HTTP 连接状态。其他类型的 IP 协议和 ICMP 不会通过主用设备解析，因为它们是在新数据包到达时在新的主用设备上建立的。
- Snort 连接状态、检查结果和引脚信息，包括严格 TCP 实施。
- ARP 表

- 第 2 层网桥表（适用于桥接组）
- ISAKMP 和 IPsec SA 表
- GTP PDP 连接数据库
- SIP 信令会话和引脚。
- 静态和动态路由表 - 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，因为主用辅助设备一开始就具有镜像主设备的规则。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。计时器到期后，过时的路由条目（由代编号确定）将从表中删除。于是 RIB 将包含新主用设备上的最新的路由协议转发信息。

注释 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。

- DHCP 服务器 - 不会复制 DHCP 地址租用。但是，在接口上配置的 DHCP 服务器将发送 ping 命令，以确保在向 DHCP 客户端授予地址前不使用地址，使得服务不会受到影响。对于 DHCP 中继代理或 DDNS，状态信息不相关。
- 访问控制策略决策 - 在故障转移期间，会保留与流量匹配（包括 URL、URL 类别、地理位置等）、入侵检测、恶意软件和文件类型相关的决策。但是，对于在故障转移时评估的连接，有以下注意事项：
  - AVC - 系统会复制 App-ID 裁定，而不是检测状态。只要 App-ID 裁定是完整的，并且在发生故障转移之前完成同步，即可实现正确的同步。
  - 入侵检测状态 - 进行故障转移时，一旦出现拾取中间流的情况，新检测既已完成，但旧状态会丢失。
  - 文件恶意软件阻止 - 文件处置必须在故障转移之前变为可用。
  - 文件类型检测和阻止 - 文件类型必须在故障转移之前加以识别。如果在原始主用设备识别文件时发生故障转移，则文件类型不同步。即使文件策略阻止该文件类型，新的主用设备也会下载该文件。
- 来自身份策略的被动用户身份决策，并非通过主动身份验证和通过强制网络门户收集的决策。
- 安全智能决策。
- RA VPN - 故障转移后，远程访问 VPN 终端用户不必对 VPN 会话重新进行身份验证，也不必重新连接。但是，在VPN连接上运行的应用，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。
- 在所有连接中，只有已建立的连接会复制到备用 ASA 上。

不支持的功能

对于状态故障转移，以下状态信息不会传送至备用 威胁防御设备：

- 非 GREv0 和 IPv4-in-IP 明文隧道中的会话。不会复制隧道内部的会话，并且新的主动节点不能重复使用现有检测判定来匹配正确的策略规则。
- 已解密的 TLS/SSL 连接 - 解密状态不同步，如果主用设备发生故障，则系统会重置已解密的连接。需要与新的主用设备建立新连接。未解密的连接（也就是匹配TLS/SSL“不解密”规则操作的连接）不受影响，并且可以正确复制。
- 组播路由。

备用设备上允许的配置更改和操作

当设备在高可用性模式下运行时，仅需要对主用设备进行配置更改。部署配置时，新的更改也会传输到备用设备。

但某些属性是备用设备所特有的。您可以在备用设备上更改以下属性：

- 管理 IP 地址和网关。
- （仅限于 CLI。）管理员用户账户和其他本地用户账户的密码。此更改只能在 CLI 中进行，不可以在 设备管理器中进行。所有本地用户都必须分别在两台设备上更改其密码。

此外，您还可以在备用设备上执行以下操作。

- 高可用性操作（例如暂停、恢复、重置和中断HA）以及在主用设备和备用设备之间进行模式切换。
- 每个设备的控制面板和事件数据是唯一的，并且是不同步的。这包括事件查看器中的自定义视图。
- 每个设备的审核日志信息是唯一的。
- 智能许可注册。前提是，您必须启用或禁用主用设备上的可选许可证，并且该操作是与备用设备同步的，用于请求或释放相应的许可证。
- 备份，但不进行恢复。要恢复备份，您必须中断设备上的HA。如果备份包括HA配置，设备将重新加入高可用性组。
- 软件升级安装。
- 生成故障排除日志。
- 手动更新地理位置或安全智能数据库。这些数据库在设备之间不同步。如果您创建更新计划，设备可以独立地保持一致。
- 您可以从 **监控 (Monitoring)** > **会话 (Monitoring)** 页面查看活动 设备管理器 用户会话，并删除会话。

高可用性的系统要求

以下主题介绍整合高可用性配置中的两台设备之前必须满足的要求。

高可用性的硬件要求

要将高可用性配置中的两台设备链接在一起，必须满足以下硬件要求。

- 设备的硬件型号必须完全相同。

  对于 Firepower 9300，高可用性仅在同种类型模块之间受支持；但是两个机箱可以包含混合模块。例如，各机箱均具有 SM-36 和 SM-44。可以在 SM-36 模块之间和 SM-44 模块之间创建高可用性对。

- 设备接口的数量和类型必须相同。

  对于 Firepower 4100/9300 机箱，启用 HA 之前，所有接口都必须在 FXOS 中进行相同的预配置。如果在启用 HA 后更改接口，请在备用设备上的 FXOS 中更改接口，然后在主用设备上进行相同更改。

- 设备安装的模块必须相同。例如，如果具有可选的网络接口模块，则必须在另一台设备中安装相同的模块。

- 不支持 Firepower 9300 的机箱内高可用性。不能在位于同一个 Firepower 9300 机箱中的独立逻辑设备之间配置 HA。

高可用性的软件要求

要将两台设备链接到高可用性配置，必须满足以下软件要求。

- 设备必须运行完全相同的软件版本，也即，主要版本号（第一个）、次要版本号（第二个）以及维护版本号（第三个）都必须相同。您可以在 设备管理器 的 **设备 (Devices)** 页面，或者可以在 CLI 中使用 **show version** 命令找到版本。允许连接具有不同版本的设备，但配置不会导入备用设备且故障转移无法使用，直到您将设备升级到同一软件版本。

- 两台设备必须在本地管理器模式下运行，也即，使用 设备管理器配置设备。如果您可以在两个系统上登录设备管理器 ，则表示这两台设备是本地管理器模式。您还可以在 CLI 中使用 **show managers** 命令进行验证。

- 必须在每台设备中完成初始设置向导。

- 每台设备都必须有自己的管理 IP 地址。管理接口的配置在两台设备之间未同步。

- 设备必须具有相同的 NTP 配置。

- 不能配置任何接口使用 DHCP 获取地址。也就是说，所有接口都必须有静态 IP 地址。

- 对于云服务，两台设备必须在同一区域注册，或者两台设备都不能注册。您不能采用混合云服务注册。

- 在配置高可用性之前，必须先部署任何待处理更改。

高可用性的许可证要求

在配置高可用性之前，设备必须处于相同的状态：两台设备均注册基础版许可证，或均处于评估模式。如果设备已注册，可以将其注册到不同的思科智能软件管理器账户，但这些账户的出口控制功能设置的状态必须相同，要么都启用这类设置，要么都禁用。但是，如果您已在设备上启用不同的可选许可证，上述设置便不再重要。如果注册两台设备，则必须为它们选择相同的思科云服务区域。

如果设备已注册，它们必须使用相同的模式，即“智能许可证”或“永久许可证预留”(PLR)。

在运行过程中，高可用性对中的设备必须具有相同的许可证。在部署过程中，主用设备进行的任何许可证更改都会在备用设备上重复进行。

高可用性配置需要两种智能许可证权利；对中的每个设备各一个。您必须确保您的账户中有足够的许可证，可应用到每个设备。如果没有足够的许可证，可能会出现一台设备合规，另一台设备不合规的情况。

例如，如果主用设备具有 基础版 许可证和 IPS ，而备用设备只有 基础版 许可证，备用设备将与思科智能软件管理器通信，以从您的帐户获取可用 IPS 。如果您的智能许可证账户没有足够的已购授权，您的账户将不合规（且备用设备也将不合规，即使主用设备合规），直到您购买正确数量的许可证。

注释 如果将用户注册到存在不同出口控制功能设置的账户，或者尝试创建一个 HA 对，注册其中的一台设备，而将另外一台设备设置为评估模式，则 HA 加入可能会失败。对于出口控制功能，如果您使用不一致的设置配置 IPSec 加密密钥，当您激活 HA 后，两个设备都将变为主用状态。这会影响受支持网段上的路由，且您必须手动断开辅助设备上的 HA 才能消除影响。

高可用性准则

型号支持

- Firepower 9300 - 可以在 Firepower 9300上配置 HA。但是，不能在位于同一个 Firepower 9300 机箱中的独立逻辑设备之间配置 HA。
- Firepower 1010：
  - 使用高可用性时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此会继续在主用设备 和备用设备上传输流量。高可用性旨在防止流量通过备用设备，但此功能不会扩展至交换机端口。在正常 高可用性网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN接口可通过故障转移监控，而交换机端口无法通过故障转移监控。理论上，您可以将单个交换机端口置于 VLAN 上并成功使用 高可用性，但更简单的设置是改用物理防火墙接口。
  - 仅可使用防火墙接口作为故障转移链路。

- 当机箱处于高可用性对时，备用设备的“活动”LED 呈琥珀色光。

- （Firepower 1000 系列、Firepower 2100）- 在 HA 中部署配置了数百个接口的设备， 会导致故障转移时间（秒）延迟增加。
- Threat Defense Virtual - 对于 Microsoft Azure 云或 Amazon Web 服务 (AWS) 云，threat defense virtual 不支持 HA 配置。

其他准则

- 169.254.0.0/16 和 fd00:0:0:*::/64 是内部使用的子网，不能用于故障转移或状态链路。
- 当您在主用设备上运行部署作业时，主用设备的配置会同步到备用设备。但是，在您部署更改之前，某些更改不会显示在待处理更改中，即使它们还未同步到备用设备上。如果您更改以下任一一项，所做的更改将会被隐藏，且您必须运行部署作业才能使它们配置在备用设备上。如果您需要立即应用更改，您将需要进行一些其他更改，这些更改会显示在待处理更改中。隐藏的更改包括对以下项目的编辑：规则计划、空间数据库、安全智能或 VDB 更新；备份计划；NTP； 管理连接的 HTTP 代理； 许可证授权；云服务选项；URL 过滤选项。
- 您应在主设备和辅助设备上执行备份。要恢复备份，您必须首先中断高可用性。不要在两台设备上恢复相同备份，因为这两台设备都会变成活动状态。相反，您要在想要首先恢复活动状态的设备上恢复备份，然后在另一台设备上恢复等效备份。
- 适用于各种身份源的**测试**按钮仅在主用设备上可用。如果您需要测试备用设备的身份源连接，必须先切换模式，使备用对等体变成主用对等体。
- 创建或中断高可用性配置会在部署配置更改后重新启动两台设备上的 Snort 检测过程。这可能会导致直通流量中断，直到进程完全重新启动。
- 最初配置高可用性时，如果辅助设备上的安全智能和地理位置数据库的版本与主设备上的版本不同，请在辅助设备上安排作业来更新数据库。下一次部署时，从主用设备运行这些作业。即使高可用性加入失败，这些作业仍将保留，并将在下一次部署时执行。
- 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，您可以根据交换机启用 STP PortFast 功能：

  interface *interface_id* **spanning-tree portfast**

  此解决方法适用于连接到路由模式和桥接组接口的交换机。链路打开时，PortFast 功能会立即使端口转换到 STP 转发模式。该端口仍会参与 STP。因此，如果端口是环路的一部分，则端口最终会转换为 STP 阻塞模式。
- 发生故障转移事件时，在连接到高可用性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规时，会发生此问题。
- 对于主用/备用高可用性和 VPN IPSec 隧道，无法使用 SNMP 通过 VPN 隧道监控主用设备和备用设备。备用设备没有有效的 VPN 隧道，将丢弃发往网络管理系统 (NMS) 的流量。您可以改为使用具有加密功能的 SNMPv3，因此不需要 IPsec 隧道。

配置高可用性

借助高可用性设置，即使设备发生故障，也可确保网络连接。设置主用/备用高可用性时，两台设备将链接到一起。如果主用设备发生故障，备用设备会接管相应的角色，因此用户几乎察觉不到连接问题。

以下过程介绍设置主用/备用高可用性 (HA) 对的　端到端流程。

过程

步骤 1 准备两台用于高可用性的设备，第 196 页。

步骤 2 配置高可用性的主设备，第 198 页。

步骤 3 配置高可用性的辅助设备，第 200 页。

步骤 4 配置故障转移运行状况监控条件，第 201 页。

条件包括对等体监控和接口监控。虽然所有故障转移条件都有默认设置，您至少应检查这些设置，验证是否适用于您的网络。

- 配置对等体运行状况监控故障转移条件，第 202 页。
- 配置接口运行状况监控故障转移条件，第 203 页。

  有关接口测试的信息，请参阅系统如何测试接口运行状况，第 204 页。

步骤 5 （推荐的可选项目。）配置备用 IP 地址和 MAC 地址，第 205 页。

步骤 6 （可选。）验证高可用性配置，第 206 页。

准备两台用于高可用性的设备

要成功配置高可用性，您需要正确做好多项准备。

过程

步骤 1 确保设备满足高可用性的硬件要求，第 193 页中列出的要求。

步骤 2 确定使用一个故障转移链路，还是使用单独的故障转移和状态故障转移链路，并确定您将使用的端口。

必须在每台设备上为每个链路使用相同的端口号。例如，在两台设备上均对故障转移链路使用 GigabitEthernet 1/3。确定您要使用哪些端口，避免将其意外用于其他用途。有关详细信息，请参阅故障转移和状态故障转移链路，第 187 页。

步骤 3 安装设备，将其连接到网络，并在每个设备上完成初始设置向导。

a) 查看避免中断故障转移和数据链路，第 189 页中的建议网络设计。
b) 必须至少连接外部接口，如连接接口，第 10 页中所述。

您还可以连接其他接口，但是必须确保在每个设备上使用相同的端口连接到指定子网。由于设备将共享相同的配置，必须将它们以并行方式连接到网络中。

注释 安装向导不允许更改管理和内部接口上的 IP 地址。因此，如果您将主要设备上的这些接口连接到网络，不要同时连接辅助设备上的同类接口，否则 IP 地址会发生冲突。您可以直接将工作站连接到其中一个接口并通过 DHCP 获取地址，以便您可以连接到 设备管理器 并配置设备。

c) 在每台设备上完成初始设置向导。确保指定外部接口的静态 IP 地址。此外，配置相同的 NTP 服务器。有关详细信息，请参阅使用设置向导完成初始配置，第 19 页。

为设备选择相同的许可和 Cisco Success Network 选项。例如，为每个设备选择评估模式或注册设备。

d) 在辅助设备上，依次选择**设备** > **系统设置** > **管理接口**并配置唯一的 IP 地址，更改网关（如有必要），并更改或禁用 DHCP 服务器设置，以满足您的需求。
e) 在辅助设备上，依次选择**设备** > **接口**并编辑内部接口。删除或更改 IP 地址。此外，删除为接口定义的 DHCP 服务器，因为不能在同一网络上有两个 DHCP 服务器。
f) 在辅助设备上部署配置。
g) 根据您的网络拓扑要求，登录到主设备，更改管理地址、网关与 DHCP 服务器设置以及内部接口 IP 地址与 DHCP 服务器设置。如果您进行任何更改，请部署配置。
h) 如果您未连接内部接口或管理接口（如果您使用单独的管理网络），现在可以将其连接到交换机。

步骤 4 验证设备是否具有完全相同的软件版本，也即，主要版本号（第一个）、次要版本号（第二个）以及维护版本号（第三个）都必须相同。您可以在设备页面 设备管理器 中，或者可以在 CLI 中使用 **show version** 命令找到版本。

如果设备未运行相同的软件版本，从 Cisco.com 获取首选的软件版本并将其安装在每台设备上。有关详细信息，请参阅升级 威胁防御，第 769 页。

步骤 5 连接和配置故障转移和状态故障转移链路。

a) 按照您的首选网络设计（从避免中断故障转移和数据链路，第 189 页选择），酌情将每台设备的故障转移接口连接到交换机或直接互连。
b) 如果使用单独的状态链路，也请相应地连接每台设备的状态故障转移接口。
c) 依次登录到每台设备，然后转至**设备** > **接口**。编辑每个接口，并验证没有配置接口名称或 IP 地址。

如果为接口配置了名称，您可能需要从安全区中删除这些接口和其他配置，然后才能删除名称。如果删除名称失败，检查错误消息以确定需要进行哪些其他更改。

步骤 6 在主设备上，连接剩余的数据接口并配置设备。

a) 选择**设备** > **接口**，编辑用于直通流量的每个接口和配置主要静态 IP 地址。
b) 将接口添加到安全区，并配置处理已连接网络上的流量所需的基本策略。有关示例配置，请参阅最佳实践： 威胁防御的使用案例，第 39 页中列出的主题。

c) 部署配置。

步骤 7 验证您是否达到高可用性的软件要求，第 193 页中所述的所有要求。

步骤 8 确认您有一致的许可（注册或评估模式）。有关详细信息，请参阅高可用性的许可证要求，第 194 页。

步骤 9 在辅助设备上，将其余数据接口连接到主要设备上对等接口连接的网络。不要配置接口。

步骤 10 在每个设备上，依次选择**设备 (Device)** > **系统设置 (System Settings)** > **云服务 (Cloud Services)** 并确认设置相同。

现在您即可在主设备上配置高可用性。

配置高可用性的主设备

要设置主用/备用高可用性对，必须先配置主设备。主设备是您打算在正常情况下应该处于主用模式的设备。辅助设备保持备用模式，直到主设备不可用。

选择您要当做主设备的设备，然后在该设备上登录 设备管理器 并按照此程序操作。

注释 创建高可用性对后，必须拆分对，才能够按照此过程中的说明编辑配置。

开始之前

确保您为故障转移和状态故障转移链路配置的接口尚未命名。如果当前接口已命名，您必须从使用这些接口的任何策略（包括安全区对象）中将其删除，然后编辑接口以删除名称。接口还必须处于路由模式，而不是被动模式。这些接口必须专用于高可用性配置：不能将其用于任何其他用途。

如果存在任何待处理的更改，必须先部署这些更改，然后才能配置高可用性。

过程

步骤 1 点击**设备**。

步骤 2 在设备摘要的右侧，点击**高可用性**组旁边的**配置**。

如果您在设备上第一次配置高可用性，该组将如下所示。

步骤 3 在“高可用性”(High Availability) 页面上，点击**主设备 (Primary Device)** 框。

如果已配置辅助设备，并已将配置复制到剪贴板，您可以点击**从剪贴板粘贴**按钮并粘贴配置。这将使用适当的值更新字段，稍后，您可以验证这些值。

步骤 4 配置**故障转移链路**属性。

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，以确定每台设备的运行状态和同步配置更改。有关详细信息，请参阅故障转移链路，第 187 页。

- **物理接口** - 选择连接到辅助设备用作故障转移链路的接口。此接口必须是未命名的接口。

  使用 EtherChannel 接口作为故障转移链路或状态链路时，必须在建立高可用性之前，确认具有相同 ID 和成员接口的同一 EtherChannel 在两台设备上都存在。如果 EtherChannel 不匹配，您需要先禁用 HA 并更正辅助设备的配置。要阻止无序数据包，仅使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。您不能在 EtherChannel 配置用作故障转移链路时对其进行修改。

- **类型** - 选择是否对接口使用 IPv4 或 IPv6 地址。只能配置一种类型的地址。
- **主 IP** - 为此设备上的接口输入 IP 地址。例如：192.168.10.1。对于 IPv6 地址，您必须采用标准表示法添加前缀长度，例如 2001:a0a:b00::a0a:b70/64。
- **辅助 IP** - 输入应在链路的另一端为辅助设备上的接口配置的 IP 地址。地址必须与主地址位于同一子网，且必须与主地址不同。例如，192.168.10.2 或 2001:a0a:b00::a0a:b71/64。
- **子网掩码**（仅限 Ipv4） - 输入主/辅助 IP 地址的子网掩码。

步骤 5 配置状态故障转移链路属性。

系统使用状态链路将连接状态信息传送到备用设备。此信息可在发生故障转移时帮助备用设备保留现有连接。您可以使用同一链路作为故障转移链路，也可以配置一个单独的链路。

- **使用相同的接口作为故障转移链路** - 如果您想对故障转移和状态故障转移通信使用单一链路，请选择此选项。如果选择此选项，请继续执行下一步。
- **物理接口** - 如果您想要使用单独的状态故障转移链路，请选择连接到辅助设备的接口，以用作状态故障转移链路。此接口必须是未命名的接口。然后，配置以下属性：
  - **类型** - 选择是否对接口使用 IPv4 或 IPv6 地址。只能配置一种类型的地址。
  - **主 IP** - 为此设备上的接口输入 IP 地址。地址必须与用于故障转移链路的地址位于不同子网。例如：192.168.11.1。对于 IPv6 地址，您必须采用标准表示法添加前缀长度，例如 2001:a0a:b00:a::a0a:b70/64。
  - **辅助 IP** - 输入应在链路的另一端为辅助设备上的接口配置的 IP 地址。地址必须与主地址位于同一子网，且必须与主地址不同。例如，192.168.11.2 或 2001:a0a:b00:a::a0a:b71/64。
  - **子网掩码**（仅限 Ipv4） - 输入主/辅助 IP 地址的子网掩码。

步骤 6 （可选。）如果您希望对设备对中两台设备之间的通信加密，请输入 **IPsec 加密密钥**字符串。

必须在辅助节点上配置完全相同的密钥，因此请记下您输入的字符串。

如果您不输入密钥，故障转移和状态故障转移链路上的所有通信都是纯文本。如果您未在接口之间使用直连电缆连接，可能会引发安全问题。

注释　如果您在评估模式下配置 HA 故障转移加密，系统将使用 DES 进行加密。如果随后您使用出口合规账户注册设备，则设备将在重新启动后使用 AES。因此，如果系统出于任何原因重新启动，包括安装升级后，对等体将无法通信，两台设备将变为主用设备。建议您在注册设备之前不要配置加密。如果您在评估模式下进行此配置，建议您在注册设备之前删除加密。

步骤 7 点击**激活高可用性**。

系统立即将配置部署到设备。不需要启动部署作业。如果您没有看到指出配置已保存和部署正在进行的消息，请滚动至页面顶部，查看错误消息。

配置也会被复制到剪贴板。您可以使用 copy 命令快速配置辅助设备。为提高安全性，加密密钥不包含在剪贴板复制内容中。

配置完成后，您会收到介绍后续操作的消息。阅读信息后，点击**明白**。

此时，您应转至“高可用性”页面，且设备状态应为“协商”(Negotiating)。此状态应在配置对等体之前切换为“主用”，且对等体应显示为“故障”，直至开始配置此设备。

现在，您可以配置辅助设备。请参阅配置高可用性的辅助设备，第 200 页。

注释　所选的接口不直接配置。但是，如果您在 CLI 中输入 **show interface**，您将看到接口正在使用指定的 IP 地址。如果您配置了单独的状态链路，接口被命名为“failover-link”和“stateful-failover-link”。

配置高可用性的辅助设备

为主用/备用高可用性配置主设备后，必须再配置辅助设备。在此设备上登录 设备管理器 并按照此过程操作。

注释　如果您尚未执行此操作，请将高可用性配置从主设备复制到剪贴板。使用复制/粘贴配置辅助设备比手动输入数据更容易。

过程

步骤 1 点击**设备**。

步骤 2 在设备摘要的右侧，点击**高可用性**组旁边的**配置**。

如果您在设备上第一次配置高可用性，该组将如下所示。

步骤 3 在“高可用性”页面上，点击**辅助设备 (Secondary Device)** 框。

步骤 4 执行以下操作之一：

- **简单方法** - 点击**从剪贴板粘贴**按钮，粘贴配置并点击**确定**。这将使用适当的值更新字段，稍后，您可以验证这些值。
- **手动方法** - 直接配置故障转移和状态故障转移链路。在辅助设备上输入与主设备完全相同的设置。

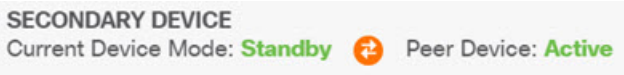
步骤 5 如果在主设备上配置了 **IPSec 加密密钥**，请在辅助设备上输入完全相同的密钥。

步骤 6 点击**激活高可用性**。

系统立即将配置部署到设备。不需要启动部署作业。如果您没有看到指出配置已保存和部署正在进行的消息，请滚动至页面顶部，查看错误消息。

配置完成后，您将收到说明已配置高可用性的消息。点击**明白**关闭该消息。

此时，您应转至“高可用性”(High Availability) 页面，且设备状态应指明此设备为辅助设备。如果与主设备连接成功，设备将与主设备同步，且最终模式应为备用、对等体应为主用模式。



注释 所选的接口不直接配置。但是，如果您在 CLI 中输入 **show interface**，您将看到接口正在使用指定的 IP 地址。如果您配置了单独的状态链路，接口被命名为“failover-link”和“stateful-failover-link”。

配置故障转移运行状况监控条件

采用高可用性配置的设备会监控自身的整体运行状况和接口运行状况。

故障转移条件定义运行状况监控度量，以此确定对等体是否发生故障。如果主用对等体违反了故障转移条件，会触发故障转移，切换到备用设备。如果备用对等体违反了故障转移条件，它将被标记为故障，且无法进行故障转移。

您可以仅在主用设备上配置故障转移条件。

下表列出了故障转移触发事件及关联的故障检测时间。

表 *5:* 基于故障转移条件的故障转移时间

故障触发事件	最小	默认	最大
主用设备断电或停止正常工作。	800 毫秒	15 秒	45 秒
主用设备接口物理链路关闭。	500 毫秒	5 秒	15 秒

故障触发事件	最小	默认	最大
主用设备接口正常运行，但是连接问题引发了接口测试。	5 秒	25 秒	75 秒

以下主题介绍如何自定义故障转移运行状况监控条件以及系统如何测试接口。

配置对等体运行状况监控故障转移条件

高可用性配置中的每个对等体均通过使用 hello 消息监控故障转移链路判断另一个对等体的运行状况。当设备在故障转移链路上没有收到三条连续的hello消息时，设备会在每个数据接口（包括故障转移链路）上发送 LANTEST 消息，以验证对等体是否响应。设备采取的操作取决于另一台设备的响应。

- 如果设备在故障转移链路上收到响应，则不会进行故障转移。
- 如果设备在故障转移链路上未收到响应，但在数据接口上收到响应，设备不会进行故障转移。故障转移链路会标记为发生故障。您应尽快恢复故障转移链路，因为当故障转移切换发生故障时，设备无法故障转移到备用设备。
- 如果设备未在任何接口上收到响应，则备用设备会切换至主用模式，并将另一台设备分类为故障设备。

您可以配置 hello 消息的轮询和保持时间。

过程

步骤 1 在主用设备上，点击**设备**。

步骤 2 点击设备摘要右侧的**高可用性**链接。

故障转移条件将在“高可用性”(High Availability) 页面的右侧列中列出。

步骤 3 定义**对等体时间配置**。

这些设置决定主用设备可以在多短的时间内故障转移至备用设备。设置的轮询时间越快，设备便可越快检测到故障并触发故障转移。但是，当网络临时堵塞时，更快的检测会导致不必要的切换。默认设置适用于大多数情况。

如果设备在一个轮询周期内未收到故障转移接口上的hello数据包，则会通过其余接口进行其他的测试。如果在保持时间内，仍未收到来自对等体设备的响应，该设备会被视为发生故障，如果故障设备为主用设备，则备用设备会进行接管，成为主用设备。

- **轮询时间** - hello 消息之间的等待时间。输入 1-15 秒或 200 到 999 毫秒。默认值为 1 秒。
- **保持时间** - 设备必须在故障转移链路上收到 hello 消息的时间，超出此时间仍未收到，则宣布对等体发生故障。保持时间必须至少是轮询时间的 3 倍。输入 1 到 45 秒或 800 到 999 毫秒。默认值为 15 秒。

步骤 4 点击**保存 (Save)**。

配置接口运行状况监控故障转移条件

您可以监控最多 211 个接口，具体取决于您的设备型号。您应监控重要的接口。例如，确保重要网络之间吞吐量的接口。仅当您为其配置备用 IP 地址且接口应始终开启时，才监控接口。

当设备在 2 个轮询期内，未在受监控的接口上收到 hello 消息时，将运行接口测试。如果对于某个接口，所有接口测试均失败，但在另一设备上的此接口继续成功传送流量，则此接口会被视为发生故障。如果达到故障接口的阈值，则会进行故障转移。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，发生故障的设备将恢复为备用模式。

您可以使用 **show monitor-interface** 命令，从 CLI 或 CLI 控制台监控接口 HA 状态。有关详细信息，请参阅监控高可用性监控接口的状态，第 218 页。

注释 接口关闭时，为了进行故障转移，该接口仍被视为是设备问题。如果设备检测到接口已关闭，将立即发生故障转移（如果您保留 1 个接口的默认阈值），而不等待接口保持时间。仅当设备将接口状态视为正常时，接口保持时间才有用，尽管设备并不从对等体接收 hello 数据包。

开始之前

默认情况下，所有已命名的物理接口均进行高可用性监控。因此，您应禁止监控不重要的物理接口。对于子接口或网桥组，您必须手动启用监控。

要完全禁用接口监控并防止因接口故障导致的故障转移，只需确保未对接口启用高可用性监控。

过程

步骤 1 在主用设备上，点击**设备**。

步骤 2 点击设备摘要右侧的**高可用性**链接。

故障转移条件将在“高可用性”(High Availability) 页面的右侧列中列出。

步骤 3 定义**接口故障阈值**。

如果故障接口的数量达到阈值，设备会将自身标记为发生故障。如果设备是主用设备，它会故障转移到备用设备。如果设备是备用设备，通过将自身标记为发生故障，主用设备会将此设备视为不可用于故障转移。

设置此条件时，请考虑您要监控多少个接口。例如，如果您仅在 2 个接口上启用监控，则永远不会达到10个接口的阈值。编辑接口属性时，通过选择**高级选项**选项卡上的**启用高可用性监控**选项，配置接口监控。

默认情况下，如果其中一个监控接口发生故障，设备会将自身标记为故障。

您可以通过选择以下**故障转移条件**选项之一设置接口故障阈值：

- **超出故障接口数**-输入接口的原始值。默认值为1。最大值实际上取决于设备型号，可能不尽相同，但您不能输入超过 211 个。使用此条件时，如果输入的数字超过设备支持的数量，将出现部署错误。请尝试较小的数字或改为使用百分比。
- **超出故障接口的百分比** - 输入 1 到 100 之间的数字。例如，如果您输入 50%，且您正在监控 10 个接口，那么如果 5 个接口发生故障，设备会将自身标记为故障。

步骤 4 定义**接口时间配置**。

这些设置决定了主用设备能够以多快的速度确定接口是否发生故障。设置的轮询时间越快，设备便可越快检测到接口故障。但是，更快的检测速度可能也会导致繁忙的接口在实际状况良好时被标记为故障，从而造成不必要的频繁故障转移。默认设置适用于大多数情况。

如果接口链路关闭，则不会执行接口测试，如果发生故障的接口数达到或超出配置的接口故障转移阈值，备用设备可能仅在一个接口轮询周期内就会变为主用状态。

- **轮询时间** - 在数据接口上发出 hello 数据包的频率。输入 1-15 秒或 500 到 999 毫秒。默认值为 5 秒。
- **保持时间** - 保持时间确定，从一个 hello 数据包丢失到接口被标记为发生故障的时长。输入 5 - 75 秒。输入的保持时间不得短于设备轮询时间的 5 倍。

步骤 5 点击**保存**。

步骤 6 对您想要监控的每个接口启用高可用性监控。

a) 选择**设备** > **接口**。

如果接口被监控，高可用性列的监视器将指示“已启用”。

b) 对要更改监控状态的接口，点击编辑图标 ( )。

您无法编辑故障转移或状态故障转移接口。接口监控不适用于这些接口。

c) 点击**高级选项**选项卡。

d) 根据需要，选中或取消选中**启用高可用性监控**复选框。

e) 点击**确定**。

步骤 7 （可选，但不推荐。）为监控的接口配置备用IP地址和MAC地址。请参阅配置备用IP地址和MAC地址，第 205 页。

系统如何测试接口运行状况

系统将持续测试监控的接口，确保高可用性正常。用于测试接口的地址取决于配置的地址类型：

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

- 如果接口上仅配置了 IPv6 地址， 设备会使用 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， 设备会使用所有的 IPv6 节点地址 (FE02::1)。

系统将在每台设备上执行以下测试：

1. 链路打开/关闭测试 - 一种接口状态测试。如果链路打开/关闭测试指示接口关闭，则视为设备测试失败。如果状态为打开，则设备执行网络活动测试。
2. 网络活动测试 - 接收的网络活动测试。此测试旨在使用 LANTEST 消息生成网络流量，以确定发生故障的设备（如有）。测试开始时，每台设备会清除其接口的收到的数据包计数。在测试期间（最多 5 秒），一旦设备收到数据包，则接口会被视为正常运行。如果一台设备收到流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备均未收到流量，则设备开始进行 ARP 测试。
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，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。如果到达列表末尾，也没有设备收到流量，设备开始进行 ping 测试。
4. Broadcast Ping 测试 - 包括发出广播 ping 请求的 ping 测试。随后设备会对最多 5 秒内收到的所有数据包进行计数。如果在此时间间隔内的任意时刻收到任何数据包，接口会被认为正常工作，并且会停止测试。如果未收到任何流量，测试将通过 ARP 测试再次开始。

配置备用 IP 地址和 MAC 地址

当您配置接口时，可以在相同网络上指定一个主用 IP 地址和一个备用 IP 地址。虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。此外，您也无法出于管理目的，连接到该接口上的备用设备。

1. 当主设备进行故障转移时，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。

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。不过，当主设备可用时，辅助（主用）设备会将 MAC 地址更改为主设备的 MAC 地址，这可能会导致网络流量中断。同样，如果您用新硬件替换主设备，将使用新 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。您可以手动配置虚拟 MAC 地址。

如果您没有配置虚拟 MAC 地址，则可能需要清除连接的路由器上的 ARP 表，以便恢复流量。当 MAC 地址发生变化时，威胁防御设备不会发送静态 NAT 地址的免费 ARP，因此连接的路由器不会知道这些地址的 MAC 地址发生变化。

过程

步骤 1 选择**设备** > **接口**。

您至少应为进行高可用性监控的接口配置备用 IP 和 MAC 地址。如果接口被监控，高可用性列的监视器将指示“已启用”。

步骤 2 对要配置备用地址的接口，点击编辑图标 ( )。

您无法编辑故障转移或状态故障转移接口。配置高可用性时，您可以为这些接口设置 IP 地址。

步骤 3 在 **IPv4 地址**和 **IPv6 地址**选项卡上配置备用 IP 地址。

此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。为要使用的每个 IP 版本配置备用地址。

步骤 4 点击**高级选项**选项卡，配置 MAC 地址。

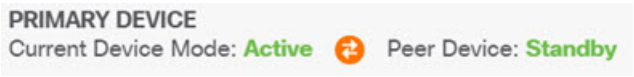
默认情况下，系统对接口使用预烧到网络接口卡 (NIC) 的 MAC 地址。因此，该接口上的所有子接口都使用相同的 MAC 地址，也因此您可能想要为每个子接口创建唯一地址。如果您配置高可用性，建议手动配置主用/备用 MAC 地址。定义 MAC 地址有助于在故障转移时保持网络中的一致性。

- **MAC 地址** - 采用 H.H.H 格式的介质访问控制地址，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。
- **备用 MAC 地址** - 用于高可用性。如果主用设备发生故障转移，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 5 点击**确定 (OK)**。

验证高可用性配置

完成高可用性配置后，验证设备的状态是否表明两台设备均运行正常并处于主用/备用模式。



您可以通过以下程序验证高可用性配置是否在工作。

过程

步骤 1 测试您的主用设备是否在使用诸如 FTP 之类的协议在不同接口上的主机之间发送文件，从而如预期传送流量。

至少应测试从一个工作站到连接到每个已配置的接口系统的连接。

步骤 2 可以通过执行以下任一操作，切换模式，使主用设备立即变成备用设备：

- 在 设备管理器上，从 **设备 (Device)** > **高可用性 (High Availability)** 页面的齿轮菜单上选择 **切换模式 (Switch Mode)** 。
- 在主用设备的 CLI 中，输入 **no failover active**。

步骤 3 重复连接测试，以验证可以通过高可用性对中的另一台设备进行相同的连接。

如果测试不成功，请验证是否已将设备的接口与另一台设备上的对等接口连接到相同的网络上。

您可以从“高可用性”(High Availability) 页面查看 HA 状态。您还可以使用设备的 CLI 或 CLI 控制台，输入 **show failover** 命令检查故障转移状态。此外，使用 **show interface** 命令，验证任何失败的连接测试中所用接口的接口配置。

如果这些操作找不到问题的症结所在，您可以尝试其他操作。请参阅高可用性故障排除（故障转移），第 220 页。

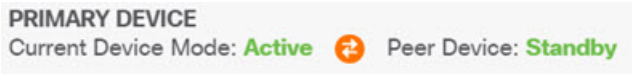
步骤 4 完成后，可以切换模式，使最初处于主用状态的设备恢复主用状态。

管理高可用性

您可以通过点击**设备 (Device)** 摘要页面上的**高可用性 (High Availability)** 链接，管理高可用性对。

“高可用性”页面包括以下内容：

- **角色和模式状态** - 左侧的状态区域显示设备是组中的主设备还是辅助设备。模式表示此设备处于主用模式还是备用模式，或者高可用性已被暂停还是设备正在等待加入对等体设备。它还显示对等体设备的状态，可以是主用、备用、暂停或失败状态。例如，当您登录主设备，并且该设备也是主用设备时，如果辅助设备正常并可在必要时用于故障转移，那么状态将如下所示。您可以点击对等体之间的图标获取设备之间的配置同步状态信息。

- **上次故障原因** - 如果高可用性 (HA) 配置由于某种原因（例如主用设备变得不可用并将故障转移到备用设备）而失败，则上次故障原因会显示在角色和模式状态的状态信息下方。此消息源自故障转移历史记录。
- **故障转移历史记录**链路 - 点击此链接可查看高可用性对中设备状态的详细历史记录。系统将打开 CLI 控制台并执行 **show failover history details** 命令。
- **部署历史记录**链接 - 点击此链接可转至审核日志，其中事件已过滤为仅显示部署作业。
- **齿轮按钮** - 点击此按钮可在设备上执行操作。

- **暂停高可用性/恢复高可用性** - 暂停高可用性会让设备停止作为高可用性对，但不删除高可用性配置。您可以随后在设备上恢复，也即重新启用高可用性。有关详细信息，请参阅暂停或恢复高可用性，第 208 页。
- **中断高可用性** - 中断高可用性将从两台设删除高可用性配置，并将它们恢复为独立设备。有关详细信息，请参阅中断高可用性，第 209 页。
- **切换模式** - 切换模式将强制主用设备变成备用设备，或备用设备变为主用设备，具体取决于您在哪台设备上执行操作。有关详细信息，请参阅切换主用和备用对等体（强制故障转移），第 210 页。

- **高可用性配置** - 此面板会显示故障转移对的配置。点击**复制到剪贴板**按钮将信息加载到剪贴板，从其中您可以将其粘贴到辅助设备的配置中。您可以也将其复制到另一个文件中做记录之用。此信息并不显示您是否已定义 IPsec 加密密钥。

注释 高可用性的接口配置不会反映在接口页面上（**设备 (Device)** > **接口 (Interfaces)**）。您无法编辑高可用性配置中使用的接口。

- **故障转移条件** - 此面板包含在评估主用设备是否已出现故障、备用设备应变成主用设备时确定运行状况条件使用的设置。调整这些条件，以便您可以获得网络所需的故障转移性能。有关详细信息，请参阅配置故障转移运行状况监控条件，第 201 页。

以下主题介绍与高可用性配置相关的各种管理任务。

暂停或恢复高可用性

可以暂停高可用性对中的设备。此功能适用于以下情形：

- 两台设备都在主用 - 主用情况下，且修复故障转移链路上的通信不能更正问题。
- 希望对主用或备用设备进行故障排除，并且不希望设备在此期间发生故障转移。
- 您想要在备用设备上安装软件升级期间阻止故障转移。

暂停高可用性时，停止将设备对用作故障转移设备。当前主用设备保持活动状态，并处理所有用户连接。但是，不会再监控故障转移条件，并且系统永远不会故障转移到现在的伪备用设备。备用设备将保留其配置，但将保持非活动状态。

暂停 HA 和中断 HA 之间的主要区别是，在暂停的 HA 设备上将保留高可用性配置。如果中断 HA，则会清除配置。因此，您可以选择在暂停系统上恢复高可用性，这样可启用现有配置并再次将两台设备设置为故障转移对。

如果您从主用设备暂停高可用性，配置将在主用和备用设备上暂停。如果从备用设备暂停，配置仅在备用设备上暂停，但主用设备不会尝试故障转移至暂停的设备。

只能恢复处于暂停状态的设备。该设备将与对等设备协商主用/备用状态。

注释 如有必要，可以输入 **configure high-availability suspend** 命令从 CLI 暂停 HA。要恢复 HA，请输入 **configure high-availability resume**。

开始之前

如果您通过 设备管理器暂停高可用性，高可用性将一直暂停直至您进行恢复，即使您重新加载设备亦如此。但是，如果您通过 CLI 暂停，这样是一种临时状态，重新加载后，设备自动恢复高可用性配置，并与对等体协商主用/备用状态。

如果您在备用设备上暂停高可用性，请检查主用设备当前是否正在运行部署作业。如果在部署作业进行期间切换模式，部署作业将失败，配置更改也会丢失。

过程

步骤 1 点击**设备**。

步骤 2 点击设备摘要右侧的**高可用性**链接。

步骤 3 从齿轮图标 (⚙) 选择适当的命令。

- **暂停高可用性** - 系统会提示您确认操作。阅读消息，并点击**确定 (OK)**。高可用性状态应显示设备处于暂停模式。
- **恢复高可用性** - 系统会提示您确认该操作。阅读消息，并点击**确定 (OK)**。设备与对等体进行协商后，高可用性状态应恢复正常，或为主用或为备用状态。

中断高可用性

如果您不想让两台设备继续以高可用性对方式运行，可以中断高可用性配置。中断高可用性后，设备会变成独立设备。设备配置将发生如下变化：

- 主用设备保留中断高可用性之前的完整配置，删除高可用性配置。
- 备用设备删除所有接口配置以及高可用性配置。所有物理接口均被禁用，但不会禁用子接口。管理接口保持活动状态，因此您可以登录到设备并重新配置。

注释 或者，您可以使用 BreakHAStatus API 资源（来自 API Explorer），并使用 **interfaceOption** 属性指导系统使用备用 IP 地址重新配置备用设备的接口。如果希望获得这个结果，则必须使用 API； 设备管理器 始终禁用这些接口。请注意，系统会重新配置 IP 地址，但不会重新配置所有接口选项，因此流量的行为可能不符合预期，直到您在中断后部署更改为止。

中断实际上会如何影响设备取决于执行中断时每台设备的状态。

- 如果设备处于运行状况正常的主用/备用状态，从主用设备中断高可用性。这将从高可用性对的两台设备删除高可用性配置。如果您仅想在备用设备上中断高可用性，您必须登录该设备，先暂停高可用性，然后再中断高可用性。
- 如果备用设备处于暂停或故障状态，从主用设备中断高可用性将仅删除主用设备上的高可用性配置。必须登录备用设备，同时在该设备上中断高可用性。
- 如果对等体仍协商高可用性或同步其配置，无法中断高可用性。等待协商或同步完成或超时。如果您认为系统会停留在这种状态，您可以暂停高可用性，然后中断高可用性。

注释 使用 设备管理器时，不能使用 **configure high-availability disable** 命令从 CLI 中断 HA。

开始之前

要获得理想结果，请将设备置于正常的主用/备用状态，然后从主用设备执行此操作。

过程

步骤 1 点击**设备**。

步骤 2 点击设备摘要右侧的**高可用性**链接。

步骤 3 从齿轮图标 (⚙)，选择**中断高可用性**。

步骤 4 阅读确认消息，决定是否选择该选项以禁用接口，然后点击**确定**。

如果您从备用设备中断高可用性，必须选择该选项以禁用接口。

系统将立即在此设备和对等体设备上部署所做的更改（如果可能）。在每个设备上完成部署，并让每台设备都变成独立设备可能需要几分钟的时间。

切换主用和备用对等体（强制故障转移）

您可以对正常运行的高可用性对切换主用/备用模式，即一个对等体处于主用状态，另一个是备用状态。例如，如果您要安装软件升级，可以将主用设备切换为备用设备，以便升级不会影响用户流量。

您可以从主用或备用设备切换模式，但从另一台设备的角度来看，对等体设备必须正在运行。如果任何设备被暂停（必须先恢复高可用性）或发生故障，则无法切换模式。

注释 如有必要，可以从 CLI 在主用和备用模式之间切换。从备用设备，输入 **failover active** 命令。从主用设备，输入 **no failover active** 命令。

开始之前

在切换模式之前，验证主用设备没有在执行部署作业。等待部署完成后再切换模式。

如果主用设备包含待处理的未部署更改，请在切换模式之前部署这些更改。否则，如果您从新主用设备运行部署作业，这些更改会丢失。

过程

步骤 1 点击**设备**。

步骤 2 点击设备摘要右侧的**高可用性**链接。

步骤 3 从齿轮图标 (⚙) 中选择**切换模式**。

步骤 4 阅读确认消息，并点击**确定 (OK)**。

系统将强制进行故障转移，以便主用设备成为备用设备，备用设备成为新的主用设备。

在故障转移后保留未部署的配置更改

对高可用性对中的设备进行配置更改时，需要在主用设备上编辑配置。然后部署更改，即可使用新配置同时更新主用和备用设备。主用设备是主设备还是辅助设备并不重要。

但是，未部署的更改不会在设备之间同步。任何未部署的更改仅在您做出这些更改的设备上可用。

因此，如果在有未部署更改的情况下进行故障转移，这些更改在新主用设备上不可用。但是，这些更改仍保留在现为备用状态的设备上。

要检索未部署的更改，您必须切换模式以强制进行故障转移，将另一台设备恢复为主用状态。当您登录到新主用设备时，未部署的更改可用，可以部署这些更改。使用**高可用性**设置齿轮菜单 (⚙) 中的**模式切换**命令。

记住以下几点：

- 如果从主用设备部署更改时备用设备上存在未部署的更改，备用设备上未部的署更改将被清除。这些更改无法检索。
- 当备用设备加入高可用性对时，备用设备上任何未部署的更改将被清除。每当设备加入或重新加入高可用性对时，都会同步配置。
- 如果包含未部署更改的设备发生灾难性的故障，并且您必须更换或重新映像该设备，未部署的更改会永久丢失。

在高可用性模式下更改许可证和注册

高可用性对中的设备必须具有相同的许可证和注册状态。要进行更改，请执行以下操作：

- 启用或禁用主用设备上的可选许可证。然后，部署配置，备用设备会请求（或释放）必要的许可证。启用许可证时，必须确保思科智能软件管理器账户具有足够的许可证，否则可能会造成一台设备合规，而另一台设备不合规。
- 单独注册或取消注册设备。两台设备必须均处于评估模式，或均已注册，才能正常使用。可以将设备注册到不同的思科智能软件管理器账户，但这些账户的出口控制功能设置的状态必须相同，要么都为启用，要么都为禁用。如果设备的注册状态不一致，将无法部署配置更改。

编辑 HA IPsec 加密密钥或 HA 配置

您可以通过登录到主用设备、进行更改并部署更改来更改任何故障转移条件。

但如果需要更改故障转移链路上使用的IPsec加密密钥，或更改故障转移链路或状态故障转移链路的接口或IP地址，则必须先中断HA配置。然后，可以使用新的加密密钥或故障转移/状态故障转移链路设置重新配置主设备和辅助设备。

将故障设备标记为运行状况正常

在常规运行状况监控过程中，高可用性配置中的设备可能会被标记为发生故障。如果设备运行状况正常，再次满足运行状况监控要求时，设备将恢复正常状态。如果您发现运行状况正常的设备频繁发生故障，您可能需要增加对等体超时，停止监控相对不重要的特定接口，或更改接口监控超时。

可以从CLI输入 **failover reset** 命令，强制将故障设备视为正常设备。我们建议您在主用设备上输入此命令，重置备用设备的状态。可以使用 **show failover** 或 **show failover state** 命令显示设备的故障转移状态。

将故障设备恢复到非故障状态不会自动将其设为主用设备。恢复后的设备仍处于备用状态，直到由于故障转移（强制或自然）变成主用设备。

重置设备状态不能解决导致设备被标记为故障设备的问题。如果您没有解决问题，或放宽监控超时，设备可能会被再次标记为故障设备。

升级 高可用性 威胁防御

使用此程序可升级高可用性设备。逐一升级它们。要最大限度地减少中断，请始终升级备用设备。也就是说，升级当前的备用设备，切换角色，然后升级新的备用设备。如果您需要更新 FXOS，请在两个机箱上执行此操作，然后再在任一机箱上进行升级 威胁防御。再次，始终升级备用设备。

⚠

注意 请勿在一台设备上进行或部署配置更改，而另一台设备正在升级或升级到混合版本对。即使系统显示为非活动，也不要在升级过程中手动重新启动或关闭；您可以将系统置于不可用状态并要求重新映像。您可以手动取消失败或正在进行的主要和维护升级，并重试失败的升级。如果问题持续存在，请联系 思科 TAC。

有关升级过程中可能遇到的这些问题和其他问题的详细信息，请参阅高可用性威胁防御升级故障排除，第 214 页。

开始之前

完成预升级核对表。确保部署中保持正常运行，并且能够成功通信。

提示 升级前核对表包括规划（首先阅读Cisco Secure Firewall Threat Defense 版本说明）、备份、获取升级包以及执行相关升级（例如 Firepower 4100/9300 的 FXOS）。它还包括必要的配置更改检查、 就绪性检查、磁盘空间检查，以及运行和计划任务的检查。对于详细的升级说明，包括升级前的检查清单，请参阅适用于您的版本的《适用于设备管理器的 Cisco Secure Firewall Threat Defense 升级指南》。

过程

步骤 1 登录备用设备。

步骤 2 选择**设备 (Device)**，然后点击“更新”(Updates) 面板中的**查看配置 (View Configuration)** 。“系统升级”(System Upgrade) 面板将显示当前运行的软件版本和您已上传的任何升级包。

步骤 3 上传升级包。

您只能上传一个软件包。如果上传新的软件包，它将替换旧的软件包。请确保您拥有适合您的目标版本和设备型号的软件包。点击**浏览 (Browse)** 或**替换文件 (Replace File)** 以开始上传。

上传完成后，系统将显示确认对话框。在点击**确定 (OK)** 之前，可以选择**立即运行升级 (Run Upgrade Immediately)** 以选择回滚选项并立即升级。如果您现在升级，请务必完成尽可能多的升级前核对表（请参阅下一步）。

步骤 4 执行最终的升级前检查，包括就绪性检查。

重新查看预升级核对表。确保您已完成所有相关任务，尤其是最终检查。 如果不手动运行就绪性检查，它将在您启动升级时运行。如果就绪检查失败，则会取消升级。有关详细信息，请参阅运行 威胁防御的升级就绪性检查 ， 第 770 页。

步骤 5 点击 **立即升级** 以开始安装过程。

a) 选择回滚选项。

您可以**升级失败时，系统将自动取消升级并回滚至上一版本**。启用此选项后，设备会在主要或维护升级失败时自动返回到升级前的状态。如果您希望能够手动取消或重试失败的升级，请禁用此选项。

b) 点击**继续 (Continue)** 升级并重新启动设备。

您将自动注销并转到状态页面，您可以在其中监控升级，直到设备重新启动。该页面包含用于取消正在进行中的安装的选项。如果禁用了自动回滚并且升级失败，则可以手动取消或重试升级。

升级时会丢弃流量。 仅对于 ISA 3000，如果您为电源故障配置了硬件旁路，则在升级期间流量会被丢弃，但在设备完成其升级后重新启动时会通过而不进行检查。

步骤 6 尽可能重新登录并验证升级是否成功。

“设备摘要”(Device Summary) 页面显示当前运行的软件版本和高可用性状态。在验证成功且恢复高可用性之前，请勿继续操作。如果成功升级后高可用性仍处于暂停状态，请参阅高可用性 威胁防御升级故障排除，第 214 页。

步骤 7 升级辅助设备。

a) 切换角色，使此设备处于活动状态：选择**设备 (Device)** > **高可用性 (High Availability)**，然后从齿轮菜单 (⚙) 中选择 **切换模式 (Switch Mode)** 。等待设备的状态更改为活动，并确认流量正常流动。注销。

b) 升级：重复上述步骤，登录新的备用设备，上传软件包，升级设备，监控进度并验证是否成功。

步骤 8 检查设备角色。

如果您有特定设备的首选角色，请立即进行更改。

步骤 9 登录到主用设备。

步骤 10 完成升级后的任务。

a) 更新系统数据库。如果没有为入侵规则、VDB 和 GeoDB 配置自动更新，请立即进行更新。

b) 完成发行说明中所述的其他任何升级后配置更改。

c) 部署。

高可用性 威胁防御升级故障排除

一般升级故障排除

当您升级任何设备时，无论是独立设备还是高可用性对，都可能发生这些问题。

升级包错误。

要查找升级包正确的型号，请在 思科支持和下载站点上选择或搜索您的型号，然后浏览至相应版本的软件下载页面。列出了可用的升级包以及安装包、修补程序和其他适用的下载。升级包文件名反映平台、软件包类型（升级、补丁、修补程序）、软件版本和内部版本。

从 6.2.1 及更高版本进行升级包经过签名，并在 .sh.REL.tar 中终止。请勿解压已签名的升级包。请勿通过邮件来重命名升级包或传送它们。

升级期间根本无法访问设备。

设备在升级期间或在升级失败时停止传输流量。升级之前，请确保来自您所在位置的流量不必遍历设备本身即可访问设备的管理界面。

设备在升级期间显示为非活动状态或无响应。

您可以手动取消正在进行的主要和维护升级；请参阅取消中 或重试中 威胁防御 升级，第 771 页。如果设备无响应，或者如果您无法取消升级，请联系思科 TAC。

⚠

注意 即使系统显示为非活动状态，也不要在升级过程中手动重新启动或关闭。您可以将系统置于不可用状态并要求重新映像。

升级成功，但系统未按预期运行。

首先，确保缓存的信息得到刷新。不要简单地刷新浏览器窗口以重新登录。相反，请从URL中删除任何“额外”路径并重新连接到主页；例如，http://threat-defense.example.com/。

如果问题仍然存在并需要返回到较早的主要或维护版本，则可以恢复；请参阅恢复中 威胁防御，第 772 页。如果无法恢复，则必须重新映像。

升级失败。

启动主要或维护升级时，请使用 **升级失败自动取消...**（自动取消）选项，用于选择升级失败时的操作，如下所示：

- 自动取消已启用（默认）：如果升级失败，则升级会取消，并且设备会自动恢复到升级前的状态。请更正所有问题，然后重试。
- 自动取消已禁用：如果升级失败，设备将保持原样。请更正问题并立即重试，或手动取消升级并稍后重试。

有关详细信息，请参阅取消中 或重试中 威胁防御 升级，第 771 页。如果无法重试或取消，或者问题持续存在，请联系思科 TAC。

高可用性升级故障排除

这些问题特定于高可用性升级。

如果未部署未提交的更改，则不会开始升级。

如果您收到一条错误消息，指出即使没有更改，也必须部署所有未提交的更改，请登录主用设备（请记住，您应该升级备用设备），创建一些细微更改，然后部署。然后，撤消更改，重新部署，并在备用设备上再次尝试升级。

如果这不起作用，并且设备根据建议运行不同的软件版本，请切换角色以使备用设备处于主用状态，然后暂停高可用性。从主用/暂停设备执行部署，恢复高可用性，然后切换角色，将主用设备再次切换为备用设备。这样，升级应该就会起作用。

从主用设备部署在备用升级期间失败，或导致应用同步错误。

如果在升级备用设备时从主用设备进行部署，可能会发生这种情况，但不支持这种情况。尽管出现错误，但仍继续进行升级。升级两台设备后，进行任何必要的配置更改并从主用设备进行部署。错误应该可以解决。

为避免这些问题，当一台设备正在升级或升级到混合版本对时，请勿在另一台设备上进行或部署配置更改。

升级期间所做的配置更改已丢失。

如果您绝对必须对混合版本对进行更改并部署，则必须对两台设备进行更改，否则在升级级别较低的主用设备后这些更改将会丢失。

升级后暂停高可用性。

升级后重新启动后，系统会暂时暂停高可用性，同时系统会执行一些最终自动化任务，例如更新库和重新启动 Snort。如果您在升级后不久登录 CLI，则很可能会注意到这一点。如果在升级完全完成且 设备管理器 可用后，高可用性无法自行恢复，请手动执行此操作：

1. 登录主用设备和备用设备，然后检查任务列表。等待所有任务在两台设备上完成运行。如果过早恢复高可用性，将来可能会出现故障转移导致中断的问题。
2. 选择 **设备** > **高可用性**，然后从齿轮菜单 (⚙) 选择 **恢复 HA** 。

混合版本对不会发生故障转移。

虽然高可用性的优势在于您可以在不中断流量或检查的情况下升级部署，但在整个升级过程中会禁用故障转移。也就是说，当一台设备处于离线状态时，不仅必须禁用故障转移（因为没有可故障转移的目标，您实际上已经进行了故障转移），而且还禁用了混合版本对的故障转移。升级期间是唯一（暂时）允许混合版本对的时间。在维护窗口期间安排升级，如果出现问题，升级的影响最小，并确保您有足够的时间在该窗口升级两台设备。

仅在一台设备上升级失败，或一台设备已恢复。该对现在运行的是混合版本。

一般操作不支持混合版本对。升级版本较低的设备或恢复较高版本的设备。对于修补程序，由于不支持恢复，如果您无法成功升级版本较低的设备，则必须中断高可用性，重新映像一个或两个设备，然后重新建立高可用性。

更换高可用性对中的设备

如有必要，您可以更换高可用性组中的一个设备，而不中断网络流量。

过程

步骤 1 如果要更换的设备能够正常使用，请确保故障转移至对等体设备，然后从该设备 CLI 使用 **shutdown** 命令正常关闭设备。如果设备不能使用，确认对等体在主用模式下运行。

如果具有管理员权限，还可以通过 设备管理器 CLI 控制台输入 **shutdown** 命令。

步骤 2 从网络中删除设备。

步骤 3 安装替换设备并重新连接接口。

步骤 4 在替换设备上完成设备安装向导。

步骤 5 在对等体设备上，转到“高可用性”(High Availability) 页面，并将配置复制到剪贴板。请注意，设备是主设备还是辅助设备。

如果有任何待处理更改，请现在部署这些更改并等待部署完成后再继续。

步骤 6 在替换设备上，点击**高可用性 (High Availability)** 中的**配置 (Configure)**，然后选择与对等体相反的设备类型。也即，如果对等体为主设备，选择**辅助**，如果对等体为辅助设备，选择**主**。

步骤 7 从对等体粘贴高可用性配置，然后输入 IPsec 密钥（如果您在使用）。点击**激活高可用性 (Activate HA)**。

部署完成后，设备将与对等体通信并加入高可用性组。系统随即导入主用对等体的配置，且根据您的选择替换设备可以在组中充当主要或辅助设备。您现在可以验证高可用性运行是否正常，而且如果需要，可切换模式使新设备变成主用设备。

监控高可用性

以下主题介绍如何监控高可用性。

请注意，事件查看器和控制面板仅显示与您所登录设备相关的数据。它们不会显示两台设备的合并信息。

监控常规故障转移状态和历史记录

您可以使用以下方法监控常规高可用性状态和历史记录：

- 在“设备摘要”上（点击**设备**），高可用性组会显示设备状态。

- 在“高可用性”(High Availability) 页面上（依次点击**设备 (Device)** > **高可用性 (High Availability)**），您可以看到两台设备的状态。如果发生任何故障，则会显示上次故障原因（来自故障转移历史记录）。点击两台设备之间的同步图标了解更多状态。

- 从“高可用性”(High Availability) 页面，点击状态旁边的**故障转移历史记录 (Failover History)** 链接。系统将打开 CLI 控制台并执行 **show failover history details** 命令。您还可以直接在 CLI 或 CLI 控制台中输入此命令。

CLI 命令

从 CLI 或 CLI 控制台中，您可以使用以下命令：

- **show failover**

  显示有关设备的故障转移状态的信息。

- **show failover history** ［**details**］

  显示过去的故障转移状态更改和状态变化的原因。添加 **details** 关键字可显示对等体的故障转移历史记录。此信息可帮助进行故障排除。

- **show failover state**

显示两个设备的故障转移状态。信息包括设备的主要或辅助状态、设备的主用/备用状态以及最新报告的故障转移原因。

- **show failover statistics**

  显示故障转移接口传输和接收的数据包计数。例如，如果输出接口显示设备发送数据包，但未收到任何数据包，那么链路可能出现问题。这可能是电缆问题、对等体上配置的IP地址，或可能是设备将故障转移接口连接到不同的子网。

```
> show failover statistics
        tx:320875
        rx:0
```

- **show failover interface**

  显示故障转移和状态故障转移链路的配置。例如：

```
> show failover interface
        interface failover-link GigabitEthernet1/3
                System IP Address: 192.168.10.1 255.255.255.0
                My IP Address    : 192.168.10.1
                Other IP Address : 192.168.10.2
        interface stateful-failover-link GigabitEthernet1/4
                System IP Address: 192.168.11.1 255.255.255.0
                My IP Address    : 192.168.11.1
                Other IP Address : 192.168.11.2
```

- **show monitor-interface**

  显示为高可用性监控的接口的相关信息。有关详细信息，请参阅监控高可用性监控接口的状态，第 218 页。

- **show running-config failover**

  显示运行配置中的故障转移命令。这些是配置高可用性的命令。

监控高可用性监控接口的状态

如果对任何接口启用了高可用性监控，您可以使用 **show monitor-interface** 命令在 CLI 或 CLI 控制台中查看受监控接口的状态。

```
> show monitor-interface
 This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
Other host: Secondary - Standby Ready
  Interface inside (192.168.1.14): Normal (Monitored)
  Interface outside (192.168.2.14): Normal (Monitored)
```

受监控接口可以具有以下状态：

- (Waiting) 加上任何其他状态，例如 Unknown (Waiting) - 接口尚未从对等体设备上的相应接口收到 hello 数据包。
- Unknown - 初始状态。此状态也可能意味着状态无法确定。
- Normal - 接口正在接收流量。
- Testing - 接口上有 5 个轮询时间未收听到 Hello 消息。
- Link Down - 接口或 VLAN 通过管理方式关闭。
- No Link - 接口的物理链路关闭。
- Failed - 在接口上没有收到流量，但在对等体接口上收听到流量。

监控与高可用性相关的系统日志消息

系统在优先级别 2 发出大量与故障转移有关的系统日志消息，级别 2 表示一种关键情况。与故障转移关联的消息 ID 的范围是：101xxx、102xxx、103xxx、104xxx、105xxx、210xxx、311xxx、709xxx 和 727xxx。例如，105032 和 105043 表示故障转移链路存在问题。有关系统日志消息的说明，请参阅 https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html中的 *Cisco* 威胁防御系统日志消息 指南。

注释 故障转移期间，系统按照逻辑先关闭接口，再启动接口，从而生成日志消息 411001 和 411002。这是正常活动。

必须先在**设备** > **日志记录设置**上配置诊断日志记录，才能查看系统日志消息。设置外部系统日志服务器，以便您可以稳定持续地监控消息。

在对等体设备上远程执行 CLI 命令

在 CLI 中，您可以使用 failover exec 命令在对等体上输入 show 命令，无需登录到对等体。

failover exec {**active** | **standby** | **mate**} 命令

必须指明哪一台设备应执行命令，主用设备还是备用设备，或输入 **mate**，如果您想要另一台设备而非您登录的设备响应。

例如，如果您想要查看对等体的接口配置和统计信息，可以输入：

```
> failover exec mate show interface
```

您不能输入 **configure** 命令。此功能与 **show** 命令搭配使用。

注释 如果您登录到主用设备，可以使用 **failover reload-standby** 命令重新加载备用设备。

不能通过 设备管理器 CLI 控制台输入这些命令。

高可用性故障排除（故障转移）

如果高可用性组中设备的表现未能达到预期，请考虑以下步骤排除配置故障。

如果主用设备显示对等体设备出现故障，请参阅设备故障状态故障排除，第 222 页。

过程

步骤 1 从每个设备（主要和辅助设备）：

- 对故障转移链路的另一设备的 IP 地址执行 ping 操作。
- 如果您使用单独的链接，对状态故障转移链路的另一设备的 IP 地址执行 ping 操作。

如果 ping 操作失败，请确保每个设备上的接口都连接到同一网段。如果您使用直连电缆连接，请检查电缆。

步骤 2 进行以下一般检查：

- 检查主要和辅助设备上是否存在重复的管理 IP 地址。
- 检查两台设备上是否存在重复的故障转移和状态故障切 IP 地址。
- 检查每台设备上的等效接口端口是否连接到同一网段。

步骤 3 检查备用设备上的任务列表或审核日志。主用设备上每次部署成功后，您都应该看到“从活动节点导入配置”任务。如果任务失败，请检查故障转移链路，并再次尝试部署。

注释 如果任务列表指示存在失败的部署任务，则可能是在部署作业期间发生了故障转移。如果启动部署任务时备用设备是主用设备，但在任务期间发生了故障转移，则部署将失效。要解决此问题，请切换模式，使备用设备再次成为主用设备，然后重新部署配置更改。

步骤 4 使用 **show failover history** 命令获取有关设备上状态更改的详细信息。

查找以下情况：

- 应用同步失败：

```
12:41:24 UTC Dec 6 2017

App Sync     Disabled     HA state progression failed due to APP SYNC timeout
```

在应用同步阶段，将配置从主用设备传输到备用设备。应用同步失败会导致设备被禁用，使设备无法再被设置为主用设备。

如果设备因应用同步问题被禁用，您可能需要对故障转移和状态故障转移链路的端点使用设备上的其他接口。必须对链路的两端使用相同的端口号。

如果 show failover 命令显示辅助设备处于伪备用状态，这可能意味着您在辅助设备上为故障转移链路配置的 IP 地址与您在主设备上配置的地址不同。确保在两台设备为故障转移链路使用相同的主要/辅助 IP 地址。

伪备用状态也可能表示您在主设备和辅助设备上配置的 IPsec 密钥不同。

有关其他应用同步问题，请参阅高可用性应用同步失败故障排除，第 222 页。

- 异常频繁的故障转移（从主用转到备用，然后再切换）可能意味着故障转移链路出现问题。最坏的情况是，两台设备可能都变为主用状态，导致流经的流量中断。对链路的两端执行 ping 操作以验证连接性。您还可以使用 **show arp** 检查故障转移 IP 地址和 ARP 映射是否正确。

  如果故障转移链路正常，并配置正确，请考虑增加对等体轮询和保持时间、接口轮询和保持时间，减少高可用性监控的接口数量，或增加接口阈值。

- 接口检查导致的故障。接口检查原因包括被视为故障的接口列表。检查这些接口，以确保它们配置正确，并且不存在硬件问题。验证链路另一端的交换机配置没有问题。如果没有任何问题，请考虑在这些接口上禁用高可用性监控，或者增加接口故障阈值或时间。

```
06:17:51 UTC Jan 15 2017

Active     Failed     Interface check

                         This Host:3

                            admin: inside

                            ctx-1: ctx1-1

                            ctx-2: ctx2-1

                         Other Host:0
```

步骤 5 如果无法检测到备用设备，而且您找不到具体原因（例如，故障转移链路上的LAN错误或电缆连接出错等），请尝试以下步骤。

a) 在备用设备上登录 CLI 并输入 **failover reset** 命令。此命令应将设备从故障状态更改为无故障状态。现在，检查主用设备上的高可用性状态。如果现在可检测到备用对等体，则问题解决。

b) 在主用设备上登录CLI并输入**failover reset**命令。这会重置主用和备用设备上的高可用性状态。理想情况下，它将重新建立设备之间的链路。检查高可用性状态。如果状态仍然不正确，请继续。

c) 在主用设备的CLI或从设备管理器首先暂停高可用性，然后恢复高可用性。CLI命令是**configure high-availability suspend** 和 **configure high-availability resume**。

d) 如果这些操作失败，请对备用设备执行 **reboot** 命令。

设备故障状态故障排除

如果一台设备在对等体设备的高可用性状态中被标记为故障设备（在**设备**或**设备** > **高可用性**页），可能有如下原因，假设设备 A 是主用设备，设备 B 是出现故障的对等体。

- 如果设备 B 尚未配置高可用性（仍然是单机模式），设备 A 显示设备 B 为故障设备。
- 如果在设备 B 上暂停高可用性，设备 A 将显示设备 B 为故障设备。
- 如果重新启动设备 B，设备 A 将显示设备 B 为故障设备，直至 B 完成重新启动并通过故障转移链路恢复通信。
- 如果应用同步 (App Sync) 在设备 B 上失败，设备 A 将显示设备 B 为故障设备。请参阅高可用性应用同步失败故障排除，第 222 页。
- 如果设备 B 在设备或接口运行状况监控中表现不合格，设备 A 将其标记为故障设备。检查设备 B 是否出现系统性问题。请尝试重启设备。如果设备大体运行状况正常，请考虑放宽设备或接口运行状况监控设置。**show failover history** 输出应提供有关接口运行状况检查失败的信息，
- 如果两台设备都变为主用状态，那么每台设备都会将对等体显示为故障设备。这通常表示故障转移链路出现问题。

  还可以指出与许可相关的问题。设备必须有一致的许可，要么均处于评估模式，要么都已注册。如果已注册，使用的智能许可证账户可以不同，但两个账户的出口控制功能设置必须相同，均为启用或禁用。对于出口控制功能，如果您使用不一致的设置配置 IPSec 加密密钥，当您激活 HA 后，两个设备都将变为主用状态。这会影响受支持网段上的路由，且您必须手动断开辅助设备上的 HA 才能消除影响。

高可用性应用同步失败故障排除

如果对等体无法加入高可用性组，或在您从主用设备部署更改时发生故障，请登录发生故障的设备，转至**高可用性 (High Availability)** 页面，然后点击**故障转移历史记录 (Failover History)** 链接。如果 **show failover history** 输出指出应用同步失败，即表示在 HA 验证阶段（在此过程中，系统检查设备是否可以作为高可用性组正常运行）出现问题。

这种故障可能会如下所示：

```
==========================================================================
From State                To State                  Reason
==========================================================================
16:19:34 UTC May 9 2018
Not Detected              Disabled                  No Error

17:08:25 UTC May 9 2018
Disabled                  Negotiation               Set by the config command

17:09:10 UTC May 9 2018
Negotiation               Cold Standby              Detected an Active mate

17:09:11 UTC May 9 2018
Cold Standby              App Sync                  Detected an Active mate

17:13:07 UTC May 9 2018
```

```
App Sync                    Disabled                    CD App Sync error is
High Availability State Link Interface Mismatch between Primary and Secondary Node
```

理想情况下，当 From State 为 App Sync 时，您希望收到的消息是“All validation passed”，并且节点的状态变为 Standby Ready。任何验证失败都会将对等体的状态转换成 Disabled (Failed)。您必须解决这些问题，使对等体能够再次用作高可用性组。请注意，如果通过对主用设备进行更改来修复应用同步错误，则必须先对其进行部署，然后再恢复高可用性以使对等节点加入。

以下消息表示发生了故障，并介绍如何解决问题。这些错误可能发生在节点加入和每次后续部署时。节点加入期间，系统会对主用设备上的最新部署配置执行检查。

- 主要和辅助节点之间的许可证注册模式不匹配。

  许可证错误指出，一个对等体已注册，而另一个对等体处于评估模式。对等体必须同时为注册状态或同处于评估模式，才能加入高可用性组。由于无法将注册设备恢复为评估模式，必须从**设备 (Device)** > **智能许可证 (Smart License)** 页面注册另一台对等体。

  如果您注册的设备为主用设备，请在注册设备后执行部署。部署将强制设备刷新并同步配置，从而允许辅助设备正确加入高可用性组。

- 主要和辅助节点之间的许可证导出合规性不匹配。

  许可证合规性错误表示，设备注册到不同的思科智能软件管理器账户，并且其中一个账户启用了出口控制功能，而另一个账户没有启用。必须使用具有相同出口控制功能设置（启用或禁用）的账户注册设备。在**设备 (Device)** > **智能许可证 (Smart License)** 页面上更改设备注册。

- 主要和辅助节点之间的软件版本不匹配。

  软件不匹配错误表示，对等体运行不同版本的 威胁防御 软件。一次在一台设备上安装软件升级时，系统仅临时允许不匹配。但是，您无法在升级对等体的过程中部署配置更改。要解决此问题，请升级对等体，然后重新部署。

- 主要和辅助节点之间的物理接口不匹配。

  HA 组中的备用设备必须具有主用设备上存在的所有物理接口，且这些接口必须具有相同的硬件名称和类型（例如 GigabitEthernet1/1）。此错误表示备用设备缺少主用设备上存在的某些接口。允许在备用设备上拥有比主用设备更多的接口，因此请切换哪台设备为主用设备或选择另一个对等体设备。但是，不匹配的接口应该是临时状态，例如，如果正在替换一台设备上的接口模块，且需要在短时间内不使用该模块进行运行。对于正常操作，两台设备应具有相同数量和类型的接口。

- 主要和辅助节点之间的故障转移链路接口不匹配。

  将每台设备的故障转移物理接口连接到网络时，必须选择相同的物理接口。例如，每台设备上的 GigabitEthernet1/8 接口。此错误表示您使用不同的接口。要解决错误，请更正对等体设备上的电缆。

- 主要和辅助节点之间的状态故障转移链路接口不匹配。

  如果您使用单独的状态故障转移链路，将每台设备的状态故障转移物理接口连接到网络时，必须选择相同的物理接口。例如，每台设备上的 GigabitEthernet1/7 接口。此错误表示您使用不同的接口。要解决错误，请更正对等体设备上的电缆。

- 主要和辅助节点之间的故障转移/状态故障转移链路 EtherChannel 成员接口不匹配。

  如果选择故障转移或状态故障转移接口的 EtherChannel 接口，则 Etherchannel 必须在每台设备上具有相同的 ID 和成员接口。此错误消息指示是故障转移还是具有不匹配的状态故障转移链路。要解决此错误，请更正 EtherChannel 接口的配置，使其使用相同的 ID，并在每台设备上包含相同的接口。

- 主要和辅助节点之间的设备型号不匹配。

  加入高可用性组的对等体必须是型号完全相同的设备。此错误消息表示，对等体的设备型号不相同。必须选择不同的对等体来配置高可用性。

- 主用和备用节点不能位于同一机箱上。

  无法使用在同一硬件机箱上托管的设备配置高可用性。在同一机箱上支持多个设备的型号上配置高可用性时，必须选择驻留在单独硬件上的设备。

- 发生未知错误，请重试。

  应用同步期间出现问题，但系统无法识别该问题。再次尝试部署配置。

- 规则数据包损坏。请更新规则数据包，并重试。

  入侵规则数据库出现问题。在发生故障的对等体上，请转至**设备 (Device)** > **更新 (Updates)**，然后点击**规则 (Rule)** 组中的**立即更新 (Update Now)**。等待更新完成，然后部署更改。然后，您可以从主用设备重试部署。

- 主节点和辅助节点之间的云服务注册状态不匹配。

  其中一个节点注册到了思科云，但另一个节点未注册。两个节点必须都注册，或者两个节点都没有注册，才能形成高可用性组。转到每台设备上的**设备** > **系统设置** > **服务**，并确保两台设备注册在同一云服务区域中。

- 主用和备用节点无法具有不同的云区域。

  设备在不同的思科云服务区域中注册。确定正确的区域，从智能许可取消注册另一台设备，并在重新注册期间选择正确的区域。如果两台设备均有错误的区域，请取消注册这两台设备，然后在正确的区域重新注册。

- 部署数据包损坏。请重试。

  这是一个系统错误。再次尝试部署，应该能解决此问题。

第 11 章

接口

以下主题介绍如何在 威胁防御 设备上配置接口。

关于 威胁防御 接口

威胁防御 包括数据接口和 管理 接口。

将电缆（以物理方式或虚拟方式）连接到接口接头时，您需要配置该接口。至少需要命名并启用该接口，该接口才会传输流量。如果该接口是网桥组的成员，此配置就已足够。对于非网桥组成员，您还需要为该接口指定一个IP地址。如果要在特定端口上创建VLAN子接口（而非单一物理接口），通常要在该子接口（而不是物理接口）上配置IP地址。通过VLAN子接口，可以将一个物理接口拆分为多个标记有不同VLANID的逻辑接口，这一点在您连接到交换机的中继端口时非常有用。请勿在被动接口上配置 IP 地址。

接口页面包括接口类型的子页面： **接口 (Interfaces)**（适用于物理接口）、**网桥组 (Bridge Groups)**、**虚拟隧道接口 (Virtual Tunnel Interfaces)**、**EtherChannel** 和 **VLAN**（适用于Firepower 1010）。请注意， Firepower 4100/9300 EtherChannel 列于 **接口 (Interfaces)** 页面上而不是 **EtherChannel** 页面上，因为仅可修改 FXOS 中的 EtherChannel 参数，而不是 设备管理器中的参数。各页显示的是可用接口、接口名称、地址、模式以及状态。您可以直接在接口列表中更改接口的状态，打开接口或将其关闭。列表将基于您的配置显示接口特征。使用网桥组、EtherChannel 或 VLAN 接口上的开/关箭头可查看成员接口，这些成员接口也会显示于相应列表中。还可以查看受支持父接口的子接口。有关如何将这些接口映射到虚拟接口和网络适配器的信息，请参阅 VMware 网络适配器和接口如何映射到 威胁防御 物理接口 ，第 16 页。

以下主题介绍了通过 设备管理器 配置接口的局限性及其他接口管理概念。

接口模式

可以为每个接口配置下列其中一种模式：

路由

每个第 3 层路由接口都需要唯一子网上的一个 IP 地址。通常会将这些接口与交换机、另一个路由器上的端口或 ISP/WAN 网关连接。

内联

将接口添加到内联集后，模式将更改为内联。不能直接选择内联作为模式。

被动

被动接口使用交换机 SPAN（交换端口分析器）或镜像端口监控在网络中传输的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。如果在被动部署中配置系统，系统将不能执行某些操作，例如，阻止流量或流量整形。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。

交换机端口 (Firepower 1010)

交换机端口使用硬件中的交换功能在第 2 层转发流量。同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受 威胁防御安全策略的限制。接入端口仅接受未标记流量，可以将其分配给单个 VLAN。中继端口接受未标记和已标记流量，且可以属于多个 VLAN。无法将管理接口配置为交换机端口。

BridgeGroupMember

网桥组是 威胁防御设备用于桥接而非路由的一组接口。所有接口位于同一网络上。网桥组由在网桥网络上有 IP 地址的桥接虚拟接口 (BVI) 表示。

如果指定 BVI，您可以在路由接口和 BVI 之间路由。在这种情况下，BVI 充当成员接口和路由接口之间的网关。如果不指定 BVI，网桥组成员接口上的流量不能离开网桥组。通常，可以指定该接口，以便将成员接口路由到互联网。

路由模式下网桥组的一种用途是在 威胁防御 设备上而非外部交换机上使用额外接口。您可以将终端直接连接到网桥组成员接口。您还可以连接交换机，以将更多终端添加到与 BVI 相同的网络。

管理/诊断接口

管理接口

管理接口与设备上的其他接口分离。它用于设备管理器管理、智能许可和数据库更新。您也可以使用数据接口而不是管理接口来管理 威胁防御 设备。管理接口使用自己的 Linux IP 地址和静态路由。您可以在**设备 (Device)** > **接口 (Interfaces)** 页面中配置其设置，也可以在 CLI 中使用 **configure network** 命令配置其设置。

对于硬件设备而言，一种配置管理接口的方法是，不将端口连接到网络。而是仅配置管理 IP 地址，并把它配置为将数据接口用作从互联网获取更新的网关。然后，打开 HTTPS/SSH 流量（默认情况下启用 HTTPS）的内部接口，并使用内部 IP 地址打开 设备管理器 （请参阅 配置管理访问列表，第 728 页）。

对于 threat defense virtual，建议的配置是将 Management0/0 连接到与内部接口相同的网络，并将内部接口用作网关。

诊断接口（旧）

对于使用 7.3 及更高版本的新设备，您不能使用旧诊断接口。仅合并的管理接口可用。

如果已升级到 7.4 或更高版本，并且没有为诊断接口进行任何配置，则接口将自动合并。

如果已升级到 7.4 或更高版本，并且已为诊断接口进行了配置，则可以选择手动合并接口，也可以继续使用单独的诊断接口。请注意，在更高版本中将删除对诊断接口的支持，因此您应计划尽快合并接口。要手动合并管理接口和诊断接口，请参阅合并管理和诊断接口，第 288 页。阻止自动合并的配置包括：

- 名为“management”的数据接口 - 此名称保留用于合并的管理接口。
- 诊断接口中的 IP 地址
- 诊断接口中启用了 DNS
- 系统日志或 RADIUS（对于远程访问 VPN）源接口为诊断接口
- AD 或 RADIUS（对于远程访问 VPN）未指定源接口，并且至少有一个接口配置为管理专用接口（包括诊断接口）- 这些服务的默认路由查找已从管理专用路由表更改为数据路由表，没有回退到管理。因此，要使用某个管理专用接口，必须选择该特定接口，而不是依赖于路由查找。
- 诊断接口中的静态路由或 SLA 监控
- 使用诊断接口的 FlexConfig
- 诊断接口的 DDNS

有关旧诊断接口工作方式的详细信息，请参阅本指南的 7.3 版本。

配置单独管理网络的建议

（硬件设备。）如果要使用单独管理网络，请将物理管理接口连接到交换机或路由器。

对于 threat defense virtual，请将 Management0/0 连接到不同于任何数据接口的独立网络。如果仍然使用默认 IP 地址，则需要更改管理 IP 地址或内部接口 IP 地址（因为它们在同一子网上）。

然后，依次选择**设备 > 接口**，编辑管理接口，并配置所连接网络上的 IPv4 或 IPv6 地址（或两者）。如果需要，可以配置 DHCP 服务器以便能向网络上的其他终端提供 IPv4 地址。如果路由器在管理网络上有到互联网的路由，则可将其作为网关来使用。如果没有，请使用数据接口作为网关。

安全区

可为每个接口分配一个安全区。然后根据区域应用您的安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。例如，可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。

每个区域都有一个与接口模式直接相关的模式。您可以仅向同一模式安全区添加接口。

对于网桥组，可将成员接口添加到区域，但不能添加桥接虚拟接口 (BVI)。

不要将管理接口包括在区域中。区域只适用于数据接口。

可在**对象 (Objects)** 页面创建安全区。

IPv6 寻址

您可以为 IPv6 配置两种类型的单播地址：

- 全局 - 全局地址是可在公用网络上使用的公用地址。对于网桥组，需要在桥接虚拟接口 (BVI) 上而非每个成员接口上配置全局地址。不能将以下任何地址指定为全局地址。
  - 内部保留的 IPv6 地址：fd00::/56（fd00:: 至 fd00:0000:0000:00ff:ffff:ffff:ffff:ffff）
  - 未指定的地址，例如 ::/128
  - 环回地址 ::1/128
  - 组播地址 ff00::/8
  - 链路本地地址 fe80::/10
- 链路本地 - 链路本地地址是只能在直连网络上使用的专用地址。路由器不使用链路本地地址转发数据包；它们仅用于在特定物理网段上通信。链路本地地址可用于地址配置或网络发现功能，例如地址解析和邻居发现。在网桥组中，对 BVI 启用 IPv6 将为每个网桥组成员接口自动配置链路本地地址。每个接口必须有自己的地址，因为链路本地地址仅在网段中可用，并且会与接口 MAC 地址绑定。

至少需要配置链路本地地址，IPv6 才会起作用。如果配置全局地址，则接口上会自动配置链路本地地址，因此无需另外专门配置链路本地地址。如果不配置全局地址，则需要自动或手动配置链路本地地址。

Auto-MDI/MDIX 功能

对于 RJ-45 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。对于千兆以太网，当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

接口的准则和限制

以下主题介绍接口的局限性。

接口配置的限制条件

使用 设备管理器 配置设备时，接口配置存在许多局限性。如果您需要以下任意功能，则必须使用 管理中心 来配置设备。

- 仅支持路由防火墙模式。无法配置透明防火墙模式的接口。
- 可以配置被动接口，但不能配置 ERSPAN 接口。
- 无法配置冗余接口。
- 您可以在 设备管理器 中为以下型号配置 EtherChannel：Firepower 1000、Firepower 2100、Secure Firewall 3100、ISA 3000。Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。Firepower 4100/9300 EtherChannel 显示在单个物理接口旁的设备管理器 **接口 (Interfaces)** 页面中。
- 仅可添加一个网桥组。
- 威胁防御 仅支持路由接口上的 IPv4 PPPoE。高可用性设备不支持 PPPoE。

各设备型号的最大 VLAN 子接口数量

设备型号限制可配置的最大 VLAN 子接口数量。请注意，仅可在数据接口上而不可在管理接口上配置子接口。

下表介绍各设备型号的限制。

型号	最大 VLAN 子接口数量
Firepower 1010	60
Firepower 1120	512
Firepower 1140 和 1150	1024
Firepower 2100	1024

型号	最大 VLAN 子接口数量
Secure Firewall 3100	1024
Firepower 4100	1024
Firepower 9300	1024
Threat Defense Virtual	50
ISA 3000	100

配置物理接口

要启用物理接口，至少必须启用它。通常，您还需要为它命名并配置IP寻址。如果要创建VLAN子接口，或者配置被动模式接口，或者要将接口添加到网桥组，无需配置IP寻址。 Firepower 4100/9300 EtherChannel 显示在单个物理接口旁的 设备管理器 **接口 (Interfaces)** 页面中，此过程也适用于EtherChannel。必须在机箱上的 FXOS 中执行 Firepower 4100/9300EtherChannels 的所有硬件配置。

注释 要将物理接口配置为 Firepower 1010 交换机端口，请参阅配置 VLAN 接口和交换机端口 (Firepower 1010)，第 249 页。

要将物理接口配置为被动接口，请参阅将物理接口配置为被动模式，第 267 页。

您可以禁用接口，以临时阻止在相连网络中的传输。无需删除该接口的配置。

过程

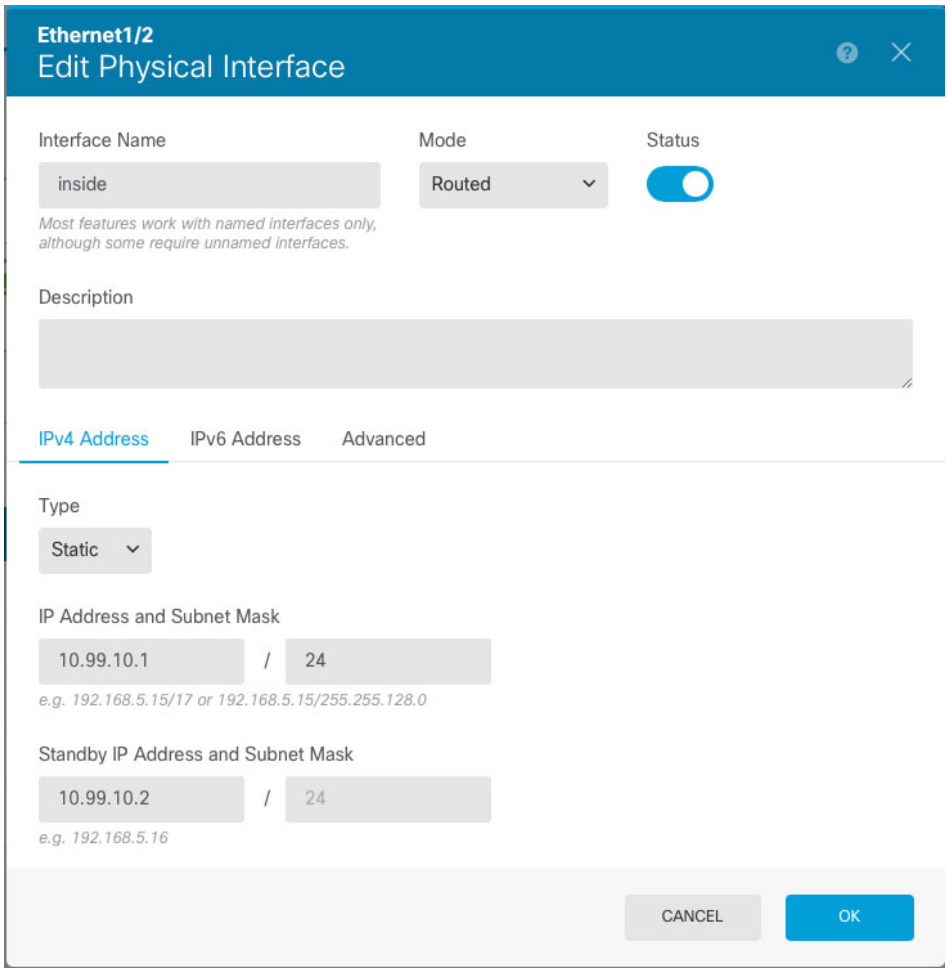
步骤 1 点击**设备**，然后点击**接口**摘要中的链接。

系统默认选择**接口 (Interfaces)** 页面。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 点击要编辑的物理接口的编辑图标 ( )。

不能编辑在高可用性配置中用作故障转移或状态故障转移链路的接口。

步骤 3 进行以下设置：



a) 设置**接口名称**。

设置接口名称，最多 48 个字符。字母字符必须为小写。例如 **inside** 或 **outside**。如果没有名称，将忽略其余的接口配置。除非配置子接口，否则接口应有名称。**注意：**请勿配置要添加至 EtherChannel 的接口的名称。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

b) 选择**模式**。

- **路由** - 路由模式接口需要对流量执行所有防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组、TCP 规范化以及防火墙策略。这是正常接口模式。
- **内联 (Inline)** - 将接口添加到内联集后，模式将更改为内联。不能直接选择内联作为模式。编辑将用于内联集中的接口时，请选择**路由 (Routed)** 模式作为初始模式，并且不要配置任何类型的 IP 寻址。
- **被动** - 被动接口使用交换机 SPAN 或镜像端口监控网络中流经的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流

量。如果在被动部署中配置系统，系统将不能执行某些操作，例如，阻止流量或流量整形。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。如果您选择此模式，无需执行此过程的其余部分。请参阅将物理接口配置为被动模式，第 267 页。请注意，无法在被动接口上配置 IP 地址。

- **交换机端口** - (Firepower 1010) 交换机端口允许在同一 VLAN 上的端口之间进行硬件切换。交换流量不受安全策略的约束。如果您选择此模式，无需执行此过程的其余部分。相反，请参阅配置 VLAN 接口和交换机端口 (Firepower 1010)，第 249 页

如果稍后将此接口添加至网桥组，则模式将自动更改为 **BridgeGroupMember**。请注意，无法在网桥组成员接口上配置 IP 地址。

c) 将**状态**滑块设置为已启用设置 ()。

对于 Firepower 4100/9300 设备上的接口，还必须启用 FXOS 中的接口。

如果要为此物理接口配置子接口，则可能已完成。点击**保存**并继续配置 VLAN 子接口和 802.1Q 中继，第 260 页。否则，请继续。

注释 即使在配置子接口时，为接口命名和提供 IP 地址也有效。这不是常规设置，但如果确定符合您的需求，则可以进行配置。

d) （可选）设置**说明**。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 4 点击 **IPv4 地址**选项卡，并配置 IPv4 地址。

从**类型**字段中选择以下任一选项：

- **DHCP** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
  - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
  - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。
- **静态** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，键入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保该地址尚未在网络中使用。

  如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

  注释 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅配置 DHCP 服务器，第 736 页。

- **PPPoE** - 如果应使用基于以太网的点对点协议 (PPPoE) 获取地址，请选择此选项。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。如果您配置高可用性，将不能使用此选项。设置以下值：
  - **组名称** - 指定您选择用于表示此连接的组名称。
  - **PPPoE 用户名** - 指定 ISP 提供的用户名。
  - **PPPoE 密码** - 指定 ISP 提供的密码。
  - **PPP 身份验证** - 选择 **PAP**、**CHAP** 或 **MSCHAP**。

    PAP 在身份验证过程中传递明文用户名和密码，这样并不安全。使用 CHAP 时，客户端可返回加密的 [challenge plus password] 和明文用户名来响应服务器质询。CHAP 比 PAP 更安全，但其不会加密数据。MSCHAP 与 CHAP 类似但更安全，因为服务器只对加密密码进行存储和比较，而不是像 CHAP 一样存储和比较明文密码。MSCHAP 还可生成密钥，以便 MPPE 进行数据加密。
  - **PPPoE 获知的路由指标** - 向获悉的路由分配管理距离。有效值为从 1 到 255。默认情况下，获悉的路由的默认管理距离为 1。
  - **从 PPPoE 获取默认路由** - 选中此复选框可支持从 PPPoE 服务器获取默认路由。
  - **IP 地址类型** - 选择**动态**可从 PPPoE 服务器获取 IP 地址。如果从 ISP 分配了静态 IP 地址，也可以选择**静态**。

步骤 5 （可选。）点击 **IPv6 地址**选项卡，并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请选择**已启用**。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

  注释 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置** - 选择此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

  虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但 威胁防御 设备在这种情况下确实会发送路由器通告消息。选择**抑制 RA** 可抑制消息，遵从 RFC 要求。

- **静态地址/前缀** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 IPv6 寻址，第 228 页。

  如果仅使用本地链路地址，请选择**本地链路**选项。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

  注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。请注意，我们建议根据修改的EUI-64格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **抑制 RA** - 是否抑制路由器通告。威胁防御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。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

  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。

  对于不希望 威胁防御 设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 6 （可选。）配置高级选项，第 272 页。

高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 7 点击**确定 (OK)**。

下一步做什么

- 将接口添加至相应的安全区。请参阅配置安全区，第 133 页。
- 向您的动态 DNS 服务提供商注册一个完全限定域名 (FQDN)，并配置 DDNS 以更新 DNS 服务器上的接口地址（IPv4 和 IPv6）。请参阅配置动态 DNS，第 739 页。

配置管理接口

管理接口是一个特殊接口，在**接口 (Interfaces)** 页面上与数据接口一起显示，但不作为数据接口运行。管理接口有以下用途：

- 您可以与该 IP 地址建立 Web 连接和 SSH 连接，并通过该接口配置设备。
- 系统通过此 IP 地址获取智能许可和数据库更新。
- 您也可以将此接口用于系统日志，

如果使用 CLI 安装向导，则在初始系统配置期间，为设备配置管理地址和网关。如果使用 设备管理器 安装向导，管理地址和网关将保留默认值。

如有必要，您可以通过 设备管理器更改这些地址。您还可以在 CLI 中使用 **configure network ipv4 manual** 和 **configure network ipv6 manual** 命令更改管理地址和网关。要恢复默认管理接口设置，请使用 **configure network** {**ipv4** | **ipv6**} **dhcp-dp-route** 命令。

您可以定义静态地址，也可以在管理网络中有另一台设备用作 DHCP 服务器时，通过 DHCP 获取地址。对于大多数平台，管理接口默认会从 DHCP 获取 IP 地址。

⚠

注意 如果更改当前连接的地址，则当保存更改时，由于这些更改会立即应用，您将丢失对 设备管理器（或 CLI）的访问。您需要重新连接到设备。确保新地址有效且在管理网络中可用。

开始之前

如果您已升级到 7.4 或更高版本，并且尚未合并管理接口和诊断接口，请参阅合并管理和诊断接口，第 288 页。

过程

步骤 1 点击**设备**，然后点击**设备** > **接口**链接。

步骤 2 编辑管理接口。

步骤 3 选择要如何定义管理**网关**。

网关确定系统如何访问互联网，以获取智能许可证、数据库更新（例如 VDB、规则、地理位置、URL）以及访问管理 DNS 和 NTP 服务器。从以下选项中选择：

静态 IP 选项：

- **使用数据接口作为网关** - 如果没有单独的管理网络连接到管理接口，请选择此选项。流量将根据路由表路由到互联网，通常会经过外部接口。此选项在 threat defense virtual 设备上不受支持。
- **为管理接口使用独特网关** - 如果有单独的管理网络连接到管理接口，请为 IPv4 和 IPv6 指定独特网关（如下所示）。

DHCP IP 选项：

- **为管理接口（可回退到数据接口）使用独特网关** - 如果 DHCP 服务器提供网关，则系统会通过管理接口将管理流量路由到网关。如果 DHCP 服务器不提供网关，则系统会根据数据接口路由表路由管理流量，通常是通过外部接口发送流量。此选项在 threat defense virtual 设备上不受支持。
- **为管理接口（无回退）使用独特网关** - 系统通过管理接口将管理流量路由到 DHCP 服务器提供的网关。如果 DHCP 服务器不提供网关，则系统将只能访问管理接口上的本地主机。要通过数据接口进行路由，请选择“回退”选项。

步骤 4 配置 **IPv4** 和/或 **IPv6** 管理地址、子网掩码或 IPv6 前缀，并根据需要配置网关。

必须配置至少一组属性。将一组设置留空将会禁用该寻址方法。

- 选择**类型** > **静态**以设置静态 IP 地址。
- 依次选择**类型** > **DHCP**，通过 DHCP 或 IPv6 自动配置功能获取地址和网关。

步骤 5 （可选） 如果配置的是静态 **IPv4** 地址，请在该接口上配置 DHCP 服务器。

如果在管理接口上配置 DHCP 服务器，则管理网络中的客户端可从 DHCP 池获取其地址。此选项在 threat defense virtual 设备上不受支持。

a) 依次点击**启用 DHCP 服务器** > **开**。
b) 输入服务器的**地址池**。

地址池是允许服务器为请求地址的客户端提供的 IP 地址的范围（最低至最高）。该 IP 地址范围必须与管理地址位于同一子网上，并且不能包括接口本身的 IP 地址、广播地址或子网地址。指定该池的开始和结束地址，用连字符隔开。例如 192.168.45.46-192.168.45.254。

步骤 6 在**高级 (Advanced)** 页面上配置管理接口 **MTU**，如果启用的是 IPv4，则介于 8 和 1500 之间；如果启用的是 IPv6，则介于 1280 和 1500 之间。

默认值为 1500 字节。

步骤 7 点击**保存 (Save)**，阅读警告，然后点击**确定 (OK)**。

配置网桥组

网桥组是将一个或多个接口分组的虚拟接口。对接口分组的主要原因是创建一组交换接口。如此，就可以将工作站或其他终端设备直接连接到网桥组中所包含的接口。您不需要通过单独的物理交换机来连接这些设备，尽管您也可以将一台交换机连接到某个网桥组成员。

组成员没有 IP 地址。相反，所有成员接口共用桥接虚拟接口 (BVI) 的 IP 地址。如果在 BVI 上启用 IPv6，系统会自动为成员接口分配唯一的链路本地地址。

单独启用和禁用成员接口。这样就可以禁用任何未使用的接口，而无需将其从网桥组删除。网桥组本身始终处于启用状态。

通常会在网桥组接口 (BVI) 上配置 DHCP 服务器，为通过成员接口连接的任何终端提供 IP 地址。不过，如果愿意的话，您也可以在连接到成员接口的终端上配置静态地址。网桥组中的所有终端都必须具有与网桥组 IP 地址位于同一子网的 IP 地址。

准则和限制

- 可以添加一个网桥组。
- 不支持将设备管理器定义的 EtherChannel 作为网桥组成员。Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。
- 在 Firepower 2100 系列或 threat defense virtual设备上不能配置网桥组。
- 对于 Firepower 1010，不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个网桥组中。
- ISA 3000 预配置网桥组 BVI1 (未命名，这意味着其不参与路由)。BVI1 包括所有数据接口：GigabitEthernet1/1 (outside1)、GigabitEthernet1/2 (inside1)、GigabitEthernet1/3 (outside2) 和 GigabitEthernet1/4 (inside2)。必须设置 BVI1 IP 地址以匹配您的网络。

开始之前

指定将成为网桥组成员的接口。具体而言，每个成员接口都必须满足以下要求：

- 该接口必须具有名称。
- 该接口不能有任何已定义的 IPv4 或 IPv6 地址，无论是静态分配的还是通过 DHCP 获得的。如果需要从当前正在使用的某个接口删除地址，则可能还需要删除该接口的其他配置，例如静态路由、DHCP 服务器或 NAT 规则，具体视具有地址的接口而定。
- 必须将该接口从所属安全区中删除（如果它在某个区域中），并删除该接口的所有NAT规则，然后才能将其添加到网桥组。

过程

步骤 1 点击**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接，再点击**网桥组 (Bridge Groups)**。

网桥组列表显示现有网桥组。点击开/关箭头可查看各网桥组的成员接口。成员接口也会单独显示于**接口 (Routing)** 或 **VLAN** 页面上。

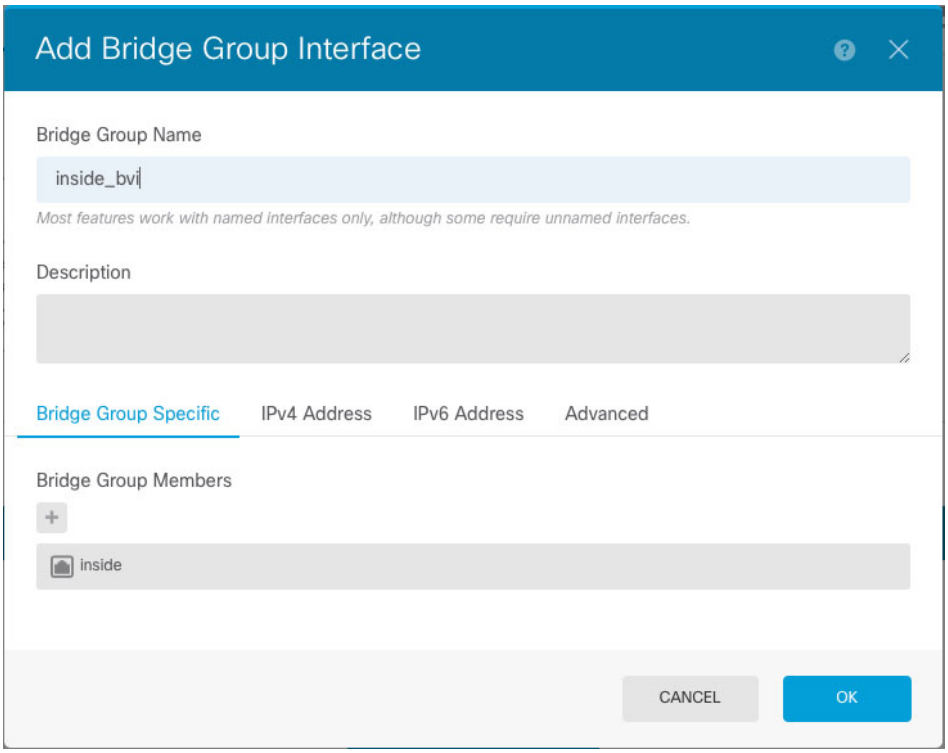
步骤 2 执行以下操作之一：

- 点击 BVI1网桥组的编辑图标 ( )。
- 点击**创建网桥组 (Create Bridge Group)** 或加号图标 ( ) 创建新组。

  注释 网桥组只能有一个。如果已经定义了一个网桥组，则应编辑该组而非尝试创建新组。如果需要创建新的网桥组，则必须先删除现有网桥组。

- 如果不再需要某个网桥组，点击该网桥组的删除图标 ( )。删除网桥组时，其成员将变成标准路由接口，并且所有 NAT 规则或安全区成员身份保持不变。可以编辑这些接口为其提供 IP 地址。如果要将其添加到新的网桥组，需要先删除 NAT 规则并将接口从所属安全区中删除。

步骤 3 进行以下配置：



a) （可选） 设置**接口名称**。

设置网桥组的名称，最多 48 个字符。字母字符必须为小写。例如 **inside** 或 **outside**。如果希望此 BVI 参与其与其他命名接口之间的路由，请设置名称。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

b) （可选） 设置**说明**。

一行说明最多可包含 200 个字符（不包括回车符）。

c) 编辑**网桥组成员**列表。

最多可向一个网桥组添加 64 个接口或子接口。

- 添加接口 - 点击加号图标 (+)，点击一个或多个接口，然后点击**确定**。
- 移除接口 - 将鼠标悬停于接口上方，然后点击右侧的 **x**。

步骤 4 点击 **IPv4 地址**选项卡，并配置 IPv4 地址。

从**类型**字段中选择以下任一选项：

- **静态** - 如果希望分配固定的地址，请选择此选项。键入网桥组的 IP 地址和子网掩码。所有连接的终端都将位于此网络中。确保该地址尚未在网络中使用。

如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

注释　如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅配置 DHCP 服务器，第 736 页。

- **动态 (DHCP)** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。网桥组通常不会使用此选项，但是您可以根据需要如此配置。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
  - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
  - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。

步骤 5　（可选。）点击 **IPv6 地址**选项卡，并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请选择**已启用**。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

  注释　禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **静态地址/前缀** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 IPv6 寻址，第 228 页。

  如果仅使用本地链路地址，请选择**本地链路**选项。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

  注释　链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。请注意，我们建议根据修改的EUI-64格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

- **抑制 RA** - 是否抑制路由器通告。威胁防御设备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。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

  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。

  对于不希望 威胁防御 设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 6　（可选。）配置高级选项，第 272 页。

请对网桥组成员接口配置大多数高级选项，不过其中一些选项可用于网桥组接口。

高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 7 点击**确定 (OK)**。

下一步做什么

- 确保已启用您打算使用的所有成员接口。
- 为网桥组配置 DHCP 服务器。请参阅配置 DHCP 服务器，第 736 页。
- 将成员接口添加到相应的安全区。请参阅配置安全区，第 133 页。
- 确保各项策略（例如身份、NAT 和访问策略）可为网桥组和成员接口提供所需的服务。

配置 EtherChannel

本节介绍 EtherChannel 及其配置方式。

注释 您可以将 设备管理器 中的 EtherChannel 添加到以下型号：

- Firepower 1000
- Firepower 2100
- Secure Firewall 3100
- ISA 3000

Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。Firepower 4100/9300 EtherChannel 显示在单个物理接口旁的 设备管理器 接口页面中。您也无法在其他型号（例如 threat defense virtual）的 设备管理器 中配置 EtherChannel。

关于 EtherChannel

802.3ad EtherChannel 是逻辑接口（称为端口通道接口），该接口由一组单独的以太网链路（通道组）组成，以便可以提高单个网络的带宽。配置接口相关功能时，可以像使用物理接口一样来使用端口通道接口。

最多可以配置 48 个 Etherchannel，具体取决于型号支持的接口数量。

通道组接口

每个通道组最多可以有 8 个主用接口。

通道组中的所有接口都必须属于同一类型且具有相同速度。添加到通道组的第一个接口确定正确的类型和速度。

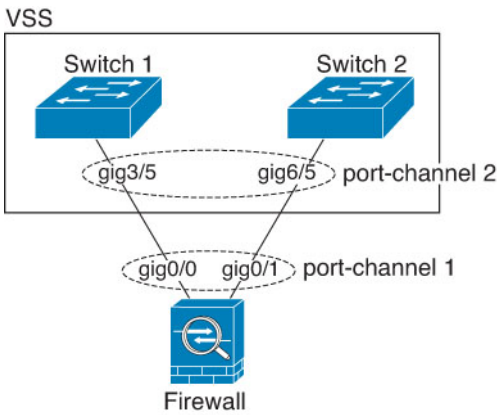
EtherChannel 汇聚通道中所有可用活动接口上的流量。系统根据源或目标 MAC 地址、IP 地址、TCP 端口号、UDP 端口号和 VLAN 编号使用专有散列算法来选择接口。

连接到其他设备上的 EtherChannel

威胁防御EtherChannel 连接到的设备还必须支持 802.3ad EtherChannel；例如，可以连接到 Catalyst 6500 交换机或 Cisco Nexus 7000。

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

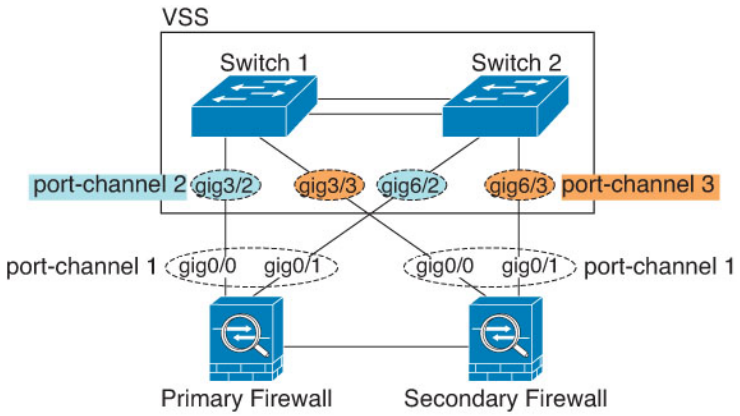
图 *12:* 连接至 ***VSS/vPC***



注释 如果 威胁防御 设备处于透明防火墙模式下，并且将 威胁防御 设备置于两组 VSS/vPC 交换机之间，请确保在使用 EtherChannel 连接到 威胁防御 设备的所有交换机端口上禁用单向链路检测 (UDLD)。如果启用 UDLD，则交换机端口可能会接收来自另一个 VSS/vPC 对中的两台交换机的 UDLD 数据包。接收交换机会将接收接口置于关闭状态，原因是“UDLD 邻居不匹配”。

如果您在主用/备用故障转移部署中使用 威胁防御 设备，则需要在 VSS/vPC 中的交换机上创建单独的 EtherChannel，为每个 威胁防御 设备创建一个。在每个 威胁防御 设备上，单个 EtherChannel 连接至两台交换机。即使您可以将所有的交换机接口分组到连接两个 威胁防御 设备的一个EtherChannel 中（在这种情况下，将不会建立 EtherChannel，因为 威胁防御 系统 ID 是单独的），但单个 EtherChannel 并不可取，因为您不希望将流量发送到备用 威胁防御 设备。

图 *13:* 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) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

您可以将 EtherChannel 中的每个物理接口配置为：

- Active - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- 开启 - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

负载均衡

威胁防御 设备通过对数据包的源 IP 地址和目标 IP 地址进行散列处理来将数据包分发给 EtherChannel 中的接口（此条件可配置）。在模数运算中，将得到的散列值除以主用链路数，得到的余数确定哪个接口拥有流量。*hash_value* **mod** *active_links* 结果为 0 的所有数据包都发往 EtherChannel 中的第一个接口，结果为 1 的发往第二个接口，结果为 2 的数据包发往第三个接口，依此类推。例如，如果您有 15 个主用链路，则模数运算的值为 0 到 14。如果有 6 个主用链路，则值为 0 到 5，依此类推。

如果主用接口发生故障且未由备用接口替代，则流量会在剩余的链路之间重新均衡。该故障会在第 2 层的生成树和第 3 层的路由表中被屏蔽，因此故障转移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都共享同一 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。

Firepower 和 Cisco Secure Firewall 硬件

端口通道接口使用内部接口 Internal-Data 0/1 的 MAC 地址。或者，您可以为端口通道接口手动配置 MAC 地址。机箱上的所有 EtherChannel 接口都使用相同的 MAC 地址，因此请注意，例如，如果使用 SNMP 轮询，则多个接口将具有相同的 MAC 地址。

注释 成员接口仅在重新启动后使用内部数据 0/1 MAC 地址。在重新启动之前，成员接口使用自己的 MAC 地址。如果在重新启动后添加新的成员接口，则必须再次重新启动以更新其 MAC 地址。

EtherChannel 的准则

桥接组

设备管理器-定义的 EtherChannel 接口作为桥接组成员。 Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。

高可用性

- 如果要将 EtherChannel 接口用作 高可用性 链路，则必须在 高可用性 对中的两台设备上预配置要使用的接口；不能在主设备上配置该接口并期望它会复制到辅助设备，因为复制需要 高可用性链路本身。
- 如果要将 EtherChannel 接口用于状态链路，则无需特殊配置；可以照常从主设备复制配置。Firepower 4100/9300 机箱 的所有接口（包括 EtherChannel）均需在两台设备上进行预配置。
- 可以使用 **monitor-interface** 命令监控 EtherChannel 余接口 以实现高可用性。如果主用成员接口故障转移到备用接口，则此活动不会在监控设备级高可用性时导致 EtherChannel 接口出现故障。仅在所有物理接口都出现故障的情况下，EtherChannel 接口或 EtherChannel 接口才会出现故障。
- 如果将 EtherChannel 接口用于高可用性或状态链路，然后防止无序数据包，则仅会使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。您不能在 EtherChannel 配置用作高可用性链路时对其进行修改。要修改配置，您需要暂时禁用高可用性，以防止在此期间发生高可用性。

型号支持

- 您可以将 设备管理器 中的 EtherChannel 添加到以下型号：
  - Firepower 1000
  - Firepower 2100
  - Cisco Secure Firewall 3100
  - ISA 3000

Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。Firepower 4100/9300 EtherChannel 显示在单个物理接口旁的 设备管理器 接口页面中。您也无法在其他型号（例如 ASA 5500-X 系列）的 设备管理器 中配置 EtherChannel。

- 无法在 Etherchannel 中使用 Firepower 1010 交换机端口或 VLAN 接口。

《通用 **EtherChannel** 准则》

- 最多可以配置 48 个 Etherchannel，具体取决于型号可用的接口数量。
- 每个通道组最多可以有 8 个主用接口。
- 通道组中的所有接口都必须具有相同的介质类型和速度能力。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在较大容量的接口上将速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口），但 Cisco Secure Firewall 3100除外，它支持不同的接口容量，只要速度设置为检测 SFP；在此情况下会使用较低的常见速度。
- 威胁防御EtherChannel 连接到的设备还必须支持 802.3ad EtherChannel。
- 威胁防御 设备不支持带有 VLAN 标记的 LACPDU。如果使用 Cisco IOS **vlan dot1Q tag native** 命令在相邻交换机上启用本地 VLAN 标记，则 威胁防御 设备将会丢弃已标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。
- 除 Firepower 4100/9300 以外的型号将 LACP 速率设置为正常（慢），并且不可配置，这意味着设备将始终从连接的交换机请求慢速速率。设备将使用连接交换机请求的速率（慢速或快速），因此我们建议将交换机上的速率设置为慢速，以便双方以相同的速率发送 LACP 消息。对于在 FXOS 中配置 EtherChannel 的 Firepower 4100/9300，LACP 速率默认设置为快速，但您可以将其配置为慢速。我们建议您将交换机配置为与您在 FXOS 中设置的值相匹配。
- 在低于 15.1(1)S2 的 Cisco IOS 软件版本中， 威胁防御 不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆叠连接 威胁防御 EtherChannel，则当主要交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为足够大的值，以将重载时间计算在内；例如，可将其设置为 8 分钟，或设置为 0 以表示无穷大。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。
- 所有 威胁防御 配置均引用 EtherChannel 接口，而不是成员物理接口。

添加 EtherChannel

添加 EtherChannel 并为其分配成员接口。

注释 您可以将 设备管理器 中的 EtherChannel 添加到以下型号：

- Firepower 1000
- Firepower 2100
- Secure Firewall 3100
- ISA 3000

Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。Firepower 4100/9300 EtherChannel 显示在单个物理接口旁的 设备管理器 接口页面中。您也无法在其他型号（例如 ASA 5500-X 系列）的 设备管理器 中配置 EtherChannel。

开始之前

- 通道组中的所有接口都必须具有相同的介质类型和速度能力。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在较大容量的接口上将速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口），但 Cisco Secure Firewall 3100除外，它支持不同的接口容量，只要速度设置为检测 SFP；在此情况下会使用较低的常见速度。
- 无法命名成员接口。

注意 如果使用的是配置中已有的接口，则删除名称将会清除引用该接口的任何配置。

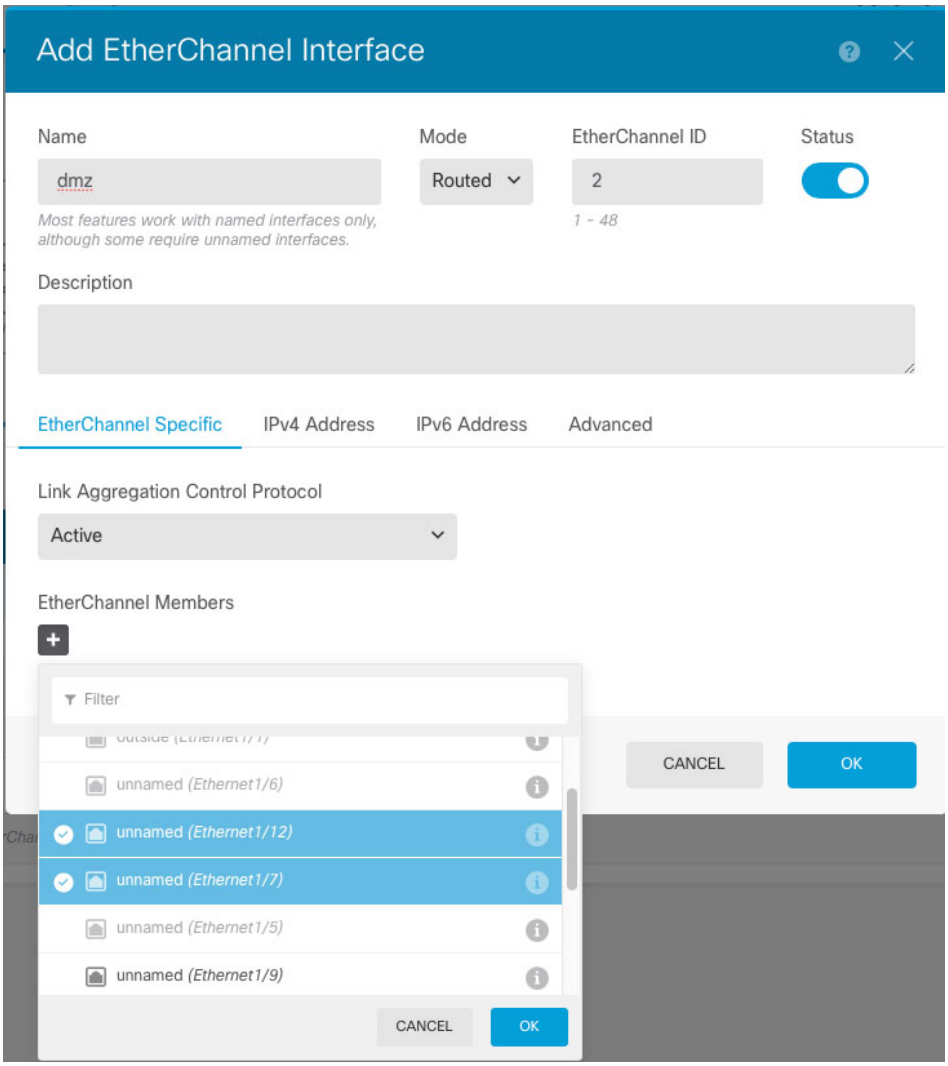
过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接，再点击 **EtherChannel**。

Etherchannel 列表显示现有 Etherchannel、其名称、地址和状态。点击开/关箭头可查看各 EtherChannel 的成员接口。成员接口也会单独显示于**接口 (Interfaces)** 页面上。

步骤 2 点击**创建 EtherChannel**（如果无当前 EtherChannel）或加号图标 ( )，然后点击 **EtherChannel** 新建 EtherChannel。

步骤 3 进行以下配置：



a) 设置**接口名称**。

设置 EtherChannel 名称，最多 48 个字符。字母字符必须为小写。例如 **inside** 或 **outside**。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

b) 设置**模式**。

- **路由** - 路由模式接口需要对流量执行所有防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组、TCP 规范化以及防火墙策略。如果您希望流量通过接口，请使用此模式。这是正常接口模式。
- **内联 (Inline)** - 将接口添加到内联集后，模式将更改为内联。不能直接选择内联作为模式。编辑将用于内联集中的接口时，请选择**路由 (Routed)** 模式作为初始模式，并且不要配置任何类型的 IP 寻址。

- **被动** - 被动接口使用交换机 SPAN 或镜像端口监控网络中流经的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。如果在被动部署中配置系统，系统将不能执行某些操作，例如，阻止流量或流量整形。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。如果您选择此模式，无需执行此过程的其余部分。请参阅将物理接口配置为被动模式，第 267 页。

c) 设置 **EtherChannel ID**（1~48 之间）（1~8 用于 Firepower 1010）。

d) 将**状态**滑块设置为已启用设置 ()。

e) （可选） 设置**说明**。

一行说明最多可包含 200 个字符（不包括回车符）。

f) 选择 **EtherChannel 模式**。

- **主用** -（推荐）发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- **开启** - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

g) 添加 **EtherChannel 成员**。

最多可向 EtherChannel 添加 8 个（未命名）接口。

- 添加接口 - 点击加号图标 ()，点击一个或多个接口，然后点击**确定**。
- 移除接口 - 将鼠标悬停于接口上方，然后点击右侧的 **x**。

步骤 4 点击 **IPv4 地址**选项卡，并配置 IPv4 地址。

从**类型**字段中选择以下任一选项：

- **DHCP** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
  - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
  - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。
- **静态** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，键入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保该地址尚未在网络中使用。

  如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

注释　如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅配置 DHCP 服务器，第 736 页。

- **PPPoE** - 如果应使用基于以太网的点对点协议 (PPPoE) 获取地址，请选择此选项。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。如果您配置高可用性，将不能使用此选项。设置以下值：
  - **组名称** - 指定您选择用于表示此连接的组名称。
  - **PPPoE 用户名** - 指定 ISP 提供的用户名。
  - **PPPoE 密码** - 指定 ISP 提供的密码。
  - **PPP 身份验证** - 选择 **PAP**、**CHAP** 或 **MSCHAP**。

    PAP 在身份验证过程中传递明文用户名和密码，这样并不安全。使用 CHAP 时，客户端可返回加密的 [challenge plus password] 和明文用户名来响应服务器质询。CHAP 比 PAP 更安全，但其不会加密数据。MSCHAP 与 CHAP 类似但更安全，因为服务器只对加密密码进行存储和比较，而不是像 CHAP 一样存储和比较明文密码。MSCHAP 还可生成密钥，以便 MPPE 进行数据加密。
  - **PPPoE 获知的路由指标** - 向获悉的路由分配管理距离。有效值为从 1 到 255。默认情况下，获悉的路由的默认管理距离为 1。
  - **从 PPPoE 获取默认路由** - 选中此复选框可支持从 PPPoE 服务器获取默认路由。
  - **IP 地址类型** - 选择**动态**可从 PPPoE 服务器获取 IP 地址。如果从 ISP 分配了静态 IP 地址，也可以选择**静态**。

步骤 5　（可选。）点击 **IPv6 地址**选项卡，并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请选择**已启用**。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

  注释　禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置** - 选择此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

  虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但 威胁防御 设备在这种情况下确实会发送路由器通告消息。选择**抑制 RA** 可抑制消息，遵从 RFC 要求。

- **静态地址/前缀** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅IPv6 寻址，第 228 页。

  如果仅使用本地链路地址，请选择**本地链路**选项。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。请注意，我们建议根据修改的EUI-64格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用IPv6地址。此接口在备用设备上使用备用地址。如果未设置备用IP地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **抑制 RA** - 是否抑制路由器通告。威胁防御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。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

  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。

  对于不希望 威胁防御 设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 6 通过点击 **高级**并设置速度来设置成员接口的速度。

您还可以配置其他高级选项。请参阅配置高级选项，第 272 页。

步骤 7 点击**确定 (OK)**。

下一步做什么

- 将 Etherchannel 添加至相应的安全区。请参阅配置安全区，第 133 页。

配置 VLAN 接口和交换机端口 (Firepower 1010)

可以将各 Firepower 1010 接口配置为作为常规防火墙接口或第 2 层硬件交换机端口运行。本节包括用于启动交换机端口配置的任务，包括启用或禁用交换模式以及创建 VLAN 接口和将交换机端口分配给 VLAN。本节还介绍如何在受支持接口上自定义以太网供电 (PoE)。

了解 Firepower 1010 端口和接口

端口和接口

对于各物理 Firepower 1010 接口，可以将其操作设置为防火墙接口或交换机端口。请参阅以下有关物理接口和端口类型的信息，以及为其分配交换机端口的逻辑 VLAN 接口：

- 物理防火墙接口 - 在路由模式下，这些接口使用已配置的安全策略在第 3 层网络之间转发流量，以应用防火墙和 VPN 服务。在路由模式下，还可以将集成路由和桥接与某些接口一起用作桥接组成员，将其他接口用作第 3 层接口。默认情况下，以太网 1/1 接口配置为防火墙接口。 还可以将这些接口配置为仅限 IPS（被动接口）。

- 物理交换机端口 - 交换机端口使用硬件中的交换功能在第 2 层转发流量。同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受 威胁防御安全策略的限制。接入端口仅接受未标记流量，可以将其分配给单个 VLAN。中继端口接受未标记和已标记流量，且可以属于多个 VLAN。默认情况下，以太网 1/2 至 1/8 配置为 VLAN 1 上的接入交换机端口。不能将 管理接口配置为交换机端口。
- 逻辑 VLAN 接口 - 这些接口的运行方式与物理防火墙接口相同，但不同的是，无法创建子接口仅 IPS 接口（内联集和被动接口）或 EtherChannel 接口。如果交换机端口需要与另一个网络进行通信，则 威胁防御 设备将安全策略应用至 VLAN 接口，并路由至另一个逻辑 VLAN 接口或防火墙接口。甚至可以将集成路由和桥接与 VLAN 接口一起用作桥接组成员。同一 VLAN 上的交换机端口之间的流量不受安全策略 威胁防御的限制，但桥接组中 VLAN 之间的流量会受到安全策略的限制，因此，可以选择将桥接组和交换机端口进行分层，以在某些分段之间实施安全策略。

以太网供电

以太网 1/7 和以太网 1/8 支持以太网供电+ (PoE+)。

注释 Firepower 1010E 上不支持 PoE。

Firepower 1010 交换机端口准则和限制

高可用性

- 使用高可用性时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此会继续在主用设备 和备用设备上传输流量。高可用性旨在防止流量通过备用设备，但此功能不会扩展至交换机端口。在正常 高可用性网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN 接口可通过故障转移监控，而交换机端口无法通过故障转移监控。理论上，您可以将单个交换机端口置于 VLAN 上并成功使用 高可用性，但更简单的设置是改用物理防火墙接口。
- 仅可使用防火墙接口作为故障转移链路。

逻辑 VLAN 接口

- 您可以创建多达 60 个 VLAN 接口。
- 如果还在防火墙接口上使用 VLAN 子接口，则无法使用与逻辑 VLAN 接口相同的 VLAN ID。
- MAC 地址：
  - - 所有 VLAN 接口共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一 MAC 地址，可手动分配 MAC 地址。请参阅配置高级选项，第 272 页。

网桥组

您不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个网桥组中。

VLAN 接口和交换机端口不支持的功能

VLAN 接口和交换机端口不支持：

- 动态路由
- 组播路由
- 等价多路径路由 (ECMP)
- 被动接口
- EtherChannel
- 故障转移和状态链路

其他准则和限制

- 您最多可以在 Firepower 1010 上配置 60 个命名接口。
- 不能将 管理接口配置为交换机端口。

默认设置

- 以太网 1/1 是一个防火墙接口。
- 以太网 1/2 至以太网 1/8 是分配给 VLAN 1 的交换机端口。
- 默认速度和复用 - 默认情况下，速度和复用设置为自动协商。

配置 VLAN 接口

本节介绍如何配置 VLAN 接口以用于关联交换机端口。您必须先为要分配至交换机端口的各 VLAN 配置 VLAN 接口。

注释 如果只希望在特定 VLAN 上的交换机端口之间启用切换，且不希望在 VLAN 和其他 VLAN 或防火墙接口之间进行路由，则将 VLAN 接口名称留空。在这种情况下，您无需配置 IP 地址；任何 IP 配置都将被忽略。

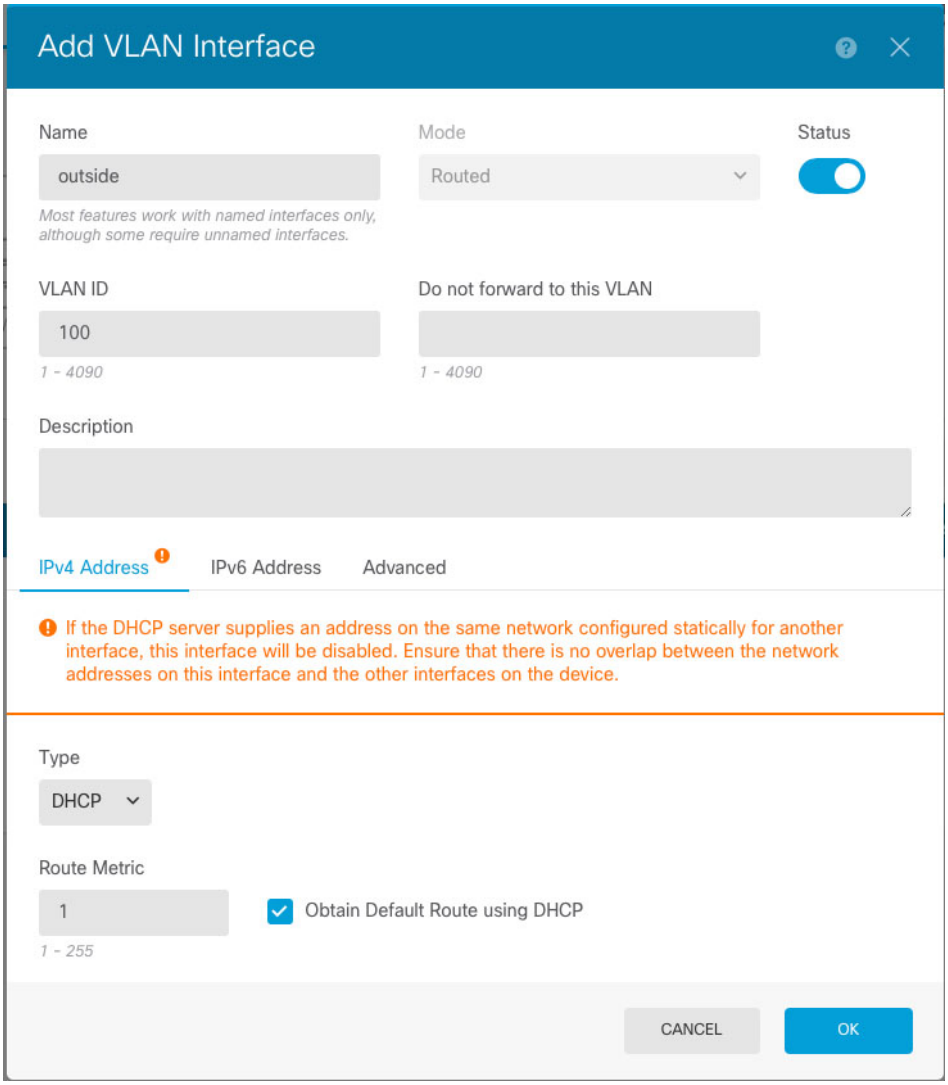
过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接，再点击 **VLAN**。

VLAN 列表显示现有 VLAN 接口。点击打开/关闭箭头，查看与各 VLAN 关联的交换机端口。交换机端口也会单独出现在**接口 (Interfaces)** 页面上。

步骤 2 点击**创建 VLAN 接口**（如果无当前 VLAN）或加号图标 (+) 以创建新的 VLAN 接口。

步骤 3 进行以下配置：



a) 设置**接口名称**。

设置 VLAN 名称，最多 48 个字符。字母字符必须为小写。例如 **inside** 或 **outside**。

如果不希望在 VLAN 和其他 VLAN 或防火墙接口之间进行路由，则将 VLAN 接口名称留空。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

b) 将**模式**保持为**路由**。

如果稍后将此 VLAN 接口添加至网桥组，则模式将自动更改为 **BridgeGroupMember**。无法在网桥组成员接口上配置 IP 地址。

c) 将**状态**滑块设置为已启用设置 ( )。

d) 设置介于 1 和 4070 之间的 **VLAN ID** 。

保存接口后，无法更改 VLAN ID；VLAN ID 既是使用的 VLAN 标记，也是您的配置中的接口 ID。

e) （可选） 在**不转发至此 VLAN** 字段中，输入此 VLAN 接口无法向其发起流量的 VLAN ID。

例如，您有一个 VLAN 分配给外部以供互联网访问，另一个 VLAN 分配给内部企业网络，第三个 VLAN 分配给您的家庭网络。家庭网络无需访问企业网络，因此，您可以使用此接口上的阻止流量来选择家庭 VLAN；企业网络可以访问家庭网络，但家庭网络不能访问企业网络。

f) （可选） 设置**说明**。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 4 点击 **IPv4 地址**选项卡，并配置 IPv4 地址。

从**类型**字段中选择以下任一选项：

- **DHCP** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
  - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
  - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。
- **静态** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，键入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保该地址尚未在网络中使用。

  如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

  注释 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅配置 DHCP 服务器，第 736 页。
- **PPPoE** - 如果应使用基于以太网的点对点协议 (PPPoE) 获取地址，请选择此选项。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。如果您配置高可用性，将不能使用此选项。设置以下值：
  - **组名称** - 指定您选择用于表示此连接的组名称。
  - **PPPoE 用户名** - 指定 ISP 提供的用户名。
  - **PPPoE 密码** - 指定 ISP 提供的密码。

- **PPP 身份验证** - 选择 **PAP**、**CHAP** 或 **MSCHAP**。

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

- **PPPoE 获知的路由指标** - 向获悉的路由分配管理距离。有效值为从 1 到 255。默认情况下，获悉的路由的默认管理距离为 1。
- **从 PPPoE 获取默认路由** - 选中此复选框可支持从 PPPoE 服务器获取默认路由。
- **IP 地址类型** - 选择**动态**可从 PPPoE 服务器获取 IP 地址。如果从 ISP 分配了静态 IP 地址，也可以选择**静态**。

步骤 5 （可选。）点击 **IPv6 地址**选项卡，并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请选择**已启用**。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

  注释 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置** - 选择此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

  虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但 威胁防御 设备在这种情况下确实会发送路由器通告消息。选择**抑制 RA** 可抑制消息，遵从 RFC 要求。

- **静态地址/前缀** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 IPv6 寻址，第 228 页。

  如果仅使用本地链路地址，请选择**本地链路**选项。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

  注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **抑制 RA** - 是否抑制路由器通告。威胁防御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。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

  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。

对于不希望 威胁防御 设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 6 （可选。）配置高级选项，第 272 页。

高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 7 点击**确定 (OK)**。

下一步做什么

- 将 VLAN 添加至相应的安全区。请参阅配置安全区，第 133 页。

将交换机端口配置为接入端口

要将交换机端口分配给单个 VLAN，请将其配置为接入端口。默认情况下，以太网 1/2 至以太网 1/8 交换机端口已启用并分配给 VLAN 1。

注释 Firepower 1010 不支持在网络中进行环路检测的生成树协议。因此，您必须确保与 威胁防御 设备的任何连接均不会在网络环路中结束。

开始之前

将 VLAN 接口添加用于要为其分配接入端口的 VLAN ID。接入端口仅接受未标记流量。请参阅配置 VLAN 接口，第 251 页。

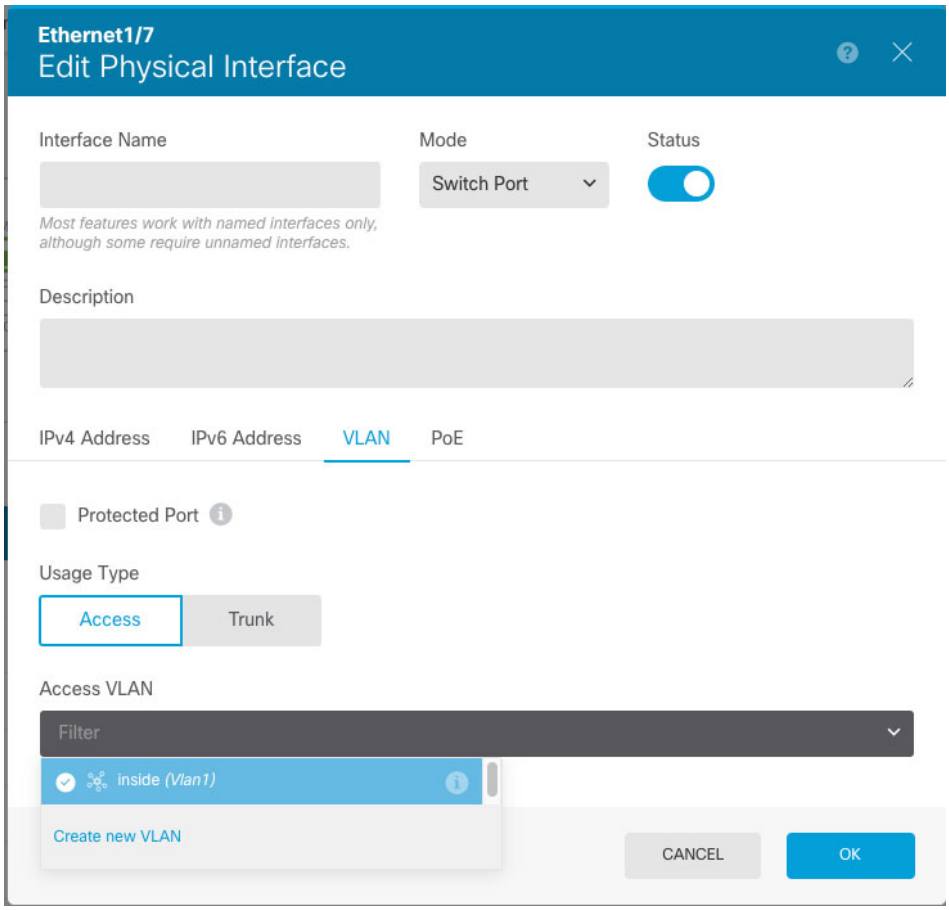
过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接。

系统默认选择**接口 (Interfaces)** 页面。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 点击要编辑的物理接口的编辑图标 ( )。

步骤 3 进行以下设置：



a) 请勿设置交换机端口的**接口名称**；仅关联 VLAN 接口是命名接口。
b) 将**模式**设置为**交换机端口**。
c) 将**状态**滑块设置为已启用设置 ( )。
d) （可选） 设置**说明**。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 4 点击 **VLAN** 设置以下内容：

a) （可选） 选中**受保护端口**复选框以将此交换机端口设置为受保护端口， 因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；由于病毒感染或其他安全漏洞，您想要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，则在您将此选项应用于各交换机端口后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

b) 对于**使用类型**，请点击**接入**。
c) 对于**接入 VLAN**，点击向下箭头以选择现有 VLAN 接口之一。

您可以通过点击**新建 VLAN** 添加新的 VLAN 接口。请参阅配置 VLAN 接口 ， 第 251 页。

步骤 5 点击**确定 (OK)**。

将交换机端口配置为中继端口

此程序介绍如何创建可以使用 802.1 Q 标记传输多个 VLAN 的中继端口。中继端口接受未标记和标记流量。允许的 VLAN 上的流量通过中继端口保持不变。

中继端口接收未标记流量后将其标记为本地 VLAN ID，以便 ASA 可以将流量转发至正确交换机端口，或可以将流量路由至另一个防火墙接口。如果 ASA 从中继端口发送本地 VLAN ID 流量，则会删除 VLAN 标记。请务必在另一台交换机上的中继端口上设置相同的本地 VLAN，以便将未标记流量标记至同一 VLAN。

开始之前

将 VLAN 接口添加用于要为其分配中继端口的各 VLAN ID。请参阅配置 VLAN 接口，第 251 页。

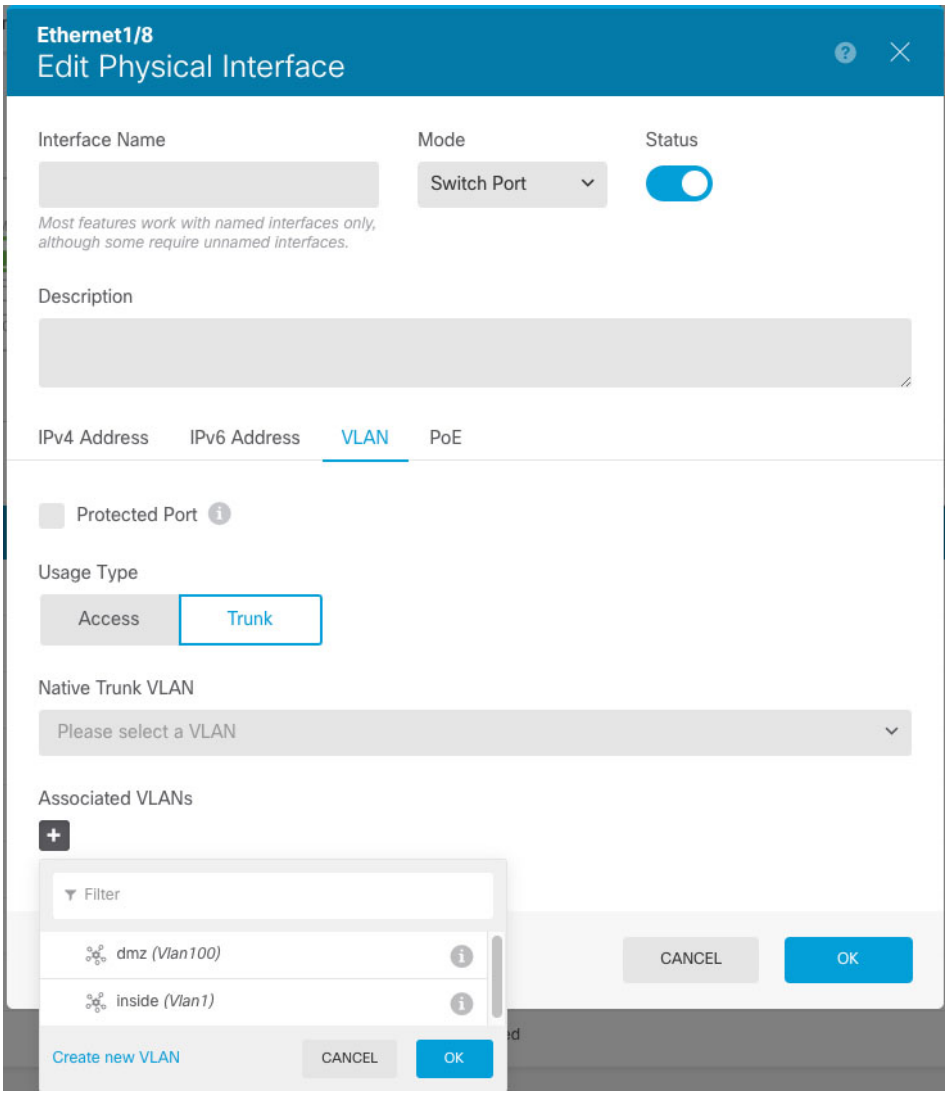
过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接。

系统默认选择**接口 (Interfaces)** 页面。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 点击要编辑的物理接口的编辑图标 ( )。

步骤 3 进行以下设置：



a) 请勿设置交换机端口的**接口名称**；仅关联 VLAN 接口是命名接口。

b) 将**模式**设置为**交换机端口**。

c) 将**状态**滑块设置为已启用设置 ( )。

d) （可选） 设置**说明**。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 4 点击 **VLAN** 设置以下内容：

a) （可选） 选中**受保护端口**复选框以将此交换机端口设置为受保护端口， 因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；由于病毒感染或其他安全漏洞，您想要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，则在您将此选项应用于各交换机

端口后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

b) 对于**使用类型**，请点击**中继**。

c) （可选）对于**本地中继 VLAN**，点击向下箭头以选择本地 VLAN 的现有 VLAN 接口之一。

默认的本地 VLAN ID 为 1。

每个端口只能有一个本地 VLAN，但各端口的本地 VLAN 可以相同也可以不同。

您可以通过点击**新建 VLAN** 添加新的 VLAN 接口。请参阅配置 VLAN 接口，第 251 页。

d) 对于**关联 VLAN**，点击加号图标 (+) 以选择一个或多个现有 VLAN 接口。

如果在此字段中包含本地 VLAN，则将忽略该本地 VLAN；从端口发送本地 VLAN 流量时，中继端口始终会删除 VLAN 标记。此外，不会接收仍具有 VLAN 标记的流量。

您可以通过点击**新建 VLAN** 添加新的 VLAN 接口。请参阅配置 VLAN 接口，第 251 页。

步骤 5 点击**确定 (OK)**。

配置以太网供电

以太网 1/7 和以太网 1/8 支持 IP 电话或无线接入点等设备的以太网供电 (PoE)。Firepower 1010 支持 IEEE 802.3af (PoE) 和 802.3at (PoE+)。PoE+ 使用链路层发现协议 (LLDP) 来协商功率级别。PoE+ 可以为受电设备提供 30 瓦的功率。仅在需要时提供功率。

如果关闭接口，则会禁用设备电源。

默认情况下，在以太网 1/7 和以太网 1/8 上启用 PoE。此过程介绍如何禁用和启用 PoE 以及如何设置可选参数。

注释 Firepower 1010E 上不支持 PoE。

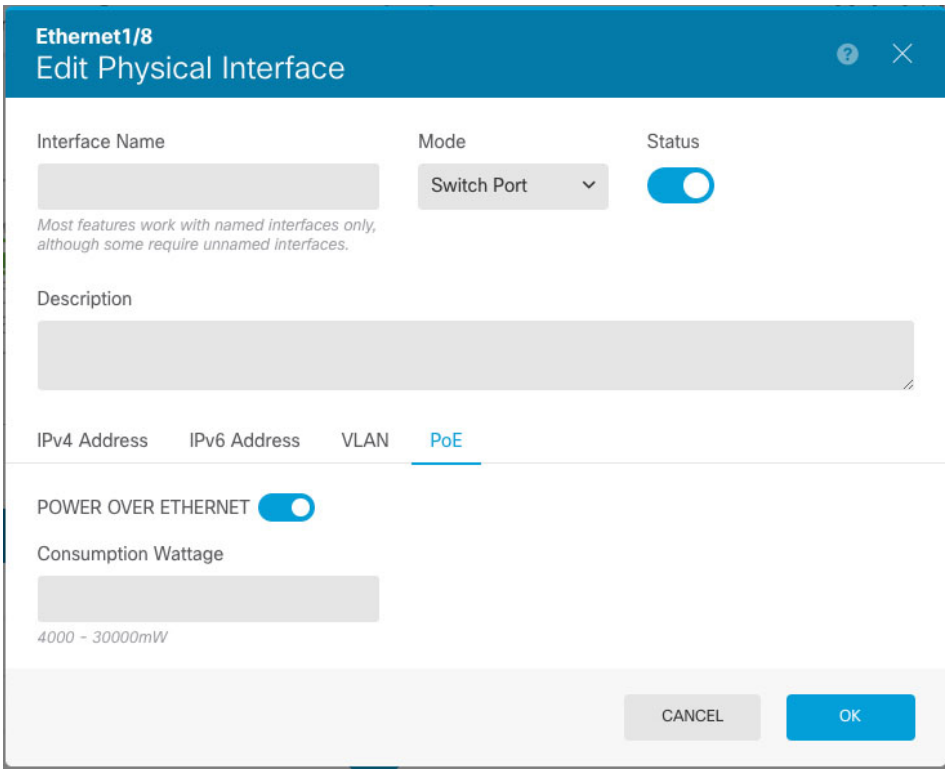
过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接。

系统默认选择**接口 (Interfaces)** 页面。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 点击以太网 1/7 或 1/8 的编辑图标 ()。

步骤 3 点击 **PoE**，并设置以下内容：



a) 要启用**以太网供电**，请点击滑块 ( ) 以便使其处于启用状态。

默认情况下，PoE 处于启用状态。

b) （可选） 如果您知道所需的确切功率，请输入**功耗瓦数**。

默认情况下，PoE 使用适合受电设备类别的瓦数将电源自动传送至受电设备。Firepower 1010 使用 LLDP 进一步协商正确的瓦数。如果知道特定瓦数并想要禁用 LLDP 协商，请输入介于 4000 和 30000 毫瓦的值。

步骤 4 点击**确定 (OK)**。

配置 VLAN 子接口和 802.1Q 中继

通过 VLAN 子接口，可将一个物理接口划分成多个标记有不同 VLAN ID 的逻辑接口。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 允许您在特定物理接口上将流量分开，所以您可以增加网络中可用的接口数量，而无需增加物理接口或设备。

如果您将物理接口连接到交换机的中继端口，请创建子接口。为交换机中继端口上显示的每个VLAN创建子接口。如果您将物理接口连接到交换机的接入端口，创建子接口将没有意义。

准则和限制

- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常表明也不希望物理接口传递流量，因为物理接口会传递未标记的数据包。由于必须启用物理接口，才能允许子接口传递流量，所以请确保物理接口不会通过未命名接口传递流量。如果要允许物理接口传递未标记数据包，可以照常命名接口。
- Firepower 1010 - 交换机端口或 VLAN 接口上不支持子接口。
- 您不能在网桥组成员接口上配置 IP 地址，但是可以根据需要修改高级设置。
- 同一父接口上的所有子接口必须为网桥组成员或路由接口；您无法混合搭配。
- 威胁防御 不支持动态中继协议 (DTP)，因此您必须无条件地将连接的交换机端口配置到中继上。
- 您可能想要为 威胁防御 设备上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 威胁防御 上特定实例内发生流量中断。

过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接。

系统默认选择**接口 (Interfaces)** 页面。要将子接口添加至 EtherChannel，请点击 **EtherChannel**。接口列表显示可用物理接口、物理接口名称、地址和状态。

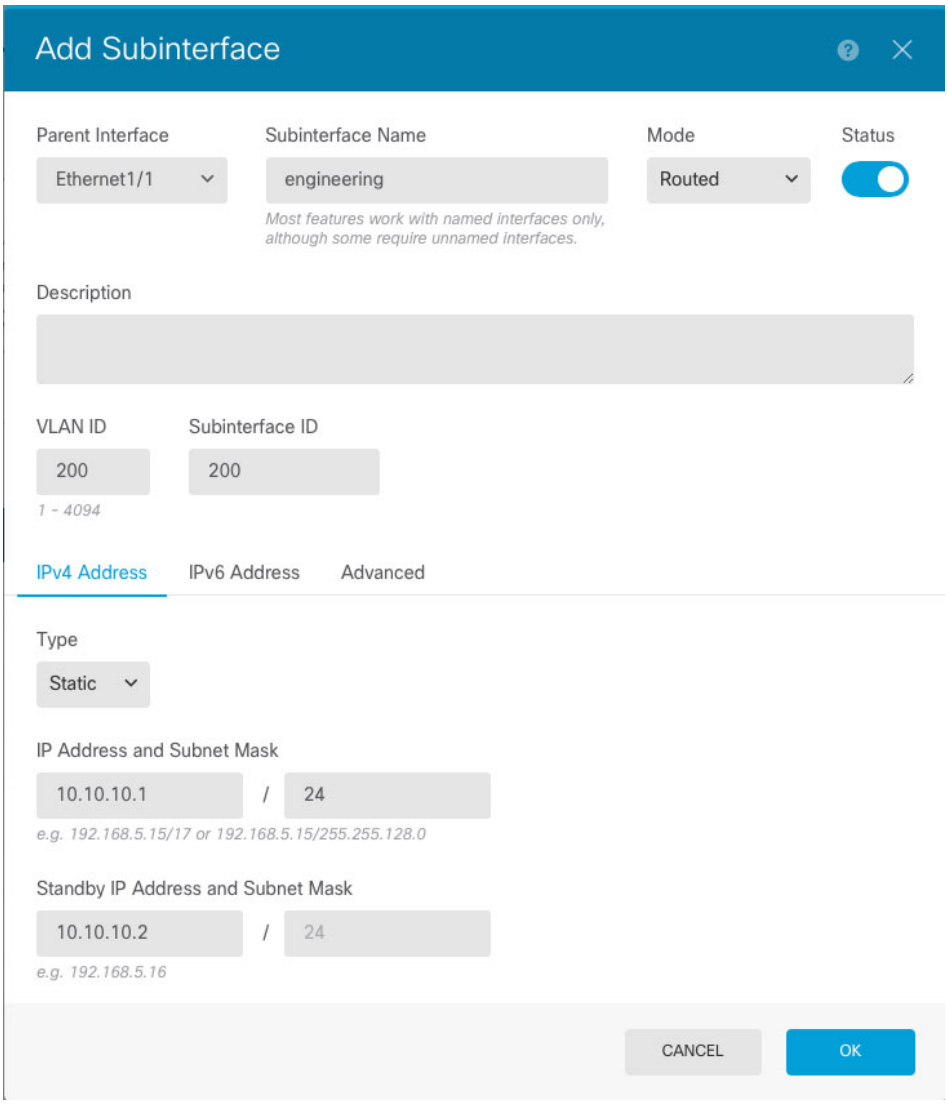
步骤 2 执行以下操作之一：

- 在**接口 (Interfaces)** 页面上，点击加号图标 () 以创建新的子接口。
- 在 **EtherChannel** 页面上，点击加号和向下箭头图标 ()，然后选择**子接口 (Subinterface)**。
- 点击要编辑的子接口的编辑图标 ()。

如果不再需要某个子接口，请点击该子接口对应的删除图标 () 将其删除。

步骤 3 将**状态**滑块设置为已启用设置 ()。

步骤 4 配置父接口、名称和说明：



a) 选择**父接口**。

父接口是将子接口添加至其中的物理接口。创建子接口后，父接口则无法更改。

b) 设置**子接口名称**，最多 48 个字符。

字母字符必须为小写。例如 **inside** 或 **outside**。如果没有名称，将忽略其余的接口配置。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

c) 将**模式**设置为**路由**。

如果稍后将此接口添加到网桥组，则该模式将自动更改为 **BridgeGroupMember**。请注意，无法在网桥组成员接口上配置 IP 地址。

d) （可选） 设置**说明**。

一行说明最多可包含 200 个字符（不包括回车符）。

e) 设置 **VLAN ID**。

输入 VLAN ID，介于 1 和 4094 之间，用于标记该子接口上的数据包。

f) 设置**子接口 ID**。

以整数形式输入介于 1 和 4294967295 之间的子接口 ID。此 ID 附加至接口 ID；例如 Ethernet1/1.100。方便起见，您可以匹配 VLAN ID，但这不是必需的。创建子接口后，则无法更改该 ID。

步骤 5 点击 **IPv4 地址**选项卡，并配置 IPv4 地址。

从**类型**字段中选择以下任一选项：

- **DHCP** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
  - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
  - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。
- **静态** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，键入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保该地址尚未在网络中使用。

  如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

  注释 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅配置 DHCP 服务器，第 736 页。
- **PPPoE** - 如果应使用基于以太网的点对点协议 (PPPoE) 获取地址，请选择此选项。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。如果您配置高可用性，将不能使用此选项。设置以下值：
  - **组名称** - 指定您选择用于表示此连接的组名称。
  - **PPPoE 用户名** - 指定 ISP 提供的用户名。
  - **PPPoE 密码** - 指定 ISP 提供的密码。
  - **PPP 身份验证** - 选择 **PAP**、**CHAP** 或 **MSCHAP**。

    PAP 在身份验证过程中传递明文用户名和密码，这样并不安全。使用 CHAP 时，客户端可返回加密的 [challenge plus password] 和明文用户名来响应服务器质询。CHAP 比 PAP 更安全，但其不会加密数据。MSCHAP 与 CHAP 类似但更安全，因为服务器只对加密密码进行

存储和比较，而不是像 CHAP 一样存储和比较明文密码。MSCHAP 还可生成密钥，以便 MPPE 进行数据加密。

- **PPPoE 获知的路由指标** - 向获悉的路由分配管理距离。有效值为从 1 到 255。默认情况下，获悉的路由的默认管理距离为 1。
- **从 PPPoE 获取默认路由** - 选中此复选框可支持从 PPPoE 服务器获取默认路由。
- **IP 地址类型** - 选择**动态**可从 PPPoE 服务器获取 IP 地址。如果从 ISP 分配了静态 IP 地址，也可以选择**静态**。

步骤 6 （可选。）点击 **IPv6 地址**选项卡，并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请选择**已启用**。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

  注释 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置** - 选择此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

  虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但 威胁防御 设备在这种情况下确实会发送路由器通告消息。选择**抑制 RA** 可抑制消息，遵从 RFC 要求。

- **静态地址/前缀** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 IPv6 寻址，第 228 页。

  如果仅使用本地链路地址，请选择**本地链路**选项。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

  注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。请注意，我们建议根据修改的EUI-64格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6地址。此接口在备用设备上使用备用地址。如果未设置备用IP地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **抑制 RA** - 是否抑制路由器通告。威胁防御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。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

  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。

  对于不希望 威胁防御 设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 7 （可选。）配置高级选项，第 272 页。

高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 8 点击**确定 (OK)**。

下一步做什么

- 将子接口添加至相应的安全区。请参阅配置安全区，第 133 页。
- 向您的动态 DNS 服务提供商注册一个完全限定域名 (FQDN)，并配置 DDNS 以更新 DNS 服务器上的接口地址（IPv4 和 IPv6）。请参阅配置动态 DNS，第 739 页。

配置被动接口

被动接口使用交换机 SPAN（交换端口分析器）或镜像端口监控在网络中传输的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。

如果系统是在被动部署中配置的，则无法执行某些操作，例如阻止流量。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。

使用被动接口监控网络上的流量，以收集流量相关的信息。例如，您可以应用入侵策略来识别攻击网络的威胁类型，或了解用户正在发出的 Web 请求的 URL 类别。您可以实施各种安全策略和规则，了解系统在主动部署的情况下会执行哪些操作，以便可以根据访问控制和其他规则丢弃流量。

但是，由于被动接口无法影响流量，因此存在很多配置限制。这些接口只是让系统知悉有流量通过：进入被动接口的数据包不会从设备流出。

以下主题更加详细地介绍了被动接口及其配置方法。

为什么使用被动接口？

被动接口的主要目的是提供一种简单的演示模式。您可以设置交换机监控单个源端口，然后使用工作站发送通过被动接口监控的测试流量。由此，可以了解 威胁防御系统如何评估连接、识别威胁等。系统性能满足要求后，可以将其主动部署在网络中，并删除被动接口配置。

不过，您也可以在生产环境中使用被动接口，以提供以下服务：

- 纯 ID 部署 - 如果您不想使用系统作为防火墙或 IPS（入侵防御系统），可以将其被动部署为 IDS（入侵检测系统）。在此部署方法中，您将使用访问控制规则将入侵策略应用于所有流量。您还必须设置系统监控交换机上的多个源端口。然后，您将可以使用控制面板监控网络上发现的威胁。但是，在此模式下，系统不会执行任何操作来阻止这些威胁。
- 混合部署 - 您可以在同一系统上搭配使用主动路由接口和被动接口。因此，在某些网络中，您可以将 威胁防御设备部署为防火墙，同时配置一个或多个被动接口监控其他网络中的流量。

被动接口的限制

定义为被动模式接口的任何物理接口具有以下限制：

- 无法为被动接口配置子接口。
- 不能将被动接口添加到网桥组。
- 不能在被动接口上配置 IPv4 或 IPv6 地址。
- 不能对被动接口选择“仅管理”选项。
- 只能将接口添加到被动模式安全区，不能将其添加到路由安全区。
- 可以将被动安全区添加到访问控制或身份规则的源条件中。不能在目标条件中使用被动区域。同时，也不能在同一规则中搭配使用被动和路由区域。
- 不能为被动接口配置管理访问规则（HTTPS 或 SSH）。
- 不能在 NAT 规则中使用被动接口。
- 不能为被动接口配置静态路由。也不能在路由协议配置中使用被动接口。
- 不能在被动接口上配置 DHCP 服务器。也不能使用被动接口通过自动配置获取 DHCP 设置。
- 不能在系统日志服务器配置中使用被动接口。
- 不能在被动接口上配置任何类型的 VPN。

为硬件 威胁防御 被动接口配置交换机

只有当网络交换机配置正确时，硬件 威胁防御设备上的被动接口才可以正常工作。以下过程基于 Cisco Nexus 5000 系列交换机。如果您有不同类型的交换机，所用的命令可能会有所不同。

其基本思路是，配置 SPAN（交换端口分析器）或镜像端口，将被动接口连接到该端口，在交换机上配置监控会话以将流量副本从一个或多个源端口发送到 SPAN 或镜像端口。

过程

步骤 1 将交换机上的端口配置为监控（SPAN 或镜像）端口。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)#
```

步骤 2 定义监控会话以识别要监控的端口。

确保您将 SPAN 或镜像端口定义为目标端口。在以下示例中，监控两个源端口。

```
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
```

```
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

步骤 3 （可选。）使用 **show monitor session** 命令验证配置。

以下示例显示会话 1 的简要输出。

```
switch# show monitor session 1 brief
   session 1
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

步骤 4 以物理方式将电缆从 威胁防御被动接口连接到交换机的目标端口。

可以在进行物理连接前后，将接口配置为被动模式。请参阅将物理接口配置为被动模式，第267页。

为 Threat Defense Virtual 被动接口配置 VLAN

只有在虚拟网络上正确配置了 VLAN 时，threat defense virtual 设备的被动接口才可以正常工作。请确保执行以下操作：

- 将 threat defense virtual 接口连接到已在混杂模式下配置的 VLAN。然后，按照将物理接口配置为被动模式，第 267 页中的说明配置接口。被动接口会看到混合 VLAN 上所有流量的副本。
- 将一个或多个终端设备（例如虚拟 Windows 系统）连接到同一 VLAN。如果 VLAN 已连接到互联网，可以使用单台设备。否则，需要至少两台设备，才可以在两者之间传递流量。要想获取 URL 类别数据，需要建立互联网连接。

将物理接口配置为被动模式

您可以将接口配置为被动模式。在被动模式下工作时，接口仅监控交换机自身（针对硬件设备）或混合 VLAN（针对 threat defense virtual）配置的监控会话中来自源端口的流量。有关需要在交换机或虚拟网络中配置哪些对象的详细信息，请参阅以下主题：

- 为硬件 威胁防御 被动接口配置交换机，第 266 页
- 为 Threat Defense Virtual 被动接口配置 VLAN，第 267 页

当您想要分析通过受监控交换机端口传入的流量，而不影响这些流量时，可使用被动模式。有关使用被动模式的端到端示例，请参阅如何被动监控网络上的流量，第 71 页。

过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接，再点击**接口**或 **EtherChannel**。

步骤 2 点击要编辑的物理接口或 EtherChannel 的编辑图标 ()。

选择当前未使用的接口。如果您要将使用中的接口转换为被动接口，需要先从任何安全区中删除该接口，并删除使用该接口的所有其他配置。

步骤 3 将**状态**滑块设置为已启用设置 ()。

步骤 4 进行以下配置：

- **接口名称** - 接口名称，最多 48 个字符。字母字符必须为小写。例如，monitor。
- **模式** - 选择**被动**。
- （可选。）**说明** - 说明最多为 200 个字符，单行，不能使用回车。

注释 无法配置 IPv4 或 IPv6 地址。在“高级”选项卡中，仅可以更改 MTU、复用和速度设置。

步骤 5 点击**确定 (OK)**。

下一步做什么

创建被动接口并不会在控制面板上填充接口上所发现流量的相关信息。您还必须执行以下操作：使用案例会介绍这些步骤。请参阅如何被动监控网络上的流量，第 71 页。

- 创建被动安全区并向其添加接口。请参阅配置安全区，第 133 页。
- 创建将被动安全区用作源区域的访问控制规则。通常，您将在这些规则中应用入侵策略以实施 IDS（入侵检测系统）监控。请参阅配置访问控制策略，第 478 页。
- 或者，为被动安全区创建 SSL 解密和身份规则，并启用安全智能策略。

配置内联集

内联集提供仅 IPS 接口。如果您有单独的防火墙来保护这些接口，并且不希望造成防火墙功能的开销，则可能需要实施仅限 IPS 的接口。

内联集类似于导线上的凹凸，用于将两个接口绑定在一起插入到现有网络中。此功能使设备可以安装在任何网络环境中，而无需配置相邻网络设备。内联接口无条件接收所有流量，但是，除非已明确丢弃，否则这些接口上接收的所有流量将在内联集外重传。

准则和限制

- 只能在以下设备型号上配置内联集：Firepower 1000 系列、Firepower 2100、Secure Firewall 3100。
- 内联集中允许的接口类型：物理、EtherChannel。
- 您不能将管理接口包含在内联集中。
- 不能更改内联集中使用的接口的属性：名称、模式、接口 ID、MTU、IP 地址。
- 如果启用分流模式，Snort Fail Open 会被禁用。
- 使用内联集时，不允许双向转发检测 (BFD) 回应数据包通过设备。如果设备的一端有两个邻居运行 BFD，则设备会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。
- 对于内联集和被动接口，设备在数据包中最多支持两个 802.1Q 报头（也称为 Q-in-Q 支持）。注意：防火墙类型的接口不支持 Q-in-Q，并且仅支持一个 802.1Q 报头。
- 内联集中的接口不支持路由、NAT、DHCP（服务器、客户端或中继）、VPN、TCP 拦截、应用检测或 Netflow。

开始之前

- 我们建议您为连接到威胁防御内联接口对且启用 STP 的交换机设置 STP PortFast。
- 配置将成为内联集成员的物理或 EtherChannel 接口。仅配置以下值：名称、双工、速度和路由模式（请勿选择被动）。请勿配置任何类型的寻址，即手动 IP 地址、DHCP 或 PPoE。

注释 将接口添加到内联集后，模式将更改为内联。不能直接选择内联作为模式。

过程

步骤 1 点击 **设备**，然后点击接口摘要中的链接，再点击 **VLAN**。

步骤 2 执行以下任一操作：

- 点击 + 创建新的内联集。
- 点击现有内联集的编辑图标 ( ) 可对其进行修改。
- 如果不再需要某个内联集，点击其删除图标 ( )。

步骤 3 配置以下选项

- 设置内联集 **名称**。
- （可选。）更改 **MTU**。

  默认 MTU 值为 1500。您可以将其设置为更高以处理更大的软件包。

步骤 4 在 **常规** 选项卡上，添加接口对。每对必须选择 2 个接口。您可以删除不需要的任何对。

将接口添加到内联集时，其模式会从“路由”(Routed) 更改为“内联”(Inline)，并且在将其从内联集中删除之前，无法编辑该接口的任何属性。

步骤 5 在 **高级** 选项卡上，设置以下可选参数：

- **模式** — **内联**模式是标准模式，您希望设备影响通过它的流量。

  在 **分流** 模式下，设备会进行内联部署，但网络流量不受干扰。相反，设备会复制每个数据包，这样它就可以对数据包进行分析。请注意，这些类型的规则在触发时会生成入侵事件，而且入侵事件表视图显示了触发数据包会在内联部署中被丢弃。在已部署内联的设备上使用分流模式有很多优点。例如，您可以设置设备和网络之间的布线，就像设备是内联，并分析设备生成的多种入侵事件。根据结果，您可以修改入侵策略，并添加最好地保护您的网络却不影响有效性的丢弃规则。准备部署设备内联时，您可以禁用分流模式，并开始丢弃可疑流量，而无需重新配置设备和网络之间的走线。请知晓，分流模式显著影响设备性能，具体取决于流量。

- **Snort 故障时自动打开** - 如果您希望在 Snort 进程繁忙或关闭时，新流量和现有流量不检查直接通过（启用）或丢弃（禁用），请启用或禁用繁忙和关闭选项之一或两项都启用。

  默认情况下，当Snort进程关闭时，流量会不进行检查就通过，而当进程繁忙时，流量会丢弃。

  当 Snort 进程处于以下状态时：

  - **繁忙**-由于流量缓冲区已满，进程无法足够快速地处理流量，这表明流量超过设备的处理能力，或者存在其他软件资源问题。
  - **关闭**-由于您部署了要求进程重启的配置，因此它会重启。

  当 Snort 进程关闭并重新启动后，它会检查新的连接。为了防止误报和漏报，此进程不检查内联、路由或透明接口上的现有连接，因为最初的会话信息可能已经在它关闭时丢失。

  注释 如果 Snort 无法打开，则依赖 Snort 进程的功能会停止运行，这些功能包括应用控制和深度检查。借助简单、易于确定的传输层和网络层特征，系统仅执行基本访问控制。

- **传播链路状态** - 配置链路状态传播。

  当内联集的一个接口断开时，链路状态传播自动关闭内联接口对的第二个接口。当被关闭的接口恢复运行时，第二个接口也将自动恢复运行。换句话说，如果一个接口的链路状态更改，设备会感知该更改并更新其他接口的链路状态以与其匹配。请注意，设备最多需要 4 秒即可传播链路状态更改。在将路由器配置为在处于故障状态的网络设备上自动重新路由流量的弹性网络环境中，链路状态传播特别有用。

步骤 6 点击**确定 (OK)**。

配置高级接口选项

高级选项包括设置 MTU、硬件设置、仅管理、MAC 地址和其他设置。

关于 MAC 地址

您可以手动配置介质访问控制 (MAC) 地址来覆盖默认地址。

对于高可用性配置，您可以同时配置接口的主用和备用 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，则新的主用设备会开始使用主用 MAC 地址，以最大限度地减少网络中断。

默认 MAC 地址

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。
- VLAN 接口 (Firepower 1010) - 所有 VLAN 接口均共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一 MAC 地址，可手动分配 MAC 地址。请参阅配置高级选项，第 272 页。
- EtherChannels - 对于 EtherChannel，属于通道组的所有接口均共享同一 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员身份不影响 MAC 地址。
- 子接口- 物理接口的所有子接口都使用同一个烧录 MAC 地址。您可能想为子接口分配唯一的 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 威胁防御 上特定实例内发生流量中断。

关于 MTU

MTU 指定 威胁防御设备 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、VLAN 标记或其他系统开销情况下的帧大小。例如，将 MTU 设置为 1500 时，预期帧大小为 1518 字节（含报头）或 1522 字节（使用 VLAN）。请勿为容纳这些报头而将 MTU 的值设得过高。

路径 MTU 发现

威胁防御设备 支持路径 MTU 发现（如 RFC 1191 中所定义），从而使两个主机之间的网络路径中的所有设备均可协调 MTU，以便它们可以标准化路径中的最低 MTU。

MTU 和分段

对于 IPv4，如果传出 IP 数据包大于指定 MTU，则该数据包将分为 2 帧或更多帧。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。对于 IPv6，通常不允许对数据包进行分段。因此，IP 数据包大小应在 MTU 大小范围内，以避免分片。

对于 UDP 或 ICMP，应用应将 MTU 考虑在内，以避免分段。

注释 只要有内存空间，威胁防御设备 就可接收大于所配置的 MTU 的帧。

MTU 和巨型帧

MTU 越大，您能发送的数据包越大。加大数据包可能有利于提高网络效率。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 威胁防御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 - 巨型帧是指大于标准最大值 1522 字节（包括第 2 层报头和 VLAN 报头）的以太网数据包，最大为 9216 字节。MTU 可设置为 9000 字节或更高，以容纳巨型帧。最大值取决于型号。

注释 加大 MTU 会为巨型帧分配更多内存，这样可能会限制其他功能（例如访问规则）的最大使用量。如果在 threat defense virtual上将 MTU 增加到默认值 1500 以上，则必须重新启动系统。如果设备已为高可用性，还须重新启动备用设备。无需重新启动其他型号，因为巨型帧支持在该型号上始终启用。

配置高级选项

高级接口选项的默认设置适用于大多数网络。只有当您解决网络问题或配置高可用性时，才需要进行配置。

以下步骤程序假定已定义接口。另外，您还可以在初始编辑或创建接口时编辑这些设置。

限制

- 对于网桥组，您可以在成员接口上配置大多数这些选项。除用于 DAD 尝试和高可用性监控之外，这些选项不适用于桥接虚拟接口 (BVI)。
- 您无法在 Firepower 1000 或 2100 设备的 MTU、复用或速度.
- 高级选项不适用于 Firepower 1010 交换机端口。
- 在 Firepower 4100/9300 上，您无法设置接口复用或速度。请使用 FXOS 为接口设置这些功能。
- 对于被动接口，您只能设置 MTU、复用以及速度。不能将接口仅用于管理。

过程

步骤 1 点击**设备**，点击**接口**摘要中的链接，然后点击接口类型以查看接口列表。

步骤 2 点击要编辑的接口的编辑图标 ()。

步骤 3 点击**高级选项 (Advanced Options)**。

步骤 4 如果您想让系统在决定是否故障转移到高可用性配置中的对等体设备时考虑接口的运行状况，请选择**对高可用性监控启用 (Enable for HA Monitoring)**。

如果不配置高可用性，可忽略此选项。如果不配置接口的名称，也可以忽略此选项。

步骤 5 要将数据接口仅用于管理，请选择**仅管理**。

仅管理接口不允许直通流量，所以将数据接口设置为仅管理的价值微乎其微。不能更改管理/诊断接口的此项设置，它们始终为仅管理。

步骤 6 要启用思科 Trustsec，请选择**传播安全组标记 (Propagate Security Group Tag)**。

您可以在物理接口、子接口、EtherChannel、VLAN、管理接口或 BVI 接口（无论是命名还是未命名）上启用或禁用 Cisco Trustsec。默认情况下，当您为接口命名时，Cisco Trustsec 会自动启用。

步骤 7 将 **MTU**（最大传输单位）更改为所需的值。

默认 MTU 为 1500 字节。最小值和最大值取决于您的平台。如果通常在网络中使用巨型帧，请设置一个较大的值。

注释 如果在 ISA 3000 系列设备， threat defense virtual上将 MTU 提高到 1500 以上。如果设备已为高可用性，还须重新启动备用设备。无需重新启动其他型号，因为巨型帧支持在该型号上始终启用。

步骤 8 （仅限物理接口）。修改速度和复用设置。

默认设置为该接口与线路另一端的接口协商最佳复用和速度，但如有必要，您可以强制实施特定的复用或速度。所列的选项仅为接口支持的设置。在网络模块上设置这些选项之前，请阅读接口配置的限制条件，第 229 页。

- **复用**-选择 **半** 或 **全**。SFP 接口仅支持 **全** 复用。
- **速度** - 具体选项取决于型号和接口类型。选择速度：**自动 (Auto)**、**无协商 (No Negotiate)** 或**检测 SFP (Detect SFP)**。 对于 Firepower 1100 和 2100 光纤端口， **无协商** 将速度设置为1000 Mbps，并禁用流量控制参数和远程故障信息的链路协商。 （仅限 Cisco Secure Firewall 3100 ）选择 **检测 SFP** 以检测已安装的 SFP 模块的速度并使用适当的速度。复用始终为全复用，并且始终启用自动协商。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。
- （仅限 Cisco Secure Firewall 3100 ） **自动协商**- 根据接口类型，设置接口以协商流量控制参数和远程故障信息的链路状态。
- **前向纠错模式**-（仅限 Cisco Secure Firewall 3100 ）对于 25 Gbps 及更高的接口，请启用前向纠错 (FEC)。对于 EtherChannel 成员接口，必须先配置前向纠错，然后才能将其添加到 EtherChannel。使用**自动 (Auto)** 时选择的设置取决于收发器类型，以及接口是固定接口（内置）还是在网络模块上。

表 *6:* 用于自动设置的默认 *FEC*

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
25G-SR	Clause 108 RS-FEC	Clause 108 RS-FEC
25G-LR	Clause 108 RS-FEC	Clause 108 RS-FEC

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
10/25G-CSR	Clause 108 RS-FEC	Clause 74 FC-FEC
25G-AOC*x*M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	自动协商	自动协商
25G-CU4/5M	自动协商	自动协商

步骤 9 修改 **IPv6 配置**设置。

- **启用 DHCP 客户端 (Enable DHCP Client)** — 使用 DHCPv6 获取地址。

  选中**使用 DHCP 获取默认路由 (Obtain default route using DHCP)**，从路由器通告中获取默认路由。

- **启用 DHCP 以获取 IPv6 地址配置** - 是否在 IPv6 路由器通告数据包中设置“托管地址配置”标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 来获取相关地址以及派生的无状态自动配置地址。
- **启用 DHCP 以获取 IPv6 非地址配置** - 是否在 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。
- **DAD 尝试** - 接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，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。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。

步骤 10 （可选，建议为子接口和高可用性设备配置。）配置 MAC 地址。

默认情况下，系统对接口使用预烧到网络接口卡 (NIC) 的 MAC 地址。因此，该接口上的所有子接口都使用相同的 MAC 地址，也因此您可能想要为每个子接口创建唯一地址。如果您配置高可用性，建议手动配置主用/备用 MAC 地址。定义 MAC 地址有助于在故障转移时保持网络中的一致性。

- **MAC 地址** - 采用 H.H.H 格式的介质访问控制，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。
- **备用 MAC 地址** - 用于高可用性。如果主用设备发生故障转移，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 11 点击**确定 (OK)**。

扫描接口更改并迁移接口

更改设备上的接口时，设备会通知 设备管理器 已发生更改。在执行接口扫描之前，您将无法部署配置。 设备管理器 支持通过其他接口迁移安全策略中的接口，因此几乎可以无缝删除接口。

关于接口扫描和迁移

扫描

更改设备上的接口时，设备会通知 设备管理器 已发生更改。执行接口扫描前，您将无法部署配置。在检测到任何已添加、已删除或已恢复接口的扫描后，您可以部署您的配置；但是，将不会部署引用已删除接口的配置部分。

需要扫描的接口更改包括添加或删除接口。例如：网络模块更改； Firepower 4100/9300 机箱上的已分配接口更改； threat defense virtual上的接口更改。

以下更改在扫描后不阻止部署：

- 安全区成员身份
- EtherChannel 接口成员身份
- Firepower 1010 VLAN 接口交换机端口成员身份
- 网桥组接口成员身份，适用于引用 BVI 的策略

注释 虽然您应手动或使用接口替换功能来修复系统日志服务器配置，但系统日志服务器出口接口更改不会阻止部署。

正在迁移

添加新接口或删除未使用接口对 威胁防御 配置的影响最小。但是，删除安全策略中使用的接口会影响配置。可以直接在 威胁防御 配置中的很多位置引用接口，包括安全区、NAT、VPN、路由、DHCP 服务器等。

设备管理器 支持通过其他接口迁移安全策略中的接口，因此几乎可以无缝删除接口。

注释 迁移功能不会将名称、IP 地址和其他配置从一个接口复制到另一个接口；相反，此功能会将安全策略更改为引用新接口，而不是旧接口。需要在迁移之前手动配置新接口设置。

如果需要删除接口，我们建议您添加新接口并迁移旧接口，然后再将其删除。如果同时添加和删除接口，迁移过程仍将正常工作；但是，您无法手动编辑已删除接口或引用这些接口的策略，因此您可能会发现分阶段执行迁移更容易。

如果替换同一类型的接口（例如，需要对网络模块执行 RMA 操作），则可以：1. 从旧机箱中移除模块；2. 执行扫描；3. 部署与已删除接口无关的更改；4. 更换模块；5. 执行新扫描；6. 部署配置，包括与接口相关的任何更改。如果新接口具有与旧接口相同的接口 ID 和特征，则无需执行迁移。

接口扫描和迁移准则和限制

不受支持的接口迁移

- BVI 物理接口
- 防火墙接口的被动接口
- 网桥组成员
- EtherChannel 接口成员
- ISA 3000 硬件旁路成员
- Firepower 1010 VLAN 接口或交换机端口
- 诊断接口
- HA 故障转移和状态链路
- 迁移不同类型的接口，例如将网桥组接口迁移至需要物理接口的功能

其他准则

- 如果需要删除接口，我们建议您添加新接口并迁移旧接口，然后再将其删除。
- 对于 threat defense virtual，仅在接口列表结尾添加和删除接口。如果在任何其他位置添加或删除接口，则虚拟机监控程序将对接口重新编号，从而致使配置中的接口 ID 与错误接口相符。
- 如果扫描/迁移出现故障，请恢复机箱上的原始接口，然后重新扫描以恢复原始状态。
- 对于备份，请务必使用新接口创建新备份。使用旧配置还原将恢复旧的接口信息，您必须再次执行扫描/替换。
- 对于HA，在主用设备上执行接口扫描前，请对两台设备进行相同的接口更改。您只需在主用设备上执行扫描/迁移。配置更改会复制到备用设备。

扫描和迁移接口

扫描 设备管理器中的接口更改，并从已删除接口迁移接口配置。如果您仅想迁移接口配置（且无需扫描），请忽略与扫描相关的以下过程中的步骤。

注释 迁移功能不会将名称、IP 地址和其他配置从一个接口复制到另一个接口；相反，此功能会将安全策略更改为引用新接口，而不是旧接口。需要在迁移之前手动配置新接口设置。

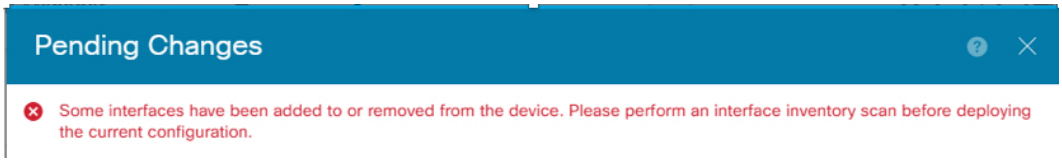
过程

步骤 1 在机箱上添加或删除接口。

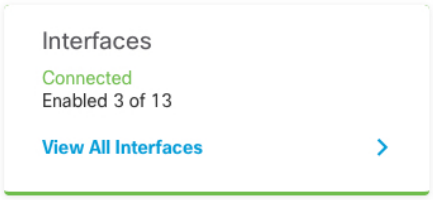
如果需要删除接口，我们建议您添加新接口并替换旧接口，然后再将其删除。

步骤 2 接口更改扫描。

执行接口扫描前，您将无法部署配置。如果尝试在扫描之前进行部署，您会看到以下错误：

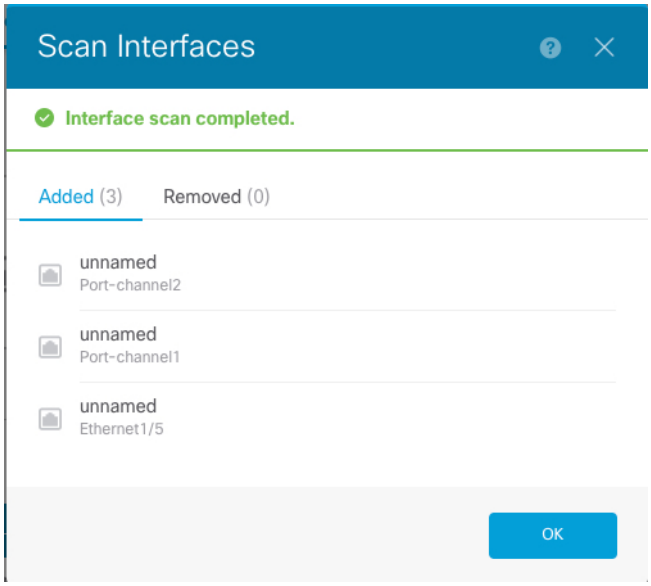


a) 点击**设备**，然后点击**接口**摘要中的**查看所有接口**链接。

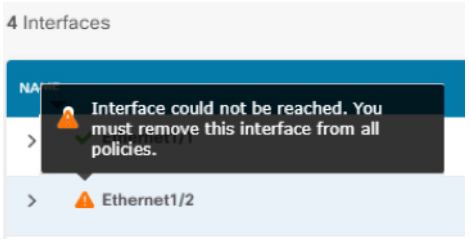


b) 点击扫描接口图标 ( )。

c) 等待接口扫描，然后点击**确定**。



扫描后，已删除接口显示在 接口 页面上，并带有警告符号：



步骤 3 要将现有接口迁移至新接口：

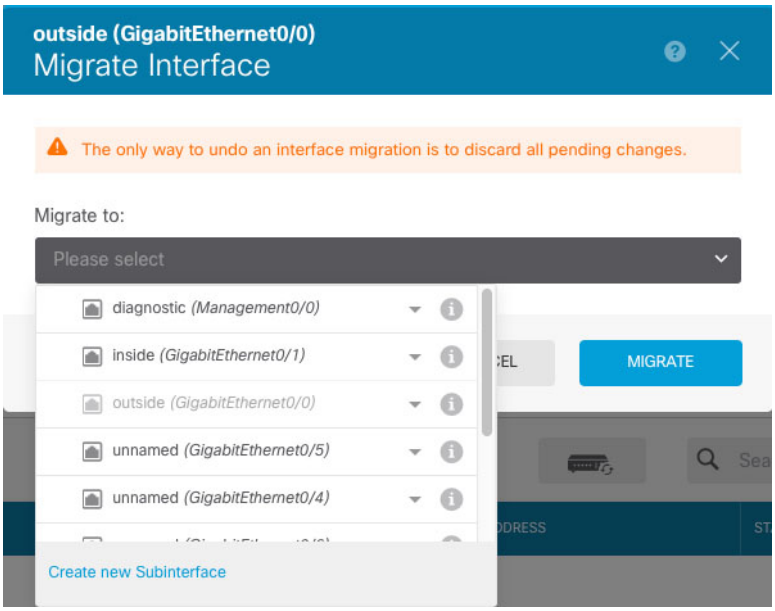
a) 使用名称、IP 地址等配置新接口。

如果要使用待删除接口的现有 IP 地址和名称，则首先需要使用虚拟名称和 IP 地址重新配置旧接口，以便可以在新接口上使用这些设置。

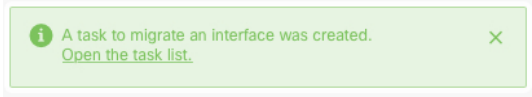
b) 点击旧接口的“迁移”图标。

此过程会将旧接口迁移至引用该接口的所有配置设置中的新接口。

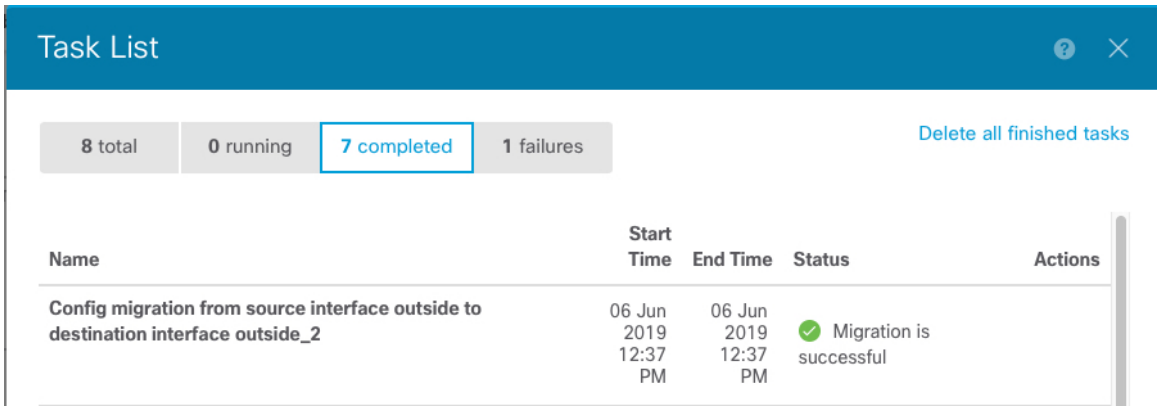
c) 从**迁移至：**下拉列表中选择新接口。



d) 一则消息将显示在**接口 (Interfaces)** 页面上。点击消息中的链接。



e) 检查**任务列表**，以确保迁移成功。

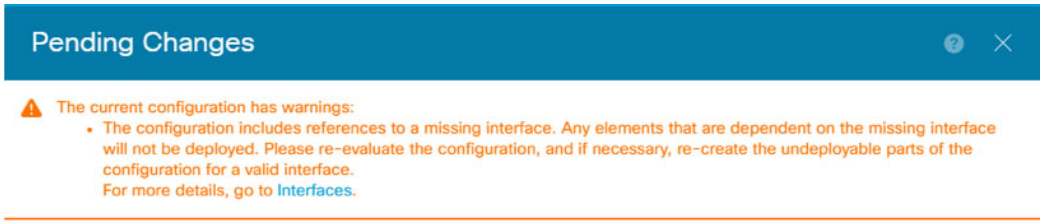


f) 如果迁移失败，您可以在 API Explorer 中查看原因。

要打开 API Explorer，点击更多选项按钮 (⋮) 并选择 **API Explorer**。选择**接口** > **GET /jobs/interfacemigrations**，然后点击**尝试！**。

步骤 4 部署配置。

将不会部署引用已删除接口的配置部分，在这种情况下，您将看到以下消息：



步骤 5 删除机箱上的旧接口，然后执行其他扫描。

系统将从**接口 (Interfaces)** 页面中删除您的策略中不再使用的已删除接口。

步骤 6 重新部署配置，以从配置中删除未使用接口。

管理 Cisco Secure Firewall 3100 的网络模块

如果在首次打开防火墙之前安装网络模块，则无需执行任何操作；网络模块已启用并可供使用。

如果您需要在初始启动后更改网络模块安装，请参阅以下程序。

配置分支端口

您可以为每个 40GB 或更高的接口配置 10GB 分支端口。此程序介绍如何断开和重新加入端口。分支端口可以像任何其他物理以太网端口一样使用，包括添加到 EtherChannel。

要获得高可用性，请在主用设备上执行此程序；接口更改将复制到另一台设备。

开始之前

- 您必须使用受支持的分支电缆。有关详细信息，请参阅硬件安装指南。
- 该接口不能在您的配置中使用。它不能有子接口或属于 EtherChannel。
- 为实现高可用性，无法命名、启用或监控接口的高可用性。

过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接。

系统默认选择**接口 (Interfaces)** 页面。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 要从 40GB 或更高接口拆分出 10GB 端口，请点击接口右侧的 **拆分**图标（）。

点击确认对话框中的 **确定 (OK)** 。 如果接口正在使用，您将看到一条错误消息。您必须先解决任何使用案例，然后才能重试分支。例如，您可以迁移配置以使用不同的接口。

例如，要拆分出 Ethernet2/1 40GB 接口，生成的子接口将被标识为 Ethernet2/1/1、Ethernet2/1/2、Ethernet2/1/3 和 Ethernet2/1/4。

在接口图形上，断开的端口具有以下外观：您可以点击左右箭头滚动浏览详细介绍分支端口状态的页面。

步骤 3 要重新加入分支端口，请点击接口右侧的 **加入** 图标（）。

点击确认对话框中的 **确定 (OK)**。 如果有任何子端口正在使用，您将看到一条错误消息。您必须先解决任何使用案例，然后才能重试重新加入。例如，您可以迁移配置以使用不同的接口。

您必须重新加入该接口的所有子端口。

步骤 4 部署配置。

增加网络模块

要在初始启动后将网络模块添加到防火墙，请执行以下步骤。添加新模块需要重新启动。

过程

步骤 1 根据硬件安装指南安装网络模块。

对于高可用性，请在两台设备上安装网络模块。

步骤 2 重新启动防火墙；请参阅 重启或关闭系统，第 791 页。对于高可用性，请重新启动备用设备，然后在备用设备上执行此程序的其余部分。

步骤 3 点击**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的**查看所有接口 (View All Interfaces)** 链路。

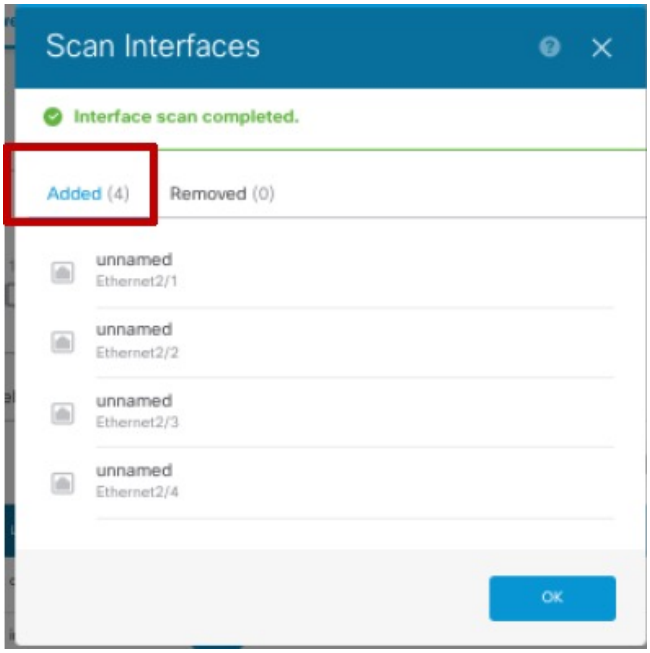
该图显示需要进行接口扫描。

图 *14:* 需要进行接口扫描

步骤 4 点击 **接口扫描 (Interface Scan)**，使用新的网络模块详细信息更新页面。

等待接口扫描，然后点击**确定**。

图 *15:* 扫描接口

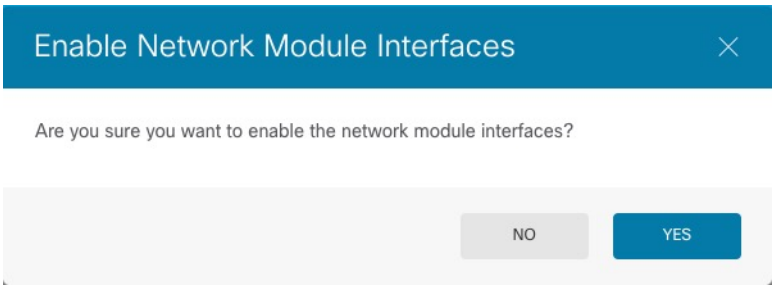


步骤 5 在接口图形上，点击滑块 ( ) 以启用网络模块。

图 *16:* 启用网络模块

步骤 6 系统将提示您确认是否要启用网络模块。点击 **Yes**。

图 *17:* 确认启用



步骤 7 对于高可用性，请更改主用设备（请参阅 切换主用和备用对等体（强制故障转移），第 210 页），然后对新的备用设备执行上述步骤。

热插拔网络模块

您可以将网络模块热插拔为相同类型的新模块，而无需重新启动。但是，您必须关闭当前模块才能安全地将其删除。此程序介绍如何关闭旧模块、安装新模块以及如何启用它。

开始之前

对于高可用性，如果故障转移链路在模块上，则不能禁用该网络模块。您必须中断高可用性（请参阅 中断高可用性，第 209 页）。热插拔模块后，您可以重新设置高可用性。

过程

步骤 1 对于高可用性，请确保要执行热插拔的设备是备用节点。请参阅切换主用和备用对等体（强制故障转移），第 210 页。

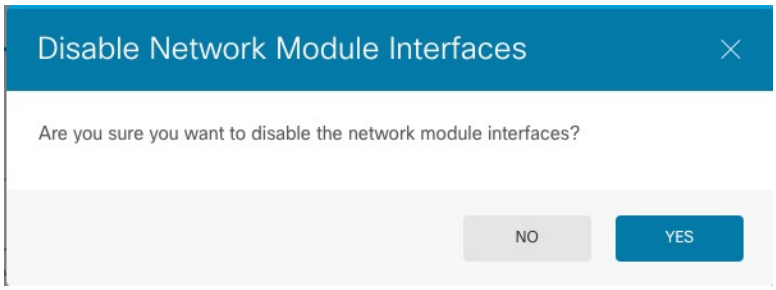
步骤 2 点击**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的**查看所有接口 (View All Interfaces)** 链路。

步骤 3 在接口图形上，点击滑块 () 以禁用网络模块。

图 *18:* 禁用网络模块

步骤 4 系统将提示您是否确认要禁用网络模块。点击 **Yes**。

图 *19:* 确认禁用



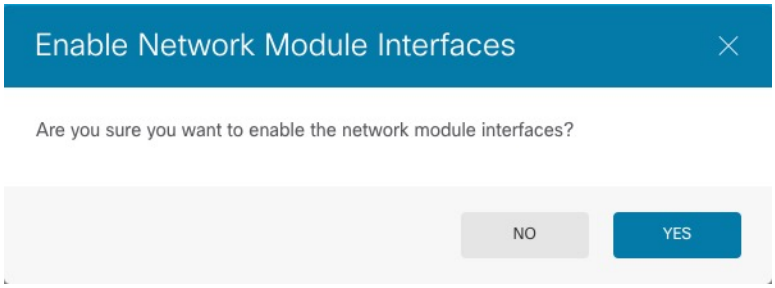
步骤 5 根据硬件安装指南安装网络模块。

步骤 6 在接口图形上，点击滑块 ( ) 以启用网络模块。

图 *20:* 启用网络模块

步骤 7 系统将提示您确认是否要启用网络模块。点击 **Yes**。

图 *21:* 确认启用



将网络模块更换为其他类型

如果您更换了其他类型的网络模块，则需要重新启动。如果新模块的接口少于旧模块，则必须手动删除与不再存在的接口相关的任何配置。

开始之前

为实现高可用性，如果故障转移链路在模块上，则不能禁用该网络模块。您将不得不中断高可用性（请参阅 中断高可用性，第 209 页），这意味着您将在重新启动主用设备时停机。设备完成重新启动后，您可以重新设置高可用性。

过程

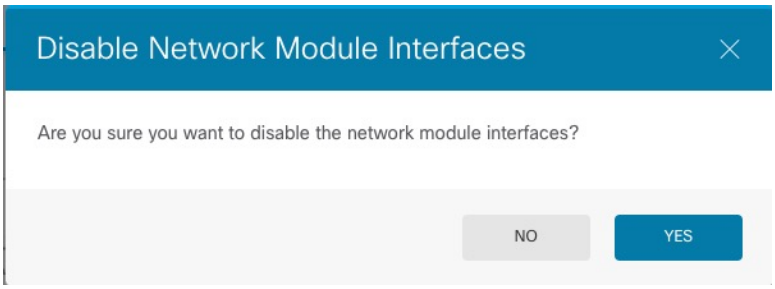
步骤 1 点击**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的**查看所有接口 (View All Interfaces)** 链路。要实现高可用性，请先在备用设备上执行此程序。

步骤 2 在接口图形上，点击滑块 ( ) 以禁用网络模块。

图 *22:* 禁用网络模块

步骤 3 系统将提示您是否确认要禁用网络模块。点击 **Yes**。

图 *23:* 确认禁用

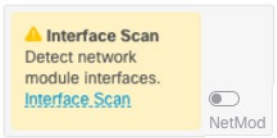


步骤 4 在设备上，根据硬件安装指南，取下旧的网络模块并更换为新的网络模块。

步骤 5 重新启动防火墙；请参阅 重启或关闭系统，第 791 页。

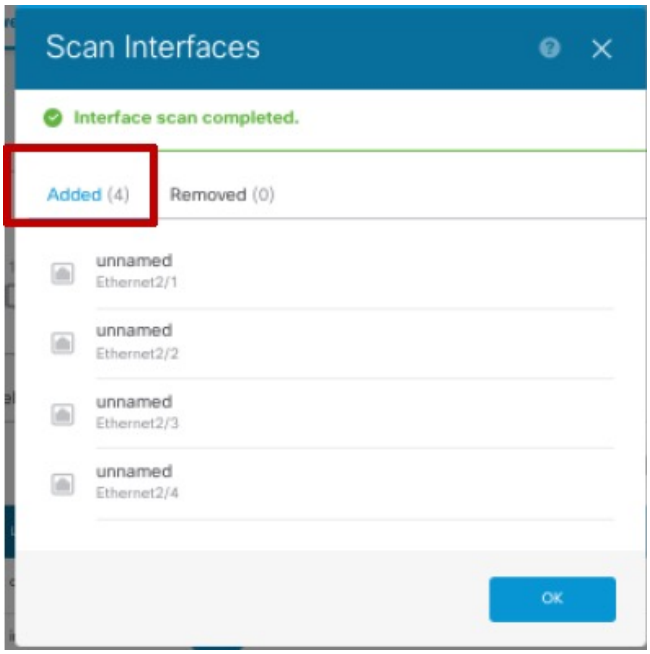
步骤 6 在 **接口 (Interfaces)** 页面上，该图显示需要进行接口扫描。点击 **接口扫描 (Interface Scan)**，使用新的网络模块详细信息更新页面。

图 *24:* 需要进行接口扫描



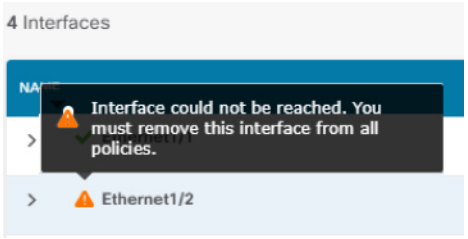
步骤 7 等待接口扫描，然后点击**确定**。

图 *25:* 扫描接口



扫描后，已删除接口显示在 **接口 (Interfaces)** 页面上，并带有警告符号：

图 *26:* 删除的接口



步骤 8 如果网络模块有 较少 接口，则需要删除直接引用已删除接口的任何配置。

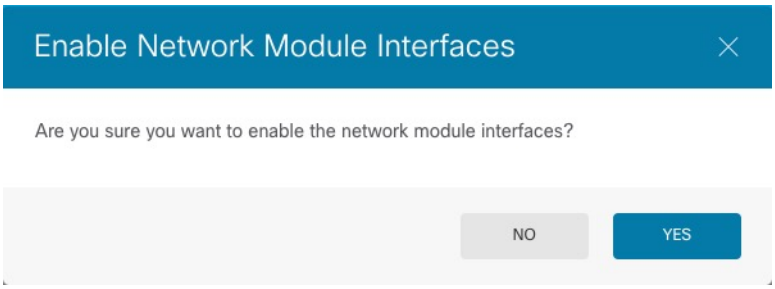
引用安全区的策略不受影响。您可以选择将配置迁移到其他接口。请参阅扫描和迁移接口，第 276 页。

步骤 9 在接口图形上，点击滑块 () 以启用网络模块。

图 *27:* 启用网络模块

步骤 10 系统将提示您确认是否要启用网络模块。点击 **Yes**。

图 *28:* 确认启用



步骤 11 要更改接口速度，请参阅 配置高级选项，第 272 页。

默认速度设置为“检测 SFP”，用于检测已安装的 SFP 的正确速度。仅当您手动将速度设置为特定值并且现在需要新的速度时，才需要修复速度。

步骤 12 如果必须更改任何配置，请点击 **部署** 图标。

无需部署即可保存网络模块更改。

步骤 13 对于高可用性，请更改主用设备（请参阅 切换主用和备用对等体（强制故障转移），第 210 页），然后对新的备用设备执行上述步骤。

拆卸网络模块

如果要永久删除网络模块，请执行以下步骤。拆卸网络模块需要重新启动。

开始之前

对于高可用性，请确保故障转移链路不在网络模块上。

过程

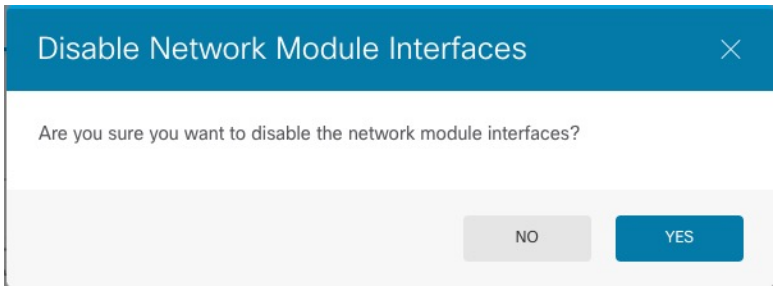
步骤 1 点击**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的**查看所有接口 (View All Interfaces)** 链路。对于高可用性，请先在备用设备上执行此程序。

步骤 2 在接口图形上，点击滑块 () 以禁用网络模块。

图 *29:* 禁用网络模块

步骤 3 系统将提示您是否确认要禁用网络模块。点击 **Yes**。

图 *30:* 确认禁用



步骤 4 在防火墙上，拆卸网络模块。

步骤 5 重新启动防火墙；请参阅 重启或关闭系统，第 791 页。

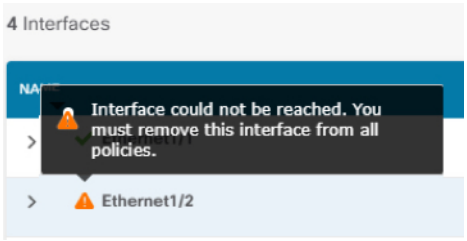
步骤 6 在 **接口 (Interfaces)** 页面上，该图显示需要进行接口扫描。点击 **接口扫描 (Interface Scan)**，使用正确的网络模块详细信息更新页面。

图 *31:* 需要进行接口扫描

步骤 7 等待接口扫描，然后点击**确定**。

扫描后，已删除接口显示在 **接口 (Interfaces)** 页面上，并带有警告符号：

图 *32:* 删除的接口



步骤 8 您需要删除直接引用已删除接口的任何配置。

引用安全区的策略不受影响。您可以选择将配置迁移到其他接口。请参阅扫描和迁移接口，第 276 页。

步骤 9 如果必须更改任何配置，请点击 **部署** 图标。

无需部署即可保存网络模块更改。

步骤 10 对于高可用性，请更改主用设备（请参阅 切换主用和备用对等体（强制故障转移），第 210 页），然后对新的备用设备执行上述步骤。

合并管理和诊断接口

威胁防御 7.4 及更高版本支持合并的管理和诊断接口。如果有任何使用诊断接口的配置，则不会自动合并接口，您需要执行以下程序。此程序要求您确认配置更改，在某些情况下，需要手动修复配置。

备份/恢复功能可保存和恢复合并状态（未合并或合并）。例如，如果合并接口，然后恢复之前的未合并配置，则恢复的配置将处于未合并状态。

下表显示了旧诊断接口上的可用配置，以及完成合并的方式。

表 *7:* 设备管理器 合并管理接口支持

旧诊断接口配置	合并行为	在管理接口上受支持？
接口		“管理”接口现在显示在**接口 (Interfaces)** 页面上，并且可在该页面上配置。以前，它可以在**系统设置 (System Settings)** > **管理接口 (Management Interface)** 页面上配置。
• IP 地址	需要手动删除。	改为使用当前的管理 IP 地址。 对于高可用性，管理接口不支持备用 IP 地址；每台设备有自己的 IP 地址，故障转移期间将保持这些地址。因此，不能使用单个管理 IP 地址与当前主用设备通信。 在**接口**窗格中设置，或在 CLI 中使用 **configure network ipv4** 或 **configure network ipv6** 命令进行设置。
• 名称“诊断”	自动更改为“管理”。 **注释** 任何其他接口都不能命名为“管理”。您必须更改名称才能继续合并。	更改为“管理”。

旧诊断接口配置	合并行为	在管理接口上受支持？
静态路由	需要手动删除。	**不支持**。 管理接口具有与数据接口不同的 Linux 路由表。威胁防御 实际上有两个“数据”路由表：一个用于数据接口，另一个用于管理专用接口（过去包括“诊断”接口，但也包括设置为管理专用的任何接口）。根据流量类型， 威胁防御 会检查一个路由表，然后回退到另一个路由表。此路由查找不再包括诊断接口，也不包括管理接口的 Linux 路由表。有关详细信息，请参阅管理流量的路由表，第 306 页。 您可以使用 **configure network static-routes** 命令在 CLI 中为 Linux 路由表添加静态路由 **注释** 使用 **configure network ipv4** 或 **configure network ipv6** 命令设置默认路由。
系统日志服务器	自动改为管理接口。	是。 系统日志服务器配置已具有从管理接口发送系统日志的选项（从 6.3 开始）。如果您特意为系统日志选择了诊断接口，系统会将其改为使用管理接口。
RADIUS 服务器	自动改为管理接口。	是。 如果您特意选择了诊断接口，系统会将其改为使用管理接口。 **注释** 如果您指定了路由查找，则 威胁防御 将无法再从管理专用接口发送流量；在这种情况下，您必须明确选择管理专用接口作为源接口。
AD 服务器	如果需要，手动指定管理接口。	是。 默认情况下，会为 AD 服务器通信执行路由查找，并且您无法指定 7.4 之前的接口。在 7.4 及更高版本中， 威胁防御 将不再能够使用路由查找从管理专用接口发送流量。在这种情况下，您现在可以明确选择管理专用接口作为源接口。
DDNS	需要手动删除。	**不支持**。
DHCP 服务器	需要手动删除。	**不支持**。
DNS 服务器	自动改为管理接口。	是。 如果您特意选择了诊断接口，系统会将其改为使用管理接口。如果未选择接口（**任何**），也会发生路由查找更改：路由查找使用数据路由表，但如果未找到路由，将不再回退到管理专用路由表。 **注释** 管理接口还具有仅用于其管理流量的单独 DNS 查找设置。
SLA 监控器	需要手动删除。	**不支持**。

旧诊断接口配置	合并行为	在管理接口上受支持？
FlexConfig	需要手动删除。	不支持。

开始之前

- 要查看设备的当前模式，请在 威胁防御 CLI 上输入 **show management-interface convergence** 命令。以下输出显示管理接口已合并：

```
> show management-interface convergence
management-interface convergence
>
```

以下输出显示管理接口未合并：

```
> show management-interface convergence
no management-interface convergence
>
```

- 对于高可用性对，请在主用设备上执行此任务。合并的配置将自动复制到备用设备。

过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链路。

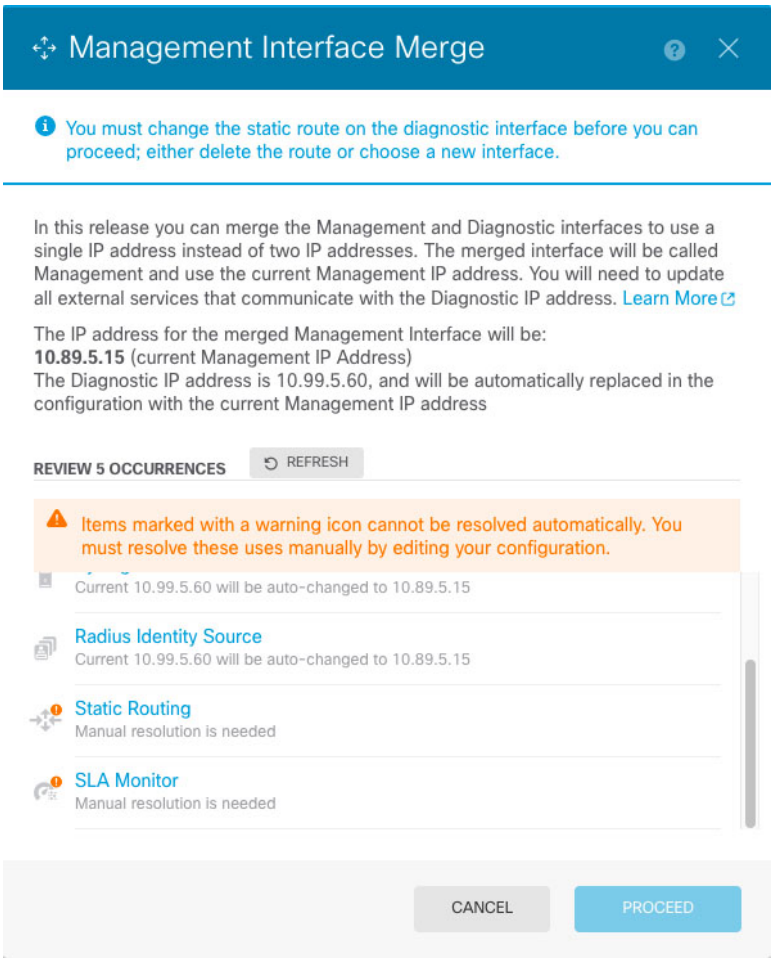
在**接口**表的顶部，您会看到**所需管理接口操作**的消息和链接。

步骤 2 编辑诊断接口，并删除 IP 地址。

在删除诊断 IP 地址之前，您无法完成合并。

步骤 3 点击**所需管理接口操作**区域中的**合并管理接口**。

管理接口合并对话框显示配置中所有使用诊断接口的情况。任何需要您手动删除或更改配置的情况将显示警告图标。还会显示自动迁移。



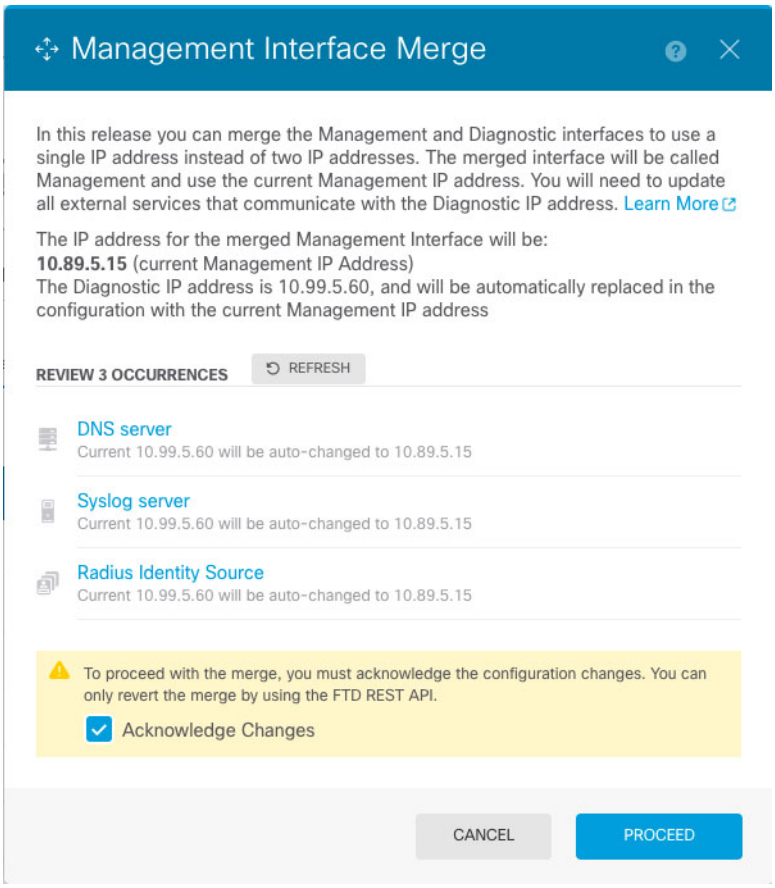
步骤 4 如果需要手动删除或更改任何列出的配置，请执行以下操作。

在进行配置更改时，您可以保持打开**管理接口合并**对话框以供参考。

a) 点击项目以打开配置页面。然后，您可以删除项目，或者改为选择数据接口。

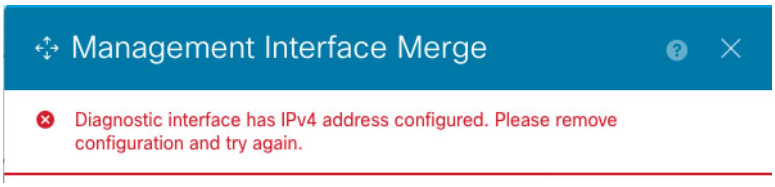
b) 要刷新**管理接口合并**对话框的内容，请点击**刷新**。

此时不应再显示任何警告。



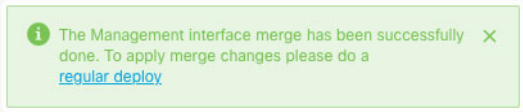
步骤 5 点击**确认更改**，然后点击**继续**。

如果您尚未删除诊断 IP 地址，则会看到以下错误：



在这种情况下，请删除诊断 IP 地址，然后再次点击**继续**。

合并配置后，您会看到成功横幅：



步骤 6 部署新的合并配置。

注意 如果您不想继续执行合并，可以在部署之前**放弃所有**更改，并撤消合并。部署合并的配置后，可以从设备管理器中取消合并接口；但是，诊断接口必须手动重新配置。请参阅取消合并管理接口，第 293 页。此外，如果恢复未合并的配置，则设备将恢复为该未合并的配置。

合并后，管理接口将显示在**接口 (Interfaces)**页面上，并且可在该页面上配置。以前，它可以在**系统设置 (System Settings)** > **管理接口 (Management Interface)** 页面上配置。

步骤 7 合并后，如果有任何与诊断接口通信的外部服务，您需要将其配置更改为使用管理接口 IP 地址。

例如：

- SNMP 客户端
- RADIUS 服务器 - RADIUS 服务器通常会验证传入流量的 IP 地址，因此您需要将该 IP 地址更改为管理地址。此外，对于高可用性对，您需要允许可同时使用主管理 IP 地址和辅助管理 IP 地址；诊断接口用于支持与主用设备一起使用的单个“浮动”IP地址，但管理接口不支持该功能。

取消合并管理接口

威胁防御 7.4 及更高版本支持合并的管理和诊断接口。如果您需要取消合并您的接口，请执行此程序。建议您在将网络迁移到合并模式部署时暂时使用未合并模式。可能并非所有未来版本都支持单独的管理接口和诊断接口。

取消合并接口不会恢复原始诊断配置（如果您是先升级然后再合并接口）。您需要手动重新配置诊断接口。此外，管理接口现在命名为“management”；不能将其重命名为“diagnostic”。

或者，如果您使用备份功能保存旧的未合并配置，则可以恢复该配置，设备将处于未合并状态，诊断配置保持不变。

开始之前

- 要查看设备的当前模式，请在 威胁防御 CLI 上输入 **show management-interface convergence** 命令。以下输出显示管理接口已合并：

```
> show management-interface convergence
management-interface convergence
>
```

以下输出显示管理接口未合并：

```
> show management-interface convergence
no management-interface convergence
>
```

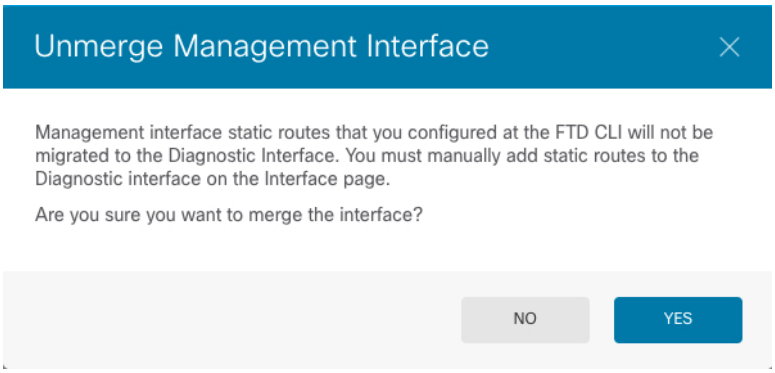
- 对于高可用性对，请在主用设备上执行此任务。未合并的配置将自动复制到备用设备。

过程

步骤 1 点击**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链路。

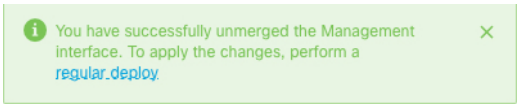
步骤 2 在管理 1/1 接口行的右侧，点击（**取消合并**），然后在**取消合并管理接口**对话框上点击**是**。

图 *33:* 取消合并管理接口



您将在**接口 (Interfaces)** 页面的顶部看到一条成功消息。

图 *34:* 取消合并成功



步骤 3 部署新的未合并配置。

如果您不想继续执行取消合并，可以在部署前**放弃所有**更改，保留合并后的接口。此外，如果恢复已合并的配置，则设备将恢复为该合并配置。

取消合并后，管理接口显示在**系统设置 (System Settings)** > **管理接口 (Management Interface)** 页面上，并且可在该页面上配置。

对电源故障配置硬件旁路 (ISA 3000)

您可以启用硬件旁路，使流量在断电期间继续在接口对之间流动。支持的接口对为铜缆接口 GigabitEthernet 1/1 和 1/2 以及 GigabitEthernet 1/3 和 1/4。如果您使用的是光纤以太网型号，则只有铜缆以太网对（GigabitEthernet 1/1 和 1/2）支持硬件旁路。默认情况下，如果支持，两个接口对均启用硬件旁路。

启用硬件旁路时，流量将在这些接口对之间的第 1 层传递。在 设备管理器 和 威胁防御 CLI 中都可以看到接口处于关闭状态。不使用防火墙功能，因此请确保您了解允许流量通过设备的风险。

我们建议您禁用 TCP 序列号随机化（如本过程中所述）。默认情况下，ISA 3000 会将通过其的 TCP 连接的初始序列号 (ISN) 重写为随机编号。硬件旁路激活后，ISA 3000 不再位于数据路径中，也不再转换序列号。接收客户端会收到意外序列号，并丢弃连接，因此需要重新建立 TCP 会话。即便禁用 TCP 序列号随机化后，某些 TCP 连接将也需要重新建立，因为链路在切换期间会临时关闭。

在 CLI 控制台或 SSH 会话中，使用 **show hardware-bypass** 命令以监控运行状态。

开始之前

要使用硬件旁路：

- 必须将接口对放置在同一网桥组内。
- 必须将接口连接到交换机的接入端口。不能将它们连接到中继端口。

过程

步骤 1 点击**设备**，然后点击接口摘要中的链接。

在页面顶部的**硬件旁路 (Hardware Bypass)** 部分显示设备允许的接口对的当前配置。

但是，在启用硬件旁路之前，必须确保在同一网桥组中配置接口对。

步骤 2 点击**编辑**以配置硬件旁路。

系统将显示**硬件旁路配置**对话框。

步骤 3 要配置自动硬件旁路行为，请为每个接口对在**断电期间硬件旁路**区域中选择以下一个选项。

- **禁用** - 禁用硬件旁路。断电期间流量不会流过设备。
- **启用** - 在断电期间激活硬件旁路。硬件旁路可确保在断电期间流量不会中断。请注意，系统不会检查绕过的流量，并且不会应用安全策略。恢复电源后，硬件旁路会自动禁用，以便流量可以经过检测正常通行。请注意，禁用硬件旁路时可能会出现短暂的流量中断。
- **持久性启用** - 在断电期间激活硬件旁路，并在恢复供电后继续启用硬件旁路。恢复供电后，您必须使用**手动硬件旁路**滑块禁用硬件旁路。此选项允许您控制何时短暂中断流量。

步骤 4 （可选） 要手动启用或禁用硬件旁路，请点击**手动硬件旁路**滑块。

例如，您可能想要测试系统，或出于某些原因需要暂时绕过设备。请注意，您必须部署配置来更改硬件旁路的状态；只更改设置是不够的。

手动启用/禁用硬件旁路时，您将看到以下系统日志消息，其中对为 1/1-1/2 或 1/3-1/4。

- %FTD-6-803002：系统不对通过 GigabitEthernet 对的流量提供保护
- %FTD-6-803003：用户已手动在 GigabitEthernet 对上禁用旁路

步骤 5 点击**确定**。

更改不会立即生效。您必须部署配置。

步骤 6 （可选。）创建禁用 TCP 序列号随机化所需的 FlexConfig 对象和策略。

a) 在**设备** > **高级配置**中点击**查看配置**。
b) 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。
c) 点击 + 按钮以创建新的对象。
d) 为对象输入名称。例如，**Disable_TCP_Randomization**。

e) 在**模板**编辑器中，输入命令禁用 TCP 序列号随机化。

命令是 **set connection random-sequence-number disable**，但您必须为策略映射中的特定类配置此命令。到目前为止，最简单的方法是全局禁用随机序列号，这需要使用以下命令：

```
policy-map global_policy
 class default_class
  set connection random-sequence-number disable
```

f) 在**取消模板**编辑器中，输入撤消此配置所需的命令。

例如，如果您全局禁用 TCP 序列号随机化，取消模板将为：

```
policy-map global_policy
 class default_class
  set connection random-sequence-number enable
```

g) 点击**确定**保存对象。

现在需要将此对象添加到 FlexConfig 策略。并非创建好对象就可以了。

h) 点击目录中的 **FlexConfig 策略**。

i) 在组列表中点击 **+**。

j) 选择 Disable_TCP_Randomization 对象，然后点击**确定**。

系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。

k) 点击**保存**。

您现在可以部署策略。

监控接口

可在以下区域查看有关接口的一些基本信息：

- **设备**。使用端口图可监控接口的当前状态。将鼠标悬停在端口上方可查看其IP地址、EtherChannel 成员身份、启用状态和链路状态。IP 地址可静态分配，也可以使用 DHCP 获取。

  接口端口使用以下颜色代码：

  - 绿色 - 接口已配置和启用，链路为运行状态。
  - 灰色 - 接口未启用。
  - 橙色/红色 - 接口已配置和启用，但链路中断。如果该接口已连接电缆，则此状态表示有错误需要更正。如果该接口未连接电缆，则此状态为预期状态。

- **监控** > **系统**。**吞吐量**控制面板显示有关流经系统的流量的信息。您可以查看所有接口的信息，也可以选择特定接口查看其信息。

- **监控** > **区域**。该控制面板显示基于安全区的统计信息，这些安全区由接口组成。您可以深入分析此信息以了解更多详情。

在 CLI 中监控接口

您还可以打开 CLI 控制台或登录设备 CLI，使用以下命令获取有关接口相关行为与统计信息的更详细信息。

- **show interface** 显示接口统计信息和配置信息。此命令有许多关键字，可用于获取所需的信息。使用 ? 作为关键字可查看可用选项。
- **show ipv6 interface** 显示有关接口的 IPv6 配置信息。
- **show bridge-group** 显示网桥虚拟接口 (BVI) 的相关信息，包括成员信息和 IP 地址。
- **show conn** 显示当前通过接口建立的连接的相关信息。
- **show traffic** 显示流过每个接口的流量的相关统计信息。
- **show ipv6 traffic** 显示流过设备的 IPv6 流量的相关统计信息。
- **show dhcpd** 显示接口上的 DHCP 使用统计信息及其他信息，特别是接口上配置的 DHCP 服务器的相关信息。
- **show switch vlan** 显示 VLAN 到交换机端口的关联。
- **show switch mac-address-table** 显示静态和动态 MAC 地址条目。
- **show arp** 显示动态、静态和代理 ARP 条目。
- **show power inline** 显示 PoE 状态。
- **show vpdn group** 显示 PPPoE 组以及已配置的用户名和身份验证。
- **show vpdn username** 显示 PPPoE 用户名和密码。
- **show vpdn session pppoe state** 显示 PPPoE 会话的状态。

接口示例

使用案例章节涵盖以下与接口相关的示例：

- 如何在设备管理器上配置设备 ， 第 39 页
- 如何添加子网 ， 第 66 页
- 如何被动监控网络上的流量 ， 第 71 页

第 IV 部分

路由

第 12 章

路由基础知识和静态路由

系统使用路由表来确定进入系统的数据包的传出接口。以下主题介绍路由的基本信息以及如何在设备上配置静态路由。

路由最佳实践

在网络中设计路由进程的过程可能十分复杂。本章假定您将威胁防御设备配置为可在现有网络中工作，并参与已在网络中建立的路由进程。

如果要创建新网络，请花时间阅读从其他位置获取的有关路由协议及如何设计适用于您网络的有效路由计划的信息。本章不介绍关于如何选择协议的建议，也不介绍协议的工作方式。

如果网络非常小，而且您只向上链接到ISP，则可能只需要一些静态路由即可，根本不需要实现路由协议。

但是，如果要建立含许多路由器的大型网络，则可能需要为内部路由至少实现一种路由协议（例如OSPF），为外部路由至少实现一种路由协议（例如BGP）。服务提供商可帮助您了解可能需要的外部路由（如果有）。如果是这种情况，请首先了解使用 威胁防御可以配置的路由协议，然后规划网络，最后根据计划来配置 威胁防御 设备。

路由概述

以下主题介绍路由在威胁防御设备中的运行方式。所谓路由是指通过网络将信息从源发送到目标的活动。在途中通常会经过至少一个中间节点。路由涉及两个基本活动：确定最佳路由路径和通过网络传输数据包。

支持的路由协议

下表介绍可使用 设备管理器在 威胁防御 设备上配置的路由协议和技术，以及完成配置所需的方法。

表 *8:* 支持的路由协议

路由功能	配置方法	说明
BGP	Smart CLI	从**设备 (Device)** > **路由 (Routing)** 页面中配置 BGP Smart CLI 对象。 使用**设备 (Device)** > **高级配置 (Advanced Configuration)**页面中的 Smart CLI 对象配置 BGP 中使用的对象，例如路由映射。
双向转发检测 (BFD)	FlexConfig	从**设备 (Device)** > **高级配置 (Advanced Configuration)**页面中使用 FlexConfig 对象配置 BFD。仅 BGP 支持 BFD。
EIGRP	Smart CLI	在**设备 (Device)** > **路由 (Routing)**页面中配置 EIGRP Smart CLI 对象。 使用**设备 (Device)** > **高级配置 (Advanced Configuration)**页面中的 Smart CLI 对象配置 EIGRP 中使用的对象（例如路由映射）。
IS-IS	FlexConfig	使用**设备 (Device)** > **高级配置 (Advanced Configuration)**页面的 FlexConfig 对象配置 IS-IS。
组播路由	FlexConfig	使用**设备 (Device)** > **高级配置 (Advanced Configuration)** 页面中的 FlexConfig 对象配置组播路由。
OSPFv2	Smart CLI	使用**设备 (Device)** > **路由 (Routing)** 页面中的 Smart CLI 对象配置 OSPFv2。 使用**设备 (Device)** > **高级配置 (Advanced Configuration)** 页面中的 Smart CLI 对象配置 OSPFv2 中使用的对象，例如路由映射。
OSPFv3	—	不支持 OSPFv3 配置。
基于策略的路由 (PBR)	FlexConfig	使用**设备 (Device)** > **高级配置 (Advanced Configuration)** 页面中的 FlexConfig 对象配置基于策略的路由 (PBR)。
RIP	FlexConfig	使用**设备 (Device)** > **高级配置 (Advanced Configuration)**页面中的 FlexConfig 对象配置 RIP。
静态路由	设备管理器	从**设备 (Device)** > **路由 (Routing)** 页面全局地或针对每个虚拟路由器配置静态路由。
虚拟路由器，VRF	设备管理器	从**设备 (Device)** > **路由 (Routing)** 页面配置虚拟路由器。

路由类型

主要有两种类型的路由：静态路由或动态路由。

静态路由是明确定义的路由。它们相对稳定且通常具有高优先级，用于确保将发往路由目标的流量发送到正确的接口。例如，您可以创建一个默认静态路由，用于覆盖尚未被任何其他路由覆盖的所有流量，即 IPv4 的 0.0.0.0/0 或 IPv6 的 ::/0。另一个示例是指向您经常使用的内部系统日志服务器的静态路由。

动态路由是从路由协议（如 OSPF、BGP、EIGRP、IS-IS 或 RIP）的操作中习得的路由协议，您不用直接定义这类路由。相反，您配置路由协议，然后系统与邻居路由器进行通信，传输并接收路由更新。

动态路由协议通过分析收到的路由更新消息调整路由表，使其适应不断变化的网络环境。如果有消息表明网络发生更改，则系统会重新计算路由并发出新的路由更新消息。这些消息会渗入网络，促使路由器重新运行其算法并相应地更改其路由表。

静态路由非常简单，发挥基本路由的作用，在网络流量相对可预测且网络设计相对简单的环境中十分适用。但是，静态路由不能更改（除非您编辑它们），因此它们不能应对网络中的更改。

除非您有一个小型网络，否则您通常会将静态路由和一个或多个动态路由协议搭配使用。您将定义至少一个静态路由，作为不匹配显式路由的流量的默认路由。

注释 可以使用 Smart CLI 配置以下路由协议：OSPF、BGP。使用 FlexConfig 配置 ASA 软件支持的其他路由协议。

路由表和路由选择

如果 NAT 转换 (xlates) 和规则无法确定传出接口，系统将使用路由表来确定数据包的路径。

路由表中的路由包括一个名为“管理距离”的指标，提供相对于既定路由的优先级。如果某个数据包与多个路由条目匹配，则使用距离最短的路由。直连网络（在接口上定义的网络）的距离为 0，因此始终首选使用此网络。静态路由的默认距离为 1，但您可以使用 1-254 之间的任意距离创建默认距离。

标识具体目标的路由优先于默认路由（即目标为 0.0.0.0/0 或 ::/0 的路由）。

路由表的填充方式

威胁防御路由表可以通过静态定义的路由、直连路由以及动态路由协议发现的路由来填充。由于威胁防御 设备除具有路由表中的静态路由和已连接路由外，还可以运行多条路由协议，因此可通过多种方式发现或输入同一路由。当在路由表中放入同一目标的两条路由时，将按如下确定保留在路由表中的路由：

- 如果两个路由具有不同的网络前缀长度（网络掩码），则会将两个路由都视为唯一并输入到路由表中。然后，由数据包转发逻辑确定使用哪一条路由。

  例如，如果 RIP 和 OSPF 进程发现以下路由：

- RIP：192.168.32.0/24
- OSPF：192.168.32.0/19

即使 OSPF 路由具有更好的管理距离，但由于两条路由具有不同的前缀长度（子网掩码），因此均会安装在路由表中。这两条路由被视为不同目标，数据包转发逻辑会确定使用哪条路由。

- 如果 威胁防御 设备从单个路由协议（例如 RIP）获悉通向同一目标的多条路径，则会在路由表中输入具有更佳指标的路由（由路由协议确定）。

  度量是与特定路由关联的值，从最高优先到最低优先进行排序。用于确定度量的参数根据路由协议而异。具有最低指标的路径选择作为最佳路径并安装在路由表中。如果有多个度量相等的通向同一目的地的路径，则会在这些等价路径上进行负载均衡。

- 如果 威胁防御 设备从多个路由协议获悉目标，则会比较路由的管理距离，并在路由表中输入管理距离较短的路由。

路由的管理距离

您可以更改由路由协议发现或重分发到路由协议中的路由的管理距离。如果来自两个不同路由协议的两条路由具有相同的管理距离，则会将具有较短默认管理距离的路由输入到路由表中。对于EIGRP 和 OSPF 路由，如果 EIGRP 路由和 OSPF 路由具有相同的管理距离，则默认选择 EIGRP 路由。

管理距离是 威胁防御设备在有两个或多个通向同一目标（来自两个不同路由协议）的路由时，用于选择最佳路径的路由参数。由于路由协议具有基于不同于其他协议的算法的度量，因此并非总能够确定通向由不同路由协议生成的同一目的地的两条路由的最佳路径。

每个路由协议使用管理距离值划分优先级。下表显示 威胁防御设备支持的路由协议的默认管理距离值。

表 *9:* 受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
VPN 路由	1
静态路由	1
EIGRP 汇总路由	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120

路由源	默认管理距离
EIGRP 外部路由	170
内部和本地 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 威胁防御设备从 OSPF 路由进程（默认管理距离 - 110）和 RIP 路由进程（默认管理距离 - 120）均收到通向特定网络的路由，则 威胁防御设备 会选择 OSPF 路由，因为 OSPF 具有更高的优先级。在这种情况下，路由器会将 OSPF 版本的路由添加到路由表。

VPN 通告路由 (V-Route/RRI)）相当于默认管理距离为 1 的静态路由。但与网络掩码 255.255.255.255 一样，它具有更高的优先级。

在本示例中，如果 OSPF 派生路由的源丢失（例如，由于电源关闭），则 威胁防御设备会使用 RIP 派生路由，直至 OSPF 派生路由再次出现。

管理距离是一项本地设置。例如，如果您更改通过 OSPF 获取的路由的管理距离，那么这种更改只会影响在其上输入该命令的 威胁防御设备的路由表。在路由更新中不会通告管理距离。

管理距离不影响路由进程。路由进程仅通告路由进程已发现或重分发到路由进程中的路由。例如，即使在 路由表中使用 OSPF 路由进程发现的路由，RIP 路由进程也会通告 RIP 路由。

备份动态和浮动静态路由

当由于安装另一条路由而导致初始尝试将路由安装在路由表中失败时，系统会注册备用路由。如果安装在路由表中的路由失败，则路由表维护进程会呼叫已注册备用路由的每个路由协议进程，并请求它们重新在路由表中安装此路由。如果有多个协议为失败路由注册了备用路由，则根据管理距离选择优先路由。

鉴于以上过程，当动态路由协议发现的路由失败时，您可以创建安装在路由表中的浮动静态路由。浮动静态路仅仅是配置有比 威胁防御设备上运行的动态路由协议更大的管理距离的静态路由。当动态路由进程发现的对应路由失败时，会在路由表中安装静态路由。

如何制定转发决策

系统按如下制定转发决策：

- 如果目的不匹配路由表中的条目，则通过为默认路由指定的接口转发数据包。如果尚未配置默认路由，则会丢弃数据包。
- 如果目的匹配路由表中的单个条目，则通过与该路由关联的接口转发数据包。
- 如果目的匹配路由表中的多个条目，则通过与具有较长网络前缀的路由相关联的接口转发数据包。

例如，发往 192.168.32.1 的数据包到达在路由表中拥有以下路由的接口：

- 192.168.32.0/24 网关 10.1.1.2

- 192.168.32.0/19 网关 10.1.1.3

在这种情况下，发往 192.168.32.1 的数据包直接发送到 10.1.1.2，因为 192.168.32.1 属于 192.168.32.0/24 网络。它也属于路由表中的其他路由，但 192.168.32.0/24 在路由表中的前缀最长（24 位对比 19 位）。在转发数据包时，较长前缀始终优先于较短的前缀。

注释 即便新的相似连接将因路由中的变化而导致不同行为，现有连接也将继续使用其已建立的接口。

管理流量的路由表

威胁防御 设备包括用于关联设备管理流量的以下路由表：

- Linux 管理路由表 - 来自管理接口的特殊管理流量（例如 设备管理器 管理会话、 许可通信和数据库更新）始终使用 Linux 管理路由表。
- 数据路由表 - 默认情况下，所有关联设备流量（以及所有通过流量）使用数据路由表。所有常规数据接口都属于此路由表。大多数服务允许您选择特定接口，因此仅使用与该接口关联的路由。
- 管理专用路由表 - 管理接口和您设置为管理专用的所有数据接口都属于此路由表。要从这些接口中的任一接口发送关联设备流量，必须在配置服务时选择特定的管理专用接口。DNS 查找存在一种例外情况：在某些情况下， 威胁防御将使用数据路由表，然后在未找到路由时自动回退到管理路由表。您可以为管理专用接口添加静态路由，但不能为特殊管理接口添加静态路由。威胁防御 设备会自动为管理接口添加一个将流量转发到 Linux 的默认路由，这时将在 Linux 路由表中执行单独的路由查找。您可以使用 威胁防御 CLI **configure network static-routes** 命令将静态路由添加到 Linux 路由表中，供管理接口使用。

注释 使用 **configure network ipv4** 或 **configure network ipv6** 命令设置默认 Linux 路由。

注释 对于尚未合并管理接口和旧诊断接口的设备，请参阅本指南 7.3 版之前的版本。

等价多路径 (ECMP) 路由

威胁防御设备支持等价多路径 (ECMP) 路由。

每个接口最多支持 8 个等价静态或动态路由。例如，您可以在外部接口上配置多个默认路由，指定不同的网关：

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
```

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

在这种情况下，流量在外部接口上的 10.1.1.2、10.1.1.3 和 10.1.1.4 之间进行负载均衡。流量基于散列源和目标 IP 地址、传入接口、协议、源与目标端口的算法在 指定网关之间进行分发。

使用流量区域跨多个接口的 ECMP

如果将流量区域配置为包含一组接口，在每个区域中最多可以跨 8 个接口配置最多 8 个等价静态或动态路由。例如，您可以在区域中跨三个接口配置多个默认路由：

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

同样，动态路由协议可以自动配置等价路由。威胁防御设备使用更稳健的负载均衡机制跨接口对流量进行负载均衡。

当某条路由丢失时，设备会将流量无缝移至其他路由。

静态路由

您可以创建静态路由，以提供网络基本路由。

关于静态路由和默认路由

要将流量路由到非连接的主机或网络，必须使用静态路由或动态路由定义到主机或网络的路由。通常，您必须配置至少一个静态路由：所有流量的默认路由（不是通过其他方式路由到默认网络网关），通常是指下一跳路由器。

默认路由

最简单的方法是配置一个默认静态路由，将所有流量都发送到上游路由器，从而依靠该路由器来为您路由流量。默认路由对网关 IP 地址进行标识，威胁防御设备将所有不具有已获悉或静态路由的数据包发送到该网关地址。默认静态路由是以 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 作为目标 IP 地址的静态路由。

应始终定义一个默认路由。

威胁防御 为数据接口和管理专用接口（包括特殊的 Linux 管理接口）提供单独的路由表。只能为数据路由表添加默认路由。 威胁防御 会自动在管理专用路由表中添加一个将流量发送到 Linux 管理接口的默认路由，这时将在 Linux 路由表中执行单独的路由查找。您可以使用 威胁防御 CLI **configure network static-routes** 命令将静态路由添加到 Linux 路由表中，供管理接口使用。

注释 使用 **configure network ipv4** 或 **configure network ipv6** 命令设置默认 Linux 路由。

静态路由

在以下情况下，您可能希望使用静态路由：

- 您的网络使用不受支持的路由器发现协议。
- 网络规模较小，并且可以轻松管理静态路由。
- 不希望流量或 CPU 开销与路由协议相关联。
- 在某些情况下，仅使用默认路由并不足够。默认网关可能无法到达目标网络，因此还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法将直接流量定向到未直接与威胁防御设备连接的任何内部网络。
- 您使用的是不支持动态路由协议的功能。

备份静态路由和静态路由跟踪

使用静态路由的一个问题是，缺乏用于确定路由处于开启还是关闭状态的内在机制。即使下一跳网关变得不可用，静态路由依然保留在路由表中。只有关联接口关闭时，静态路由才会从路由表中删除。

通过实施路由跟踪，使用服务级别协议 (SLA) 监控，您可以跟踪静态路由的可用性，并在主路由发生故障时，自动安装备用路由。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 ISP 不可用。

在使用路由跟踪时，将目标网络上的目标 IP 地址关联到跟踪的路由。随后，系统会使用 ICMP 回应请求，以定期验证可以访问此地址。如果系统在指定时间内未收到回应，它便会认为此主机不可访问，并从路由表中删除关联的路由。然后，系统会使用具有较高指标的未跟踪备份路由替代已删除的路由。

因此，要对给定目标使用备份静态路由（包括默认路由），您必须执行以下操作：

1. 创建 SLA 监控，以监控目标网络上的可靠 IP 地址，例如网关或始终启用的服务器（例如 web 服务器或系统日志服务器）。对于在目标网络保持正常运行且可被访问时仍可能会离线的系统，不要监控其 IP 地址。请参阅配置 SLA 监控器对象，第 311 页。
2. 创建通往目标的主路由，并选择适用于此路由的 SLA 监控。通常，此路由的指标应为 1。请参阅配置静态路由，第 309 页。
3. 创建备份静态路由，以便在主路由发生故障时使用。此路由的指标应比主路由的大。例如，如果主路由为 1，则备用路由可能是 10。通常，您还会为备份路由选择一个不同的接口。

静态路由准则

网桥组

- 在路由模式下，必须指定 BVI 作为网关；不能指定成员接口。

- 对于源自 威胁防御设备（例如系统日志或 SNMP）且通过网桥组成员接口为非直接连接网络定义的流量，需要配置默认路由或静态路由，以使 威胁防御设备了解通过哪个网桥组成员接口发出流量。如果存在无法通过单个默认路由进行访问的服务器，则必须配置静态路由。
- 静态路由跟踪不支持网桥组成员接口或 BVI。

IPv6

- IPv6 不支持静态路由跟踪（SLA 监控器）。

等价多路径 (ECMP) 流量区域

- 将 ECMP 流量区域的成员接口保留在同一安全区中，以防止对这些接口应用不同的访问规则、SSL 或身份规则。
- 对于给定 ECMP 流量区域中的网络，最多可以有 8 个等价路由。
- 您最多可以创建 256 个 ECMP 流量区域，每个区域最多 8 个接口。
- ECMP 流量区域可以包含已命名的物理接口、子接口和 EtherChannel。它们不能包含以下内容：
  - 网桥组 (BVI) 或其成员
  - EtherChannel 成员接口
  - HA 接口（故障转移或状态链路）
  - 仅限用于管理的接口
  - 用于站点间 VPN 或远程访问 VPN 连接的接口。
  - 虚拟隧道接口 (VTI) 或其源接口。
  - 为 VPN 管理访问配置的接口。
- 不能在区域的接口上启用 DHCP 中继。

配置静态路由

定义静态路由，以告知系统从何处发送的数据包不会绑定至直连到系统接口的网络。

对于网络 0.0.0.0/0，至少需要一个静态路由，即默认路由。如果数据包的传出接口无法由现有 NAT xlate（转换）、静态 NAT 规则或其他静态路由确定，则此路由为所发送的数据包定义目的。

如果无法使用默认网关到达所有网络，则可能需要其他静态路由。例如，默认路由通常是外部接口上的上游路由器。如果还有其他未直连到设备的内部网络，并且通过默认网关无法访问它们，则需要对每个此类内部网络使用静态路由。

对于直连到系统接口的网络，无法定义静态路由。系统自动创建这些路由。

过程

步骤 1 点击**设备**，然后点击**路由**摘要中的链接。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置静态路由的路由器的查看图标 ()。

步骤 3 在**静态路由页**中，执行以下某项操作：

- 要添加新路由，请点击 **+**。
- 点击要编辑的路由的编辑图标 ()。

如果不再需要路由，请点击该路由的垃圾桶图标将其删除。

步骤 4 配置路由属性。

- **名称 (Name)** - 路由的显示名称。
- **说明** - 路由目的的可选说明。
- **接口** - 选择要通过其发送流量的接口。通过此接口需能够访问网关地址。

  对于网桥组，您应为网桥组接口 (BVI) 而不是为成员接口配置路由。

  如果已启用虚拟路由与转发，则可以选择属于其他虚拟路由器的接口。如果在虚拟路由器中创建用于不同虚拟路由器中接口的静态路由，该路由将跨越虚拟路由器边界，且存在来自该虚拟路由器的流量泄漏到另一个虚拟路由器的风险。这可能是期望的结果，但请仔细确定您是否需要此路由泄漏。选择接口时，接口所属的虚拟路由器的名称将显示在接口右侧。
- **协议** - 选择路由是用于 **IPv4** 地址，还是用于 **IPv6** 地址。
- **网络** - 选择标识目标网络或主机（应使用此路由中的网关）的网络对象。

  要定义默认路由，请使用预定义的 any-ipv4 或 any-ipv6 网络对象，或创建一个适用于 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 网络的对象。
- **网关** - 选择标识网关 IP 地址的主机网络对象。流量将发送至此地址。您无法将同一个网关用于多个接口上的路由。

  如果要在虚拟路由器中定义路由，且该接口属于不同的虚拟路由器，则必须将该网关留空。系统会将通往这些网络的流量路由至另一个虚拟路由器，然后使用目标虚拟路由器的路由表来确定网关。
- **度量** - 路由的管理距离，该值介于 1 和 254 之间。静态路由的默认值为 1。如果接口和网关之间还有其他路由器，请输入跳数作为管理距离。

  管理距离是用于比较路由的参数。数字越小，为该路由指定的优先级越高。连接的路由（直连到设备接口的网络）始终优先于静态路由。

步骤 5 （可选；仅限 IPv4 路由。）选择应跟踪此路由的生存能力的 **SLA 监控器**。

SLA 监控器可验证目标网络上始终可用的主机是否可访问。如果无法访问，则系统可以安装备份路由。因此，如果配置 SLA 监控器，则还应为此网络配置另一个具有更大度量指标的静态路由。例

如，如果此路由的度量指标为 1，请创建一个指标为 10 的备份路由。有关详细信息，请参阅备份静态路由和静态路由跟踪，第 308 页。

如果 SLA 监控器对象尚不存在，请点击列表底部的**创建 SLA 监控器**链接，立即创建对象。

注释　如果由于无法对受监控的地址进行 ping 操作而删除受监控路由，则会在静态路由表中指示该路由，并显示一条警告，指出该路由无法访问。确定问题是暂时的还是需要重新配置路由。考虑路由可行的概率，但受监控地址不够可靠。

步骤 6　点击**确定 (OK)**。

配置 SLA 监控器对象

配置服务级别协议 (SLA) 监控对象，以与静态路由配合使用。通过使用 SLA 监控，您可以跟踪静态路由的运行状况，并自动使用新路由替换故障路由。有关路由跟踪的详细信息，请参阅备份静态路由和静态路由跟踪，第 308 页。

选择监控目标时，您需要确保它能够响应 ICMP 回应请求。目标可以是主机网络对象中定义的任何 IP 地址，但您应考虑使用以下地址：

- ISP 网关地址（用于支持双 ISP）。
- 下一跳网关地址，如果您关注网关的可用性。
- 目标网络上的服务器，例如系统需要与之进行通信的系统日志服务器。
- 目标网络上的持久性 IP 地址。可能会在夜间关闭的工作站不是一个理想选择。

过程

步骤 1　选择**对象**，然后从目录中选择 **SLA 监控**。

步骤 2　执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3　输入对象的名称和说明（后者为可选项）。

步骤 4　定义 SLA 监控器所需选项：

- **监控地址** - 选择定义目标网络上待监控地址的主机网络对象。如果所需的对象不存在，可以点击**创建新网络 (Create New Network)**。

  仅当将 SLA 监控器附加至静态路由后，才会监控该地址。

- **目标接口** - 选择用于发送回应请求数据包的接口。这通常是您将在其上定义静态路由的接口。接口源地址用作回应请求数据包中的源地址。

步骤 5 （可选。）调整 **IP ICMP 回应选项**。

所有 ICMP 选项均具有适用于大多数情况的默认设置，但可以对其进行调整以满足您的要求。

- **阈值** - 要声明的上升阀值的毫秒数，在 0 到 2147483647 之间。默认值为 5000（5 秒）。该值不应大于为超时设置的值。阈值仅用于指示超出阈值事件，这不会影响可达性。您可以使用阈值事件的发生频率来评估超时设置。
- **超时** - 在收到请求数据包的响应之前，路由监控操作应等待的时间（以毫秒为单位），在 0 到 604800000 毫秒（7 天）之间。默认值为 5000 毫秒（5 秒）。如果在此期间，监控器有至少一个回应请求未得到响应，此过程将会安装备份路由。
- **频率** - SLA 探测之间的毫秒数，从 1000 到 604800000，以 1000 的倍数表示。设置的频率不可小于超时时间。默认值为 60000 毫秒（60 秒）。
- **服务类型** - 定义 ICMP 回应请求数据包 IP 报头中服务类型 (ToS) 的整数，在 0 到 255 之间。默认值为 0。
- **数据包数量** - 每次轮询中要发送的数据包的数量，在 1 到 100 之间。默认为 1 个数据包。
- **数据量** - 回应请求数据包中使用的数据负载的大小，在 0 到 16384 字节之间。默认值为 28。此设置仅指定负载的大小；不指定整个数据包的大小。

步骤 6 点击**确定 (OK)**。

您现在可以在静态路由中使用 SLA 监控对象。

配置 ECMP 流量区域

通常，如果要使用相同的路由度量为特定网络前缀配置多条路由，您需要在同一接口上配置路由。因此，系统使用等价多路径 (ECMP) 路由计算来平衡通过接口发送到网关的流量。

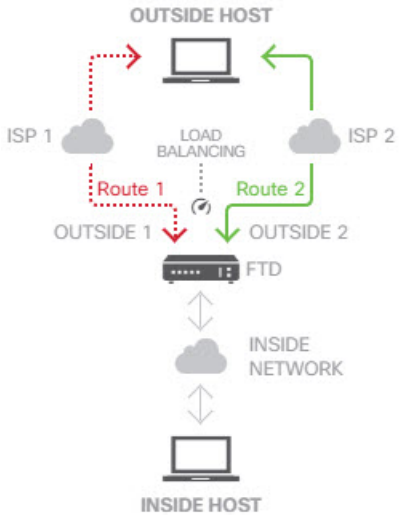
例如，您可以在外部接口上配置多个指定不同网关的默认路由，系统允许这种配置而无需执行其他更改：

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

您还可以使用 ECMP 为同一网络前缀和路由度量在多个接口（虚拟路由器内）之间平衡流量。如果可通过单独的接口访问网关，则需要进行此配置。例如，假设您有两个ISP，并且希望在ISP之间平衡负载，但不希望在 ISP 网关之间划分内部地址空间。可通过 outside1 接口访问一个 ISP，通过 outside2 接口访问另一个 ISP。要实现此目的，您需要创建一个包含 outside1 和 outside2 接口的路由流量区域。

```
isp-zone containing outside1 and outside2
```

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.1.1.3
```



注释 ECMP 路由流量区域与安全区无关。创建包含 outside1 和 outside2 接口的安全区不会实现用于 ECMP 路由的流量区域。

以下程序介绍如何配置 ECMP 区域以利用跨接口的 ECMP 处理。

过程

步骤 1 点击**设备**，然后点击**路由**摘要中的链接。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置静态路由的路由器的查看图标 ( )。

步骤 3 点击 **ECMP 流量区域**选项卡。

步骤 4 在 **ECMP 流量区域 (ECMP Traffic Zones)** 页面上，执行以下一项操作：

- 要添加新区域，请点击 **+** 或**添加 ECMP 流量区域**。
- 点击要编辑的区域的编辑图标 ( )。

如果不再需要某个区域，请点击该区域的垃圾桶图标将其删除。必须先删除依赖于区域的所有静态路由，然后才能删除区域。

步骤 5 为区域输入**名称**和说明（后者为可选项）。

步骤 6 选择最多 8 个**接口**以包含在区域中：

- 点击 **+** 添加接口。
- 点击接口右侧的 **x** 以将其删除。

在选择接口时，请记住以下限制：

- 您可以选择物理接口、子接口和 EtherChannel。
- ECMP 流量区域不能包括以下类型的接口：网桥组 (BVI) 或其成员、EtherChannel 成员接口、HA 接口（故障转移或状态链路）、纯管理接口、虚拟隧道接口 (VTI) 或配置用于 VPN 管理访问的接口。
- 不能包含用于远程访问或站点间 VPN 连接的接口。
- 无论是作为服务器还是代理，都不能选择为 DHCP 中继启用的接口。
- 接口必须分配给同一虚拟路由器。
- 一个接口只能位于一个流量区域中。

步骤 7 点击**确定**。

下一步做什么

现在，您可以转至“静态路由”选项卡，并为同一目的地创建通过这些接口的等价路由。或者，如果通过系统分发等价路由，则动态路由协议可以自动配置等价路由。

监控路由

要对路由进行监控和故障排除，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。您还可以从“路由”(Routing) 页面的**命令 (Commands)** 菜单选择其中一些命令。

- **show route** 显示数据接口的路由表，包括直连网络的路由。
- **show ipv6 route** 显示数据接口的 IPv6 路由表，包括直连网络的路由。
- **show network** 显示管理接口的配置，包括管理网关。通过管理接口的路由不由数据接口路由表处理，除非您指定数据接口作为管理网关。
- **show network-static-routes** 显示使用 **configure network static-routes** 命令为管理接口配置的静态路由。通常不会有任何静态路由，因为在大多数情况下，管理网关足以支持管理路由。这些路由不可用于数据接口上的流量。该命令在 CLI 控制台中不可用。
- **show ospf** 显示有关 OSPF 进程和已获知路由的信息。使用 **show ospf ?** 获取可包含的选项列表，以查看有关 OSPF 的特定信息。
- **show bgp** 显示有关 BGP 进程和已获知路由的信息。使用 **show bgp ?** 获取可包含的选项列表，以查看有关 BGP 的特定信息。
- **show eigrp** 选项显示有关 EIGRP 进程和已获知路由的信息。使用 **show eigrp ?** 获取您可以包含的选项列表；您必须提供一个选项。
- **show isis** 选项显示有关 IS-IS 进程和已获知路由的信息。使用 **show isis ?** 获取您可以包含的选项列表；您必须提供一个选项。

- **show rip database** 显示有关 RIP 进程和已获知路由的信息。
- **show vrf** 显示有关系统上定义的虚拟路由器的信息。
- **show zone** 显示有关 ECMP 流量区域的信息，包括属于每个区域的接口。

第 13 章

虚拟路由器

可以创建虚拟路由器来隔离接口子集之间的流量。

关于虚拟路由器和虚拟路由与转发 (VRF)

可以创建多个虚拟路由器来为接口组维护单独的路由表。由于每个虚拟路由器都有自己的路由表，因此您可以完全分隔流经设备的流量。

因此，您可以通过一组通用的网络设备为两个或多个不同的客户提供支持。您还可以使用虚拟路由器为自身网络的元素提供更多隔离，例如，将开发网络与一般用途的企业网络隔离。

虚拟路由器将实施虚拟路由和转发功能的“轻型”版本（或 VRF Lite），它不支持 BGP 的多协议扩展 (MBGP)。

创建虚拟路由器时，您需要为路由器分配接口。您可以将给定接口分配给一个且仅有一个虚拟路由器。然后即可定义静态路由，并为每个虚拟路由器配置路由协议（例如 OSPF 或 BGP）。还可在整个网络中配置单独的路由进程，以便所有参与设备的路由表都使用每个虚拟路由器相同的路由进程和表。使用虚拟路由器，可在同一物理网络上创建逻辑分隔的网络，以确保流经每个虚拟路由器的流量的隐私。

由于路由表独立存在，因此可以在虚拟路由器上使用相同或重叠的地址空间。例如，可以将 192.168.1.0/24 地址空间用于两个独立的虚拟路由器，分别由两个独立物理接口提供支持。

请注意，每个虚拟路由器有单独的管理和数据路由表。例如，如果将管理专用接口分配给虚拟路由器，则该接口的路由表会与分配给虚拟路由器的数据接口分离开来。

配置策略以感知虚拟路由器

创建虚拟路由器时，该虚拟路由器的路由表会自动与全局虚拟路由器或任何其他虚拟路由器分离开来。但是，安全策略不会自动识别虚拟路由器。

例如，如果编写适用于“任何”源或目标安全区的访问控制规则，则该规则将应用于所有虚拟路由器上的所有接口。这实际上可能正是您所希望得到的结果。例如，可能所有客户都想阻止访问相同系列的令人反感的 URL 类别。

但是，如果需要仅向其中一个虚拟路由器应用策略，则需要创建仅包含来自该单一虚拟路由器的接口的安全区。然后，在安全策略的源和目标条件中使用虚拟路由器限制的安全区。

通过使用其成员身份限制为分配给单个虚拟路由器的接口的安全区，您可以在以下策略中编写虚拟路由器感知规则：

- 访问控制策略。
- 入侵和文件策略。
- SSL 解密策略。
- 身份策略和用户到 IP 地址映射。如果在虚拟路由器中使用重叠地址空间，请确保为每个虚拟路由器创建单独的领域，并在身份策略规则中正确应用。

如果在虚拟路由器中使用重叠地址空间，则应使用安全区确保应用适当的策略。例如，如果在两个单独的虚拟路由器中使用 192.168.1.0/24 地址空间，则指定 192.168.1.0/24 网络的访问控制规则将应用于两个虚拟路由器中的流量。如果这不是期望的结果，您可以通过只为其中一个虚拟路由器指定源/目标安全区来限制该规则的应用。

对于不使用安全区的策略（例如 NAT），您可以通过选择分配给单个虚拟路由器的接口作为源接口和目标接口来编写虚拟路由器的特定规则。如果从两个独立的虚拟路由器中选择源接口和目标接口，则必须确保虚拟路由器之间具有适当的路由，以确保规则正常工作。

在虚拟路由器之间路由

您可以配置静态路由来路由虚拟路由器之间的流量。

例如，如果您在全局虚拟路由器中设有外部接口，则可以在每个其他虚拟路由器中设置静态默认路由，以将流量发送到该外部接口。然后，无法在给定虚拟路由器内路由的任何流量将被发送到全局路由器，以进行后续路由。

虚拟路由器之间的静态路由被称为路由泄漏，这是因为您会将流量泄漏到其他虚拟路由器。泄漏路由（例如，VR1 路由到 VR2）时，可以仅发起从 VR2 到 VR1 的连接。要使流量从 VR1 流向 VR2，必须配置反向路由。当您为另一个虚拟路由器中的接口创建静态路由时，不需要指定网关地址，而只需选择目标接口。

对于虚拟路由器间路由，系统会在源虚拟路由器中查找目标接口。然后，系统会查找目标虚拟路由器中下一跳的MAC地址。因此，目标虚拟路由器必须具有用于目标地址的所选接口的动态（获知）或静态路由。

通过配置将在不同虚拟路由器中使用源接口和目标接口的NAT规则，还允许在虚拟路由器之间路由流量。如果未选择NAT进行路由查找的选项，则每当发生目标转换时，规则就会将流量从目标接口发送到 NATed 地址。但是，目标虚拟路由器应具有一个已转换目标 IP 地址的路由，以便下一跳查找可以取得成功。

按设备型号划分的最大虚拟路由器数量

可以创建的最大虚拟路由器数量取决于设备型号。下表列出了最大限制。您可以通过输入 **show vrf counters** 命令对系统进行复核，该命令显示该平台的用户定义最大虚拟路由器数量（不包括全局虚拟路由器）。下表中的数字包括用户和全局路由器。对于 Firepower 4100/9300，这些数字适用于原生模式。

对于支持多实例功能的平台（例如 Firepower 4100/9300），通过以下方式确定每个容器实例的最大虚拟路由器数：将最大虚拟路由器数除以设备上的核心数，然后乘以分配给该实例的核心数，并四舍五入到最接近的整数。例如，如果平台最多支持 100 个虚拟路由器，并且它有 70 个核心，则每个核心最多支持 1.43 个虚拟路由器（四舍五入为一个）。因此，分配有 6 个核心的实例将支持 8.58 个虚拟路由器（四舍五入为 8 个），分配有 10 个核心的实例将支持 14.3 个虚拟路由器（四舍五入为 14 个）。

设备型号	最大虚拟路由器数量
Firepower 1010	此型号不支持虚拟路由器。
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Firepower 2110	10
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Secure Firewall 3105	10
Secure Firewall 3110	15
Secure Firewall 3120	25
Secure Firewall 3130	50
Secure Firewall 3140	100
Firepower 4112	60
Firepower 4115	80
Firepower 4125	100

设备型号	最大虚拟路由器数量
Firepower 4145	100
Firepower 9300 设备，所有型号	100
Threat Defense Virtual，所有平台	30
ISA 3000	10

虚拟路由器准则

设备型号准则

您可以在所有支持的设备型号上配置虚拟路由器，但以下情况除外：

- Firepower 1010

其他准则

- 您只能在全局虚拟路由器上配置以下功能：
  - OSPFv3
  - RIP
  - EIGRP
  - IS-IS
  - BGPv6
  - 组播路由
  - 基于策略的路由
  - VPN
- 您可以为每个虚拟路由器单独配置以下功能：
  - 静态路由及其 SLA 监控器。
  - OSPFv2
  - BGPv4
- 当查询或与远程系统通信时，系统会使用以下功能（传出流量）。这些功能仅使用全局虚拟路由器中的接口。如果为该功能配置了接口，则接口必须属于全局虚拟路由器。一般情况下，无论何时，系统出于管理目的必须查找连接外部服务器的路由，它会在全局虚拟路由器中执行路由查找。

  - DNS服务器用于解析访问控制规则中使用的完全限定名称，或解析**ping**命令的名称。如果指定 **any** 作为 DNS 服务器的接口，则系统仅考虑全局虚拟路由器中的接口。
  - 用于 VPN 的 AAA 服务器或身份领域。您只能在全局虚拟路由器的接口上配置 VPN，因此用于 VPN 的外部 AAA 服务器（如 Active Directory）必须可通过全局虚拟路由器中的接口访问。
  - 系统日志服务器。
  - SNMP。

- 在 NAT 中，如果指定将分配给不同虚拟路由器的源接口和目标接口，NAT 规则将通过一个虚拟路由器转移另一个虚拟路由器的流量。确保不会无意中混合NAT规则中的接口。通常将使用源接口和目标接口，并忽略路由表，包括手动 NAT 中的目标转换。但是，如果 NAT 规则确实需要执行路由查找，则仅在VRF表中查找入站接口。如有必要，请在源虚拟路由器中为目标接口定义静态路由。请注意，如果将接口保留为 **any**，则该规则适用于所有接口，而不考虑虚拟路由器成员关系。使用虚拟路由器时，请仔细测试NAT规则，以确保实现预期行为。如果您忘记定义所需的路由泄漏，在某些情况下，该规则将不会匹配您预期匹配的所有流量，并且不会应用转换。
- 如果您配置虚拟路由器间路由，例如，将路由从一个虚拟路由器泄漏到另一个虚拟路由器，则系统会在源虚拟路由器中查找目标接口。然后，系统会查找目标虚拟路由器中下一跳的 MAC 地址。因此，目标虚拟路由器必须具有用于目标地址的所选接口的动态（获知）或静态路由。
- 使用从虚拟路由器 1 到虚拟路由器 2（例如）的虚拟路由器间路由（泄漏路由）时，不需要在虚拟路由器 2 中配置镜像（反向）路由以允许返回流量。但是，如果要允许在两个方向上发起连接，请确保在两个方向上（从虚拟路由器 1 到 2 以及从虚拟路由器 2 到 1）泄漏路由。
- 如果将接口从一个虚拟路由器移至另一个虚拟路由器，则会保留已为该接口配置的所有功能。检查配置，以确保静态路由、IP 地址和其他策略在新虚拟路由器的环境中有意义。
- 如果在多个虚拟路由器中使用重叠地址空间，请注意，从思科身份服务引擎 (ISE) 下载的静态安全组标签 (SGT) 到 IP 地址的映射不会感知虚拟路由器。如果需要为每个虚拟路由器创建不同的SGT映射，请为每个虚拟路由器设置单独的身份领域。如果打算将相同的IP地址映射到各个虚拟路由器中的相同 SGT 编号，则无需执行此操作。
- 如果在多个虚拟路由器中使用重叠地址空间，控制面板数据可能具有误导性。与相同IP地址的连接将会汇聚，因此，当两个或多个终端共享给定地址时，系统显示与该地址之间的往来流量更多。如果使用单独的身份领域仔细构建身份策略，则基于用户的统计信息应更准确。
- 不能在单独的虚拟路由器中使用重叠的 DHCP 地址池。
- 只能在全局虚拟路由器中的接口上使用 DHCP 服务器自动配置。为用户定义的虚拟路由器分配的接口不支持自动配置功能。
- 如果在虚拟路由器之间移动接口（包括从全局虚拟路由器移至新路由器），将删除为该接口定义的任何现有连接。
- 安全智能策略不会感知虚拟路由器。如果将 IP 地址、URL 或 DNS 名称添加到阻止列表，则会被所有虚拟路由器阻止。

管理虚拟路由器

您可以创建多个虚拟路由与转发（VRF）实例（称为虚拟路由器），以便为接口组维护单独的路由表。由于每个虚拟路由器都有自己的路由表，因此您可以完全分隔流经设备的流量。

因此，您可以通过一组通用的网络设备为两个或多个不同的客户提供支持。您还可以使用虚拟路由器为自身网络的元素提供更多隔离，例如，将开发网络与一般用途的企业网络隔离。

默认情况下，虚拟路由已禁用。整个设备使用一组全局路由表，用于数据（通过）和管理（传入/传出）流量。

启用虚拟路由时，初始路由页面显示系统定义的虚拟路由器的列表。如果不启用虚拟路由器，则初始路由页面显示系统定义的静态路由的列表。

始终有一个全局虚拟路由器。全局路由器保留尚未分配给单个虚拟路由器的所有接口。

过程

步骤 1 点击**设备**，然后点击**路由**摘要中的链接。

步骤 2 如果尚未启用虚拟路由器，请点击**添加多个虚拟路由器**链接，然后点击**创建第一个自定义虚拟路由器**。

创建第一个虚拟路由器在本质上与创建任何附加虚拟路由器的方式基本相同。有关详细信息，请参阅创建虚拟路由器或编辑接口分配，第 323 页。

步骤 3 执行以下任一操作：

- 要配置适用于所有虚拟路由器的全局 BGP 设置，请点击 **BGP 全局设置**按钮。您可以使用 Smart CLI 配置这些设置，如配置 Smart CLI 对象，第 820 页中所述。只有在一个或多个虚拟路由器中配置 BGP 时，才需要配置全局 BGP 设置。
- 要创建新的虚拟路由器，请点击表上方的 **+** 按钮。
- 要编辑虚拟路由器的路由属性（例如，创建静态路由或定义路由进程），请在虚拟路由器的“操作”单元格中点击查看图标 ( )。
- 要编辑虚拟路由器的名称、说明或接口分配，请在虚拟路由器的“操作”单元格中点击查看图标 ( )，然后选择**虚拟路由器属性**选项卡。
- 要在查看虚拟路由器时进行切换，请点击虚拟路由器名称（位于路由表上方）旁边的向下箭头，然后选择所需的虚拟路由器。点击**返回虚拟路由器 (Go Back to Virtual Routers)** 箭头 ( ) 返回到列表页面。
- 要删除虚拟路由器，请在虚拟路由器的“操作”单元格中点击删除图标 ( )，或在查看虚拟路由器的内容时，点击虚拟路由器名称旁边的删除图标。删除最后一个虚拟路由器（全局路由器除外，因为您无法删除）时，将禁用 VRF。

- 要监控虚拟路由器中的路由，请为该虚拟路由器点击表中的**show**命令之一的链接。点击该命令将打开 CLI 控制台，您可以在其中检查 CLI 命令的输出。显示有关路由、OSPF 和 OSPF 邻居的信息。请注意，命令输出基于已部署的配置；无法查看任何与未部署的编辑相关的内容。

  查看虚拟路由器时，您还可以通过从**命令**下拉列表中选择命令来执行这些命令。

创建虚拟路由器或编辑接口分配

在虚拟路由器上配置静态路由或路由进程之前，您必须先创建路由器并向其分配接口。

开始之前

转至**接口 (Interfaces)**页面，确保要添加到虚拟路由器的每个接口都具有名称。只能将具有名称的接口添加至虚拟路由器。

过程

步骤 1 点击 **设备 (Device)** > **路由 (Routing)**。

步骤 2 执行以下操作之一：

- 如果尚未创建虚拟路由器，请点击**添加多个虚拟路由器 (Add Multiple Virtual Routers)** 链接，然后点击**创建第一个自定义虚拟路由器 (Create First Custom Virtual Router)**
- 点击虚拟路由器列表上方的 + 按钮以新建虚拟路由器。
- 点击虚拟路由器的编辑图标 () 以编辑属性和接口列表。
- 查看虚拟路由器时，点击**虚拟路由器属性 (Virtual Router Properties)** 选项卡，以编辑您正在查看的虚拟路由器的属性。
- 查看虚拟路由器时，点击虚拟路由器名称旁边的向下箭头，然后点击**新建虚拟路由器 (Create New Virtual Router)**。

步骤 3 配置虚拟路由器的属性：

- **名称** - 虚拟路由器名称。
- **说明** - 虚拟路由器的可选说明。
- **接口** - 点击 **+** 选择应属于虚拟路由器的各个接口。要删除接口，请将鼠标悬停在接口上，然后点击接口卡右侧的 **X** 。您可以将物理接口、子接口和 Etherchannel 分配给虚拟路由器，但不能分配给 VLAN。

  除非您有意将其他接口的路由泄漏到虚拟路由表中，否则路由表将限制为这些接口。

步骤 4 点击**确定 (OK)**或**保存 (Save)**。

您将转到此虚拟路由器的视图，然后在其中配置静态路由或路由进程。

在虚拟路由器中配置静态路由和路由进程

每个虚拟路由器都具有自己的静态路由和路由进程，它们将独立于为任何其他虚拟路由器定义的路由和路由进程运行。

配置静态路由时，可以选择该虚拟路由器以外的目标接口。这会将路由泄漏到包含目标接口的虚拟路由器。确保只泄漏需要泄漏的路由，以确保发送的流量不会超过您想要发往其他虚拟路由器的流量。例如，如果您有一条连接互联网的路径，则有必要将每个虚拟路由器的路由泄漏到面向互联网的虚拟路由器，以便将流量发往互联网。

过程

步骤 1 选择**设备** > **路由**。

步骤 2 在虚拟路由器的“操作”(Action) 单元格中点击查看图标 () 以打开虚拟路由器。

步骤 3 执行以下任一操作：

- 要配置静态路由，请点击**静态路由 (Static Routing)** 选项卡，然后创建或编辑路由。有关详细信息，请参阅配置静态路由，第 309 页。
- 要配置等价多路径 (ECMP) 流量区域，请点击 **ECMP 流量区域 (ECMP Traffic Zones)** 选项卡，然后创建区域。有关详细信息，请参阅配置 ECMP 流量区域，第 312 页。
- 要配置 BGP 路由进程，请点击 **BGP** 选项卡，然后创建定义该进程所需的 Smart CLI 对象。有关详细信息，请参阅边界网关协议 (BGP)，第 395 页。

  还有适用于所有虚拟路由器的 BGP 全局设置。必须返回“虚拟路由器列表”页面，点击 **BGP 全局设置 (BGP Global Settings)** 按钮来配置这些属性。
- 要配置 OSPF 路由进程，请点击 **ospf** 选项卡，然后创建定义最多 2 个进程所需的 Smart CLI 对象及其关联的接口配置。有关详细信息，请参阅开放最短路径优先 (OSPF)，第 359 页。
- （仅限全局虚拟路由器。）要配置 EIGRP 路由进程，请点击 **EIGRP** 选项卡，然后创建定义单个进程所需的 Smart CLI 对象。有关详细信息，请参阅增强型内部网关路由协议 (EIGRP)，第 379 页。

删除虚拟路由器

如果不再需要虚拟路由器，可以将其删除。不能删除全局虚拟路由器。

删除虚拟路由器时，您将删除该虚拟路由器中配置的所有静态路由和路由进程。

分配给虚拟路由器的所有接口都将重新分配给全局路由器。

过程

步骤 1 选择**设备** > **路由**。

步骤 2 执行以下操作之一：

- 在虚拟路由器列表中，请在虚拟路由器的“操作”列中点击删除图标 ()。
- 查看要删除的虚拟路由器时，请点击路由器名称旁边的删除图标 ()。

系统提示您确认要删除虚拟路由器。

步骤 3 点击**确定**，确认删除。

虚拟路由器示例

以下主题提供了一些关于实施虚拟路由器的示例。

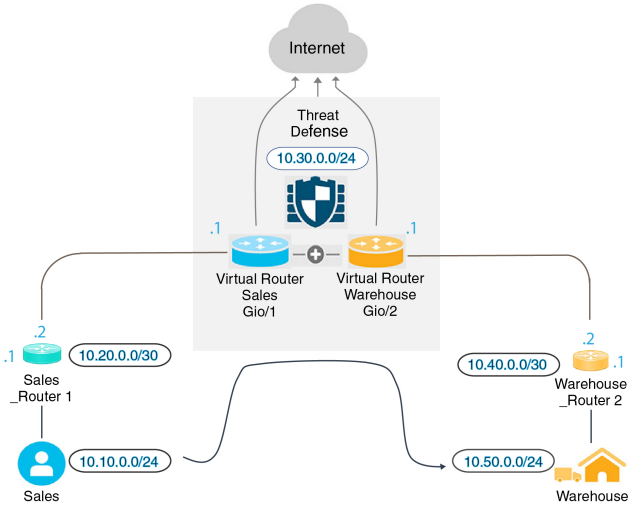
相关主题

如何通过站点间 VPN 保护来自多个虚拟路由器的网络流量，第 649 页
如何对不同虚拟路由器中的内部网络进行 RA VPN 访问，第 718 页

如何通过多个虚拟路由器路由到远程服务器

使用虚拟路由器时，您可能会遇到一种情况，即一个虚拟路由器中的用户需要访问只能通过单独虚拟路由器进行访问的服务器。

以下图为例。销售团队的工作站连接到“销售”虚拟路由器。仓库服务器通过“仓库”虚拟路由器连接。如果销售团队需要在 IP 地址为 10.50.0.5/24 的仓库服务器上查找信息，则需要泄漏从“销售”虚拟路由器到“仓库”虚拟路由器的路由。“仓库”虚拟路由器还必须具有通往仓库服务器的路由，该服务器在仓库路由器 2 之后多跳。



开始之前

此示例假定您已：

- 在 威胁防御 设备上配置“销售”和“仓库”虚拟路由器，其中 GigabitEthernet 0/1 分配给“销售”虚拟路由器，GigabitEthernet 0/2 分配给“仓库”虚拟路由器。
- 销售路由器 1 具有静态或动态路由，用于将流量从 10.20.0.1/30 接口发送到 10.50.0.5/24。

过程

步骤 1 为 10.50.0.5/24 或 10.50.0.0/24 创建网络对象。此外，为网关 10.40.0.2/30 创建对象。

如果要将路由限制为仓库服务器的单个 IP 地址，请使用主机对象来定义 10.50.0.5。或者，如果销售团队应有权访问仓库中的其他系统，则为 10.50.0.0/24 网络创建网络对象。在本例中，我们将为主机 IP 地址创建路由。

a) 选择**对象**，然后从目录中选择**网络**。

b) 点击 **+**，然后填写仓库服务器的对象属性：

c) 点击**确定**。

d) 点击 +，然后填入仓库网络的路由器网关的对象属性：

e) 点击**确定**。

步骤 2 定义指向“仓库”虚拟路由器中 Gi0/2 接口的“销售”虚拟路由器中的路由泄漏。

在本例中，Gi0/1 命名为“inside”，Gi0/2 命名为“inside-2”。

a) 选择**设备**，然后点击**路由**摘要中的**查看配置**。

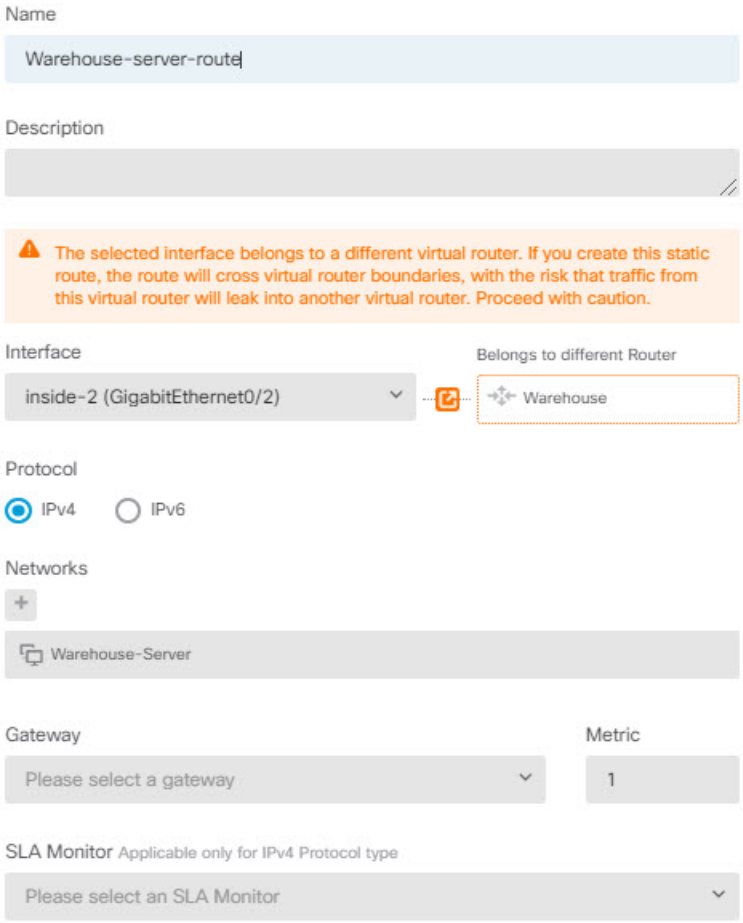
b) 在虚拟路由器列表中，请在“销售”虚拟路由器的操作列中点击查看图标 ( )。

c) 在**静态路由**选项卡上，点击 + 并配置路由：

- **名称** - 任何名称，例如 Warehouse-server-route。
- **接口** - 选择 **inside-2**。您将看到一条警告，指出接口位于不同的路由器中，并且您将创建路由泄漏。这是您需要执行的操作。
- **协议** - 在本例中，使用 **IPv4**。您也可以使用 IPv6 地址来实现此示例。
- **网络** - 选择 Warehouse-Server 对象。

- **网关** - 将此项目留空。将路由泄漏到另一个虚拟路由器时，您不必选择网关地址。

对话框应如下所示：

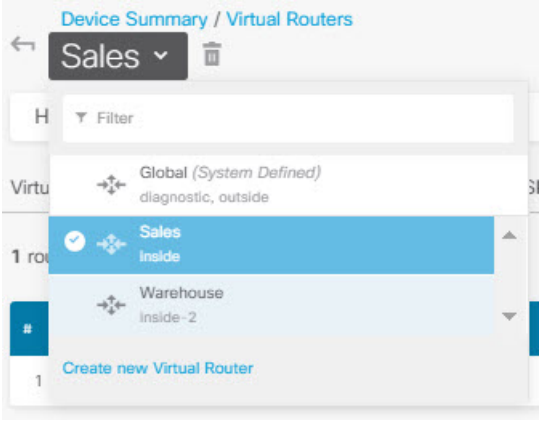


d) 点击**确定**。

步骤 3 在“仓库”虚拟路由器中，定义指向仓库路由器 2 网关的路由。

或者，可以通过配置将动态发现仓库路由器 2 路由的路由协议来完成此操作。在本例中，我们将定义静态路由。

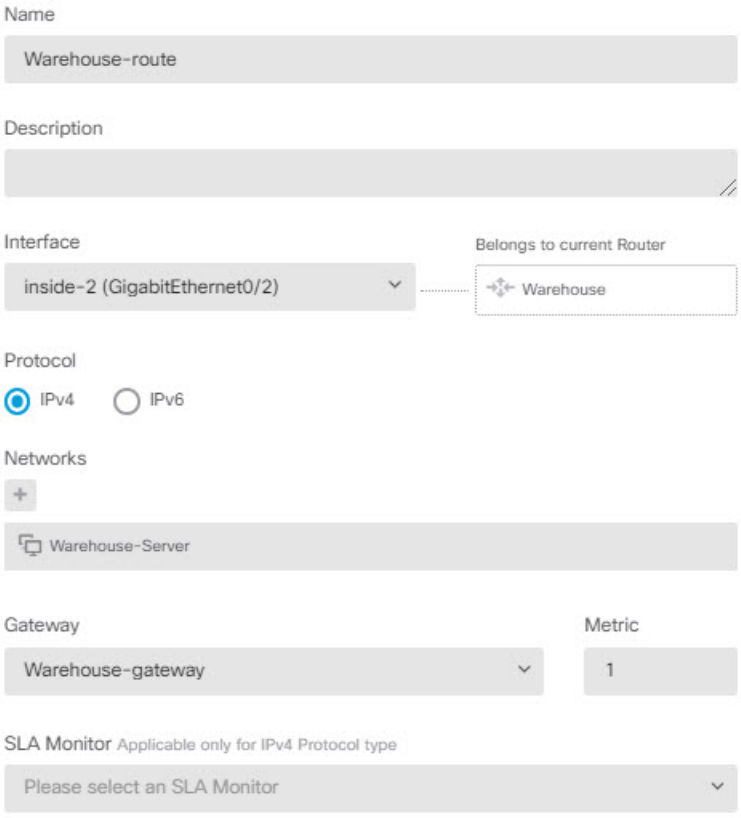
a) 从当前名为“销售”的虚拟路由器下拉列表中，选择“仓库”虚拟路由器以交换路由器。



b) 在**静态路由**选项卡上，点击 + 并配置路由：

- **名称** - 任何名称，例如 Warehouse-route。
- **接口** - 选择 **inside-2**。
- **协议** - 选择 **IPv4**。
- **网络** - 选择 Warehouse-Server 对象。
- **网关** - 选择 Warehouse-gateway 对象。

对话框应如下所示：

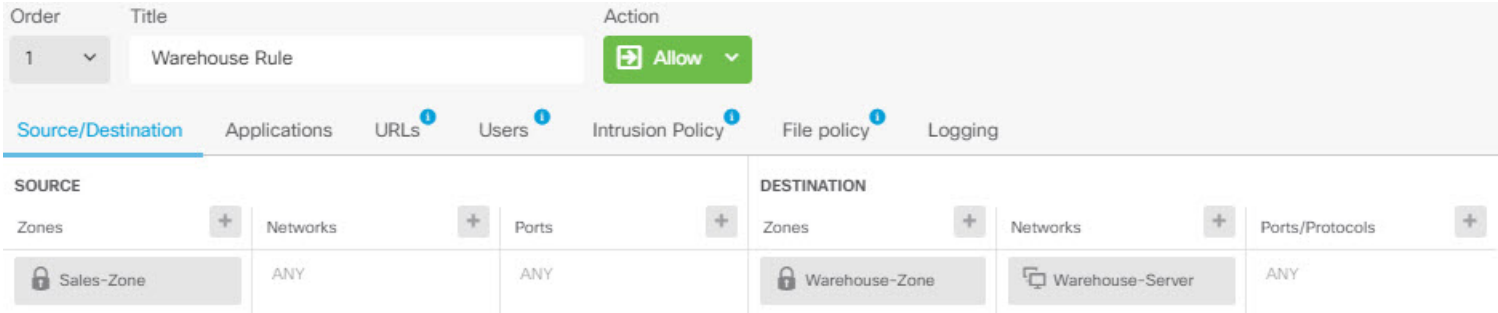


c) 点击**确定**。

步骤 4 确保存在允许访问仓库服务器的访问控制规则。

最简单的规则将允许从“销售”虚拟路由器中的源接口到目标 Warehouse-Server 网络对象的“仓库”虚拟路由器中的目标接口的流量。您可以根据需要对流量应用入侵检测。

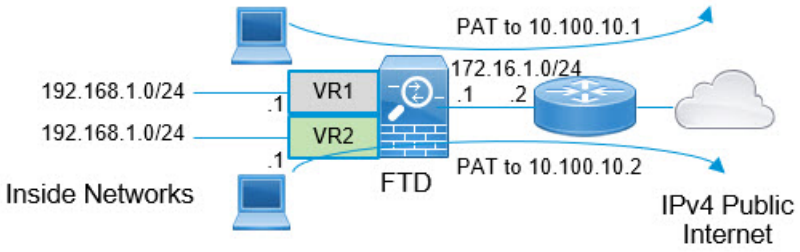
例如，如果“销售”虚拟路由器中的接口位于“销售区域”安全区中，而“仓库”虚拟路由器中的接口位于“仓库区域”安全区中，则访问控制规则将如下所述：



如何提供对包含重叠地址空间的多个虚拟路由器的互联网访问权限

使用虚拟路由器时，您可以为驻留在单独路由器中的多个接口设置相同的网络地址。例如，可以将 inside 和 inside-2 接口定义为均使用 IP 地址 192.168.1.1/24，从而将终端托管在其在 192.168.1.0/24 网络中的分段上。但是，由于在这些单独虚拟路由器中路由的 IP 地址相同，因此您需要认真处理流出虚拟路由器的流量，以确保返回流量流向正确目标地址。

例如，要允许通过两个使用相同地址空间的虚拟路由器访问互联网，您需要将 NAT 规则分别应用于每个虚拟路由器中的接口，最好使用单独的 NAT 或 PAT 池。可以使用 PAT 将虚拟路由器 1 中的源地址转换为 10.100.10.1，并将虚拟路由器 2 中的源地址转换为 10.100.10.2。下图显示了此设置，其中面向互联网的外部接口是全局路由器的一部分。请注意，必须使用明确选择的源接口来定义 NAT/PAT 规则，因为使用“任何”作为源接口将使系统无法识别正确源，这是因为两个不同的接口上可能存在相同的 IP 地址。



注释 此示例已简化，其中每个虚拟路由器包含一个接口。如果“内部”虚拟路由器配有多个接口，则需要为每个“内部”接口创建 NAT 规则。即使您拥有不使用重叠地址空间的虚拟路由器中的一些接口，通过在 NAT 规则中明确标识源接口，也可以简化故障排除过程，并确保更加清楚地区分来自与互联网绑定的各虚拟路由器之间的流量。

过程

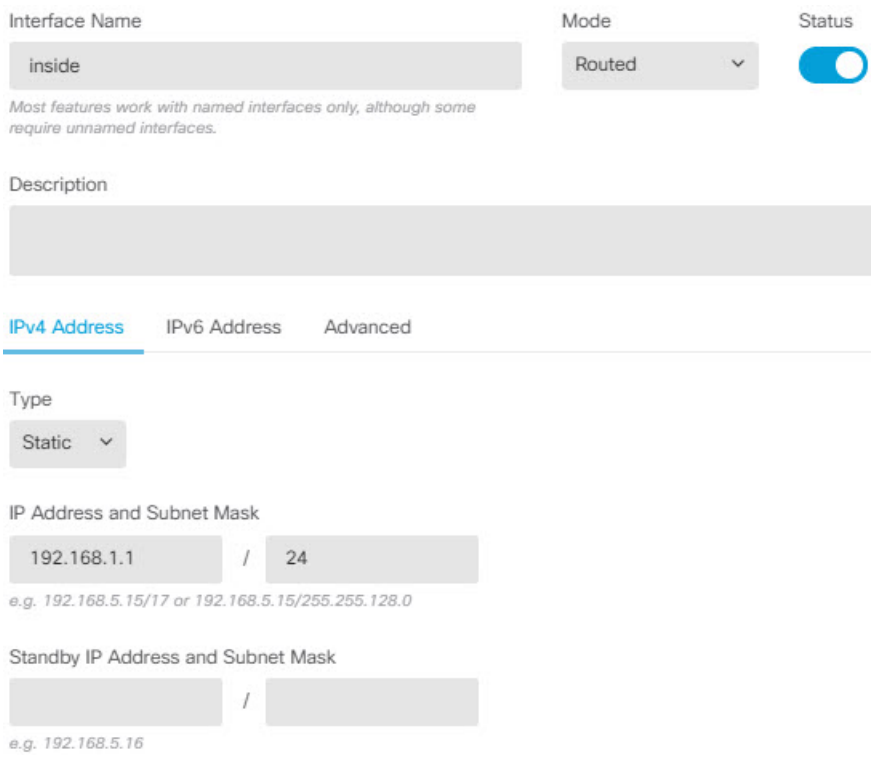
步骤 1 为虚拟路由器 1 (VR1) 配置内部接口。

a) 点击**设备 (Device)**，然后点击**接口 (Interface)** 摘要中的**查看所有接口 (View All Interfaces)**。

b) 对于将分配给 VR1 的接口，在“操作”(Action) 列中点击编辑图标 ( )。

c) 至少配置以下属性：

- **名称** - 在本例中为 **inside**。
- **模式** - 选择**路由**。
- **状态** - 启用接口。
- **IPv4 地址** > **类型** - 选择**静态**。
- **IPv4 地址和子网掩码** - 输入 192.168.1.1/24。



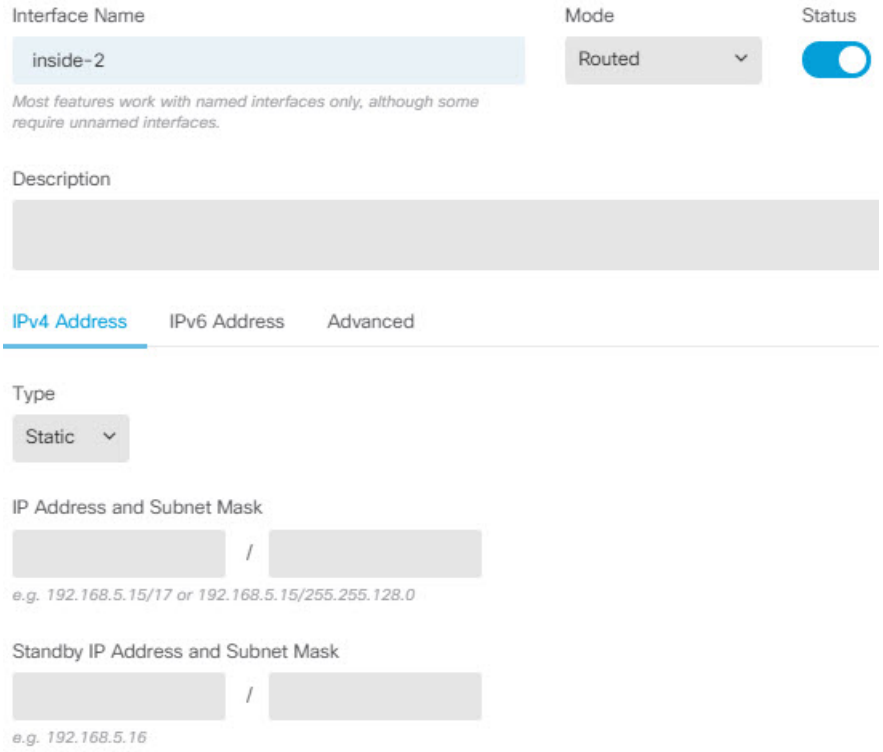
d) 点击**确定 (OK)**。

步骤 2 为虚拟路由器 2 (VR2) 配置 inside-2 接口，但不指定 IP 地址。

a) 在“接口列表”(Interfaces listing) 页面上，点击您将分配给 VR2 的接口的“操作”(Action) 列中的编辑图标 。

b) 至少配置以下属性：

- **名称** - 在本例中为 **inside-2**。
- **模式** - 选择**路由**。
- **状态** - 启用接口。
- **IPv4 地址** > **类型** - 选择**静态**。
- **IPv4 地址和子网掩码** - 将这些字段留空。如果您现在尝试配置与内部接口相同的地址，系统将显示一条错误消息，并阻止您创建非功能性配置。无法通过同一路由器中的不同接口路由到同一地址空间。



c) 点击**确定 (OK)**。

步骤 3 配置虚拟路由器 VR1，其中包括到外部接口的静态默认路由泄漏。

a) 选择**设备 (Device)**，然后点击**路由 (Routing)** 摘要中的**查看配置 (View Configuration)**。

b) 点击“路由”(Routing) 页面顶部的**添加多个虚拟路由器 (Add Multiple Virtual Routers)**。

c) 在说明性面板的右下角，点击**创建第一个自定义虚拟路由器 (Create First Custom Virtual Router)**。

d) 填写虚拟路由器 VR1 的属性。

- **名称** - 输入 VR1 或您选择的其他名称。
- **接口 (Interfaces)** - 点击 **+**，选择 **inside**，然后点击**确定 (OK)**。

e) 点击**确定 (OK)**。

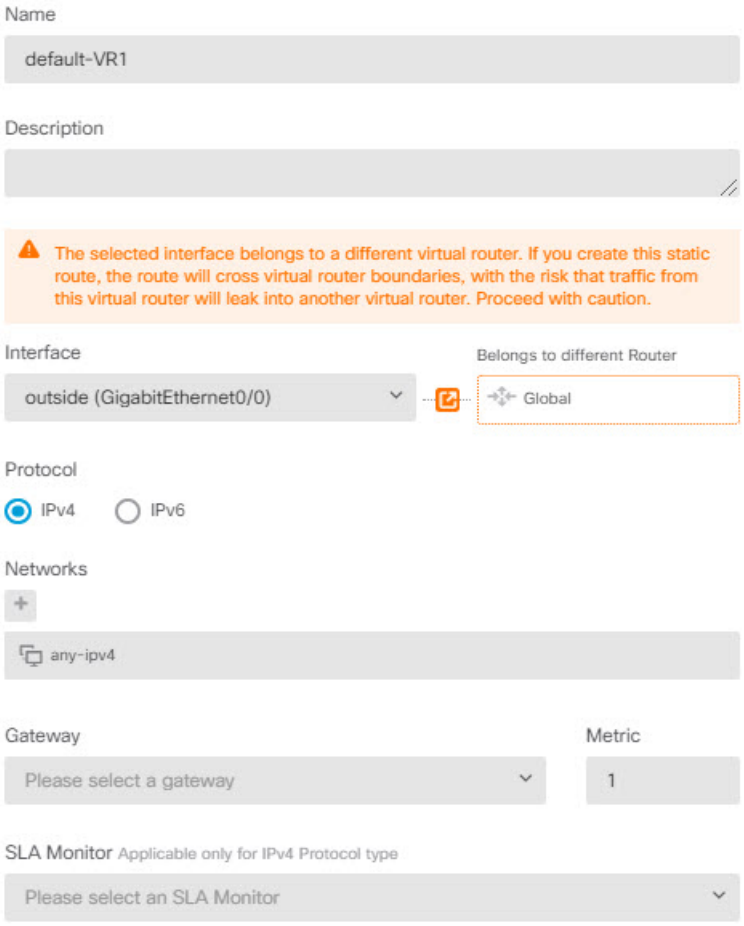
对话框将关闭，并显示虚拟路由器列表。

f) 在虚拟路由器列表中，请在 VR1 虚拟路由器的操作列中点击查看图标 ( )。

g) 在**静态路由 (Static Routing)** 选项卡上，点击 **+** 并配置路由：

- **名称** - 任何名称（例如，**default-VR1**）。
- **接口** - 选择 **outside**。您将看到一条警告，指出接口位于不同的路由器中，并且您将创建路由泄漏。这是您需要执行的操作。
- **协议** - 在本例中，使用 **IPv4**。
- **网络** - 选择 **any-ipv4** 对象。这将是无法在 VR1 内路由的任何流量的默认路由。
- **网关** - 将此项目留空。将路由泄漏到另一个虚拟路由器时，您不必选择网关地址。

对话框应如下所示：



h) 点击**确定 (OK)**。

步骤 4 配置虚拟路由器 VR2，其中包括到外部接口的静态默认路由泄漏。

a) 查看 VR1 时，点击后退按钮（ ）可返回到虚拟路由器列表。

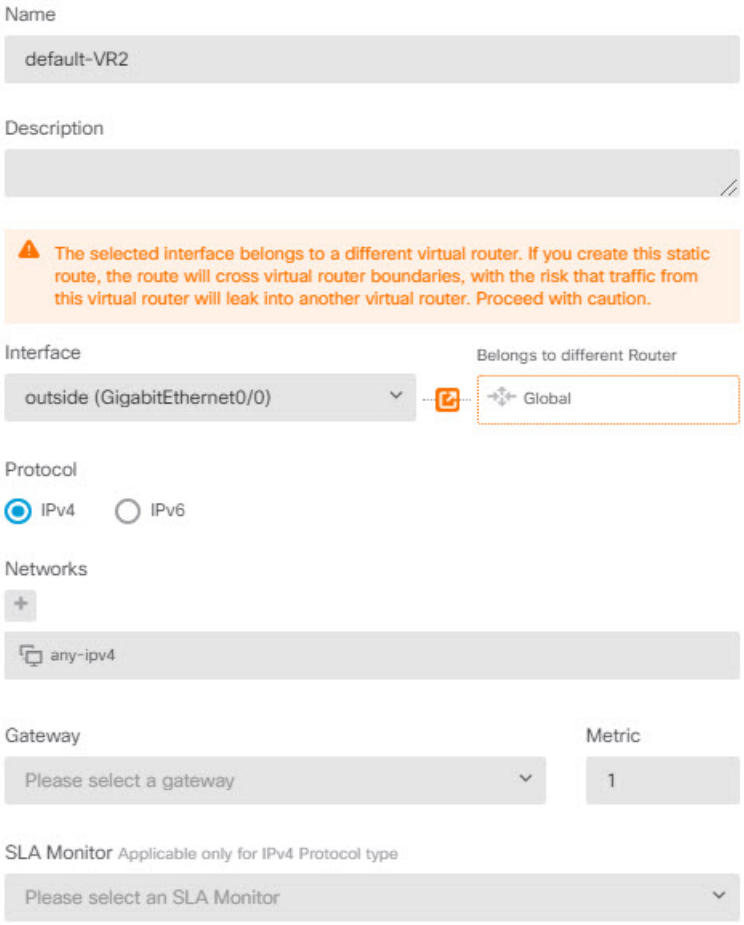
b) 点击列表顶部的 +。
c) 填写虚拟路由器 VR2 的属性。
   - **名称** - 输入 VR2 或您选择的其他名称。
   - **接口 (Interfaces)** - 点击 +，选择 **inside-2**，然后点击**确定 (OK)**。

d) 点击**确定 (OK)**。

   对话框将关闭，并显示虚拟路由器列表。

e) 在虚拟路由器列表中，请在 VR2 虚拟路由器的操作列中点击查看图标 ( )。
f) 在**静态路由 (Static Routing)** 选项卡上，点击 + 并配置路由：
   - **名称** - 任何名称（例如，**default-VR2**）。
   - **接口** - 选择 **outside**。您将看到一条警告，指出接口位于不同的路由器中，并且您将创建路由泄漏。这是您需要执行的操作。
   - **协议** - 在本例中，使用 **IPv4**。
   - **网络** - 选择 **any-ipv4** 对象。这将是用于无法在 VR2 内路由的任何流量的默认路由。
   - **网关** - 将此项目留空。将路由泄漏到另一个虚拟路由器时，您不必选择网关地址。

   对话框应如下所示：

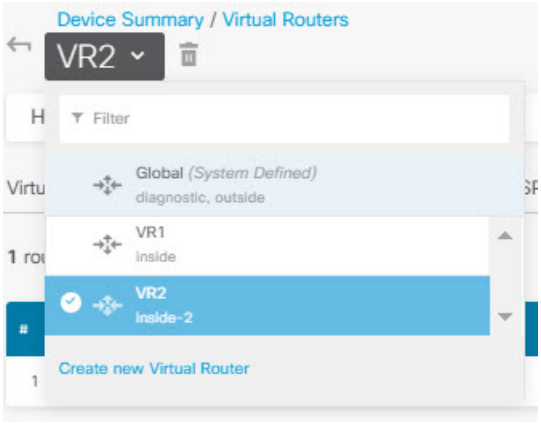


g) 点击**确定 (OK)**。

步骤 5 在全局路由器中创建到外部接口的默认路由。

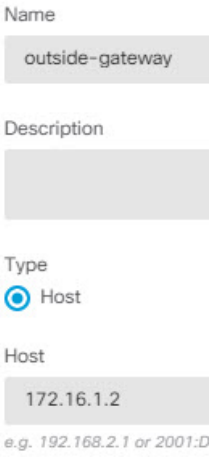
此路由用于为从两个虚拟路由器泄漏到全局路由器的外部接口的流量分配正确的网关。

a) 查看 VR2 时，点击页面顶部的 VR2 名称以打开虚拟路由器列表，然后选择全局路由器。

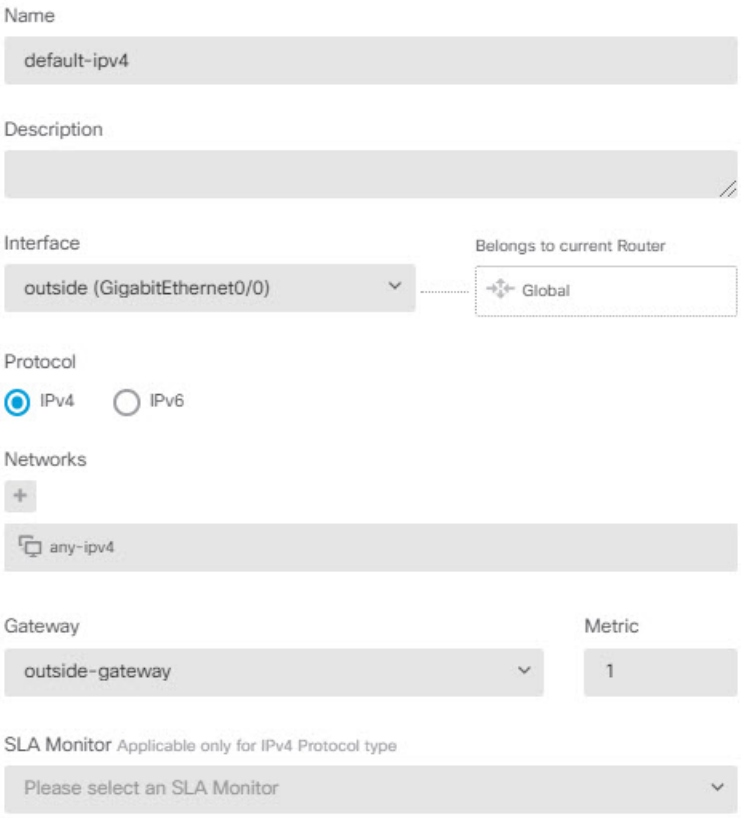


b) 在全局路由器的“静态路由”(Static Routing) 选项卡上，点击 + 并配置路由：

- **名称** - 任何名称（例如，default-ipv4）。
- **接口** - 选择 **outside**。
- **协议** - 在本例中，使用 **IPv4**。
- **网络** - 选择 **any-ipv4** 对象。这将是用于任何 IPv4 流量的默认路由。
- **网关 (Gateway)** - 假设对象尚不存在，点击**创建新网络对象 (Create New Network Object)**，然后为外部接口上网络链路另一端的网关的 IP 地址（在本例中为 172.16.1.2）定义主机对象。创建对象后，在静态路由的“网关”字段中选择该对象。



对话框应如下所示：



c) 点击**确定 (OK)**。

步骤 6 返回**接口 (Interfaces)** 页面，并将 IP 地址添加到 inside-2。

a) 点击**设备 (Device)**，然后点击**接口 (Interface)** 摘要中的**查看所有接口 (View All Interfaces)**。

b) 对于将分配给 VR2 的 inside-2 接口，点击“操作”(Action) 列中的编辑图标 ( )。

c) 在 **IPv4 地址**选项卡上，输入 192.168.1.1/24 作为 IP 地址和子网掩码。

d) 点击**确定 (OK)**。

现在将不会出现重复 IP 地址的错误，因为 inside 和 inside-2 接口现在位于不同的虚拟路由器中。

步骤 7 创建 NAT 规则，以将 PAT 内-外流量传输到 10.100.10.1。

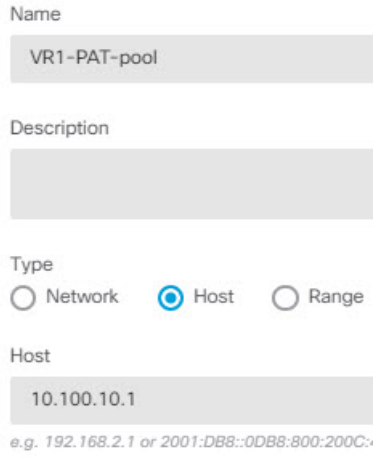
a) 选择**策略 (Policies)**，然后点击 **NAT**。

b) 如果内-外接口已有名为 InsideOutsideNatRule 的手动 NAT 规则来应用接口 PAT，请点击对应于该规则的编辑 ( ) 图标。否则，点击 **+** 创建新规则。

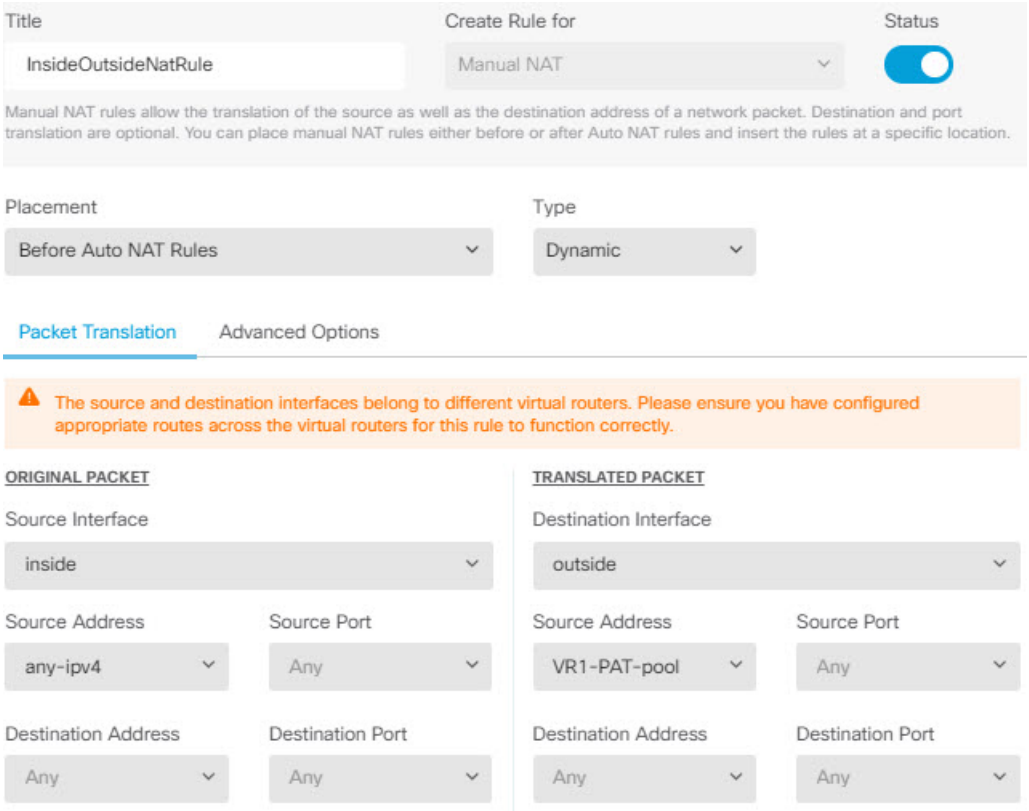
请注意，如果编辑现有规则，现在会出现一条警告，指出源接口和目标接口位于不同的虚拟路由器中，并且您需要定义路由。这是您之前在本程序中执行的操作。

c) 假设要编辑一个现有规则，请点击**转换后的数据包 (Translated Packet)** > **源地址 (Source Address)** 中的下拉箭头，然后点击**创建新网络 (Create New Network)**（假设您没有用于定义 10.100.10.1 的主机对象）。

d) 配置 PAT 地址的主机网络对象。此对象应类似于以下所示：



e) 选择新对象作为**转换后的数据包** > **源地址**。NAT 规则应类似于以下内容：



f) 点击**确定 (OK)**。

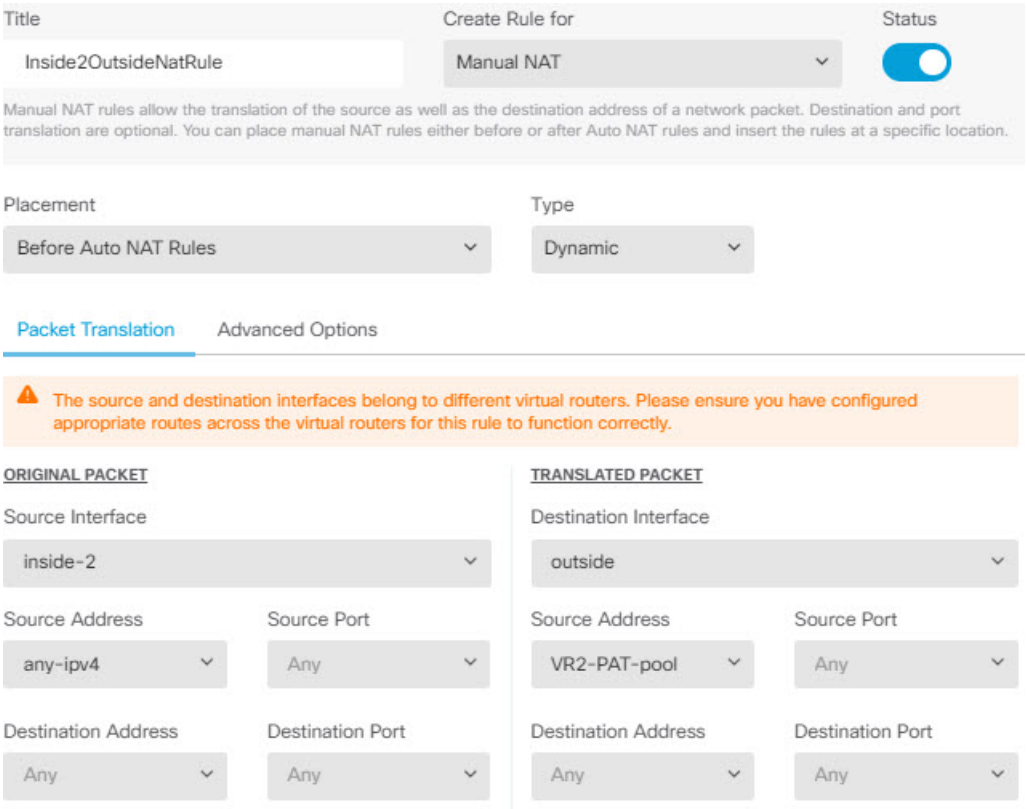
步骤 8 创建 NAT 规则，将从 inside-2 流向外部的流量 PAT 到 10.100.10.2。

此规则与 VR1 的规则完全相同，但以下项除外：

- **名称** - 必须唯一，例如 Inside2OutsideNatRule。
- **原始数据包** > **源接口** - 选择 inside-2。

- **转换后的数据包** > **源地址** - 为 10.100.10.2 创建新的主机网络对象。

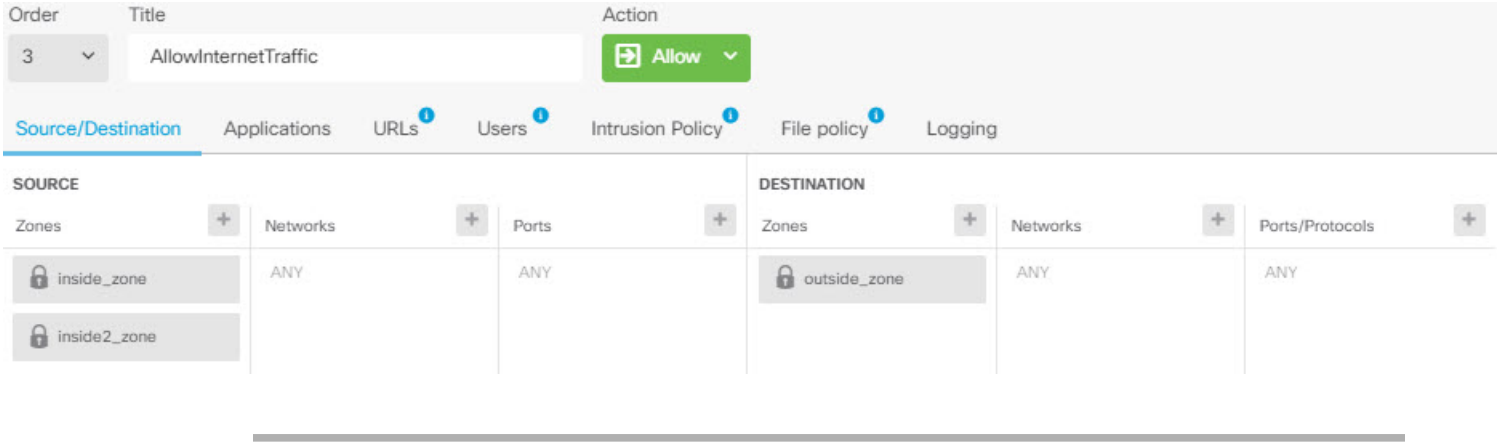
此规则应类似于以下内容：



步骤 9 选择**策略** > **访问控制**，并配置访问控制规则以允许将 inside_zone 和 inside2_zone 中的流量传输到 outside_zone。

最后，您需要配置访问控制策略以允许从 inside 和 inside-2 接口向外部接口传输流量。由于访问控制规则要求使用安全区，因此您需要为每个接口创建区域。或者，可以创建单个区域来同时保存 inside 和 inside-2，但您可能希望在此处或其他策略中创建其他规则，以区分在这些路由器中对流量的处理方式。

假设您创建了以接口命名的区域，则允许所有流量流向互联网的基本规则将如下所示：可以根据需要将入侵策略应用于此规则。可以定义其他规则来阻止不需要的流量，例如，用于实施URL过滤操作。



监控虚拟路由器

要对虚拟路由器进行监控和故障排除，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。您还可以从“路由”(Routing) 页面的**命令 (Commands)** 菜单选择其中一些命令。

- **show vrf** 显示有关系统上定义的虚拟路由器的信息。
- **show ospf** ［**vrf** *name* | **all**］

  显示有关虚拟路由器中 OSPF 进程的信息。您可以指定虚拟路由器以仅查看有关该虚拟路由器中进程的信息，或者忽略此选项，以便查看所有虚拟路由器上的 VRF 信息。使用 **show ospf ?** 可查看其他选项。
- **show bgp** ［**vrf** *name* | **all**］

  显示有关虚拟路由器中 BGP 进程的信息。您可以指定虚拟路由器以仅查看有关该虚拟路由器中进程的信息，或者忽略此选项，以便查看所有虚拟路由器上的 VRF 信息。使用 **show bgp ?** 可查看其他选项。
- **show eigrp** 选项

  显示有关 EIGRP 进程的信息。选择 **show eigrp ?** 可查看可用选项。

第 14 章

用于路由调整的路由映射和其他对象

各种路由协议均允许调整路由分发和汇聚等活动。对于某些调整功能，您可以使用路由映射或其他对象来确定应遵循调整策略的路由。路由映射还具有在匹配路由上设置选项的额外功能，以便您可以更改下一跳路由器可用于应用自定义行为的路由。

是否需要创建这些对象中的任何对象，取决于您对调整所实施的路由协议行为的需求。通过首先评估您的要求，您可以确定您要配置的调整命令所需的对象类型。

配置路由映射

您可以将路由映射用于各种用途，某些路由协议支持的用途比其他协议更多。最典型的用途是通过调整将路由重新分发到其他路由协议中。

路由映射 Permit 和 Deny 子句

路由映射由一个或多个 **permit** 或 **deny** 子句组成。这些子句的顺序很重要：系统根据映射从上到下的顺序评估路由，并应用首先匹配的第一个子句。如果路由不与任何子句匹配，则视为与路由映射不匹配。

每个 permit 子句可以包含零个或多个 **match** 和 **set** 语句。**match** 语句确定哪些路由与子句匹配，而 **set** 语句修改路由的某些特征，例如路由度量。您不需要任何 set 语句：您可以匹配路由以执行重新分发（或其他服务），而无需以任何方式更改路由。

每个 deny 子句可以包含零个或多个 match 语句。但是，由于“被拒绝”的路由与路由映射不匹配，因此包含 set 子句毫无意义，因为无法应用 set 操作。

路由映射 Match 和 Set 语句

每个路由映射子句均具有两种类型的值：

- match 值用于选择应将此子句应用于的路由。
- set 值用于修改路由的某些属性。

例如，对于要重新分发的每条路由，路由器首先评估路由映射中子句的匹配条件。如果路由符合条件，则按 permit 或 deny 子句的规定重新分发或拒绝路由。对于 permit 子句的匹配项，路由的某些属性可能会被 set 命令中的值修改。如果路由与条件不匹配，则此子句不适用于路由，系统会根据路由映射中的下一个子句继续评估路由。路由映射扫描将继续，直到发现匹配路由的子句或达到路由映射的结尾。如果没有匹配项，系统将认为路由与路由映射不匹配（相当于 deny 操作）。

对于单个子句中的 match 和 set 语句：

- 多个 match 语句之间采用逻辑“与”运算。也就是说，路由必须满足每个语句才视为与子句匹配。
- 单个 match 语句中的多个值之间采用逻辑“或”运算。也就是说，如果路由匹配该 match 语句中的任何值，则该路由将被视为匹配整个语句。
- 如果没有 match 语句，则所有路由都与该子句匹配。
- 如果路由映射 permit 子句中没有 set 语句，则系统将在不修改路由当前属性的情况下，将功能（例如重新分发）应用于路由。
- deny 子句中的所有 set 语句都会被忽略。“被拒绝”的路由与路由映射根本不匹配，因此添加 set 子句毫无意义，因为系统无法应用 set 操作。
- 空子句（即不包含 match 或 set 语句的子句）会与之前的子句未匹配的所有路由匹配。例如：
  - 空 permit 子句允许重新分发剩余路由而不进行修改。
  - 空 deny 子句不允许重新分发其余路由。如果路由映射在经过完整扫描后，未发现明确的匹配项，则默认采用此操作。

配置路由映射

您可以将路由映射用于各种用途，某些路由协议支持的用途比其他协议更多。最典型的用途是通过调整将路由重新分发到其他路由协议中。

路由映射由一个或多个 **permit** 或 **deny** 子句组成。这些子句的顺序很重要：系统根据映射从上到下的顺序评估路由，并应用首先匹配的第一个子句。如果路由不与任何子句匹配，则视为与路由映射不匹配。

每个 permit 子句可以包含零个或多个 **match** 和 **set** 语句。**match** 语句确定哪些路由与子句匹配，而 **set** 语句修改路由的某些特征，例如路由度量。您不需要任何 set 语句：您可以匹配路由以执行重新分发（或其他服务），而无需以任何方式更改路由。

每个 deny 子句可以包含零个或多个 match 语句。但是，由于“被拒绝”的路由与路由映射不匹配，因此包含 set 子句毫无意义，因为无法应用 set 操作。

有关 match 和 set 语句评估方式的详细说明，详见路由映射 Match 和 Set 语句，第 344 页。

开始之前

您可以在路由映射中使用各种其他对象来定义匹配条件，例如访问列表、AS 路径访问列表、社区列表、策略列表和前缀列表。必须先创建这些对象，然后才能创建路由映射。

对于 ACL 匹配，可以对 IPv4 地址使用标准或扩展 ACL，但对 IPv6 仅可使用扩展 ACL。由于 match 子句仅基于 IPv4 或 IPv6，因此请确保您的 ACL 具有用于 match 语句的正确地址方案。

另请注意，与其他路由协议相比，BGP 的匹配和设置条件不同。确保为使用路由映射的路由进程选择正确的匹配/设置条件。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在目录中选择 **Smart CLI** > **对象**。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 选择**路由映射**作为 **CLI 模板**。

步骤 5 为 Smart CLI 对象输入**名称**。请注意，此名称还作为路由映射名称输入 CLI 模板第一行中（在 **route-map** 命令中）。

步骤 6 创建第一个子句：

a) 点击 *redistribution* 变量，然后选择以下选项之一：

- **permit** - 匹配。为正在配置的功能选择匹配此规则的连接。
- **deny** - 不匹配。匹配此规则的连接将从功能中排除。请注意，“被拒绝”的流量不会被丢弃，而只是无法获得向它应用的服务。例如，如果使用此路由映射定义要重新分发的路由，则系统不会重新分发“已拒绝”的地址空间。

b) 点击 **sequence-number** 变量并为子句输入编号，范围为 1 到 65535。

此编号是相对于路由映射中的其他编号子句而言。典型的做法是以 10 为单位跳着计数，即 10、20、30，以便留出空间在将来插入新的子句。

步骤 7 点击**显示已禁用**，并为子句配置 **match** 语句。

a) 点击 **configure** *clause* 命令左侧的 + 以启用命令。

b) 点击 *clause*，为 BGP 路由映射选择 **bgp-match-clause**，或者为所有其他路由协议选择 **match-clause**。

c) （BGP 路由映射。）配置以下 **match** 语句的任意组合，以标识您在此子句中定位的特定路由。请务必点击 - 图标禁用所有未配置的命令。

- **match as-path**。点击变量，然后选择定义要匹配的自治系统编号的 AS 路径对象。
- **match community**。点击变量，然后选择定义要匹配的社区的社区列表对象。
- **match policy-list**。点击变量，然后选择定义该子句的匹配条件的策略列表对象。
- **match tag**。点击变量并输入要匹配的路由标记值，范围为 0-4294967295。

d) （所有其他路由协议。）配置以下 **match** 语句的任意组合，以标识您在此子句中定位的特定路由。请务必点击 - 图标禁用所有未配置的命令。您可能需要点击 + 以启用其中一些命令。

- **match interface**。点击变量并选择要匹配的路由中的所有接口。
- **configure match ipv4/ipv6 ip address** *list-type*。为您的 IP 版本启用正确的命令。然后，点击 *list-type* 变量并选择是否要基于 **access-list** 或 **prefix-list** 匹配路由中的 IP 地址。这将添加一个 **match ipv4/ipv6 address** 命令，您可以点击该变量并选择定义要匹配的 IP 地址的访问列表或前缀列表。
- **configure match ipv4/ipv6 ip next-hop** *list-type*。点击 *list-type* 变量，然后选择是否要基于 **access-list** 或 **prefix-list** 匹配路由中下一跳路由器的 IP 地址。这将添加一个 **match ipv4/ipv6 next-hop** 命令，您可以点击该变量并选择定义要匹配的 IP 地址的访问列表或前缀列表。
- **configure match ipv4/ipv6 ip route-source** *list-type*。点击 *list-type* 变量，然后选择是否要基于 **access-list** 或 **prefix-list** 匹配路由中路由源的 IP 地址。这将添加一个 **match ipv4/ipv6 route-source** 命令，您可以点击该变量并选择定义要匹配的 IP 地址的访问列表或前缀列表。
- **match metric**。点击变量并输入要匹配的路由度量，范围为 1-4294967295.。
- **match route-type**。（OSPF、EIGRP。）点击此变量并选择路由映射：
  - **external-1**、**external-2**。OSPF 或 EIGRP 外部第 1 类或第 2 类路由。
  - **internal**。OSPF 区域内和区域间路由或 EIGRP 内部路由。
  - **local**。本地生成的 BGP 路由。
  - **nssa-external-1**、**nssa-external-2**。外部次末节区域 (NSSA) 第 1 类或第 2 类路由。

步骤 8 （可选，仅限 permit 子句。）对于允许的路由，即匹配的路由，可以配置 **set** 语句来修改路由属性。您无需修改路由；例如，您可以照原样重新分发它们。

a) 点击 **...** > **复制**（在 permit 子句中 configure match-clause 或 **configure bgp-match-clause** 命令左侧）。系统在 permit 子句末尾添加一个新的 **configure** *clause* 命令。

b) 点击 *clause*，根据为 match 子句做出的选择，选择 **bgp-set-clause** 或 **set-clause**。

c) （BGP 路由映射。）配置以下 **set** 语句的任意组合，以修改匹配路由的属性。请务必点击 - 图标禁用所有未配置的命令。

- **configure set as-path** *options*。点击 *options* 并选择 **properties**，这会添加您需要配置的以下命令。通过向路径添加项目，甚至复制 AS 编号，可以延长路径并减少路由被选为最佳路由的可能性。
  - **set as-path prepend** *as-path*。点击 *as-path*，并输入最多 10 个要添加到路由 AS_PATH 属性开头的自治系统编号。此更改适用于出站 BGP 路由映射。
  - **set as-path prepend last-as** *value*。点击 *value*，并输入系统应在 AS_PATH 变量的开头添加通告邻居的自治系统编号的次数。此更改适用于入站 BGP 路由映射。
  - **set as-path tag**。将路由标记转换为路径。仅在将路由重分布到 BGP 中时适用。
- **set community** *community-number properties*。点击 *community-number* 并输入路由的社区，范围为1-4694967295。或者，您可以点击 *properties* 并添加以下选项之一：
  - **internet** - 系统向所有对等体（内部和外部）通告具有此社区的路由。
  - **no-advertise** - 系统不向任何对等体（内部或外部）通告具有此社区的路由。
  - **no-export** - 系统仅向同一自治系统中的对等体或仅向联盟内的其他子自治系统通告具有此社区的路由。不会向外部对等体通告这些路由。
- **set local-preference**。点击变量，然后输入自治系统路径的首选项值，范围为 0-4294967295。除非在全局 BGP 选项中进行更改，否则 BGP 路由的默认首选项为 100。首选使用具有最高优先级编号的路由。
- **set weight**。点击变量并输入路由权重 0-65535。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。
- **set origin** *options*。BGP 路由的起点基于主要 IP 路由表中路由的路径信息。您可以通过点击 *options* 更改此设置，然后选择要如何设置 BGP 源代码。
  - **igp**。将源设置为远程内部网关协议 (IGP) 系统。
  - **incomplete**。将源设置为未知继承项。
- **configure next-hop ipv4/ipv6** *options*。这些是单独的命令。为相应 IP 版本点击 *options* 并选择以下选项之一：在实施基于策略的路由时通常会设置下一跳网关。
  - **specific-ip**。如果要为此路由显式设置下一跳网关的 IP 地址，请选择此选项。系统将添加 **set ip/ipv6 next-hop ip-address** 命令。点击变量并输入下一跳网关的 IP 地址。您可以添加多个以空格分隔的 IP 地址。如果第一个网关的地址无法访问，系统将尝试下一个地址，以此类推。
  - **user-peer-address**。如果要将下一跳网关设置为 BGP 对等体的 IP 地址，请选择此选项。如果在 BGP 对等体的出站路由映射中使用此选项，则通告的匹配路由的下一跳将设置为本地路由器的对等地址，从而禁用下一跳计算。无需为此命令执行额外配置。
- **set ipv4/ipv6 address** *prefix-list*。这些是单独的命令。根据您选择的前缀列表的内容更改路由的 IP 地址。

- **set automatic-tag**。让系统自动计算路由的标记值。

d) （所有其他路由协议。）配置以下 **set** 语句的任意组合，以修改匹配路由的属性。请务必点击 - 图标禁用所有未配置的命令。

- **set metric**。点击变量，然后输入度量值，范围为从 0-4294967295。此值不适用于 EIGRP。
- **set metric-type**。点击此变量，然后选择度量类型。
  - **type-1**、**type-2**。OSPF 中的外部路由类型。默认为第 2 类。
  - **internal**。设置通告给外部 BGP (eBGP) 邻居的前缀上的多出口标识符 (MED) 值，以匹配路由下一跳的内部网关协议 (IGP) 度量。此设置适用于生成的内部 BGP (iBGP) 路由和 eBGP 派生的路由。

步骤 9 添加 permit/deny 子句以完成路由映射。

要添加子句，请点击 **...** > **复制**（在 **permit** 或 **deny** 行的左侧）。在您点击了“复制”命令的子句之后，系统会立即添加一个新的 *redistribution sequence-number* 子句。

虽然路由映射子句按序号的顺序而不是在对象中出现的顺序进行评估，但如果按序号插入新的子句，则更容易编辑对象。不能在对象内移动子句。

请注意，复制子句只是插入一个新的空子句，没有预配置的特征。创建“复制”ACE 后，按照上述说明继续进行配置，以满足您的需求。

步骤 10 点击**确定**保存对象。

现在，您可以为需要路由映射的功能在路由进程配置或 FlexConfig 对象中使用该对象。

配置访问列表

访问列表对象（也称为访问控制列表 [ACL]），选择服务将应用到的流量。您可在配置特定功能（例如路由映射）时使用这些对象。对于识别为ACL所允许的流量，系统会提供服务，而“阻止”流量则会从服务中排除。从服务中排除流量未必意味着完全丢弃该流量。

您可以配置以下类型的 ACL：

- 扩展 - 根据源地址/端口和目标地址/端口识别流量。支持 IPv4 和 IPv6 地址。
- 标准 - 仅根据目标地址识别流量。仅支持 IPv4。

ACL 由一个或多个访问控制条目 (ACE) 或规则组成。ACE 的顺序非常重要。当评估 ACL 以确定数据包是否与被“允许”的 ACE 匹配时，系统将按每个 ACE 条目的排列顺序对照每个 ACE 来测试数据包。找到匹配项后，不再检查更多 ACE。例如，如果要匹配 10.100.10.1，但排除 10.100.10.0/24 的其余部分，则 10.100.10.1 的允许条目必须放在 10.100.10.0/24 的 deny 条目之前。一般来说，将更具体的规则置于 ACL 的顶部。

不匹配允许条目的数据包被视为拒绝或排除在匹配之外。

以下主题介绍如何配置 ACL 对象。

配置扩展访问列表

当要根据源和目标地址、协议和端口匹配流量时或者如果流量为 IPv6，可使用扩展 ACL 对象。

开始之前

在您在对象中创建的 ACE 中，创建您所需的所有网络或端口对象。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在目录中选择 **Smart CLI** > **对象**。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 **+** 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 选择**扩展访问列表**作为 **CLI 模板**。

步骤 5 为 Smart CLI 对象输入**名称**。请注意，此名称还作为 ACL 名称输入 CLI 模板的第一行（在 **access list** 命令中）。

步骤 6 创建应作为 ACL 中首要规则的 ACE。

单个 **configure access list entry** 命令中包含的每个命令列表实质上都是一个ACE，但在部署时，系统可能会将命令划分为一系列 ACE，尤其是在您添加多个网络对象时。

a) 在 configure access list entry 命令中，点击 *action*，并选择一项以下操作：

- **permit** - 匹配。系统会为您所配置的功能选择与此 ACE 匹配的连接。
- **deny** - 不匹配。系统会为该功能排除与此 ACE 匹配的连接。请注意，“被拒绝”的流量不会被丢弃，而只是无法获得向它应用的服务。例如，在路由映射中，如果使用此 ACL 定义要重新分发的路由，则系统会不重新分发“被拒绝”的地址空间。

b) 在 **permit/deny network** 命令中，点击变量可选择定义连接的源 IP 地址和目标 IP 地址的网络对象。您可以选择多个对象。要指定“任何”地址，请选择 any-ipv4 和 any-ipv6 对象。

c) 在 **configure permit/deny port** 命令中，点击 *options*，并选择以下一个选项，这会将关联的 permit/deny 命令添加到模板中：

- **any** - 如果端口无关紧要，则选择此选项。也就是说，系统将匹配所有类型的 IP 流量。

- **any-source** - 如果源 TCP/UDP 端口无关紧要，但您希望指定目标端口，则选择此选项。点击 **permit/deny port** 命令中的 *destination-port* 变量，然后选择端口对象。
- **any-destination** - 如果 TCP/UDP 端口无关紧要，但您希望指定源端口，则选择此选项。点击 **permit/deny port** 命令中的 *source-port* 变量，选择端口对象。
- **source-destination** - 如果源和目的 TCP/UDP 端口都很重要，则选择此选项。点击 **permit/deny port** 命令中的 *source-port* 和 *destination-port* 变量，并选择端口对象。

d) 在 **configure logging** 命令中，选择 **disabled**。日志记录适用于执行访问控制的 ACL，但您不能将这些对象用于访问控制。因此，无论您选择什么选项，系统都会忽略日志记录选项。

步骤 7 添加 ACE 以完成 ACL。

要添加 ACE，请点击 **...** > **复制**（在 **configure access list entry** 行的左侧）。在您点击了“复制”命令的相应 ACE 后面，系统会紧接着添加一个新的 ACE 组。

因此，当对象中有很多 ACE 时，请谨慎选择“复制”哪个 ACE。您无法在对象内移动 ACE，因此如果出错，您需要在正确的位置手动重新创建 ACE。

请注意，复制 ACE 只是插入一个新的且没有预配置特征的空 ACE。创建“复制”ACE 后，按照上述说明继续进行配置，以满足您的需求。

步骤 8 点击**确定**保存对象。

现在，您可以为需要扩展 ACL 的功能在路由映射对象或 FlexConfig 对象中使用该对象。

配置标准访问列表

如果仅需要根据目标 IPv4 地址匹配流量并且您所配置的功能支持标准 ACL，请使用标准 ACL 对象。否则，请使用扩展 ACL。

开始之前

在您在对象中创建的 ACE 中创建您需要的任何网络对象。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在目录中选择 **Smart CLI** > **对象**。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 **+** 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 选择**标准访问列表**作为 **CLI 模板**。

步骤 5 为 Smart CLI 对象输入**名称**。请注意，此名称还作为 ACL 名称输入 CLI 模板的第一行（在 **access list** 命令中）。

步骤 6 创建应作为 ACL 中首要规则的 ACE。

单个 **configure action** 命令中包含的每个命令列表都是一个 ACE。

a) 在 **configure action** 命令中，点击操作并选择以下选项之一：

- **permit** - 匹配。系统会为您所配置的功能选择与此 ACE 匹配的连接。
- **deny** - 不匹配。系统会为该功能排除与此 ACE 匹配的连接。请注意，“被拒绝”的流量不会被丢弃，而只是无法获得向它应用的服务。例如，在路由映射中，如果使用此 ACL 定义要重新分发的路由，则系统会不重新分发“被拒绝”的地址空间。

b) 在 **permit/deny host** 命令中，点击变量以选择定义连接目标 IP 地址的网络对象。对象可以指定网络或主机地址。您可以为每个 **permit/deny host** 命令选择一个对象；在命令中点击. **...** > **复制**，以指定其他地址，这些地址将成为具有相同操作的唯一性 ACE。要指定“任何”地址，请选择 any-ipv4 对象。

步骤 7 添加 ACE 以完成 ACL。

要添加 ACE，请点击 **...** > **复制**（在 **configure action** 行的左侧）。在您点击了“复制”命令的相应 ACE 后面，系统会紧接着添加一个新的 ACE 组。

因此，当对象中有很多 ACE 时，请谨慎选择“复制”哪个 ACE。您无法在对象内移动 ACE，因此如果出错，您需要在正确的位置手动重新创建 ACE。

请注意，复制 ACE 只是插入一个新的且没有预配置特征的空 ACE。创建“复制”ACE 后，按照上述说明继续进行配置，以满足您的需求。

步骤 8 点击**确定**保存对象。

现在，您可以将路由映射对象或 FlexConfig 对象中的对象用于需要标准 ACL 的功能。

配置 AS 路径访问列表

您可以使用 AS 路径访问列表根据更新中的自治系统编号过滤 BGP 邻居更新。系统将接受允许的 AS 编号的更新，而拒绝被拒绝的 AS 编号的更新，即不会将其添加到路由表。

您还可以在出站方向应用 AS 路径过滤，并过滤发送到邻居的更新。

此外，您可以在路由映射中使用 AS 路径对象进行 BGP 地址汇聚，

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在目录中选择 **Smart CLI** > **对象**。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 选择 **ASPath** 作为 **CLI 模板**。

步骤 5 为 Smart CLI 对象输入**名称**。该名称必须是 1-500 范围内的数字。请注意，此名称还作为 AS 路径访问列表名称输入 CLI 模板的第一行（在 **as-path** 命令中）。

步骤 6 配置 AS 路径条目。

每个条目都包含在以操作选项开头的单独一行中。

a) 点击 *action* 并选择以下选项之一：

- **permit** - 匹配。为正在配置的功能选择匹配此规则的连接。
- **deny** - 不匹配。匹配此规则的连接将从功能中排除。请注意，“被拒绝”的流量不会被丢弃，而只是无法获得向它应用的服务。例如，在路由映射中，如果使用此对象定义要重新分发的路由，则系统不会重新分发“已被拒绝”的地址空间。

b) 点击正则表达式，并输入定义应与此条目匹配的 AS 编号的正则表达式。

最简单形式的正则表达式只是一个完整的 AS 路径编号，您可以允许或拒绝来自单个自治系统的路由更新。

AS 编号范围为从 1 至 4294967295，或从 1.0 至 65535.65535。AS 编号是分配的唯一值，用于在互联网上标识各个网络。系统支持 RFC 5396 中定义的 asplain 和 asdot 表示法。需要使用哪种表示法取决于您是否在 BGP 全局设置中启用 **bgp asnotation dot** 命令。

步骤 7 添加条目以完成 AS 路径访问列表。

要添加条目，请点击 **...** > **复制**（在操作行的左侧）。系统会在您点击“复制”命令的条目后立即添加新条目。

因此，当对象中有许多条目时，请明智地选择“复制”哪个条目。您无法在对象内移动条目，因此，如果出错，您需要在正确的位置手动重新创建条目。系统按自上而下的顺序评估规则，并应用第一个匹配的规则。

请注意，复制条目只是插入一个新的空条目，而没有预配置的特征。创建“复制”ACE 后，按照上述说明继续进行配置，以满足您的需求。

步骤 8 点击**确定**保存对象。

现在，您可以将 BGP 对象、路由映射对象或 FlexConfig 对象中的对象用于需要 AS 路径访问列表的功能。

配置社区列表

如果启用 BGP 进程发送社区信息，则可以使用社区列表作为路由映射中的 match 子句来设置匹配路由的属性。例如，您可以更改某些社区的路由首选项。

社区是一种可选属性或标签，运营商将其附加到一组共享某些公共属性的目的地的通告路由中。特定社区编号将由您的 ISP 通告：您需要从 ISP 获取编号及其含义，然后选择使用路由映射处理它们的方式。

社区列表是按顺序排列的，并以类似于访问和前缀列表的自上而下且应用第一个匹配项的方式来确定匹配项。

社区列表分为以下两种类型：

- 标准 - 当您希望以特定的已知社区（例如从运营商处获取的社区）为目标时，请使用标准列表。
- 扩展 - 如果要根据正则表达式匹配来匹配一组社区，请使用扩展列表。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在目录中选择 **Smart CLI** > **对象**。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 选择**标准社区列表**或**扩展社区列表**作为 **CLI 模板**。

步骤 5 为 Smart CLI 对象输入**名称**。请注意，此名称还作为社区列表名称输入 CLI 模板第一行中（在 **community-list** 命令中）。

步骤 6 （标准列表。）配置社区列表条目。

每个条目都包含在以操作选项开头的单独一行中。

a) 点击 *action* 并选择以下选项之一：

- **permit** - 匹配。为正在配置的功能选择匹配此规则的连接。
- **deny** - 不匹配。匹配此规则的连接将从功能中排除。请注意，“被拒绝”的流量不会被丢弃，而只是无法获得向它应用的服务。例如，在路由映射中，如果使用此规则定义要重新分发的路由，则系统不会重新分发“已拒绝”的地址空间。

b) 点击社区编号并输入最多 10 个以空格分隔的社区。一条规则的多个社区之间采用逻辑“与”预算，因此仅当匹配路由中的所有社区时才存在匹配项。

以十进制格式 (1-4294967295) 或 AA：NN 格式（每个值为 1-66535）输入社区，具体取决于为 BGP 进程启用的编号方法。从您的 ISP 或其他 BGP 邻居那里获取这些编号。

c) （可选。）点击属性，并将其他已知社区添加到规则中。

- **internet** - 系统向所有对等体（内部和外部）通告具有此社区的路由。
- **no-advertise** - 系统不向任何对等体（内部或外部）通告具有此社区的路由。
- **no-export** - 系统仅向同一自治系统中的对等体或仅向联盟内的其他子自治系统通告具有此社区的路由。不会向外部对等体通告这些路由。

步骤 7 （扩展列表。）配置社区列表条目。

a) 点击操作并选择 **permit** 或 **deny**。上文介绍了这些操作。

b) 点击正则表达式，然后输入定义应与此条目匹配的社区的正则表达式。

使用 * 或 + 字符匹配的指令优先成为最长的结构。嵌套结构按从外向内的顺序匹配。串联结构从左侧开始匹配。如果正则表达式可与输入字符串的两个不同部分匹配，则它将优先匹配最早输入的部分。有关编写正则表达式的详细信息，请参阅《Cisco IOS 终端服务配置指南》的“正则表达式”附录。

步骤 8 添加条目以完成社区列表。

要添加条目，请点击 **...** > **复制**（在操作行的左侧）。系统会在您点击“复制”命令的条目后立即添加新条目。

因此，当对象中有许多条目时，请明智地选择“复制”哪个条目。您无法在对象内移动条目，因此，如果出错，您需要在正确的位置手动重新创建条目。

请注意，复制条目只是插入一个新的空条目，而没有预配置的特征。创建“复制”ACE 后，按照上述说明继续进行配置，以满足您的需求。

步骤 9 点击**确定**保存对象。

现在，您可以在路由映射或路由进程中或在 FlexConfig 对象中将对象用于需要社区列表的功能。

配置策略列表

您可以使用路由映射中的策略列表来替换一个或多个 match 子句。因此，如果您有一组要重复使用的 match 子句，可以使用策略映射简化配置，从而无需在每个路由映射中重复这些 match 子句。您可以使用引用 BGP 中的策略列表的路由映射。

在路由映射中，除了策略列表之外，还可以添加其他 match 子句。策略列表 match 子句仅匹配传入属性。

策略列表仅支持匹配的 IPv4 地址；不能匹配 IPv6 地址。

对于策略映射中的 match 子句：

- 多个 match 子句之间采用逻辑“与”运算。也就是说，路由必须满足每个子句才视为与策略列表匹配。
- 单个 match 子句中的多个值之间采用逻辑“或”运算。也就是说，如果路由匹配该 match 语句中的任何值，则该路由将被视为匹配整个语句。

开始之前

如果要为访问列表、前缀列表或 AS 路径访问列表配置 match 子句，则必须在创建策略列表之前创建这些对象。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在目录中选择 **Smart CLI** > **对象**。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 **+** 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 选择**策略列表**作为 **CLI 模板**。

步骤 5 为 Smart CLI 对象输入**名称**。请注意，此名称还作为策略列表名称输入 CLI 模板的第一行（在 **policy-list** 命令中）。

步骤 6 点击 **policy-list** 命令中的操作，选择以下选项之一：

- **permit** - 匹配。系统为您正在配置的功能选择匹配此列表的连接。
- **deny** - 不匹配。匹配此列表的连接将从功能中排除。请注意，“被拒绝”的流量不会被丢弃，而只是无法获得向它应用的服务。例如，在路由映射中，如果使用此对象定义要重新分发的路由，则系统不会重新分发“已被拒绝”的地址空间。

步骤 7 点击模板上方的**显示已禁用**可显示 match 命令。您必须点击要启用的 match 语句左侧的 **+** 图标。配置以下 match 语句的任意组合，以定义要定位的路由。

- **match as-path**。点击变量，然后选择定义要匹配的自治系统编号的 AS 路径对象。
- **configure match ip address** *list-type*. 点击 *list-type* 变量，然后选择是否要基于 **access-list** 或 **prefix-list** 匹配路由中的 IP 地址。这将添加一个 **match ip address** 命令，您可以点击该变量并选择标准访问列表或定义要匹配的 IP 地址的 IPv4 前缀列表。
- **configure match ip next-hop** *list-type*。点击 *list-type* 变量，然后选择是否要基于 **access-list** 或 **prefix-list** 匹配路由中下一跳路由器的 IP 地址。这将添加一个 **match ip next-hop** 命令，您可以点击该变量并选择标准访问列表或定义要匹配的 IP 地址的 IPv4 前缀列表。

- **configure match ip route-source** *list-type*。点击 *list-type* 变量，然后选择是否要基于 **access-list** 或 **prefix-list** 匹配路由中路由源的 IP 地址。这将添加一个 **match ip route-source** 命令，您可以点击该变量并选择标准访问列表或定义要匹配的 IP 地址的 IPv4 前缀列表。
- **match community** *community-list options*。点击 *community-list* 变量，然后选择定义要匹配的社区的社区列表对象。如果希望路由仅在列表中的所有社区都匹配时才匹配社区列表，请点击选项并选择 **exact-match**。
- **match interface**。点击变量并选择要匹配的路由中的所有接口。
- **match metric**。点击变量，然后输入要匹配的路由多出口鉴别器 (MED) 度量，范围为 1-4294967295。
- **match tag**。点击变量并输入要匹配的路由标记值，范围为 0-4294967295。

步骤 8 点击**确定**保存对象。

现在，您可以在路由映射对象中使用该对象，以用于 BGP 路由。

配置前缀列表

前缀列表类似于访问控制列表。前缀列表是允许/拒绝规则的有序列表，其中允许表示应与列表匹配的地址前缀，而拒绝表示不应与列表匹配的地址前缀。系统从上到下评估匹配项，并根据第一个匹配的规则（不一定是最佳匹配的规则）分配操作。因此，您需要谨慎指定序号，以确保获得您所需的匹配结果。

您可以将前缀列表用于 OSPF 过滤，或路由重新分发或注入的 BGP、OSPF 或 EIGRP 路由映射，或用于 BGP 邻居过滤。

IPv4 和 IPv6 地址有单独的前缀列表，但列表的结构相同。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在目录中选择 **Smart CLI** > **对象**。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 **+** 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 选择 **IPv4 前缀列表**或 **IPv6 前缀列表**作为 **CLI 模板**。

步骤 5 为Smart CLI对象输入**名称**。请注意，此名称还作为前缀列表名称输入CLI模板的第一行（在**prefix-list**命令中）。

步骤 6 配置前缀列表条目，即 **seq** 行。

每个条目都包含在以 **seq** 选项开头的单独一行中。

a) 在 **seq** 中，点击 *sequence-number* 并输入此规则的编号（1-4294967294）。该编号为相对于其他规则的序号，其中 1 是系统评估的第一个规则。常见做法是以 5 为单位跳着数，也就是 5、10、15 等。这样可以为您留出了插入新规则的空间，而无需更改其他规则的序号。

b) 点击 *action* 并选择以下选项之一：

- **permit** - 匹配。为正在配置的功能选择匹配此规则的连接。
- **deny** - 不匹配。匹配此规则的连接将从功能中排除。请注意，“被拒绝”的流量不会被丢弃，而只是无法获得向它应用的服务。例如，在路由映射中，如果使用此规则定义要重新分发的路由，则系统不会重新分发“已拒绝”的地址空间。

c) 点击 *ip-address-mask*，然后输入网络地址和掩码（IPv4为 CIDR 格式）或 IPv6 的前缀长度。例如，10.100.10.0/24 (IPv4) 或 2001:DB8:0:CD30::/60 (IPv6)。

系统会为此地址/掩码使用精确匹配，除非您还添加 **ge** 或 **le** 选项之一。例如，除非您在规则中添加 **ge 9**，否则 10.100.10.10/8 不会匹配 10.100.10.0/24。

可以采用如下掩码或前缀长度：

- IPv4 = 0-32
- IPv6 = 0-128

d) （可选。）对于比 IP 地址和掩码/前缀长度更具体的前缀，可以使用 **ge** 和 **le** 关键字指定要匹配的前缀长度范围。如果不使用这些关键字，则系统仅考虑完全匹配来匹配规则。

ge *min-prefix-length* 用于指定要匹配的最小前缀长度。该最小值必须大于掩码/前缀长度并小于或等于 **le** 选项中定义的最大前缀长度（如有）。

le *max-prefix-length* 用于指定要匹配的最大前缀长度。该最大值必须大于或等于最小前缀长度（如有），或者大于掩码/前缀长度（如果未定义该最小值）。

除了上述相对长度限制外，这些选项中的长度还有以下外部限制：

- IPv4 = 1-32
- IPv6 = 0-128

步骤 7 添加条目以完成前缀列表。

要添加条目，请点击 **...** > **复制**（在 **seq** 行左侧）。系统会在您点击“复制”命令的条目后立即添加新条目。

为方便起见，最好尽量按顺序保留条目。但是，部署后，前缀列表将按顺序重写，即使您在对象中打乱了顺序。

请注意，复制条目只是插入一个新的空条目，而没有预配置的特征。创建“复制”ACE 后，按照上述说明继续进行配置，以满足您的需求。

步骤 8 点击**确定**保存对象。

现在，您可以在路由映射或路由过程中或在 FlexConfig 对象中将对象用于需要前缀列表的功能。

示例

以下是如何使用前缀列表匹配前缀的一些示例。为简单起见，示例中省略了序号。每个规则的实际行为由匹配覆盖的地址空间子集的任何顺序较早的规则修改。

- 拒绝默认路由 0.0.0.0/0：

```
deny 0.0.0.0/0
```

- 允许前缀 10.0.0.0/8：

```
permit 10.0.0.0/8
```

- 在前缀为 192/8 的路由中接受最多 24 位的掩码长度：

```
permit 192.168.0.0/8 le 24
```

- 在前缀为 192/8 的路由中拒绝大于 25 位的掩码长度：

```
deny 192.168.0.0/8 ge 25
```

- 允许在所有地址空间中使用 8 到 24 位的掩码长度：

```
permit 0.0.0.0/0 ge 8 le 24
```

- 拒绝在所有地址空间中使用大于 25 位的掩码长度：

```
deny 0.0.0.0/0 ge 25
```

- 拒绝前缀为 10/8 的所有路由：

```
deny 10.0.0.0/8 le 32
```

- 对于前缀为 192.168.1/24 的路由，拒绝长度大于 25 位的所有掩码：

```
deny 192.168.1.0/24 ge 25
```

- 允许所有前缀为 0/0 的路由：

```
permit 0.0.0.0/0 le 32
```

第 15 章

开放最短路径优先 (OSPF)

开放最短路径优先 (OSPF) 是链路状态内部网关协议。OSPF 路由器将链路状态信息泛洪到相邻路由器，以便 OSPF 区域中的所有路由器全面掌握网络拓扑信息。

根据 IP 版本配备单独的 OSPF 版本：面向 IPv4 网络的 OSPFv2 和面向 IPv6 网络的 OSPFv3。这些版本相互独立；也就是说，OSPFv3 不是 OSPFv2 的替代品。

可以使用 Smart CLI 对象配置 OSPFv2，从而将设备集成到 OSPFv2 网络拓扑中。无法配置 OSPFv3。

配置 OSPFv2 进程和区域

使用 威胁防御最多可配置 2 个 OSPFv2 进程。进程编号仅供内部指示；无需匹配其他设备上使用的任何进程编号，但为了跟踪方便，您可采用一致的编号。

如果对任何内部网络使用专用网络编号（例如 192.168.1.0/24），则可能需要将专用地址与公共地址分离开来，对这些内部网络使用一个 OSPFv2 进程，对外部公共可寻址网络使用第二个进程。即使不使用专用编号，也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。如果使用 NAT，而 OSPF 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。

相反，网络中确实存在区域编号，并且必须使用其他邻接路由器使用的相同编号。如果配置单区域网络，请使用“区域 0”（也称为主干区域）。对于采用分层网络设计的多区域网络，您必须了解网络中定义的区域以及该设备应参与的区域。

如果使用虚拟路由器，则可以为每个虚拟路由器配置 2 个 OSPFv2 进程。

以下过程介绍如何创建单个 OSPFv2 进程。重复此过程以创建第二个进程。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 OSPF 的路由器的查看图标 ()。

步骤 3 点击 **OSPF** 选项卡。

步骤 4 执行以下操作之一：

- 要创建新进程，请点击 **+** > **OSPF** 或点击**创建 OSPF 对象** > **OSPF** 按钮。
- 点击要编辑的对象的编辑按钮 ()。请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

如果不再需要进程，请点击该对象的垃圾桶图标将其删除。

步骤 5 输入对象的名称和说明（可选）。

步骤 6 配置基本进程属性：

- **router ospf** *process-id*。点击 *process-id* ，然后输入一个介于 1-65535 之间的数字。此数字仅在此设备中有意义，无需与其他路由器上配置的任何进程编号匹配。编号在虚拟路由器中必须是唯一的。
- **log-adj-changes** *log-state*。点击 *log-state* 并选择以下选项之一：
  - **enable**（推荐）- 在 OSPFv2 邻居启动或关闭时会生成系统日志消息。如果选择此选项，则会向对象添加额外的 **log-adj-changes** *log-type* 行。点击 *log-type*，然后选择 **detail** 是否要为每种状态更改生成系统日志消息，而不仅只在邻接设备启动或关闭时生成。

    如果不需要详细消息，只需将 *log-type* 选项保留即可。请勿从对象中删除此行。
  - **disable**- 系统不会生成系统日志消息。向对象添加 **no log-adj-changes** 行：不要删除此行。

步骤 7 点击对象正文上方的**显示已禁用**链接，添加所有其他可能的配置行。

步骤 8 配置区域编号。

a) 点击 **area** *area-id* 行左侧的 **+** 以启用命令。在启用命令之前，您无法对其进行配置。

b) 点击 *area-id* 并输入区域编号。此区域编号需要与定义 OSPFv2 区域的其他路由器所使用的编号相同。您可以将区域 ID 指定为十进制数字或 IP 地址。有效十进制值范围为 0 到 4294967295。

步骤 9 配置应在区域内路由的网络和接口。

a) 点击 **configure area** *area-id* 选项行左侧的 **+**。

b) 点击 *area-id* 并输入 **area** 命令中相同的区域编号。

c) 点击选项并选择 **properties**。此操作会添加多个行，包括默认情况下启用的 **network** 命令行。

d) 在 **network** 命令中，点击 *network-object*，然后选择用于定义此区域中应包含网络的对象。通常是一个直连网络。例如，如果内部接口的 IP 地址为 192.168.1.1/24，则此命令的关联网络对象将包含 192.168.1.0/24。如果对象尚不存在，请点击**创建新网络**并立即创建。

e) （可选。）在 **network** 命令中，点击 *tag-interface* 并选择托管或路由到网络的接口。如果选择接口，系统会阻止您更改接口的地址，因为在路由进程中会使用该地址。这有助于提醒您，对接口地址进行的任何更改都可能会影响您的路由配置。

如果您在此处选择一个接口，然后再更改接口的地址，则必须先将其从路由进程中删除。然后，在更改 IP 地址后，记得返回此处并选择新的网络和接口，以确保路由进程配置正确。

f) 所有其他新的区域行均为可选项，默认情况下禁用。仅在需要这些服务时才进行配置。有关详细信息，请参阅自定义 OSPF 进程和区域特性，第 361 页。

步骤 10 如果要为多区域网络配置进程，请将鼠标悬停在 **area** 和 **configure area** 行左侧带圆圈的 **-** 上并点击 **...** > **复制**。然后，按照上述说明配置新区域及其网络。重复此过程，直到定义此路由进程应参与的所有区域。

步骤 11 点击**确定 (OK)**。

自定义 OSPF 进程和区域特性

OSPF 中包括许多具有默认值的选项。这些值适用于许多网络。但是，您可能需要调整一个或多个设置才能实现所需精确行为。以下主题介绍可用于自定义 OSPFv2 路由进程的各种方式。

配置 OSPF 进程的高级设置

您可以配置多个设置来控制 OSPFv2 进程的整体行为，包括距离度量、计时器、正常重启，以及用于发送链路状态通告和其他路由更新的路由器 ID。其中许多设置的默认值适用于大多数网络。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 OSPF 的路由器的查看图标 ( )。

步骤 3 点击 **OSPF** 选项卡。

步骤 4 添加或编辑 OSPF 进程对象。

步骤 5 查找 **setup ospf** 行。

添加对象时，必须点击**显示已禁用**链接以查看该行。然后，点击 **+** 以启用该命令，然后点击配置并选择 **advanced**。默认情况下将启用的命令已使用其默认值启用。

编辑对象时，该行将已启用。

此过程的其余部分假定您已点击**显示已禁用**。如果看不到命令，请确保公开已禁用的命令。

步骤 6 （可选。）配置路由器 ID。

点击 + 启用 **router-id** 命令，然后点击变量，并输入从此设备发送任何路由器更新时应使用的 IPv4 地址。OSPF 系统中的任何两个路由器都不能具有相同的路由器 ID，因此请确保它在该区域中是唯一的。

如果未明确指定进程的路由器ID，系统会使用分配给主用接口的最高IP地址。因此，如果您禁用所选接口，或者更改其地址，则路由器 ID 可能会更改。通过明确分配路由器 ID，可以确保进程的一致性。

步骤 7 （可选。）在计算汇总路由成本时，请配置 RFC 1583 兼容性。

点击 + 启用 **configure summary-route-cost** 命令，然后点击此变量并选择 **any**关闭 RFC 1583 兼容性或选择 **rfc1583** 打开 RFC 1583 兼容性。

即使 OSPF 对象中默认未启用此命令，但实际上 RFC 1583 兼容性也是在计算汇总路由成本时使用的默认方法。如果您检查 CLI 中定义的配置，便会发现系统仅显示已禁用的设置。

在启用了RFC 1583兼容性的情况下，可能会出现路由环路。禁用它可以防止路由环路的出现。确保在 OSPF 路由域中的所有 OSPF 路由器上均设置相同的 RFC 1583 兼容性。

步骤 8 （可选。）抑制对应于组播 OSPF (MOSPF) 链路状态通告 (LSA) 的系统日志消息。

点击 + 启用 **ignore lsa mospf** 命令。

系统不支持 LSA 类型 6 MOSPF 数据包。您可以启用此命令，确保系统在收到这些数据包时不会发送系统日志消息，从而减少系统日志服务器中的噪音。

步骤 9 配置距离度量。

默认情况下已启用以下 **distance** 命令。您可以根据路由类型更改 OSPF 路由管理距离。距离范围为从 1 到 255，数字越大，受信任程度越低。比较来自不同进程的类似路由时，这些度量用于判断已获知路由的相对值。

- **distance ospf inter-area 110**。点击数字，然后设置区域间所有路由的距离。
- **distance ospf intra-area 110**。点击数字，然后设置区域内所有路由的距离。
- **distance ospf external 110**。点击数字，然后设置通过重新分发获取的其他路由域中的路由的距离。

步骤 10 配置 OSPF 进程的路由计算计时器。

以下计时器命令已使用这些默认值启用。

- **timers lsa arrival 1000**。点击数字并设置系统接受来自 OSPF 邻居的相同链路状态通告 (LSA) 的最小间隔，范围介于 0 到 600000 毫秒之间。使用此命令指示接受从邻居到达的相同 LSA 必须经过的最短间隔。忽略在此最短时间间隔之前实现的 LSA。
- **timers pacing flood 33**。点击数字，然后设置泛洪队列中的 LSA 在两次更新之间调速的时间，范围为从 5 到 100 毫秒。
- **timers pacing lsp-group 240**。点击数字，然后设置 OSPF 链路状态通告 (LSA) 收集到组中以及刷新、验证校验和或老化的间隔，范围为从 10 到 1800 秒。

- **timers pacing retransmission 66**。点击数字，然后设置重新传输队列中 LSA 调速的时间间隔，范围为从 5 毫秒到 200 毫秒。除非满足 OSPF 数据包泛洪要求的所有其他选项均已用尽，否则不建议更改数据包重新传输定步计时器。具体而言，应配置汇总、末节区域使用、队列调整和缓冲区调整，然后再更改默认泛洪计时器。
- **timers throttle lsa 0 5000 5000**。点击数字，然后设置“开放最短路径优先”(OSPF) 链路状态通告 (LSA) 生成的速率限制值。LSA 和 SPF 限制提供一种动态机制，在网络不稳定时减慢 OSPF 中的 LSA 更新的速度，并确保加速 OSPF 融合。值为：
  - **开始时间间隔**（第一个数字）- 首次生成 LSA 的最小延迟，范围为从 1 到 600000 毫秒。本地 OSPF 拓扑更改后立即生成 LSA 的第一个实例。仅在经过此间隔后才会生成下一 LSA。指定 0 以生成 LSA 且不会产生任何延迟。
  - **保持时间**（第二个数字）- 再次生成 LSA 的最小延迟，范围为从 1 到 600000 毫秒。此值用于计算 LSA 生成的后续速率限制时间。
  - **最大间隔**（第三个数字）- 再次生成 LSA 的最大延迟，范围为从 1 到 600000 毫秒。
- **timers throttle spf 5000 10000 10000**。点击数字，然后设置“最短路径优先”(SPF) 生成的速率限制值。值为：
  - **开始间隔**（第一个数字）- 接收 SPF 计算变更的延迟，范围为从 1 到 600000 毫秒。
  - **保持时间**（第二个数字）- 第一次与第二次 SPF 计算之间的延迟，范围为从 1 到 600000 毫秒。
  - **最大间隔**（第三个数字）- SPF 计算的最长等待时间，范围为从 1 到 600000 毫秒。

步骤 11 （可选。）将默认外部路由生成到 OSPF 路由域。

点击 **+** 启用 **default-information originate** 命令。您可以选择启用并配置以下命令来微调功能：

- **default-information originate always**。即使没有默认路由，也始终通告默认路由。
- **default-information originate metric 1 metric-type** *metric-type-value*。用于生成默认路由的指标类型和值。
  - 点击 **metric** 数字并输入 OSPF 默认指标值，范围为从 0 到 16777214。除非您知道需要使用不同的值，否则请输入 10。
  - 点击 **metric-type** 数字，然后选择 1 或 2 作为与通告到 OSPF 路由域中的默认路由关联的外部链路类型。默认值为 2。
- **default-information originate route-map** *route-map*。选择一个路由映射，用于指定在满足路由映射的情况下生成默认路由的路由进程。

步骤 12 （可选。）如果为设备配置了高可用性 (HA)，请配置无间断转发 (NSF) 平稳重启。

系统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。无间断转发(NSF)功能允许在恢复路由协议信息的同时沿已知路由继续转发数据。此功能在以下情况下有用：

存在组件故障（例如，在 HA 模式中主用设备故障转移到备用设备，或者在集群中主设备发生故障而从属设备被选为新的主设备），或者已计划无中断软件升级。

通过使用 NSF Cisco（RFC 4811 和 RFC 4812）或 NSF IETF (RFC 3623)，您可以在 OSPFv2 上配置平稳重启。

您可以将设备配置为支持 NSF 或支持 NSF。支持 NSF 功能的设备可以向邻居表明其自己的重启活动，而支持 NSF 感知的设备可以帮助重新启动邻居。

- 可以将设备配置为 NSF 感知设备，而与其所处的模式无关。
- 设备必须处于高可用性（故障转移）或跨区 EtherChannel (L2) 集群模式下，您才能将其配置为支持 NSF 功能的设备。

注释 如果还配置了平稳重启，则不能将 OSPF 进程配置为使用 fast hello 数据包。由于 fast hello 数据包不会发生平稳重启，这是因为主用设备和备用设备之间的角色更改所需的时间超过所配置的 dead 间隔。

要配置平稳重启，请执行以下操作：

a) 点击 **+** 启用 **configure nsf graceful-restart** 命令。

b) 点击机制变量，然后选择以下选项之一：

- **cisco** 根据思科 RFC 4811 和 RFC 4812 配置可支持 NSF 功能的设备。
- **ietf** 根据 IETF RFC 3623 配置可支持 NSF 功能的设备。
- **both** 将设备配置为 NSF 感知助手，而不是可支持 NSF 功能的设备。
- **none** 禁用平稳重启（如果之前已配置）。

c) 您在上一步中所做的选择会根据您的规范添加实施正常重启所需的命令。请勿禁用这些命令。只有一个命令可选择性地需要进一步配置。以下是对已添加命令的说明；此命令的 **no** 形式会关闭相关功能。

- **nsf cisco helper**。启用思科无间断转发 (NSF) 助手模式。支持 NSF 的 威胁防御 设备执行平稳重启时，助手 威胁防御 设备将协助无间断转发恢复过程。
- **nsf ietf helper** *mode-option*。启用 IETF 无间断转发（NSF）助手模式。支持 NSF 的 威胁防御 设备执行平稳重启时，助手 威胁防御 设备将协助无间断转发恢复过程。或者，您可以点击*mode* 选项，并启用严格链路状态通告 (LSA) 检查。严格 LSA 检查启用后，如果助手系统检测到将导致重启系统的 LSA 变更，或平稳重启过程启动时重启系统的重新传输列表上有更改的 LSA，它将终止帮助重启系统的过程。
- **capability lls**。启用本地链路信令 (LLS)，这是执行思科平稳重启时所必需的操作。
- **capability opaque**。启用不透明链路状态通告 (LSA)，这是执行 IETF 平稳重启时所必需的操作。

步骤 13 点击**确定 (OK)**。

配置 OSPF 区域属性

您可以配置多个 OSPF 区域参数。可以定义在此区域中通告的网络，以及过滤和虚拟链路。此外，这些区域参数包括设置身份验证、定义末节区域以及向默认汇总路由分配特定开销。身份验证提供基于密码的区域非授权访问防御。

配置区域参数时，您需要了解系统在该区域内的工作方式。

在多个区域中具有接口的路由器称为区域边界路由器 (ABR)。充当网关以在使用 OSPF 的路由器与使用其他路由协议的路由器之间重新分发流量的路由器称为自治系统边界路由器 (ASBR)。

ABR 使用链路状态通告 (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，您可以具有单独的专用和公共区域（以系统作为 ABR）。3 类 LSA（区域间路由）可以从一个区域过滤到另一个区域，从而允许您在不通告专用网络即的情况下配合使用 NAT 和 OSPF。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 OSPF 的路由器的查看图标 ( )。

步骤 3 点击 **OSPF** 选项卡。

步骤 4 添加或编辑 OSPF 进程对象。

步骤 5 配置区域编号。

a) 点击 **area** *area-id* 行左侧的 + 以启用命令。在启用命令之前，您无法对其进行配置。

b) 点击 *area-id* 并输入区域编号。此区域编号需要与定义 OSPFv2 区域的其他路由器所使用的编号相同。您可以将区域 ID 指定为十进制数字或 IP 地址。有效十进制值范围为 0 到 4294967295。

步骤 6 配置应在区域内路由的网络和接口。

a) 点击 **configure area** *area-id* 选项行左侧的 +。

b) 点击 *area-id* 并输入 **area** 命令中相同的区域编号。

c) 点击选项并选择 **properties**。此操作会添加多个行，包括默认情况下启用的 **network** 命令行。

d) 在 **network** 命令中，点击 *network-object*，然后选择用于定义此区域中应包含网络的对象。通常是一个直连网络。例如，如果内部接口的 IP 地址为 192.168.1.1/24，则此命令的关联网络对象将包含 192.168.1.0/24。如果对象尚不存在，请点击**创建新网络**并立即创建。

e) （可选。）在 **network** 命令中，点击 *tag-interface* 并选择托管或路由到网络的接口。如果选择接口，系统会阻止您更改接口的地址，因为在路由进程中会使用该地址。这有助于提醒您，对接口地址进行的任何更改都可能会影响您的路由配置。

如果您在此处选择一个接口，然后再更改接口的地址，则必须先将其从路由进程中删除。然后，在更改 IP 地址后，记得返回此处并选择新的网络和接口，以确保路由进程配置正确。

步骤 7 （可选。）配置发送到末节区域或次末节区域 (NSSA) 的默认汇总路由的开销。

仅当将区域配置为末节或 NSSA 时，此选项才有意义，如下所述。点击 + 以在区域属性中启用以下命令：

area *area-id* **default-cost 1**

（如有必要）输入正确的区域ID。然后，点击数字并输入路由的相对开销，范围为从0到16777214。默认值为 1。编号越高，路由将在用于目标的另一个路由上使用的可能性越低。

步骤 8 （可选。）为区域配置前缀过滤。

可以在区域边界路由器 (ABR) 的OSPFv2区域之间过滤在第3类链路状态通告 (LSA) 中通告的前缀。前缀过滤功能可改善您对各 OSPF 区域之间的路由重新分发的控制。借助前缀过滤，可以仅允许将指定的前缀从一个区域发送到另一个区域，并限制其他所有前缀。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。

在配置此命令之前，您必须在**设备 (Device)** > **高级配置 (Advanced Configuration)** 页面上创建前缀列表（这些列表是 Smart CLI 对象）。可为入站或出站通告配置单独的前缀列表：选择 filter-direction 参数的方向。

area *area-id* **filter-list prefix** *prefix-list filter-direction*

步骤 9 （可选。）将区域配置为末节区域。

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。必须在末节区域中使用默认路由，才能使其正常工作。要进一步减少发送到末节区域中的 LSA 数量，您可以在 ABR 上使用 **area stub** 命令的 **no-summary** 关键字，以防止其将汇总链路通告（3 类 LSA）发送到该末节区域中。

要将区域配置为末节区域，请执行以下操作：

a) 点击设置项 area-id（作为类型行）左侧的 +。
b) 点击类型并选择 **stub**。这将在此设置行后添加 area stub 命令。
c) 或者，在 **area stub** 命令中点击 *stub-parameters*，然后选择 **no-summary**。

步骤 10 （可选。）将区域配置为次末节区域 (NSSA)。

次末节区域 (NSSA) 类似于末节区域。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 区域边界路由器 (ABR) 转换为在整个路由域中泛洪的 5 类 LSA。在转换过程中支持汇总和过滤。

如果您是ISP或网络管理员，并且必须将使用OSPFv2的中心站点连接到通过将连接区域作为NSSA运行而使用其他路由协议的远程站点，则可以简化管理。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，这意味着需要保持两种路由协议。通常将运行一个简单协议（例如 RIP）以处理重新分发。在使用 NSSA 的情况下，您可以通过将企业路由器和远程路由器之间的区域定义为 NSSA 来将 OSPFv2 扩展至覆盖远程连接。

使用此功能之前，请遵循以下准则：

- 您可以设置用于到达外部目标的 7 类默认路由。配置时，路由器会生成到 NSSA 或 NSSA 区域边界路由器中的 7 类默认路由。
- 同一区域内的每个路由器都必须同意区域为 NSSA；否则，路由器无法相互通信。

要将区域配置为 NSSA，请执行以下操作：

a) 点击 **setup** *area-id* **as** *type* 行左侧的 +。
b) 点击类型并选择 **nssa**。这将在设置行后添加多个命令，包括 **area nssa** 命令（必须保持启用状态）。
c) （可选。）要在 NSSA 中生成 7 类默认路由，请点击“+”以启用以下命令：

area *area-id* **nssa default-information-originate metric 1 metric-type 2**

可以选择性地调整以下值：

- 点击 **metric** 数字并输入 OSPF 默认指标值，范围为从 0 到 16777214。除非您知道需要使用不同的值，否则请输入 10。
- 点击 **metric-type** 数字，然后选择 1 或 2 作为与通告到 OSPF 路由域中的默认路由关联的外部链路类型。默认值为 2。

d) （可选。）如果系统是 ABR，并且您想要从其他路由协议中重新分发以仅将路由导入正常区域而不导入 NSSA 中，请点击 + 启用以下命令：

area *area-id* **nssa no-redistribution**

e) （可选。）如果不想将汇总路由注入 NSSA 中，请点击 + 启用以下命令：

area *area-id* **nssa no-summary**

步骤 11 （可选。）为区域配置虚拟链路。

在 OSPF 中，所有区域必须连接到主干区域。如果中断与主干的连接，可以通过建立虚拟链路进行修复。您可以配置与已连接到主干区域的路由器的虚拟链路。

a) 点击 **configure area** *area-id* **virtual-link** *ip_address option* 行左侧的 +。
b) 点击 *ip_address*，然后输入要为其建立虚拟链路的路由器的路由器 ID。
c) （可选。）点击选项并选择 **properties** 调整以下属性，这些属性具有适用于大多数网络的默认值。这些命令的第一部分被省略，因为此部分相同命令中的参数：

- **authentication** *auth-type*。点击 + 启用命令，点击 *auth type* ，然后选择 **none**、**password** 或 **message-digest**。如果您选择了除 none 以外的其他选项，请配置关键选项。这些选项与您在 OSPF 接口上配置的选项相同，如配置 OSPFv2 接口设置和 OSPF 身份验证，第 373 页中所述。仅在其他路由器将使用身份验证的情况下才配置身份验证。
- **hello-interval 10**。点击数字，然后输入在接口上两次发送 hello 数据包之间的间隔，范围为从 1 到 65535 秒。
- **retransmit-interval 5**。点击数字，然后输入虚拟链路的两次 LSA 重新传输之间的时间，范围为从 1 到 65535 秒。
- **transmit-delay 1**。点击数字，然后输入 OSPF 收到拓扑更改与启动“最短路径优先”(SPF) 计算之间的延迟时间，范围为从 0 到 65535 秒。

d) 您可以点击 **...** > **复制**（位于 **configure area virtual-link** 命令的旁边）以定义另一个虚拟链路。根据需要定义任意数量的虚拟链路。

步骤 12 （可选。）如果系统是区域边界路由器 (ABR)，请配置要合并的各范围或汇总区域的各路由。

配置 **area range** 命令时，所得结果是通过 ABR 将单个汇总路由通告给其他区域。在区域边界压缩路由信息。在区域之外，对于每个地址范围通告单个路由。此行为称为路由汇总。可以为一个区域配置多个 **area range** 命令。这样，OSPF 将可以汇总许多组不同地址范围的地址。

要配置路由汇总，请执行以下操作：

a) 点击 **area** *area-id* **range** *network-object range-parameters* 行左侧的 **+**。
b) 点击 *network-object*，然后选择用于定义要汇总其内路由的地址范围的网络对象。
c) （可选。）点击 *range-parameters*，然后选择以下其中一个属性：

- **advertise**。设置地址范围状态以通告并生成 3 类汇总链路状态通告 (LSA)。如果选择 no 选项，则此项为默认设置。
- **not-advertise**。地址范围状态设置为 DoNotAdvertise。抑制 3 类汇总 LSA，并保持向其他网络隐藏组件网络。

d) 您可以点击 **...** > **复制**（位于 **area range** 命令的旁边）以定义另一个路由汇聚。根据需要定义任意数量的虚拟链路。

步骤 13 如果要为多区域网络配置进程，请将鼠标悬停在 **area** 和 **configure area** 行左侧带圆圈的 **-** 上并点击 **...** > **Duplicate**。然后，按照上述说明配置新区域及其网络和其他设置。重复此过程，直到定义此路由进程应参与的所有区域。

步骤 14 点击**确定 (OK)**。

配置静态 OSPF 邻居

您需要定义静态 OSPF 邻居来通过点对点非广播网络（即 VPN 隧道）通告 OSPF 路由。

您不需要定义常规广播网络上的静态邻居，因为这些路由器可以形成邻接关系。

开始之前

确定系统应通过其访问邻居的接口。您必须先配置此接口的OSPF设置，然后才能定义邻居路由器。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 OSPF 的路由器的查看图标 ( )。

步骤 3 点击 **OSPF** 选项卡。

步骤 4 添加或编辑 OSPF 接口对象，并为所选接口启用 **ospf network point-to-point non-broadcast** 命令。保存更改。

步骤 5 添加或编辑 OSPF 进程对象。

步骤 6 点击**显示已禁用**以显示所有命令，然后点击 **+** 以启用 **neighbor** 命令。

步骤 7 配置邻居地址。

neighbor *ip-address* **interface** *interface*

- 点击 *ip-address*，然后输入邻居路由器的 IP 地址。
- 点击 *interface*，然后选择系统可以通过其访问路由器的接口。

步骤 8 如有必要，请为邻居路由器配置静态路由。

如果路由器的 IP 地址与所选接口位于同一网络中，则无需静态路由。例如，如果您选择 IP 地址为 10.100.10.1/24 的接口，且邻居地址为 10.100.10.2/24，则不需要静态路由。

步骤 9 您可以点击 **...** > **复制**（位于 **neighbor** 命令的旁边）以定义另一个静态邻居。根据需要定义任意数量的虚拟链路。

步骤 10 点击**确定 (OK)**。

配置 OSPF 汇总地址

将来自其他协议的路由重新分发到 OSPF 中时，将在外部 LSA 中单独通告每个路由。但是，您可以将系统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。可将标签值用作匹配值，以通过路由映射控制重新分发过程。

路由汇总是通告地址的整合。可以汇总从其他路由协议获知的路由。用于通告汇总的指标是所有较为具体路由的最小指标。汇总路由帮助减小路由表的大小。

对 OSPF 使用汇总路由会导致 OSPF ASBR 将一个外部路由通告为该地址覆盖的所有重新分发的路由的聚合。只能汇总重新分发到 OSPF 中的来自其他路由协议的路由。

开始之前

为要汇总的所有地址创建网络对象。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 OSPF 的路由器的查看图标 ( )。

步骤 3 点击 **OSPF** 选项卡。

步骤 4 添加或编辑 OSPF 进程对象。

步骤 5 点击**显示已禁用**以显示所有命令，然后点击 + 启用 **configure** *network-object* **as** *option* **summary-address** 命令。

步骤 6 点击 *network-object*，然后选择用于定义要汇总的地址空间的对象。

步骤 7 点击 *option* 并选择以下选项之一：

- **advertising**。通告与地址匹配的路由。

- **non-advertising**。抑制与地址匹配的路由。

步骤 8 （可选。）要将标签值添加到汇总的路由，请点击 + 启用 **summary-address tag** 命令，点击 *tag-number* 变量，然后输入标签编号，范围为从 0 到 4294967295。

OSPF 本身不使用此值。可以使用它在自治系统边界路由器 (ASBR) 之间传递信息。如果未指定任何值，则会将远程自治系统编号用于来自 BGP 和 EGP 的路由；对于其他协议，使用零 (0)。

标签值主要用于根据标签编号控制重新分发。如果不在重新分发的路由映射中使用它，则无需在此处进行配置。

步骤 9 您可以点击 **...** > **复制**（位于 **configure summary-address** 命令的旁边）以定义另一个路由汇聚。根据需要定义任意数量的虚拟链路。

步骤 10 点击**确定 (OK)**。

配置 OSPF 过滤规则

创建每个过滤规则所需的 Smart CLI 标准访问权限列表对象。使用拒绝访问控制条目 (ACE) 过滤掉与条目匹配的路由，并允许应更新的路由的 ACE。

开始之前

您可以配置区域边界路由器 (ABR) 3 类 LSA 过滤器，以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。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 OSPF 的路由器的查看图标 ( )。

步骤 3 点击 **OSPF** 选项卡。

步骤 4 添加或编辑 OSPF 进程对象。

步骤 5 点击**显示已禁用**以显示所有命令，然后点击 + 以启用 **configure filter-rules** *direction* 命令。

步骤 6 点击方向，然后选择 **in** 以对传入更新进行过滤，或选择 **out** 来过滤出站更新。

步骤 7 对于入站过滤器，可以选择性地指定用于过滤更新的接口。如果不指定接口，则过滤器将应用于在任何接口上接收的所有更新。

a) 点击 + 启用 **distribute-list** *acl-name* **in interface** *interface* 命令。

b) 点击 *interface* 变量并选择接口。

步骤 8 对于出站过滤器，您可以选择性地指定协议，以将过滤器限制为通告到该路由进程的路由。

有两种形式的 **distribute-list out** 命令，一种是在 *protocol* 变量后跟一个 *identifier* 变量，另一种则不带标识符。您可以选择以下协议，但是，这些协议会根据您是否必须提供其他标识符信息来在这些命令版本之间划分。

- **connected**。适用于为直接连接到系统接口的网络而建立的路由。
- **static**。适用于手动创建的静态路由。
- **rip**。适用于通告到 RIP 的路由。
- **bgp** *automonous-system*。适用于通告到 BGP 的路由。点击 *identifier*，然后输入在系统中定义的 BGP 进程的自治系统编号。
- **eigrp** *automonous-system*。适用于通告到 EIGRP 的路由。点击 *identifier*，然后输入在系统中定义的 EIGRP 进程的自治系统编号。
- **ospf** *process-id*。适用于通告到 OSPF 的路由。点击*identifier*，然后为系统上定义的其他 OSPF 进程输入进程 ID。

步骤 9 您可以点击 **...** > **复制**（位于 **configure filter-rules** 命令的旁边）以定义另一个过滤规则。根据需要定义任意数量的虚拟链路。

步骤 10 点击**确定 (OK)**。

配置 OSPF 重新分发

您可以控制从其他路由协议、连接路由和静态路由中将路由重新分发到 OSPF 进程的过程。

开始之前

最佳实践是在将重新分发到 OSPF 之前，配置您将从中重新分发路由的路由进程，并部署更改。

如果要应用路由映射以微调重新分发的路由，请创建 Smart CLI 路由映射对象。将重新分发与路由映射匹配的路由，并且不会重新分发所有不匹配的路由。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 OSPF 的路由器的查看图标 ( )。

步骤 3 点击 **OSPF** 选项卡。

步骤 4 添加或编辑 OSPF 进程对象。

步骤 5 点击**显示已禁用**以显示所有命令，然后点击 **+** 以启用 **configure redistribution** 命令。

步骤 6 点击 *protocol* 变量，并选择要从中重新分发路由的源进程。可以重新分发 **connected** 和 **static** 路由，或由 **bgp**、 **eigrp**、 **isis** 、**ospf** 或 **rip** 生成的路由。

步骤 7 如果选择路由进程，请点击 *identifier* 变量，然后输入所需的值：

- **bgp**、**eigrp**。输入自治系统编号。
- **ospf**。输入进程 ID 编号。
- **connected**、**static**、**isis**、**rip**。输入 **none**。即使您输入其他值，它也会被忽略。

步骤 8 （可选；仅限 IS-IS。）在 **redistribute isis level-2** 命令中，点击 **level-2** 并选择是否要仅重新分发在 IS-IS 区域 (**level-1**) 中、在 IS-IS 区域 (**level-2**) 之间或两者 (**level-1-2**) 中获知的路由。

步骤 9 （可选；所有协议。）如果将标签应用于路由以控制重新分发，请点击 **+** 启用 **redistribute tag** *tag-number* 命令，然后点击此变量并输入与要重新分发的路由关联的标签。标签编号范围为从 0 到 4294967295。

步骤 10 （可选；所有协议。）如果要重新分发所有子网的路由，而不仅仅是符合标准类要求的路由，请点击 **+** 启用 **redistribute subnets** 命令。

例如，如果不启用此命令，将不会重新分发 10.100.10.0/24 的特定路由，而只会重新分发 10.0.0.0/8 的路由。

步骤 11 （可选；所有协议。）要根据路由映射微调重新分配的路由，请点击 **+** 启用 **redistribute** *route-map* 命令，点击此变量，然后选择用于定义限制条件的路由映射。

如果不应用路由映射，则会重新分发进程的所有路由（适合为重新分发而配置的其他命令）。

步骤 12 （可选；所有协议。）要微调用于重新分发的路由的度量，请点击 **+** 启用以下命令并配置选项：

redistribute *protocol* **metric** *metric-value* **metric-type** *metric-type-value*

点击此变量并配置以下内容：

- **metric**。所分配的路由的指标值，范围为从 0 到 16777214。在同一设备上从一个 OSPF 进程重新分发到另一个OSPF进程时，如果未指定指标值，则会将指标从一个进程携带至另一个进程。将其他进程重新分发到 OSPF 进程时，默认指标为 20。
- **metric-type**。指标类型是与通告到 OSPF 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）。默认值为 2。

步骤 13 （可选；仅限OSPF。）当您从其他OSPF进程重新分发路由时，默认情况下会启用以下命令。可以点击 **-** 禁用不需要的命令。

这些命令用于指定将 OSPF 路由重新分发到其他路由域的条件。

- **redistribute ospf match external 1**。自治系统的外部路由，但是会作为 1 类外部路由导入 OSPF。
- **redistribute ospf match external 2**。自治系统的外部路由，但是会作为 2 类外部路由导入 OSPF。
- **redistribute ospf match internal**。特定自治系统的内部路由。
- **redistribute ospf match nssa-external 1**。自治系统的外部路由，但是会作为 1 类外部路由导入 OSPF，并仅标记为次末节区域 (NSSA)。
- **redistribute ospf match nssa-external 2**。自治系统的外部路由，但是会作为 2 类外部路由导入 OSPF，并仅标记为次末节区域 (NSSA)。

步骤 14 您可以点击 **...** > **复制**（位于 **configure redistribution** 命令的旁边），以配置另一种协议的重新分发。为适合您的网络的每种协议配置重新分发。

步骤 15 点击**确定 (OK)**。

配置 OSPFv2 接口设置和 OSPF 身份验证

任何面向邻居 OSPF 路由器的接口都使用 hello 数据包和其他方法与路由器通信，以验证邻居的运行状况并共享路由更新。虽然部分特征具有默认设置，但最佳做法是使用 OSPF 接口设置对象明确设置选项。为与 OSPF 邻居路由器邻接的每个接口创建对象。

注释 特定网络上的路由器必须具有相同的身份验证值、邻居丢失检测 hello 和 dead 间隔值。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 OSPF 的路由器的查看图标 ( )。

步骤 3 点击 **OSPF** 选项卡。

步骤 4 执行以下操作之一：

- 要创建新对象，请点击 **+** > **OSPF 接口设置**，或点击**创建 OSPF 对象** > **OSPF 接口设置**按钮。
- 点击要编辑的对象的编辑按钮 ( )。请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

如果不再需要接口设置对象，请点击该对象的垃圾桶图标将其删除。

步骤 5 输入对象的名称和说明（可选）。

步骤 6 为接口配置身份验证。

configure authentication *auth-type*

要配置 OSPF 身份验证，必须在每个 OSPF 接口上配置密码或身份验证密钥，然后在此区域本身启用身份验证。必须在接口和区域上选择相同的身份验证方法。

可以点击 *auth type* 选择以下选项。

- **none** - 不使用 OSPF 身份验证。在链路上运行的任何 OSPF 路由器都可以与此路由器建立邻接关系。将以下命令添加到对象：**ospf authentication null**。
- **password** - 使用共享密码对 OSPF 连接进行身份验证。可以逐个接口配置每个网络的单独密码。但是，同一网络上的所有相邻路由器都必须具有相同的密码才能交换 OSPF 信息。

选择此选项时，系统会添加两个命令：**ospf authentication** 和 **ospf authentication-key** *key*。点击变量以配置以下内容：

- *key* - 选择包含密码的密钥对象。密码不得超过 8 个字符。可以在两个字符之间包含空格。密码开头或结尾的空格将被忽略。如果对象尚不存在，请点击列表底部的**创建新密钥**，立即创建对象。

- **message-digest** - 使用消息摘要 (MD5) 对 OSPF 连接进行身份验证。MD5 身份验证负责验证通信的完整性、认证信源并检查时效性。必须将两台路由器配置为使用相同的 MD5 密钥。

  选择此选项时，系统会添加两个命令：**ospf authentication message-digest** 和 **ospf message-digest-key** *key-id* **md5** *key*。点击变量以配置以下内容：

  - *key-id* - 身份验证密钥编号，从 1 到 255。您必须使用相同的密钥 ID 和关联的 MD5 密钥配置邻居路由器。
  - *key* - 选择包含 MD5 密钥的密钥对象。密钥是不超过 16 个字符的字母数字密码。字符之间可包含空格。密钥开头或结尾的空格将被忽略。如果对象尚不存在，请点击列表底部的**创建新密钥**，立即创建对象。

步骤 7 （可选。）配置链路状态通告 (LSA) 计时器。

这些计时器具有默认值，因此只有在网络需要不同的设置时才需要更改。配置以下命令：

- **ospf retransmit interval 5** - 属于 OSPF 接口的邻接设备的 LSA 重新传输间隔秒数：秒数必须大于连接的网络上任意两个路由器之间的预期往返延迟。范围是从 1 到 8192 秒。默认值为 5 秒。点击 5，然后键入新数字以更改该值。
- **ospf transmit-delay 1** - 在 OSPF 接口上发送链路状态更新数据包所需的预计秒数，介于 1 到 8192 秒。默认值为 1 秒。点击 1，然后键入新数字以更改该值。

步骤 8 （可选。）所有其他设置均具有默认值，或处于可选状态。仅当需要其他操作时，才可以更改或启用它们。点击**显示已禁用**链接以显示选项。

以下是其他接口设置。要启用设置，请点击命令左侧的 **+**，然后配置命令（如有需要）。

- **ospf cost** *value* - 在 OSPF 接口上发送数据包的（链路状态指标）开销，介于 1 到 65535 之间。值 1 表示直接连接到接口的网络。点击变量，并根据您在网络中使用的数字输入表示接口功能的开销。

  在确定值时，接口带宽越高，在该接口上发送数据包所需的关联开销就越低。换句话说，较大的开销值表示低带宽接口，而较低开销值表示高带宽接口。您选择的特定数字没有固有含义：该值与您在OSPF区域中为接口配置的其他值相关。然后，这些值会影响目标的最佳路由计算。

  威胁防御设备上的 OSPF 接口默认开销为 10。此默认值与 Cisco IOS 软件不同，后者的默认开销为 1（适用于快速以太网和千兆以太网）和 10（适用于 10BaseT）。如果您在网络中使用 ECMP，则必须此情况考虑在内。

- **ospf database-filter all out** - 在同步和泛洪期间，过滤掉流向 OSPF 接口的所有传出 LSA。

- **ospf mtu-ignore** - 在接收数据库数据包时禁用 OSPF 最大传输单位 (MTU) 不匹配检测。OSPF 检查邻居在公用接口上是否使用同一 MTU。当邻居交换数据库描述符 (DBD) 数据包时，将执行此检查。如果 DBD 数据包中的接收 MTU 高于传入接口上配置的 MTU，则不建立 OSPF 邻接。如果不能将接口上的 MTU 值调整为相同值，则可以禁用 MTU 检查功能。
- **ospf network point-to-point non-broadcast** - 将 OSPF 接口配置为点对点非广播网络。允许您通过 VPN 隧道传输 OSPF 路由。如果配置此选项，则不可能动态发现邻居。您还必须：
  - 更新 OSPF 进程对象，以定义此接口的单个静态邻居。另外，更新邻居路由器的 OSPF 进程，将此设备定义为其静态邻居。
  - 创建指向邻居路由器的静态路由（在每个路由器上）。
- **ospf priority** *value* - 路由器相对于网络中其他路由器的优先级，介于 0 到 255 之间。默认优先级为 1。如果连接到网络的两台路由器同时尝试成为指定路由器，则优先采用具有较高优先级的路由器。如果优先级相同，则优先采用具有较高路由器 ID 的路由器。优先级设置为 0 的路由器没有资格成为指定路由器或备用指定路由器。点击变量，根据网络中使用的相对编号系统选择优先级。
- **ospf lost-neighbor-detection** *detection-mechanism* - 定义系统如何确定邻居路由器是否已关闭。如果声明OSPF路由器关闭，则OSPF必须重新计算路由。有关配置邻居丢失检测的详细信息，请参阅配置 OSPFv2 邻居丢失检测和 Fast Hello 数据包（OSPF 接口设置），第 375 页。

步骤 9 点击**确定 (OK)**。

配置 OSPFv2 邻居丢失检测和 Fast Hello 数据包（OSPF 接口设置）

OSPF 进程定期向每个邻居路由器发送 hello 数据包，以验证邻居是否仍可响应。持续响应失败表示邻居路由器（完全或仅邻接接口）无法用于路由，OSPF 必须重新计算路由，且OSPF 系统必须在更新的路由表中收敛。

可调整以下值来微调您的网络。理想情况下，您希望最大限度地减少声明邻居关闭和重新计算路由的频率。另一方面，您还希望最大限度地减少 OSPF 路由器（或接口）真正关闭时，网络在正常路由表中重新收敛所需的时间。

- Hello 间隔 - 这是 hello 数据包的发送间隔。默认间隔为 10 秒。如果需要，您可以配置 fast hello 数据包，其中 hello 的发送间隔为次秒级。Fast hello 数据包可以最快的速度检测路由表中的关闭邻居并重新收敛。
- Dead 间隔 - 如果未发现来自邻居的 hello 数据包即宣布邻居无效的时间长度。默认值为 40 秒（默认 hello 间隔的 4 倍），除非使用 fast hello 数据包，在这种情况下，dead 间隔始终为 1 秒。指定较小的 dead 间隔将更快地检测被关闭的邻居并促进收敛，但可能导致路由更加不稳定。在任何情况下，都必须将 dead 间隔配置为大于 hello 间隔。您必须在网络中的所有 OSPF 路由器上设置相同的 dead 间隔。

您可以在 OSPF 接口设置对象中配置邻居丢失检测。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 OSPF 的路由器的查看图标 ( )。

步骤 3 点击 **OSPF** 选项卡。

步骤 4 执行以下操作之一：

- 要创建新对象，请点击 **+** > **OSPF 接口设置**，或点击**创建 OSPF 对象** > **OSPF 接口设置**按钮。
- 点击要编辑的对象的编辑按钮 ( )。请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

步骤 5 如果未显示 **ospf lost-neighbor-detection** *detection-mechanism* 命令，请点击**显示已禁用**链接。

步骤 6 点击命令左侧的 **+** 以启用命令。

步骤 7 点击 *detection-mechanism* ，然后选择要实施的机制：

- **dead-interval**- 配置标准 hello 间隔（以秒为单位）。添加了以下命令；根据需要调整值：
  - **ospf hello-interval 10**- hello 间隔，介于 1 到 8192 秒之间。默认值为 10。此值必须小于 dead 间隔。点击值以输入所需数字。
  - **ospf dead-interval 40** - dead 间隔，介于 1 到 8192 秒之间。建议 dead 间隔值为 hello 间隔的 4 倍，但可以配置较短时间以实现更快收敛。
- **hello-multiplier** - 配置次秒 fast hello 数据包。添加了以下命令，您必须配置该值。
  - **ospf dead-interval minimal hello-multiplier** *value* - 点击变量并输入每秒应发送的 hello 数据包数量，介于 3 到 20 之间。**minimal** 关键字将停顿间隔设置为 1 秒。

步骤 8 点击**确定 (OK)**。

监控 OSPF

要对 OSPF 进行监控和故障排除，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。您还可以从“路由”(Routing) 页面的**命令 (Commands)** 菜单选择其中一些命令。

使用 **show ospf ?** 获取其他选项的列表。例如，您可以指定进程 ID、区域 ID 和虚拟路由器来限制您看到的信息，还可以指定其他选项以仅查看您要查找的信息。以下列表只是一份摘要。

- **show ospf**

  显示有关 OSPFv2 路由进程的一般信息。

- **show ospf border-routers**

  向 ABR 和 ASBR 显示内部 OSPFv2 路由表条目。

- **show ospf database**

  显示与特定路由器 OSPFv2 数据库相关的信息列表。

- **show ospf events**

  显示 OSPF 内部事件信息。

- **show ospf flood-list**

  显示等待通过接口泛洪的 LSA 的列表，以观察 OSPF v2 数据包步调设置。OSPFv2 更新数据包自动设置步调，因此其不会以小于33毫秒的间隔进行发送。如果没有步调设置，则在链路速度缓慢，邻居无法足够快速地接收更新或者路由器可能会用尽缓冲区空间的情况下，某些更新数据包可能会丢失。

  在重新发送的间隔内也会使用步调设置，以提高效率并尽量减少重新传输丢失。您还可以显示等待从接口发出的 LSA。通过步调设置，可以更高效地发送 OSPFv2 更新数据包和重新传输数据包。

- **show ospf interface**

  显示与 OSPFv2 相关的接口信息。

- **show ospf neighbor**

  逐个接口显示 OSPFv2 邻居信息。

- **show ospf nsf**

  显示 OSPFv2 相关的无间断转发 (NSF) 信息。

- **show ospf request-list**

  显示路由器请求的所有 LSA 的列表。

- **show ospf retransmission-list**

  显示等待重新发送的所有 LSA 的列表。

- **show ospf rib**

  显示 OSPF 路由器信息库 (RIB)。

- **show ospf statistics**

  显示各种 OSPF 统计信息，例如 SPF 的执行次数、原因和持续时间。

- **show ospf summary-addresses**

  显示在 OSPFv2 进程下配置的所有汇总地址重新分发信息的列表。

- **show ospf traffic**

  显示由特定 OSPFv2 实例发送或接收的不同类型的数据包的列表。

- **show ospf virtual-links**

  显示与 OSPFv2 相关的虚拟链路信息。

第 16 章

增强型内部网关路由协议 (EIGRP)

增强型内部网关路由协议 (EIGRP) 是一种混合动态距离向量和链路状态内部网关路由协议。它最初是思科开发的专有协议，现在是 RFC 7868 中定义的开放标准。您可以配置 EIGRP 来管理自治系统中的内部路由。

EIGRP 最佳实践

以下是关于配置 EIGRP 的一些提示：

- 如果要将设备插入现有 EIGRP 自治系统，请检查自治系统中其他路由器的配置，以确定系统编号和所有其他自定义配置。确保在您要添加的 威胁防御 设备上实施相同的或至少一致的自定义配置。
- 确定是要配置完整 EIGRP 进程还是末节进程：
  - 如果 威胁防御 设备位于自治系统的中心位置，并且在此位置连接到多个其他 EIGRP 路由器，则您可能需要配置完整 EIGRP 进程。请参阅配置全路由 EIGRP 进程， 第 382 页。
  - 如果 威胁防御 设备位于自治系统的边缘，并且在此位置仅连接到一台其他 EIGRP 路由器，而以其他方式托管所连接的网络，则最好将其配置为末节路由器。在配置末节进程时，可以使 威胁防御 设备将有关所连接路由的信息发送至 EIGRP 邻居，以便自治系统中的其他 EIGRP 路由器可以获得通往 威胁防御 设备连接的网络的路由。请参阅配置末节路由 EIGRP 进程， 第 383 页。
- 默认设置适用于大多数网络，因此仅当您在自治系统中的其他 EIGRP 路由器上调整了这些设置时，才需要调整默认设置。您只需配置自治系统编号并指定要路由的网络，即可实现功能完备的 EIGRP 进程。

- 配置路由器 ID，以确保使用稳定的地址来标识路由器。这有助于简化路由故障排除。请参阅配置 EIGRP 高级设置，第 385 页。
- 请勿启用自动路由汇总（**auto-summary** 命令），除非您确定这样不会形成路由环路，并且会为您的网络带来一些好处。如何确定自动汇总是否适用于您的网络不属于本文档的讨论范围。

关于 EIGRP

增强型内部网关路由协议 (EIGRP) 是一种混合动态距离向量和链路状态内部网关路由协议。EIGRP 将路由更新发送到同一自治系统内的路由器。通常，EIGRP 使用组播更新发现邻居路由器，但您可以配置组播边界之外的静态邻居，而这些静态邻居会获取单播更新。

EIGRP 的收敛技术基于扩散更新算法 (DUAL)。此算法可以确保路由计算过程中每个瞬间的无环路运行，使拓扑更改涉及的所有设备可以同步。未受拓扑更改影响的设备不参与重新计算。

在有限的范围内，您可以调整路由度量以控制路由的选择。以下主题介绍有关这些高级概念的一些背景知识。

注释 如果调整这些度量，则必须对自治系统中的所有路由器进行相同的调整，否则可能会出现路由环路。

DUAL 有限状态机

DUAL 有限状态机 (FSM) 贯穿于所有路由计算的决策过程中。它跟踪所有邻居通告的所有路由。DUAL 使用距离信息（称为度量）来选择高效的无环路路径。

DUAL 根据可行后继路由选择要插入路由表的路由。后继路由是指用于数据包转发的邻居设备，其具有通往目的地的开销最小的路径，且可保证不属于路由环路的一部分。

当拓扑发生变化时，DUAL 将测试可行后继路由。如果有可行后继路由，DUAL 会使用其所找到的任何可行后继路由来避免不必要的重新计算。

当没有可行后继路由而只有通告目的地的邻居时，必须重新计算以确定新的后继路由。重新计算路由所需的时间量会影响收敛时间。

EIGRP 度量权重

EIGRP 在路由和度量计算中使用度量权重（称为 K 值）。为了在大多数网络中提供最佳性能，我们精心挑选了 EIGRP 默认度量。

与 IOS 路由器不同，您无法为 威胁防御 设备上运行的 EIGRP 调整这些默认 K 值。由于您需要在自治网络内的所有系统上使用相同的 K 值，因此不应在包含 威胁防御 设备的自治系统内的任何路由器上更改这些值。

有关如何使用 K 值的说明，请参阅 EIGRP 开销度量，第 381 页。

EIGRP 开销度量

除了链路特征外，EIGRP 还使用度量权重（K 值）来计算复合开销度量。为避免因链路特征变化而造成网络波动，您可以调整此计算中使用的一些值。

实际计算非常复杂，使用五个 K 值（作为乘数）和五个向量属性。但是，三个 K 值默认为 0，并且由于您无法更改默认 K 值，因此实际计算会大大简化：

开销度量 = 256 *（带宽 + 延迟）

您可以更改的是从 EIGRP 进程或向此进程重新分发的路由的带宽和延迟值。具体而言，您可以在 **default-metric** 命令（为所有类型的重新分发路由设置默认值）或 **redistribute metric** 命令（为特定类型的路由设置度量）中调整这些值。请注意以下提示：

- 带宽是路由的最小带宽（以千比特/秒为单位）。它可以是 1 到 4294967295 千字节/秒。该公式的带宽按以下公式缩放和求逆：

  （10^7/最小带宽，以千比特/秒为单位）

- 延迟是路由延迟（以十微秒为单位）。

威胁防御不使用的其他特征是延迟可靠性、路由上的有效负载和路由上的最小 MTU（最大传输单位）。即使未使用这些值，也必须在调整这些命令时对其进行配置。

有关 EIGRP 如何计算开销度量的详细信息，请参阅《*IP* 路由：*EIGRP* 配置指南》。例如，https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-16-7/ire-xe-16-8-book/ire-enhanced-igrp.html。

EIGRP 准则

IPv6 准则

不支持 IPv6。

其他准则

- 最多支持一个 EIGRP 进程。
- 您无法更改 EIGRP 进程的自治系统编号。相反，请删除进程，部署更改，然后使用新的自治系统编号配置新进程。
- 您不能在 EIGRP 进程中包含属于网桥虚拟接口 (BVI) 的网络。
- 每当应用配置更改时，都会发生 EIGRP 邻接摆动，这会导致修改邻居发送或接收的路由信息（尤其是在分发列表、偏移列表中）和更改汇总。路由器同步后，EIGRP 会在邻居之间重新建立邻接关系。断开并重新建立邻接关系后，系统将清除邻居之间的所有已获知路由，并使用新的分发列表重新执行邻居之间的完整同步。

配置核心 EIGRP 进程

以下主题介绍如何在设备上启动并运行 EIGRP。对于不应作为 EIGRP 路由器完全参与自治网络的系统，可以配置完整路由进程，也可以将其配置为末节进程。

配置全路由 EIGRP 进程

您可以配置一个 EIGRP 进程。如果配置多个虚拟路由器，则仅在全局虚拟路由器中支持 EIGRP。

以下程序使用 EIGRP 路由的所有默认值为一组网络设置基本 EIGRP 路由。完成此程序就足以在设备上启用 EIGRP。您可以根据需要完成其他程序来调整 EIGRP 进程。

开始之前

确定您的网络中用于 EIGRP 的自治系统编号。

为要在 EIGRP 自治系统内路由的每个网络创建定义这些网络的网络对象。例如，如果要对 192.168.1.0/24 和 192.168.2.0/24 网络使用 EIGRP，请创建两个网络对象，每个网络对象一个。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击全局虚拟路由器的查看图标 ( )。

步骤 3 点击 **EIGRP** 选项卡。

步骤 4 执行以下操作之一：

- 要创建新进程，请点击 **+** 或点击**创建 EIGRP 对象 (Create EIGRP Object)** 按钮。
- 点击要编辑的对象的编辑按钮 ( )。请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

如果不再需要进程，请点击该对象的垃圾桶图标将其删除。

步骤 5 为 Smart CLI 对象输入**名称**和说明（后者为可选项）。

步骤 6 配置基本进程属性：

router eigrp *autonomous-system*

点击变量，然后输入一个介于 1-65535 之间的数字。使用在网络中其他路由器上使用的相同自治系统编号，该编号应与此设备在同一路由域内运行。

步骤 7 配置应在 EIGRP 自治系统内路由的网络和接口。

a) 点击对象正文上方的**显示已禁用 (Show Disabled)** 链接，添加所有其他可能的配置行。

b) 点击 **network** *network-object* 行左侧的 **+**。

c) 在 **network** 命令中，点击变量，然后选择定义应包含在此自治系统内的网络的对象。

通常是一个直连网络。例如，如果内部接口的 IP 地址为 192.168.1.1/24，则此命令的关联网络对象将包含 192.168.1.0/24。如果对象尚不存在，请点击**创建新网络**并立即创建。

已定义网络范围内的直连和静态网络由此进程通告。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与EIGRP路由，但是该接口已连接到希望通告的网络，请参阅配置 EIGRP 被动路由接口，第 387 页。

d) 如果要路由其他网络，请点击 **...** > **复制**（在 **network** 命令左侧）以添加一个新网络。继续添加 **network** 行，直到您配置了要路由的所有网络。

步骤 8 （可选。）如有必要，请调整其他最初禁用的命令的设置。请参阅自定义 EIGRP 进程，第 385 页。

步骤 9 点击**确定 (OK)**。

配置末节路由 EIGRP 进程

您可以将设备配置为 EIGRP 末节路由器。末节路由可降低系统中的内存和处理要求。作为末节路由器，系统不需要维护完整的 EIGRP 路由表，因为它将所有非本地流量转发到分布路由器。通常情况下，除了发送末节路由器的默认路由以外，分布路由器不需要发送任何其他信息。

只有指定的路由会从末节路由器传播到分布路由器。作为末节路由器，系统使用消息“无法访问”来响应对汇总、已连接路由、重新分发的静态路由、外部路由和内部路由的所有查询。系统会向所有相邻路由器发送特定对等体信息包，报告自己的状态为末节路由器。收到通知其末节状态数据包的任何邻居都不会查询末节路由器是否存在任何路由，且具有末节对等体的路由器也不会查询该对等体。末节路由器依赖于分布路由器将正确的更新发送到所有对等体。

开始之前

确定您的网络中用于 EIGRP 的自治系统编号。

为要在 EIGRP 自治系统内路由的每个网络创建定义这些网络的网络对象。例如，如果要对 192.168.1.0/24 和 192.168.2.0/24 网络使用 EIGRP，请创建两个网络对象，每个网络对象一个。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击全局虚拟路由器的查看图标 ()。

步骤 3 点击 **EIGRP** 选项卡。

步骤 4 执行以下操作之一：

- 要创建新进程，请点击 **+** 或点击**创建 EIGRP 对象 (Create EIGRP Object)** 按钮。
- 点击要编辑的对象的编辑按钮 ()。请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

如果不再需要进程，请点击该对象的垃圾桶图标将其删除。

步骤 5 为 Smart CLI 对象输入**名称**和说明（后者为可选项）。

步骤 6 配置基本进程属性：

router eigrp *autonomous-system*

点击变量，然后输入一个介于 1-65535 之间的数字。使用在网络中其他路由器上使用的相同自治系统编号，该编号应与此设备在同一路由域内运行。

步骤 7 配置应在 EIGRP 自治系统内路由的网络和接口。

a) 点击对象正文上方的**显示已禁用 (Show Disabled)** 链接，添加所有其他可能的配置行。

b) 点击 **network** *network-object* 行左侧的 **+**。

c) 在 **network** 命令中，点击变量，然后选择定义应包含在此自治系统内的网络的对象。

通常是一个直连网络。例如，如果内部接口的 IP 地址为 192.168.1.1/24，则此命令的关联网络对象将包含 192.168.1.0/24。如果对象尚不存在，请点击**创建新网络**并立即创建。

已定义网络范围内的直连和静态网络由此进程通告。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与EIGRP路由，但是该接口已连接到希望通告的网络，请参阅配置 EIGRP 被动路由接口，第 387 页。

d) 如果要路由其他网络，请点击 **...** > **复制**（在 **network** 命令左侧）以添加一个新网络。继续添加 **network** 行，直到您配置了要路由的所有网络。

步骤 8 配置末节设置。

a) 点击 **setup eigrp** *configuration* 行左侧的 **+**。

b) 点击此变量，然后选择 **advanced**。

c) 点击 **setup eigrp stub** *stub-options* 命令左侧的 **+**。

d) 要限制设备与自治系统中的任何其他路由器共享任何路由，使其仅接收来自 EIGRP 邻居路由器的更新，请点击 *stub-options* 并选择 **receive**。然后，配置以下命令：

eigrp stub *stub-parameters*

点击此变量，然后选择 **receive-only**。

e) 要允许设备向 EIGRP 邻居路由器通告路由，请点击 *stub-options* 并选择 **other**。然后，配置以下命令以选择应通告的路由类型。

eigrp stub *connected-parameter redistributed-parameter static-parameter summary-parameter*

点击变量进行选择。您必须至少选择一种路由类型，但可以选择全部或任意组合。

- *connected-parameter*。选择 **connected** 可通告连接的路由。如果 **network** 语句未涵盖连接的路由，则可能需要在 EIGRP 进程中为连接的路由配置重新分发。
- *redistributed-parameter*。选择 **redistributed** 以通告从其他路由协议重新分发到 EIGRP 路由进程的路由。
- *static-parameter*。选择 **static** 可通告静态路由。您还必须启用 **configure redistribution** 命令并配置静态路由的重新分发。

- *summary-parameter*。选择 **summary** 通告汇总路由。

步骤 9 （可选。）如有必要，请调整其他最初禁用的命令的设置。请参阅自定义 EIGRP 进程，第 385 页。

步骤 10 点击**确定 (OK)**。

自定义 EIGRP 进程

EIGRP 包括很多具有默认值的选项。这些值适用于许多网络。但是，您可能需要调整一个或多个设置才能实现所需精确行为。以下主题介绍可用于自定义 EIGRP 路由进程的各种方式。

配置 EIGRP 高级设置

您可以配置多个控制 EIGRP 进程的整体行为的设置，包括自动路由汇总、距离度量、日志记录，以及用于发送链路状态通告和其他路由更新的路由器 ID。其中许多设置的默认值适用于大多数网络。

开始之前

此程序假设您已配置 EIGRP 进程；请参阅配置核心 EIGRP 进程，第 382 页。

创建进程时，默认情况下会启用某些高级选项。编辑 EIGRP 对象时，您将看到这些已启用的选项。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击全局虚拟路由器的查看图标 ()。

步骤 3 点击 **EIGRP** 选项卡。

步骤 4 点击 EIGRP 对象编辑按钮 ()。

请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

步骤 5 点击对象正文上方的**显示已禁用**，添加所有其他可能的配置行。

步骤 6 **setup eigrp** 配置行应已启用为 **setup eigrp advanced**。否则，请点击该行左侧的 + 启用它，然后点击变量并选择 **advanced**。

步骤 7 （可选，不推荐。）要自动汇总网络编号边界上的路由，请点击 **auto-summary** 命令旁边的 +。

如果存在非连续网络，这可能会引起路由问题。

例如，如果路由器同时连接到 172.16.1.0、172.16.2.0 和 172.16.3.0 网络，且这些网络全部参与 EIGRP，则 EIGRP 路由进程会为这些路由创建汇总地址 172.16.0.0。如果另一个路由器向该网络添加 172.16.10.0 和 172.16.11.0 网络，且这些网络均参与 EIGRP，则它们也会汇总为 172.16.0.0。因此，自动汇总路由会导致流量路由到错误的路由器。

步骤 8 （可选，推荐。）配置路由器 ID。

点击 + 启用 **router-id** 命令，然后点击变量，并输入从此设备发送任何路由器更新时应使用的 IPv4 地址。EIGRP 自治系统中的任何两个路由器都不能具有相同的路由器 ID，因此请确保它在该系统中是唯一的。

如果未明确指定进程的路由器 ID，系统会使用分配给主用接口的最高 IP 地址。因此，如果您禁用所选接口，或者更改其地址，则路由器 ID 可能会更改。通过明确分配路由器 ID，可以确保进程的一致性。

步骤 9 （可选。）配置内部和外部 EIGRP 路由的管理距离。

在配置该进程时，默认情况下会启用以下命令。如果要配置新对象，则可能需要点击 + 启用该命令。

distance eigrp 90 170

由于各个路由协议的度量基于各不相同的算法，因此对于不同路由协议生成的到达同一目的地的两个路由，并非始终可以确定“最佳路径”。管理距离是系统在有两个或多个路由通过两个不同路由协议通向同一目的地时，系统用于选择最佳路径的路由参数。

EIGRP 的管理距离为 1 到 255。当系统选择最佳路由时，这些数字与分配给其他路由进程的管理值相关。一般来说，值越大，信任评分就越低。默认值应能够满足大多数网络需求。如果您希望优先考虑 EIGRP 路由，或者希望降低使用 EIGRP 路由的可能性，请调整这些值。

这些数字意味着以下各项：

- 第一个值 (90)：**内部距离**。EIGRP 内部路由的管理距离。内部路由是从同一中的其他实体学习的路由。
- 第二个值 (170)：**外部距离**。EIGRP 外部路由的管理距离。外部路由是为其从外部的邻居学习最佳路径的路由

步骤 10 从其他路由进程重新分发路由时，使用 **default-metric** 命令。仅当您还配置了重新分发时，才需要配置此项。有关详细信息，请参阅配置 EIGRP 路由重新分发，第 392 页。

步骤 11 配置邻居日志记录。

在配置该进程时，默认情况下会启用以下命令。如果要配置新对象，则可能需要点击 + 启用该命令。如果要禁用日志记录，请点击 - 以禁用命令。

- **eigrp log-neighbor-changes** 启用 EIGRP 邻居邻接日志记录。
- **eigrp log-neighbor-warnings 10** 启用 EIGRP 邻居警告消息的日志记录。该数字是系统发送重复的邻居警告消息的时间间隔，范围为 1 到 65535 秒。系统不会记录在此间隔期间重复出现的警告。

步骤 12 如果要配置 **setup stub** 命令，请参阅配置末节路由 EIGRP 进程，第 383 页。

步骤 13 点击**确定 (OK)**。

为 EIGRP 配置要通告的网络

使用 **network** 命令来识别网络，并暗示应包括在 EIGRP 路由中的接口。对于参与 EIGRP 路由的接口，它必须位于网络条目定义的地址范围内。对于要通告的直连网络和静态网络，它们也必须位于网络条目的范围内。

开始之前

此程序假设您已配置 EIGRP 进程；请参阅配置核心 EIGRP 进程，第 382 页。

创建用于定义要通告的网络的网络对象。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击全局虚拟路由器的查看图标 ()。

步骤 3 点击 **EIGRP** 选项卡。

步骤 4 点击 EIGRP 对象编辑按钮 ()。

请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

步骤 5 点击对象正文上方的**显示已禁用**，添加所有其他可能的配置行。

步骤 6 假设您已配置网络，请点击 **...** > **复制**（在 **network** 行）旁边，可创建新的空命令。

如果尚未定义网络，请点击空 **network** *network-object* 行旁边的 +。

步骤 7 在 **network** 命令中，点击变量，然后选择定义应包含在此自治系统内的网络的对象。

通常是一个直连网络。例如，如果内部接口的 IP 地址为 192.168.1.1/24，则此命令的关联网络对象将包含 192.168.1.0/24。如果对象尚不存在，请点击**创建新网络**并立即创建。

已定义网络范围内的直连和静态网络由此进程通告。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅配置 EIGRP 被动路由接口，第 387 页。

步骤 8 如果要路由其他网络，请点击 **...** > **复制**（在 **network** 命令左侧）以添加一个新网络。继续添加 **network** 行，直到您配置了要路由的所有网络。

步骤 9 点击**确定 (OK)**。

配置 EIGRP 被动路由接口

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到您希望通告的网络，您可以配置其中包含该接口所连接网络的 **network** 命令，并使用 **passive-interface** 命令阻止该接口发送或接收 EIGRP 更新。

默认情况下，系统会启用 **no passive-interface default** 命令，该命令将所有接口设置为活动状态，以发送和接收 EIGRP 更新。

以下程序说明如何将接口改为被动接口。

开始之前

此程序假设您已配置 EIGRP 进程；请参阅配置核心 EIGRP 进程，第 382 页。

在创建进程时，应添加 **network** 命令以指示应使用 EIGRP 路由哪些网络。要配置其他需要路由的网络，请参阅为 EIGRP 配置要通告的网络，第 387 页。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击全局虚拟路由器的查看图标 ( )。

步骤 3 点击 **EIGRP** 选项卡。

步骤 4 点击 EIGRP 对象编辑按钮 ( )。

请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

步骤 5 点击对象正文上方的**显示已禁用**，添加所有其他可能的配置行。

步骤 6 如果编辑对象，则启用 **configure interface passive** 命令及其子项 **no passive-interface default**。

对于新对象，请点击 **+** 以启用 **configure routing-interface** *parameters* 命令。

步骤 7 要将接口配置为默认属于主动接口，则选择性地将接口设置为被动接口：

a) 在 **configure routing-interface** 命令中，点击此变量，然后选择 **passive**。

此操作会启用 **no passive-interface default** 命令，此命令将使 EIGRP 接口默认为主动接口。

b) 点击 **passive-interface** *interface* 命令旁边的 **+**，点击变量，然后选择应为被动状态且不参与 EIGRP 路由更新的接口。

c) 如果需要配置其他被动接口，请点击 **...** > **复制**（在 **passive-interface** *interface* 命令旁边）。继续操作，直到您为每个应配置为被动状态的接口设置了 **passive-interface** 命令。

步骤 8 要将接口配置为默认被动接口，则选择性地将接口设为主动接口：

a) 在 **configure routing-interface** 命令中，点击此变量，然后选择 **active**。

此操作将启用 **passive-interface default** 命令，此命令将使 EIGRP 接口默认为被动状态。

b) 点击 **no passive-interface** *interface* 命令旁边的 **+**，点击该变量，然后选择应主动参与 EIGRP 路由更新的接口。

c) 如果需要配置其他主动接口，请点击 **...** > **复制**（在 **no passive-interface** *interface* 命令旁边）。继续操作，直到您为每个应配置为主动状态的接口设置了 **no passive-interface** 命令。

步骤 9 要将接口切换回执行默认行为（被动或主动），请点击将该特定接口设置为被动或主动状态的命令旁边的 **-**。这会删除例外，并使接口根据您设置的默认操作执行相应行为。

步骤 10 点击**确定 (OK)**。

配置静态 EIGRP 邻居

EIGRP hello 数据包以组播数据包的形式发送。如果 EIGRP 邻居位于整个非广播网络（例如 VPN 隧道）内，则必须手动定义该邻居。当手动定义 EIGRP 邻居时，hello 数据包作为单播消息发送至该邻居。

您不需要定义常规广播网络上的静态邻居，因为这些路由器可以形成邻接关系。

开始之前

此程序假设您已配置 EIGRP 进程；请参阅配置核心 EIGRP 进程，第 382 页。

确定系统应通过其访问邻居的接口。

您还可以为邻居配置日志记录设置，如配置 EIGRP 高级设置，第 385 页中所述。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击全局虚拟路由器的查看图标 ( )。

步骤 3 点击 **EIGRP** 选项卡。

步骤 4 点击 EIGRP 对象编辑按钮 ( )。

请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

步骤 5 点击**显示已禁用**以显示所有命令，然后点击 **+** 以启用 **neighbor** 命令。

步骤 6 配置邻居地址。

neighbor *ip-address* **interface** *interface*

- 点击 *ip-address*，然后输入邻居路由器的 IP 地址。
- 点击 *interface*，然后选择系统可以通过其访问路由器的接口。

步骤 7 如有必要，请为邻居路由器配置静态路由。

如果路由器的 IP 地址与所选接口位于同一网络中，则无需静态路由。例如，如果您选择 IP 地址为 10.100.10.1/24 的接口，且邻居地址为 10.100.10.2/24，则不需要静态路由。

步骤 8 您可以点击 **...** > **复制**（在 **neighbor** 命令的旁边）以定义另一个静态邻居。根据需要定义任意数量的虚拟链路。

步骤 9 点击**确定 (OK)**。

控制 EIGRP 候选默认路由传播

您可以控制从 EIGRP 进程发送或接收候选默认路由。默认情况下，系统将根据路由过滤和重新分发设置通告或接受所有候选路由。

您无法直接关闭发送或接收默认路由。如果要阻止从 EIGRP 传播默认路由，请使用拒绝 any-ipv4 网络的标准 ACL 配置这些命令。

开始之前

此程序假设您已配置 EIGRP 进程；请参阅配置核心 EIGRP 进程，第 382 页。

创建每个过滤规则所需的 Smart CLI 标准访问权限列表对象。使用拒绝访问控制条目 (ACE) 过滤掉与条目匹配的路由，并允许应更新的路由的 ACE。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击全局虚拟路由器的查看图标 ()。

步骤 3 点击 **EIGRP** 选项卡。

步骤 4 点击 EIGRP 对象编辑按钮 ()。

请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

步骤 5 点击对象正文上方的**显示已禁用**，添加所有其他可能的配置行。

步骤 6 点击 + 以启用以下一个或两个命令：

- **default-information in** *acl* 用于控制候选默认路由的接收。
- **default-information out** *acl* 用于控制候选默认路由的发送。

步骤 7 点击变量并选择应用过滤器的标准 ACL。

步骤 8 点击**确定 (OK)**。

配置 EIGRP 过滤器规则

您可以根据标准访问控制列表中定义的网络前缀过滤传入或传出路由更新。过滤可改善对重新分发至 EIGRP 自治系统或传出至其他路由进程的的路由的控制。

开始之前

此程序假设您已配置 EIGRP 进程；请参阅配置核心 EIGRP 进程，第 382 页。

创建每个过滤规则所需的 Smart CLI 标准访问权限列表对象。使用拒绝访问控制条目 (ACE) 过滤掉与条目匹配的路由，并允许应更新的路由的 ACE。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击全局虚拟路由器的查看图标 ( )。

步骤 3 点击 **EIGRP** 选项卡。

步骤 4 点击 EIGRP 对象编辑按钮 ( )。

请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

步骤 5 点击**显示已禁用**以显示所有命令，然后点击 **+** 以启用 **configure filter-rules** *direction* 命令。

步骤 6 点击方向，然后选择 **in** 以对传入更新进行过滤，或选择 **out** 来过滤出站更新。

此操作将 **distribute-list** 命令添加到对象中。

步骤 7 对于入站过滤器，可以选择性地指定用于过滤更新的接口。如果不指定接口，则过滤器将应用于在任何接口上接收的所有更新。点击 **+** 以启用以下选项之一：

- **distribute-list** *acl-name* **in**

  选择标准 ACL 对象。

- **distribute-list** *acl-name* **in interface** *interface*

  选择要过滤传入更新的标准 ACL 对象和接口。

步骤 8 对于出站过滤器，您可以选择性地指定协议（以将过滤器限制为该路由进程生成的路由）以及要过滤更新的接口。点击 **+** 以启用以下选项之一：

- **distribute-list** *acl-name* **out**

  选择标准 ACL 对象。

- **distribute-list** *acl-name* **out interface** *interface*

  选择标准 ACL 对象和要过滤传出更新的接口。

- **distribute-list** *acl-name* **out** *protocol*

  选择标准 ACL 对象和以下路由类型之一：

  - **connected**。适用于为直接连接到系统接口的网络而建立的路由。
  - **static**。适用于手动创建的静态路由。
  - **rip**。对于 RIP 生成的路由。

- **distribute-list** *acl-name* **out** *protocol identifier*

  选择标准 ACL 对象和以下路由类型之一：

  - **ospf** *process-id*。对于 OSPF 生成的路由。点击 identifier，然后输入在系统中定义的 OSPF 进程的进程 ID。

- **bgp** *automonous-system*。对于 BGP 生成的路由。点击 identifier，然后输入在系统中定义的 BGP 进程的自治系统编号。

步骤 9 您可以点击 **...** > **复制**（位于 **configure filter-rules** 命令的旁边）以定义另一个过滤规则。根据需要定义任意数量的虚拟链路。

步骤 10 点击**确定 (OK)**。

配置 EIGRP 路由重新分发

您可以控制从其他路由协议、连接路由和静态路由中将路由重新分发到 EIGRP 进程的过程。

开始之前

最佳实践是在配置重新分发到EIGRP之前，配置您将从中重新分发路由的路由进程，并部署更改。

如果要应用路由映射以微调重新分发的路由，请创建 Smart CLI 路由映射对象。将重新分发与路由映射匹配的路由，并且不会重新分发所有不匹配的路由。

此程序假设您已配置 EIGRP 进程；请参阅配置核心 EIGRP 进程，第 382 页。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击全局虚拟路由器的查看图标 ( )。

步骤 3 点击 **EIGRP** 选项卡。

步骤 4 点击 EIGRP 对象编辑按钮 ( )。

请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

步骤 5 点击**显示已禁用**以显示所有命令。

步骤 6 （可选。）点击 **+** 以启用 **default-metric** 命令，该命令位于 **setup eigrp advanced** 命令组中。

如果未为路由类型配置特定 **redistribute metric** 命令，**default-metric** 命令可设置用于重新分发的路由的度量。

default-metric *bandwidth-metric delay-metric reliability-metric effective-bandwidth path-MTU*

点击此变量并配置以下项。您必须配置所有度量变量。

- *bandwidth-metric*。点击变量，然后输入此路由上连接的带宽，范围为 1 到 4294967295 千字节/秒。
- *delay-metric*。点击变量，然后输入路由上的连接延迟，以十微秒为单位，范围为0到4294967295。
- *reliability-metric*。点击变量，然后输入路由的 EIGRP 可靠性度量，范围为 0 到 255，其中 255 表示可靠性为 100%。此度量将被忽略，但您仍必须配置它。

- *effective-bandwidth*。点击变量，然后输入路由的 EIGRP 有效带宽，范围为 1 到 255，其中 255 表示负载为 100%。此度量将被忽略，但您仍必须配置它。
- *path-MTU*。点击变量并输入路径的平均传输单位 (MTU)，范围为 1 到 65535。此度量将被忽略，但您仍必须配置它。

步骤 7 点击 **+** 启用 **configure redistribution** 命令。

步骤 8 点击 *protocol* 变量，并选择要从中重新分发路由的源进程。您可以重新分发 **connected** 和 **static** 路由，或 **bgp**、**isis**、**ospf** 或 **rip** 生成的路由。

步骤 9 如果选择路由进程，请点击 *identifier* 变量，然后输入所需的值：

- **bgp**。输入自治系统编号。
- **ospf**。输入进程 ID 编号。
- **connected**、**static**、**isis**、**rip**。输入 **none**。即使您输入其他值，它也会被忽略。

步骤 10 （可选；仅限 IS-IS。）在 **redistribute isis route-level** *route-level* 命令中，点击变量，并选择是否仅在 IS-IS 区域内 (**level-1**)、IS-IS 区域之间 (**level-2**) 或在这两种范围内 (**level-1-2**) 重新分发路由。

步骤 11 （可选；所有协议。）要根据路由映射微调重新分配的路由，请点击 **+** 启用 **redistribute** *route-map* 命令，点击此变量，然后选择用于定义限制条件的路由映射。

如果不应用路由映射，则会重新分发进程的所有路由（适合为重新分发而配置的其他命令）。

步骤 12 （可选；所有协议。）要微调用于重新分发的路由的度量，请点击 **+** 启用以下命令并配置选项：

redistribute *protocol* **metric** *bandwidth-metric delay-metric reliability-metric effective-bandwidth path-MTU*

点击变量并配置值，具体说明详见上文 **default-metric** 命令部分。您必须配置所有度量变量。

步骤 13 （可选；仅限 OSPF。）当您从 OSPF 进程重新分发路由时，默认情况下会启用以下命令。可以点击 **-** 禁用不需要的命令。

这些命令用于指定将 OSPF 路由重新分发到其他路由域的条件。

- **redistribute ospf match external 1**。自治系统的外部路由，但是会作为 1 类外部路由导入 OSPF。
- **redistribute ospf match external 2**。自治系统的外部路由，但是会作为 2 类外部路由导入 OSPF。
- **redistribute ospf match internal**。特定自治系统的内部路由。
- **redistribute ospf match nssa-external 1**。自治系统的外部路由，但是会作为 1 类外部路由导入 OSPF，并仅标记为次末节区域 (NSSA)。
- **redistribute ospf match nssa-external 2**。自治系统的外部路由，但是会作为 2 类外部路由导入 OSPF，并仅标记为次末节区域 (NSSA)。

步骤 14 您可以点击 **...** > **复制**（位于 **configure redistribution** 命令的旁边），以配置另一种协议的重新分发。为适合您的网络的每种协议配置重新分发。

步骤 15　点击确定 (OK)。

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。

- **show eigrp events** ［{*start end*} | **type**］

  显示 EIGRP 事件日志。

- **show eigrp interfaces** ［*if-name*］［**detail**］

  显示参与 EIGRP 路由的接口。

- **show eigrp neighbors** ［**detail** | **static**］［*if-name*］

  显示 EIGRP 邻居表。

- **show eigrp topology** ［*ip-addr* ［*mask*］ | **active** | **all-links** | **pending** | **summary** | **zero-successors**］

  显示 EIGRP 拓扑表。

- **show eigrp traffic**

  显示 EIGRP 流量统计信息。

第 17 章

边界网关协议 (BGP)

BGP 用于交换互联网的路由信息，并且是互联网运营商 (ISP) 之间所使用的协议。如果您的系统是运营商网络的网关，则可能需要实施 BGP。您可以在设备上为单个自治系统配置一个 BGP 进程。

关于 BGP

BGP 是一种外部和内部自主系统路由协议。自治系统是一个或一组接受共同管理并采用共同路由策略的网络。BGP 用于交换互联网的路由信息，并且是互联网运营商 (ISP) 之间所使用的协议。

路由表更改

在 BGP 邻居之间首次建立 TCP 连接时，BGP 邻居会交换完整路由信息。当检测到对路由表所做的更改时，BGP 路由器仅会向其邻居发送已更改的路由。BGP 路由器不会发送定期路由更新，并且 BGP 路由更新仅对到达目标网络的最佳路径进行通告。

注释 系统通过扫描完整的 AS 路径（在 AS_PATH 属性中指定）并检查本地系统的 AS 编号是否未出现在 AS 路径中来完成 AS 环路检测。默认情况下，EBGP 将获知的路由通告给同一对等体，以防止在执行环路检查时 ASA 上出现额外的 CPU 周期，并避免现有传出更新任务中出现延迟。

当存在多个到达某个特定目标的路由时，通过BGP获悉的路由的属性可用于确定到达该目标的最佳路径。这些属性称为 BGP 属性，可在路由选择过程中使用：

- 权重 - 这是思科定义的路由器本地属性。权重属性不会向相邻路由器进行通告。如果路由器获悉有多个到达同一目标的路由，则首选权重最高的路由。
- 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，本地优先属性在整个本地 AS 中传播。如果有多个来自 AS 的出口点，则使用具有最高本地优先属性的出口点作为特定路由的出口点。

- 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 属性选择路由，所以它仅作为建议。首选 MED 指标较低的路由。
- 源 - 源属性指示 BGP 获悉某个特定路由的方式。源属性可能具有下面三个可能值中的一个，用于路由选择。
  - IGP - 此路由是源 AS 的内部路由。当使用网络路由器配置命令向 BGP 注入路由时，会设置该值。
  - EGP - 此路由通过外部边界网关协议 (EBGP) 获悉。
  - 不完整 - 路由源未知或通过其他方式获悉。当路由重新分发到 BGP 时，可能会出现源不完整的情况。
- AS_path - 当路由通告通过一个自治系统时，会在按顺序排列的 AS 编号列表中添加 AS 编号，标识路由通告已经穿越的 AS。仅将拥有最短 AS_path 列表的路由添加至 IP 路由表中。
- 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 下一跳地址会携带至本地 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）。路由映射用于设置社区属性。预定义的社区属性如下：
  - no-export - 不向 EBGP 对等体通告相应路由。
  - no-advertise - 不向任何对等体进行通告。
  - internet - 此路由向互联网社区进行通告；网络中的所有路由器均属于此类型。

何时使用 BGP

客户网络（例如，大学和公司）通常使用 OSPF 等内部网关协议 (IGP) 在其网络内交换路由信息。客户连接到 ISP，然后 ISP 使用 BGP 交换客户路由和 ISP 路由。在自治系统 (AS) 之间使用 BGP 时，该协议称为外部 BGP (EBGP)。如果运营商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

BGP 也可用于通过 IPv6 网络承载有关 IPv6 前缀的路由信息。

BGP 路径选择

BGP 可能会从不同来源接收同一路由的多个通告。BGP 仅选择一个路径作为最佳路径。选择此路径后，BGP 将选定的路径放在 IP 路由表中，并将此路径传播给其邻居。BGP 按显示的顺序使用以下条件为目标选择路径：

- 如果路径指定的下一跳不可访问，则放弃更新。
- 首选权重最高的路径。
- 如果权重相同，则首选具有最高本地优先值的路径。

- 如果本地优先值相同，则首选 BGP 在此路由器上运行所发起的路径。
- 如果未发起路由，则首选 AS_path 最短的路由。
- 如果所有路径的 AS_path 长度相同，则首选源类型最低的路径（其中，IGP 低于 EGP，EGP 低于不完整路径）。
- 如果源代码相同，则首选 MED 属性最低的路径。
- 如果路由的 MED 相同，则首选外部路径而非内部路径。
- 如果路径依然相同，则首选穿过最近的 IGP 邻居的路径。
- 在 BGP 多路径，第 397 页的路由表中确定是否需要安装多个路径。
- 如果两个路径都是外部路径，则首选第一个接收的路径（最早的路径）。
- 首选具有由 BGP 路由器 ID 指定的最低 IP 地址的路径。
- 如果多个路径的发起方或路由器 ID 相同，则首选集群列表长度最短的路径。
- 首选来自最低邻居地址的路径。

BGP 多路径

BGP 多路径允许将多个等成本 BGP 路径的 IP 路由表安装到相同的目标前缀。然后，跨安装的所有路径共享到目标前缀的流量。

这些路径连同最佳路径一起安装在表中，以实现负载共享。BGP 多路径不影响最佳路径选择。例如，路由器仍会根据算法将其中一个路径指定为最佳路径，并将此最佳路径通知其 BGP 对等体。

要想成为多路径的候选对象，指向同一目标的路径需要具有与最佳路径特性相同的以下特性：

- 重量
- 本地优先级
- AS-PATH 长度
- 源代码
- 多出口鉴别器 (MED)
- 以下选项之一：
  - 相邻的 AS 或子 AS（在添加 BGP 多路径之前）
  - AS 路径（在添加 BGP 多路径之后）

某些 BGP 多路径功能对多路径候选对象有一些额外要求：

- 此路径应从外部或联盟外部邻居 (eBGP) 获悉。
- BGP 下一跳的 IGP 指标应等于最佳路径 IGP 指标。

这些是内部 BGP (iBGP) 多路径候选对象的额外要求：

- 此路径应从内部邻居 (eBGP) 获悉。
- BGP 下一跳的 IGP 指标应等于最佳路径 IGP 指标，除非路由器是面向非等成本 iBGP 多路径配置的。

BGP 可将最多 *n* 个最近收到的路径从多路候选对象插入到 IP 路由表中，其中 *n* 是要安装到路由表的路由数，如配置 BGP 多路径时所指定的那样。禁用多路径时的默认值为 1。

对于非等成本的负载平衡，您还可以使用 BGP 链路带宽。

注释 等效的下一自跳将在从 eBGP 中选择的最佳路径上执行，并且是在最佳路径转发至内部对等体之前执行。

配置 BGP

以下主题介绍如何配置 BGP。

配置 BGP 全局设置

如果配置BGP，则全局设置应用于所有虚拟路由器（如果使用虚拟路由器）。您配置的其他BGP设置可用于定义 BGP 进程。使用虚拟路由器时，您可以为每个虚拟路由器创建单独的 BGP 进程。

开始之前

创建BGP全局设置对象后，如果不再需要该对象，可以将其删除。只需根据此程序编辑对象，然后点击对话框底部的**删除 BGP 全局设置对象**按钮即可。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 在主路由或虚拟路由器页面上，点击 **BGP 全局设置 (BGP Global Settings)** 按钮。

如果您查看的是虚拟路由器，则必须返回到主虚拟路由器列表。

步骤 3 如果尚未配置 BGP 全局设置对象，请点击**创建 BGP 全局设置对象**。

步骤 4 （可选。）您可以更改对象名称或输入对象的说明。默认对象名称为 BgpGeneralSettings。

步骤 5 至少配置以下基本设置：

- **router bgp** *as-number*。点击 *as-number*，输入 BGP 进程的自治系统 (AS) 编号。AS 编号范围为从 1 至 4294967295，或从 1.0 至 65535.65535。AS 编号是分配的唯一值，用于在互联网上标识各个网络。系统支持 RFC 5396 中定义的 asplain 和 asdot 表示法。

- **log-neighbor-changes** *state*。点击 *state*，然后选择“启用”或“禁用”。启用时，建议配置 BGP 邻居更改（向上或向下）和重置。这有助于解决网络连接问题并衡量网络稳定性。
- **transport path-mtu-discovery** *state*。点击 *state*，然后选择“启用”或“禁用”。启用后（建议启用），系统会确定两个 IP 主机之间的网络路径上的最大传输单位 (MTU) 大小，然后采用最高 MTU 路径。这可以避免 IP 分片。
- **fast-external-fallover** *state*。点击 *state*，然后选择“启用”或“禁用”。启用后（建议启用），系统会通过直接连接的外部对等体面向 BGP 对等会话使用快速外部故障转移。如果链路断开，会话将立即重置。如果禁用 BGP 快速外部故障转移，则 BGP 路由进程将等待，直到默认保持计时器过期（3 个保持连接间隔）再重置对等会话。
- **enforce-first-as** *state*。点击 *state*，然后选择“启用”或“禁用”。启用后（建议启用），系统将拒绝从 eBGP 对等体收到的传入更新，这些对等体不会将其自治系统编号列为 AS_PATH 属性中的第一个分段。启用此命令可以防止错误配置或未经授权的对等体通过通告路由（如同其源自另一个自治系统）来错误定向流量（欺骗本地路由器）。

步骤 6 （可选。）点击对象正文上方的**显示已禁用**链接，添加所有其他可能的配置行。

您可以通过点击选项左侧的+启用以下选项。

- **bgp asnotation dot**。将 BGP 4 字节自治系统编号的默认显示和正则表达式匹配格式从 asplain（十进制值）更改为 asdot（点分表示法）。系统使用 asplain 作为自治系统编号的默认显示格式，但即使不启用此命令，您也可以采用 asplain 和 asdot 格式配置 4 字节自治系统编号。

  此外，正则表达式中匹配 4 字节自治系统编号的默认格式为 asplain，因此，您必须确保在不启用此命令的情况下，匹配 4 字节自治系统编号的所有正则表达式均以 asplain 格式书写。
- **bgp scan time 60**。点击数字，然后输入 BGP 路由器的扫描间隔以进行下一跳验证，范围为从 5 到 60 秒。默认值为 60 秒。
- **configure nexthop trigger** *state*。点击 *state*，然后选择 **enable** 或 **disable**。BGP 下一跳地址跟踪由事件驱动。在对等会话建立后，将自动跟踪 BGP 前缀。下一跳更改在路由信息库 (RIB) 中更新后迅速报告给 BGP。此优化通过缩短 RIB 中所安装路由的下一跳更改响应时间来改善整体 BGP 收敛。在两个 BGP 扫描程序周期之间运行最佳路径计算时，仅处理和跟踪更改。如果启用下一跳地址跟踪，则会添加以下命令。请注意，如果不在新对象中配置常规选项，则默认设置为启用此功能。
  - **bgp nexthop trigger enable**。BGP 下一跳地址跟踪可显著缩短 BGP 响应时间。不过，不稳定的内部网关协议 (IGP) 对等体可能会引起 BGP 的不稳定。我们建议您积极抑制不稳定的 IGP 对等会话以减轻对 BGP 可能的影响。
  - **bgp nexthop trigger delay 5**。点击数字以更改 BGP 下一跳地址跟踪的路由表审核之间的延迟间隔。通过将两次完整路由表走查之间的延迟间隔调整为匹配 IGP 的调整参数，可提高 BGP 下一跳地址跟踪的性能。默认延迟间隔为 5 秒，即快速调整 IGP 的最佳值。如果 IGP 收敛更缓慢，您可将延迟间隔更改为 20 秒或更长时间，具体取决于 IGP 收敛时间。可以将延迟时间设置为 0 到 100 秒。
- **bgp aggregate-timer 30**。点击数字，设置汇聚 BGP 路由的间隔，范围为从 6 到 60 秒。默认值为 30 秒。

- **bgp router-id** *router-id*。点击 *router-id*，并输入应用作全局路由器 ID 的 IPv4 地址。此 ID 用于虚拟路由器中本身不指定路由器 ID 的任何 BGP 进程。如果不启用此命令，路由器 ID 将被设置为分配给虚拟路由器的物理接口上的最高 IP 地址。使用此命令可确保路由器 ID 保持稳定。
- **bgp maxas-limit** *value*。点击 *value*，然后输入 BGP 更新消息 AS-path 属性中的最大自治系统编号数量，范围为从 1 到 254。AS_path 属性是形成供数据包传播的定向路由的源和目标路由器之间的中间 AS 编号序列。系统会丢弃在 AS 路径中超过指定值的多个自治系统的路由。除了在 AS-path 段内设置自治系统编号数量限值以外，该命令还将 AS-path 的段数限制为 10。如果不启用此命令，则不会丢弃任何路由。

步骤 7 （可选。）配置 BGP 高级选项。

必要时，点击**显示已禁用**链接显示以下命令。在编辑这些设置时，系统会显示 **timers** 和 **bestpath** 选项集，因为它们具有一些即使未显式设置也会启用的默认设置。

configure bgp advanced *advanced-option*

点击 *advanced-option*，然后选择下列其中一项。可以通过点击左栏中的 ... 并选择**复制**来配置所有这些选项。

- **timers**。配置与 BGP 邻居路由器通信时使用的计时器。

  timers bgp 60 180 0

  - 第一个值（默认值为 60）：**保持连接间隔**。点击数字，然后输入系统向其 BGP 邻居发送保持连接消息的频率，范围为从 0 到 65535 秒。建议不要指定小于等于 20 的值，否则可能会发现路由发生不必要的摆动。
  - 第二个值（默认值 180）：**保持时间**。点击数字，然后输入系统在未接收到保持连接消息之后、声明 BGP 邻居失效之前应等待的时长，范围为从 0 到 65535 秒。
  - 第三个值（默认值 0）：**最短保持时间**。点击数字并指定 BGP 邻居上配置的最小可接受保持时间。最短可接受保持时间必须小于或等于指定为此系统保持时间的间隔。范围为从 0 到 65535 秒。

- **bestpath**。配置 BGP 最佳路径选择算法中使用的选项。默认情况下会配置 **bgp default local-preference** 命令，但是您可以通过点击该命令对应的 **+** 来添加更多命令。
  - **bgp default local-preference 100**。点击数字，然后输入指示此系统相对于 BGP AS 中其他路由器的首选项的值，范围为从 0 到 4294967295。默认值为 100。值越大，表示优先级越高。此首选项会发送到本地自治系统中的所有路由器和接入服务器。此属性仅在 iBGP 对等体之间进行交换，用于确定本地策略。
  - **bgp always-compare-med**。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)。默认情况下，系统不会比较来自不同自治系统中不同邻居的路径的 MED。
  - **bgp bestpath compare-routerid**。当从两个不同对等体接收两个相同的路由时，使用路由器 ID 作为最佳路径选择（除了路由器 ID，所有属性都相同）。此命令启用后，如果所有其他属性均相同，将选择最低路由器 ID 作为最佳路径。否则，将使用接收的第一个路由。
  - **bgp deterministic-med**。选择从相邻 AS 通告的最佳 MED 路径。

- **bgp bestpath med missing-as-worst**。将缺少 MED 属性的路径设置为最不优先考虑的路径。默认情况下，系统会将缺少 MED 的路由视为最佳路由。

- **graceful-restart**。为采用高可用性或集群配置的系统配置平稳重启。
  - **bgp graceful-restart**。启用平稳重启以实现无间断转发。通过平稳重启，系统可以通告重启期间保持地址组转发状态的能力。
  - **bgp graceful-restart restart-time 120**。点击数字，然后输入在重启事件发生后系统等待支持平稳重启的邻居恢复正常运行的最大时间间隔，范围为从 1 到 3600 秒。默认值为 120 秒。
  - **bgp graceful-restart stalepath-time 360**。点击数字，然后输入系统保留重启对等体过时路径的最大时间间隔，范围为从 1 到 3600 秒。此计时器到期后，将删除所有过时路径。默认值为 360 秒。

步骤 8 点击**确定 (OK)**。

配置 BGP 进程

在配置 BGP 全局设置后，您可以配置 BGP 进程。如果使用的是虚拟路由器，则可以为每个虚拟路由器创建一个单独进程。您最多可以为系统或每个虚拟路由器配置一个 BGP 进程。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 BGP 的路由器的查看图标 ()。

步骤 3 点击 **BGP** 选项卡。

步骤 4 执行以下操作之一：

- 要创建新进程，请点击 **+** 或点击**创建 BGP 对象 (Create BGP Object)** 按钮。
- 点击要编辑的对象的编辑按钮 ()。请注意，编辑对象时，您可能会看到未直接配置的行。系统会公开这些行，显示正在配置的默认值。

如果不再需要进程，请点击该对象的垃圾桶图标将其删除。

步骤 5 输入对象的名称和（可选）说明。

步骤 6 配置进程的最低设置：

- **router bgp** *as-number*。点击 *as number*，并为已经为全局设置项指定的 BGP 进程输入相同的自治系统 (AS) 编号。AS 编号范围为从 1 至 4294967295，或从 1.0 至 65535.65535。AS 编号是分配的唯一值，用于在互联网上标识各个网络。系统支持 RFC 5396 中定义的 asplain 和 asdot 表示法。

- **configure address-family** *ip-protocol*。点击 *ip-protocol*，然后选择 IPv4 或 IPv6。如果您使用的是虚拟路由器，则只能为全局路由器配置 IPv6。您可以为任何虚拟路由器配置 IPv4。如果选择一个选项，会添加 **address-family ipv4 unicast** 或 **address-family ipv6 unicast** 命令，并且您必须配置以下命令：
  - **configure address-family {ipv4 | ipv6}** *settings*。点击设置并选择 **general** 或 **advanced**。您必须在这些选项下配置至少一个命令以实现最小进程，但这对于有意义的进程来说是不够的。

步骤 7 点击**显示已禁用 (Show Disabled)** 并自定义该流程，以便在您的网络中正常运行。

如上文所述，在配置一组最低限度的命令之后，即可保存对象并稍后自定义进程设置。以下主题介绍各选项集。必须最低限度地配置网络设置，以确定进程将为其分配路由的网络。“常规”和“高级”设置都具有适用于大多数情况的命令默认设置。

- 配置 BGP 常规设置，第 402 页
- 配置 BGP 高级设置，第 403 页
- 为要通告的 BGP 配置网络，第 405 页
- 配置 BGP 路由注入，第 406 页
- 配置 BGP 汇聚地址设置，第 407 页
- 配置针对 IPv4 的 BGP 过滤器设置，第 408 页
- 配置 BGP 邻居，第 409 页
- 根据其他路由协议配置 BGP 路由重新分发，第 416 页

步骤 8 （可选。）为此进程配置路由器 ID。

您可以在 BGP 全局设置中配置用于 BGP 进程的路由器 ID。也可以选择性地在进程对象中配置它。进程对象中配置的任何路由器 ID 都会覆盖全局路由器 ID。这使您可以轻松地覆盖特定虚拟路由器的全局值。

如果未显示以下命令，请点击**显示已禁用 (Show Disabled)**，然后点击它旁边的 **+** 以启用该命令。

- **bgp router-id** *router-id*。点击 *router-id*，并输入应用作此进程的路由器 ID 的 IPv4 地址。如果不启用此命令，路由器 ID 将设置为全局路由器 ID，或分配给虚拟路由器的物理接口上的最高 IP 地址。使用此命令可确保路由器 ID 保持稳定。

步骤 9 点击**确定 (OK)**。

配置 BGP 常规设置

常规设置定义管理距离、计时器以及仅适用于 IPv4 的下一跳地址跟踪。这些选项具有适用于大多数网络的默认设置。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 BGP 的路由器的查看图标 ( )。

步骤 3 点击 **BGP** 选项卡。

步骤 4 添加或编辑 BGP 进程对象。

步骤 5 查找 **configure address-family ipv4** 或 **ipv6** 行。如果 **general** 选项已选中，请转到下一步。但是：

- 如果仍显示 *settings* 变量，请点击它并选择 **general**。
- 如果已配置高级选项，请点击命令左侧的 **...** 按钮，然后选择**复制**。然后，点击 *settings* 并选择 **general**。

步骤 6 配置以下命令：

- **distance bgp 20 200 200**。配置 BGP 的管理距离，范围为从 1 到 255。当系统选择最佳路由时，这些数字与分配给其他路由进程的管理值相关。一般来说，值越大，信任评分就越低。如果知道另一个协议为节点提供的路由优于通过外部 BGP (eBGP) 实际获知的路由，或 BGP 应首选特定内部路由，则使用此命令。距离为 255 的路由未安装在路由表中。这些数字意味着以下各项：
  - 第一个值（默认为 20）：**外部距离**。点击数字，然后输入外部 BGP 路由的管理距离。从外部自治系统获悉的路由是外部路由。
  - 第二个值（默认为 200）：**内部距离**。点击数字，然后输入内部 BGP 路由的管理距离。从本地自治系统中的对等体获悉的路由是内部路由。更改内部 BGP 路由的管理距离存在风险，不推荐这样做。配置不正确会导致路由表不一致和路由中断。
  - 第三个值（默认为 200）：**本地距离**。点击数字，然后输入本地 BGP 路由的管理距离。本地路由适用于 BGP 路由进程中由 **network** 命令列出的网络（即该进程所通告的网络），或适用于将从另一个进程重新分发到 BGP 的网络。

步骤 7 点击**确定 (OK)**。

配置 BGP 高级设置

使用“高级”设置来配置仅在特殊情况下需要的各种选项。默认情况下，这些选项都处于禁用状态。

开始之前

如果要配置 **table-map** 命令，必须先转到**设备 (Device)** > **高级配置 (Advanced Configuration)**页面，并创建该命令所需的 Smart CLI 路由映射对象。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 BGP 的路由器的查看图标 ( )。

步骤 3 点击 **BGP** 选项卡。

步骤 4 添加或编辑 BGP 进程对象。

步骤 5 查找 **configure address-family ipv4** 或 **ipv6** 行。如果 **advanced** 选项已选中，请转到下一步。但是：

- 如果仍显示 *settings* 变量，请点击它并选择 **advanced**。
- 如果已配置常规选项，请点击命令左侧的 **...** 按钮，然后选择**复制**。然后，点击 *settings* 并选择 **advanced**。

步骤 6 配置以下命令。在最初创建对象时，您需要点击**显示已禁用**来查看除第一个命令外的所有命令。

点击 **+** 以启用命令。

- **bgp redistribute-internal**。将 iBGP 配置为重新分发到内部网关协议 (IGP)，例如 EIGRP 或 OSPF。在将 iBGP 重新分发到 IGP 时应格外小心。使用 IP prefix-list 和 route-map 语句限制要重新分发的前缀数量。将未过滤的 BGP 路由表重新分发到 IGP 可能会对正常 IGP 网络运行产生不良影响。默认情况下启用此命令，因此您只需点击 **-** 按钮即可将其关闭。
- **bgp suppress-inactive**。禁止将未安装在 RIB 中的路由（非活动路由）通告给对等体。默认情况下，BGP 会通告非活动路由。请注意，BGP 使用 RIB-failure 标志来标记未安装在 RIB 中的路由。此标志还将显示在 **show bgp** 命令的输出中；例如 Rib-Failure (17)。此标志并不表示路由或 RIB 出现错误或问题。
- **auto-summary**。（仅 IPv4。）自动将子网路由汇总到网络级路由中。路由汇总可减少路由表中路由信息的数量。如果您必须在已断开连接的子网之间执行路由，则禁用自动汇总。当禁用自动汇总时，会通告子网。
- **synchronization**。启用在 BGP 与您内部网关协议 (IGP) 系统（例如 OSPF）之间的同步。通常，BGP 发言方不会向外部邻居通告路由，除非路由是本地路由或存在于 IGP 中。使用此功能，自治主系统中的路由器和接入服务器可在 BGP 将某个路由分配给其他自治系统之前获得该路由。如果自治系统中的其他路由器不进行 BGP 通信，请使用此命令。
- **table-map** *route-map options*。（仅 IPv4。）应用一个路由映射，该路由映射可用于为 BGP 路由表中更新的路由设置度量值、标记值或流量指数，或用于控制是否将路由下载到 RIB。点击路由映射，并选择定义路由映射的 Smart CLI 对象。在路由映射中，可以将 match 子句用于 IP 访问列表、自治系统路径、社区、前缀列表和下一跳。

  可以通过点击选项并选择空白或 **filter** 来确定如何使用路由映射。

  - 如果不选择 **filter**，则在将路由安装在 RIB 中之前，系统会使用路由映射来设置路由的特定属性。路由将始终下载，无论它是被路由映射允许还是拒绝。
  - 如果选择 **filter**，路由映射还会控制是否将 BGP 路由下载到 RIB 。仅会下载路由映射中允许的路由，不会下载已被拒绝的路由。

- **default-information originate**。配置 BGP 以通告默认路由（网络 0.0.0.0）。该 **default-information originate** 命令的配置类似于 **network** 命令的配置。但是，**default-information originate** 命令要求显式重新分发路由 0.0.0.0，并且您还必须在此对象中配置此路由。**network** 命令只要求 OSPF 等内部网关协议 (IGP) 路由表中存在路由 0.0.0.0 即可。因此，此 **network** 命令是分配默认路由的首选。
- **maximum paths 1**。控制可安装在路由表中的并行 BGP 路由的最大数量（从 1 到 8）。使用此命令，可以为 BGP 对等会话配置等价或非等价多路径负载共享。要将路由安装为 BGP 路由表中的多路径，路由的下一跳不能与已安装的另一个路由相同。配置 BGP 多路径负载共享时，BGP 路由进程仍会通告到 BGP 对等成员的最佳路径。对于等价路由，来自路由器 ID 最小的相邻设备的路径被通告为最佳路径。

  要配置 BGP 等价多路径负载共享，所有路径属性必须相同。路径属性包括权重、本地优先级、自治系统路径（整个属性，而不只是长度）、源代码、多出口标识符 (MED) 和内部网关协议 (IGP) 距离。
- **maximum paths ibgp 1**。控制可安装在路由表中的内部 BGP 路由的最大数量（从 1 到 8）。有关多路径 iBGP 的注意事项与上述 **maximum paths** 命令所述的注意事项相同。

步骤 7 点击**确定 (OK)**。

为要通告的 BGP 配置网络

您需要定义将通过 BGP 路由进程通告的网络。

开始之前

创建用于定义要通告的网络的网络对象。可以根据为 BGP 配置的地址系列定义 IPv4 或 IPv6 网络或两者。

如果网络对象指定了较大的网络空间，则还可以创建路由映射以应用于该网络对象，从而过滤掉您不想通告的较大空间内的子网。仅会通告与路由映射规范匹配的路由。使用 Smart CLI 创建路由映射对象。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 BGP 的路由器的查看图标 ( )。

步骤 3 点击 **BGP** 选项卡。

步骤 4 添加或编辑 BGP 进程对象。

网络命令位于 **configure address family ipv4** 或 **ipv6** 命令下的命令集内。您必须配置地址系列，以配置要通告的网络。

每个地址组中的 **network** 命令必须指定与您要配置的地址系列匹配的地址。

步骤 5 点击**显示已禁用**以显示所有命令，然后点击 **+** 启用 **network** 或 **network route-map** 命令，并配置选项：

- *network-object*。点击此变量，并选择用于定义要通告的网络的网络对象： IPv4 网络地址和掩码或 IPv6 网络地址和前缀。
- **route-map** *map-tag*。点击此变量，并选择将应用于网络对象（以过滤应通告范围内的哪些地址）的路由映射。
- （可选；仅限 IPv6。）*prefix-name*。点击此变量，并输入 DHCPv6 前缀的名称，以通告前缀。如果配置此选项，网络对象将用作前缀的子网。要使用此选项，您必须启用 DHCPv6 前缀授权客户端，这要求您在接口配置模式下使用 FlexConfig 将 **ipv6 dhcp client pd** 命令添加到接口。

步骤 6 您可以点击 **...** > **复制**（位于 **network** 或 **network route-map** 命令的旁边）以配置要通告的其他网络。

步骤 7 点击**确定 (OK)**。

配置 BGP 路由注入

可以配置有条件的路由注入，以将更具体的路由注入BGP路由表。条件路由注入允许您发起更具体的前缀到BGP路由表中而无需对应的匹配。任何注入的前缀必须具有有效的父路由。只能注入等于汇聚路由（现有前缀）或比其更具体的前缀。

开始之前

必须创建在定义前缀时所需的路由映射。这些路由映射必须符合程序中介绍的要求。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 BGP 的路由器的查看图标 ( )。

步骤 3 点击 **BGP** 选项卡。

步骤 4 添加或编辑 BGP 进程对象。

路由注入命令位于 **configure address family ipv4** 或 **ipv6** 命令下的命令集内。您必须配置地址系列，以配置要通告的网络。

步骤 5 点击**显示已禁用 (Show Disabled)** 以显示所有命令，然后点击 **+** 以启用 **bgp inject-map** 命令。

步骤 6 配置以下命令属性：

- **inject-map** *inject-map*。点击此变量，然后选择用于定义将要创建并安装到路由表中的前缀的路由映射。注入的前缀将安装到本地 BGP RIB 中。必须具有有效的父路由；只能注入等于汇聚路由（现有前缀）或比其更具体的前缀。路由映射必须使用前缀列表来指定要注入的路由。
- **exist-map** *exist-map*。点击此变量，然后选择用于定义 BGP 发言者将跟踪的前缀的路由映射。此路由映射必须使用前缀列表来指定汇聚前缀和路由源。路由源是一个路由器（例如10.2.1.1/32）而不是子网。

- *options*。（可选）点击此变量，然后选择**copy-attributes**。此选项可配置注入的前缀，以继承与汇聚路由相同的属性。如果不选择此关键字，则注入的前缀将使用本地发起的路由的默认属性。

步骤 7 您可以点击 **...** > **复制**（位于 **bgp inject-map** 命令的旁边）以配置其他路由注入规则。

步骤 8 点击**确定 (OK)**。

配置 BGP 汇聚地址设置

BGP邻居存储和交换路由信息，随着配置的BGP发言方的增加，路由信息的量也随之增加。路由聚合是将多个不同路由的属性组合在一起的过程，以便仅通告一个路由。聚合前缀使用无类别域内路由 (CIDR) 原则将相邻的网络合并成一个可在路由表中汇总的无类别 IP 地址集。因此，通告的路由更少。

如果在命令中配置不带关键字的汇聚路由，则在指定范围内，如果有更具体的BGP路由可用，则系统将在BGP路由表中创建一个汇聚条目。（路由信息库 [RIB] 中必须存在与汇聚匹配的更长前缀。）汇聚路由将被通告为来自您的自治系统，并将设置原子汇聚属性以显示信息可能会丢失。除非指定 **as-set** 关键字，否则需设置原子汇聚属性。

以下操作步骤介绍如何将特定路由汇聚配置为一个路由。

开始之前

如果要应用路由映射来微调要汇聚的路由或在汇聚路由上设置的属性，请创建 Smart CLI 路由映射对象。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 BGP 的路由器的查看图标 ( )。

步骤 3 点击 **BGP** 选项卡。

步骤 4 添加或编辑 BGP 进程对象。

汇聚命令位于 **configure address family ipv4** 或 **ipv6** 命令下的命令集内。您必须配置地址系列以配置汇聚。

步骤 5 点击**显示已禁用**以显示所有命令，然后点击 **+** 以启用 **configure aggregate-address** 命令。

步骤 6 点击 *map-type* 变量，然后选择要应用于此特定汇聚路由的路由映射类型。

此选项只会确定将添加到对象的 **aggregate-address** 命令中包含的参数。最多可以应用 3 个单独的路由映射，以抑制路由汇聚，通告路由以及定义要应用于汇聚路由的属性。

- 如果不需要应用任何路由映射，请选择 **no-map**。
- 如果要对所有三个选项应用路由映射，请选择 **all**。

- 如果要应用一个或两个而非全部映射，请选择适当的关键字组合：**suppress-map**、**advertise-map**、**attribute-map**、**suppress-advertise**、**suppress-attribute**、**advertise-attribute**。

步骤 7 配置要汇聚的路由的属性。

以下是属性的完整列表。所显示的内容取决于您选择的映射类型。

- *network-object*。点击此变量，然后选择用于定义要汇聚的地址空间的网络对象。对象必须使用与您要配置的地址类型匹配的 IPv4 或 IPv6 寻址。例如，可以汇聚所有 10.0.0.0/8 子网的路由。
- **suppress-map** *suppress-route-map*。点击此变量，然后选择路由映射以抑制指定路由的通告。可以使用路由映射的匹配子句来选择性地抑制一些更具体的路由，而让其他路由保留非抑制状态。路由映射可以根据访问列表和自治系统路径来匹配路由。
- **advertise-map** *advertise-route-map*。点击此变量，然后选择用于选择具体路由的路由映射，这些特定路由将用于构建汇聚路由的不同组件，例如 AS_SET 或社区。若汇聚的组件位于各单独的中且您希望使用 AS_SET 进行汇聚，然后将它通告给其中某些自治系统，则此属性很有用。必须牢记从 AS_SET 中省去特定自治系统编号，以防止接收路由器处的 BGP 环路检测机制丢弃汇聚。路由映射可以根据访问列表和自治系统路径来匹配路由。
- **attribute-map** *attribute-route-map*。点击此变量，然后选择将更改汇聚路由的属性的路由映射。若构成 AS_SET 的路由之一配置了某个属性（如 community no-export，该属性可防止导出汇聚路由），则此命令的此形式很有用。
- *options*。点击此变量，然后选择以下选项之一、全部或不选择以下任一选项：
  - **as-set**。生成适用于汇聚路由的自治系统集路径信息。为此路由通告的路径将是 AS_SET，由包含在所有正在汇总的路径中的元素组成。汇聚多个路径时，请勿使用此关键字，因为已汇总路由的自治系统路径可达性信息会发生更改，必须不断撤回并更新此路由。
  - **summary-only**。抑制向所有邻居通告更具体的路由。

步骤 8 您可以点击 **...** > **复制**（位于 **configure aggregate-address** 命令的旁边）以配置其他要汇聚的路由。

步骤 9 点击**确定 (OK)**。

配置针对 IPv4 的 BGP 过滤器设置

可以创建过滤器规则来限制系统从/向其他路由协议获取/通告的路由信息。

此处介绍的配置适用于所有本地进程，并用于过滤对所有 BGP 邻居的更新。可以在邻居设置中为每个邻居配置不同的过滤规则。

开始之前

创建每个过滤规则所需的 Smart CLI 标准访问权限列表对象。使用拒绝访问控制条目 (ACE) 过滤掉与条目匹配的路由，并允许应更新的路由的 ACE。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 BGP 的路由器的查看图标 ( )。

步骤 3 点击 **BGP** 选项卡。

步骤 4 添加或编辑 BGP 进程对象。

过滤命令位于 **configure address family ipv4** 命令下的命令集内。您必须配置地址系列以配置过滤功能。这些规则不适用于 IPv6。

步骤 5 点击**显示已禁用**以显示所有命令，然后点击 **+** 以启用 **configure filter-rules** *direction* 命令。

步骤 6 点击方向，然后选择 **in** 以对传入更新进行过滤，或选择 **out** 来过滤出站更新。

步骤 7 对于入站过滤器，可以选择性地指定用于过滤更新的接口。如果不指定接口，则过滤器将应用于在任何接口上接收的所有更新。

a) 点击 **+** 启用 **distribute-list** *acl-name* **in interface** *interface* 命令。

b) 点击 *interface* 变量并选择接口。

步骤 8 对于出站过滤器，您可以选择性地指定协议，以将过滤器限制为通告到该路由进程的路由。

有两种形式的 **distribute-list out** 命令，一种是在 *protocol* 变量后跟一个 *identifier* 变量，另一种则不带标识符。您可以选择以下协议，但是，这些协议会根据您是否必须提供其他标识符信息来在这些命令版本之间划分。

- **connected**。适用于为直接连接到系统接口的网络而建立的路由。
- **static**。适用于手动创建的静态路由。
- **rip**。适用于通告到 RIP 的路由。
- **bgp** *automonous-system*。适用于通告到 BGP 的路由。点击 *identifier*，然后输入在系统中定义的 BGP 进程的自治系统编号。
- **eigrp** *automonous-system*。适用于通告到 EIGRP 的路由。点击 *identifier*，然后输入在系统中定义的 EIGRP 进程的自治系统编号。
- **ospf** *process-id*。适用于通告到 OSPF 的路由。点击 *identifier*，然后输入在系统中定义的 OSPF 进程的进程 ID。

步骤 9 您可以点击 **...** > **复制**（位于 **configure filter-rules** 命令的旁边）以定义另一个过滤规则。根据需要定义任意数量的虚拟链路。

步骤 10 点击**确定 (OK)**。

配置 BGP 邻居

您需要定义 BGP 将与之交换路由更新的邻居。

开始之前

对于路由映射和前缀列表等，有几个可选命令需要使用 Smart CLI 对象。检查您需要配置的选项，以确定是否需要对象。在配置关联的 BGP 命令之前，必须创建 Smart CLI 对象。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 BGP 的路由器的查看图标 ( )。

步骤 3 点击 **BGP** 选项卡。

步骤 4 添加或编辑 BGP 进程对象。

邻居命令位于 **configure address family ipv4** 或 **ipv6** 命令下的命令集内。必须为每个地址系列单独配置邻居。

步骤 5 点击**显示已禁用**以显示所有命令，然后点击 **+** 以启用 **configure neighbor** 命令。

步骤 6 在邻居命令上配置基本邻居参数：

- **neighbor** *neighbor-address*。点击此变量，然后根据要配置的地址组输入 BGP 邻居路由器的 IPv4 或 IPv6 地址。
- **remote-as** *as-number*。点击此变量，然后输入 BGP 邻居路由器的自治系统编号。
- *config-options*。点击此变量，然后选择 **properties**。默认情况下，所配置的唯一属性会激活邻居。可以根据此程序中的说明调整其他选项。

步骤 7 （可选。）配置邻居常规设置

a) 点击 **+** 启用 **configure neighbor** *neighbor-address* **remote-as** *settings* 命令。如果看不到该命令，请点击**显示已禁用**。

b) 点击 *settings*，并选择 **general**。

c) 在 **configure neighbor description** 命令中，点击变量并输入邻居的描述信息（例如其位置或用途，最多可包含 80 个字符），或点击 **-** 以在不需要描述信息的情况下禁用该命令。说明中不能包含空格或问号。

d) （仅 IPv4。）**configure neighbor shutdown** 命令最初已启用。此命令会禁用与此 BGP 邻居的通信，终止任何活动会话并删除所有关联的路由信息。如果要主动与此邻居通信，请点击 **-** 禁用此命令。

e) 在 **configure neighbor fall-over bfd** 命令中，点击 *option*，并选择 **single-hop** 或 **multi-hop**（取决于您的 BFD 配置），或点击 **-** 禁用命令。

此命令可注册 BGP 以接收来自双向转发检测 (BFD) 的转发路径检测失败消息。是选择单跳还是多跳将取决于您已创建并已连接到面向此邻居的接口的 BFD 模板的类型。确保您在此处所做选择的与 BFD 模板一致。必须使用 FlexConfig 来构建和应用 BFD 模板。

步骤 8 （可选。）配置邻居高级设置

a) 如果已配置，请点击 **...** > **复制**（针对 **configure neighbor** *neighbor-address* **remote-as** *settings* 命令），或直接点击 **+** 启用（如果尚未使用）。如果看不到该命令，请点击**显示已禁用**。

b) 点击 *settings*，并选择 **advanced**。

c) 在 **neighbor password** 命令中，点击 *secret* 变量，然后选择其中包含用于对邻居进行身份验证的密码的密钥对象。如果不希望使用消息摘要 5 (MD5) 身份验证，请点击 - 禁用该命令。在编辑 BGP 对象时，您可以创建主要目标。

密钥对象必须包含密钥密码（最大长度为 25 个字符，区分大小写）。此字符串包含任意字母数字字符，包括空格以及特殊字符 ` ~ ! @ # $ % ^ & * ( ) - _ = + | \ } ] { [ " ` : ; / > <., ?。但是，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。

确保将邻居配置为使用相同的密码。

d) 在 **configure neighbor hops** 命令中，点击 *options* 变量并选择以下选项之一。如果对等体不是多跳（即，不直接连接到此系统），则点击 - 禁用该命令。应谨慎使用这些选项，因为您可以使用路由环路和振荡路由来完成以下操作：建议仅配置直接连接的对等体。

- **ebgp-multihop**。接受并尝试建立与未直接连接的网络上的外部对等体的 BGP 连接。如果选择此选项，会添加以下命令：
  - **neighbor ebgp-multihop 255**。点击 255，然后以跳数（范围为从 1 到 255）形式输入生存时间值。
  - **neighbor disable-connected-check**。点击 **+** 启用此命令，以禁用连接验证可与使用环回接口的单跳对等体建立 eBGP 对等会话。不使用此命令时，如果对等体没有直连到同一网段，连接验证将阻止建立对等会话。
- **ttl-security-hop**。保护 BGP 对等会话，并且配置用于分隔两个外部 BGP (eBGP) 对等体的最大跳数。如果选择此选项，会添加以下命令：

  neighbor ttl-security hops *hop-count*。点击此变量，然后输入将用于分隔对等体的最大跳数，范围为从 1 到 254。

  neighbor ttl-security 命令提供了一种轻型安全机制，用于保护 BGP 对等会话免受基于 CPU 利用率的攻击。这些类型的攻击通常是暴力拒绝服务 (DoS) 攻击，即通过使数据包报头中包含伪造的源和目标 IP 地址的 IP 数据包充斥网络来尝试禁用网络。

  此功能通过仅接受 TTL 计数等于或大于本地配置值的 IP 数据包来利用 IP 数据包的设计行为。准确伪造 IP 数据包中的 TTL 计数通常被视为不可能。如果没有源或目标网络的内部访问权限，则准确伪造数据包以匹配来自信任对等体的 TTL 计数是不可能的。

  要最大限度地提高此功能的有效性，“hop-count”值应严格配置为匹配本地与外部网络之间的跃点数。但是，为多跃点对等会话配置此功能时，您还应该考虑路径变化。确保在网络中的所有路由器上配置此功能。

e) 在 **neighbor version** 命令中，点击 *version-number* 变量并输入 4 以强制软件使用 BGP 版本 4，或点击 - 禁用命令。默认情况下，软件将使用版本 4，并在必要时向下动态协商为版本 2。在此命令中配置 4 将禁止版本协商。

f) 在 **neighbor transport connection-mode** 命令中，点击 *options* 变量并选择 TCP 连接是 **active** 还是 **passive**，或者点击 - 禁用命令并使模式保持默认状态。

g) 在 **neighbor transport path-mtu-discovery** 命令中，点击 *options* 变量并选择 **blank** 启用路径 MTU 发现功能，或点击 **disable** 将其禁用。选择空白与点击 - 均可禁用命令，因为系统默认会执行路径 MTU 发现操作。通过路径 MTU 发现操作，BGP 会话可以利用更大的 MTU 链路。

步骤 9 （可选。）配置邻居迁移设置。

迁移设置将配置 **neighbor local-as** 命令。通过添加和删除从 eBGP 邻居接收的路由的自治系统编号，**neighbor local-as** 命令可用于定制 AS_PATH 属性。为了支持自治系统编号迁移，此命令的配置允许路由器作为其他自治系统的成员显示为外部对等体。此功能允许网络运营商在正常服务时段将客户迁移到新配置而无需中断现有的对等布置，简化了在 BGP 网络中更改自治系统编号的过程。

可以仅对真正的 eBGP 对等会话执行此迁移。此命令不适用于联盟的不同子自治系统中的两个对等体。

注意 BGP 预置路由穿越的每个 BGP 网络的自治系统号，以维护网络可达性信息和防止路由环路。应将此命令配置为仅用于自治系统迁移，并在完成迁移后取消配置此命令。此程序应仅由经验丰富的网络操作员尝试执行。配置不当可能会造成路由环路。

a) 如果已配置，请点击 **...** > **复制**（针对 **configure neighbor** *neighbor-address* **remote-as** *settings* 命令），或直接点击 **+** 启用（如果尚未使用）。如果看不到该命令，请点击**显示已禁用**。

b) 点击 *settings*，并选择 **migration**。这会添加以下命令：

configure *neighbor-address* **local-as** *local-as-number options*

c) 点击 *local-as-number* 变量，然后输入本地自治系统 (AS) 编号，以 AS_PATH 属性开头，范围为从 1 到 4294967295（asplain 表示法）或 1.0 到 65535.65535（asdot 表示法）。您无法指定来自本地 BGP 路由过程或来自远程对等体网络的自治系统编号。

d) 点击 *options* 变量，然后选择以下选项之一。请注意，如果选择此列表中的项目（除 **none** 外），还会选择列表中此项目上方的所有选项。这是预期行为：这些选项不是真正独立的选项。

- **none**。不得配置以下任何选项。
- **no-prepend**。不向从 eBGP 邻居接收的任何路由预置本地自治系统编号。
- **replace-as**。将真实自治系统编号替换为 eBGP 更新中的本地自治系统编号。来自本地 BGP 路由过程的自治系统编号不会预置到前面。
- **dual-as**。将 eBGP 邻居配置为使用实际自治系统号（来自本地 BGP 路由过程）或使用本地自治系统编号建立对等会话。

步骤 10 （可选，仅限 IPv4。）配置邻居高可用性 (HA) 设置。

HA 模式设置将配置 **neighbor ha-mode graceful-restart** 命令，该命令可为单个 BGP 邻居启用或禁用平稳重启功能。如果以前为 BGP 对等体启用了平稳重启，则使用 disable 关键字可禁用平稳重启功能。

会话建立过程中，在 OPEN 消息中支持无间断转发 (NSF) 和 NSF 感知的对等体之间协商平稳重启功能。如果在 BGP 会话建立后启用平稳重启功能，您需要通过软重置或硬重置来重新启动该会话。

HA 模式设置将为单个邻居配置平稳重启。您可以使用 BGP 全局设置来为所有邻居启用平稳重启。

a) 如果已配置，请点击 **...** > **复制**（针对 **configure neighbor** *neighbor-address* **remote-as** *settings* 命令），或直接点击 **+** 启用（如果尚未使用）。如果看不到该命令，请点击**显示已禁用**。
b) 点击 *settings*，并选择 **ha-mode**。
c) 如果要禁用平稳重启，请点击 **neighbor ha-mode graceful-restart** 命令上的 *options*，然后选择 **disable**。选择空白撤消之前的禁用操作。

步骤 11 （可选。）配置邻居激活选项。

配置新邻居时，默认情况下会激活该邻居。如果您希望在最初时禁用邻居，则需要启用激活设置，或者配置其他激活设置。

a) 点击 **+** 启用 **configure neighbor** *neighbor-address* **activate** *activate-options* 命令。如果看不到该命令，请点击**显示已禁用**。
b) 点击 *activate-options*，然后选择 **properties**。
c) 添加处于启用状态下的 **neighbor** *neighbor-address* **activate** 命令。点击 **-** 禁用此命令并将邻居配置为在最初时禁用。当您准备好与其通信时，您将需要编辑此对象才能启用邻居。

步骤 12 （可选。）在邻居激活设置中配置过滤。

a) 如果已配置，请点击 **...** > **复制**（针对 **configure neighbor** *neighbor-address* **activate** *settings* 命令），或直接点击 **+** 启用（如果尚未使用）。如果看不到该命令，请点击**显示已禁用**。
b) 点击 *settings*，并选择 **filtering**。
c) 配置过滤，以使用下列邻居命令的任意组合来控制从/向该邻居接收/发送的前缀。点击 **-** 禁用不想使用的任何命令。所有这些命令都允许在入站和出站方向上进行过滤：如果要配置两个方向，请为命令点击 **...** > **复制**。

   请勿将 **neighbor distribute-list** 和 **neighbor prefix-list** 命令同时应用于同一方向的邻居。这两个命令互相排斥，其中只有一个命令可以应用于每个入站或出站方向。

   - **distribute-list** *acl options*。（仅 IPv4。）根据所选标准访问列表 (ACL) 过滤前缀。然后，点击 *options*，并选择是否在 **in** 或 **out** 方向上应用过滤器。
   - **route-map** *route-map options*。根据所选路由映射过滤前缀。然后，点击 *options*，并选择是否在 **in** 或 **out** 方向上应用过滤器。在路由映射中，可以根据访问列表、路径、前缀和分发列表配置过滤。
   - **prefix-list** *prefix-list options*。根据所选 IPv4 或 IPv6 前缀列表过滤前缀。然后，点击 *options*，并选择是否在 **in** 或 **out** 方向上应用过滤器。
   - **filter-list** *as-path options*。根据所选 AS 路径过滤器对象过滤前缀。然后，点击 *options*，并选择是否在 **in** 或 **out** 方向上应用过滤器。

d) 在 **configure prefix-limit neighbor** *neighbor-address limit-options* 命令中，点击 *limit-options*，然后选择以下选项之一，或点击 **-** 禁用命令。选择任何选项都会添加某种形式的 **neighbor maximum-prefix** 命令，其中包含您需要配置的其他选项。使用此命令控制可以从邻居接收的前缀的数量。

   - **none**。配置命令的基本形式，无需其他参数。点击此变量并配置以下值：
     - max-prefix-limit。从此邻居允许的前缀的最大数量，范围为从 1 到 2147483647。如果您选择任何其他选项，则还必须配置此变量。

- **75**（阈值）。路由器开始生成警告消息时所处的最大值的百分比，范围为从 1 到 100。默认值为 75%。

- **restart**。当达到限制时，停止与邻居的对等会话。点击 *restart-interval* 变量，然后配置系统在重启会话之前应等待的时间，范围为从 1 到 65535 分钟。
- **warning-only**。当达到限制时，请勿停止会话，而只需发出警告系统日志消息，并继续会话。

步骤 13 （可选。）在邻居激活设置中配置路由。

a) 如果已配置，请点击 **...** > **复制**（针对 **configure neighbor** *neighbor-address* **activate** *settings* 命令），或直接点击 **+** 启用（如果尚未使用）。如果看不到该命令，请点击**显示已禁用**。

b) 点击 *settings*，并选择 **routes**。

c) 在 **neighbor advertisement-interval** 命令中，点击 *value* 变量，然后输入两次向此邻居发送路由更新的操作之间的最小路由通告间隔，范围为从 0 到 600 秒，或者点击 **-** 禁用命令，然后将间隔保留为默认值 0（适用于在虚拟路由器中的 iBGP 和 eBGP 会话）或 30（适用于不在虚拟路由器中的 eBGP 会话）。值 0 表示系统将在路由表每次发生更改时发送更新，而不考虑频率。

d) 在 **neighbor advertise-map** 命令中，配置以下选项以有条件地将选定路由通告给邻居，或点击 **-** 禁用该命令，从而无条件地将所有路由更新发送到邻居。

有条件通告的路由（前缀）在两个路由映射中定义：通告映射以及存在映射或非存在映射。

与存在映射或非存在映射关联的路由映射指定 BGP 发言者将跟踪的前缀。

与通告映射关联的路由映射指定条件满足时将通告到指定邻居的前缀。

如果配置存在映射，则前缀在通告映射和存在映射中都存在时才满足条件。

如果配置非存在映射，则前缀在通告映射中存在并且在非存在映射中不存在时才满足条件。

如果条件未满足，则路由将撤消并且不会进行条件通告。可能已动态通告或未通告的所有路由都需要在 BGP 路由表中存在才能进行条件通告。

- *advertise-route-map*。点击此变量，然后选择在满足存在映射或非存在映射的条件时用于定义应通告的路由的路由映射。
- *options condition-route-map*。点击 options 并选择以下选项之一：
  - **exist-map**。点击此变量并选择存在路由映射。
  - **non-exist-map**。点击此变量并选择非存在路由映射。

e) 添加处于启用状态下的 **neighbor** *neighbor-address* **remove-private-as** 命令。点击“-”禁用此命令。此命令将从 eBGP 出站路由更新中删除专用自治系统编号。专用 AS 值范围为从 64512 到 65535。

f) 在 **configure neighbor default-originate** 命令中，点击 *options* 并选择下列选项之一，或点击“-”禁用此命令。

- **none**。允许系统无条件地向邻居发送默认路由。

- **route-map**。让系统有条件地向邻居发送默认路由。与路由映射一起使用时，如果路由映射包含匹配 IP 地址子句并且有与 IP 访问列表确切匹配的路由，则注入默认路由。可以使用路由映射中的标准访问列表或扩展访问列表来定义默认路由。必须点击将添加到对象的**neighbor default-originate** 命令中的 *route-map* 变量，然后选择路由映射。

步骤 14 （可选。）在邻居激活设置中配置计时器。

如果为邻居配置计时器，则这些设置会覆盖在全局 BGP 设置中为所有 BGP 邻居配置的计时器。

a) 如果已配置，请点击 **...** > **复制**（针对 **configure neighbor** *neighbor-address* **activate** *settings* 命令），或直接点击 **+** 启用（如果尚未使用）。如果看不到该命令，请点击**显示已禁用**。
b) 点击 *settings*，并选择 **timers**。
c) 在 **neighbors timers** 命令中，配置以下变量：

- *keepalive-interval*。系统向此邻居发送保持连接消息的频率，范围为从 0 到 65535 秒。如果不配置此命令，默认值为 60 秒。
- *hold-time*。在未收到系统声明此邻居“无响应”的保持连接间隔消息后的间隔，范围为从 0 到 65535 秒。如果不配置此命令，默认值为 180 秒。
- **0**（最小保持时间）。可在此邻居上配置的最小可接受保持时间，范围为从 0 到 65535 秒。此值必须小于或等于为此系统配置的保持时间。如果邻居的保持时间小于此值，系统将不会与邻居建立 BGP 会话。

步骤 15 （可选。）配置高级邻居激活设置。

a) 如果已配置，请点击 **...** > **复制**（针对 **configure neighbor** *neighbor-address* **activate** *settings* 命令），或直接点击 **+** 启用（如果尚未使用）。如果看不到该命令，请点击**显示已禁用**。
b) 点击 *settings*，并选择 **advanced**。
c) 确定要启用以下 **neighbor** 命令中的哪个命令。点击 **-** 禁用不需要的选项。

- **send-community**。将社区属性发送到邻居。
- **weight** *value*。点击此变量以将初始权重分配给从该邻居获知的路由，范围为从 0 到 65535。如果不配置此命令，则通过另一个 BGP 对等体获知的路由默认权重为 0，而源自本地路由器的路由默认权重为 32768。但是，通过使用路由映射设置的任何路由权重会覆盖通过使用此命令配置的权重。
- **next-hop-self**。将路由器配置为 BGP 发言邻居的下一跳。此命令在无网状结构的网络（例如帧中继或 X.25）中非常有用，在该类网络中，BGP 邻居可能没有对同一 IP 子网上所有其他邻居的直接访问权限。

步骤 16 您可以点击 **...** > **复制**（位于 **configure neighbor** 命令的旁边）以定义另一个邻居。根据需要定义任意数量的虚拟链路。

步骤 17 点击**确定 (OK)**。

根据其他路由协议配置 BGP 路由重新分发

您可以控制从其他路由协议、连接路由和静态路由中将路由重新分发到 BGP 进程的过程。

开始之前

最佳实践是在将重新分发到 BGP 之前，配置您将从中重新分发路由的路由进程，并部署更改。

如果要应用路由映射以微调重新分发的路由，请创建 Smart CLI 路由映射对象。将重新分发与路由映射匹配的路由，并且不会重新分发所有不匹配的路由。

过程

步骤 1 点击**设备**，然后点击**路由**摘要。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置 BGP 的路由器的查看图标 ( )。

步骤 3 点击 **BGP** 选项卡。

步骤 4 添加或编辑 BGP 进程对象。

重新分发命令位于 **configure address family ipv4** 或 **ipv6** 命令下的命令集内。您必须配置地址系列以配置重新分发。

步骤 5 点击**显示已禁用**以显示所有命令，然后点击 **+** 以启用 **configure ipv4/ipv6 redistribution** 命令。

步骤 6 点击 *protocol* 变量，并选择要从中重新分发路由的源进程。可以重新分发 **connected** 和 **static** 路由，或由 **eigrp**（仅限 IPv4）、 **isis**、 **ospf** 或 **rip**（仅限 IPv4）生成的路由。

步骤 7 如果选择路由进程，请点击 *identifier* 变量，然后输入所需的值：

- **eigrp**。输入自治系统编号。
- **ospf**。输入进程 ID 编号。
- **connected**、**static**、**isis**、**rip**。输入 **none**。即使您输入其他值，它也会被忽略。

步骤 8 （可选；仅限 IS-IS。）在 **redistribute isis level-2** 命令中，点击 **level-2** 并选择是否要仅重新分发在 IS-IS 区域 (**level-1**) 中、在 IS-IS 区域 (**level-2**) 之间或两者 (**level-1-2**) 中获知的路由。

步骤 9 （可选；所有协议。）要微调用于重新分发的路由的度量，请点击 **+** 启用以下命令并配置选项：

redistribute *protocol* **metric** *metric-value*

点击此变量，然后输入要分配的路由的指标值，范围为从 0 到 4294967295。

步骤 10 （可选；所有协议。）要根据路由映射调整重新分配的路由，请点击 **+** 启用 **redistribute route-map** 命令，点击此变量，然后选择用于定义限制条件的路由映射。

如果不应用路由映射，则会重新分发进程的所有路由（适合为重新分发而配置的其他命令）。

步骤 11 （可选；仅限 OSPF。）当您从 OSPF 进程重新分发路由时，默认情况下会启用以下命令。可以点击 **-** 禁用不需要的命令。

这些命令用于指定将 OSPF 路由重新分发到其他路由域的条件。

- **redistribute ospf match external 1**。自治系统的外部路由，但是会作为 1 类外部路由导入 OSPF。
- **redistribute ospf match external 2**。自治系统的外部路由，但是会作为 2 类外部路由导入 OSPF。
- **redistribute ospf match internal**。特定自治系统的内部路由。
- **redistribute ospf match nssa-external 1**。自治系统的外部路由，但是会作为 1 类外部路由导入 OSPF，并仅标记为次末节区域 (NSSA)。
- **redistribute ospf match nssa-external 2**。自治系统的外部路由，但是会作为 2 类外部路由导入 OSPF，并仅标记为次末节区域 (NSSA)。

步骤 12 您可以点击 **...** > **复制**（位于 **configure redistribution** 命令的旁边），以配置另一种协议的重新分发。为适合您的网络的每种协议配置重新分发。

步骤 13 点击**确定 (OK)**。

监控 BGP

要对 BGP 进行监控和故障排除，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。您还可以从“路由”(Routing) 页面的**命令 (Commands)** 菜单选择其中一些命令。

使用 **show bgp ?** 获取其他选项的列表。例如，您可以指定自治系统编号和虚拟路由器，以限制您看到的信息，还可以指定其他选项以仅查看您要查找的信息。以下列表只是一份摘要。

- **show bgp**

  显示 BGP 路由表中的条目。

- **show bgp cidr-only**

  显示带有非自然网络掩码的路由（即，无类别域间路由，或 CIDR）。

- **show bgp community**

  显示属于指定 BGP 社区的路由。

- **show bgp community-list**

  显示 BGP 社区列表允许的路由。

- **show bgp filter-list** *access-list-number*

  显示与指定的过滤器列表相符的路由。

- **show bgp injected-paths**

  显示 BGP 路由表中所有注入的路径。

- **show bgp ipv4 unicast**

  显示 IP 版本 4 (IPv4) BGP 路由表中的单播会话条目。

- **show bgp ipv6 unicast**

  显示 IPv6 BGP 路由表中的条目。

- **show bgp neighbors**

  显示到邻居的 BGP 和 TCP 连接的相关信息

- **show bgp paths**

  显示数据库中的所有 BGP 路径。

- **show bgp prefix-list**

  显示有关前缀列表或前缀列表条目的信息。

- **show bgp regexp** *regexp*

  显示与自治系统路径正则表达式相匹配的路由。

- **show bgp rib-failure**

  显示无法安置在路由信息库 (RIB) 表中的 BGP 路由。

- **show bgp summary**

  显示所有 BGP 连接的状态。

- **show bgp update-group**

  显示有关 BGP 更新组的信息。

第 V 部分

安全策略

第 18 章

SSL 解密

某些协议（如 HTTPS）使用安全套接字层 (SSL) 或其后续版本传输层安全性 (TLS) 来加密流量以进行安全传输。由于系统无法检查加密连接，因此，如果要应用可考虑借助更高层流量特性进行访问决策的访问规则，则必须将其解密。

关于 SSL 解密

通常情况下，访问控制策略会评估连接以确定是允许还是阻止相应连接。但是，如果启用 SSL 解密策略，则连接将首先被发送至 SSL 解密策略，以确定应将其解密还是阻止。然后，访问控制策略评估所有未阻止连接（无论是否解密），作出最终的允许/阻止决策。

注释 您必须启用 SSL 解密策略，才能在身份策略中实施有效的身份验证规则。如果您启用 SSL 解密来启用身份策略，但不想另外实施 SSL 解密，请选择“不解密”作为默认操作，并且不要创建其他 SSL 解密规则。身份策略会自动生成所需的任何规则。

以下主题更详细地介绍了加密流量管理和解密。

为什么要实施 SSL 解密？

无法检查 HTTPS 连接等加密流量。

许多连接均是合法加密的连接，比如与银行和其他金融机构的连接。许多网站使用加密保护隐私或敏感数据。例如，您与 设备管理器 的连接已加密。

但是，用户也可能会隐藏加密连接中的不良流量。

通过实施 SSL 解密，可解密和检查连接，确保不含威胁或其他不良流量，然后重新加密后再允许继续连接。（解密流量通过访问控制策略，并根据检查的加密连接特征而不是加密特征匹配规则。）这平衡了应用访问控制策略的需求与用户保护敏感信息的需求。

还可以配置 SSL 解密规则，阻止明确不想要允许其进入网络的加密流量类型。

请记住，解密并重新加密流量会增加设备的处理负载，从而降低整体系统性能。

可应用于加密流量的操作

配置 SSL 解密规则时，可应用以下主题中所述的操作。这些操作也可用于默认操作（适用于与显示规则不匹配的任何流量）。

注释 通过 SSL 解密策略的任何流量均必须通过访问控制策略。除了 SSL 解密策略中丢弃的流量外，最终的允许或丢弃决定还取决于访问控制策略。

解密重签名

如果选择解密或重签流量，系统将扮演中间人的角色。

例如，用户在浏览器中键入 https://www.cisco.com。流量到达 威胁防御 设备，然后设备使用规则中指定的 CA 证书与用户进行协商，并在用户和 威胁防御 设备之间建立 SSL 隧道。同时，设备连接至 https://www.cisco.com ，并在服务器和 威胁防御 设备之间建立 SSL 隧道。

因此，用户将看到配置用于 SSL 解密规则的 CA 证书，而不是来自 www.cisco.com 的证书。用户必须信任该证书才能完成连接。威胁防御 设备随后对用户和目标服务器之间的流量执行双向解密/重新加密。

注释 如果客户端不信任用于对服务器证书重新签名的CA，则会警告用户不应信任该证书。为了避免此情况，请将 CA 证书导入到客户端信任的 CA 库。或者，如果组织拥有专用 PKI，则可以颁发由根 CA（自动受组织中的所有客户端信任）签名的中级 CA 证书，然后将该 CA 证书上传到设备。

如果使用解密重签名操作配置规则，则除了已配置的任何规则条件之外，该规则会根据所引用的内部 CA 证书的签名算法类型来匹配流量。由于您可以选择用于 SSL 解密策略的单个重签名证书，因此可以限制匹配重签规则的流量。

例如，仅当重签名证书是基于 EC 的 CA 证书时，使用椭圆曲线 (EC) 算法加密的出站流量才能匹配解密重签名规则。同样，仅当全局重签名证书为 RSA 时，使用 RSA 算法加密的流量才可与解密重签名规则匹配；即使所有其他配置的规则条件匹配，使用 EC 算法加密的出站流量也与规则不匹配。

解密已知密钥

如果您拥有目标服务器，则可使用已知密钥实现解密。在这种情况下，用户打开 https://www.cisco.com 的连接后，用户会看到 www.cisco.com 的实际证书，即使出示证书的是 威胁防御 设备。

您的组织必须是域和证书的所有者。以 cisco.com 为例，让最终用户查看思科证书的唯一可能方式是，您实际拥有域 cisco.com（即您是思科系统公司）并拥有由公共 CA 签名的 cisco.com 证书。您仅可使用已知密钥对您的组织拥有的站点进行解密。

使用已知密钥进行解密的主要目的是对通往 HTTPS 服务器的流量进行解密，以保护服务器免受外部攻击。如要检查流向外部 HTTPS 站点的客户端流量，由于您不是服务器所有者，所以必须使用解密重签名。

注释 要使用已知密钥解密，必须将服务器证书和密钥上传为内部身份证书，再在 SSL 解密策略设置中将其添加至已知密钥证书。然后，可编写已知密钥解密规则，其中服务器地址为目标地址。有关将证书添加至 SSL 解密策略的信息，请参阅为已知密钥和重签解密配置证书，第 436 页。

不解密

如果选择绕行某些类型的流量的解密，则不会对流量进行任何处理。系统会使加密流量继续进入访问控制策略，根据流量所匹配的访问控制规则对其执行允许或丢弃操作。

阻止

您可以简单地阻止匹配 SSL 解密规则的加密流量。阻止 SSL 解密策略可防止连接到访问控制策略。

阻止 HTTPS 连接后，用户看不到系统默认阻止响应页面。相反，用户会看到浏览器显示安全连接故障的默认页面。错误消息不会指明该站点由于策略而被阻止。相反，错误可能显示为没有通用的加密算法。据此消息，无法明确看出是您有意阻止了该连接。

自动生成的 SSL 解密规则

无论您是否启用 SSL 解密策略，系统都会自动为实施主动身份验证的各身份策略规则生成解密重签名规则。这是为 HTTPS 连接启用主动身份验证的必然要求。

启用 SSL 解密策略后，您可以在“身份策略主动身份验证规则”标题下看到这些规则。这些规则归入 SSL 解密策略顶部。这些规则为只读格式。仅可通过更改身份策略进行更改。

处理不可解密流量

有几个特点使得连接不可解密。如果连接具有以下任何特征，则默认操作将应用于该连接，而不管该连接本可能会与哪个规则匹配。如果将“阻止”选作默认操作（而不是“不解密”），则可能会出问题，包括过度丢弃合法流量的问题。您可以更改默认行为，如配置高级和无法解密的流量设置，第 437 页中所述。

- 压缩会话 - 数据压缩应用于连接。
- SSLv2 会话 - 支持的最低 SSL 版本是 SSLv3。
- 未知密码套件 - 系统无法识别连接的密码套件。
- 不受支持的密码套件 - 系统不支持根据检测到的密码套件进行解密。
- 会话未缓存 - SSL 会话已启用会话重复使用，客户端和服务器使用会话标识符重新建立了该会话，并且系统未缓存该会话标识符。
- 握手错误 - SSL 握手协商期间出错。
- 解密错误 - 解密操作期间出错。
- 被动接口流量 - 被动接口（被动安全区）上的所有流量均无法解密。

SSL 解密许可证要求

使用 SSL 解密策略无需特殊许可证。

但需要 **URL** 许可证创建将 URL 类别和信誉作为匹配条件的规则。有关配置许可证的信息，请参阅启用或禁用可选许可证，第 87 页。

SSL 解密准则

配置和监控 SSL 解密策略时，请注意以下事项：

- 对于与设置为信任或阻止的访问控制规则匹配的任何连接，如果这些规则满足以下条件，则绕过 SSL 解密策略：
  - 将安全区、网络、地理位置和端口仅用作流量匹配条件。

- 排在任何要求检测的其他规则之前，例如，基于应用或URL匹配连接的规则，或允许应用入侵或文件检测的规则。

- 使用URL类别匹配时，请注意，有时候站点登录页的类别与站点本身的类别不同。例如，Gmail的类别是“基于网页的邮件”，而登录页的类别是“互联网门户网站”。要对到这些站点的连接解密，必须在规则中添加这两个类别。
- 如果漏洞数据库 (VDB) 更新删除（弃用）应用，则必须对使用已删除应用的任何 SSL 解密规则或应用过滤器进行更改。修复这些规则前，您无法部署更改。此外，您无法在解决问题之前安装系统软件更新。在“应用过滤器对象”页面上或规则的“应用”选项卡上，这些应用在应用名称后显示“（已弃用）”。
- 如果您有任何主动身份验证规则，将无法禁用 SSL 解密策略。要禁用 SSL 解密策略，您必须禁用身份策略，或者删除任何使用主动身份验证的身份规则。

如何实施和维护 SSL 解密策略

您可以使用 SSL 解密策略将加密流量转换为纯文本流量，以便可应用 URL 过滤、入侵和恶意软件控制以及其他需要深度数据包检测的服务。如果策略允许流量通过，则流量在离开设备前会被重新加密。

SSL 解密策略仅适用于加密流量。系统不会根据 SSL 解密规则评估未加密连接。

与其他一些安全策略不同的是，您需要监控并积极维护 SSL 解密策略，这是因为目标服务器上的证书可能会过期甚至发生变更。此外，客户端软件的变更可能会改变解密某些连接的能力，这是因为解密重签名操作无法与中间人攻击区分开来。

以下程序介绍了实施和维护 SSL 解密策略的端到端流程。

过程

步骤 1 如果要实施解密重签名规则，请创建所需的内部 CA 证书。

必须使用内部证书颁发机构 (CA) 证书。您有以下选择：由于用户必须信任证书，因此应上传客户端浏览器已配置为可信任的证书，或确保所上传的证书已添加到浏览器信任存储区。

- 创建由设备自身签署的自签名内部 CA 证书。请参阅生成自签名的内部证书和内部 CA 证书，第 146 页。
- 上传由外部受信任 CA 或组织内部 CA 签署的内部 CA 证书和密钥。请参阅上传内部证书和内部 CA 证书，第 145 页。

步骤 2 如果要实施解密已知密钥规则，请从各内部服务器收集证书和密钥。

只可将解密已知密钥用于您所控制的服务器，这是因为必须从服务器中获取证书和密钥。上传这些证书和密钥，作为内部证书（而不是内部CA证书）。请参阅上传内部证书和内部CA证书，第 145 页。

步骤 3 启用 SSL 解密策略，第 428 页。

启用该策略时，还需要配置一些基本设置。

步骤 4 配置默认 SSL 解密操作，第 429 页。

如有疑问，请选择**不解密**作为默认操作。在适当的情况下，访问控制策略仍然可以丢弃与默认 SSL 解密规则匹配的流量。

步骤 5 配置 SSL 解密规则，第 430 页。

标识要解密的流量以及要应用的解密类型。

步骤 6 如要配置已知密钥解密，请编辑 SSL 解密策略设置，以加入这些证书。请参阅为已知密钥和重签解密配置证书，第 436 页。

步骤 7 如有需要，下载用于解密重签名规则的 CA 证书并将其上传到客户端工作站上的浏览器。

有关下载证书并将其分发给客户端的信息，请参阅为解密重签名规则下载 CA 证书，第 438 页。

步骤 8 定期更新重新和已知密钥证书。

- 重签名证书 - 在证书过期之前更新此证书。如果通过 设备管理器生成证书，则有效期为 5 年。要检查证书的有效期，请依次选择 **对象 (Objects)** > **证书 (Certificates)**，在列表中查找该证书，然后在“操作”(Actions) 列中点击证书的信息图标 ( )。“信息”对话框显示有效期和一些其他属性。此外，也可从此页面上传替换证书。
- 已知密钥证书 - 对于任何已知密钥解密规则，需要确保已上传目标服务器的当前证书和密钥。只要所支持的服务器上的证书和密钥发生更改，就必须上传新的证书和密钥（作为内部证书）并更新 SSL 解密设置，以使用新证书。

步骤 9 上传外部服务器缺失的受信任 CA 证书。

系统包含各种由第三方颁发的受信任根证书和中间证书。为解密重签名规则协商威胁防御和目标服务器之间的连接时，需要这些证书。

将根 CA 的信任链链中的所有证书都上传到受信任 CA 证书列表中，包括根 CA 证书和所有中间 CA 证书。否则，更难以检测由中间 CA 颁发的受信任证书。在**对象 (Objects)** > **证书 (Certificates)** 页面上上传证书。请参阅上传受信任的 CA 证书，第 148 页。

配置 SSL 解密策略

您可以使用 SSL 解密策略将加密流量转换为纯文本流量，以便可应用 URL 过滤、入侵和恶意软件控制以及其他需要深度数据包检测的服务。如果策略允许流量通过，则流量在离开设备前会被重新加密。

SSL 解密策略仅适用于加密流量。系统不会根据 SSL 解密规则评估未加密连接。

注释 VPN 隧道在 SSL 解密策略评估之前已解密，因此该策略永远不适用于隧道本身。但是，隧道内的任何加密连接都要通过 SSL 解密策略进行评估。

以下程序介绍了如何配置 SSL 解密策略。有关创建和管理 SSL 解密的端到端流程说明，请参阅如何实施和维护 SSL 解密策略，第 425 页。

开始之前

SSL 解密规则表包含两个部分：

- **身份策略主动身份验证规则** - 如果启用身份策略并创建使用主动身份验证的规则，系统将自动创建使这些策略生效所需的 SSL 解密规则。这些规则始终在您自己创建的 SSL 解密规则之前进行评估。只可通过更改身份策略来间接更改这些规则。
- **SSL 本机规则** - 这些是已经配置的规则。只能将规则添加到此部分。

过程

步骤 1 依次选择**策略** > **SSL 解密**。

如果尚未启用该策略，请点击**启用 SSL 解密**并按启用 SSL 解密策略，第 428 页中的说明配置策略设置。

步骤 2 配置策略的默认操作。

最安全的选择是**不解密**。有关详细信息，请参阅配置默认 SSL 解密操作，第 429 页。

步骤 3 管理 SSL 解密策略。

在配置 SSL 解密设置后，此页面将按顺序列出所有规则。规则依据流量按照从上到下的顺序进行匹配，由第一个匹配项确定要应用的操作。从此页面中可以执行以下操作：

- 要禁用该策略，请点击 **SSL 解密策略**开关。可以通过点击**启用 SSL 解密**重新启用该策略。
- 要编辑策略设置（包括策略中使用的证书列表），请点击 **SSL 解密设置** 按钮 (); 请参阅 配置 SSL 解密设置，第 436 页。此外，还可以下载与解密重签名规则一起使用的证书，以便将其分发给客户端。请参阅以下主题：
  - 为已知密钥和重签解密配置证书，第 436 页
  - 为解密重签名规则下载 CA 证书，第 438 页
- 要配置规则，请执行以下操作：
  - 要创建新规则，请点击 + 按钮。请参阅配置 SSL 解密规则，第 430 页。
  - 要编辑现有规则，请点击该规则的编辑图标 ()（在“操作”列中）。也可以选择在表中点击某规则属性来编辑该属性。

- 要删除不再需要的规则，请点击该规则的删除图标 ( )（在“操作”列中）。

- 要移动规则，请编辑规则并从**顺序**下拉列表中选择新位置。
- 如果有任何规则存在问题，例如，因为删除或更改了URL类别而出现问题，请点击搜索框旁边的**查看问题规则**链接，对表格进行过滤，仅显示存在问题的规则。请编辑并更正（或删除）这些规则，以便它们可提供所需的服务。

启用 SSL 解密策略

在可以配置 SSL 解密规则之前，必须启用该策略并配置一些基本设置。以下程序介绍了如何直接启用该策略。此外，还可在启用身份策略时启用该策略。身份策略要求启用 SSL 解密策略。

开始之前

如果从未设置 SSL 解密策略的版本进行升级，但已使用主动身份验证规则配置身份策略，则 SSL 解密策略已启用。确保已选择要使用的解密重签名证书，并且可以选择启用预定义规则。

过程

步骤 1 依次选择**策略** > **SSL 解密**。

步骤 2 点击**启用 SSL 解密 (Enable SSL Decryption)** 配置策略设置。

- 如果是第一次启动该策略，系统将打开“SSL 解密配置”对话框。继续进行后续步骤。
- 如果已对策略进行过一次配置然后禁用了策略，则只需使用之前的设置和规则即可再次启动该策略。可以点击 **SSL 解密设置 (SSL Decryption Settings)** 按钮 ( ) 并按照为已知密钥和重签解密配置证书，第 436 页中所述的方式配置设置。

步骤 3 在**解密重签名证书**中，选择相应内部 CA 证书，以用于利用重签名证书实施解密的规则。

您可以使用预定义的 NGFW-Default-InternalCA 证书，也可以使用您创建或上传的证书。如果尚无证书，请点击**创建内部 CA** 进行创建。

如果尚未在客户端浏览器中安装证书，请点击下载按钮 ( ) 获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅为解密重签名规则下载 CA 证书，第 438 页。

步骤 4 （可选。）点击**受信任 CA 证书**下的 **+**，并选择您希望策略信任的证书或证书组。

默认组 Cisco-Trusted-Authorities 包括所有系统定义的受信任 CA 证书。如果您已上传其他证书，则可以在此处添加这些证书，或者将其收集到您自己的组中并在此处选择该组。您可以替换 Cisco-Trusted-Authorities 组，也可以直接添加组。系统将提示用户接受其列表中未显示证书签名机构的任何站点的证书：系统不会仅仅因为证书不受信任而阻止访问此类站点。

如果将列表留空或仅选择空证书组，则 SSL 解密策略将信任所有证书。

步骤 5 选择初始 SSL 解密规则。

系统包含可能对您有用的下列预定义规则：

- **Sensitive_Data** - 该规则不对与金融服务和医疗URL类别（包括银行、医疗服务等）网站匹配的流量进行解密。必须启用 URL 许可证才能实现该规则。

步骤 6 点击**启用 (Enable)**。

配置默认 SSL 解密操作

如果加密连接没有匹配特定 SSL 解密规则，则由 SSL 解密策略的默认操作来处理。

过程

步骤 1 依次选择**策略** > **SSL 解密**。

步骤 2 点击**默认操作**字段的任意位置。

步骤 3 选择应用于匹配流量的操作。

- **不解密** - 允许加密连接。然后，访问控制策略将评估加密连接，并根据访问控制规则丢弃或允许该连接。
- **阻止** - 立即丢弃连接。连接将不传递到访问控制策略。

步骤 4 （可选。）针对默认操作配置日志记录。

要在控制面板数据或事件查看器中包括匹配默认操作的流量，必须对匹配默认操作的流量启用日志记录。从以下选项中选择：

- **连接结束时** - 在连接结束时生成事件。
  - **将连接事件发送到** - 如果要将事件副本发送至外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**创建新系统日志服务器**，并创建对象。（要对系统日志服务器禁用日志记录，请从服务器列表中选择**任何**）。

    由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

- **无日志记录 (No logging)** - 不生成任何事件。

步骤 5 点击**保存 (Save)**。

配置 SSL 解密规则

使用 SSL 解密规则确定如何处理加密连接。SSL 解密策略中的规则按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件条件的第一个规则。

只可在“SSL 本机规则”部分创建和编辑规则。

注释 在 SSL 解密策略评估连接之前，系统将对 VPN 连接（站点间和远程访问）流量进行解密。因此，SSL 解密规则永远不会应用于 VPN 连接，且在创建这些规则时不需要考虑 VPN 连接。但是，系统会对 VPN 隧道中使用的所有加密连接进行评估。例如，SSL 解密规则将对通过 RA VPN 连接到内部服务器的 HTTPS 连接进行评估，即使 RA VPN 隧道本身没有接受评估（原因在于其已解密）。

开始之前

如要创建解密已知密钥规则，请确保上传目标服务器的证书和密钥（作为内部证书），并编辑 SSL 解密策略设置，以使用该证书。已知密钥规则通常在该规则目标网络条件中指定目标服务器。有关详细信息，请参阅为已知密钥和重签解密配置证书，第 436 页。

过程

步骤 1 依次选择**策略** > **SSL 解密**。

如果未配置任何 SSL 解密规则（不是为主动身份验证的身份规则自动生成的规则），可以点击**添加预定义规则**来添加预定义规则。系统将提示您选择所需的规则。

步骤 2 执行以下任一操作：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

要删除不再需要的规则，请点击该规则的删除图标 ( )。

步骤 3 在**顺序**中，选择要将该规则插入在已排序有序规则列表插入该规则的位置。

只可将规则插入 **SSL 本机规则**部分。身份策略主动身份验证规则将根据身份策略自动生成并且为只读形式。

先匹配的规则先应用，所以您必须确保流量匹配条件条件较具体的规则显示在次之用来匹配流量的较通用条件条件的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

步骤 4 在**名称**中输入规则的名称。

名称不能包含空格。可以使用字母数字字符和以下特殊字符：+ . _ -

步骤 5 选择应用于匹配流量的操作。

有关每个选项的详细讨论，请参阅下列内容：

- 解密重签名，第 422 页
- 解密已知密钥，第 423 页
- 不解密，第 423 页
- 阻止，第 423 页

步骤 6 使用以下选项卡的任意组合，定义流量匹配条件：

- **源/目标** - 流量通过的安全区（接口）、IP 地址或该 IP 地址的国家/地区或大洲（地理位置）或者流量中使用的 TCP 端口。默认设置为任何区域、地址、地理位置和 TCP 端口。请参阅 SSL 解密规则的源/目标条件，第 432 页。
- **应用** - 应用或按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认设置为任何加密应用。请参阅 SSL 解密规则的应用条件，第 433 页。
- **URL** - Web 请求的 URL 类别。默认情况下，进行匹配时不考虑 URL 类别和信誉。请参阅 SSL 解密规则的 URL 条件，第 434 页。
- **用户** - 身份源，用户或用户组。身份策略决定了用户和组的信息是否可用于流量匹配。只有配置身份策略，才能使用此条件条件。请参阅 SSL 解密规则的用户条件，第 434 页。
- **高级** - 从连接中使用的证书派生的特性，例如 SSL/TLS 版本和证书状态。请参阅 SSL 解密规则的高级条件，第 435 页。

要修改条件，请点击该条件内的 + 按钮，选择所需的对象或元素，然后在弹出对话框中点击**确定 (OK)**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象**。点击对象或元素对应的 **x**，可将其从策略中移除。

向 SSL 解密规则中添加条件时，请考虑以下提示：

- 您可以为每个规则配置多个条件。要使规则应用于流量，流量必须匹配该规则中的所有条件。例如，可以使用单一规则来基于 URL 类别对流量进行解密。
- 最多可以为规则中的每个条件添加 50 个标准。匹配某个条件所有条件标准的流量满足该条件。例如，您可以使用单一规则为最多 50 个应用或应用过滤器执行应用控制。因此，单一条件中的项目之间为 OR 关系，但不同条件类型之间（例如，源/目的和应用之间）为 AND 关系。
- 匹配 URL 类别需要 URL 过滤许可证。

步骤 7 （可选。）针对规则配置日志记录。

对于与控制面板或事件查看器中包括的规则匹配的流量，必须为其启用日志记录。从以下选项中选择：

- **连接结束时** - 在连接结束时生成事件。
  - **将连接事件发送到** - 如果要将事件副本发送至外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**创建新系统日志服务器**，并创建对象。（要对系统日志服务器禁用日志记录，请从服务器列表中选择“任何”）。

    由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

- 无日志记录 **(No logging)** - 不生成任何事件。

步骤 8 点击**确定 (OK)**。

SSL 解密规则的源/目标条件

SSL 解密规则的源/目标条件定义了流量通过的安全区（接口）、IP 地址或该 IP 地址所在的国家/地区或大洲（地理位置）或是流量中所用的 TCP 端口。默认设置为任何区域、地址、地理位置、协议和任何 TCP 端口。TCP 是与 SSL 解密规则匹配的唯一协议。

要修改条件，请点击该条件内的 **+** 按钮，选择所需的对象或元素，然后点击**确定**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象**。点击对象或元素对应的 **x**，可将其从策略中移除。

您可以通过以下条件来标识规则中要匹配的源和目标。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至**目标区域**。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至**源区域**。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保从外部主机到内部主机的所有流量均被解密，则应将外部区域选为**源区域**，并将内部区域选为**目标区域**。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置**源网络**。
- 要匹配流向 IP 地址或地理位置的流量，请配置**目标网络**。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络** - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。

注释 对于解密已知密钥规则，请选择使用目标服务器 IP 地址的对象（该对象使用您上传的证书和密钥）。

- **地理位置** - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。

源端口、目标端口/协议

定义流量中所用协议的端口对象。仅可指定用于 SSL 解密规则的 TCP 协议和端口。

- 要匹配来自 TCP 端口的流量，请配置**源端口**。
- 要匹配流向 TCP 端口的流量，请配置**目标端口/协议**。
- 要同时匹配来自特定 TCP 端口的流量和流向特定 TCP 端口的流量，请配置源端口和目标端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

SSL 解密规则的应用条件

SSL 解密规则的应用条件定义 IP 连接中使用的应用，或定义按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认为任何具有 SSL 协议标记的应用。您无法将 SSL 解密规则与任何未加密应用相匹配。

虽然您可以在规则中指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条 SSL 解密规则，用于解密或阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任意一个，系统会解密或阻止会话。

另外，思科会通过系统和漏洞数据库 (VDB) 更新频繁更新和添加其他应用检测器。因此，高风险应用规则可自动应用到新应用中，而无需您手动更新规则。

您可以直接在规则指定应用和过滤器，也可以创建定义这些特征的应用过滤器对象。规格相当，尽管如果要创建复杂规则，使用对象可便于遵守每个条件 50 个项目的系统限制。

要修改应用和过滤器列表，请点击该条件内的 **+** 按钮，选择在单独选项卡中列出的相应应用或应用过滤器对象，然后在弹出对话框中点击**确定**。在任一选项卡中，您可以点击**高级过滤器**选择过滤器条件或帮助您搜索特定应用。点击应用、过滤器或对象的 **x**，可将其从策略中移除。点击**另存为过滤器**链接，可将尚不是对象的组合条件另存为新应用过滤器对象。

有关应用条件以及如何配置高级过滤器和选择应用的更多信息，请参阅配置应用过滤器对象，第 134 页。

在 SSL 解密规则中使用应用条件时，请考虑以下提示。

- 系统可以识别使用 StartTLS 进行加密的未加密应用。这包括诸如 SMTPS、POPS、FTPS、TelnetS 和 IMAPS 之类的应用。此外，系统还可以根据 TLS ClientHello 消息中的服务器名称指示或服务器证书使用者可分辨名称值来识别某些加密应用。
- 仅在服务器证书交换后，系统才可识别使用。如果在 SSL 握手期间交换的流量与包含应用条件的 SSL 规则中的所有其他条件相匹配，但是识别未完成，则 SSL 策略允许数据包通过。此行为允许完成握手，以便可以识别应用。在系统完成其识别后，系统将 SSL 规则操作应用于与其应用条件相匹配的剩余会话流量。

- 如果所选应用已由VDB更新删除，则会在应用名称后显示“（已弃用）”。必须从过滤器中删除这些应用，否则将阻止后续部署和系统软件升级。

SSL 解密规则的 URL 条件

SSL 解密规则的 URL 条件定义了 Web 请求中的 URL 所属的类别。还可以指定要解密、阻止或允许不解密的站点的相对信誉。默认不基于 URL 类别匹配连接。

例如，您可以阻止所有加密的赌博网站，或解密不受信任社交网站。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止或解密。有关 URL 类别匹配的详细信息，请参阅按照类别和信誉过滤 URL，第 468 页。

“类别”选项卡

点击 **+**，选择所需的类别，然后点击**确定**。点击类别或对象的 **x**，可将其从策略中删除。

默认为将规则应用于每个选定类别的所有 URL，不考虑信誉。要根据信誉限制规则，请点击每个类别的向下箭头，取消选中**任何**复选框，然后使用**信誉**滑块选择信誉级别。信誉滑块的左侧指明待允许而不解密的站点，右侧是要解密或阻止的站点。如何使用信誉取决于规则操作：

- 如果该规则解密或阻止连接，则选择某个信誉级别也会选择高于该级别的所有信誉。例如，如果配置规则以解密或阻止**问题站点**（第 2 级），系统还会自动解密或阻止**不受信任**（第 1 级）站点。
- 如果规则允许连接而不解密（不解密），则选择某个信誉级别也会选择低于该级别的所有信誉。例如，如果配置规则不解密**可靠站点**（第4级），该规则还会自动不解密**受信任**（第 5 级）站点。

选择**包含信誉未知的站点**选项，可使具有未知信誉的URL包括在信誉匹配项中。新站点通常未评级，并且站点的信誉可能会由于其他原因而未知或无法确定。

检查 URL 的类别

您可以检查特定 URL 的类别和信誉。在**待检查的 URL** 框中输入 URL，然后点击**前往**。系统会将您转至外部网站以查看结果。如果您对分类持有不同意见，请点击**提交 URL 类别争议**链接，将您的想法反馈给我们。

SSL 解密规则的用户条件

SSL 解密规则的“用户”条件对 IP 连接的用户或用户组进行了定义。只有配置身份策略和相关联的目录服务器，才能在规则中包括用户或用户组条件。

您的身份策略决定是否收集某个特定连接的用户身份。如果建立了身份，则主机的 IP 地址与所识别的用户相关联。因此，源 IP 地址映射到用户的流量将被视为来自该用户。IP 数据包本身不包含用户身份信息，所以此 IP 地址到用户的映射是最接近的近似值。

由于最多可以向规则中添加50个用户或组，所以选择组比选择单个用户通常更有意义。例如，您可以创建规则，对从外部网络发往工程组的流量进行解密，并单独创建一个不会对从该组传出的流量进行解密的规则。然后，要将该规则应用于新工程师，您只需添加将工程师添加到目录服务器的“工程”组即可。

您还可以选择身份源，以应用于该源中的所有用户。因此，如果您支持多个 Active Directory 域，您可以根据域提供不同的解密处理。

要修改用户列表，请点击该条件内的 + 按钮，并使用以下任一方法选择所需的用户或用户组。点击用户或组对应的 **x**，或将其从策略中移除。

- **身份源** - 选择身份源，例如 AD 领域或本地用户数据库，以将规则应用于从所选源获取的所有用户。如果所需的领域尚不存在，请点击**创建新身份领域**并立即创建。
- **组** - 选择所需的用户组。只有在目录服务器中配置了组，才能使用组。如果您选择了某个组，规则将应用于该组的所有成员，包括子组。如果要区别对待某个子组，您需要针对该子组创建一条单独的访问规则，并将其置于访问控制策略中适用于父组的规则之上。
- **用户** - 选择单个用户。用户名使用身份源作为前缀，例如“领域\用户名”。

  特殊身份领域中存在一些内置用户：

  - **身份验证失败** - 系统提示用户进行身份验证，但用户未在允许的最大尝试次数内输入有效的用户名/密码对。身份验证失败本身不会阻止用户访问网络，但您可以写入访问规则来限制这些用户访问网络。
  - **访客** - “访客”用户与“身份验证失败”用户类似，只是您的身份规则配置为将这些用户称为“访客”。系统提示“访客”用户进行身份验证，但他们在最大尝试次数内未成功通过身份验证。
  - **无需身份验证** - 系统不提示用户进行身份验证，因为该类用户的连接与指定不进行身份验证的身份规则匹配。
  - **未知** - 没有用户的 IP 地址映射，也没有身份验证失败的记录。通常，这意味着尚无来自该地址的 HTTP 流量。

SSL 解密规则的高级条件

高级流量匹配条件与根据连接中使用的证书派生的属性有关。您可以配置以下任何或全部选项。

证书属性

如果流量与任何选定属性匹配，则它与相应规则的证书属性选项匹配。您可以配置以下内容：

证书状态

证书**无效**还是**有效**。如果您不关心证书状态，请选择**任意**（默认）。

如果满足以下所有条件，证书即视为有效，否则视为无效：

- 策略信任颁发证书的 CA。
- 可根据证书的内容对证书的签名进行适当的验证。
- 颁发者 CA 证书存储在策略的受信任 CA 证书列表中。
- 策略的受信任 CA 未撤销证书
- 当前日期介于证书的有效期开始日期和有效期结束日期之间。

自签名

服务器证书是否包含相同的使用者和颁发者可分辨名称。选择以下一个选项：

- **自签名** - 服务器证书自签名。
- **CA 签名** - 服务器证书由证书颁发机构签名。也就是说，颁发者和使用者不同。
- **任意** - 不考虑按照匹配条件，证书是否为自签名。

支持的版本

要匹配的 SSL/TLS 版本。该规则适用于仅使用任何选定版本的流量。默认设置是所有版本。选项包括： **SSL 3.0**、 **TLS 1.0**、 **TLS 1.1**、 **TLS 1.2**、 **TLS 1.3**。

例如，如果仅希望允许 TLSv1.2/3 连接，则可创建用于更低版本的阻止规则。

您必须使用 Snort 3 才能匹配 TLS 1.3 连接。

使用任何未列出版本（例如 SSL v2.0）的流量均由 SSL 解密策略的默认操作处理。

配置 SSL 解密设置

如果您有任何解密流量的规则，则必须配置证书设置。您还可以修改设置，以更改将解密应用于加密流量的方式。下面的主题介绍了几个选项。

为已知密钥和重签解密配置证书

如果通过重签或使用已知密钥实施解密，则需要确定 SSL 解密规则可以使用的证书。确保所有证书均有效且未过期。

特别是对于已知密钥的解密，需要确保系统拥有要解密连接的各目标服务器的当前证书和密钥。通过解密已知密钥规则，可以使用目标服务器的实际证书和密钥进行解密。因此，必须确保 威胁防御设备始终拥有当前证书和密钥，否则将无法成功解密。

只要在已知密钥规则中更改目标服务器上的证书或密钥，就要上传新的内部证书和密钥。将上述证书作为内部证书（而不是内部 CA 证书）上传。可以在下列程序中上传证书，也可以转到**对象 (Objects)** > **证书 (Certificates)**页面并在此页面中上传。

过程

步骤 1 依次选择**策略** > **SSL 解密**。

步骤 2 点击 **SSL 解密设置**按钮 ( )。

如有必要，请选择 **基本** 选项卡。

步骤 3 在**解密重签名证书**中，选择相应内部 CA 证书，以用于利用重签名证书实施解密的规则。

您可以使用预定义的 NGFW-Default-InternalCA 证书，也可以使用您创建或上传的证书。如果尚无证书，请点击**创建内部 CA** 进行创建。

如果尚未在客户端浏览器中安装证书，请点击下载按钮 ( ) 获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅为解密重签名规则下载 CA 证书，第 438 页。

步骤 4 对于使用已知密钥解密的每条规则，上传目标服务器的内部证书和密钥。

a) 点击**解密已知密钥证书**下的 +。

b) 选择内部身份证书，或点击**创建新的内部证书**以便立即上传。

c) 点击**确定 (OK)**。

步骤 5 （可选。）点击**受信任 CA 证书**下的 **+**，并选择您希望策略信任的证书或证书组。

默认组 Cisco-Trusted-Authorities 包括所有系统定义的受信任 CA 证书。以下是您可能希望更改此设置的主要情况：

- 您希望使用不在默认组中的受信任 CA 证书。然后，您可以在 SSL 解密策略设置中选择默认组和新组。如果您已上传其他受信任 CA 证书，可以执行此操作。
- 您希望使用的受信任 CA 证书列表比默认组中限制更严格。然后，您将创建一个具有受信任证书的完整列表（而不只是您所增加的受信任证书）的组，并将其选择为 SSL 解密策略设置中的唯一组。

系统将提示用户接受其列表中未显示证书签名机构的任何站点的证书：系统不会仅仅因为证书不受信任而阻止访问此类站点。

如果将列表留空或仅选择空证书组，则 SSL 解密策略将信任所有证书。

步骤 6 点击**保存 (Save)**。

配置高级和无法解密的流量设置

如果不想使用默认行为，可以配置高级解密设置和无法解密的流量的设置。

过程

步骤 1 选择 **策略 > SSL 解密**。

步骤 2 点击 **SSL 解密设置**按钮 ( )。

步骤 3 在 **高级** 选项卡上，选择是否启用 **TLS 1.3 解密**。

如果启用 TLS 1.3 解密，则还必须在应用于 TLS 1.3 的每个规则的高级选项卡上选择 TLS 1.3 选项。您必须运行 Snort 3 才能解密 TLS 1.3。

步骤 4 在**无法解密的操作**选项卡上，修改系统处理与实施解密的规则匹配的连接的方式，但对于连接无法解密的情况。

默认设置是对这些连接应用与默认操作相同的操作。例外情况是解密错误，您可以选择阻止或仅阻止并重置。

有关这些类别的说明，请参阅处理不可解密流量，第 424 页。

步骤 5 点击**确定 (OK)**。

为解密重签名规则下载 CA 证书

如果决定对流量进行解密，则用户必须拥有加密流程中使用的内部CA证书，该证书由使用TLS/SSL的应用中被定义为受信任根证书颁发机构所颁发。通常，当生成证书或即使导入证书后，证书不会立即在这些应用中定义为受信任。默认情况下，在大多数网络浏览器中，当用户发送 HTTPS 请求时，他们将看到一条来自客户端应用的警告消息，告知他们网站的安全证书有问题。通常，错误消息表明网站的安全证书并非由受信任证书颁发机构所颁发或网站由未知机构所认证，但该警告可能还表明可能存在中间人攻击。一些其他客户端应用不会向用户显示此警告消息，也不允许用户接受无法识别的证书。

可以通过以下方式为用户提供所需的证书：

通知用户接受根证书

可以通知您组织中的用户，告知其公司的新策略并指示其接受组织提供的根证书作为受信任来源。用户应接受该证书并将其保存在受信任根证书颁发机构存储区，以确保在下次访问该站点时系统不会再次提示。

注释 用户需要接受并信任创建替换证书的 CA 证书。如果仅信任替换服务器证书，用户访问各个不同 HTTPS 站点时将继续看到警告。

将根证书添加到客户端设备

能够以受信任根证书颁发机构身份将根证书添加到网络上的所有客户端设备。这样，客户端应用将自动接受包含根证书的事务。

可以通过以下方式向用户提供证书：通过邮件发送或将其放在共享站点上，将证书整合到企业工作站映像中并使用应用更新工具将其自动分发给用户。

以下程序介绍了如何下载内部 CA 证书并将其安装在 Windows 客户端上。

过程

步骤 1 从 设备管理器下载证书。

a) 选择 **策略** > **SSL 解密**。

b) 点击 **SSL 解密设置**按钮 ( )。

c) 点击**下载**按钮 ( )。

d) 选择一个下载位置，或者更改文件名（但是不要更改扩展名），然后点击**保存 (Save)**。

此时可以取消“SSL 解密设置”对话框。

步骤 2 在客户端系统上，在网络浏览器的受信任根证书颁发机构存储区安装证书，或向客户端提供证书，以便用户自行安装。

该流程因操作系统和浏览器类型的不同而不同。例如，对于 Windows 上运行的 Internet Explorer 和 Chrome 浏览器，可以采用以下流程。（对于 Firefox，请依次选择**工具 (Tools)** > **选项 (Options)** > **高级 (Advanced)** 页面，进行安装。）

a) 从**开始**菜单中，依次选择**控制面板** > **Internet 选项**。
b) 选择**内容**选项卡。
c) 点击**证书**按钮，打开“证书”对话框。
d) 选择**受信任根证书颁发机构**选项卡。
e) 点击**导入**，然后根据向导找到并选择下载的文件 (<uuid>_internalCA.crt) 并将其添加到受信任根证书颁发机构存储区。
f) 点击**完成**。

系统应显示消息，指示已成功导入。您可能会看到一个中间对话框，警告：如果生成自签名证书而不是从知名第三方证书颁发机构获取证书，则 Windows 无法验证该证书。

此时，可以关闭“证书”和“Internet 选项”对话框。

示例：从网络阻止较旧的 SSL/TLS 版本

某些组织需要通过政府法规或公司策略来阻止使用较旧版本的 SSL 或 TLS。可以使用 SSL 解密策略来阻止使用您禁止的 SSL/TLS 版本的流量。请考虑将此规则置于 SSL 解密策略的顶部，以确保立即捕获禁止的流量。

以下示例阻止所有 SSL 3.0 和 TLS 1.0 连接。

开始之前

此过程假定已启用 SSL 解密策略，如启用 SSL 解密策略，第 428 页中所述。

过程

步骤 1 依次选择**策略** > **SSL 解密**。

步骤 2 点击 **+** 按钮创建新规则。

步骤 3 按顺序选择 **1** 将规则置于策略的顶部，或选择最适合您网络的数字。

默认情况下，会将该规则添加到策略的末尾。

步骤 4 在**标题**中，输入规则名称，例如，Block_SSL3.0_and_TLS1.0。

步骤 5 在**操作**中，选择**阻止**。这将立即丢弃与该规则匹配的任何流量。

步骤 6 保留以下选项卡上所有选项的默认值：**源/目标**、**应用**、 **URL** 和 **用户**。

步骤 7 点击 **高级** 选项卡，并在 **受支持版本**下，选择 SSL 3.0 和 TLS 1.0，但取消选中 TLS1.1、TLS1.2、TLS 1.3。

步骤 8 （可选）如果希望控制面板和事件反映阻止连接，请点击**日志记录**选项卡并选择**在连接结束时**。如果正在使用外部系统日志服务器，还可以选择该服务器。

步骤 9 点击**确定**。

您现在可以部署策略。部署后，通过系统的任何 SSL 3.0 或 TLS 1.0 连接均将弃用。

注释 SSL 2.0 连接由策略的默认操作处理。如果要确保已弃用这些，请将默认操作更改为阻止。

下一步做什么

如果实施此规则，我们具有以下建议：

- 对于任何类型的解密规则，请包括“高级”选项卡的默认设置，其中，所有 SSL/TLS 选项均已选中。通过应用至所有版本，可以简化握手过程。但是，您的初始阻止规则仍将阻止 SSL 3.0 和 TLS 1.0 连接。
- 通常建议使用“不解密”作为策略的默认操作。但是，由于SSL 2.0连接始终由默认操作处理，因此您可能希望改用“阻止”。但是，如果要将“不解密”应用为所有可解密流量的默认操作，请在策略末尾创建“不解密”规则，其中，您接受所有流量匹配条件的默认值。此规则将匹配与表中的较早规则不匹配的任何受支持 TLS 连接，并作为这些 TLS 版本的默认值。

SSL 解密监控和故障排除

以下主题介绍如何对 SSL 解密策略进行监控和故障排除。

监控 SSL 解密

您可以在控制面板和事件中查看有关匹配日志记录已启用的规则（或默认操作）的流量解密信息。

SSL 解密控制面板

要评估整体解密统计信息，请查看**监控** > **SSL 解密**控制面板。控制面板显示以下信息：

- 加密流量与纯文本流量百分比。
- 按照 SSL 规则的流量解密百分比。

事件

除了控制面板，事件查看器（**监控** > **事件**）包括加密流量 SSL 信息。以下是评估事件的一些提示：

- 对于因匹配阻止匹配流量的 SSL 规则（或默认操作）而被丢弃的连接，**操作**应为“阻止”，**原因**应指示“SSL 阻止”。

- **SSL 实际操作**字段指示系统应用于连接的实际操作。这可能与 **SSL 预期操作**有所不同，SSL 预期操作指示在匹配规则上定义的操作。例如，连接可能与应用解密的规则匹配，但出于某些原因不能被解密。

处理解密重签名适用于浏览器而非应用的 Web 站点（SSL 或证书颁发机构锁定）

智能手机和其他设备的某些应用使用 SSL（或证书颁发机构）锁定技术。SSL 锁定技术将原始服务器证书的散列值嵌入到应用本身内部。因此，当应用收到来自 威胁防御设备的重签名证书时，散列验证会失败并中止连接。

主要表现是，用户使用站点应用无法连接到网站，但可以使用网络浏览器连接，即使在应用无法正常工作的同一台设备上使用浏览器也可以连接。例如，用户不能使用 Facebook iOS 或 Android 应用，但可以通过 https://www.Facebook.com 转至 Safari 或 Chrome，进行成功连接。

由于 SSL 锁定专用于避免中间人攻击，因此此问题无法解决。必须从以下选项中选择一项：

- 支持应用用户，在这种情况下无法解密流向网站的任何流量。为站点应用创建“Do Not Decrypt”规则（在 SSL 解密规则的“应用”选项卡上），并确保该规则排在应用于连接的任何解密重签名规则前面。
- 强制用户只使用浏览器。如果必须解密流向网站的流量，需要向用户说明，通过您的网络连接时，他们无法使用站点应用，只能使用浏览器。

更多详细信息

如果站点在浏览器中可用，但不能在同一设备的应用中使用，几乎可以肯定这是一个 SSL 锁定实例。但是，如果您想要更深入地挖掘，除了浏览器测试之外，还可以使用连接事件确定 SSL 锁定。

应用可能会通过两种方式处理散列验证失败：

- 第 1 组应用，例如 Facebook，从服务器收到 SH、CERT、SHD 消息后立即发送 SSL 警告消息。警告通常是一个表示 SSL 锁定的“Unknown CA (48)”警告。紧接着警告消息发送 TCP 重置。在事件详细信息中，您应看到以下现象：
  - SSL 流标志包括 ALERT_SEEN。
  - SSL 流标志不包括 APP_DATA_C2S 或 APP_DATA_S2C。
  - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE。
- 第 2 组应用，例如 Dropbox，不会发送任何警告。而是，等到完成握手后发送 TCP 重置。在事件中，您应看到以下现象：
  - SSL 流标志不包括 ALERT_SEEN、APP_DATA_C2S 或 APP_DATA_S2C。
  - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、

CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、
SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED。

第 19 章

身份策略

您可以使用身份策略从连接中收集用户身份信息。然后，可以在控制面板中基于用户身份查看使用情况，并根据用户或用户组配置访问控制。

身份策略概述

您可以使用身份策略检测与连接关联的用户。通过识别用户身份，可以将威胁、终端和网络智能与用户身份信息关联。通过将网络行为、流量和事件直接与单个用户相关联，系统可帮助您确定策略违规、攻击或网络漏洞的来源。

例如，可以确定入侵事件所攻击的主机的所有人是谁，并确定是谁发起了内部攻击或端口扫描。此外，还可以确定高带宽用户，以及正在访问不良网站或应用的用户。

用户检测不仅仅是收集数据进行分析，您也可以基于用户名或用户组名编写访问规则，根据用户身份选择性允许或阻止到资源的访问。

可以使用以下方法获取用户身份：

- 被动身份验证 - 对所有类型的连接，从其他身份验证服务获取用户身份而不提示输入用户名和密码。
- 主动身份验证 - 提示输入用户名和密码，并根据指定身份源进行身份验证，获取源 IP 地址的用户身份（仅限于 HTTP 连接）。

以下主题提供了有关用户身份的详细信息。

通过被动身份验证确定用户身份

被动身份验证在收集用户身份信息时不提示用户输入用户名和密码。系统会从您指定的身份源获取映射。

您可以从以下源被动获取用户到 IP 地址的映射：

- 远程访问 VPN 登录。被动身份支持以下用户类型：
  - 在外部验证服务器中定义的用户账户。
  - 在 设备管理器中定义的本地用户账户。
- 思科身份服务引擎 (ISE)；思科身份服务引擎被动身份连接器 (ISE-PIC)。

如果给定用户是通过多个源所识别，则 RA VPN 身份占优先地位。

通过主动身份验证确定用户身份

身份验证是确认用户身份的行为。

如果 HTTP 流量来自系统没有其用户身份映射的 IP 地址，通过主动身份验证，您可以决定是否针对为系统配置的目录对发起该流量的用户进行身份验证。如果身份验证成功，该 IP 地址则被视为具有该通过身份验证的用户的身份。

如身份验证不成功，用户对网络的访问并不会受阻。为这些用户提供哪些访问权限最终由访问规则决定。

处理未知用户

当您为身份策略配置目录服务器后，系统会从目录服务器下载用户和组成员信息。此信息每24小时在午夜刷新一次，或在每次您编辑和保存目录配置时刷新（即使您未进行任何更改）。

如果某用户在活动身份验证身份规则提示时成功进行了身份验证，但该用户的名称不在下载的用户身份信息中，则该用户会被标记为“未知”。您不会在与身份相关的控制面板中看到该用户的ID，该用户也不会匹配组规则。

但是，系统将应用面向未知用户的任何访问控制规则。例如，如果您阻止未知用户的连接，那么即使这些用户成功进行了身份验证（即目录服务器可识别用户并且密码有效），他们也会被阻止。

因此，当您对目录服务器进行更改（例如添加或删除用户，或更改组成员身份）时，直到系统从目录下载更新之后这些更改才会反映在策略实施中。

如果您不希望每天都等到午夜进行更新，可以通过编辑目录领域信息（依次选择**对象** > **身份源**，然后编辑领域）强制进行更新。点击**保存**，然后部署更改。系统随即会下载更新。

注释 您可以依次转至**策略** > **访问控制**，点击**添加规则 (+)** 按钮，并在**用户**选项卡上查看用户列表，从而检查系统上是否有新的或已删除的用户信息。如果找不到新用户，或者还是可以找到已删除的用户，则系统的信息未更新。

如何实施身份策略

要启用用户身份采集，以便得知与 IP 地址关联的用户，您需要配置多个项目。正确配置后，您将能够看到监控控制面板和事件中的用户名。您还将能够在访问控制和 SSL 解密规则中使用用户身份作为流量匹配条件。

以下过程概述您必须配置哪些内容才能正常使用身份策略。

过程

步骤 1 配置 AD 身份领域。

不论您是主动（提示进行用户验证）使用用户身份，还是被动使用，都需要配置包含用户身份信息的 Active Directory (AD) 服务器。请参阅配置 AD 身份领域，第 155 页。

如果配置被动身份，则可以创建 AD 领域序列，使系统可以提取多个 AD 领域中的身份。如果您的网络中有多个 AD 域，此方法将非常有用。

步骤 2 如果您想要使用被动身份验证身份规则，请配置被动身份源。

根据您要在设备中实现的服务和网络中可用的服务，您可以配置任何以下内容。

- 远程访问 VPN - 如果您要支持到设备的远程访问 VPN 连接，用户登录可以提供基于 AD 服务器或本地用户（ 设备管理器中定义的用户）的身份。有关配置远程访问 VPN 的信息，请参阅配置远程访问 VPN，第 662 页。
- 思科身份服务引擎 (ISE) 或思科身份服务引擎被动身份连接器 (ISE PIC) - 如果您使用这些产品，您可以将设备配置为 pxGrid 订阅方，并从 ISE 获取用户身份。请参阅配置身份服务引擎，第 163 页。

步骤 3 依次选择**策略** > **身份**，并启用身份策略。请参阅配置身份策略，第 447 页。

步骤 4 配置身份策略设置，第 447 页。

基于您在系统中配置的源，自动选择被动身份源。如果您想要配置主动身份验证，您必须为强制网络门户和 SSL 重签解密（如果尚未启用 SSL 解密策略）配置证书。

步骤 5 配置身份策略默认操作，第 449 页。

如果您打算仅使用被动身份验证，您可以将默认操作设置为被动身份验证，无需创建特定规则。

步骤 6 配置身份规则，第 449 页。

创建将从相关网络收集被动或主动用户身份的规则。

主动身份验证最佳实践

如果身份规则要求对用户进行主动身份验证，则该用户将重定向到连接该用户所通过的界面上的强制网络门户，然后系统会提示用户进行身份验证。

由于此重定向指向接口 IP 地址，因此身份策略证书不完全匹配，并且用户会收到不受信任的证书错误。用户必须接受证书才能继续操作并对设备进行身份验证。由于这种行为类似于中间人攻击，用户不愿意接受不受信任的证书。

为避免此问题，您可以将主动身份验证配置为使用设备上一个接口的完全限定域名 (FQDN)。使用正确配置的证书时，用户不会收到不受信任的证书错误，并且身份验证将更加无缝，且看起来更加安全。

开始之前

主动身份验证仅适用于 HTTP 流量，只要设备没有用户工作站或其他客户端设备的当前用户映射，就会对最终用户造成中断。您可以通过实施被动身份验证来避免中断。

过程

步骤 1 在 DNS 服务器中，为要用于收集主动身份验证的接口的接口 IP 地址定义完全限定域名 (FQDN)。

也称为强制网络门户，这必须是路由接口。

步骤 2 使用证书颁发机构 (CA)，获取此 FQDN 的证书。

您可以为特定的 FQDN 创建证书，例如 ftd1.captive-port.example.com。或者，您可以：

- 获取可应用于许多不同设备上的强制网络门户接口的通配符证书，例如 *.captive-port.example.com。通配符也可以更广泛，适用于各种终端，例如 *.eng.example.com，甚至是 *.example.com。
- 在证书中包含多个使用者备选名称 (SAN)。

步骤 3 选择**对象** > **证书**，并上传证书。

步骤 4 选择**对象** > **网络**，并为 DNS 名称创建 FQDN 网络对象。

步骤 5 在**策略 (Policies)** > **身份 (Identity)** 页面上，使用证书和 FQDN 对象更新身份策略设置。

步骤 6 在身份策略中创建使用主动身份验证的规则。

配置身份策略

您可以使用身份策略从连接中收集用户身份信息。然后，可以在控制面板中基于用户身份查看使用情况，并根据用户或用户组配置访问控制。

下文概述了如何配置通过身份策略获取用户身份所需的元素。

过程

步骤 1 依次选择**策略** > **身份**。

如果尚未定义身份策略，请点击**启用身份策略**并按配置身份策略设置，第447页中的说明配置设置。

步骤 2 管理身份策略。

在配置身份设置后，此页面将按顺序列出所有规则。规则依据流量按照从上到下的顺序进行匹配，由第一个匹配项确定要应用的操作。从此页面中可以执行以下操作：

- 要启用或禁用身份策略，请点击**身份策略**开关。
- 要更改身份策略设置，请点击**身份策略配置**按钮（  ）。
- 要更改**默认操作**，请点击操作并选择所需的操作。请参阅配置身份策略默认操作，第 449 页。
- 要移动规则，请编辑规则并从**顺序**下拉列表中选择新位置。
- 要配置规则，请执行以下操作：
  - 要创建新规则，请点击 + 按钮。
  - 要编辑现有规则，请点击该规则的编辑图标 ()（在“操作”列中）。也可以选择在表中点击某规则属性来编辑该属性。
  - 要删除不再需要的规则，请点击该规则的删除图标 ()（在“操作”列中）。

有关创建和编辑身份策略的更多信息，请参阅配置身份规则，第 449 页。

配置身份策略设置

要正常使用身份策略，必须配置提供用户身份信息的源。必须配置的设置因配置的规则类型而异，而规则类型可以是被动和/或主动的。

这些设置显示在设置对话框的不同部分。您可以看到两个部分，也可以看到一个部分，具体取决于如何访问对话框。如果您尝试创建身份验证类型的规则，而没有事先配置所需的设置，系统将自动显示对话框。

以下过程介绍完整对话框。

开始之前

确保目录服务器、威胁防御设备和客户端之间的时间设置一致。这些设备间的时间偏差可能会导致用户身份验证操作失败。“一致”说明您可以使用不同的时区，但时间相对于这些时区应是相同的；例如，10 AM PST = 1 PM EST。

过程

步骤 1 依次选择**策略** > **身份**。

步骤 2 点击**身份策略配置**按钮（  ）。

步骤 3 配置**被动身份验证**选项。

对话框显示已经配置的被动身份验证源。

如有必要，您可以通过此对话框配置 ISE。如果您尚未配置 ISE 对象，可以点击**集成 ISE** 链接，立即创建对象。如果对象存在，将显示对象及其状态（已启用或已禁用）。

必须配置至少一个已启用被动身份源，才能创建被动身份验证规则。

步骤 4 配置**主动身份验证**选项。

如果身份规则要求对用户进行主动身份验证，则该用户将被重定向到强制网络门户端口，然后系统会提示他们进行身份验证。在配置这些设置之前，请阅读主动身份验证最佳实践，第 446 页。

- **服务器证书** - 选择在主动身份验证期间提供给用户的内部证书。如果尚未创建所需的证书，请点击下拉列表底部的**创建新的内部证书**。

  如果用户不上传其浏览器已经信任的证书，则必须接受该证书。

- **重定向到主机名**（仅限 Snort 3.0）- 选择定义接口的完全限定主机名的网络对象，该接口应用作主动身份验证请求的强制网络门户。如果该对象尚不存在，请点击**创建新网络**。

  FQDN 必须解析为设备上接口之一的 IP 地址。通过使用 FQDN，您可以为客户端将识别的主动身份验证分配证书，从而避免用户在被重定向到 IP 地址时收到不受信任证书警告。证书可以在证书的使用者备选名称 (SAN) 中指定 FQDN、通配符 FQDN 或多个 FQDN。

  如果身份规则要求对用户进行主动身份验证，但您未指定重定向 FQDN，则用户将被重定向到他们连接的接口上的强制网络门户端口。

- **端口** - 强制网络门户端口。默认端口是 885 (TCP)。如果配置了其他端口，则该端口必须在 1025-65535 的范围内。

  注释 如果您不提供**重定向到主机名** FQDN，HTTP Basic、HTTP 响应页面和 NTLM 身份验证方法会使用接口的 IP 地址将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 *firewall-hostname.AD-domain-name* 进行重定向。如果您想在不提供**重定向到主机名** FQDN 的情况下使用 HTTP 协商，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。建议您始终提供**重定向到主机名** FQDN 以确保行为一致，而无论采用哪种身份验证方法。

步骤 5 （仅主动身份验证。）在**解密重签名证书**中，选择相应内部 CA 证书，以用于利用重签名证书实施解密的规则。

您可以使用预定义的 NGFW-Default-InternalCA 证书，也可以使用您创建或上传的证书。如果尚无证书，请点击**创建内部 CA** 进行创建。

如果尚未在客户端浏览器中安装证书，请点击下载按钮 ( ) 获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅为解密重签名规则下载 CA 证书，第 438 页。

注释 只有在未配置 SSL 解密策略的情况下，系统才会提示您进行 SSL 解密设置。要在启用身份策略之后更改这些设置，请编辑 SSL 解密策略设置。

步骤 6 点击**保存 (Save)**。

配置身份策略默认操作

身份策略对不匹配任何身份规则的连接实施默认操作。

实际上，不设置规则是策略的有效配置。如果想在所有流量源上使用被动身份验证，只需将被动身份验证配置为默认操作。

过程

步骤 1 依次选择**策略** > **身份**。

步骤 2 点击**默认操作**，并从以下选项中选择一个：

- **被动身份验证（任何身份源）**-通过对不匹配任何身份规则的连接使用所有配置的被动身份源，确定用户身份。如果不配置任何被动身份源，使用被动身份验证作为默认选择等同于使用“无身份验证”。
- **无身份验证（不需要身份验证）**- 不对不匹配任何身份规则的连接确定用户身份。

配置身份规则

身份规则确定是否应收集用户身份信息以匹配流量。如果您不想获取用户身份信息以匹配流量，则可以配置“无身份验证”。

请记住，无论规则配置如何，都仅对 HTTP 流量进行主动身份验证。因此，无需创建规则将非 HTTP 流量从主动身份验证中排除。如果您希望获取所有 HTTP 流量的用户身份信息，只需将主动身份验证规则应用于所有源和目的。

注释 而且请记住，身份验证失败对网络访问没有影响。身份策略仅收集用户身份信息。如果要阻止无法进行身份验证的用户访问网络，则必须使用访问规则。

开始之前

规则自上而下进行评估。对于与给定规则的指定网络条件匹配的连接，系统将根据规则中指定的身份领域对用户进行评估。如果用户不属于该领域，他们将被标记为未知，并且不会评估身份策略中的其他规则。因此，如果有多个领域需要评估，请务必使用领域序列而不是单个领域。

过程

步骤 1 依次选择**策略** > **身份**。

步骤 2 执行以下任一操作：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

要删除不再需要的规则，请点击该规则的删除图标 ( )。

步骤 3 在**顺序**中，选择要将该规则插入在已排序有序规则列表插入该规则的位置。

先匹配的规则先应用，所以您必须确保流量匹配条件条件较具体的规则显示在次之用来匹配流量的较通用条件条件的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

步骤 4 在**名称**中输入规则的名称。

步骤 5 选择**操作**，如有必要，还要选择 **AD 身份源**。

您必须选择包括用于被动和主动身份验证规则的用户账户的 AD 身份领域。如果所需的领域尚不存在，请点击**创建新身份领域 (Create New Identity Realm)** 并立即创建。对于被动身份验证，您可以选择 AD 领域序列，而不是单个 AD 领域对象。

- **被动身份验证** - 使用被动身份验证确定用户身份。系统将会显示所有已配置的身份源。此规则会自动使用所有已配置的源。
- **主动身份验证** - 使用主动身份验证确定用户身份。主动身份验证仅适用于 HTTP 流量。如果任何其他类型的流量与要求或允许主动身份验证的身份策略匹配，则不会尝试进行主动身份验证。
- **无身份验证** - 不获取用户身份。基于身份的访问规则不会应用于此流量。这些用户将标记为**无需身份验证**。

步骤 6 （仅主动身份验证。）选择您的目录服务器支持的身份验证方法（**类型**）。

- **HTTP 基本身份验证** - 使用未加密的 HTTP 基本身份验证 (BA) 连接对用户进行身份验证。用户通过其浏览器的默认身份验证弹出窗口登录网络。这是默认值。
- **NTLM** - 使用 NT LAN Manager (NTLM) 连接对用户进行身份验证。仅当选择了一个 AD 领域时，此选项才可用。用户使用其浏览器的默认身份验证弹出窗口登录网络，不过您可以将 IE 和

Firefox 浏览器配置为使用其 Windows 登录域信息以透明方式进行身份验证（请参阅启用透明用户身份验证，第 452 页）。

- **HTTP 协商** - 允许设备协商用于用户代理（用户发起流量流所用的应用）和 Active Directory 服务器之间的方法。协商有助于使用广受支持的最强方法，顺序为先 NTLM，然后是 Basic 方法。用户通过其浏览器的默认身份验证弹出窗口登录网络。
- **HTTP 响应页面** - 提示用户使用系统提供的网页进行身份验证。这是一种 HTTP Basic 身份验证方法。

注释 如果您不提供**重定向到主机名** FQDN，HTTP Basic、HTTP 响应页面和 NTLM 身份验证方法会使用接口的 IP 地址将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 *firewall-hostname.AD-domain-name* 进行重定向。如果您想在不提供**重定向到主机名** FQDN 的情况下使用 HTTP 协商，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。建议您始终提供**重定向到主机名** FQDN 以确保行为一致，而无论采用哪种身份验证方法。

步骤 7 （仅主动身份验证。）依次选择**以访客身份回退** > **开/关**，确定是否将未通过主动身份验证的用户标记为访客用户。

用户有三次机会成功进行身份验证。如果仍不成功，选择此选项可以确定是否标记用户。您可以根据这些值编写访问规则。

- **以访客身份回退** > **开** - 系统将用户标记为**访客**。
- **以访客身份回退** > **关** - 系统将用户标记为**未通过身份验证**。

步骤 8 在**源/目标**选项卡上定义流量匹配条件。

请记住，仅在使用 HTTP 流量时才会尝试进行主动身份验证。因此，无需为非 HTTP 流量配置无身份验证规则，也无需为任何非 HTTP 流量创建主动身份验证规则。但是，被动身份验证适用于任何类型的流量。

身份规则的源/目标条件定义了流量通过的安全区（接口）、IP 地址或该 IP 地址所在的国家/地区或大洲（地理位置）或是流量中所用的协议和端口。默认设置为任何区域、地址、地理位置、协议和端口。

要修改条件，请点击该条件内的 + 按钮，选择所需的对象或元素，然后在弹出对话框中点击**确定 (OK)**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象**。点击对象或元素对应的 **x**，可将其从策略中移除。

可以配置以下流量匹配条件。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至**目标区域**。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至**源区域**。

- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保从源自内部网络的所有流量收集用户身份，请选择内部区域作为**源区域**，同时将目标区域留空。

注释 不能在同一规则中搭配使用被动和路由安全区。此外，被动安全区只能被指定为源区域，不能作为目标区域。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置**源网络**。
- 要匹配流向 IP 地址或地理位置的流量，请配置**目标网络**。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络** - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。
- **地理位置** - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。

  注释 为了确保使用最新地理位置数据过滤流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

源端口、目标端口/协议

定义流量中所用协议的端口对象。对于 TCP/UDP，这可能包括端口。

- 要匹配来自协议或端口的流量，请配置**源端口**。源端口只能为 TCP/UDP。
- 要匹配流向协议或端口的流量，请配置**目标端口/协议**。
- 要同时匹配来自特定 TCP/UDP 端口的流量和流向特定 TCP/UDP 端口的流量，请配置源端口和目标端口。如果同时将源和目标端口添加至条件，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

步骤 9 点击**确定 (OK)**。

启用透明用户身份验证

如果将身份策略配置为允许进行主动身份验证，可以使用以下身份验证方法获取用户身份：

HTTP Basic

使用HTTP Basic身份验证时，系统会始终提示用户使用其目录用户名和密码进行身份验证。密码以明文形式传输。因此，Basic 身份验证不是一种安全的身份验证。

Basic 身份验证方法是默认的身份验证机制。

HTTP Response Page

这是一种 HTTP Basic 身份验证类型，使用时，用户会看到登录浏览器页面。

NTLM、HTTP Negotiate（适用于 Active Directory 的集成 Windows 身份验证）

使用集成的 Windows 身份验证，用户可以登录到域来使用其工作站。访问服务器（包括主动身份验证期间的 威胁防御强制网络门户）时，浏览器将尝试使用此域登录。密码不进行传输。如果身份验证成功，则以透明方式对用户进行身份验证；用户不了解存在或解决的任何身份验证挑战。

如果浏览器使用域登录凭证无法满足某个身份验证请求，则系统会提示用户提供用户名和密码，这与 Basic 身份验证的用户体验是相同的。因此，如果配置集成的 Windows 身份验证，用户无需在访问同一域内的网络或服务器时提供凭证。

请注意，HTTP Negotiate 会选择 Active Directory 服务器和用户代理支持的最强方法。如果协商选择HTTP Basic作为身份验证方法，则不会获取透明身份验证。强度顺序依次为NTLM、Basic。协商必须选择 NTLM，才能进行透明身份验证。

您必须将客户端浏览器配置为支持集成的 Windows 身份验证才能进行透明身份验证。以下部分介绍了支持集成的Windows身份验证的一些常用浏览器的集成Windows身份验证常规要求和基本配置。有关更详细的信息，用户应参阅其浏览器（或其他用户代理）的帮助，因为各方法可能会因软件版本而不同。

提示 并非所有浏览器都支持集成的Windows身份验证，例如Chrome和Safari（基于编写本文档时可用版本）。系统会提示用户提供用户名和密码。请参阅浏览器的文档确定您使用的版本是否支持。

透明身份验证的要求

用户必须将其浏览器或用户代理配置为实施透明身份验证。用户可以单独执行此操作，您也可以代其进行配置，并使用软件分发工具将此配置推送至客户端工作站。如果您选择让用户自己执行此操作，请确保提供适用于您的网络的特定配置参数。

无论是浏览器还是用户代理，您都必须实施以下常规配置：

- 将用户连接网络所采用的 威胁防御重定向主机名或接口添加到“受信任站点”列表。如果不使用重定向主机名，可以使用 IP 地址，也可以使用完全限定域名（如果可用，例如，inside.example.com）。也可以使用通配符或部分地址创建一个通用的受信任站点。例如，使用 *.example.com 或只是 example.com 通常可以覆盖所有内部站点，从而信任您网络中的所有服务器（使用您自己的域名）。如果添加接口的物理地址，可能需要将多个地址添加到受信任站点，从而涵盖用户对网络的所有接入点。

- 集成的 Windows 身份验证不通过代理服务器工作。因此，您要么不使用代理，要么必须将 威胁防御重定向主机名或接口添加到被排除通过该代理的地址中。如果您决定必须使用代理，系统会提示用户进行身份验证，即使使用 NTLM 亦是如此。

提示 配置透明身份验证不是必须的，却可为最终用户提供方便。如果不配置透明身份验证，系统会向用户显示所有身份验证方法的登录质询。

配置 Internet Explorer 以进行透明身份验证

要配置 Internet Explorer 以进行 NTLM 透明身份验证，请执行以下操作：

过程

步骤 1 依次选择**工具** > **互联网选项**。

步骤 2 依次选择**安全**选项卡和**本地 Intranet** 区域，然后执行以下操作：

a) 点击**站点**按钮，打开受信任站点列表。

b) 确保至少选择以下其中一个选项：

- **自动检测 Intranet 网络**。如果选择此选项，系统将禁用其他所有选项。
- **包括所有不使用代理服务器的站点**。

c) 点击**高级**打开“本地 Intranet 站点”对话框，然后将您要信任的站点添加到**添加站点**框中，然后点击**添加**。

如果您有多个URL，请重复该过程。使用通配符指定部分URL，例如**`http://*.example.com`**或只是 **`*.example.com`**。

关闭对话框返回到“互联网选项”对话框。

d) 在**本地 Intranet** 仍处于选中状态的情况下，点击**自定义级别**打开“安全设置”对话框。找到**用户身份验证** > **登录**设置，然后选择**只在 Intranet 区域自动登录**。点击**确定**。

步骤 3 在“互联网选项”对话框中，点击**连接**选项卡，然后点击 **LAN 设置**。

如果选中**为 LAN 使用代理服务器**，您需要确保 威胁防御接口绕过该代理。适当执行以下任一操作：

- 选择**对于本地地址不使用代理服务器**。
- 点击**高级**并将地址输入**对于以下列字符开头的地址不使用代理服务器**框。您可以使用通配符，例如 **`*.example.com`**。

配置 Firefox 以进行透明身份验证

要配置 Firefox 进行 NTLM 透明身份验证，请执行以下操作：

过程

步骤 1 打开 **about:config**。借助过滤器栏找到您需要修改的首选项。

步骤 2 要支持 NTLM，请修改以下首选项（在 network.automatic 上过滤）：

- **network.automatic-ntlm-auth.trusted-uris** - 双击首选项，输入URL，然后点击**确定 (OK)**。您可以通过将 URL 以逗号分隔来输入多个 URL；包括该协议是可选的。例如：

  ```
  http://host.example.com, http://hostname, myhost.example.com
  ```

  您也可以 使用部分URL。Firefox匹配该字符串的末尾，而不是一个随机子字符串。因此，您可以仅指定域名来包括您的整个内部网络。例如：

  ```
  example.com
  ```

- **network.automatic-ntlm-auth.allow-proxies** - 确保值为 **true**，这是默认值。如果值当前为 false，请双击以更改该值。

步骤 3 检查 HTTP 代理设置。可以通过选择**工具 (Tools)** > **选项 (Options)**，然后点击“选项”对话框中的**网络 (Network)** 选项卡来查找这些设置。点击“连接”(Connection) 组中的**设置 (Settings)** 按钮。

- 如果选择**无代理**，则无需进行任何配置。
- 如果选择**使用系统代理设置**，则需要修改 about:config 中的 **network.proxy.no_proxies_on** 属性，以添加您在 **network.automatic-ntlm-auth.trusted-uris** 中包括的可信赖 URI。
- 如果选择**手动代理配置**，则更新**无代理对象**列表以包括这些可信赖的 URI。
- 如果选择其他某个选项，请确保用于这些配置的属性不包括这些可信赖的 URI。

监控身份策略

如果要求身份验证的身份策略正常工作，您应该会在**监控** > **用户**控制面板和其他有用户信息的控制面板上看到用户信息。

此外，**监控** > **事件**中显示的事件应该有用户信息。

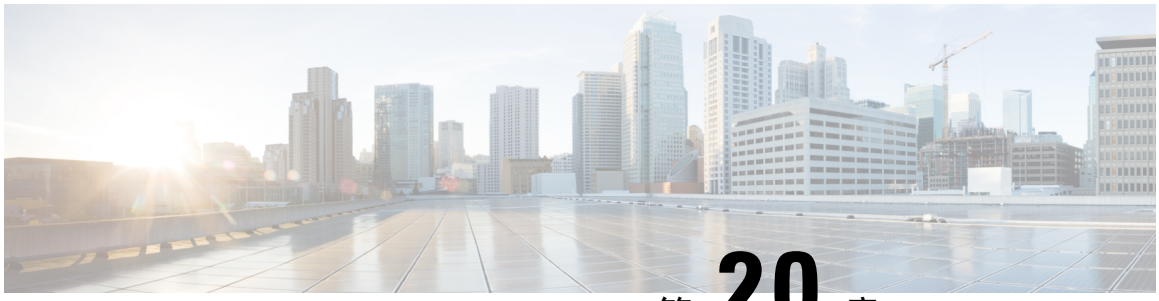
如果没有看到任何用户信息，请验证目录服务器是否在正常运行。使用目录服务器配置对话框中的**测试**按钮验证连接。

如果目录服务器在正常运行并且可用，请验证要求主动身份验证的身份规则的流量匹配条件是否是以与您的用户匹配的方式编写的。例如，请确保源区域有用户流量进入设备的接口。主动身份验证身份规则仅与 HTTP 流量匹配，因此用户必须通过设备发送该类型的流量。

对于被动身份验证，使用ISE对象中的**测试**按钮（如果您在使用该源）。如果您使用远程访问VPN，请验证服务正常运行，并且用户可以进行VPN连接。有关识别和解决问题的更多详细信息，请参阅这些功能的故障排除主题。

身份策略示例

使用案例章节涵盖实施身份策略的示例。请参阅如何深入了解您的网络流量，第 44 页。



第 20 章

安全情报

通过安全智能策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。以下主题介绍如何实施安全智能。

关于安全情报

通过安全智能策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。在使用访问控制策略评估不良流量前，系统会将其丢弃，从而减少系统资源的使用量。

您可以根据以下条件阻止流量：

- 思科 Talos 情报小组 (Talos) 源 - Talos 提供对定期更新的安全智能源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。系统定期下载智能源更新，从而提供新的威胁智能，而无需重新部署配置。

注释 默认情况下，Talos 源每小时更新一次。您可以从**设备 (Device)** > **更新 (Updates)**页面更改更新频率，甚至根据需要更新智能源。

- 网络和 URL 对象 - 如果您知道要阻止的特定 IP 地址或 URL，则可为其创建对象并将其添加到阻止列表或例外列表。请注意，您无法使用 FQDN 或范围规格的网络对象。

创建用于 IP 地址（网络）和 URL 的单独列表。

注释 如果 HTTP/HTTPS 请求针对使用 IP 地址而不是主机名的 URL，则系统会在网络地址列表中查找 IP 地址信誉。无需在网络和 URL 列表中复制 IP 地址。

创建阻止列表例外

对于每个阻止列表，您可以创建关联的例外列表，也称为不阻止列表。例外列表的唯一目的是豁免阻止出现在阻止列表中的 IP 地址或 URL。也就是说，如果发现需使用且已知安全的地址或 URL 位于在阻止列表上配置的智能源中，则可豁免该网络/URL，而无需从阻止列表中完全删除该类别。

随后访问控制策略会评估被豁免的流量。有关允许或丢弃连接的最终决定基于连接匹配的访问控制规则。访问规则还会决定恶意软件检查是否应用于连接。

安全智能源类别

下表介绍思科 Talos 情报小组 (Talos) 源中的可用类别。这些类别可用于网络和 URL 阻止操作。

这些类别可能会随时间而变化，因此新下载的源可能会存在类别更改。配置安全智能时，您可以点击类别名称旁边的信息图标以查看说明。

表 *10:* 思科 *Talos* 情报小组 *(Talos)* 源类别

安全情报类别	说明
攻击者	出站恶意活动已知的活动扫描工具和主机
Banking_fraud	从事与电子银行相关的欺诈活动的网站
Bogon	Bogon 网络和未分配的 IP 地址
Bots	托管二进制恶意软件丢弃程序的站点
CnC	托管僵尸网络的命令和控制服务器的站点
加密货币挖矿活动	提供对用于挖掘加密货币的池和钱包的远程访问的主机
Dga	用于生成作为与命令和控制服务器的交汇点的大量域名的恶意软件算法
Exploitkit	指定用于识别客户端中的软件漏洞的软件包
High_risk	根据来自安全图的 OpenDNS 预测安全算法进行匹配的域和主机名
IOC	观察到涉及感染指标 (IOC) 的主机
Link_sharing	未经许可共享版权文件的网站
恶意	表现出不一定属于另一种更精细的威胁类别的恶意行为的站点
恶意软件	托管恶意软件二进制或漏洞包的站点

安全情报类别	说明
Newly_seen	最近注册或尚未通过遥测发现的域。 **注意** 目前，此类别没有任何有效的源，已预留以供将来使用。
Open_proxy	允许匿名 Web 浏览的开放代理
Open_relay	已知用于垃圾邮件的开放邮件中继
网络钓鱼	托管网络钓鱼页面的站点
解决方案	主动参与恶意或可疑活动的 IP 地址和 URL
垃圾邮件	已知用于发送垃圾邮件的邮件主机
间谍软件	已知包含、提供或支持间谍软件和广告软件活动的网站
可疑	看似可疑并具有类似于已知恶意软件的特征的文件
Tor_exit_node	已知为 Tor Anonymizer 网络提供出口节点服务的主机

安全智能许可证要求

必须启用**IPS** 许可证，才能使用安全智能。请参阅启用或禁用可选许可证，第 87 页。

配置安全智能

通过安全智能策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。所有允许的连接仍会通过访问控制策略进行评估，并且最终可能会被丢弃。必须启用 IPS 许可证 (IPS license)，才能使用安全智能。

过程

步骤 1 依次选择**策略 (Policies)** > **安全智能 (Security Intelligence)**。

步骤 2 如果未启用策略，请点击**启用安全智能 (Enable Security Intelligence)**按钮。

您可以通过点击**安全智能 (Security Intelligence)** 开关切换到**关闭 (Off)** 随时禁用策略。配置将被保留，因此，当您再次启用该策略时，无需重新配置。

步骤 3 配置安全智能。

网络（IP 地址）和 URL 有单独的阻止列表。

a) 点击**网络**或 **URL** 选项卡显示要配置的列表。

b) 在阻止/丢弃列表中，点击 **+**，选择要立即丢弃其连接的对象或智能源。

对象选择器按类型对单独选项卡上的对象和智能源进行分门别类。如果所需的对象尚不存在，请点击列表底部的**创建新对象**链接，立即创建对象。有关思科 Talos 情报小组 (Talos) 源的说明，请点击源旁边的 **i** 按钮。另请参阅安全智能源类别，第 458 页。

注释　安全智能会忽略使用 /0 掩码的 IP 地址块。这包括 any-ipv4 和 any-ipv6 网络对象。不得选择将这些对象用于网络阻止操作。

c) 在“不阻止”列表中，点击 + 并选择阻止列表的任何例外情况。

配置该列表的唯一原因是对阻止列表中的 IP 地址或 URL 进行例外处理。被免除的连接随后将通过访问控制策略进行评估，且仍然可能会被丢弃。

d) 重复此过程以配置其他阻止列表。

步骤 4　（可选。）点击**编辑日志记录设置**按钮 (⚙) 来配置日志记录。

如果启用了日志记录，系统会记录与阻止列表条目匹配的任意项。系统不记录例外条目的匹配项，但如果被免除的连接与启用日志记录的访问控制规则匹配，您会收到日志消息。

配置以下设置：

- **连接事件日志记录** - 点击开关以启用或禁用日志记录。
- **系统日志** - 如果要将事件副本发送到外部系统日志服务器，请选择该选项并选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**添加系统日志服务器**并创建对象。

  由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

监控安全智能

如果启用安全智能策略的日志记录，则系统会为与阻止列表中项目匹配的每个连接生成安全智能事件。这些连接已有匹配的连接事件。

已丢弃连接的统计信息显示在“监控”(Monitoring) 页面上的各控制面板中。

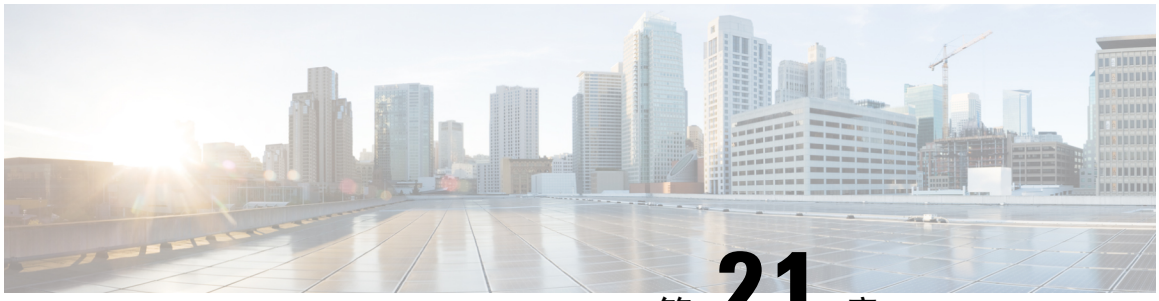
监控 > **访问和 SI 规则**控制面板显示排名靠前的访问规则及匹配流量的安全智能等效对象。

此外，可依次选择**监控** > **事件**，然后选择**安全智能**视图，查看安全智能事件以及**连接**选项卡上的相关连接事件。

- 事件中的“SI 类别 ID”字段指示阻止列表中匹配的对象，如网络或 URL 对象或源。
- 连接事件中的“原因”字段解释为什么应用了事件中显示的操作。例如，与“IP 阻止”或“URL 阻止”等原因配对的“阻止”操作表示某连接已被安全智能丢弃。

安全智能示例

使用案例章节涵盖实施安全智能策略的示例。请参阅如何阻止威胁，第 51 页。



第 21 章

访问控制

以下主题介绍访问控制规则。这些规则控制允许通过设备传递的流量，并会对流量应用入侵检测等高级服务。

访问控制最佳实践

访问控制策略是保护内部网络和防止用户访问不良外部网络资源（例如不良网站）的主要工具。因此，我们建议您特别注意此策略并对其进行调整，以实现所需的保护和连接级别。

以下程序概述您应对访问控制策略执行的基本操作。这只是一个概述，并不介绍执行每个任务的详尽步骤。

要进入访问控制策略，请选择**策略** > **访问控制**。

过程

步骤 1 配置策略的默认操作。

默认操作处理不与策略中的特定规则匹配的连接。默认情况下，此操作为**阻止**，以便阻止规则中遗漏的任何流量。因此，您只需要编写允许所需流量的访问控制规则。这是配置访问控制策略的传统方式。

您可以执行相反的操作，即在默认情况下允许流量，并编写丢弃已知不良流量的规则，这样您就无需为要允许的所有流量制定规则。这样更便于使用新服务，但会使新不良流量在您不经意间进入网络，构成风险。

步骤 2 点击**访问策略设置 (Access Policy Settings)** (⚙) 按钮，并启用 **TLS 服务器身份发现 (TLS Server Identity Discovery)** 选项。

此选项可改进 TLS 1.3 连接的初始应用检测以及 URL 类别和信誉识别。如果未启用此选项，则 TLS 1.3 流量将不与预期规则匹配。此选项还可以提高解密规则的效率。

步骤 3 尽可能少创建访问控制规则。

使用传统防火墙，您可能最终会获得数万条用于 IP 地址和端口的各种组合的规则。借助下一代防火墙，您可以使用高级检测功能并避免这其中的一些细化规则。您设置的规则越少，系统评估流量的速度就越快，您在规则集内查找和修复问题就越容易。

步骤 4 对访问控制规则启用日志记录。

仅当启用日志记录时，系统才会为匹配流量收集统计信息。如果不启用日志记录，您的监控控制面板信息将不准确。

步骤 5 将非常具体的规则放在策略前面，并确保具体规则位置高于任何可以匹配相同连接的更通用的规则。

系统自上而下地评估策略，并应用流量匹配的第一个策略。因此，如果您输入阻止所有流向特定子网的流量的规则，然后在此规则之后设置一条允许访问该子网内的单个 IP 地址的规则，则系统不会允许流量流向该地址，因为第一个规则将阻止它。

此外，应将仅基于传统条件（例如入向/出向接口和源/目标 IP 地址、端口或地理位置）来控制流量的规则放在需要深度检测的规则（例如应用于用户条件、URL 过滤或应用过滤的规则）前面。由于这些规则不需要执行检测，因此将它们放到前面可以让您更快地为与规则匹配的连接做出访问控制决策。

有关更多建议，请参阅访问控制规则顺序最佳实践，第 474 页。

步骤 6 将阻止规则和允许规则配对以控制部分流量。

例如，您可能希望允许大量 HTTP/HTTPS 流量，但需要阻止访问某些不良网站（例如色情或赌博网站）。您可以通过创建以下规则并使其在策略中保持相应先后顺序（例如，规则 11 和 12）来实现此目的。

- 将控制不良 URL 类别的 URL 过滤阻止规则应用于内部安全区（源）和外部安全区（目的地），以及任何 IP 地址、端口或地理位置。例如，阻止僵尸网络、虐待儿童的内容、挖矿劫持、DNS 隧道、电子银行欺诈、漏洞攻击、极端行为、过滤器规避行为、赌博、黑客攻击、仇恨言论、高风险站点和位置、非法活动、非法下载、违禁药物、恶意站点、恶意软件站点、移动威胁、P2P 恶意软件节点、网络钓鱼、色情、垃圾邮件、间谍软件和广告软件。
- 将适用于 HTTP 和 HTTPS 应用的应用过滤“允许”规则应用于内部安全区（源）和外部安全区（目的地）以及任何 IP 地址、端口或地理位置。在 URL 过滤规则“阻止”规则阻止对不良 Web 资源的访问后，此规则允许所有其他 HTTP/HTTPS 访问。

步骤 7 无论 IP 地址或端口如何，都可使用高级下一代防火墙功能来控制流量。

攻击者或其他恶意行为者可能会频繁更改 IP 地址和端口，以规避传统访问控制流量匹配条件。因此，请改用以下下一代功能：

- 用户条件 - 配置身份策略，以获取有关发起流量的用户的信息。理想情况下，您的 Active Directory 服务器会将用户分为不同的组，并且您可以创建基于用户组成员身份允许或阻止流量的访问控制规则。例如，允许工程师访问您的开发子网，但隐式阻止不属于工程师组的所有其他人访问此子网。使用组而不使用单个用户名，这样您就无需在向网络中添加人员时不断更新规则。
- 应用条件 - 使用应用过滤条件来允许或阻止某些类型的应用。这样，如果用户更改 HTTP 连接的端口，系统可以识别出它是 HTTP，即使它不连接到端口 80。有关更多建议，请参阅应用过滤最佳实践，第 467 页。
- URL 类别和信誉条件 - 使用基于类别的 URL 过滤来根据站点类型动态允许或阻止站点。在站点类型或类别中，您可以根据站点信誉的好坏来调整规则。通过使用类别和信誉，您无需在站点更改 URL 时不断调整规则，而如果您尝试按 URL 手动阻止站点，就必须执行此类调整。有关更多建议，请参阅有效 URL 过滤的最佳实践，第 471 页。

  您还可以将 URL 类别/信誉过滤规则应用于 DNS 查找请求中的 FQDN。系统可以阻止对被阻止的类别/信誉的 DNS 响应，从而有效地阻止用户的连接尝试。有关详细信息，请参阅基于 URL 类别和信誉过滤 DNS 请求，第 473 页。

步骤 8 将入侵检测应用于所有“允许”规则。

下一代防火墙的一个强大功能是，您可以使用同一设备应用入侵检测和访问控制。将入侵策略应用于每个“允许”规则，这样如果确实有攻击通过正常良性路径进入您的网络，您也可以捕获该攻击并丢弃攻击连接。

如果默认操作为“允许”，您还可以对与默认操作匹配的流量应用入侵保护。

步骤 9 此外，还应配置安全智能策略以阻止不良 IP 地址和 URL。

安全智能策略在访问控制策略之前应用，以便可以在系统评估访问控制规则之前阻止不良连接。这可以尽早阻止此类连接，并帮助您降低访问控制规则的复杂性。

步骤 10 考虑实施 SSL 解密策略。

系统不会对加密的流量进行深度检测。如果配置 SSL 解密策略，则访问控制策略将应用于已解密版本的流量。因此，深度检测可以识别攻击（使用入侵策略），并且规则匹配效果更好，因为应用和 URL 过滤会得到更高效的应用。然后，访问控制策略允许的所有流量都会在从设备发送出去之前重新加密，因此最终用户不会失去加密保护。

步骤 11 启用对象组搜索以简化规则的部署。

从版本 7.2 开始，默认情况下会在新部署上启用此功能，但不会在升级后的系统上自动启用。

启用对象组搜索可以降低包含网络对象的访问控制策略的内存要求。但是，请务必注意，对象组搜索还可能会降低规则查找性能，从而提高 CPU 利用率。您应该在 CPU 影响与降低特定访问控制策略的内存要求之间取得平衡。在大多数情况下，启用对象组搜索可提高网络运营性能。

可执行 **object-group-search access-control** 命令来通过使用 FlexConfig 设置此选项；可在取消模板中使用该命令的 **no** 形式。

访问控制概述

以下主题介绍访问控制策略。

访问控制规则和默认操作

使用访问控制策略允许或阻止对网络资源的访问。该策略包含一系列有序的规则，按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件条件的第一个规则。

您可以根据以下条件控制访问：

- 传统网络特征，例如源和目标 IP 地址、协议、端口和接口（以安全区形式）。
- 源或目标（以网络对象形式）的完全限定域名 (FQDN)。流量匹配基于从 DNS 查询为该名称返回的 IP 地址。
- 思科身份服务引擎 (ISE) 分配给源或目的地的安全组标记 (SGT)。
- 正在使用的应用。您可以基于特定应用控制访问，也可以创建涵盖应用类别、标记特定特征的应用、应用类型（客户端、服务器、Web）或应用风险或业务相关性评级的规则。
- Web 请求的目的 URL，包括 URL 的通用类别。您可以基于目标站点的公共信誉优化类别匹配。
- DNS 查找请求中 FQDN 的 URL 类别和信誉。您可以阻止不需要的类别或信誉不佳的 DNS 响应，从而有效防止后续连接尝试。
- 发出请求的用户或用户所属的用户组。

对于您允许的未加密流量，可以应用 IPS 检测来检查威胁并阻止看似攻击的流量。另外，您还可以使用文件策略来检查是否存在禁止文件或恶意软件。

与访问规则不匹配的流量由访问控制**默认操作**处理。默认情况下，如果允许流量，则可以对流量应用入侵检测。但您不能对默认操作处理的流量执行文件或恶意软件检测。

应用过滤

您可以使用访问控制规则基于连接中使用的应用过滤流量。系统会识别各种各样的应用，因此您不需要弄明白如何在不阻止所有 Web 应用的情况下阻止某个 Web 应用。

对于一些常用的应用，您可以根据应用的不同方面进行过滤。例如，您可以创建一个阻止 Facebook 游戏但不阻止所有 Facebook 功能的规则。

您还可以基于一般应用特点创建规则，通过选择风险或业务相关性、类型、类别或标记来阻止或允许整组应用。**但是，在应用过滤器中选择类别时，请查看匹配的应用列表，确保不包含非预期应用。**有关可能分组的详细说明，请参阅应用条件，第 483 页。

已加密和已解密流量的应用控制

如果应用使用加密，系统可能无法识别该应用。

系统可以检测使用 StartTLS 加密的应用流量，包括 SMTPS、POP、FTPS、TelnetS 和 IMAPS。此外，系统还可以根据 TLS ClientHello 消息中的服务器名称指示或服务器证书中的使用者可分辨名称值来识别某些加密应用。

请使用应用过滤器对话框通过选择以下标记来确定应用是否需要解密，然后检查应用列表。

- **SSL 协议** - 不需要解密标记为“SSL 协议”的流量。系统可以识别此流量并应用您的访问控制操作。用于所列出应用的访问控制规则应与预期的连接匹配。
- **解密流量** - 只有先解密流量，系统才能识别此流量。配置用于此流量的 SSL 解密规则。

过滤通用工业协议 (CIP) 和 Modbus 应用 (ISA 3000)

可以在思科 ISA 3000设备上启用通用工业协议 (CIP) 和 Modbus 预处理器，并在访问控制规则中过滤 CIP 和 Modbus 应用。所有 CIP 应用名称均以“CIP”开头，例如 CIP Write。仅有一个应用适用于 Modbus。

要启用预处理器，必须在 CLI 会话（SSH 或控制台）中进入专家模式，并发出以下命令以启用其中一个或两个监控和数据采集 (SCADA) 应用。

sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}

例如，要启用两个预处理器：

```
> expert
admin@firepower:~$ sudo /usr/local/sf/bin/enable_scada.sh both
```

注释 必须在每次部署后发出此命令。部署期间禁用这些预处理器。

应用过滤最佳实践

设计应用过滤访问控制规则时，请牢记以下建议。

- 要处理网络服务器所推荐的流量（例如广告流量），请匹配被推荐的应用（而非推荐应用）。
- 避免将应用与 URL 条件组合在同一规则中，尤其是对于加密流量。
- 如果要为标记为**解密流量**的流量编写规则，请确保具有解密匹配流量的 SSL 解密规则。仅可在解密连接中识别这些应用。
- TLS 1.3 加密大多数握手消息，因此证书信息不容易获得。对于使用 TLS 1.3 加密的流量，要高效地匹配使用应用或URL过滤的访问规则，系统必须获取服务器的明文证书。我们建议您在访问控制设置中启用 **TLS 1.3 证书可视性** 。如果启用此选项，系统将根据客户端 Hello 数据包中的 IP 地址和服务器名称指示 (SNI) 检查站点的证书是否存储在缓存中。如果不可用，系统将使用 TLS 1.2 探测器获取证书，然后可将其用于应用/URL 类别和信誉识别，而无需解密连接。
- 系统可以检测多个类型的 Skype 应用流量。要控制 Skype 流量，请从应用过滤器列表中选择 Skype 标记（而不是选择个别应用）。这确保系统可以相同方式检测和控制所有 Skype 流量。
- 要控制 Zoho 邮件访问，请选择 Zoho 和 Zoho 邮件应用。

URL 过滤

您可以使用访问控制规则基于 HTTP 或 HTTPS 连接中使用的 URL 过滤流量。请注意，HTTP 的 URL 过滤比 HTTPS 更直接，因为 HTTPS 会被加密。

您可以使用以下方法实施 URL 过滤：

- 基于类别和信誉的 URL 过滤 - 使用 URL 过滤许可证，您可以根据 URL 的一般分类（类别）和风险级别（信誉）控制对网站的访问。这是迄今为止阻止非必要网站的最简单、最有效的方法。
- 手动 URL 过滤 - 使用任何许可证均可手动指定各个 URL 和 URL 组，以便对网络流量实现精细的自定义控制。手动过滤的主要目的是创建基于类别的阻止规则的例外，但可以将手动规则用于其他目的。

以下主题提供了有关 URL 过滤的详细信息。

按照类别和信誉过滤 URL

通过 URL 过滤许可证，您可以基于所请求 URL 的类别和信誉控制对网站的访问：

- 类别 - URL 的一般分类。例如，ebay.com 属于“拍卖”类别，而 monster.com 属于“职位搜索”类别。URL 可以属于多个类别。
- 信誉 - URL 被用于可能违反组织安全策略之目的的可能性。范围可从“不受信任”（第 1 级）到“受信任”（第 5 级）。

URL 类别和信誉可帮助您快速配置 URL 过滤。例如，您可以使用访问控制阻止“违禁药物”类别中不受信任的 URL。

有关类别说明，请参阅 https://www.talosintelligence.com/categories。

使用类别和信誉数据还会简化策略创建和管理。代表安全威胁的站点或提供不良内容的站点的出现和消失速度，可能比您更新和部署新策略的速度要快。由于思科使用新站点、已更改分类与信誉更新 URL 数据库，因此，规则会自动调整以适应新信息。无需为新站点编辑规则。

如果启用常规 URL 数据库更新，则可确保系统使用最新信息进行 URL 过滤。还可启用与思科 综合安全智能 (CSI) 的通信，获取类别和信誉已知的 URL 的最新威胁智能。有关详细信息，请参阅配置 URL 过滤首选项，第 754 页。

注释 要查看事件和应用详细信息中的 URL 类别和信誉信息，必须至少创建一条具有 URL 标准的规则。

查找 URL 的类别和信誉

您可以检查特定 URL 的类别和信誉。您可以转至访问控制规则或 SSL 解密规则的 URL 选项卡，或转至**设备** > **系统设置** > **URL 过滤首选项**。其中，您可以在**待检查的 URL** 字段中输入 URL，然后点击**前往**。

您将转至显示查询结果的网站。您可以使用此信息，帮助您查看基于类别和信誉的URL过滤规则的表现。

如果您对分类持不同意见，您可以点击 设备管理器 中的 **提交 URL 类别争议**，告诉我们您的想法。

手动 URL 过滤

您可以通过手动过滤各个 URL 或 URL 组，补充或选择性地覆盖基于类别和信誉的 URL 过滤。您可以在没有特殊许可证的情况下执行此类 URL 过滤。

例如，您可以使用访问控制阻止不适合于您组织的某类网站。但是，如果该类别包含适合的网站，且要为其提供访问权限，则可以为该站点创建手动“允许”规则，并将该规则置于适用于该类别的“阻止”规则前。

要配置手动 URL 过滤，请使用目标 URL 创建一个 URL 对象。基于如下规则解释该 URL：

- 如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配。然后，如果满足以下任一条件，则 URL 被视为匹配项：
  - 字符串位于 URL 的开头。
  - 字符串后面有一个点。
  - 字符串开头包含一个点。
  - 字符串后面跟有 :// 字符。

  例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。

注释 我们建议您不要使用手动URL过滤阻止或允许个别网页或部分网站（即，带有 / 字符的 URL），因为这样可能会重组服务器并将页面移至新路径。

- 系统忽略加密协议（HTTP 与 HTTPS）。换句话说，如果阻止网站，系统将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个应用条件指定特定协议。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 example.com 而不是 http://example.com。
- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公钥中的使用者公用名创建该对象。此外，系统会忽略使用者公用名中的子域，因此，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

  但请注意，证书中的使用者公用名可能与网站的域名完全无关。例如，youtube.com 证书中的使用者公用名是 *.google.com（当然，这可能会随时更改）。如果使用 SSL 解密策略解密 HTTPS 流量以便 URL 过滤规则可用于解密策略，则可能获得更一致的结果。

注释 如果由于证书信息不再可用，浏览器恢复 TLS 会话，则 URL 对象将不匹配 HTTPS 流量。因此，即使精心配置 URL 对象，也可能会得到不一致的 HTTPS 连接结果。

过滤 HTTPS 流量

由于 HTTPS 流量加密，所以直接对 HTTPS 流量执行 URL 过滤并不像对 HTTP 流量执行 URL 过滤那样直接。因此，应考虑使用 SSL 解密策略解密想要过滤的所有 HTTPS 流量。这样，URL 过滤访问控制策略可有效用于解密流量，并会获得与常规 HTTP 流量相同的结果。

但是，如果打算允许某些HTTPS流量在未加密情况下通过访问控制策略，则需了解规则匹配HTTPS流量与匹配 HTTP 流量的方式不同。要过滤加密流量，系统将根据 SSL 握手期间传递的信息确定请求的URL：用于加密流量的公钥证书中的使用者公用名。URL中的网站主机名与使用者公用名之间可能没有多大关系。

如果启用 DNS 请求过滤，则可以改进类别/信誉规则的 HTTPS 匹配。系统可以在 DNS 解析阶段确定类别和信誉，并在用户可以开始 HTTPS 连接尝试之前阻止对不需要的组合做出 DNS 回复。对于允许的 DNS 响应，系统将提供可用于后续 HTTPS 连接的类别/信誉信息。请参阅 DNS 请求过滤，第 472 页。

HTTPS 过滤与 HTTP 过滤不同，它不考虑使用者公用名内的子域。手动过滤 HTTPS URL 时，请勿包含子域信息。例如，使用 example.com 而不是 www.example.com。此外，请查看站点所使用的证书内容，以确保使用者公用名中使用的域名正确，且该名称不会与其他规则冲突（例如，想要阻止的站点名称可能与想要允许的站点名称重叠）。例如，youtube.com 证书中的使用者公用名是 *.google.com（当然，这可能会随时更改）。

注释 如果由于证书信息不再可用，浏览器恢复 TLS 会话，则 URL 对象将不匹配 HTTPS 流量。因此，即使精心配置 URL 对象，也可能会得到不一致的 HTTPS 连接结果。

按加密协议控制流量

在执行 URL 过滤时，系统会忽略加密协议（HTTP 和 HTTPS）。对于手动 URL 标准和基于信誉的 URL 标准均会发生此情况。换句话说，URL 过滤以相同方式处理发送到以下网站的流量：

- http://example.com
- https://example.com

要配置仅匹配HTTP流量或HTTPS流量（而不是同时匹配这两种流量）的规则，请在“目标”条件中指定 TCP 端口或在规则中添加应用条件。例如，可以通过构造两个访问控制规则（各规则具有 TCP 端口或应用和 URL 标准）来允许对某个站点进行 HTTPS 访问，同时禁止 HTTP 访问。

第一个规则允许 HTTPS 流量到达网站：

操作：允许
TCP 端口或应用：HTTPS（TCP 端口 443）
URL：example.com

第二个规则阻止对同一网站进行 HTTP 访问：

操作：阻止
TCP 端口或应用：HTTP（TCP 端口 80）

URL：example.com

比较 URL 和应用过滤

URL 和应用过滤具有许多相似之处。但应将其用于明显不同的目的：

- URL 过滤最好用于阻止或允许访问整个 Web 服务器。例如，如果不希望在网络上进行任何类型的赌博，则可创建用于阻止赌博类别的 URL 过滤规则。通过该规则，用户无法访问该类别内所有 Web 服务器上的任何页面。
- 应用过滤适用于阻止特定应用（无论托管站点如何），或阻止在其他方面受允许的其他网站的特定功能。例如，可以在不阻止所有 Facebook 功能的情况下阻止 Facebook 游戏应用。

由于组合应用与 URL 条件可能会导致非预期结果，尤其是对于加密流量，因此，分别创建用于 URL 和应用条件的单独规则是个好方法。如果需要将应用与 URL 条件合并到单个规则中，应将这些规则直接置于仅应用或仅 URL 规则后，除非应用+URL 规则作为更一般的仅应用或仅 URL 规则的例外。由于 URL 过滤阻止规则比应用过滤阻止规则更广泛，因此，您应将其置于仅应用规则之上。

如果将应用条件与 URL 条件组合在一起，则可能需要更仔细地监控网络，以确保不允许访问不必要的站点和应用。

有效 URL 过滤的最佳实践

设计 URL 过滤访问控制规则时，请牢记以下建议。

- 尽可能使用类别和信誉阻止。这可以确保在将新站点添加到类别时自动将其阻止，且如果站点的信誉变得更佳（或更劣），则根据信誉对阻止情况进行调整。
- 使用 URL 类别匹配时，请注意，有时候站点登录页的类别与站点本身的类别不同。例如，Gmail 属于“基于 Web 的邮件”类别，而登录页面属于搜索引擎和门户 (Search Engines and Portals)类别。如果您为类别制定了包含不同操作的不同规则，可能会出现意想不到的结果。
- 使用 URL 对象定位整个网站，并对类别阻止规则进行例外处理。也就是说，允许特定网站（否则，该网站会被阻止于某个类别规则中）。
- 如果要手动阻止 Web 服务器（使用 URL 对象），则在安全智能策略中这样做更有效。评估访问控制规则前，安全智能策略丢弃连接，以便可获得更快、更有效的阻止。
- 为对 HTTPS 连接进行最有效的过滤，请使用 SSL 解密规则解密正在为其编写访问控制规则的流量。任何解密的 HTTPS 连接均会在访问控制策略中作为 HTTP 连接予以过滤，以避免 HTTPS 过滤的所有限制。
- TLS 1.3 加密大多数握手消息，因此证书信息不容易获得。对于使用 TLS 1.3 加密的流量，要高效地匹配使用应用或 URL 过滤的访问规则，系统必须获取服务器的明文证书。我们建议您在访问控制设置中启用 **TLS 1.3 证书可视性** 。如果启用此选项，系统将根据客户端 Hello 数据包中的 IP 地址和服务器名称指示 (SNI) 检查站点的证书是否存储在缓存中。如果不可用，系统将使用 TLS 1.2 探测器获取证书，然后可将其用于应用/URL 类别和信誉识别，而无需解密连接。
- 将 URL 阻止规则置于任何应用过滤规则前，因为 URL 过滤阻止整个 Web 服务器，而应用过滤将针对特定的应用使用，而不考虑 Web 服务器。

- 如果要阻止类别未知的高风险站点，请选择未分类类别，并将信誉滑块调整为“可疑”或“不受信任”。
- 您还可以通过启用 DNS 请求过滤来提高总体 URL 过滤效率。当使用 DNS 请求过滤时，系统会在执行 DNS 查找时确定 FQDN 的 URL 类别和信誉，以便在后续 HTTP/HTTPS 请求的目的地相同时提供这些信息。此外，如果阻止类别/信誉，则尝试连接将在 DNS 请求阶段停止，而不是在 Web 会话建立阶段停止。请参阅DNS 请求过滤，第 472 页。

阻止网站时用户看到的内容

使用 URL 过滤规则阻止网站时，用户所看到的内容视该站点是否加密而异。

- HTTP 连接 - 用户会看到系统默认阻止响应页面，而不是为超时或重置连接而正常显示的浏览器页面。此页面将明确指示，您有意阻止了该连接。
- HTTPS（已加密）连接 - 用户不会看到系统默认阻止响应页面。相反，用户会看到浏览器显示安全连接故障的默认页面。错误消息不会指明该站点由于策略而被阻止。相反，错误可能显示为没有通用的加密算法。据此消息，无法明确看出是您有意阻止了该连接。

此外，网站可能是被属于非显式URL过滤规则的其他访问控制规则，甚至是被默认操作而阻止。例如，如果阻止整个网络或地理位置，也会阻止该网络或该地理位置的任何网站。受这些规则阻止的用户可能（也可能不能）得到以下限制中所述的响应页面。

如果实施URL过滤，请考虑向最终用户说明他们在站点被有意阻止时可能会看到的内容，以及您将阻止的站点类型。否则，他们可能会花费大量时间来解决受阻止的连接故障。

HTTP 响应页面的限制

当系统阻止网络流量时，并不总是显示 HTTP 响应页面。

- 如果网络流量由于提升的访问控制规则（放在前面的仅包含简单网络条件的阻止规则）被阻止，系统则不显示响应页面。
- 如果网络流量在系统识别请求的 URL 之前被阻止，则系统不显示响应页面。
- 对于被访问控制规则阻止的已加密连接，系统不会显示响应页面。

DNS 请求过滤

您可以将 URL 类别和信誉数据库应用于 DNS 查找请求，即使是对于非 HTTP/HTTPS 的连接尝试也可以如此。

例如，如果用户尝试建立到 www.example.com 的 FTP 连接，您可以将系统配置为在看到针对该完全限定域名 (FQDN) 的 DNS 查找请求时查找 www.example.com 的类别和信誉。如果返回的类别/信誉的 DNS/URL 过滤规则是阻止规则，则系统会阻止 DNS 回复。因此，用户无法获取 FQDN 的 IP 地址，并且连接尝试失败。

通过启用 DNS 查找请求过滤，您可以将 URL 过滤规则扩展到除 HTTP/HTTPS 之外的协议，并防止 FTP、TFTP、SCP、ICMP 和任何其他协议与您阻止进行网络访问的站点建立连接。只要用户使用

FQDN 名称并因此需要进行 DNS 查找，此方法就有效。如果用户使用 IP 地址，就没有 DNS 请求，且无法阻止 DNS 请求。

对于 HTTP/HTTPS 流量，在 DNS 请求时执行类别/信誉查找可能会提高系统性能，因为它可以在尝试建立 Web 会话之前阻止连接。这对于加密的 HTTPS 可能特别有用。通过在 DNS 请求阶段拒绝，系统永远不会看到HTTPS连接，因此您的解密规则不需要评估，系统也不需要执行更困难的任务，即将加密会话与正确的访问控制规则进行匹配。

DNS 请求过滤准则

在配置 DNS 请求过滤时，请记住以下几点：

- DNS请求过滤仅适用于DNS会话。如果允许DNS回复（即，URL过滤规则操作为“允许”），则用户使用返回的IP地址建立的后续连接将单独与您的访问控制规则进行匹配。连接可能与其他规则匹配，因此由于其他原因而被阻止或允许。例如，如果允许 FTP 尝试通过 DNS 查找获取 IP 地址，则可能有另一个禁止 FTP 连接的访问控制规则，连接最终将被阻止。
- 将根据匹配规则允许或阻止与 URL/DNS 请求过滤规则之前的访问控制规则相匹配的 DNS 查找请求。将不会对这些连接执行类别/信誉查找。
- 此功能要求您根据类别/信誉实施 URL 过滤。您必须具有此类 URL 过滤的 URL 过滤许可证。如果没有基于类别/信誉的 URL 过滤规则，则 DNS 请求过滤不相关，因此不应启用。
- 由 DNS 过滤生成的连接事件包括以下特别需要关注的字段：DNS 查询、URL 类别和 URL 信誉。DNS 查询字段显示查找请求的完全限定域名 (FQDN)。对于 DNS 过滤事件，URL 字段将为空。
- DNS 请求过滤仅使用 URL 类别和信誉数据库。在匹配访问控制规则中定义的任何 URL 对象或其他手动 URL 过滤都将被忽略。如果要实施 DNS 名称手动阻止，请使用安全智能 DNS 策略。

基于 URL 类别和信誉过滤 DNS 请求

以下程序介绍如何实施 DNS 查找请求过滤。

开始之前

您必须启用 URL 许可证（如果尚未启用）。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 如有必要，请点击**访问策略设置** ( ) 按钮，选择 **DNS 流量的信誉实施**选项，然后点击**确定**。

此选项为访问控制策略启用 DNS 请求过滤。默认情况下，此选项已启用。

步骤 3 评估现有的 URL 过滤规则或创建新的规则，以根据也适用于 DNS 请求的 URL 类别和信誉实施过滤。

URL 过滤通常仅适用于 HTTP/HTTPS 流量，因此没有理由根据应用或端口限制这些规则。但是，如果有这些限制，请确保规则也适用于 DNS 请求：

- 在**源/目标**选项卡上，如果**目标端口**字段的值为**任何**，则无需更改。如果指定了端口，请将 **DNS over UDP** 和 **DNS over TCP** 添加到列表。
- 在**应用**选项卡上，如果应用列表仅包含**任何**，则无需更改。如果指定了任何应用或应用过滤器，请将 **DNS** 应用添加到列表或过滤器。其他与 DNS 相关的选项与此目的无关。

有关创建访问控制规则的信息，请参阅配置访问控制规则，第 480 页。

步骤 4 评估前面的规则，确保 DNS 请求与这些规则不匹配。

仅当 DNS 请求与具有类别和信誉指定的 URL 过滤规则匹配时，才会确定类别和信誉。任何与访问控制策略中的规则比 URL 过滤规则更早匹配的任何 DNS 请求都会绕过 DNS 请求过滤。此类 DNS 请求根据匹配规则（被阻止或允许）进行处理。

入侵、文件和恶意软件检测

入侵策略和文件策略共同发挥作用，作为允许流量到达其目标之前的最后一道防线。

- 入侵策略监管系统的入侵防御功能。
- 文件策略监管系统的文件控制和恶意软件防御功能。

处理所有其他流量后，才会检验网络流量中是否存在入侵、禁止文件和恶意软件。通过将入侵策略或文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略和/或文件策略检测流量。

您只能对**允许**流量的规则配置入侵策略和文件策略。对于设置为**信任**或**阻止**流量的规则，系统不会执行检测。此外，如果访问控制策略的默认操作是**允许**，则您可以配置入侵策略，但不能配置文件策略。

对由访问控制规则处理的任何单个连接，文件检测均发生在入侵检测之前。也就是说，系统不检测文件策略所阻止的文件是否存在入侵。在文件检测中，基于类型的简单阻止优先于恶意软件检测和阻止。文件在会话中得以检测和阻止之前，来自该会话的数据包均可能接受入侵检测。

注释 默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。检测仅适用于未加密的流量。

访问控制规则顺序最佳实践

先匹配的规则先应用，所以您必须确保流量匹配条件条件较具体的规则显示在次之用来匹配流量的较通用条件条件的策略上方。请考虑以下建议：

- 特定规则应在一般规则之前，特别当特定规则是一般规则的例外时。
- 仅基于第 3/4 层条件丢弃流量的任何规则（如 IP 地址、安全区和端口号）应尽早出现。我们建议这些规则应在需要检查的任何规则前，如具有应用或 URL 条件的规则，因为可快速评估第 3/4 层条件而无需检查。当然，这些规则的任何例外必须置于这些规则之上。
- 尽可能将特定丢弃规则置于策略顶部附近。这确保了对非预期流量尽可能做出最早的决定。
- 包括应用和 URL 条件的任何规则应直接位于仅应用或仅 URL 规则前，除非应用+URL 规则作为更一般仅应用或仅 URL 规则的例外。组合应用和 URL 条件可能会导致非预期结果，尤其是对于加密流量，因此，我们建议您尽可能创建单独的 URL 和应用过滤规则。

NAT 和访问规则

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

其他安全策略如何影响访问控制

其他安全策略可能影响访问控制规则的运行和对连接的匹配。配置访问规则时，请记住以下几点：

- **SSL 解密**策略 - 访问控制前评估 SSL 解密规则。因此，如果加密连接与应用某类型解密的 SSL 解密规则相匹配，则该连接为通过访问控制策略评估的纯文本（解密）连接。访问规则无法查看加密版本的连接。此外，访问控制策略绝不会看到任何与丢弃流量的 SSL 解密规则相匹配的连接。最后，匹配“不解密”规则的任何加密连接将以其加密状态接受评估。
- **身份**策略 - 仅当存在用于源 IP 地址的用户映射时，连接才与用户（以及用户组）匹配。侧重于用户或组成员关系的访问规则可能仅匹配身份策略成功收集的用户身份的那些连接。
- **安全智能**策略 - 访问控制策略绝不会看到任何被丢弃的连接。匹配“不阻止”列表的连接随后会与访问控制规则相匹配，最终，访问控制规则决定如何处理（允许或丢弃）连接。
- **VPN**（站点间或远程访问）- 始终根据访问控制策略对 VPN 流量进行评估，并根据匹配规则允许或丢弃连接。但在评估访问控制策略前，VPN 隧道本身将被解密。访问控制策略评估嵌入 VPN 隧道中的连接，而不是隧道本身。

访问控制许可证要求

使用访问控制策略无需特殊许可证。

但若要使用访问控制策略中的特定功能，则需以下许可证。有关配置许可证的信息，请参阅启用或禁用可选许可证，第 87 页。

- **URL** 许可证 - 创建将 URL 类别和信誉作为匹配条件的规则。

- **IPS**许可证 - 为访问规则或默认操作配置入侵策略。还需要此许可证才能使用文件策略（还需要恶意软件防御许可证）。
- **恶意软件防御**许可证 - 在访问规则上配置文件策略。文件策略还需要IPS 。

访问控制策略的准则和限制

以下是访问控制的一些其他限制。请在评估是否会从规则中获取预期结果时考虑这些内容。

- 如果URL数据库更新包括已添加（新增、传入）、已弃用（传出）或已删除的类别，则您可以在一个宽限期内对受影响的访问控制规则进行更改。受影响的规则都标有信息性消息，包含对影响规则的问题的说明，以及思科 Talos 情报小组 (Talos) 网站的链接，其中包含有关类别更改的详细信息。您需要更新规则，以便它可以使用最新 URL 数据库中相应的类别。

  要适应宽限期，请将新添加的传入类别添加到适当的规则，同时不删除已弃用的传出类别：规则应包含新的和旧的类别。当旧类别标记为删除时，新类别才会生效。当旧类别最终被删除时，您需要编辑规则来移除已删除的类别并重新部署配置。只有在修复所有使用旧类别的规则后，系统才不会阻止您部署配置。点击表格上方的**查看问题规则**链接，过滤出需要注意的规则。

- 设备管理器 可以从目录服务器下载多达 50,000 个用户的信息。如果您的目录服务器上有超过 50,000 个用户账户，则在访问规则中选择用户时或查看基于用户的控制面板信息时，您不会看到所有可能的名称。您仅可以对已下载的名称编写规则。

  此 50,000 个用户的限制也适用于与组相关联的名称。如果组成员超过 50,000 个，则只能将下载的 50,000 个名称与组成员身份进行匹配。

- 如果漏洞数据库 (VDB) 更新删除（弃用）应用，则必须对使用已删除应用的任何访问控制规则或应用过滤器进行更改。修复这些规则前，您无法部署更改。此外，您无法在解决问题之前安装系统软件更新。在“应用过滤器对象”页面上或规则的“应用”选项卡上，这些应用在应用名称后显示“（已弃用）”。

- 要将完全限定域名 (FQDN) 网络对象用作源或目标条件，您还必须在**设备** > **系统设置** > **DNS 服务器**上配置适用于数据接口的 DNS。系统不使用管理 DNS 服务器设置查找访问控制规则中使用的 FQDN 对象。有关排除 FQDN 解析问题的信息，请参阅常规 DNS 问题故障排除，第 744 页。

  请注意，通过 FQDN 控制访问是尽力而为机制。考虑以下几点：

  - 由于 DNS 回复可能具有欺骗性，因此只能使用完全受信任的内部 DNS 服务器。
  - 有些 FQDN，特别是非常受欢迎的服务器，可能有成百上千个 IP 地址，而且这些地址经常都会变化。由于系统使用的是缓存的 DNS 查询结果，用户可能会获得尚未在缓存中的地址，因此他们的连接将与 FQDN 规则不匹配。使用 FQDN 网络对象的规则只对解析为 100 个以内地址的名称有效。

    建议您不要为解析为超过 100 个地址的 FQDN 创建网络对象规则，因为连接中的地址是设备DNS缓存中已解析和可用地址的可能性很低。对于这些情况，请使用基于URL的规则，而不是 FQDN 网络对象规则。

- 对于受欢迎的 FQDN，不同的 DNS 服务器可以返回一组不同的 IP 地址。因此，如果您的用户使用的DNS服务器与您所配置的不同，基于FQDN的访问控制规则可能不适用于客户端对于该站点使用的所有 IP 地址，而您的规则也不会实现预期结果。
- 一些 FQDN DNS 条目的生存时间 (TTL) 值非常小。这会导致查询表频繁地进行重新编译，从而可能会影响总体系统性能。

- 如果编辑的规则正在使用中，所做的更改不会应用于Snort不再检查的已建连接。此新规则用于根据未来的连接进行匹配。此外，如果Snort当前正在检查连接，它可以将更改的匹配或操作条件应用于现有连接。如果您需要确保将所做的更改应用于当前的所有连接，您可以登录设备CLI并使用 **clear conn** 命令终止已建连接，但前提是，连接源稍后将尝试重新建立连接，并根据新规则进行相应匹配。
- 系统需要 3 至 5 个数据包才能识别连接中的应用或 URL。因此，正确的访问控制规则可能不会立即匹配给定连接。但是，一旦应用/URL 已知，系统会根据匹配规则处理连接。对于加密连接，这发生于 SSL 握手中的服务器证书交换之后。
- 对于在用于应用识别的连接中没有负载的数据包，系统会应用默认策略操作。
- 尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。例如，如果仅将安全区条件留空，而不是创建包含所有接口的区域，则系统可以更有效地匹配所有接口的流量。指定多个条件时，系统必须匹配您指定的条件内容的各组合。
- 如果为源或目标条件指定 IP 地址，请不要在同一规则中混合使用 IPv4 和 IPv6 地址。而是为 IPv4 和 IPv6 地址创建单独的规则。
- 运行时，威胁防御 设备会根据访问规则中使用的任何网络对象的内容，将访问控制规则扩展为多个访问控制列表条目。您可以通过启用对象组搜索来减少搜索访问规则所需的内存。启用对象组搜索后，系统不会扩展网络对象，而是根据这些组定义在访问规则中搜索匹配项。对象组搜索不会影响访问规则的定义方式或它们在 设备管理器中的显示方式，而只会影响将连接与访问控制规则匹配时设备如何对其进行解释和处理。

  启用对象组搜索可以降低包含网络对象的访问控制策略的内存要求。但是，请务必注意，对象组搜索还可能会降低规则查找性能，从而提高 CPU 利用率。您应该在 CPU 影响与降低特定访问控制策略的内存要求之间取得平衡。在大多数情况下，启用对象组搜索可提高网络运营性能。

  可执行 **object-group-search access-control** 命令来通过使用 FlexConfig 设置此选项；可在取消模板中使用该命令的 **no** 形式。

  从版本 7.2 开始，默认情况下会在新部署上启用此功能，但不会在升级后的系统上自动启用。
- 违反相关 RFC 的 GRE 隧道将被丢弃。例如，如果 GRE 隧道在保留位中包含非零值，则与 RFC 相反，它将被丢弃。如果需要允许不合规的GRE隧道，则需要使用远程管理器并配置信任会话的预过滤器规则。不能使用 设备管理器配置预过滤器规则。

配置访问控制策略

使用访问控制策略可监控对网络资源的访问。该策略包含一系列有序的规则，按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件条件的第一个规则。如果没有匹配流量的规则，则应用页面底部显示的默认操作。

要配置访问控制策略，请依次选择**策略** > **访问控制**。

访问控制表将按顺序列出所有规则。对于每条规则：

- 点击最左列规则编号旁边的>按钮，可打开规则图表。图表可帮助您查看规则控制流量的方式。再次点击该按钮可关闭图表。
- 大多数单元格允许行内编辑。例如，您可以点击操作选择不同的操作，或者点击某个源网络对象以添加或更改源条件条件。
- 要移动规则，请将鼠标悬停在规则上，直到显示移动图标 ()，然后点击规则并将其拖放到新位置。您还可以通过编辑规则并在**顺序**列表中选择新位置来移动规则。一定要按您想要处理它们的顺序排列这些规则。特定规则应该靠近顶部，特别是定义一般规则例外情况的规则
- 最右列包含规则的操作按钮；将鼠标悬停在该单元格上可查看按钮。您可以编辑 () 或删除 () 规则。
- 点击**访问控制设置** () 按钮，以配置应用于访问控制策略而不是策略中特定规则的设置。
- 点击表格上方的**切换命中计数**图标 ()，添加或删除表中的命中计数列。命中计数列位于名称列的右侧，显示规则的总命中计数以及最后一次命中的日期和时间。点击切换按钮可即刻获取命中计数信息。点击**刷新**图标 () 可获取最新信息。
- 如果有任何规则存在问题，例如，因为删除或更改了URL类别而出现问题，请点击搜索框旁边的**查看问题规则**链接，对表格进行过滤，仅显示存在问题的规则。请编辑并更正（或删除）这些规则，以便它们可提供所需的服务。

以下主题介绍如何配置策略。

配置默认操作

如果连接未匹配特定访问规则，则由访问控制策略的默认操作来处理该连接。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 点击**默认操作**字段的任意位置。

步骤 3 选择应用于匹配流量的操作。

- **信任** - 允许流量，而无需进行任何类型的进一步检测。

- **允许** - 允许流量接受入侵策略检测。
- **阻止** - 无条件地丢弃流量。不检测流量。

步骤 4 如果操作为**允许**请选择一条入侵策略。

有关策略选项的说明，请查看入侵策略设置，第 486 页。

步骤 5 （可选。）针对默认操作配置日志记录。

要在控制面板数据或事件查看器中包括匹配默认操作的流量，必须对匹配默认操作的流量启用日志记录。请参阅日志记录设置，第 487 页。

步骤 6 点击**确定 (OK)**。

配置访问控制策略设置

您可以配置应用于访问控制策略而不是策略中特定规则的设置。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 点击**访问策略设置** (⚙) 按钮。

步骤 3 配置设置：

- **TLS 服务器身份发现**- TLS 1.3 加密大多数握手消息，因此证书信息不容易获得。对于使用 TLS 1.3 加密的流量，要匹配使用应用或 URL 过滤的访问规则，系统必须获取服务器的明文证书。如果启用此选项，系统将根据客户端 Hello 数据包中的 IP 地址和服务器名称指示 (SNI) 检查站点的证书是否存储在缓存中。如果不可用，系统将使用 TLS 1.2 探测器获取证书，然后可将其用于应用/URL 类别和信誉识别。建议您启用此选项，以确保将加密连接与正确的访问控制规则进行匹配。此设置仅获取证书；连接保持加密状态。启用此选项即可获取 TLS 1.3 证书；您无需创建相应的 SSL 解密规则。但是，除了访问控制处理之外，缓存的证书还用于更有效的解密规则处理。
- **DNS 流量的信誉实施** - 启用此选项可将 URL 过滤类别和信誉规则应用于 DNS 查找请求。如果查找请求中的完全限定域名 (FQDN) 具有要阻止的类别和信誉，系统会阻止 DNS 回复。由于用户未收到 DNS 解析，因此用户无法完成连接。使用此选项可将 URL 类别和信誉过滤应用于非 Web 流量。有关详细信息，请参阅DNS 请求过滤，第 472 页。

步骤 4 点击**确定 (OK)**。

配置访问控制规则

使用访问控制规则可监控对网络资源的访问。访问控制策略中的规则按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件条件的第一个规则。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 执行以下任一操作：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

要删除不再需要的规则，请点击该规则的删除图标 ( )。

步骤 3 在**顺序**中，选择要将该规则插入在已排序有序规则列表插入该规则的位置。

先匹配的规则先应用，所以您必须确保流量匹配条件条件较具体的规则显示在次之用来匹配流量的较通用条件条件的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

步骤 4 在**名称**中输入规则的名称。

名称不能包含空格。可以使用字母数字字符和以下特殊字符：+ . _ -

步骤 5 选择应用于匹配流量的操作。

- **信任** - 允许流量，而无需进行任何类型的进一步检测。
- **允许** - 允许流量，不受策略中的入侵及其他检测设置约束。
- **阻止** - 无条件地丢弃流量。不检测流量。

步骤 6 使用以下选项卡的任意组合，定义流量匹配条件：

- **源/目的地** - 流量传输所用的安全区（接口）、IP 地址或该 IP 地址的国家/地区或大洲（地理位置）、分配给该地址的安全组标记(SGT)或者流量中使用的协议和端口。默认设置为任何区域、地址、地理位置、SGT、协议和端口。请参阅 源/目标条件，第 481 页。
- **应用** - 应用或按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认设置为任何应用。请参阅应用条件，第 483 页。
- **URL** - Web 或 DNS 查找请求的 URL 或 URL 类别。默认设置为任何 URL。请参阅 URL 条件，第 484 页。
- **用户** - 身份源，用户或用户组。身份策略决定了用户和组的信息是否可用于流量匹配。只有配置身份策略，才能使用此条件条件。请参阅 用户条件，第 485 页。

要修改条件，请点击该条件内的 + 按钮，选择所需的对象或元素，然后在弹出对话框中点击**确定(OK)**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象**。点击对象或元素对应的**x**，可将其从策略中移除。

向访问控制规则中添加条件时，请考虑以下提示：

- 您可以为每个规则配置多个条件。要使规则应用于流量，流量必须匹配该规则中的所有条件。例如，可以使用单一规则对特定主机或网络执行 URL 过滤。
- 最多可以为规则中的每个条件添加50个标准。匹配某个条件所有条件标准的流量满足该条件。例如，您可以使用单一规则为最多50个应用或应用过滤器执行应用控制。因此，单一条件中的项目之间为 OR 关系，但不同条件类型之间（例如，源/目的和应用之间）为 AND 关系。
- 有些功能需要您启用适当的许可证。

步骤 7 （可选。）对于使用“允许”操作的策略，可以对未加密流量配置进一步的检测。点击以下任一链接：

- **入侵策略** - 依次选择**入侵策略** > **开**，然后选择入侵检测策略，可检测流量中是否存在入侵和漏洞攻击。请参阅入侵策略设置，第 486 页。
- **文件策略** - 选择文件策略可检测流量中是否存在包含恶意软件的文件和应被阻止的文件。请参阅文件策略设置，第 486 页。

步骤 8 （可选。）针对规则配置日志记录。

默认情况下，对于匹配规则的流量不会生成连接事件，但如果选择了文件策略，则默认生成文件事件。您可以更改此行为。要在控制面板数据或事件查看器中包括匹配策略的流量，必须对匹配策略的流量启用日志记录。请参阅日志记录设置，第 487 页。

无论匹配访问规则的日志记录配置如何，系统始终为设置为丢弃或发送警报的入侵规则生成入侵事件。

步骤 9 点击**确定 (OK)**。

源/目标条件

访问规则的“源/目标”条件定义用于传递流量的安全区（接口）、IP 地址或 IP 地址的国家/地区或大洲（地理位置）、分配给地址的安全组标记 (SGT) 或流量中使用的协议和端口。默认设置为任何区域、地址、地理位置、SGT、协议和端口。

要修改条件，请点击该条件内的 + 按钮，选择所需的对象或元素，然后点击**确定**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象**。点击对象或元素对应的 **x**，可将其从策略中移除。

您可以通过以下条件来标识规则中要匹配的源和目标。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至**目标区域**。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至**源区域**。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保到达内部主机的所有流量均进行入侵检测，则应将内部区域选为**目标区域**，同时将源区域保留为空。要在规则中实施入侵过滤，则规则操作必须为**允许**，并且必须在该规则中选择入侵策略。

注释 不能在同一规则中搭配使用被动和路由安全区。此外，被动安全区只能被指定为源区域，不能作为目标区域。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置**源网络**。
- 要匹配流向 IP 地址或地理位置的流量，请配置**目标网络**。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络** - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。您可以使用通过完全限定域名 (FQDN) 定义地址的对象；通过 DNS 查询确定地址。
- **地理位置** - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。

注释 为了确保使用最新的地理位置数据来过滤流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

源端口、目标端口/协议

定义流量中所用协议的端口对象。对于 TCP/UDP，这可能包括端口。对于 ICMP，可包括代码和类型。

- 要匹配来自协议或端口的流量，请配置**源端口**。源端口只能为 TCP/UDP。
- 要匹配流向协议或端口的流量，请配置**目标端口/协议**。如果仅将目标端口添加至条件，则可以添加使用不同传输协议的端口。ICMP 和其他非 TCP/UDP 规格仅可用于目标端口，不允许用于源端口。
- 要同时匹配来自特定 TCP/UDP 端口的流量和流向特定 TCP/UDP 端口的流量，请配置源端口和目标端口。如果同时将源和目标端口添加至条件，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

源 SGT 组、目的地 SGT 组

从身份服务引擎 (ISE) 下载的标识分配给流量的安全组标记 (SGT) 的 SGT 组对象。仅当定义 ISE 身份源时，才能使用这些对象；否则，此部分将不会显示。有关如何使用 SGT 进行访问控制的详细信息，请参阅如何使用 TrustSec 安全组标记控制网络访问，第 491 页。

- 要匹配源具有组中定义的一个 SGT 的流量，请配置**源 SGT 组**。
- 要匹配流向具有组中定义的一个 SGT 的目的地的流量，请配置**目的地 SGT 组**。
- 如果同时向一条规则添加源和目的地 SGT 条件，匹配规则的流量必须来自具有其中一个指定标记的源并流向其中一个标记目的地。

应用条件

访问规则的“应用”条件对 IP 连接中使用的应用进行定义，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认设置为任何应用。

虽然您可以在规则中指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

另外，思科会通过系统和漏洞数据库 (VDB) 更新频繁更新和添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

您可以直接在规则指定应用和过滤器，也可以创建定义这些特征的应用过滤器对象。规格相当，尽管如果要创建复杂规则，使用对象可便于遵守每个条件 50 个项目的系统限制。

要修改应用和过滤器列表，请点击该条件内的 + 按钮，选择在单独选项卡中列出的相应应用或应用过滤器对象，然后在弹出对话框中点击**确定**。在任一选项卡中，您可以点击**高级过滤器**选择过滤器条件或帮助您搜索特定应用。点击应用、过滤器或对象的 **x**，可将其从策略中移除。点击**另存为过滤器**链接，可将尚不是对象的组合条件另存为新应用过滤器对象。

注释 如果所选应用已由 VDB 更新删除，则会在应用名称后显示“（已弃用）”。必须从过滤器中删除这些应用，否则将阻止后续部署和系统软件升级。

您可以使用以下**高级过滤器**条件来标识规则中要匹配的应用或过滤器。这些元素与应用过滤器对象中使用的元素相同。

注释 单个过滤器条件中的多个选项具有 OR 关系。例如，风险高 OR 非常高。过滤器之间的关系是 AND，因此是风险高 OR 非常高，AND 业务相关性低 OR 非常低。在选择过滤器时，显示屏中的应用列表更新，只显示符合条件的应用。您可以使用这些过滤器来帮助查找要单独添加的应用，或确认是否要选择所需的过滤器以添加到规则中。

风险

应用所用的用途可能违反组织安全策略的可能性，从非常低到非常高。

业务相关性

在组织的业务运营环境（非娱乐性）下使用应用的可能性，从非常低到非常高。

类型

应用类型：

- **应用协议** - 应用协议（例如 HTTP 和 SSH），代表主机之间的通信。
- **客户端协议** - 客户端（例如 Web 浏览器和邮件客户端），代表主机上运行的软件。
- **Web 应用** - Web 应用（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL。

类别

说明应用的最基本功能的应用通用分类。

标记

关于应用的其他信息，与类别类似。

对于加密流量，系统可以仅使用标记有 **SSL 协议**的应用识别和过滤流量。只有在未加密或已解密的流量中才能检测到没有此标记的应用。此外，系统仅将**已解密的流量**标记分配给可在已解密的流量中检测到的应用，而不会将它们分配给加密或未加密的流量中检测到的应用。

应用列表（显示屏底部）

在从列表上方的选项中选择过滤器时，此列表将进行更新，所以您可查看当前符合过滤器的应用。在计划将过滤器条件添加到规则中时，使用此列表可确认您的过滤器是否针对所需的应用。如果您计划添加特定应用，请从此列表中选择它们。

URL 条件

访问规则中的 URL 条件对 Web 请求中使用的 URL 或请求的 URL 所属的类别进行定义。对于类别匹配，您还可以指定要允许或阻止的站点的相对信誉。默认设置为允许所有 URL。

如果启用 DNS 查找请求过滤，则类别和信誉设置也会应用于查找请求中的完全限定域名 (FQDN)。仅类别和信誉设置适用于 DNS 请求过滤。忽略手动 URL 过滤。

URL 类别和信誉可供您快速创建访问控制规则的 URL 标准。例如，您可阻止所有赌博网站或不受信任的社交网站。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止。

使用类别和信誉数据还会简化策略创建和管理。此方法可保证系统将按预期控制网络流量。最后，由于思科的威胁智能会不断更新有关新 URL 以及现有 URL 的新类别和新风险的信息，因此可以确保系统使用最新信息来过滤所请求的 URL。代表安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的恶意站点出现和消失的速度可能比您更新和部署新策略的速度要快。

要修改 URL 列表，请点击该条件内的 + 按钮，使用以下任一方法选择所需的类别或 URL。点击类别或对象的 **x**，可将其从策略中删除。

URL 选项卡

点击 +，选择 URL 对象或组，然后点击**确定 (OK)**。如果所需的对象不存在，可以点击**创建新 URL (Create New URL)**。

注释 在配置特定目标站点的 URL 对象之前，请仔细阅读有关手动 URL 过滤的信息。

“类别”选项卡

点击 +，选择所需的类别，然后点击**确定**。

有关类别说明，请参阅 https://www.talosintelligence.com/categories。

默认为将规则应用于每个选定类别的所有 URL，不考虑信誉。要根据信誉限制规则，请点击每个类别的向下箭头，取消选中**任何**复选框，然后使用**信誉**滑块选择信誉级别。信誉滑块的左侧指示要允许的站点，右侧是要阻止的站点。如何使用信誉取决于规则操作：

- 如果该规则阻止或监控网络访问，则选择某个信誉级别也会选择高于该级别的所有信誉。例如，如果将规则配置为阻止或监控**问题站点**（第 2 级），该规则还会自动阻止或监控**不受信任**（第 1 级）站点。
- 如果该规则允许网络访问，则选择某个信誉级别也会选择低于该级别的所有信誉。例如，如果您将规则配置为允许**可靠站点**（第 4 级），该规则还会自动允许**受信任**（第 5 级）站点。

选择**包含信誉未知的站点**选项，可使具有未知信誉的URL包括在信誉匹配项中。新站点通常未评级，并且站点的信誉可能会由于其他原因而未知或无法确定。

检查 URL 的类别

您可以检查特定 URL 的类别和信誉。在**待检查的 URL** 框中输入 URL，然后点击**前往**。系统会将您转至外部网站以查看结果。如果您对分类持有不同意见，请点击**提交 URL 类别争议**链接，将您的想法反馈给我们。

用户条件

访问规则的“用户”条件对IP连接的用户或用户组进行了定义。只有配置身份策略和相关联的目录服务器，才能在访问规则中包括用户或用户组条件。

您的身份策略决定是否收集某个特定连接的用户身份。如果建立了身份，则主机的IP地址与所识别的用户相关联。因此，源IP地址映射到用户的流量将被视为来自该用户。IP数据包本身不包含用户身份信息，所以此 IP 地址到用户的映射是最接近的近似值。

由于最多可以向规则中添加50个用户或组，所以选择组比选择单个用户通常更有意义。例如，您可以创建一条规则允许“工程”组访问开发网络，并创建一条后续规则拒绝对该网络的所有其他访问。然后，要将该规则应用于新工程师，您只需添加将工程师添加到目录服务器的“工程”组即可。

您还可以选择身份源，以应用于该源中的所有用户。因此，如果您支持多个 Active Directory 域，您可以根据域提供不同的资源访问。

要修改用户列表，请点击该条件内的 + 按钮，并使用以下任一方法选择所需的身份。点击身份对应的 **x**，可将其从策略中删除。

- **身份源** - 选择身份源，例如 AD 领域或本地用户数据库，以将规则应用于从所选源获取的所有用户。如果所需的领域尚不存在，请点击**创建新身份领域**并立即创建。
- **组** - 选择所需的用户组。只有在目录服务器中配置了组，才能使用组。如果您选择了某个组，规则将应用于该组的所有成员，包括子组。如果要区别对待某个子组，您需要针对该子组创建一条单独的访问规则，并将其置于访问控制策略中适用于父组的规则之上。
- **用户** - 选择单个用户。用户名使用身份源作为前缀，例如“领域\用户名”。

  特殊身份领域中存在一些内置用户：

  - **身份验证失败** - 系统提示用户进行身份验证，但用户未在允许的最大尝试次数内输入有效的用户名/密码对。身份验证失败本身不会阻止用户访问网络，但您可以写入访问规则来限制这些用户访问网络。
  - **访客** - “访客”用户与“身份验证失败”用户类似，只是您的身份规则配置为将这些用户称为“访客”。系统提示“访客”用户进行身份验证，但他们在最大尝试次数内未成功通过身份验证。
  - **无需身份验证** - 系统不提示用户进行身份验证，因为该类用户的连接与指定不进行身份验证的身份规则匹配。
  - **未知** - 没有用户的 IP 地址映射，也没有身份验证失败的记录。通常，这意味着尚无来自该地址的 HTTP 流量。

入侵策略设置

Cisco 通过防火墙系统提供多种入侵策略。Cisco 思科 Talos 情报小组 (Talos) 交付的一些入侵策略由 Cisco.Talos 设计，其设定了入侵和预处理器规则的状态和高级设置。对于允许流量的访问控制规则，您可以选择入侵策略来检测流量中是否存在入侵和攻击程序。入侵策略根据模式检查已解码数据包中是否存在攻击，并且可以阻止或修改恶意流量。

运行 Snort 2 时，这些是唯一可用的策略，并且您无法修改这些策略。不过，您可以更改要对给定规则执行的操作，如更改入侵规则操作 (Snort 2)，第 522 页中所述。

运行 Snort 3 时，您可以选择其中一个策略，也可以创建自己的入侵策略。

要启用入侵检测，请选择**入侵策略** > **开**，然后选择所需策略。点击下拉列表中策略的信息图标，可查看每个策略的说明。

有关预定义策略的详细信息，请参阅系统定义的网络分析和入侵策略，第 498 页。

文件策略设置

使用文件策略来检测恶意软件，或 恶意软件，使用恶意软件防御。另外，您还可以使用文件策略执行文件控制，以允许控制特定类型的所有文件，而不考虑文件中是否包含恶意软件。

恶意软件防御使用 Cisco Secure Malware Analytics 云 检索网络流量中检测到的潜在恶意软件的处置，并获取本地恶意软件分析和文件预分类更新。管理接口必须可连接互联网，以便访问 Cisco Secure

Malware Analytics 云 并搜索恶意软件。当设备检测到符合条件的文件时，它将使用该文件的 SHA-256 散列值来查询 Cisco Secure Malware Analytics 云 中是否存在该文件的处置。可能的处置包括：

- 恶意软件 - Cisco Secure Malware Analytics 云 将文件归类为恶意软件。如果其中的任何文件为恶意软件，存档文件（例如 zip 文件）会被标记为恶意软件。
- 安全 - Cisco Secure Malware Analytics 云 将文件归类为安全，不含恶意软件。如果其中的所有文件都安全，存档文件将会标记为安全。
- 未知 - Cisco Secure Malware Analytics 云 尚未指定该文件的处置。如果其中的任何文件属于未知状态，存档文件会被标记为未知。
- 不可用 - 系统无法通过查询 Cisco Secure Malware Analytics 云 来确定文件的处置。您可能看到很少一部分事件为此处置；这是预期行为。如果您连续看到许多“不可用”事件，请确保管理地址的互联网连接正常运行。

可用的文件策略

您可以选择下列文件策略之一：

- **无** - 不评估传输的文件中是否存在恶意软件，且不阻止特定的文件。对于文件传输受信任或不可能传输文件的规则或您相信自己的应用或URL过滤可适当保护网络的规则，请选择此选项。
- **阻止所有恶意软件**- 查询 Cisco Secure Malware Analytics 云 以确定通过网络传输的文件是否包含恶意软件，然后阻止存在威胁的文件。
- **全部执行云查找**- 查询 Cisco Secure Malware Analytics 云以获取和记录通过网络传输的文件的处置，同时仍允许文件传输。
- （**自定义文件策略**）- 可以使用 威胁防御 API filepolicies 资源和其他 FileAndMalwarePolicies 资源（例如 filetypes、filetypecategories、ampcloudconfig、ampservers 和 ampcloudconnections）创建您自己的文件策略。创建策略并部署更改后，可以在编辑 设备管理器中的访问控制规则时选择策略。选择策略说明后，策略说明会显示在策略下方。

日志记录设置

访问规则的日志记录设置确定是否对匹配规则的流量发出连接事件。只有启用日志记录，才能在事件查看器中查看与该规则相关的事件。另外，您还必须启用日志记录，才能使匹配流量反映到可用于监控系统的各种控制面板中。

您应该根据您组织的安全和合规性需求记录连接。如果您的目标是限制所生成事件的数量和提高性能，则只能启用对分析至关重要的连接的日志记录。然而，如果出于分析目的，您想要广泛了解网络流量，则可启用其他连接的日志记录。

注意 在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件使数据库不堪重负。在对“阻止”规则启用日志记录之前，请考虑该规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口。

您可以配置以下日志记录操作。

选择日志操作

可以选择下列操作之一：

- **在连接开始和结束时记录** - 在连接开始和结束时发出事件。由于连接结束事件包含连接开始事件所含的一切，以及连接期间可能收集的所有信息，所以思科建议不要对允许的流量选择此选项。记录两种事件可能会影响系统性能。但是，这是针对阻止的流量唯一允许的选项。
- **在连接结束时记录** - 如果要在连接结束时启用连接日志记录（建议对允许或受信任的流量执行此操作），请选择此选项。
- **在连接时不执行日志记录** - 选择此选项，可对规则禁用日志记录。这是默认值。

注释 当访问控制规则调用的入侵策略检测到入侵并生成入侵事件时，系统会在发生入侵的位置自动记录连接终止，无论该规则的日志记录配置如何。对于入侵受阻的连接，连接日志中的连接操作为**阻止**，原因为**入侵阻止**，即使执行入侵检测，也必须使用“允许”规则。

文件事件

如果要对禁止文件或恶意软件事件启用日志记录，请选择**日志文件**。只有在规则中选择了文件策略，才能配置此选项。如果对规则选择了文件策略，则该选项默认处于启用状态。思科建议您将此选项保留为已启用。

当系统检测到受禁文件时，它会自动记录以下类型的事件之一：

- 文件事件，代表检测到或阻止的文件，包括恶意软件文件。
- 恶意软件事件，仅代表检测到或阻止的恶意软件文件。
- 可追溯的恶意软件事件，在之前检测到的文件的恶意软件处置变更时生成。

对于文件受阻的连接，连接记录中的连接操作为**阻止**，即便要执行文件和恶意软件检测，也必须使用“允许”规则。连接原因是**文件监控**（检测到某种文件类型或恶意软件）或者是**恶意软件阻止**或**文件阻止**（文件被阻止）。

将连接事件发送到

如果要将事件副本发送到外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**创建新系统日志服务器**，并创建对象。（要对系统日志服务器禁用日志记录，请从服务器列表中选择**任何**）。

由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

此设置仅适用于连接事件。要将入侵事件发送到系统日志，请在入侵策略设置中配置服务器。要将文件/恶意软件事件发送到系统日志，请在**设备** > **系统设置** > **日志记录设置**中配置服务器。

监控访问控制策略

以下主题介绍如何监控访问控制策略。

在控制面板中监控访问控制统计信息

监控控制面板上的大多数数据与您的访问控制策略直接相关。请参阅监控流量和系统控制面板，第 98 页。

- **监控 (Monitoring)** > **访问和 SI 规则 (Access And SI Rules)**显示点击量最高的访问规则及安全智能规则等效对象和相关统计信息。
- 可以在**网络概述**、**目标**和**区域**控制面板找到常规统计信息。
- 可以在 **URL 类别**和**目标**控制面板找到 URL 过滤结果。必须至少有一个 URL 过滤策略，才可在 **URL 类别**控制面板看到任何信息。
- 可以在**应用**和 **Web 应用**控制面板找到应用过滤结果。
- 还可以在**用户**控制面板找到基于用户的统计信息。只有实施身份策略才能收集用户信息。
- 可以在**攻击者**和**目标**控制面板找到入侵策略统计信息。必须将入侵策略应用于至少一个访问控制规则，才能在这些控制面板上看到任何信息。
- 可以在**文件日志**和**恶意软件**控制面板找到文件策略和恶意软件过滤统计信息。必须将文件策略应用于至少一个访问控制规则，才能在这些控制面板上看到任何信息。
- **监控** > **事件**还显示与访问控制规则相关的连接和数据的事件。

检查规则命中计数

您可以查看每个访问控制规则的命中计数。命中计数表示连接与规则匹配的频率。可以使用此信息来确定最活跃的规则和不活跃的规则。

通过重新启动和升级，计数仍然存在。

您还可以使用 **show rule hits** 命令在设备 CLI 中查看规则命中计数信息。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 点击**切换命中计数**图标 ( )。

命中计数列位于名称列的右侧，显示规则的总命中计数以及最后一次命中的日期和时间。点击切换按钮可即刻获取命中计数信息。

您可以使用命中计数信息执行以下操作：

- 在按钮左侧，您将看到有关命中次数最后更新时间的信息。点击**刷新**图标()可获取最新数字。
- 要打开给定规则命中计数的详细视图，请点击表中的命中计数数字，打开命中计数对话框。命中计数信息包括命中数和与规则匹配的最后一次连接的日期和时间。点击**重置**链接可将计数器重置为零。

  如果您想要一次性重置所有规则的命中计数，请打开与设备的 SSH 会话并发布 **clear rule hits** 命令。
- 再次点击**切换命中计数**图标 ()，从表中删除命中计数列。

监控访问控制系统日志消息

除了在事件查看器中查看事件外，您还可以配置访问控制规则、入侵策略、文件/恶意软件策略和安全智能策略，以将事件发送到系统日志服务器。事件使用以下消息 ID：

- 430001 - 入侵事件。
- 430002 - 连接开始时记录的连接事件。
- 430003 - 在连接结束时记录的连接事件。
- 430004 - 文件事件。
- 430005 - 恶意软件事件。

在 CLI 中监控访问控制策略

您还可以打开 CLI 控制台或登录设备 CLI，使用以下命令获取有关访问控制策略和统计信息的更多详细信息。

- **show access-control-config** 显示访问控制规则的摘要信息以及每个规则的命中计数。
- **show access-list** 显示基于访问控制规则生成的访问控制列表 (ACL)。ACL 提供初始过滤器并尝试尽可能提供快速决策，以使应丢弃的连接不需要接受检测（从而避免不必要的资源消耗）。此信息包括命中计数。
- **show rule hits** 显示汇总命中计数，这比使用 **show access-control-config** 和 **show access-list** 显示的计数更加准确。如果您想要重置命中次数，请使用 **clear rule hits** 命令。
- **show snort statistics** 显示 Snort 检测引擎（主要检测程序）的相关信息。Snort 实施应用过滤、URL 过滤、入侵防护以及文件和恶意软件过滤。
- **show conn** 显示当前通过接口建立的连接的相关信息。
- **show traffic** 显示流过每个接口的流量的相关统计信息。
- **show ipv6 traffic** 显示流过设备的 IPv6 流量的相关统计信息。

访问控制示例

使用案例章节涵盖多个实施访问控制规则的示例。请参阅下面的示例：

- 如何深入了解您的网络流量，第 44 页。此示例展示收集整体的连接和用户信息的一些基本概念。
- 如何阻止威胁，第 51 页。此示例展示如何应用入侵策略。
- 如何阻止恶意软件，第 55 页。此示例展示如何应用文件策略。
- 如何实施可接受使用策略（URL 过滤），第 58 页。此示例展示如何执行 URL 过滤。
- 如何控制应用的使用，第 63 页。此示例展示如何执行应用过滤。
- 如何添加子网，第 66 页。此示例展示如何将新的子网集成到整个网络，包括允许流量所需的访问规则。
- 如何被动监控网络上的流量，第 71 页

以下是其他示例。

如何使用 TrustSec 安全组标记控制网络访问

如果使用思科身份服务引擎 (ISE) 定义并使用安全组标记 (SGT) 来对 Cisco TrustSec 网络中的流量进行分类，则可以编写使用 SGT 作为匹配条件的访问控制规则。因此，可以基于安全组成员身份阻止或允许访问，而不是直接使用 IP 地址。

关于安全组标记 (SGT)

在思科身份服务引擎(ISE)中，可以创建安全组标记(SGT)，并将主机或网络IP地址分配至各标记。您还可以将 SGT 分配给用户账户，并将 SGT 分配给用户流量。如果网络中的交换机和路由器配置为执行此操作，则在数据包进入ISE（Cisco TrustSec 云)控制的网络时，这些标记会分配给数据包。

在 设备管理器中配置 ISE 身份源时， 威胁防御 系统会自动从 ISE 下载 SGT 列表。然后，可以使用 SGT 作为访问控制规则中的流量匹配条件。

例如，可以创建生产用户标记，并将 192.168.7.0/24 网络与标记相关联。如果将该网络用于用户终端（例如笔记本电脑、Wi-fi 客户端等），这将适用。可以创建用于生产服务器的单独标记，并将相关服务器或子网的IP地址分配给该标记。然后，在威胁防御中，可以根据标记允许或阻止从用户网络到生产服务器的访问。如果稍后修改 ISE 中标记所关联的主机或网络地址，则无需更改定义用于 威胁防御 设备的访问控制规则。

威胁防御 评估 SGT 作为访问控制规则的流量匹配条件时，会使用以下优先级：

1. 数据包中定义的源 SGT 标记（如有）。对于数据包中的 SGT 标记，必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息，请参阅 ISE 文档。
2. 分配给用户会话的 SGT，从 ISE 会话目录下载。您需要启用此选项才能侦听此类 SGT 匹配的会话目录信息，但是，当您首次创建 ISE 身份源时，此选项会默认打开。SGT 可以与源或目标相

匹配。尽管非必需，但您通常还会使用 ISE 身份源和 AD 域来设置被动身份验证身份规则，以收集用户身份信息。

3. 使用 SXP 下载的 SGT-IP 地址映射。如果 IP 地址在 SGT 范围内，则流量与使用 SGT 的访问控制规则相匹配。SGT 可以与源或目标相匹配。

   ISE 使用安全组交换协议 (SXP) 将 IP 到 SGT 的映射数据库传播至网络设备。当您将 威胁防御 设备配置为使用 ISE 服务器时，必须打开该选项才能从 ISE 侦听 SXP 主题。因此，威胁防御 设备直接从 ISE 了解安全组标记和映射，且每当 ISE 发布更新的安全组标记和映射时均会收到通知。这可确保安全组标签和映射列表在设备上保持最新状态，以便 威胁防御 能够有效地实施 ISE 中定义的策略。

基于安全组标记 (SGT) 配置访问控制

要配置使用安全组标记 (SGT) 作为匹配条件的访问控制规则，必须先配置设备以从 ISE 服务器获取 SGT 映射。

以下程序根据您想要获取 ISE 中定义的所有映射（包括通过 SXP 发布的 SGT 到 IP 地址映射）来解释端到端流程。或者：

- 如果要仅使用数据包中的 SGT 信息，而不使用从 ISE 下载的映射，只需创建 SGT 组动态对象并将其用作访问控制规则中的源 SGT 条件。请注意，在这种情况下，您只能使用 SGT 标记作为源条件；这些标记永远不会匹配目标条件。
- 如果仅希望在数据包中使用 SGT 和用户会话 SGT 映射，则无需打开该选项以订阅 ISE 身份源中的 SXP 主题，也无需配置 ISE 以发布 SXP 映射。您可以将此信息用于源匹配条件和目标匹配条件。

开始之前

假设您已在网络中配置 Cisco TrustSec，而您只是将 威胁防御 设备作为策略实施点添加。如果尚未部署 Cisco TrustSec，请从 ISE 开始并配置您的网络，然后返回至此过程。说明 Cisco TrustSec 超出本文档范围。

过程

步骤 1 确保已定义 SGT，已正确配置 ISE 以发布 SXP 主题，并且所有所需的静态映射都已部署到位。

请参阅在 ISE 中配置安全组和 SXP 发布，第 494 页。

步骤 2 更新身份服务引擎对象以侦听 SXP 主题。

您可以使用 ISE 通过 SXP 获取用户会话 SGT 映射和/或静态 SGT 到 IP 地址映射。默认情况下，配置 ISE 身份源时，仅获取用户会话映射；必须打开该选项才能从 ISE 侦听 SXP 主题。

a) 依次选择**对象** > **身份源**。
b) 编辑 ISE 对象。如果尚未配置，请点击 + > **身份服务引擎**，并查看配置身份服务引擎，第 163 页。
c) 在**订用**下，选择 **SXP 主题**。

如果您正在使用被动身份验证或需要“用户到 SGT”映射，请确保还选择了**会话目录主题**。

d) 点击**确定 (OK)**。

步骤 3 部署更改并等待系统从 ISE 下载标记和映射。

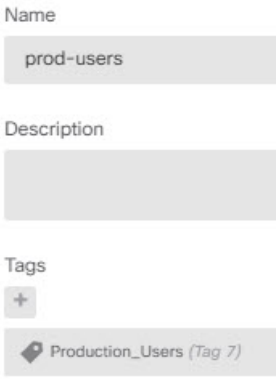
配置 ISE 身份源并部署更改后，系统会从 ISE 服务器检索安全组标记 (SGT) 信息。在部署更改之前，无法进行下载。

步骤 4 创建访问控制规则所需的 SGT 组对象。

您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

对象的数量和内容取决于要编写的访问控制规则。重复以下过程，创建您所需的所有对象。

a) 依次选择**对象** > **SGT 组**。
b) 点击 + 以添加新对象，或编辑现有对象。
c) 为新对象输入名称和说明（后者为可选项）。
d) 在**标记 (Tags)** 下，点击 + 并选择应包含在组中的所有标记。



e) 点击**确定 (OK)**。

步骤 5 创建使用 SGT 组对象的访问控制规则。

例如，以下规则允许从生产用户到生产服务器的流量。该规则完全取决于 SGT；不受源/目标接口或任何其他条件的限制。因此，该规则将动态应用于来自不同接口的流量，且在 ISE 中更改安全组成员身份。如果数据包未明确包含源 SGT，则源/目的地匹配将基于数据包 IP 地址，与从用户会话信息或从 SXP 发布的映射获取的“SGT 到 IP 地址”映射进行比较。

a) 依次选择**策略** > **访问控制**。
b) 点击 + 新建一条规则或编辑现有规则。
c) 输入规则名称并选择**允许**作为操作。

d) 在**源/目的地 (Source/Destination)** 选项卡上，点击**源 (Source)** > **SGT 组 (SGT Groups)**下的 **+**，然后选择为生产用户创建的对象。
e) 在**源/目的地 (Source/Destination)** 选项卡上，点击**目的地 (Destination)** > **SGT 组 (SGT Groups)**下的 **+**，然后选择为生产服务器创建的对象。
f) 请根据需要配置其他选项。例如，您可以启用日志记录并应用入侵策略。
g) 点击**确定 (OK)**。

步骤 6 部署配置。

在 ISE 中配置安全组和 SXP 发布

您必须在思科身份服务引擎 (ISE) 中执行许多配置，才能创建 TrustSec 策略和安全组标记 (SGT)。有关实施 TrustSec 的更完整信息，请参阅 ISE 文档。

以下操作步骤将挑选出必须在 ISE 中配置的核心设置的要点，以便 威胁防御 设备能够下载和应用静态 SGT-IP 地址映射，然后在访问控制规则中用于源 SGT 和目标 SGT 匹配。有关详细信息，请参阅 ISE 文档。

此操作步骤的屏幕截图基于 ISE 2.4。在后续版本中，这些功能的确切路径可能会发生变化，但概念和要求是相同的。虽然建议使用 ISE 2.4 或更高版本（最好是 2.6 或更高版本），但配置应从 ISE 2.2 补丁 1 开始。

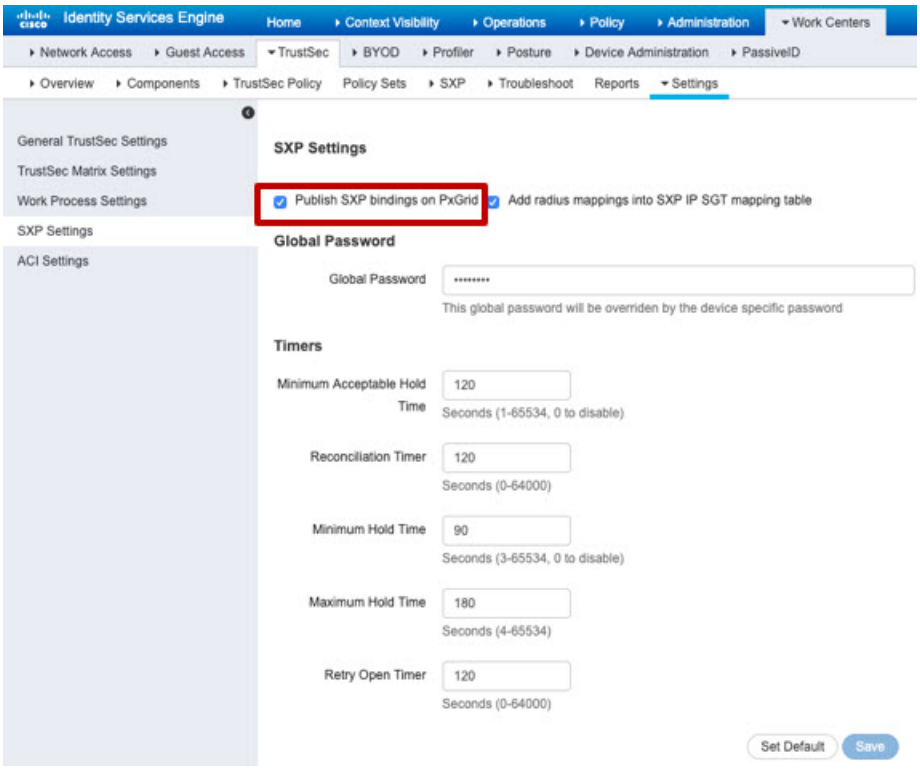
开始之前

您必须拥有 ISE Plus 许可证，才能发布从 SGT 到 IP 地址的静态映射和获取从用户会话到 SGT 的映射，以便 威胁防御 设备可以接收这些映射。

过程

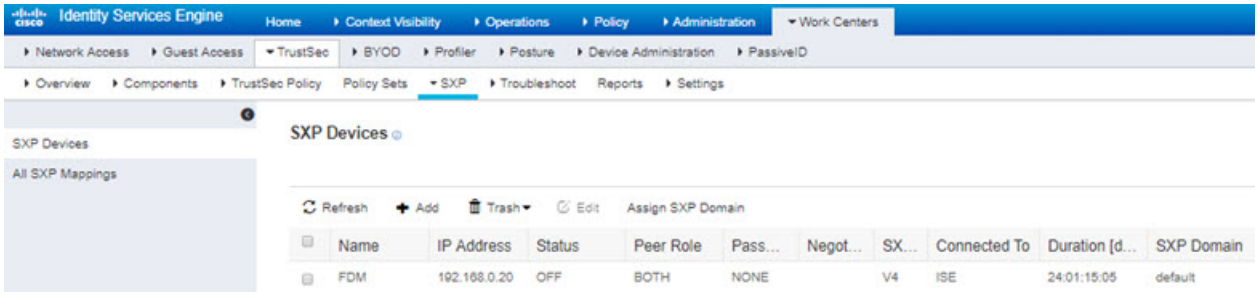
步骤 1 选择**工作中心** > **TrustSec** > **设置** > **SXP 设置**，然后选择**在 PxGrid 上发布 SXP 绑定**选项。

选择该选项后，ISE 使用 SXP 发送 SGT 映射。您必须选择此选项， 威胁防御 设备才能“收听”从列表至 SXP 主题等一切内容。必须选择此选项， 威胁防御 设备才能获取静态 SGT-IP 地址映射信息。如果您仅想使用数据包中定义的 SGT 标记或分配给用户会话的 SGT，则没有必要。

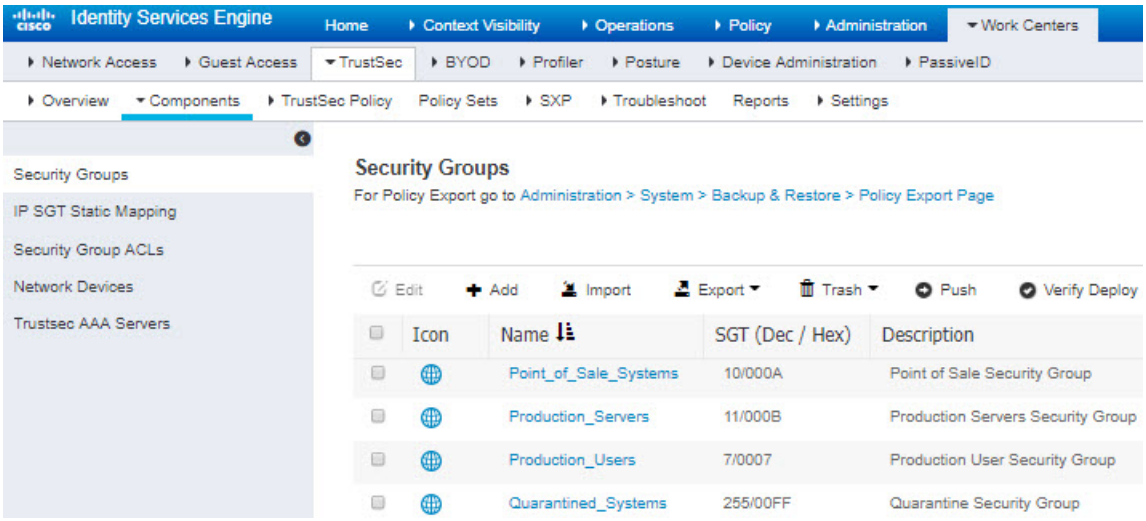


步骤 2 选择**工作中心** > **TrustSec** > **SXP** > **SXP 设备**，然后添加设备。

这并不一定是真正的设备，您甚至可以使用 威胁防御 设备的管理 IP 地址。该表只需要至少一台设备来促使 ISE 发布静态 SGT-IP 地址映射。如果您仅想使用数据包中定义的 SGT 标记或分配给用户会话的 SGT，则无需执行此步骤。

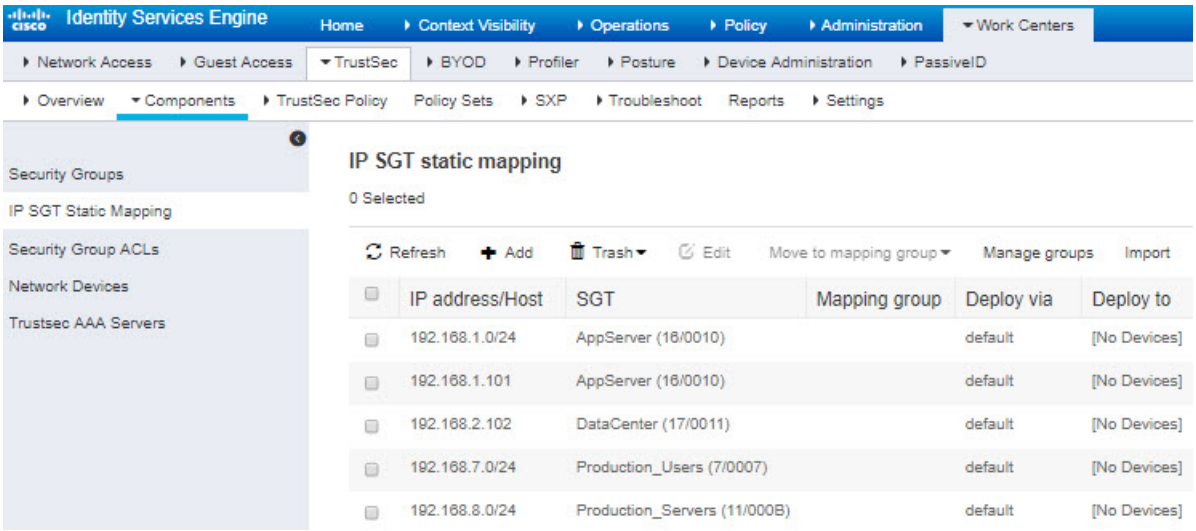


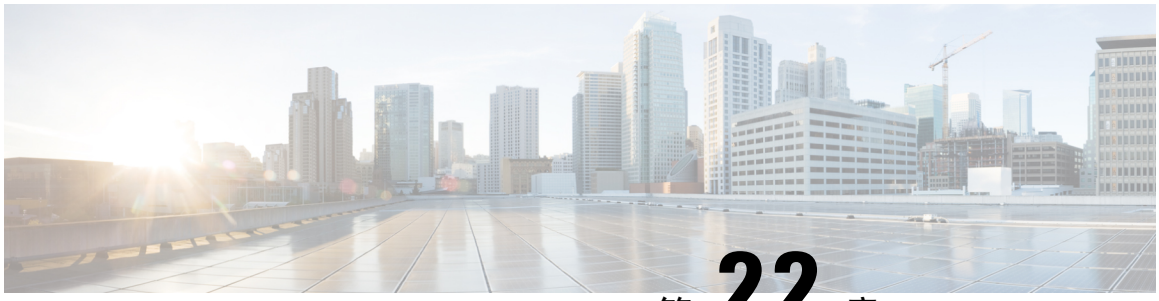
步骤 3 选择**工作中心** > **TrustSec** > **组件** > **安全组**并验证是否定义了安全组标记。按需新建。



步骤 4 选择工作中心 > **TrustSec** > 组件 > **IP SGT 静态映射**，并将主机和网络 IP 地址映射至安全组标记。

如果您仅想使用数据包中定义的 SGT 标记或分配给用户会话的 SGT，则无需执行此步骤。





第 22 章

入侵策略

以下主题说明了入侵策略和密切相关的网络分析策略 (NAP)。入侵策略包括用于检查流量中的威胁并阻止看似为攻击的流量的规则。网络分析策略控制流量预处理，通过规范化流量和识别协议异常来准备要进一步检查的流量。

由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略必须相互补充。

关于入侵和网络分析策略

网络分析和入侵策略配合使用，以检测和防止入侵威胁。

- 网络分析策略 (NAP) 监管流量如何解码和预处理，以便可以进一步对其进行评估，尤其是对于可能指示入侵尝试的异常流量。
- 入侵策略使用入侵和预处理器规则（统称为入侵规则），根据模式检测已解码数据包是否存在攻击。入侵规则可防止（丢弃）有威胁的流量并生成事件，或直接检测（警告）有威胁流量并仅生成事件。

在系统分析流量时，进行解码和预处理的网络分析阶段发生在入侵防御阶段之前并与其分隔开来。网络分析和入侵策略共同提供广泛且深入的数据包检测。它们可以帮助您检测、提醒和防范可能威胁主机及其数据的可用性、完整性和保密性的网络流量。

系统定义的网络分析和入侵策略

系统包括几对相辅相成的同名网络分析和入侵策略。例如，名称同为“平衡安全和连接”的NAP策略和入侵策略要一起使用。系统提供的策略由思科 Talos 情报小组 (Talos) 配置。对于这些策略，Talos设置入侵和预处理器规则状态，并提供预处理器和其他高级设置的初始配置。

随着新的漏洞被发现，Talos会发布入侵规则更新。这些规则更新可以修改系统提供的任何网络分析或入侵策略，并且可以提供新的和已更新的入侵规则及预处理器规则、现有规则的已修改状态，以及已修改的默认策略设置。规则更新还可以从系统提供的策略中删除规则，并且提供新规则类别，以及修改默认变量集。

您可以手动更新规则数据库，或配置定期更新计划。更新必须部署，才能生效。有关更新系统数据库的更多信息，请参阅更新系统数据库，第 766 页。

以下是系统提供的策略：

“平衡安全和连接”网络分析和入侵策略

这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数网络和部署类型的良好起点。系统默认使用“平衡安全和连接”网络分析策略。

“连接优先于安全”网络分析和入侵策略

这些策略专为连接（即能够获取所有资源）优先于网络基础设施安全的网络而构建。此入侵策略启用的规则远远少于“安全优先于连接”策略中启用的规则。仅会启用阻止流量的最重要规则。

“安全优先于连接”网络分析和入侵策略

这些策略专为网络基础设施安全优先于用户便利性的网络而构建。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。

“最大检测”网络分析和入侵策略

此类策略适用于网络基础设施安全比在“安全优先于连接”策略中还要重要、且有可能产生更大运行影响的网络。例如，入侵策略将启用大量威胁类别中的规则，包括恶意软件、攻击程序包、旧漏洞和常见漏洞及已知外部攻击程序。

检测模式：预防与检测

默认情况下，所有入侵策略在防御模式下运行，以实施入侵防御系统(IPS)。在防御检测模式下，如果连接与实施流量丢弃操作的入侵规则匹配，则该连接会被主动阻止。

如果想要测试入侵策略对网络的影响，则可以更改为“检测”模式，从而实施入侵检测系统 (IDS)。在此检测模式下，丢弃规则的处理方式类似于报警规则，在这种情况下，系统会通知您匹配的连接，但操作结果变为“将被阻止”，而事实上绝不会阻止连接。

您可以更改每个入侵策略的检测模式，以便组合使用防御与检测功能。

Snort 3 网络分析策略 (NAP) 也有检测模式。与入侵策略不同，NAP 策略是全局策略，因此您必须在防御或检测模式下运行所有NAP处理。您应使用为入侵策略使用的相同模式。如果您混合使用防御和检测策略，请选择“防御”以匹配最严格的入侵策略。

入侵和预处理器规则

入侵规则是系统用于检测利用网络漏洞企图的一组指定关键字和参数。当系统分析网络流量时，它将数据包与每个规则中指定的条件相比较，并在数据包满足规则中指定的所有条件的情况下触发规则。

系统包含思科 Talos 情报小组 (Talos) 创建的以下类型的规则：

- 入侵规则，可细分为共享对象规则和标准文本规则
- 预处理器规则，是指与网络分析策略中的预处理器和数据包解码器检测选项关联的规则。默认情况下禁用大多数预处理器规则。

以下主题更深入地介绍入侵规则。

入侵规则属性

当您查看入侵策略时，可以看到可用于识别威胁的所有入侵规则的列表。

每个策略的规则列表都是相同的。不同的是为每个规则配置的操作。由于规则数量在 30,000 条以上，所以滚动列表需要时间。滚动列表时会显示规则。

以下是定义每个规则的属性：

>（签名说明）

点击左列的 > 按钮可打开签名说明。说明内容是 Snort 检测引擎用来根据规则匹配流量的实际代码。代码介绍不在本文范围之内，有关详细信息，请参阅 管理中心配置指南；请从 http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html中选择适合您的软件版本的书籍。查找入侵规则编辑的相关信息。

签名包含某些项目的变量。有关详细信息，请参阅默认入侵变量集，第 500 页。

GID

生成器标识符 (ID)。此数字指示评估规则并生成事件的系统组件。1 表示标准文本入侵规则，3 表示共享对象入侵规则。（对于 设备管理器用户，这些规则类型差异没有意义。）这些是在配置入侵策略时主要关注的规则。有关其他 GID 的信息，请参阅生成器标识符，第 501 页。

SID

Snort 标识符 (ID)，也称为签名 ID。低于 1000000 的 Snort ID 由思科 Talos 情报小组 (Talos) 创建。

操作

此规则在所选入侵策略中的状态。此策略内每个规则的默认操作后面会添加“（默认）”。要使规则返回其默认设置，请选择此操作。可能的操作包括：

- **警报** - 当此规则与流量匹配时，创建一个事件但不丢弃连接。
- **丢弃** - 当此规则与流量匹配时，创建一个事件同时丢弃连接。
- **禁用** - 不针对此规则匹配流量。不生成事件。

状态

对于Snort 2规则，“状态”为单独的一列。如果更改规则的默认操作，此列将显示“已覆盖”。否则，该列为空。

对于 Snort 3 规则，“覆盖”状态显示在“操作”属性的底部（如果您已更改）。

消息

这是规则的名称，规则触发的事件中也会显示该名称。消息通常标识签名匹配的威胁。通过互联网可搜索每个威胁的详细信息。

默认入侵变量集

入侵规则签名包含某些项目的变量。以下是这些变量的默认值，其中最常用的变量是 $HOME_NET 和 $EXTERNAL_NET。请注意，协议与端口号分开指定，所以端口变量只是数字。

- $DNS_SERVERS = $HOME_NET（表示任何 IP 地址）。
- $EXTERNAL_NET = 任何 IP 地址。
- $FILE_DATA_PORTS = $HTTP_PORTS、143、110。
- $FTP_PORTS = 21、2100、3535。
- $GTP_PORTS = 3386、2123、2152。
- $HOME_NET = 任何 IP 地址。
- $HTTP_PORTS = 144 个端口号：36、80-90、311、383、443、555、591、593、631、666、801、808、818、901、972、1158、1212、1220、1414、1422、1533、1741、1830、1942、2231、2301、2381、2578、2809、2980、3029、3037、3057、3128、3443、3507、3702、4000、4343、4848、5000、5117、5222、5250、5450、5600、5814、6080、6173、6767、6988、7000、7001、7005、7071、7080、7144、7145、7510、7770、7777-7779、8000、8001、8008、8014、8015、8020、8028、8040、8060、8080-8082、8085、8088、8118、8123、8161、8180-8182、8222、8243、8280、8300、8333、8344、8400、8443、8500、8509、8787、8800、8888、8899、8983、9000、9002、9060、9080、9090、9091、9111、9290、9443、9447、9710、9788、9999、10000、11371、12601、13014、15489、19980、23472、29991、33300、34412、34443、34444、40007、41080、44449、50000、50002、51423、53331、55252、55555、56712。
- $HTTP_SERVERS = $HOME_NET（表示任何 IP 地址）。
- $ORACLE_PORTS = 任何
- $SHELLCODE_PORTS = 180。
- $SIP_PORTS = 5060、5061、5600
- $SIP_SERVERS = $HOME_NET（表示任何 IP 地址）。
- $SMTP_SERVERS = $HOME_NET（表示任何 IP 地址）。
- $SNMP_SERVERS = $HOME_NET（表示任何 IP 地址）。

- $SQL_SERVERS = $HOME_NET（表示任何 IP 地址）。
- $SSH_PORTS = 22。
- $SSH_SERVERS = $HOME_NET（表示任何 IP 地址）。
- $TELNET_SERVERS = $HOME_NET（表示任何 IP 地址）。

生成器标识符

生成器标识符 (GID) 标识评估入侵规则并生成事件的子系统。标准文本入侵规则的生成器 ID 为 1，共享对象入侵规则的生成器 ID 为 3。对于各种预处理器也有几套规则。下表解释了 GID。

表 *11:* 生成器 *ID*

ID	组件
1	标准文本规则。
2	标记的数据包。 （标记生成器规则，根据标记会话生成数据包。）
3	共享对象规则。
102	HTTP 解码器。
105	Back Orifice 检测器。
106	RPC 解码器。
116	数据包解码器。
119、120	HTTP 检查预处理器。 （GID 120 规则与服务器特定 HTTP 流量相关。）
122	Portscan 检测器。
123	IP 分片重组器。
124	SMTP 解码器。 （针对 SMTP 动词的攻击）
125	FTP 解码器。
126	Telnet 解码器。
128	SSH 预处理器。
129	流预处理器。

ID	组件
131	DNS 预处理器。
133	DCE/RPC 预处理器。
134	规则延迟，数据包延迟。 （规则延迟暂停 (SID 1) 或重新启用 (SID 2) 一组入侵规则，或系统由于超出数据包延迟阈值 (SID 3) 而停止检查数据包时，生成这些规则的事件。）
135	基于速率的攻击检测器。 （与网络上主机的连接过多。）
137	SSL 预处理器。
138、139	敏感数据预处理器。
140	SIP 预处理器。
141	IMAP 预处理器。
142	POP 预处理器。
143	GTP 预处理器。
144	Modbus 预处理器。
145	DNP3 预处理器。

网络分析策略

网络分析策略控制流量预处理。预处理器通过规范化流量和标识协议异常，准备要进行进一步检查的流量。网络分析相关预处理发生在安全智能丢弃和 SSL 解密之后进行，但在访问控制和入侵或文件检测开始之前进行。

默认情况下，系统使用“平衡安全和连接”网络分析策略预处理由访问控制策略处理的所有流量。但是，如果在任何访问控制规则上配置入侵策略，系统将使用与所应用的最严格入侵策略匹配的网络分析策略。例如，如果在访问控制规则中同时使用“安全优先于连接”策略和“平衡”策略，则系统将对所有流量使用“安全优先于连接”NAP。对于 Snort 3 自定义入侵策略，此分配根据分配给入侵策略的基本模板策略完成。

使用 Snort 3 时，您可以明确选择一个策略，并选择性地自定义其设置。建议您选择名称与用于通过设备的大多数流量的入侵策略匹配的策略，无论是直接使用入侵策略，还是将其用作自定义入侵策略中的基本策略。然后，您可以更改检测模式，或调整特定检查器或绑定程序设置，以考虑网络中的流量。

此外，请考虑您是否在入侵策略中启用了预处理器规则。如果您启用需要预处理器的规则，请确保同时在 NAP 中启用相应检查器。对于每个检查器，您还可以调整检查器的属性，包括检查的端口（绑定程序），以自定义网络的检查器行为。

注释 如果您使用的是 Snort 2，系统将使用同名的 NAP 策略作为您在任何访问控制规则中应用的最严格的入侵策略，并且您无法编辑检查器或绑定程序设置。

入侵策略的许可证要求

只有启用**IPS** 许可证，才能在访问控制规则中应用入侵策略。有关配置许可证的信息，请参阅启用或禁用可选许可证，第 87 页。

网络分析策略无需额外的许可证。

在访问控制规则中应用入侵策略

要将入侵策略应用于网络流量，请在允许流量的访问控制规则中选择该策略。不得直接分配入侵策略。

可以根据所保护网络的相对风险分配不同的入侵策略，以提供可变的入侵保护。例如，可以对内部网络与外部网络之间的流量使用更严格的“安全优先于连接”策略。另一方面，可以对内部网络之间的流量应用更宽松的“连接优于安全”策略。

此外，还可以通过对所有网络使用相同的策略来简化配置。例如，“平衡安全和连接”策略用于提供良好的保护，且不会对连接产生过多的影响。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 创建新规则或编辑**允许**流量的现有规则。

如果允许默认操作，还可在默认操作中指定入侵策略。

不得将入侵策略应用于信任或阻止流量的规则。

步骤 3 点击**入侵策略**选项卡。

步骤 4 依次选择**入侵策略** > **开**，然后选择要在匹配流量中使用的入侵检测策略。

在 Snort 2 和 Snort 3 之间切换

Snort 是产品的主要检测引擎。虽然可以自由切换 Snort 版本，但 Snort 2.0 中的某些入侵规则未在 Snort 3.0 中提供，反之亦然。如果对其中一项规则更改了规则操作，则在从 Snort 3 切换到 Snort 2 或再次切换回 Snort 3 时，不会保留该更改。您对两个版本中现有规则的规则操作更改都将被保留。请注意，Snort 3 与 Snort 2 中的规则之间的映射可以是一对一或一对多的，因此系统将尽可能保留更改。

如果更改Snort版本，系统将执行自动部署以实施更改。您可以在任务列表中查看进度。这些任务是 Snort 版本更改和自动部署 - Snort 版本切换。由于部署以及必须停止并重新启动 Snort 的事实，所有现有连接（包括 VPN）都将被丢弃并必须重新建立，这将导致瞬时流量丢失。

注释 如果您尝试切换Snort版本但切换失败，您将无法放弃待处理的更改，并且系统不允许进行后续切换尝试。如果发生这种情况，您必须使用 ToggleInspectionEngine API 完成切换，您可以在 API Explorer 中使用该 API。您必须将 bypassPendingChangeValidation 属性设置为 TRUE。

开始之前

要确定当前启用的 Snort 版本，请使用此程序，或依次选择**策略** > **入侵**。查看表上方的 **Snort 版本**行。当前版本是完整版本号中的第一个数字。例如，2.9.17-95 是 Snort 2 版本。

如果设备位于气隙网络中，请考虑在切换之前手动上传新版本的最新规则包。

如果降级到2.0，您创建的所有自定义入侵策略都将转换为自定义策略中使用的基本策略。尽可能保留“覆盖”规则操作。如果多个自定义策略使用相同的基本策略，则系统将保留大多数访问控制策略中使用的自定义策略“覆盖”操作，而其他自定义策略的“覆盖”操作将丢失。现在，使用这些“复制”策略的访问控制规则将使用根据最常用自定义策略创建的基本策略。所有自定义策略都将被删除。如果要保留自定义策略以便稍后导入，请在切换回 Snort 3 后使用 威胁防御 API 导出配置。

此外，降级到 2.0 会删除所有 NAP 自定义，并且系统会根据访问控制规则中使用的入侵策略切换为使用最合适的 NAP。

主动身份验证中的主机名重定向也需要 Snort 3，如果您切换到 Snort 2，它将被删除。

您必须部署所有待处理更改，然后才能切换 Snort 版本。

过程

步骤 1 选择**设备**，然后点击“更新”摘要中的**查看配置**。

查看**入侵规则**组。系统会显示当前的 Snort 版本。

步骤 2 在**入侵规则**组中，您可以通过点击**升级到 Snort 3.0** 或**降级到 Snort 2.0** 来更改 Snort 版本。

步骤 3 当系统提示您确认操作时，请选择获取最新入侵规则包的选项，然后点击**是**。

我们建议您获取最新的规则包。系统仅下载活动 Snort 版本的包，因此无法安装您要切换到的 Snort 版本的最新包。

您必须等到切换版本的任务完成后，才能编辑入侵策略。

为入侵事件配置系统日志

可以为入侵策略配置外部系统日志服务器，从而将入侵事件发送至系统日志服务器。必须根据入侵策略配置系统日志服务器，从而将入侵事件发送到服务器。根据访问规则配置系统日志服务器只可将连接事件（而不是入侵事件）发送到系统日志服务器。

如果选择多个系统日志服务器，事件将发送到每个服务器。

入侵事件的消息 ID 为 430001。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击**入侵策略设置**按钮 (⚙) 来配置系统日志。

步骤 3 点击**将入侵事件发送到**字段下的 **+**，然后选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**创建新系统日志服务器**，并创建相应对象。

步骤 4 点击**确定 (OK)**。

配置网络分析策略 (Snort 3)

网络分析策略 (NAP) 应用于设备上所有允许的连接。NAP 确定启用了哪些检查器，以及检查器使用的属性值。绑定程度确定应与各种检查器关联的端口和协议。

协调 NAP 与您在访问控制规则中应用的入侵策略：

- 如果您在访问控制规则中使用单个入侵策略，请选择同名的 NAP。然后，根据入侵策略中的设置对检查器和属性进行调整。例如，如果您为某个特定检查器（例如 CIP）启用入侵规则，请确保在 NAP 中启用该检查器。
- 如果您使用多个入侵策略，请选择与您使用的最严格的入侵策略匹配的 NAP。
- 如果您使用自定义入侵策略，请根据自定义入侵策略的基本入侵策略选择 NAP。
- 如果不需要自定义任何检查器或绑定程序，请考虑将系统配置为根据您的入侵策略使用情况自动选择最合适的 NAP。这是默认选项。

开始之前

除非您阻止，否则系统会定期将 LSP 更新下载到检测规则中。这些更新可以添加或删除检查器和属性，以及更改属性的默认设置。如果对已删除的检查器进行了覆盖，则会保留这些覆盖，并且您将看到不再支持检查器的警告。在这种情况下，请删除检查器并进行任何其他标记调整，以确保您的 NAP 完全有效。

过程

步骤 1 依次选择**策略** > **入侵**。

验证表上方显示的 Snort 版本是否为 3.x。

步骤 2 点击**入侵策略设置按钮** (⚙)。

步骤 3 在**默认网络分析策略**中，选择以下选项之一：

- **自动** - 自动选择与访问控制规则中应用的最常用入侵策略（或自定义规则的基本策略）相匹配的NAP。如果不应用任何入侵策略，则会使用“安全性和连接性均衡”NAP。NAP在防御模式下运行，您无法自定义入侵或绑定程序设置。在自动模式下运行时，此程序的其余部分不适用。
- **自定义** - 明确选择应当使用的 NAP。点击策略名称旁边的**编辑**链接可选择不同的策略。然后，您可以选择检测模式，并自定义检查器和绑定程序设置，如以下步骤所述。

步骤 4 在“编辑网络分析策略”对话框中，选择策略并配置其设置。

a) 在**网络分析策略**中，选择应全局应用于所有允许连接的策略。

b) 选择**检测模式**。

检测模式决定了如何处理不合规的流量。为了获得最佳效果，请使用与入侵策略所用模式相同的检测模式。

- **防御** - 根据策略中的设置阻止所有解码器异常、规范化异常或协议异常。如果启用SSL解密策略，或者在访问控制策略设置中启用了 **TLS 服务器身份发现** 选项，则必须使用此选项。
- **检测** - 只会就解码器异常、规范化异常或协议异常发出警报。不会阻止任何流量。

c) （可选。）配置并管理对检查器和绑定程序的覆盖：

- 要编辑覆盖，请参阅配置检查器和绑定程序覆盖 ， 第 507 页。
- 要下载架构或覆盖，请参阅下载覆盖和架构 ， 第 508 页。
- 要上传覆盖，请参阅上传覆盖 ， 第 509 页。
- 要重置所有覆盖，请点击 NAP 文件上方的**重置检查器/绑定程序覆盖**链接。系统会要求您确认重置。如命令名称所示，只能对检查器或绑定程序执行删除操作。例如，删除所有绑定程序覆盖不会改变检查器覆盖。
- 要撤销对选定检查器的所有更改，请点击**将检查器重置为默认值**。

- 要过滤视图以仅查看具有覆盖的检查器，请点击**仅显示覆盖**。点击**显示所有检查器**可删除过滤器

d) 点击**确定 (OK)**。

配置检查器和绑定程序覆盖

当您选择基本NAP时，您选择的是该基准策略中包含的检查器设置。大多数情况下，这些是适当的设置。

但是，您可以覆盖所选NAP中的设置。例如，您可以启用或禁用单个检查器，或者更改属性或绑定程序的值。

以下程序介绍了如何直接配置覆盖。或者，您也可以下载架构，离线进行更改，然后上传您的覆盖。您还可以上传从另一台设备下载的覆盖。

开始之前

说明每个检查器、绑定程序和属性不在本文档范围之内。有关详细信息（包括示例），请参阅 https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/snort3-inspectors/snort-3-inspector-reference.html 上提供的 *Snort 3* 检查器参考。

过程

步骤 1 依次选择**策略** > **入侵**，点击**入侵策略设置**按钮 ( )，为 NAP 设置选择**自定义**，然后点击策略名称旁边的**编辑**链接。

步骤 2 点击包含您要更改的设置的选项卡：

- **检查器** - 检查器检查特定类型的流量（例如 FTP）是否存在协议异常。
- **绑定程序** - 绑定程序检查器确定何时需要使用服务检查器来检查流量。绑定程序检查器中的配置包括端口、主机、CIDR 以及定义网络分析策略中的另一个检查器何时需要检查流量的服务。

步骤 3 根据需要编辑设置。

- 使用以下项控制 JSON 编辑器中的视图：
  - 使用**过滤器**编辑框对 JSON 文件执行全文搜索。
  - 点击**展开所有字段 (Expand All Fields)** 按钮 ( )，打开 JSON 文件中的所有文件夹。
  - 点击**折叠所有字段**按钮 ( )，关闭 JSON 文件中的所有文件夹。
  - 点击**撤销上次操作**按钮 ( )，撤销最近的更改。
  - 点击**重做**按钮 ( )，重做上次撤销的更改。

- 选择**树**，查看 JSON 文件的格式化视图，其中包括操作菜单、错误标志和其他可指导您进行编辑的功能。
- 选择**代码**，查看原始 JSON 文件。

- 在“树”视图中，点击**菜单**按钮 (▮) 可操作文件的内容。您可以执行以下操作：
  - **插入**属性。使用“自动”选项可允许编辑器确定适当的数据类型。否则，请添加数组、对象或字符串。如果您添加无效属性，系统会将检查器或绑定程序标记为存在必须解决的问题。
  - **附加**属性。此操作与“插入”的作用相同，但会将属性放在相应部分的末尾。
  - **复制**所选属性。
  - **移除**（删除）所选属性。编辑属性时，弹出消息也可能提供**删除**命令。
- 要启用当前禁用的检查器，或更改任何布尔属性的设置，请点击属性值前面的复选框。例如，要启用检查器，请将 **enabled : false** 属性更改为：

- 要更改字符串或数字属性的值，请点击相应属性并根据需要编辑值。如果您输入的内容违反了相应字段的规则，错误消息会解释不符之处。例如，如果您输入的值超出范围，则数值会指示值的有效范围。
- 要重置覆盖，请执行以下操作：
  - 点击**重置检查器/绑定程序覆盖**可删除您对所有检查器或绑定程序所做的所有更改，并返回默认值。如命令名称所示，只能对检查器或绑定程序执行删除操作。例如，删除所有绑定程序覆盖不会改变检查器覆盖。
  - 点击**将检查器重置为默认值**可仅撤销对所选检查器所做的所有更改。
- 要过滤视图以仅查看具有覆盖的检查器，请点击**仅显示覆盖**。点击**显示所有检查器**可删除过滤器
- 如果某个检查器不再受支持，则系统会用一条消息标记该检查器。点击消息中的**删除检查器**链接可删除该检查器。

步骤 4 完成后点击**确定**。

下载覆盖和架构

您可以下载 NAP 架构，或下载您为策略配置的覆盖。

每当您更改基本NAP时，建议下载覆盖，以防您想返回到之前的设置。此外，您可以在一台设备上使用 JSON 编辑器来实施要在所有设备上使用的覆盖，下载覆盖，然后将该覆盖文件上传到其他设备。

如果您想离线编辑文件，然后将覆盖上传到此设备或多台设备，则下载架构非常有用。您应该只复制/粘贴您需要更改的部分，而不是上传整个文件，以确保只有您所做的更改才被视为覆盖。

过程

步骤 1 依次选择**策略** > **入侵**，点击**入侵策略设置**按钮 ( )，为 NAP 设置选择**自定义**，然后点击策略名称旁边的**编辑**链接。

步骤 2 执行以下操作之一：

- 要下载当前选择的 NAP 的架构，请点击齿轮图标 ( ) 并选择**下载** > **策略架构**。
- 要下载已保存的覆盖集，因为它们在当前编辑会话之前就已存在，请点击齿轮图标 ( ) 并选择**下载** > **上次保存的覆盖**。该文件包括覆盖的属性及其包含的对象。
- 要下载您在当前编辑会话中创建的覆盖，请点击齿轮图标 ( ) 并选择**下载** > **当前未保存的覆盖**。该文件包括覆盖的属性及其包含的对象。

上传覆盖

您可以下载 NAP 策略架构，离线编辑文件，然后上传文件，而不是使用嵌入式 JSON 编辑器编辑属性。然后，在上传的文件中配置的所有覆盖都将应用于选定的 NAP。

您还可以上传在另一台设备上配置覆盖后下载的文件。

通过上传覆盖，您可以将同一文件上传到多台设备，并轻松应用相同的覆盖。

开始之前

要覆盖网络分析策略中的检查器配置，您应只上传您需要的更改。不应上传整个配置，因为它会使覆盖本质上具有粘性，因此，将不会应用对默认值或配置的任何后续更改作为 LSP 更新的一部分。确保上传的覆盖仅专注于您想要更改的属性。

过程

步骤 1 依次选择**策略** > **入侵**，点击**入侵策略设置**按钮 ( )，为 NAP 设置选择**自定义**，然后点击策略名称旁边的**编辑**链接。

步骤 2 点击齿轮图标 ( ) 并选择**上传** > **覆盖**。

步骤 3 （可选。）点击其中一个**下载**链接，以保存现有覆盖的副本。

您可以下载上次保存的覆盖（在当前编辑会话之前创建的覆盖）或当前未保存的覆盖（在当前编辑会话期间创建的覆盖）。

步骤 4 点击“确认上传覆盖”对话框上的**是**，以确认您要继续。

步骤 5 点击**浏览**或拖放以选择包含覆盖的 JSON 文件，然后点击**确定**。

管理入侵策略 (Snort 3)

当您使用 Snort 3 作为检测引擎时，您可以创建自己的入侵策略，并根据自己的目的对其进行自定义。系统随附基于同名思科 Talos 情报小组 (Talos) 定义的策略的预定义策略。虽然可以编辑这些策略，但最好根据基础 Talos 策略创建自己的策略，并在需要调整规则操作时进行更改。

其中每个预定义策略包含相同的入侵规则（也称为签名）列表，但针对每个规则所采取的操作有所不同。例如，一条规则在某个策略中可能处于启用状态，但在另一个策略中可能被禁用。

如果您发现某个特定规则为您提供的误报过多，在这种情况下该规则会阻止您不希望阻止的流量，可以禁用该规则而不必切换到安全性较低的入侵策略。也可将其更改为匹配警告，而不丢弃流量。

相反，如果您知道自己需要防御特定的攻击，但相关规则在您所选的入侵策略中被禁用，可以启用该规则而不必更改为更安全的策略。

使用与入侵相关的控制面板和事件查看器（两者均在**监控 (Monitoring)** 页面）可评估入侵规则对流量的影响。请记住，仅将匹配入侵规则的流量设为警告或丢弃时，才会看到入侵事件和入侵数据；系统不评估禁用的规则。

注释 如果切换到 Snort 2，则无法创建自定义策略，并且入侵策略的使用略有不同。请不要参阅此主题，而是参阅管理入侵策略 (Snort 2)，第 521 页。

过程

步骤 1 依次选择**策略** > **入侵**。

验证表上方显示的 Snort 版本是否为 3.x。

步骤 2 执行以下任一操作：

- 使用**搜索/过滤器**框查找策略。您只能按名称搜索。
- 点击齿轮图标 (⚙) 可启用将日志记录发送至系统日志服务器。请参阅为入侵事件配置系统日志，第 505 页。
- 点击齿轮图标 (⚙) 可配置网络分析策略 (NAP)。请参阅配置网络分析策略 (Snort 3)，第 505 页。
- 点击 + 可创建新的策略。请参阅配置自定义入侵策略 (Snort 3)，第 511 页。
- 点击编辑图标 (✎) 可查看策略中的属性和规则，并进行编辑。请参阅查看或编辑入侵策略属性 (Snort 3)，第 512 页。

- 点击删除图标 () 可删除策略。

配置自定义入侵策略 (Snort 3)

如果预定义策略不符合您的需求，您可以创建新的入侵策略以自定义规则行为。通常，最好根据预定义策略创建自定义策略，而不是修改这些策略。如果您发现自定义无法实现所需的结果，这样可以确保您轻松实施 Cisco Talos 定义的策略之一。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 执行以下操作之一：

- 要创建新策略，请点击 **+**。
- 要编辑某个现有策略，请点击该策略的编辑图标 ()。当显示策略详细信息时，点击页面顶部策略属性部分中的**编辑 (Edit)** 链接。

步骤 3 为该策略输入**名称**和说明（后者为可选项）。

步骤 4 为策略配置**检测模式**。

- **防御** - 始终应用入侵规则操作。匹配丢弃规则的连接将被阻止。
- **检测** - 入侵规则仅生成警报。匹配丢弃规则的连接将生成警报消息，但不会阻止连接。

步骤 5 为策略选择**基本模板**。

基本模板由 Cisco Talos 提供。点击每个模板的信息图标可查看有关策略的详细信息。请注意，在安装新的规则包时，策略名称可以更改，并且会显示新策略。

- **最大限度检测 (Cisco Talos)** - 此策略只强调安全性。不保证网络连接性和吞吐量，也可能出现误报。此策略应仅用于高安全性区域，并且必须配备安全监控器来调查警报，以确定其有效性。
- **安全优先于连接 (Cisco Talos)** - 此策略可能以牺牲网络连接和吞吐量为代价而强调安全。对流量进行更深入的检测，评估更多的规则，并且预期会出现误报以及延迟增加，但都在合理的范围内。
- **平衡安全和连接 (Cisco Talos)** -（默认设置。）此策略试图在网络连接性和吞吐量与安全性需求之间达到精细均衡。虽然不像“安全优先于连接”那样严格，但此策略试图在保持用户安全的同时降低对正常流量的干扰。
- **连接优先于安全 (Cisco Talos)** - 此策略可能以牺牲安全为代价而强调网络连接和吞吐量。对流量的检测不够深入，评估的规则也较少。
- **无活动规则 (Cisco Talos)** - 此策略是配置典型预处理器设置但未启用任何规则或内置警报的基本策略。如果要确保仅启用要应用的策略，请使用此策略作为基础策略。

步骤 6 点击**确定**。

系统会将您返回到入侵策略列表。现在，您可以查看新策略并根据需要调整规则操作。

查看或编辑入侵策略属性 (Snort 3)

“入侵策略”(Intrusion Policy) 页面显示策略列表，包括预定义和用户定义的策略及其说明。要编辑策略，必须先查看策略的属性。

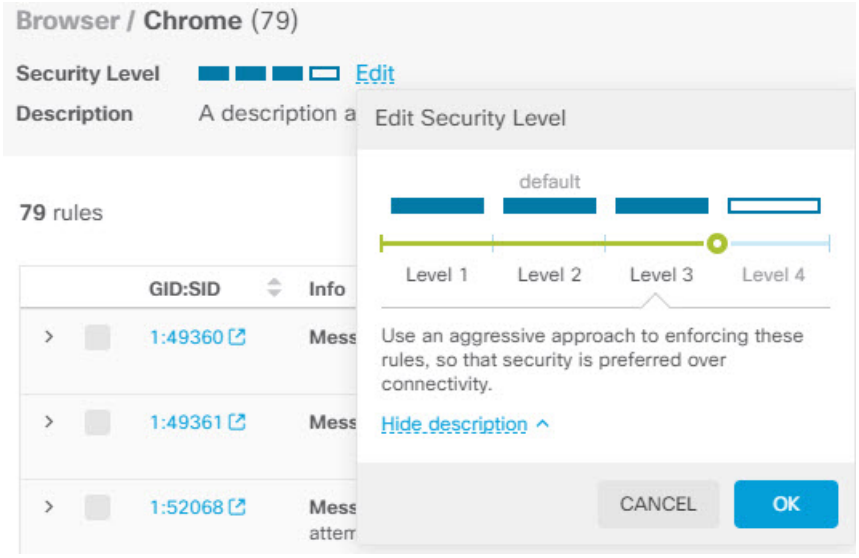
过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击策略的编辑图标 ()。

策略包含以下部分：

- **策略名称**下拉列表。
  - 您可以通过从下拉列表中选择策略轻松切换到其他策略，也可以通过点击后退按钮 () 返回到策略列表。
  - 您可以通过点击策略名称 () 旁边的删除图标来删除此策略。
- **常规属性**。此部分显示入侵模式、基本策略和说明。点击**编辑**以更改这些属性或策略名称。
- **规则组**目录。此列表显示策略中具有活动规则的所有规则组。这些组具有层次结构，其中父组包含子组，子组将较大的父组内的规则划分为不同子集。每个组都是规则的逻辑集合，一个规则可以出现在多个组中。
  - 要添加当前在策略中没有活动规则的组，请点击 + > **添加现有规则组**并选择该组。请参阅在入侵策略中添加或删除规则组 (Snort 3)，第 514 页。
  - 要更改组的安全级别，请在列表中选择子组。规则列表改为在顶部显示安全级别，下面列出组中的规则。点击安全级别旁边的**编辑**链接并选择新级别。编辑时，点击**查看说明**可获取有关每个安全级别的信息。请注意，更改级别可以更改哪些规则处于活动状态，也可以更改给定规则的操作，安全级别越多，活动规则往往就越多，而且具有“丢弃”操作的规则也越多。点击**确定**，确认更改。（安全级别不适用于自定义规则组。）



- 要删除组中的所有规则，请在列表中选择子组。然后，点击组名称最右侧的**排除**链接，并确认要排除该组。排除组仅会禁用组中的所有规则，而不会删除组。

  但是，如果组包含与其他已启用组共享的规则，则共享规则会保留仍处于活动状态的组应用的所有操作。在所有情况下，无论组成员身份如何，我们都会为单个规则保留最严格的设置。

- 要添加自定义规则的新自定义规则组，请点击 + > **上传自定义规则**。有关详细信息，请参阅上传自定义入侵规则，第 518 页。

- 要更改自定义规则组的名称或说明，请点击**编辑**。

- 要删除自定义规则组，请点击**删除**。有关详细信息，请参阅管理自定义入侵规则和规则组，第 517 页。

- 要在自定义规则组中添加新的自定义规则，请点击规则表上方的 +。请参阅配置单独自定义入侵规则，第 520 页。

- 要编辑、复制、删除或管理自定义规则的组成员身份，请将鼠标悬停在规则右侧，然后点击相应的按钮或命令。有关详细信息，请参阅配置单独自定义入侵规则，第 520 页。

- **规则列表**。您可以使用搜索字段来帮助您使用全文搜索查找规则。您还可以选择过滤项目来对 GID 或 SID 的任意组合进行搜索， 仅显示用户定义的规则（您添加的规则）， 仅显示操作被覆盖的规则，或者仅根据其操作（禁用、警报、丢弃）显示规则。规则是延迟加载的，因此滚动浏览整个未过滤的列表需要相当长的时间。过滤列表时，点击刷新按钮可重新加载已过滤的视图。

  - 要更改规则的操作，请点击规则的**操作**单元格，然后选择以下新操作：仅生成**警报**，**阻止**匹配规则的流量，或**禁用**规则。系统会指示每个规则的默认操作。

  - 要一次更改多个规则的操作，请点击要更改的规则左列中的复选框，然后从规则表上方的**操作**下拉列表中选择新操作。点击 GID:SID 表标题中的复选框以选择列表中的所有规则。一次最多可以更改 5000 条规则。

- 要更新自定义规则组中的规则，请点击**上传规则文件**。有关详细信息，请参阅上传自定义入侵规则，第 518 页。
- 要获取有关规则的更多信息，请点击 **GID:SID** 单元格中的链接。该链接会将您引导至 Snort.org。
- 要更改列出的规则，您可以点击规则组目录中的子组（而不是父组）。您可以通过点击规则组列表顶部的**全部规则**返回到全部规则列表。
- 要更改排列顺序，请点击列的表标题。规则的默认排序方式是首先为覆盖规则，然后是丢弃规则，然后是警报规则。
- 要查看入侵规则 (LSP) 更新中进行了哪些更改，请在过滤器字段中选择 **LSP 更新**，然后选择要查看其更改的更新，并指定是要查看所有更改，还是仅查看规则添加或更改。

在入侵策略中添加或删除规则组 (Snort 3)

入侵规则划分为多个本地组。组具有层次结构，其中父组包含相关的子组。规则本身仅显示在子组中：父组只是一个组织结构。给定规则可以出现在多个组中。

您创建的任何自定义规则组都位于“用户定义的组”文件夹中。自定义规则组没有层次结构。

在入侵策略中添加或删除规则的最简单方法是添加或删除组。由于组中的规则在逻辑上是关联的，因此您很可能希望使用给定组中的大多数（如果不是全部）规则。

以下程序介绍如何添加组和更改组的安全级别。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击要更改的策略的编辑图标 ( )。

步骤 3 （添加组。）如果规则组列表中未显示该组，请点击 + > **添加现有规则组**并执行以下操作：

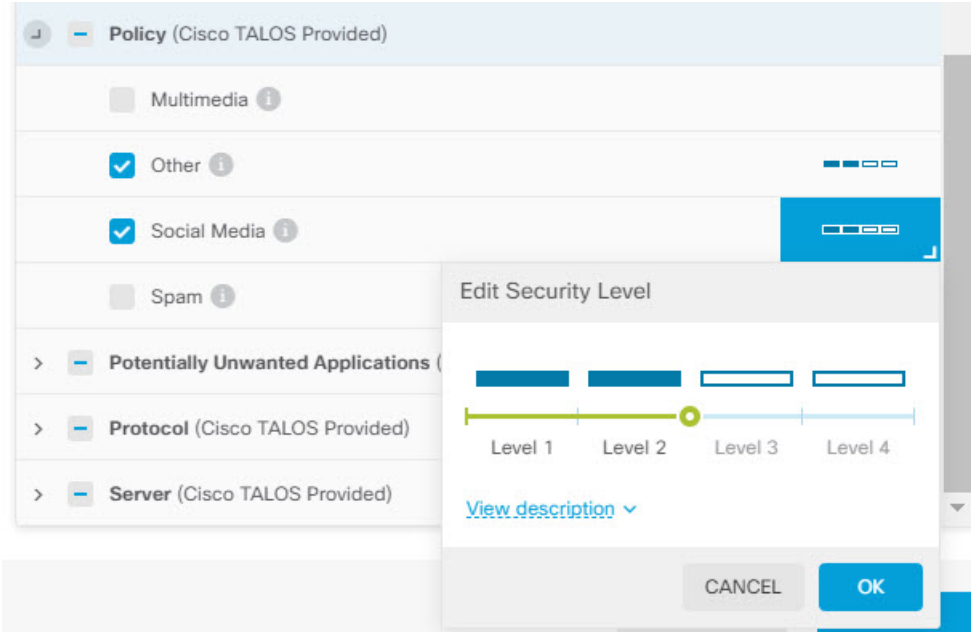
a) 查找子组。

- 父组名称旁边的复选标记表示已选择父组中的所有子组。
- 父组名称旁边的减号表示一个或多个子组没有为此策略启用规则。可以添加这些组。
- 子组名称旁边的复选标记表示该组已被选中。

b) 选择要添加的组（即，选中其复选框）。

c) （可选，不适用于自定义规则组。）每个组都有一个默认安全级别，具体取决于自定义策略所用的基本策略。如果要更改它，请点击安全级别图标，选择新级别，然后点击**确定**。

级别 1 是最不安全的状态，强调连接优先于安全，而级别 4 是最严格的状态，提供最高级别的安全。您可以点击**查看说明**，在选择每个级别时查看其说明。



d) 继续选择（或取消选择）组，直到完成所有更改。

e) 点击**确定**。

步骤 4 （删除组。）如果要禁用组中的所有规则，可以使用以下任一方法：

- 选择组，然后点击规则列表上方组名称最右侧的**排除**链接。
- 使用添加组的方法，但取消选择不需要的组（即，取消选中其复选框），然后点击**确定**。
- 您可以删除自定义规则组，以将其从系统和使用该规则组的所有入侵策略中完全删除。选择组，然后点击**删除**。

更改入侵规则操作 (Snort 3)

每个入侵策略包含相同的规则。不同的是针对每个规则所采取的操作因策略而异。

通过更改规则操作，可以禁用为您提供过多误报的规则，也可以将规则更改为针对匹配流量发出警报或丢弃该流量。您还可以启用已禁用的规则，以警告或丢弃匹配的流量。

更改规则操作的最简单方法是更改规则组的安全级别。当您更改组的安全级别时，组内规则的操作也会更改。这可能意味着某些规则会启用（或禁用），或者操作可以根据您选择的安全状态评估在警报和丢弃之间切换。但是，如果需要，可以更改单个规则操作。

注释 给定规则的默认操作基于组和严重性的整体选择。更改组的严重性或排除组可以更改规则的默认操作。

开始之前

自定义规则组没有安全级别。不能使用安全级别技术更改自定义规则的规则操作。

过程

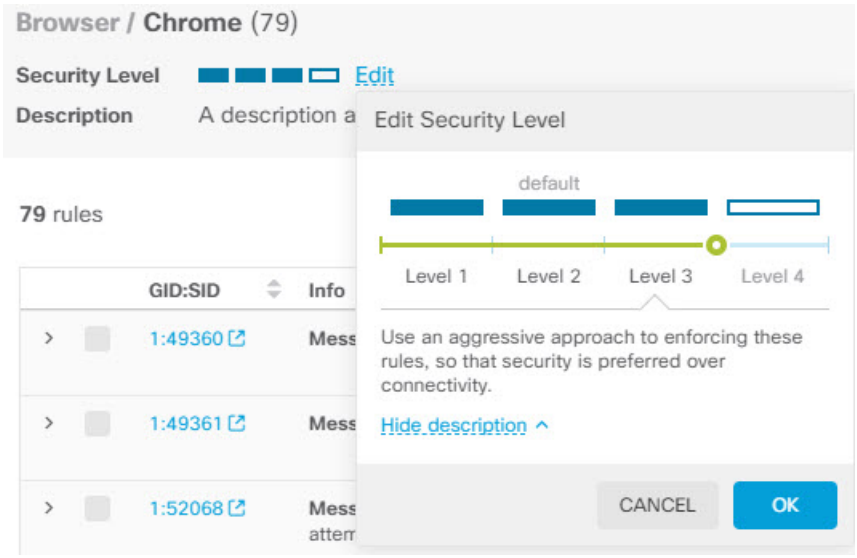
步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击您要更改其规则操作的策略的查看图标 ( )。

步骤 3 （这是建议方法。）更改规则组的安全级别。

a) 点击规则组列表中的子规则组。

b) 在规则列表上方，点击组安全级别旁边的**编辑**。



注释 如果要禁用组中的所有规则，请勿点击**编辑**。相反，请点击**排除**并确认要排除组。系统不会删除该组，而只是禁用其规则。跳过其余步骤。

c) 为组选择新级别。点击**查看说明**，查看您所选择的每个级别的说明。

级别 1 是最不安全的状态，强调连接优先于安全，而级别 4 是最严格的状态，提供最高级别的安全。

d) 点击**确定**。

步骤 4 （手动方法。）更改一个或多个规则的操作。

a) 查找您要更改其操作的规则。

使用**搜索/过滤器**框搜索规则信息中的字符串。您还可以选择过滤项目以对 GID 或 SID 的任意组合进行搜索，或者仅根据其操作（禁用、警报、丢弃）显示规则。规则是延迟加载的，因此滚动浏览整个未过滤的列表需要相当长的时间。过滤列表时，点击刷新按钮可重新加载已过滤的视图。

如果您正在与思科技术支持部门合力解决某个问题，最好可以从事件中或通过该部门获取 Snort 标识符 (SID) 和生成器标识符 (ID)。然后，您可以精确搜索规则。

b) 要更改操作，请执行以下操作之一：

- 一次更改一个规则 - 点击规则的**操作**列，选择所需的操作：
  - **警报** - 当此规则与流量匹配时，创建一个事件但不丢弃连接。
  - **丢弃** - 当此规则与流量匹配时，创建一个事件同时丢弃连接。
  - **禁用** - 不针对此规则匹配流量。不生成事件。
- 一次更改多个规则 - 点击要更改的规则的复选框，然后点击表上方的**批量**下拉列表并选择所需操作。点击 GID:SID 表标题中的复选框以选择列表中的所有规则。一次最多可以更改 5000 条规则。

管理自定义入侵规则和规则组

系统中附带思科 Talos 情报小组 (Talos) 定义的数千条入侵规则。如果您知道其他攻击，则可以创建和上传自定义入侵规则来过滤这些攻击，并发出警报或丢弃这些攻击。您也可以一次创建、编辑和删除一个规则。

对于上传的规则，您可以使用文本编辑器离线创建规则。建议您在上传的每个文本文件中包含一组自定义规则。然后，您可以轻松上传对规则的更改，将新规则合并到自定义规则组中，或将规则替换为新的已编辑副本规则。

介绍如何创建这些规则不属于本文档的范围。有关如何为 Snort 编写入侵规则（包括如何将 Snort 2 规则转换为 Snort 3 格式）的详细信息，请参阅 https://snort.org/documents 上的指南。例如，https://snort.org/documents/rules-writers-guide-to-snort-3-rules 上提供的面向规则编写者的 *Snort 3* 规则编写简介。

开始之前

您可以在上传自定义规则的过程中创建自定义规则组，如上传自定义入侵规则，第 518 页中所述，也可以在创建单个规则或管理规则成员时创建。创建组后，您可以管理组及其内容。

请注意，自定义组可用于所有入侵策略，而不仅仅是创建组时编辑的策略。因此，对组所做的更改会应用于所有策略。例如，如果删除某个自定义规则组，该规则组将从所有策略中删除，并且不再对其中任何策略可用。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击策略的编辑图标 ( )。

建议您将自定义规则添加到自定义入侵策略，而不是添加到其中一个内置策略。

步骤 3 执行以下任一操作：

- 要创建组，请点击 + > **上传自定义规则**。请参阅上传自定义入侵规则，第 518 页。
- 要编辑某个组的名称或说明，请在“用户定义的组”文件夹的组目录中选择该组。然后，您可以点击**编辑**并进行更改。
- 要从策略中排除该组及其规则，请在“用户定义的组”文件夹的组目录中选择该组。然后，您可以点击**排除**来删除该组。
- 要从系统及使用该组的所有策略中删除该组，请在“用户定义的组”文件夹的组目录中选择该组。然后，点击**删除**。请注意，如果某个规则仅存在于已删除的组中，那么该规则也会从系统中删除。但是，如果某个规则也存在于您不会删除的其他自定义规则组中，则该规则将保留在这些组中。
- 要批量替换或更新某个组中的规则，请在“用户定义的组”文件夹的组目录中选择该组。然后，点击该组的规则表上方“操作”下拉列表旁边的**上传规则文件**。流程与上传自定义入侵规则，第 518 页中介绍的流程相同。
- 要创建和管理单个规则及其向规则组的分配，请参阅配置单独自定义入侵规则，第 520 页。

上传自定义入侵规则

如果您知道其他规则当前未涵盖的攻击，则可以创建和上传自定义入侵规则来过滤这些攻击，并发出警报或丢弃这些攻击。导入规则的操作必须是 alert 或 drop，并且规则的默认操作由导入文件中的操作定义。导入后，您可以更改规则操作并根据需要禁用规则。

您必须离线创建这些规则。在 设备管理器中，您只需上传规则文件，而不是直接配置规则。规则文件应为文本文件。您可以使用换行符将规则设置为可读格式，或将规则放在一行中，并且允许使用空行。规则格式在 snort.org 中进行了说明。

例如，包含三个规则的上传文件可能如下所示：

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (
   msg: "My Custom Rule: EXPLOIT-KIT Styx exploit kit landing page request";
   flow:to_server,established;
   http_raw_uri;
   bufferlen:>100;
   http_uri;
   content:"/i.html?",depth 8; pcre:"/\/i\.html\?[a-z0-9]+\=[a-zA-Z0-9]{25}/";
   flowbits:set,styx_landing;
   metadata: copied from talos sid 29452;
   service:http;
   classtype:trojan-activity;
   gid:1;
   sid:1000000;
   rev:1;
)

alert tcp $HOME_NET 8811 -> $EXTERNAL_NET any (
   msg:"My Custom rule: MALWARE-BACKDOOR fear1.5/aciddrop1.0 runtime detection - initial
```

```
connection";
   flow:to_client,established;
   flowbits:isset,Fear15_conn.2;
   content:"Drive",nocase;
   metadata:copied from talos sid 7710;
   classtype:trojan-activity;
   gid:1;
   sid:1000001;
   rev:1;
)

alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (
   msg:"My Custom Rule: INDICATOR-COMPROMISE download of a Office document with embedded
PowerShell";
   flow:to_client,established;
   flowbits:isset,file.doc;
   file_data;
   content:"powershell.exe",fast_pattern,nocase;
   metadata:copied from talos sid 37244;
   classtype:trojan-activity;
   gid:1;
   sid:1000002;
   rev:1;
)
```

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击策略的编辑图标 ()。

建议您将自定义规则添加到自定义入侵策略，而不是添加到其中一个内置策略。

步骤 3 执行以下操作之一：

- 在组列表上方，点击**+** > **上传自定义规则 (Action)**。
- 如果要将规则上传到某个已创建的自定义规则组，您可以选择该自定义规则组，然后点击该组的规则表上方**操作 (Action)** 下拉列表旁边的**上传规则文件 (Upload Rule File)**。

步骤 4 点击**浏览 (Browse)** 并选择自定义规则文件，或将文件拖放到“上传文件”对话框中。

等待上传完成。

步骤 5 选择处理冲突的方式：

当您添加的规则与系统中已有的规则相同时，会发生冲突。仅当您上传的规则或编辑的规则版本与之前上传的规则或规则版本相同时，才会出现这种情况。

选择以下选项之一：

注释 **合并**和**替换**基本相同。上传的规则的修订版本号必须高于已上传的修订版本号，才能对现有规则进行任何更改。唯一的区别是，如果上传文件缺少目标自定义规则组中的规则，**替换**选项将从规则组中删除这些规则。**合并**选项将保留这些“缺失”规则。

- **合并** - 如果上传文件中的规则具有更高的修订版本号，则上传文件中也存在于所选组中的任何已更改规则都将合并这些更改。任何未更改的规则或组中在上传中没有对应规则的规则将保持不变。系统将添加上传中的任何新规则。这是默认选项。
- **替换** - 如果上传的规则的修订版本号更高，则上传文件中的规则将替换所选组中的规则。任何不在上传文件中的现有规则都将从组中删除。上传版本的修订版本号相同或更低的现有规则将保持不变。系统将添加上传中的任何新规则。

步骤 6 点击 **+**，然后为上传的规则选择自定义规则组。

如果您想使用的自定义规则组尚不存在，请点击**创建新组 (Create New Group)** 立即创建组。新组需要名称和说明（后者为可选项）。然后，您可以选择该新组。

如果要替换规则，则只能选择单个组。如果要合并规则，则可以选择多个组。

步骤 7 点击**确定 (OK)**。

文件将上传并放置在该新组中。您应该会看到一个摘要，说明上传了多少规则以及更新、删除或忽略了多少规则。

如果文件中有错误，上传将失败。您可以点击**下载错误文件 (Download Error File)** 链接，获取有关错误的更多信息。

该组在此入侵策略中自动激活。可以将该组和新规则添加到其他策略，但不会在任何其他策略中自动启用该组和规则。有关将组添加到其他策略的信息，请参阅在入侵策略中添加或删除规则组 (Snort 3)，第 514 页。

配置单独自定义入侵规则

您可以一次配置一个自定义入侵规则，而不是通过文件上传批量配置。当您需要快速调整某个规则，或者需要一次只创建或修改几个规则时，此方法十分有效。

配置入侵规则时，请记住以下几点：

- 所有自定义规则的 GID 都应为 1。
- 规则的 SID 在系统中的所有规则中必须是唯一的。它的值还必须等于或高于一百万 (1000000)。
- 如果您编辑某个规则，必须更改该规则的版本。通常情况下，版本号每次递增 1。
- 您可以复制思科 Talos 情报小组 (Talos) 规则来创建自己的规则版本，但仍必须更改复制规则的 SID 以确保其唯一性。

系统会执行一些有效性检查，以确保规则的格式正确，并且您会看到有关任何问题的错误消息。但是，系统无法确定规则是否合理。

有关如何为 Snort 编写入侵规则（包括如何将 Snort 2 规则转换为 Snort 3 格式）的详细信息，请参阅 https://snort.org/documents 上的指南。例如，https://snort.org/documents/rules-writers-guide-to-snort-3-rules 上提供的面向规则编写者的 *Snort 3* 规则编写简介。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击策略的编辑图标 ( )。

建议您将自定义规则添加到自定义入侵策略，而不是添加到其中一个内置策略。

步骤 3 执行以下操作之一：

- 要添加入侵规则，请点击规则表上方的**添加新的入侵规则**按钮 (+)。添加规则时，您必须选择一个或多个自定义规则组以包含新规则。如有必要，您可以在添加规则时创建新组。
- 要通过复制和编辑某个现有规则来添加规则，请将鼠标悬停在该规则的右端，然后点击复制( ) 按钮。该按钮仅在鼠标悬停时才会显示。对于自定义规则，**复制**命令位于更多选项 (...) 按钮下。
- 要编辑某个自定义规则，请在自定义规则组中找到该规则，然后点击该规则的编辑 ( ) 按钮。您所做的编辑将应用于该规则所在的所有组。在进行更改时，确保规则版本号每次至少递增 1。
- 要删除某个自定义规则，请点击该规则的删除 ( ) 按钮。该规则将从包含该规则的所有规则组中删除。如果您只想从组中删除某个规则，请使用**管理组分配**选项，而不是删除该规则。
- 要更改包含规则的组，请点击更多选项 (...) 按钮，然后选择**管理组分配**。随后即可添加或删除组。您所做的更改只会影响组成员身份，不会更改或删除规则。

步骤 4 对于新规则和组，请将规则添加到策略。

如果您在创建新规则或编辑现有规则时创建新组，该组不会自动添加到您的策略，规则也不会自动启用。系统会提示您将该组添加到正在编辑的策略。如果在添加或编辑规则时未添加该组，您可以稍后按照以下流程添加该组：

a) 点击组目录上方的 + > **添加现有规则组**。
b) 在“用户定义的组”文件夹下找到该组，选中，然后点击**确定**。
c) 在目录中选择该组，并验证新规则是否在该组中并具有所需操作。

管理入侵策略 (Snort 2)

您可以应用预定义的任何入侵策略。其中每个策略包含相同的入侵规则（也称为签名）列表，但针对每个规则所采取的操作有所不同。例如，一条规则在某个策略中可能处于活动状态，但在另一个策略中可能被禁用。

如果您发现某个特定规则为您提供的误报过多，在这种情况下该规则会阻止您不希望阻止的流量，可以禁用该规则而不必切换到安全性较低的入侵策略。也可将其更改为匹配警告，而不丢弃流量。

相反，如果您知道自己需要防御特定的攻击，但相关规则在您所选的入侵策略中被禁用，可以启用该规则而不必更改为更安全的策略。

使用与入侵相关的控制面板和事件查看器（两者均在**监控 (Monitoring)** 页面）可评估入侵规则对流量的影响。请记住，仅将匹配入侵规则的流量设为警告或丢弃时，才会看到入侵事件和入侵数据；系统不评估禁用的规则。

以下主题详细介绍入侵策略和规则调整。

配置入侵策略的检测模式 (Snort 2)

默认情况下，所有入侵策略在防御模式下运行，以实施入侵防御系统(IPS)。在防御检测模式下，如果连接与实施流量丢弃操作的入侵规则匹配，则该连接会被主动阻止。

如果想要测试入侵策略对网络的影响，则可以更改为“检测”模式，从而实施入侵检测系统 (IDS)。在此检测模式下，丢弃规则的处理方式类似于报警规则，在这种情况下，系统会通知您匹配的连接，但操作结果变为“将被阻止”，而事实上绝不会阻止连接。

您可以更改每个入侵策略的检测模式，以便组合使用防御与检测功能。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击您要更改其检测模式的入侵策略选项卡。

规则表上方指示**检测模式**。

步骤 3 点击检测模式旁边的**编辑**链接，更改策略的模式，然后点击**确定**。

选项包括：

- **防御** - 始终应用入侵规则操作。匹配丢弃规则的连接将被阻止。
- **检测** - 入侵规则仅生成警报。匹配丢弃规则的连接将生成警报消息，但不会阻止连接。

更改入侵规则操作 (Snort 2)

每个预定义的入侵策略包含相同的规则。不同的是针对每个规则所采取的操作因策略而异。

通过更改规则操作，可以禁用为您提供过多误报的规则，也可以将规则更改为针对匹配流量发出警报或丢弃该流量。您还可以启用已禁用的规则，以警告或丢弃匹配的流量。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击您要更改其规则操作的“入侵策略”选项卡。

预定义的策略包括：

- 连接优先于安全
- 平衡安全和连接
- 安全优先于连接
- 最大检测数

步骤 3 查找您要更改其操作的规则。

这些规则首先根据所列的已覆盖规则进行排序，并在已覆盖规则组中根据操作进行排序。否则，这些规则将先后根据 GID 和 SID 进行排序。

使用搜索框查找希望更改的规则。如果您正在与思科技术支持部门合力解决某个问题，最好可以从事件中或通过该部门获取 Snort 标识符 (SID) 和生成器标识符 (ID)。

有关每个规则的元素的详细信息，请参阅入侵规则属性，第 499 页。

要搜索列表，请执行以下操作：

a) 点击**搜索**框，打开“搜索属性”对话框。
b) 输入生成器 ID 的组合 (**GID**)、Snort ID (**SID**) 或规则**操作**，然后点击**搜索**。

例如，您可以选择**操作=丢弃**来查看丢弃匹配连接的策略中的所有规则。搜索框旁边的文本表示与您的条件匹配的规则数量，例如“找到 9416 条规则中的 8937 条”。

要清除搜索条件，请点击搜索框中条件的 x。

步骤 4 点击规则的**操作**列，选择所需的操作：

- **警报** - 当此规则与流量匹配时，创建一个事件但不丢弃连接。
- **丢弃** - 当此规则与流量匹配时，创建一个事件同时丢弃连接。
- **禁用** - 不针对此规则匹配流量。不生成事件。

规则的默认操作用操作后面附加“（默认）”表示。如果更改了默认设置，状态列会针对该规则指示“已覆盖”。

监控入侵策略

可以在**监控 (Monitoring)** 页面上的**攻击者 (Attackers)** 和**目标 (Targets)** 控制面板找到入侵策略统计信息。必须将入侵策略应用于至少一个访问控制规则，才能在这些控制面板上看到任何信息。请参阅监控流量和系统控制面板，第 98 页。

要查看入侵事件，请依次选择**监控** > **事件**，然后点击**入侵**选项卡。将鼠标悬停在某个事件上方，点击**查看详细信息**链接以获取更多信息。在详细信息页面中，点击**查看 IPS 规则 (View IPS Rule)** 转至相关入侵策略中的规则（您可以在此页面更改规则操作）。如果规则阻止过多安全连接，则可通过

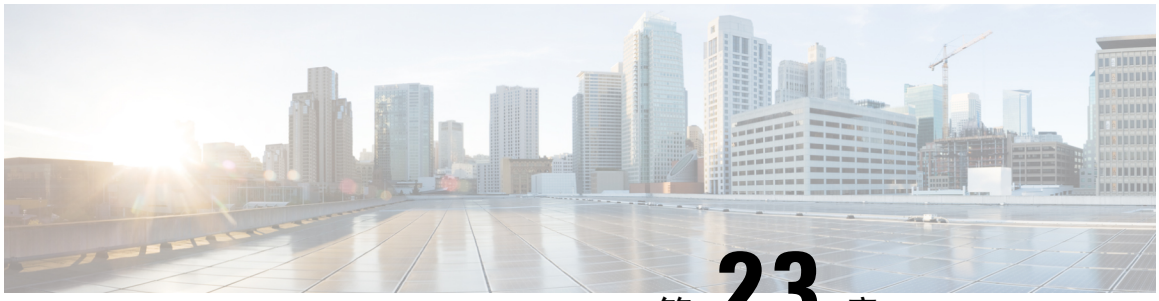
将操作从丢弃更改为警告减少误报带来的影响。相反，如果对于某条规则看到的是大量攻击流量，则可将警告规则更改为丢弃规则。

如果为入侵策略配置系统日志服务器，入侵事件的消息 ID 则为 430001。

入侵策略示例

使用案例章节涵盖以下实施入侵策略的示例。

- 如何阻止威胁，第 51 页
- 如何被动监控网络上的流量，第 71 页



第 23 章

网络地址转换 (NAT)

以下主题介绍网络地址转换 (NAT) 及其配置方法。

为何使用 NAT？

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

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

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

NAT 的其他功能包括：

- 安全 - 隐藏内部 IP 地址可以阻止直接攻击。
- IP 路由解决方案 - 使用 NAT 时不会出现重叠 IP 地址。
- 灵活性 - 可以更改内部 IP 寻址方案，而不影响外部的可用公用地址；例如，对于可以访问互联网的服务器，可以维护供互联网使用的固定 IP 地址，但在内部，可以更改服务器地址。

- 在 IPv4 和 IPv6 之间转换（仅路由模式）- 如果想将 IPv6 网络连接到 IPv4 网络，可以利用 NAT 在两种类型的地址之间转换。

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

NAT 基础知识

以下主题介绍一些 NAT 基础知识。

NAT 术语

本文档使用以下术语：

- 实际地址/主机/网络/接口 - 实际地址是指在主机上定义的转换前地址。在内部网络访问外部网络时，要转换内部网络的典型 NAT 场景中，内部网络会成为“实际”网络。请注意，您可以转换连接到设备的任何网络，而不是只在网络内部转换。因此，如果配置 NAT 以转换外部地址，“实际”可以是指访问内部网络时的外部网络。
- 映射地址/主机/网络/接口 - 映射地址是指实际地址转换而成的地址。在内部网络访问外部网络时，要转换内部网络的典型 NAT 场景中，外部网络会成为“映射”网络。

注释 在地址转换过程中，不会转换为设备接口配置的 IP 地址。

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

NAT 类型

可以使用以下方法实施 NAT：

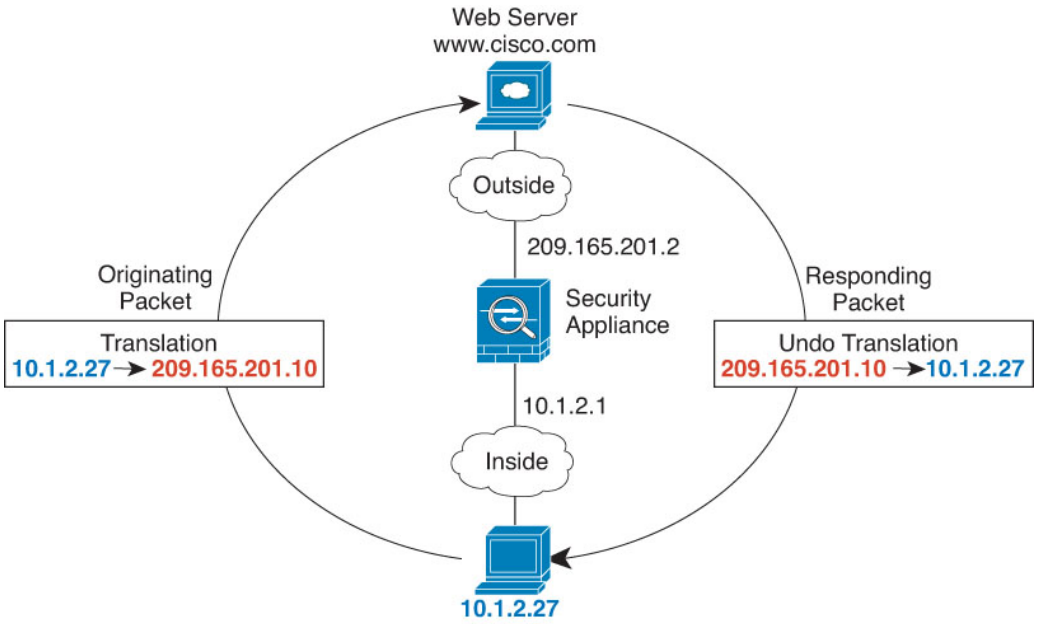
- 动态 NAT - 按先到先得的方式，将一组实际 IP 地址映射到一组映射 IP 地址（通常较小）。仅实际主机可以发起流量。请参阅动态 NAT，第 538 页。
- 动态端口地址转换 (PAT) - 使用 IP 地址的唯一源端口，将一组实际 IP 地址映射到单一 IP 地址。请参阅动态 PAT，第 543 页。
- 静态 NAT - 实际 IP 地址和映射 IP 地址之间的一致映射。允许发起双向流量。请参阅静态 NAT，第 547 页。

- 身份 NAT - 系统将实际地址静态转换为其本身，基本绕过 NAT。当您想转换一大组地址，但又想豁免一小部分地址时，可能就要这样配置 NAT。请参阅身份 NAT，第 555 页。

路由模式下的 NAT

下图显示路由模式下的一个典型 NAT 示例，专用网络位于内部。

图 *35: NAT* 示例：路由模式



1. 当位于 10.1.2.27 的内部主机向 Web 服务器发送数据包时，数据包的实际源地址 10.1.2.27 会转换为映射地址 209.165.201.10。
2. 当服务器响应时，它会将响应发送到映射地址 209.165.201.10，威胁防御设备 接收数据包，因为威胁防御设备 执行代理 ARP 以认领数据包。
3. 接下来，威胁防御设备 变更从映射地址 209.165.201.10 回到实际地址 10.1.2.27 的转换，然后再发送到主机。

自动 NAT 和手动 NAT

可以通过以下两种方法实施地址转换：自动 *NAT* 和手动 *NAT*。

我们建议使用自动 NAT，除非您需要手动 NAT 提供的额外功能。自动 NAT 更容易配置，而且可能对应用（例如 IP 语音 [VoIP]）更加可靠。（对于 VoIP，对不属于规则中使用的任何对象的间接地址进行转换可能会失败。）

自动 NAT

配置为网络对象参数的所有 NAT 规则都被视为自动 *NAT* 规则。这是一种为网络对象配置 NAT 的快捷方法。但是，您无法为对象组创建这些规则。

尽管这些规则配置为对象的一部分，但是您通过对象管理器无法看到对象定义中的 NAT 配置。

当数据包进入接口时，系统会根据自动 NAT 规则来检查源和目标 IP 地址。如果进行独立匹配，可根据独立规则转换数据包中的源地址和目标地址。这些规则互不牵连，可以根据流量使用不同的规则组合。

因为规则从未配对，所以不能指定源 A/目的 A 应当有不同于源 A/目的 B 的转换。手动 NAT 用于实现这样的功能：您可以识别单个规则中的源和目标地址。

手动 NAT

手动 NAT 供您在单个规则中同时标识源和目标地址。同时指定源和目标地址，可以让您指定源 A/目的 A 有不同于源 A/目的 B 的转换。

注释 对于静态 NAT，规则是双向的，因此，请注意，这整个指南中命令和说明中使用的“源”和“目标”，即便是给定的连接，也可能源自“目标”地址。例如，如果配置支持端口地址转换的静态 NAT，然后将源地址指定为某台 Telnet 服务器，并且希望进入该 Telnet 服务器的所有流量都将端口从 2323 转换为 23，那么您就必须指定要转换的源端口（实际端口：23，映射端口：2323）。必须指定源端口是因为您已将 Telnet 服务器地址指定为源地址。

目标地址是可选的。如果指定目标地址，可以将其映射到其本身（身份 NAT），也可以将其映射到不同的地址。目的映射始终是静态映射。

比较自动 NAT 和手动 NAT

这两类 NAT 之间的主要差异是：

- 定义实际地址的方法。
  - 自动 NAT - NAT 规则成为网络对象的参数。网络对象 IP 地址用作原始（实际）地址。
  - 手动 NAT- 标识实际地址和映射地址的网络对象或网络对象组。在这种情况下，NAT 不是网络对象的参数；网络对象或组是NAT配置的参数。能够使用实际地址的网络对象组意味着手动 NAT 更具可扩展性。
- 实施源和目标 NAT 的方法。
  - 自动 NAT- 每个规则都可应用到数据包的源或目标。因此，可能使用两条规则，一条用于源IP地址，一条用于目标IP地址。这两条规则不能绑在一起对源/目的组合进行特定转换。
  - 手动 NAT- 单一规则可以同时转换源和目标。数据包仅匹配一条规则，且不再检查其他规则。即使您不配置可选目标地址，匹配的数据包仍仅匹配一个 手动 NAT 规则。源和目的绑在一起，使您可以根据源/目的组合进行不同的转换。例如，源 A/目的 A 可以有不同于源 A/目的 B 的转换。

- NAT 规则顺序。
  - 自动 NAT- 在 NAT 表中自动排序。
  - 手动 NAT - 在 NAT 表中手动排序（在自动 NAT 规则之前或之后）。

NAT 规则顺序

自动 NAT 和手动 NAT 规则存储在分为三个部分的单个表中。首先应用第一部分规则，其次是第二部分，最后是第三部分，直到找到匹配项为止。例如，如果在第一部分找到匹配项，则不评估第二部分和第三部分。下表显示每个部分的规则顺序。

注释 还有一个第 0 部分，其中包含系统创建供自己使用的任何 NAT 规则。这些规则优先于所有其他规则。系统会自动创建这些规则并根据需要清除 xlate。您不能在第 0 部分中添加、编辑或修改规则。

表 *12: NAT* 规则表

表部分	规则类型	部分中的规则顺序
第 1 部分	手动 NAT	系统按照在配置中出现的顺序应用第一个匹配的规则。因为会应用第一个匹配规则，所以必须确保具体规则位于更加通用的规则前面，否则无法按预期应用特定规则。默认情况下，手动 NAT 规则会添加到第 1 部分。 “具体规则优先”是指： • 静态规则应放在动态规则前面。 • 包含目的地转换的规则应仅放在具有源转换的规则前面。 如果无法消除重叠规则（其中可能有多个规则基于源或目标地址而应用），请特别注意遵循这些建议。

表部分	规则类型	部分中的规则顺序
第 2 部分	自动 NAT	如果在第 1 部分未找到匹配项，则会按照以下顺序应用第 2 部分的规则： **1.** 静态规则。 **2.** 动态规则。 **在每个规则类型中，遵循以下排序准则：** **1.** 实际 IP 地址数量 - 从最小到最大。例如，带一个地址的对象将在带 10 个地址的对象之前进行评估。 **2.** 如果数量相同，则按从最低到最高的顺序使用 IP 地址编号。例如，10.1.1.0 在 11.1.1.0 之前进行评估。 **3.** 如果使用同一 IP 地址，则按字母数字顺序使用网络对象名称。例如，abracadabra 在 catwoman 之前进行评估。
第 3 部分	手动 NAT	如果仍未找到匹配项，则按照在配置中出现的顺序，应用第三部分规则的第一个匹配项。此部分应当包含最通用的规则。还必须确保此部分的特定规则位于通用规则之前，否则会应用通用规则。

例如，对于第二部分规则，在网络对象中定义以下 IP 地址：

- 192.168.1.0/24（静态）
- 192.168.1.0/24（动态）
- 10.1.1.0/24（静态）
- 192.168.1.1/32（静态）
- 172.16.1.0/24（动态）（对象 def）
- 172.16.1.0/24（动态）（对象 abc）

结果排序可能是：

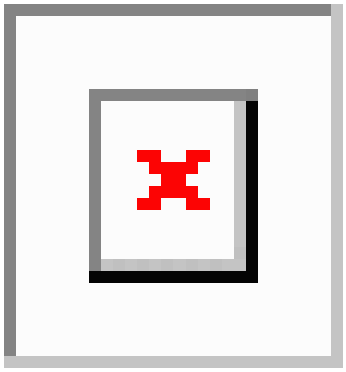
- 192.168.1.1/32（静态）
- 10.1.1.0/24（静态）
- 192.168.1.0/24（静态）
- 172.16.1.0/24（动态）（对象 abc）
- 172.16.1.0/24（动态）（对象 def）
- 192.168.1.0/24（动态）

NAT 接口

除了网桥组成员接口，您可以将NAT规则配置为应用到任何接口（也就是，所有接口），或者也可以标识特定的实际接口和映射接口。还可以为实际地址指定任何接口，为映射地址指定特定接口，反之亦然。

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

图 *36:* 指定任何接口



然而，“任何”接口的概念不适用于网桥组成员接口。当指定“任何”接口时，NAT 将排除所有网桥组成员接口。因此，要将NAT应用于网桥组成员，必须指定成员接口。这样可能导致有许多只有一个接口不同的类似规则。您不能为桥接虚拟接口(BVI)本身配置NAT，只能为成员接口配置NAT。

不能为被动接口配置 NAT。

为 NAT 配置路由

威胁防御 设备需要成为发送到转换（映射）地址的所有数据包的目标。

在发送数据包时，设备使用目标接口（如果指定了接口）或路由表查找（如果未指定接口）来确定出口接口。对于身份 NAT，即使指定了目标接口，您也可以选择使用路由查找。

所需的路由配置类型取决于映射地址的类型，以下主题对此进行了说明。

地址与映射接口在相同的网络中

如果使用与目标（映射）接口在同一网络中的地址，威胁防御设备使用代理ARP应答映射地址的任何 ARP 请求，从而拦截发往映射地址的流量。此解决方案可以简化路由，因为 威胁防御设备 不必成为任何其他网络的网关。如果外部网络包含足够多的空闲地址，并且您正在使用 1:1 转换（例如动态 NAT 或静态 NAT），此解决方案是理想选择。动态 PAT 可显著增加您可以通过少量地址实现的转换数量，因此即使外部网络中的可用地址较少，依然可以使用此方法。对于 PAT，甚至可以使用映射接口的 IP 地址。

唯一网络中的地址

如果需要比目标（映射）接口网络上提供的地址更多的地址，则可以识别其他子网中的地址。上游路由器需要对指向 威胁防御设备 的映射地址进行静态路由。

与实际地址相同的地址（身份 NAT）

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

通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。例如，如果为“任何”IP 地址配置一条大体的身份 NAT 规则，则使代理 ARP 保持启用状态会给直接连接到映射接口的网络上的主机造成问题。在这种情况下，当映射网络上的主机要与同一网络上的其他主机通信时，ARP 请求中的地址匹配 NAT 规则（匹配“任何”地址）。然后，威胁防御设备 将代理地址的 ARP，即使数据包实际上不以 威胁防御设备 为目标。（请注意，即便已设置手动 NAT 规则，也会造成此问题；虽然NAT规则必须匹配源地址和目标地址，但仅会根据“源”地址作出代理ARP决定）。如果在实际主机 ARP 响应之前收到 威胁防御设备 ARP 响应，则流量会错误地发送到 威胁防御设备。

NAT 准则

以下主题提供有关实施 NAT 的详细准则。

接口准则

标准路由物理接口或子接口都支持 NAT。

但是，在网桥组成员接口（作为桥接虚拟接口或 BVI 一部分的接口）上配置 NAT 有以下限制：

- 为网桥组的成员配置 NAT 时，需要指定成员接口。您不能为网桥组接口 (BVI) 本身配置 NAT。
- 在网桥组成员接口之间执行 NAT 时，必须指定源接口和目标接口。不能指定“任何”作为接口。
- 当目标接口为网桥组成员接口时，不能配置接口 PAT，因为没有连接到该接口的 IP 地址。
- 当源接口和目标接口是同一网桥组的成员时，不能在 IPv4 和 IPv6 网络 (NAT64/46) 之间进行转换。静态 NAT/PAT 44/66、动态 NAT44/66 和动态 PAT44 是唯一允许的方法；不支持动态 PAT66。

IPv6 NAT 准则

NAT 支持 IPv6，但有以下准则和限制。

- 对于标准路由模式接口，您还可以在 IPv4 和 IPv6 之间进行转换。

- 对于同一个网桥组的成员接口，不能在 IPv4 和 IPv6 之间进行转换，而只能在两个 IPv6 或两个 IPv4 网络之间进行转换。此限制不适用于一个接口为网桥组成员，另一个为标准路由接口的情况。
- 在同属一个网桥组的接口之间进行转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于一个接口为网桥组成员，另一个为标准路由接口的情况。
- 对于静态 NAT，可以指定一个最大 /64 的 IPv6 子网。不支持更大的子网。
- 将 FTP 和 NAT46 配合使用时，当 IPv4 FTP 客户端连接到 IPv6 FTP 服务器时，客户端必须使用扩展被动模式 (EPSV) 或扩展端口模式 (EPRT)；在使用 IPv6 时，不支持 PASV 和 PORT 命令。

IPv6 NAT 最佳实践

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

- NAT66（IPv6 对 IPv6）- 我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。如果不想允许返回流量，您可以启用单向静态 NAT 规则（仅限于手动 NAT）。
- NAT46（IPv4 对 IPv6）- 我们建议使用静态 NAT。因为 IPv6 地址空间远远大于 IPv4 地址空间，所以可以轻松满足静态转换需求。如果不想允许返回流量，您可以启用单向静态 NAT 规则（仅限于手动 NAT）。转换为 IPv6 子网（/96 或更低）时，默认情况下，生成的映射地址为有嵌入 IPv4 的 IPv6 地址，其中 32 位 IPv4 地址嵌入在 IPv6 前缀后面。例如，如果 IPv6 前缀为 /96 前缀，则 IPv4 地址附在最后的 32 位地址中。例如，如果将 192.168.1.0/24 映射到 201b::0/96，则 192.168.1.4 将被映射到 201b::0.192.168.1.4（通过混合表示法显示）。如果前缀较小（例如 /64），则 IPv4 地址附在前缀的后面，后缀 0 附在 IPv4 地址后面。
- NAT64（IPv6 到 IPv4）- 可能没有足够的 IPv4 地址来容纳大量的 IPv6 地址。我们建议使用动态 PAT 池提供大量的 IPv4 转换。

对检测到的协议的 NAT 支持

检测打开辅助连接或者在数据包中嵌入 IP 地址的一些应用层协议，以提供以下服务：

- 创建小孔 - 一些应用协议在标准端口或协商的端口上打开辅助 TCP 或 UDP 连接。检测会为这些辅助端口打开小孔，使您无需创建访问控制规则予以允许。
- NAT 重写 - 诸如 FTP 等协议会在数据包数据中嵌入用于辅助连接的 IP 地址和端口，作为协议的一部分。如果 NAT 转换涉及到任一终端，则检测引擎会重写数据包数据以反映嵌入式地址和端口的 NAT 转换。在没有 NAT 重写的情况下，辅助连接不起作用。
- 协议实施 - 一些检测会为检测到的协议实施某种程度的 RFC 一致性。

下表列出了应用 NAT 重写及其 NAT 限制的检测到的协议。当编写包括这些协议的 NAT 规则时，请记住这些限制。此处未列出的协议不应用 NAT 重写。这些检测包括 GTP、HTTP、IMAP、POP、SMTP、SSH 和 SSL。

注释 仅列出的端口支持 NAT 重写。如果在非标准端口上使用这些协议，请勿对连接使用 NAT。

表 *13: NAT* 支持的应用检测

应用	检测到的协议、端口	NAT 限制	创建了小孔
DCERPC	TCP/135	无 NAT64。	是
Diameter	TCP/3868 TCP/5868（用于 TCP/TLS） SCTP/3868	无 NAT/PAT。	是
DNS over UDP	UDP/53	无可用于通过 WINS 进行名称解析的 NAT 支持。	否
ESMTP	TCP/25	无 NAT64。	否
FTP	TCP/21	没有限制。	兼容
GTP	UDP/3386 (GTPv0) UDP/2123 (GTPv1+)	无扩展 PAT。 无 NAT。	—
H.323 H.225（呼叫信令） H.323 RAS	TCP/1720 UDP/1718 对于 RAS， 则为 UDP/1718-1719	无 NAT64。	是
ICMP ICMP 错误	ICMP （从不会对定向到设备接口的 ICMP 流量进行检测。）	没有限制。	否
IP 选项	RSVP	无 NAT64。	否
M3UA	SCTP/2905	无面向嵌入式地址的 NAT 或 PAT。	-
NetBIOS Name Server over IP	UDP/137、138（源端口）	无 NAT64。	否
RSH	TCP/514	无 PAT。 无 NAT64。	兼容

应用	检测到的协议、端口	NAT 限制	创建了小孔
RTSP	TCP/554 （对于 HTTP 隐藏没有任何处理。）	无 NAT64。	兼容
SIP	TCP/5060 UDP/5060	无扩展 PAT。 无 NAT64 或 NAT46。	兼容
Skinny (SCCP)	TCP/2000	无 NAT64、NAT46 或 NAT66。	兼容
SQL*Net （版本 1、2）	TCP/1521	无 NAT64。	兼容
SCTP	SCTP	虽然可以对 SCTP 流量执行静态网络对象 NAT（无动态 NAT/PAT），但检测引擎不用于 NAT。	不支持
Sun RPC	TCP/111 UDP/111	无 NAT64。	是
TFTP	UDP/69	无 NAT64。 不转换负载 IP 地址。	是
XDMCP	UDP/177	无 NAT64。	兼容

FQDN 目的准则

您可以使用完全限定域名 (FQDN) 网络对象而不是 IP 地址在手动 NAT 规则中指定转换（映射）目的。例如，您可以基于发往 www.example.com Web 服务器的流量创建规则。

使用 FQDN 时，系统基于返回的地址获取 DNS 解析并编写 NAT 规则。如果从 DNS 服务器获取多个地址，则使用的地址基于以下条件：

- 如果某个地址与指定接口位于相同的子网上，则使用该地址。如果没有地址位于相同的子网上，则使用返回的第一个地址。
- 转换后的源和转换后的目的的 IP 类型必须匹配。例如，如果转换后的源地址为 IPv6，则 FQDN 对象必须指定 IPv6 作为地址类型。如果转换后的源为 IPv4，则 FQDN 对象可以指定 IPv4 或 IPv4 和 IPv6。在这种情况下，将选择 IPv4 地址。

不能在用于手动 NAT 目的的网络组中包含 FQDN 对象。在 NAT 中，必须单独使用 FQDN 对象，因为只有单个目的主机才适用于此类 NAT 规则。

如果 FQDN 无法解析为 IP 地址，则在获得 DNS 解析之前该规则不起作用。

其他 NAT 准则

- 对于作为网桥组成员的接口，您需要为成员接口编写 NAT 规则。您无法为桥接虚拟接口 (BVI) 本身编写 NAT 规则。
- 您不能为站点间 VPN 中使用的虚拟隧道接口 (VTI) 编写 NAT 规则。为 VTI 的源接口编写规则不会将 NAT 应用于 VPN 隧道。要编写应用于 VTI 上通过隧道传输的 VPN 流量的 NAT 规则，您必须使用“任何”作为接口，而不能明确指定接口名称。
- （仅限于 自动 NAT。）您仅可为给定对象定义单个 NAT 规则，如果要为某个对象配置多个 NAT 规则，则需要创建通过不同名称指定同一 IP 地址的多个对象。
- 如果在接口上定义了 VPN，则接口上的入站 ESP 流量不受 NAT 规则的约束。系统仅允许已建立的 VPN 隧道的 ESP 流量，而丢弃与现有隧道不相关的流量。此限制适用于 ESP 和 UDP 端口 500 和 4500。
- 如果在应用动态 PAT 设备之后的某设备上定义站点间 VPN，以便 UDP 端口 500 和 4500 不是实际使用的端口，必须从 PAT 设备之后的设备发起连接。响应方无法发起安全关联 (SA)，因为不知道正确的端口号。
- 如果更改 NAT 配置，并且不想等待现有转换超时后再使用新 NAT 配置，则可以在设备 CLI 中使用 **clear xlate** 命令清除转换表。然而，清除转换表将断开使用转换的当前所有连接。

  如果创建应应用于现有连接（例如 VPN 隧道）的新 NAT 规则，则需要使用 **clear conn** 来终止连接。然后，尝试重新建立连接应符合 NAT 规则，且连接应正确进行 NAT。

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

- 不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。
- NAT 中使用的网络对象不能包含超过 131838 个 IP 地址，无论是显式还是隐式包含在地址或子网范围中。将地址空间分成更小的范围，并为较小的对象编写单独的规则。
- （仅限于手动 NAT。）在 NAT 规则中使用 **any** 作为源地址时，“任何”流量（IPv4 与 IPv6）的定义取决于规则。只有数据包为 IPv6 至 IPv6 或 IPv4 至 IPv4，威胁防御设备 才能对数据包执行 NAT；借助此前提条件，威胁防御设备 可确定 NAT 规则中的 **any** 的值。例如，如果配置从“任何”到 IPv6 服务器的规则，且该服务器已从 IPv4 地址映射，则**任何**指“任何 IPv6 流量”。如果配置从“任何”到“任何”的规则，并且将源映射至接口 IPv4 地址，则**任何**指“任何 IPv4 流量”，因为映射的接口地址意味着目标也是 IPv4。
- 可以在多条 NAT 规则中使用同一映射对象或组。
- 映射 IP 地址池不能包括：
  - 映射接口的 IP 地址。如果为该规则指定“任何”接口，则禁止所有接口 IP 地址。对于接口 PAT（仅路由模式），指定接口名称而不是接口地址。

- 故障转移接口 IP 地址。
- （动态 NAT。）启用 VPN 时的备用接口 IP 地址。

- 避免在静态和动态 NAT 策略中使用重叠地址。例如，使用重叠地址，如果 PPTP 的辅助连接命中静态而非动态 xlate，将无法建立 PPTP 连接。
- 无法在 NAT 规则的源地址和远程访问 VPN 地址池中使用重叠地址。
- 如果在规则中指定目标接口，则该接口用作出口接口，而不是在路由表中查找路由。但是，对于身份 NAT，您可以选择改为使用路由查找。
- NAT 仅适用于直通流量。系统生成的流量不进行 NAT。
- 请不要使用大写或小写字母的任意组合来命名网络对象或组 pat-pool。
- 不能在协议无关组播 (PIM) 寄存器的内部负载上使用 NAT。
- (手动 NAT) 为双 ISP 接口设置（使用路由配置中的服务级别协议的主接口和备用接口）编写 NAT 规则时，请勿在规则中指定目标条件。确保主接口的规则在备用接口的规则之前。这允许设备在主 ISP 不可用时根据当前路由状态选择正确的 NAT 目的接口。如果指定目标对象，NAT 规则将始终为其他规则选择主接口。
- 如果您收到不应与为接口定义的 NAT 规则匹配的流量的 ASP drop reason nat-no-xlate-to-pat-pool，请为受影响的流量配置身份 NAT 规则，以便流量可以不经转换地通过。
- 如果为 GRE 隧道终端配置 NAT，则您必须在终端上禁用保持连接，否则将无法建立隧道。终端将保持连接发送到原始地址。

配置 NAT

网络地址转换可能非常复杂。我们建议规则应尽可能保持简单，以避免出现转换问题和难以进行故障排除的情况。在实施 NAT 之前仔细规划，这非常重要。以下程序说明了规划的基本方法。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 决定您需要哪些类型的规则。

可以创建动态 NAT、动态 PAT、静态 NAT 和身份 NAT 规则。有关概述，请参阅 NAT 类型，第 526 页。

步骤 3 决定应将哪些规则作为手动或自动 NAT 来实施。

有关这两种实施选项的比较，请参阅自动 NAT 和手动 NAT，第 527 页。

步骤 4 遵循以下部分中的说明创建规则。

- 动态 NAT，第 538 页

- 动态 PAT，第 543 页
- 静态 NAT，第 547 页
- 身份 NAT，第 555 页

步骤 5 管理 NAT 策略和规则。

您可以执行以下操作来管理策略及其规则。

- 要编辑规则，请点击规则的编辑图标 ( )。
- 要删除某条规则，请点击该规则的删除图标 ( )。

动态 NAT

以下主题介绍动态 NAT 以及如何配置动态 NAT。

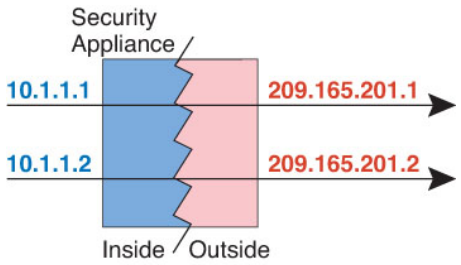
关于动态 NAT

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

注释 在转换期间，如果访问规则允许连接转换后主机，远程主机可以发起这种连接。因为地址不可预测，所以与主机的连接不可能发生。然而，在这种情况下，可以依靠访问规则的安全性。远程主机的成功连接可重置连接的空闲计时器。

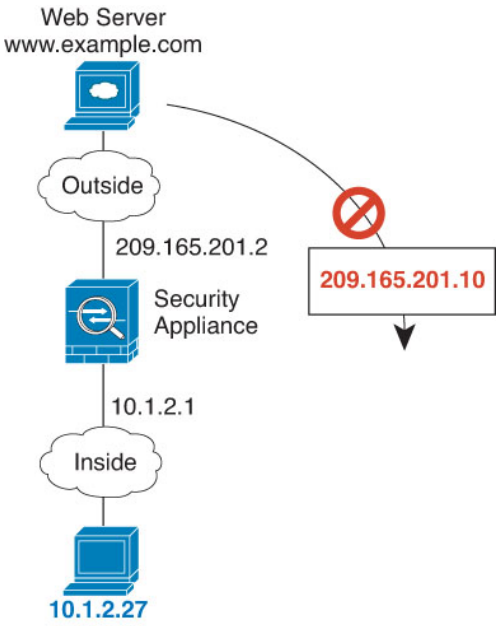
下图显示典型的动态 NAT 场景。仅实际主机可以创建 NAT 会话，允许返回响应流量。

图 *37:* 动态 *NAT*



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

图 *38:* 远程主机尝试向映射地址发起连接



动态 NAT 的优缺点

动态 NAT 有以下缺点：

- 如果映射池的地址少于实际组，并且流量数量大于预期，地址可能会用尽。

  如果经常发生这种情况，请使用 PAT 或 PAT 回退方法，因为 PAT 可以使用单一地址的端口提供超过 64,000 次转换。

- 不得不利用映射池中的大量可路由地址，而且可能没有大量的可路由地址可用。

动态 NAT 的优点在于，某些协议不能使用 PAT。PAT 不适用于以下项：

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

配置动态自动 NAT

使用动态自动 NAT 规则将地址转换为可在目标网络中路由的其他 IP 地址。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义NAT规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。

- **转换后的地址** - 该地址可以是网络对象或组，但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。 如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ()。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**自动 NAT**。
- **类型** - 选择**动态**。

步骤 4 配置以下数据包转换选项：

- **源接口**、**目标接口** -（网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。
- **原始地址** - 包含您要转换的地址的网络对象。
- **转换后的地址** - 包含映射地址的网络对象或组。

步骤 5 （可选。）点击**高级选项**链接并选择所需的选项：

- **转换与此规则匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 596 页。
- **跳转到接口 PAT（目标接口）** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。

步骤 6 点击**确定 (OK)**。

配置动态手动 NAT

当自动 NAT 不能满足您的需求时，请使用动态手动 NAT 规则。例如，如果您要根据目标进行不同的转换。动态 NAT 会将地址转换为可在目标网络中路由的其他 IP 地址。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源地址** - 地址可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何**。
- **转换后的源地址** - 此选项可以是网络对象或组，但不能包含在子网中。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。 如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。

如果您要在规则中为**原始目标地址**和**转换后的目标地址**配置静态转换，还可以为这些地址创建网络对象。

对于动态 NAT，您还可以对目标执行端口转换。在对象管理器中，请确保有可用于**原始目标端口**和**转换后的目标端口**的端口对象。系统将忽略您指定的源端口。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

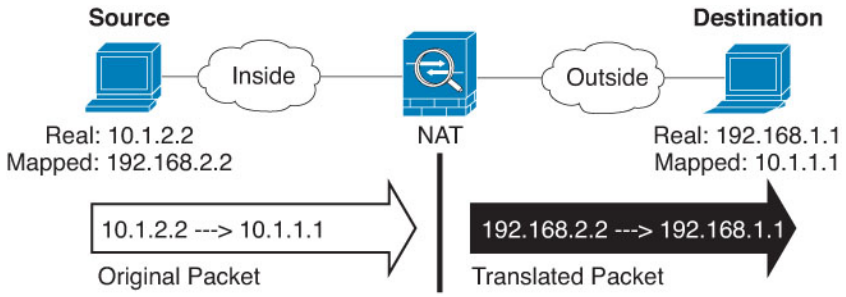
- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**手动 NAT**。
- **规则位置** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。
- **类型** - 选择**动态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。

步骤 4 配置以下接口选项：

- **源接口**、**目标接口** -（网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



- **原始源地址** - 包含将要转换的地址的网络对象或组。
- **原始目标地址** -（可选。）包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

  可以依次选择**接口**以使原始目标基于源接口（不能为“任意”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源地址** - 包含映射地址的网络对象或组。
- **转换后的目标地址** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标地址**选择了一个对象，则可以通过选择相同的对象设置身份 NAT（即无转换）。

步骤 7 （可选。）确定用于服务转换的目标服务端口：**原始目标端口**、**转换后的目标端口**。

动态 NAT 不支持端口转换，因此，请将**原始源端口**和**已转换源端口**字段保留为空。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

步骤 8 （可选。）点击**高级选项**链接并选择所需的选项：

- **转换与此规则匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的 DNS 回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 596 页。
- **跳转到接口 PAT（目标接口）** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。

步骤 9 点击**确定 (OK)**。

动态 PAT

以下主题介绍动态 PAT。

关于动态 PAT

通过将实际地址和源端口转换为映射地址和唯一端口，动态 PAT 可以将多个实际地址转换为单一映射地址。

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

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

图 *39:* 动态 *PAT*

对于转换持续时间，如果访问规则允许，目标网络上的远程主机可以发起到转换后主机的连接。因为端口地址（实际和映射）不可预测，所以到该主机的连接不可能发生。然而，在这种情况下，可以依靠访问规则的安全性。

在连接过期后，端口转换也将过期。

注释 建议每个接口使用不同的 PAT 池。如果多个接口使用同一池，尤其是用于“任何”接口时，该池将被快速耗尽，且没有端口可用于新的转换。

动态 PAT 的优缺点

通过动态 PAT，可以使用单一映射地址，从而保存可路由地址。甚至可以将 威胁防御设备 接口 IP 地址用作 PAT 地址。但是，不能将接口 PAT 用于接口上的 IPv6 地址。

在同属一个网桥组的接口之间进行转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于一个接口为网桥组成员，另一个为标准路由接口的情况。

动态 PAT 不适用于某些数据流不同于控制路径的多媒体应用。有关详细信息，请参阅对检测到的协议的 NAT 支持，第 533 页。

动态 PAT 还可以创建大量显示为来自单一 IP 地址的连接，服务器可能将此流量解释为 DoS 攻击。

配置动态自动 PAT

使用动态自动 PAT 规则可将地址转换为唯一的 IP 地址/端口组合，而不是仅转换为多个 IP 地址。可以转换为单个地址，即目标接口的地址或其他地址。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义NAT规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的地址** - 可以通过以下选项指定 PAT 地址：
  - **目标接口** - 要使用目标接口 IPv4 地址，不需要网络对象。您不能将接口 PAT 用于 IPv6。
  - **单个 PAT 地址** - 创建包含单个主机的网络对象。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ()。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**自动 NAT**。
- **类型** - 选择**动态**。

步骤 4 配置以下数据包转换选项：

- **源接口**、**目标接口** - （网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。
- **原始地址** - 包含您要转换的地址的网络对象。
- **转换后的地址** - 以下项之一：
  - （接口 PAT。）要使用目标接口的 IPv4 地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。您不能将接口 PAT 用于 IPv6。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。

步骤 5 （可选。）点击**高级选项**链接并选择所需的选项：

- **跳转到接口 PAT（目标接口）**- 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。如果已配置接口 PAT 作为转换后的地址，则不能选择此选项。您也不能将此选项用于 IPv6 网络。

步骤 6 点击**确定 (OK)**。

配置动态手动 PAT

当自动 PAT 不能满足您的需求时，请使用动态手动 PAT 规则。例如，如果您要根据目标进行不同的转换。动态 PAT 可将地址转换为唯一的 IP 地址/端口组合，而不是仅转换为多个 IP 地址。可以转换为单个地址，即目标接口的地址或其他地址。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源地址** - 地址可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何**。
- **转换后的源地址** - 您可通过以下选项指定 PAT 地址：
  - **目标接口** - 要使用目标接口 IPv4 地址，不需要网络对象。您不能将接口 PAT 用于 IPv6。
  - **单个 PAT 地址** - 创建包含单个主机的网络对象。

如果您要在规则中为**原始目标地址**和**转换后的目标地址**配置静态转换，还可以为这些地址创建网络对象。

对于动态 PAT，您还可以对目标执行端口转换。在对象管理器中，请确保有可用于**原始目标端口**和**转换后的目标端口**的端口对象。系统将忽略您指定的源端口。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**手动 NAT**。
- **规则位置** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。

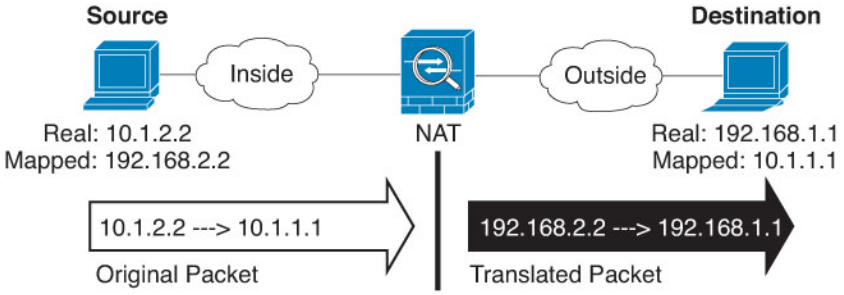
- **类型** - 选择**动态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。

步骤 4 配置以下接口选项：

- **源接口**、**目标接口** -（网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



- **原始源地址** - 包含将要转换的地址的网络对象或组。
- **原始目标地址** -（可选。）包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

  可以依次选择**接口** 以使原始目标基于源接口（不能为“任意”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源地址** - 以下项之一：
  - （接口 PAT。）要使用目标接口的 IPv4 地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。您不能将接口 PAT 用于 IPv6。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。
- **转换后的目标地址** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 （可选。）确定用于服务转换的目标服务端口：**原始目标端口**、**转换后的目标端口**。

动态 NAT 不支持端口转换，因此，请将**原始源端口**和**已转换源端口**字段保留为空。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

步骤 8 （可选。）点击**高级选项**链接并选择所需的选项：

- **跳转到接口 PAT（目标接口）**- 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。如果已配置接口 PAT 作为转换后的地址，则不能选择此选项。您也不能将此选项用于 IPv6 网络。

步骤 9 点击**确定 (OK)**。

静态 NAT

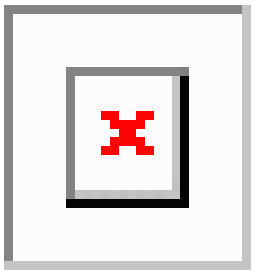
以下主题介绍静态 NAT 以及如何实施静态 NAT。

关于静态 NAT

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

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

图 *40:* 静态 *NAT*



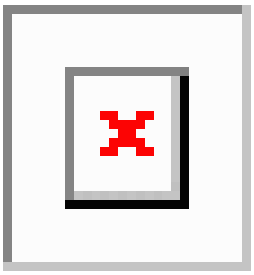
支持端口转换的静态 NAT

支持端口转换的静态 NAT 让您可以指定实际和映射协议及端口。

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

下图显示支持端口转换的典型静态NAT场景，其中显示映射到本身的端口和映射到不同值的端口；在这两种情况下，IP 地址映射到不同值。转换始终处于活动状态，所以，转换后主机和远程主机可以发起连接。

图 *41:* 支持端口转换的典型静态 *NAT* 场景



支持端口转换的静态 NAT 规则支持仅访问指定端口的目标 IP 地址。如果您尝试访问其他端口上 NAT 规则未涵盖的的目标 IP 地址，连接将被阻止。此外，对于手动 NAT，如果流量与 NAT 规则的源 IP 地址不匹配，但与目标 IP 地址匹配，流量将被丢弃，不管目标端口为何。因此，您必须为允许发送到目标 IP 地址的所有其他流量添加额外规则。例如，您可以为 IP 地址配置静态 NAT 规则（不含端口规范），并将其放置在端口转换规则后面。

注释 对于需要对辅助信道执行应用检查的应用（例如 FTP 和 VoIP），NAT 会自动转换辅助端口。

下面是使用支持端口转换的静态 NAT 的其他情况。

具有身份端口转换的静态 NAT

可以简化对内部资源的外部访问。例如，如果您有在不同端口上提供服务（例如 FTP、HTTP 和 SMTP）的三个单独的服务器，可以为外部用户提供单个 IP 地址以访问这些服务。然后，可以配置具有身份端口转换的静态NAT，从而根据尝试访问的端口将单个外部IP地址映射到实际服务器的正确 IP 地址。您无需更改端口，因为服务器使用的是标准端口（分别是 21、80 和 25)。

对非标准端口进行端口转换的静态 NAT

还可以利用支持端口转换的静态 NAT 将一个公认端口转换为一个非标准端口，反之亦然。例如，如果内部 Web 服务器使用端口 8080，可以允许外部用户连接到端口 80，然后取消转换到原始端口 8080。同样，要进一步提高安全性，可以告知 Web 用户连接到非标准端口 6785，然后取消转换到端口 80。

具有端口转换的静态接口 NAT

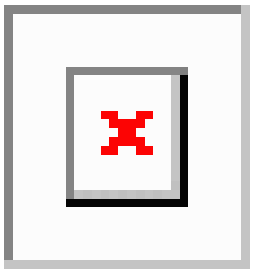
可以配置静态NAT，以将一个实际地址映射到一个接口地址/端口组合。例如，如果要将对设备外部接口的 Telnet 访问重定向至内部主机，则可以将内部主机 IP 地址/端口 23 映射到外部接口地址/端口 23。

一对多静态 NAT

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

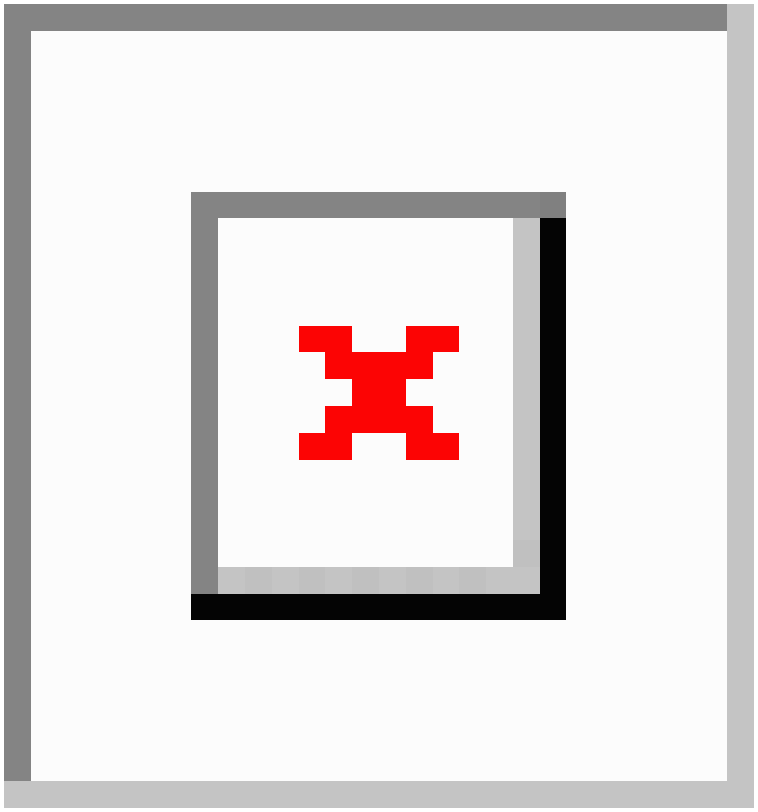
下图显示典型的一对多静态NAT场景。由于实际主机进行的发起的流量始终使用第一个映射地址，因此从技术上说，实际主机 IP/第一个映射 IP 的转换是唯一的双向转换。

图 *42:* 一对多静态 ***NAT***



例如，在 10.1.2.27 上有一个负载均衡器。根据请求的 URL，它会将流量重新定向到正确的 Web 服务器。

图 *43:* 一对多静态 ***NAT*** 示例



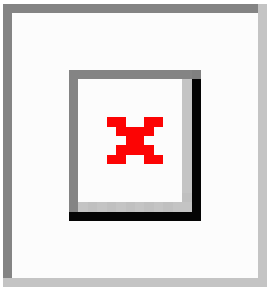
其他映射场景（不推荐）

NAT 具有很高的灵活性，允许任何类型的静态映射场景：不仅包括一对一、一对多，还包括少对多、多对少和多对一映射。我们推荐仅使用一对一或一对多映射。其他映射选项可能会导致意外后果。

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

下图显示典型的少对多静态 NAT 场景。

图 *44:* 少对多静态 *NAT*

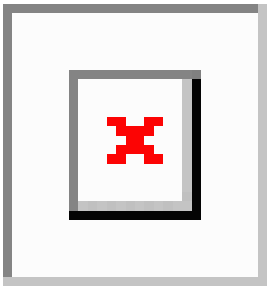


对于实际地址多于映射地址的多对少或多对一配置，映射地址会在实际地址用尽之前先用尽。仅最低实际 IP 地址和映射池之间的映射可以导致双向发起。剩余的更高的实际地址可以发起流量，但不能将流量发起到这些地址（由于五元组 [源 IP、目标 IP、源端口、目标端口、协议] 的唯一性，连接的返回流量会定向到正确的实际地址）。

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

下图显示一个典型的多对少静态 NAT 场景。

图 *45:* 多对少静态 *NAT*



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

配置静态自动 NAT

使用静态自动 NAT 规则将地址转换为可在目标网络中路由的其他 IP 地址。您还可以通过静态 NAT 规则执行端口转换。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义NAT规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的地址** - 您可以通过以下选项指定转换后的地址：
  - **目标接口** - 要使用目标接口 IPv4 地址，不需要网络对象。该选项配置具有端口转换的静态接口NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口PAT用于IPv6。
  - **地址** - 创建包含主机、范围或子网的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；其只能包含一种类型。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ()。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**自动 NAT**。
- **类型** - 选择**静态**。

步骤 4 配置以下数据包转换选项：

- **源接口**、**目标接口** - （网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。
- **原始地址** - 包含您要转换的地址的网络对象。
- **转换后的地址** - 以下项之一：
  - 要使用一组地址，请选择包含映射地址的网络对象或组。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。

- （具有端口转换的静态接口 NAT。）要使用目标接口的地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。您不能将接口 PAT 用于 IPv6。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。

- （可选。）**原始端口**、**转换后的端口** - 如果需要转换 TCP 或 UDP 端口，请选择定义原始端口和转换后的端口的端口对象。对象必须用于相同的协议。如果对象不存在，请点击**创建新对象 (Create New Object)** 链接。例如，如有必要，可以将 TCP/80 转换为 TCP/8080。

步骤 5 （可选。）点击**高级选项**链接并选择所需的选项：

- **转换与此规则相匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 596 页。 如果您在进行端口转换，则此选项不可用。
- **不在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。

步骤 6 点击**确定 (OK)**。

配置静态手动 NAT

当自动 NAT 不能满足您的需求时，请使用静态手动 NAT 规则。例如，如果您要根据目标进行不同的转换。静态 NAT 会将地址转换为可在目标网络中路由的其他 IP 地址。您还可以通过静态 NAT 规则执行端口转换。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源地址** - 地址可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何**。

- **转换后的源地址** - 可以通过以下选项指定转换后的地址：

  - **目标接口** - 要使用目标接口 IPv4 地址，不需要网络对象。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。

  - **地址** - 创建包含主机、范围或子网的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；其只能包含一种类型。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。

如果您要在规则中为**原始目标地址**和**转换后的目标地址**配置静态转换，还可以为这些地址创建网络对象。如果只需要配置支持端口转换的目标静态接口 NAT，则可以跳过为目标映射地址添加对象的过程，并在规则中指定接口。

您还可以对源和/或目标执行端口转换。在对象管理器中，确保有可以用于原始端口和转换后的端口的端口对象。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

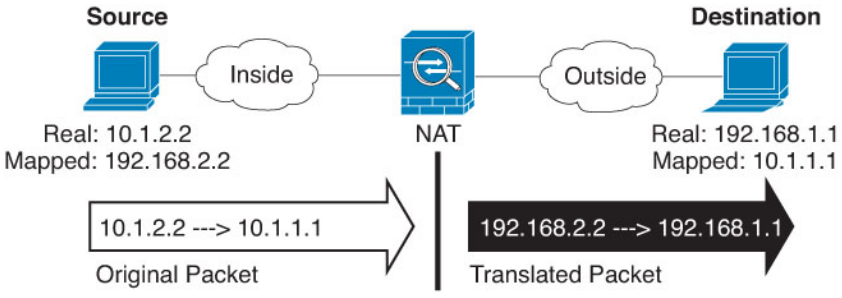
- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**手动 NAT**。
- **规则位置** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。
- **类型** - 选择**静态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。

步骤 4 配置以下接口选项：

- **源接口**、**目标接口** -（网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



- **原始源地址** - 包含将要转换的地址的网络对象或组。
- **原始目标地址** -（可选。）包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

可以依次选择**接口**以使原始目标基于源接口（不能为“任意”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源地址** - 以下项之一：
  - 要使用一组地址，请选择包含映射地址的网络对象或组。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
  - （具有端口转换的静态接口 NAT。）要使用目标接口的 IPv4 地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。
- **转换后的目标地址** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 （可选。）为服务转换确定源或目的服务端口。

如果要配置支持端口转换的静态 NAT，可以为源和/或目的转换端口。例如，可以在 TCP/80 和 TCP/8080 之间进行转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

- **原始源端口**、**转换后的源端口** - 定义源地址的端口转换。
- **原始目标端口**、**转换后的目标端口** - 定义目标地址的端口转换。

步骤 8 （可选。）点击**高级选项**链接并选择所需的选项：

- **转换与此规则相匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的 DNS 回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 596 页。如果您在进行端口转换，则此选项不可用。
- **不在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。

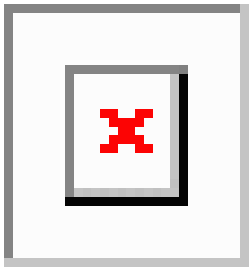
步骤 9 点击**确定 (OK)**。

身份 NAT

可能有一个 NAT 配置，在其中需要将 IP 地址转换为其本身。例如，如果创建一条将 NAT 应用于每个网络的大体的规则，但想使一个网络免于 NAT，则可以创建一条静态 NAT 规则，以将地址转换为其本身。

下图显示典型的身份 NAT 场景。

图 *46: 身份 NAT*



以下主题介绍如何配置身份 NAT。

配置身份自动 NAT

使用静态身份自动 NAT 规则可防止地址转换。即，防止将地址转换为自身。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义NAT规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的地址** - 其内容与原始源对象完全相同的网络对象或组。您可以使用相同的对象。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**自动 NAT**。
- **类型** - 选择**静态**。

步骤 4 配置以下数据包转换选项：

- **源接口、目标接口** -（网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。
- **原始地址** - 包含您要转换的地址的网络对象。
- **转换后的地址** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

不要为身份 NAT 配置**原始端口**和**转换后的端口**选项。

步骤 5 （可选。）点击**高级选项**链接并选择所需的选项：

- **转换与此规则匹配的 DNS 回复** - 请勿为身份 NAT 配置此选项。
- **不在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。
- **对目标接口执行路由查找** - 如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在NAT规则中配置的目标接口来确定目标接口。

步骤 6 点击**确定 (OK)**。

配置身份手动 NAT

当自动 NAT 不能满足您的需求时，请使用静态身份手动 NAT 规则。例如，如果您要根据目标进行不同的转换。使用静态身份 NAT 规则可防止地址转换。即，防止将地址转换为自身。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源地址** - 地址可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何**。
- **转换后的源地址** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

如果您要在规则中为**原始目标地址**和**转换后的目标地址**配置静态转换，还可以为这些地址创建网络对象。如果只需要配置支持端口转换的目标静态接口 NAT，则可以跳过为目标映射地址添加对象的过程，并在规则中指定接口。

您还可以对源和/或目标执行端口转换。在对象管理器中，确保有可以用于原始端口和转换后的端口的端口对象。您可以为身份 NAT 使用相同的对象。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

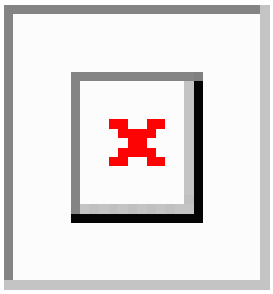
- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**手动 NAT**。
- **规则位置** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。
- **类型** - 选择**静态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。

步骤 4 配置以下接口选项：

- **源接口**、**目标接口** -（网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例，其中在内部主机上执行身份 NAT，但转换外部主机。



- **原始源地址** - 包含将要转换的地址的网络对象或组。
- **原始目标地址** -（可选。）包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

  您可以选择**接口**以使原始目标基于源接口（不能为“任何”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源地址** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。
- **转换后的目标地址** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标地址**选择了一个对象，则可以通过选择相同的对象设置身份 NAT（即无转换）。

步骤 7 （可选。）为服务转换确定源或目的服务端口。

如果要配置支持端口转换的静态 NAT，可以为源和/或目的转换端口。例如，可以在 TCP/80 和 TCP/8080 之间进行转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

- **原始源端口**、**转换后的源端口** - 定义源地址的端口转换。
- **原始目标端口**、**转换后的目标端口** - 定义目标地址的端口转换。

步骤 8 （可选。）点击**高级选项**链接并选择所需的选项：

- **转换与此规则匹配的 DNS 回复** - 请勿为身份 NAT 配置此选项。
- **不在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。
- **对目标接口执行路由查找** - 如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在 NAT 规则中配置的目标接口来确定目标接口。

步骤 9 点击**确定 (OK)**。

威胁防御 的 NAT 规则属性

使用网络地址转换 (NAT) 规则将 IP 地址转换为其他 IP 地址。通常使用 NAT 规则将私有地址转换为可公开路由的地址。该转换可以是从一个地址到另一个地址，或者您可以使用端口地址转换 (PAT) 将许多地址转换为一个地址，并且使用端口号区分源地址。

NAT 规则包括以下基本属性。自动 NAT 和手动 NAT 规则的属性相同，除非另行指明。

标题

为规则输入名称。名称不能包含空格。

创建规则用于

转换规则是**自动 NAT** 还是**手动 NAT**。自动 NAT 比手动 NAT 简单，但是手动 NAT 允许根据目标地址为源地址创建单独的转换。

状态

您希望该规则有效还是被禁用。

位置（仅手动 NAT。）

要添加规则的位置。可以将其插入类别中（在自动NAT规则之前或之后），或者所选规则的上方或下方。

类型

转换规则是**动态**还是**静态**。在实施PAT时，动态转换会自动从地址池中选择映射的地址或地址/端口组合。如果要精确定义映射的地址/端口，请使用静态转换。

以下主题介绍了其余的 NAT 规则属性。

自动 NAT 的数据包转换属性

使用**数据包转换**选项定义源地址和映射的转换后地址。以下属性仅适用于自动 NAT。

源接口、目标接口

（网桥组成员接口的必选项。）应用此NAT规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

原始地址（始终为必填项）。

包含您要转换的源地址的网络对象。该地址必须是网络对象（而非组），而且可以是主机、范围或子网。

转换后的地址（通常为必填项）。

您要转换到的映射地址。您在此处选择的选项取决于定义的转换规则类型。

- **动态 NAT** - 包含映射地址的网络对象或组。该地址可以是网络对象或组，但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。 如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。
- **动态 PAT** - 以下项之一：
  - （接口 PAT。）要使用目标接口的 IPv4 地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。您不能将接口 PAT 用于 IPv6。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。
- **静态 NAT** - 以下项之一：
  - 要使用一组地址，请选择包含映射地址的网络对象或组。该对象或组可以包含主机、范围或子网。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
  - （具有端口转换的静态接口 NAT。）要使用目标接口的地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。该选项配置具有端口转换的静

态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。

- **身份 NAT** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

原始端口、转换后的端口（仅静态 NAT）。

如果需要转换 TCP 或 UDP 端口，请选择定义原始端口和转换后的端口的端口对象。对象必须用于相同的协议。例如，如有必要，可以将 TCP/80 转换为 TCP/8080。

手动 NAT 的数据包转换属性

使用**数据包转换**选项定义源地址和映射的转换后地址。以下属性仅适用于手动 NAT。所有选项均为可选，除非另行指明。

源接口、目标接口

（网桥组成员接口的必选项。）应用此NAT规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

原始源地址（始终为必填项）。

包含您要转换的地址的网络对象或组。该地址可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以在规则中指定**任何**。

转换后的源地址（通常为必填项。）

您要转换到的映射地址。您在此处选择的选项取决于定义的转换规则类型。

- **动态 NAT** - 包含映射地址的网络对象或组。该地址可以是网络对象或组，但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。 如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。
- **动态 PAT** - 以下项之一：
  - （接口PAT。）要使用目标接口的地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。您不能将接口 PAT 用于 IPv6。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。
- **静态 NAT** - 以下项之一：
  - 要使用一组地址，请选择包含映射地址的网络对象或组。该对象或组可以包含主机、范围或子网。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
  - （具有端口转换的静态接口 NAT。）要使用目标接口的地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。

- **身份 NAT** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

原始目标地址

包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

您可以选择**接口**以使原始目标基于源接口（不能为“任何”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

转换后的目标地址

包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

您可以使用指定完全限定域名作为转换目的的网络对象；有关更多信息，请参阅FQDN 目的准则，第 535 页。

原始源端口、转换后的源端口、原始目标端口、转换后的目标端口

为原始和转换后的数据包定义源和目标服务的端口对象。您可以转换端口，或者选择同一对象以便在没有转换端口的情况下使规则敏感察觉到该服务。在配置服务时请记住以下规则：

- （动态 NAT 或 PAT。）不能对**原始源端口**和**转换后的源端口**进行转换。您可以仅对目标端口进行转换。
- NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，您可以将同一对象用于实际端口和映射端口。

高级 NAT 属性

在配置NAT时，可以在**高级**选项中配置提供专业化服务的属性。所有这些属性都是可选的：仅当需要服务时才对其进行配置。

转换与此规则匹配的 DNS 回复

是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 596 页。 如果在静态 NAT 规则中进行端口转换，则此选项不可用。

贯穿到接口 PAT（目标接口）（仅动态 NAT。）

当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。如果已配置了接口 PAT 配置作为转换的地址，则不能选择此选项。您不能将此选项用于 IPv6 网络。

不在目标接口上使用代理 ARP（仅静态 NAT。）

为映射IP地址的传入数据包禁用代理ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理ARP，

在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。

对目标接口执行路由查找（仅静态身份 NAT。仅路由模式。）

如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在 NAT 规则中配置的目标接口来确定目标接口。

转换 IPv6 网络

当需要在仅 IPv6 网络和仅 IPv4 网络之间传递流量时，需要使用 NAT 在地址类型之间进行转换。即使两个都是 IPv6 网络，您也可能需要对外部网络隐藏内部地址。

对于 IPv6 网络，您可以使用以下转换类型：

- NAT64、NAT46 - 将 IPv6 数据包转换成 IPv4 数据包，反之亦然。您需要定义两个策略，一个用于 IPv6 向 IPv4 的转换，另一个用于 IPv4 向 IPv6 的转换。虽然您可以使用单一 手动 NAT 规则完成此任务，但如果 DNS 服务器位于外部网络，则可能需要重写 DNS 响应。由于在指定了目标的情况下，无法在手动 NAT 规则中启用 DNS 重写，所以最好创建两个自动 NAT 规则。

注释 NAT46 仅支持静态映射。

- NAT66 - 将 IPv6 数据包转换为不同的 IPv6 地址。我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。

注释 NAT64 和 NAT 46 仅可以在标准路由接口上使用。NAT66 可在路由接口和网桥组成员接口上使用。

NAT64/46：将 IPv6 地址转换为 IPv4 地址

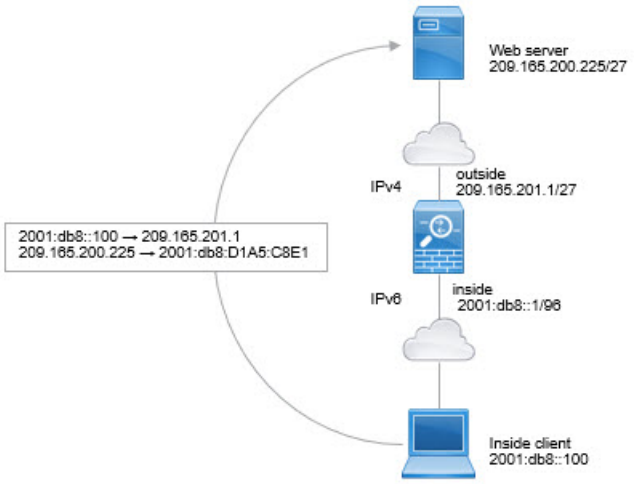
当流量从 IPv6 网络进入仅 IPv4 网络时，您需要将 IPv6 地址转换为 IPv4 地址，并将流量从 Ipv4 返回 IPv6。您需要定义两个地址池，一个 IPv4 地址池用于绑定 IPv4 网络中的 IPv6 地址，另一个 IPv6 地址池用于绑定 IPv6 网络中的 IPv4 地址。

- NAT64 规则的 IPv4 地址池一般较小，通常可能没有足够的地址与 IPv6 客户端地址一对一映射。与动态或静态 NAT 相比，动态 PAT 可以更容易满足可能的大量 IPv6 客户端地址需要。
- NAT46 规则的 IPv6 地址池可以等于或大于要映射的 IPv4 地址数。这允许每个 IPv4 地址映射到不同的 IPv6 地址。NAT46 仅支持静态映射，因此您不能使用动态 PAT。

您需要定义两个策略，一个用于源 IPv6 网络，一个用于目标 IPv4 网络。虽然您可以使用单一 手动 NAT 规则完成此任务，但如果 DNS 服务器位于外部网络，则可能需要重写 DNS 响应。由于在指定了目标的情况下，无法在手动 NAT 规则中启用 DNS 重写，所以最好创建两个自动 NAT 规则。

NAT64/46 示例：内部 IPv6 网络与外部 IPv4 互联网

以下是一个非常简单的示例，假设您具有仅包含 IPv6 的内部网络，且您希望将发送到互联网的流量转换为 IPv4。此示例假定您无需 DNS 转换，以便可以在单个手动 NAT 规则中执行 NAT64 和 NAT46 转换。



在本例中，借助外部接口的 IP 地址，使用动态接口 PAT 将内部 IPv6 网络转换为 IPv4。将外部 IPv4 流量静态转换为 2001:db8::/96 网络中的地址，允许在内部网络中传输。

过程

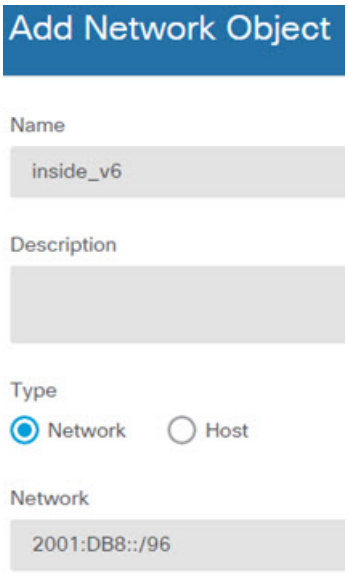
步骤 1 创建用于内部 IPv6 网络的网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义内部 IPv6 网络。

为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:db8::/96。



d) 点击**确定**。

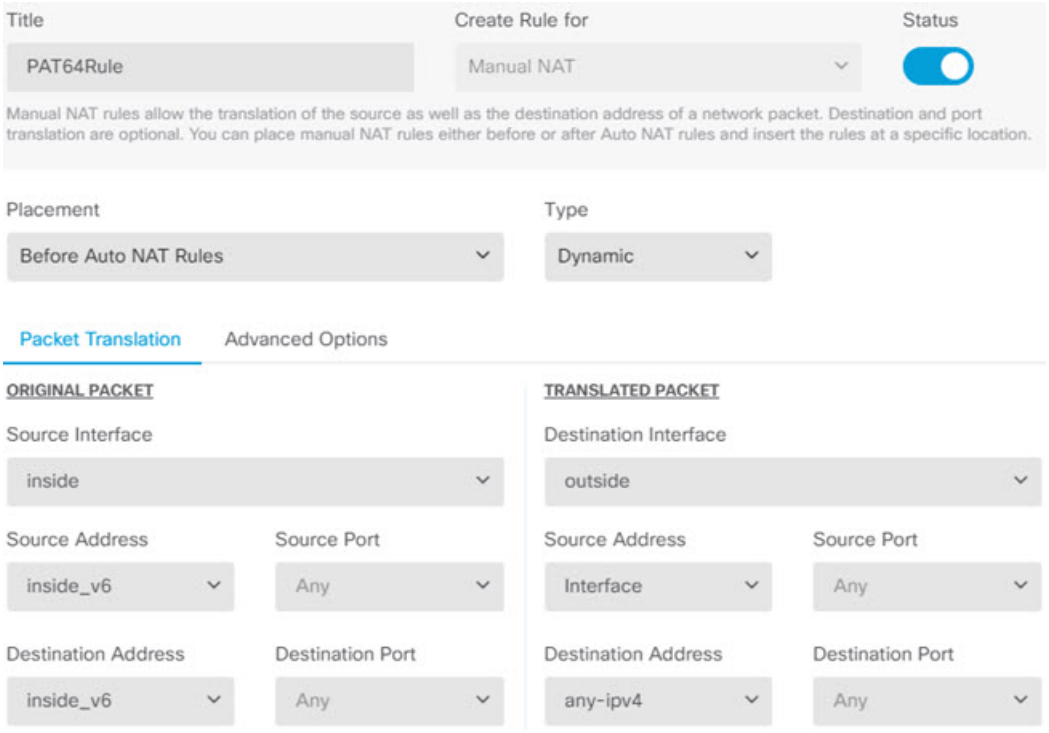
步骤 2 创建手动 NAT 规则以将 IPv6 网络转换为 IPv4 并再次返回。

a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = PAT64Rule（或您选择的其他名称）。
- **创建规则用于** = **手动 NAT**。
- **位置** = **自动 NAT 规则之前**
- **类型** = **动态**。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始数据包源地址** = inside_v6 网络对象。
- **转换后数据包源地址** = 接口。此选项使用目标接口的 IPv4 地址作为 PAT 地址。
- **原始数据包目标地址** = inside_v6 网络对象。
- **转换后数据包目标地址** = any-ipv4 网络对象。

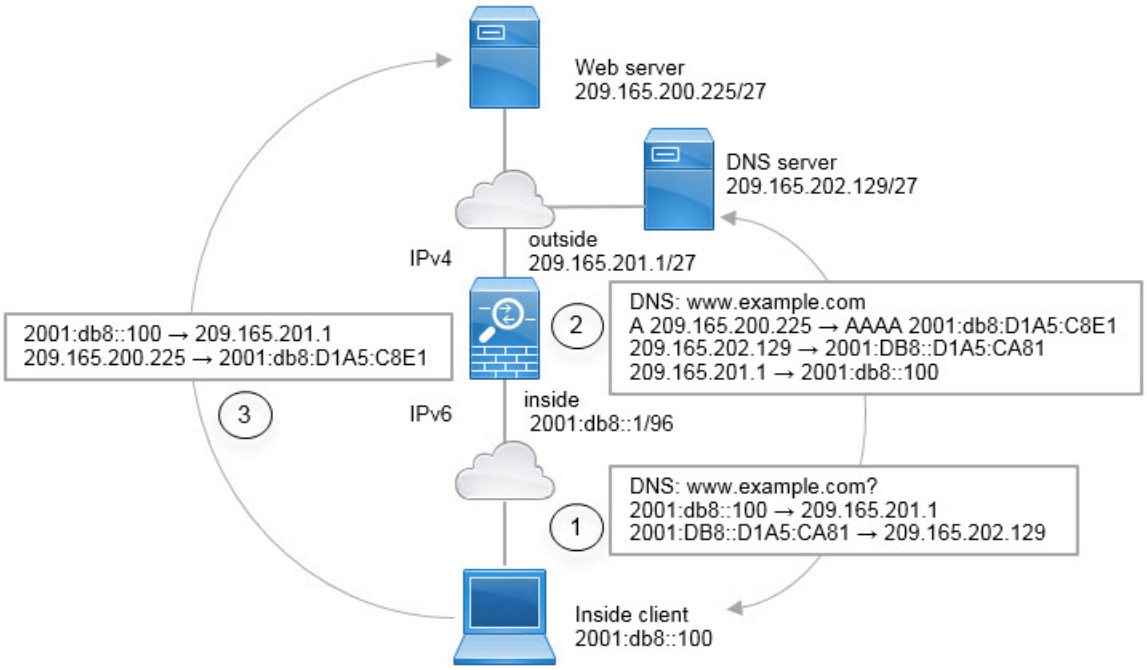


d) 点击**确定**。

使用此规则时，从内部接口上的 2001:db8::/96 子网流向外部接口的任何流量都将接受使用外部接口 IPv4 地址进行的 NAT64 PAT 转换。相反，外部网络中的任何 IPv4 地址到达内部接口，都将使用嵌入式 IPv4 地址方法转换为 2001:db8::/96 网络中的一个地址。

NAT64/46 示例：包含外部 IPv4 互联网和 DNS 转换的内部 IPv6 网络

下面是一个典型的示例：内部网络只支持 IPv6，但外部互联网上有一些内部用户所需的服务只支持 IPv4。



在本例中，借助外部接口的 IP 地址，使用动态接口 PAT 将内部 IPv6 网络转换为 IPv4。将外部 IPv4 流量静态转换为 2001:db8::/96 网络中的地址，允许在内部网络中传输。对 NAT46 规则启用 DNS 重写，使外部 DNS 服务器的回复可以从 A (IPv4) 记录转换为 AAAA (IPv6) 记录，地址也能从 IPv4 地址转换为 IPv6 地址。

当内部 IPv6 网络中地址为 2001:DB8::100 的客户端尝试打开 www.example.com 时，此 Web 请求的典型顺序如下。

1. 客户端的计算机向地址为 2001:DB8::D1A5:CA81 的 DNS 服务器发送 DNS 请求。NAT 规则对 DNS 请求中的源和目的进行以下转换：
   - 2001:DB8::100 转换为 209.165.201.1 上的唯一端口（NAT64 接口 PAT 规则。）
   - 2001:DB8::D1A5:CA81 转换为 209.165.202.129（NAT46 规则。）D1A5:CA81 是 209.165.202.129 的 IPv6 对应物。）
2. DNS 服务器以 A 记录进行响应，指出 www.example.com 位于 209.165.200.225。NAT46 规则（已启用 DNS 重写）将 A 记录转换为 IPv6 对应物 AAAA 记录，并在 AAAA 记录中将 209.165.200.225 转换为 2001:db8:D1A5:C8E1。此外，DNS 响应中的源地址和目标地址未转换：
   - 209.165.202.129 转换为 2001:DB8::D1A5:CA81
   - 209.165.201.1 转换为 2001:db8::100
3. IPv6 客户端现在有 Web 服务器的 IP 地址，于是向位于 2001:db8:D1A5:C8E1 的 www.example.com 发出 HTTP 请求。（D1A5:C8E1 是 209.165.200.225 的 IPv6 对应物。）HTTP 请求中的源和目的进行转换：
   - 2001:DB8::100 转换为 209.156.101.54 上的唯一端口（NAT64 接口 PAT 规则。）

- 2001:db8:D1A5:C8E1 转换为 209.165.200.225（NAT46 规则。）

以下步骤程序介绍了如何配置此示例。

过程

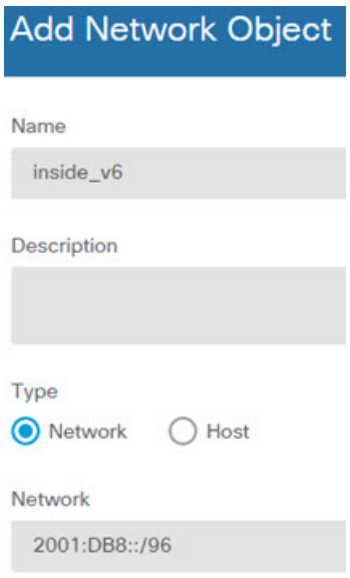
步骤 1 创建定义内部 IPv6 网络和外部 IPv4 网络的网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义内部 IPv6 网络。

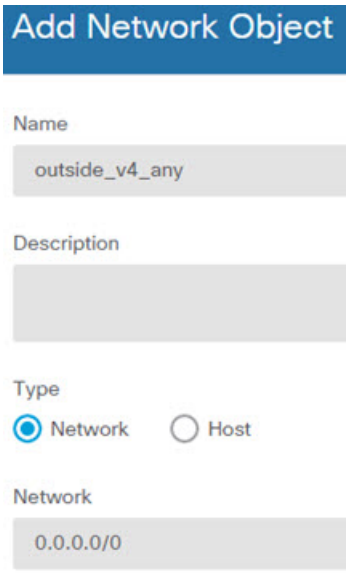
为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:db8::/96。



d) 点击**确定**。

e) 点击 + 并定义外部 IPv4 网络。

为网络对象命名（例如，outside_v4_any），选择**网络**，然后输入网络地址 0.0.0.0/0。



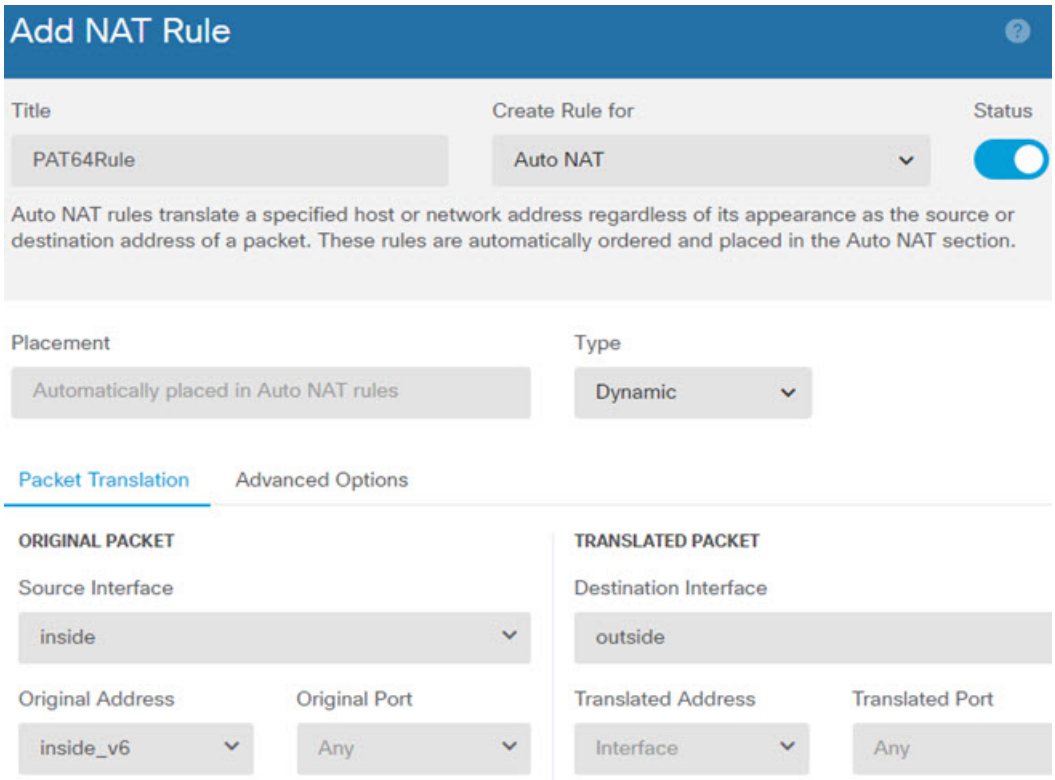
步骤 2 为内部 IPv6 网络配置 NAT64 动态 PAT 规则。

a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = PAT64Rule（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = inside_v6 网络对象。
- **转换后的地址** = **接口**。此选项使用目标接口的 IPv4 地址作为 PAT 地址。



d) 点击**确定**。

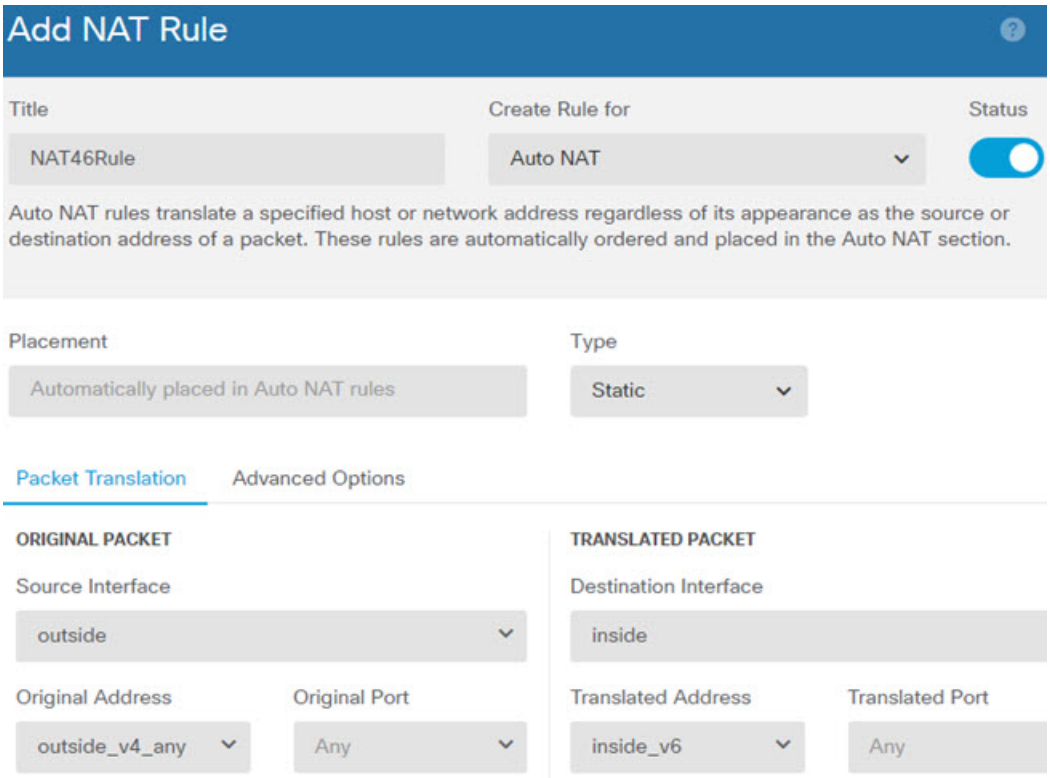
使用此规则时，从内部接口上的 2001:db8::/96 子网流向外部接口的任何流量都将接受使用外部接口 IPv4 地址进行的 NAT64 PAT 转换。

步骤 3 为外部 IPv4 网络配置静态 NAT46 规则。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = NAT46Rule（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 外部。
- **目标接口** = 内部。
- **原始地址** = outside_v4_any 网络对象。
- **转换后的地址** = inside_v6 网络对象。
- 在**高级选项**选项卡中，选择**转换与此规则匹配的 DNS 回复**。



c) 点击**确定**。

使用此规则时，外部网络中的任何 IPv4 地址到达内部接口，都将使用嵌入式 IPv4 地址方法转换为 2001:db8::/96 网络中的一个地址。此外，DNS 响应从 A (IPv4) 记录转换为 AAAA (IPv6) 记录，其地址也从 IPv4 地址转换为 IPv6 地址。

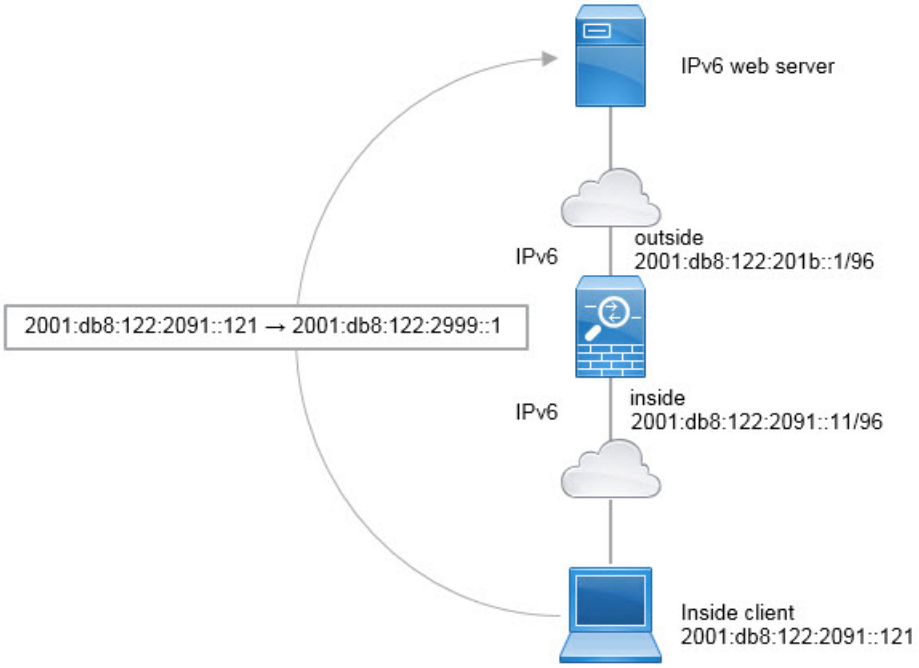
NAT66：将 IPv6 地址转换为不同的 IPv6 地址

当从一个 IPv6 网络进入另一个 IPv6 网络时，您可以将地址转换为外部网络上的不同 IPv6 地址。我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。

因为您不是在不同的地址类型之间转换，所以您需要一个单一的 NAT66 转换规则。使用自动 NAT 可轻松地为这些规则建模。但是，如果不想允许返回流量，您可以仅使用手动 NAT 将静态 NAT 规则设为单向。

NAT66 示例：网络间的静态转换

您可以使用自动 NAT 在 IPv6 地址池之间配置静态转换。以下示例说明如何将 2001:db8:122:2091::/96 网络中的内部地址转换为 2001:db8:122:2999::/96 网络中的外部地址。



注释 此示例假定，内部接口不是网桥组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

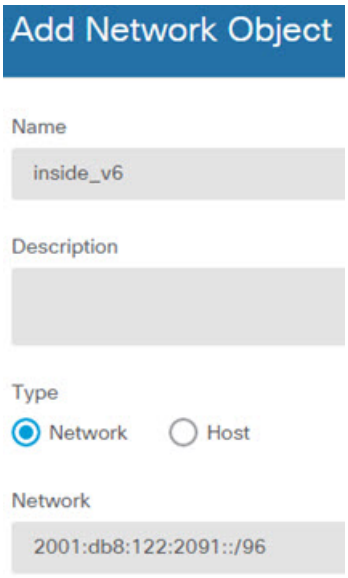
步骤 1 创建定义内部 IPv6 网络和外部 IPv6 NAT 网络的网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义内部 IPv6 网络。

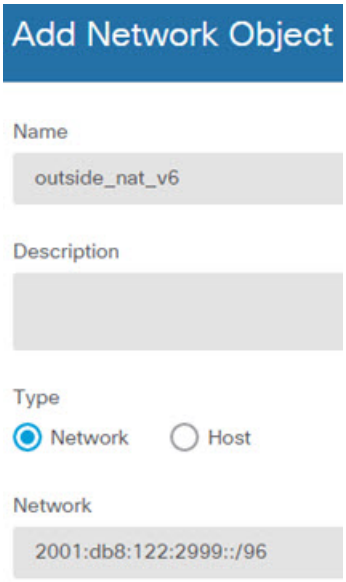
为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:db8:122:2091::/96。



d) 点击**确定**。

e) 点击 + 并定义外部 IPv6 NAT 网络。

为网络对象命名（例如，outside_nat_v6），选择**网络**，然后输入网络地址 2001:db8:122:2999::/96。



步骤 2 为内部 IPv6 网络配置静态 NAT 规则。

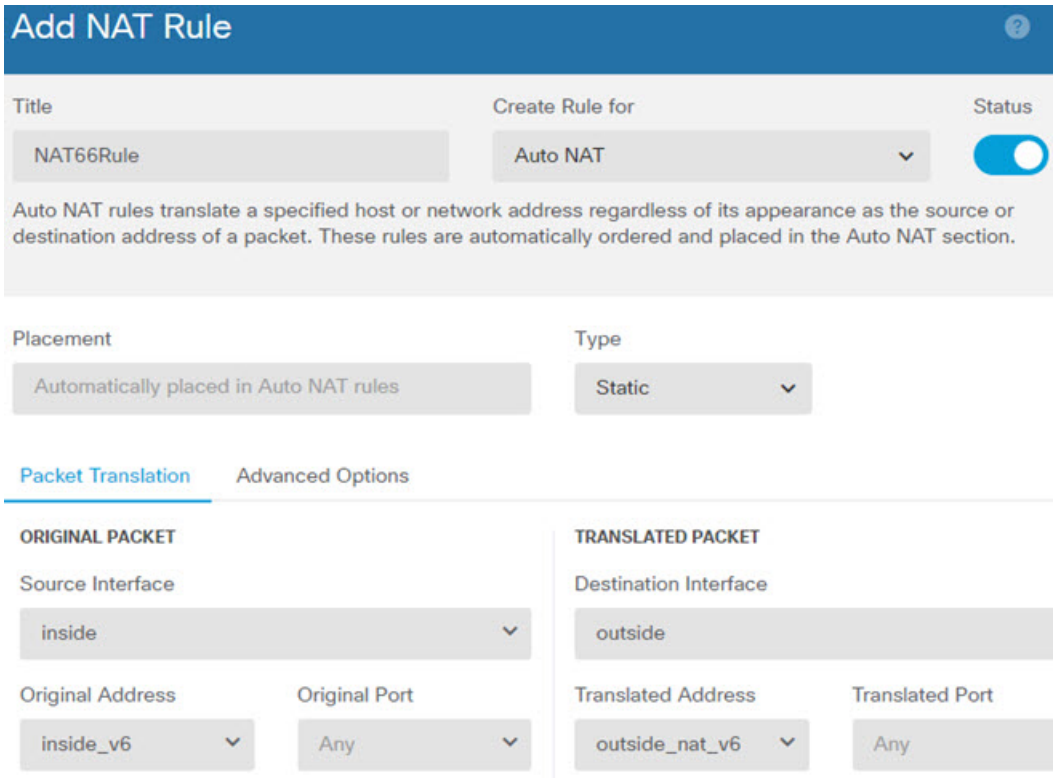
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = NAT66Rule（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。

- **类型** = 静态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = inside_v6 网络对象。
- **转换后的地址** = outside_nat_v6 网络对象。



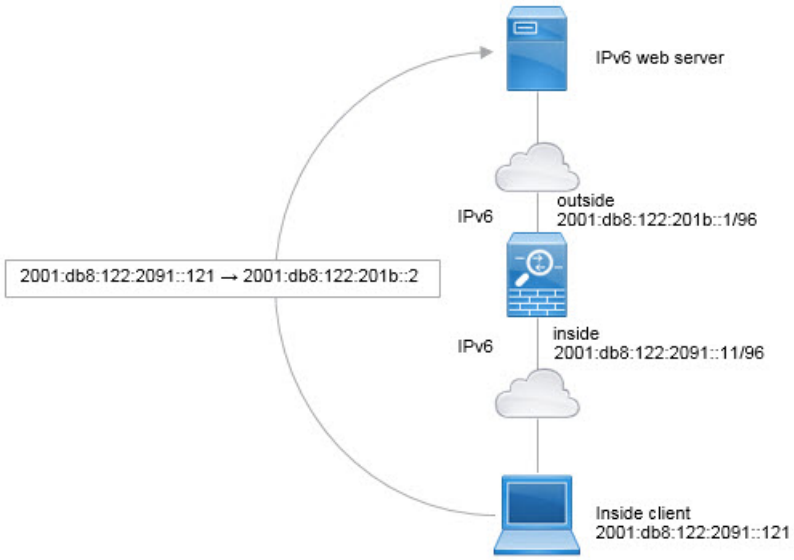
d) 点击**确定**。

使用此规则，从内部接口上的 2001:db8:122:2091::/96 子网到外部接口的任何流量都会经静态 NAT66 转换为 2001:db8:122:2999::/96 网络上的地址。

NAT66 示例：简单 IPv6 接口 PAT

实施 NAT66 的一个简单方法是将内部地址动态分配给外部接口 IPv6 地址上的不同端口。

不过，无法通过 设备管理器使用接口的 IPv6 地址配置接口 PAT。相反，要使用同一网络中的一个空闲地址作为动态 PAT 池。



注释 此示例假定，内部接口不是网桥组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

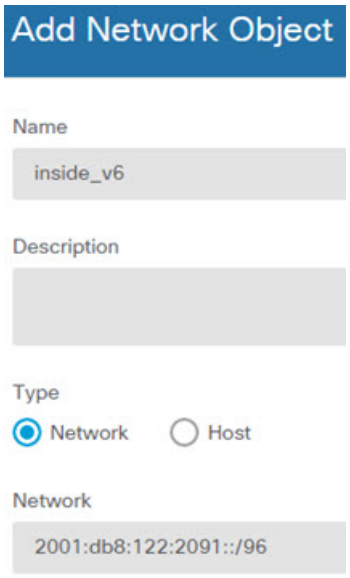
步骤 1 创建定义内部 IPv6 网络和 IPv6 PAT 地址的网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义内部 IPv6 网络。

为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:db8:122:2091::/96。



d) 点击**确定**。

e) 点击 + 并定义外部 IPv6 PAT 地址。

为网络对象命名（例如，ipv6_pat），选择**主机**，然后输入主机地址 2001:db8:122:201b::2。

步骤 2 为内部 IPv6 网络配置动态 PAT 规则。

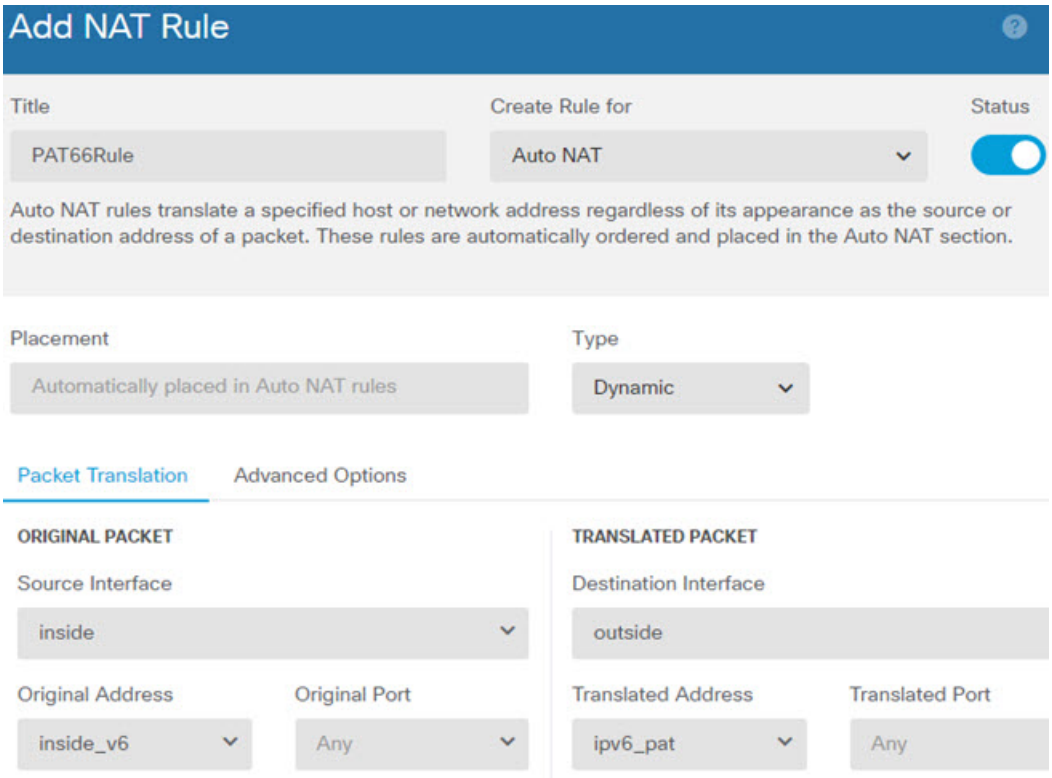
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = PAT66Rule（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。

- **类型** = 动态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = inside_v6 网络对象。
- **转换后的地址** = ipv6_pat 网络对象。



d) 点击**确定**。

使用此规则，从内部接口上的 2001:db8:122:2091::/96 子网到外部接口的任何流量都会经动态 PAT66 转换为 2001:db8:122:201b::2 上的端口。

监控 NAT

要对 NAT 连接进行监控和故障排除，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。

- **show nat** 显示 NAT 规则和每个规则的命中计数。还有其他关键字可用于显示 NAT 的其他方面信息。
- **show xlate** 显示当前处于活动状态的实际 NAT 转换。

- **clear xlate** 允许删除处于活动状态的 NAT 转换。如果更改 NAT 规则，您可能需要删除活动的转换，因为现有连接继续使用旧的转换槽，直到连接结束。清除转换允许系统根据您的新规则，在客户端的下一次连接尝试中为客户端构建新的转换。（您无法在CLI控制台中使用此命令。）

NAT 示例

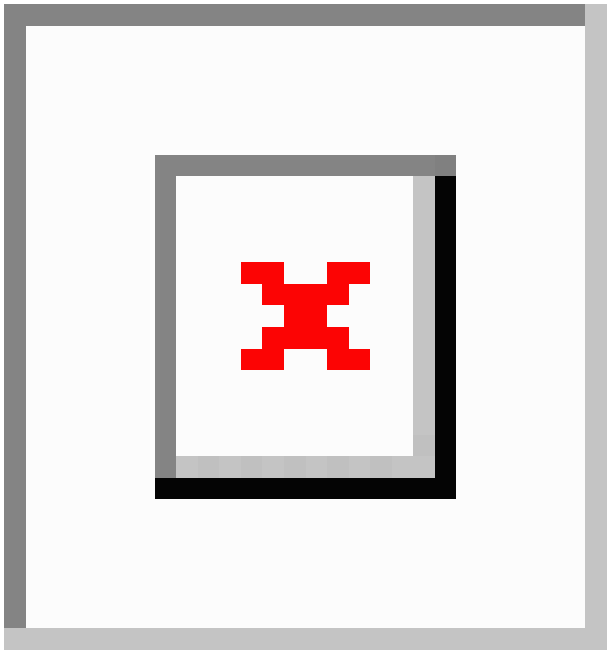
以下主题提供了在威胁防御设备上配置 NAT 的示例。

提供对内部 Web 服务器的访问权限（静态自动 NAT）

以下示例为内部 Web 服务器执行静态 NAT。实际地址位于专用网络上，因此公共地址是必需的。需要静态 NAT，以便主机能够在固定地址发起到 Web 服务器的流量。

注释 此示例假定，内部接口不是网桥组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，请选择 Web 服务器连接到的具体网桥组成员接口，例如 inside1_3。

图 *47:* 面向内部 *Web* 服务器的静态 *NAT*



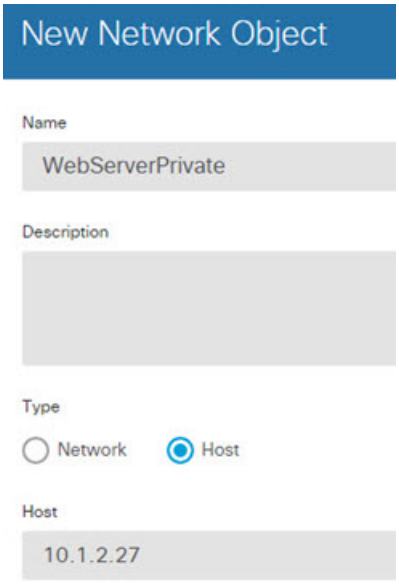
过程

步骤 1 创建定义服务器私有和公共主机地址的网络对象。

a) 选择**对象**。

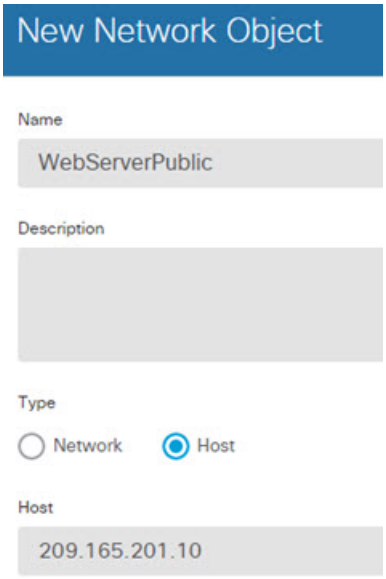
b) 从目录中选择**网络**，然后点击 +。
c) 定义 Web 服务器的私有地址。

为网络对象命名（例如，WebServerPrivate），选择**主机**，然后输入实际主机 IP 地址 10.1.2.27。



d) 点击**确定**。
e) 点击 + 并定义公共地址。

为网络对象命名（例如，WebServerPublic），选择**主机**，然后输入实际主机地址 209.165.201.10。

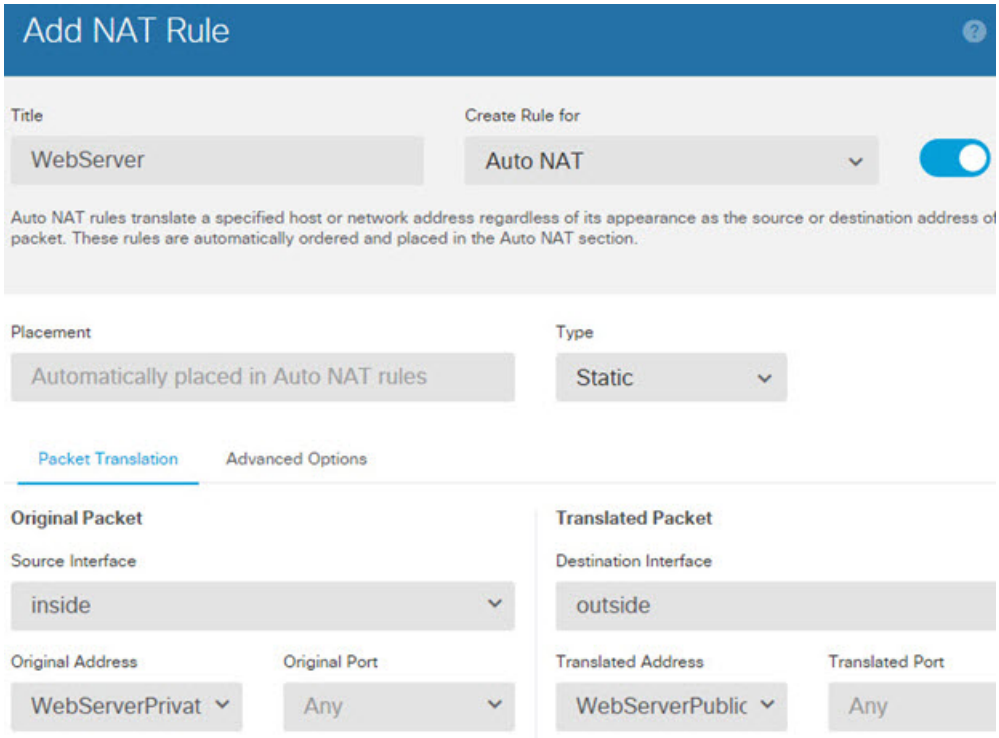


f) 点击**确定**。

步骤 2 配置对象的静态 NAT。

a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。
c) 配置以下属性：
- **标题** = WebServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = WebServerPrivate 网络对象。
- **转换后的地址** = WebServerPublic 网络对象。



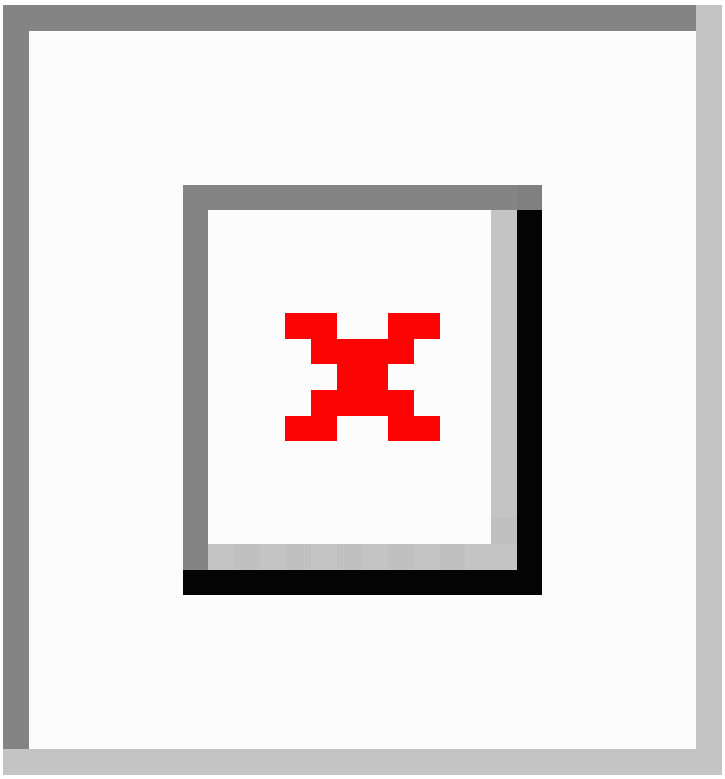
d) 点击**确定 (OK)**。

FTP、HTTP 和 SMTP 的单个地址（具有端口转换的静态自动 NAT）

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

注释 此示例假设内部接口是连接到交换机的标准路由接口，其中服务器连接到交换机。如果您的内部接口是网桥组接口 (BVI)，并且服务器连接到单独的网桥组成员接口，请选择对于相应规则，每个服务器连接的特定成员接口。例如，该规则可能以 inside1_2、inside1_3 和 inside1_4 而非 inside 作为源接口。

图 *48:* 支持端口转换的静态 *NAT*



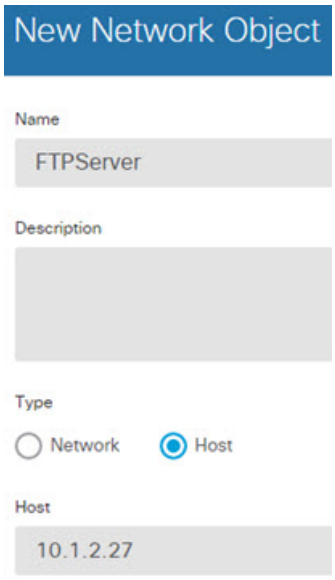
过程

步骤 1 为 FTP 服务器创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 为网络对象命名（例如，FTPserver），选择**主机**，然后输入 FTP 服务器的实际 IP 地址 10.1.2.27。

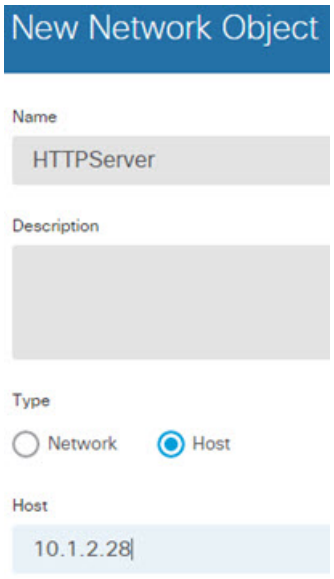


d) 点击**确定**。

步骤 2 为 HTTP 服务器创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，HTTPserver)，选择**主机**，然后输入实际主机地址 10.1.2.28。

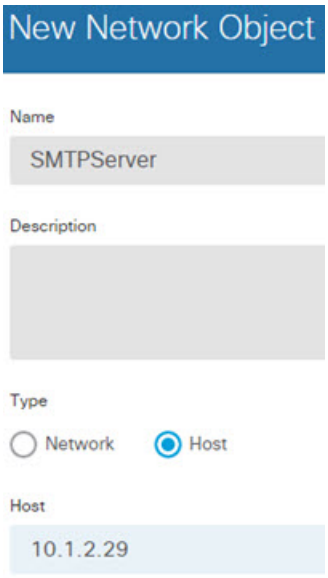


c) 点击**确定**。

步骤 3 为 SMTP 服务器创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，SMTPserver)，选择**主机**，然后输入实际主机地址 10.1.2.29。

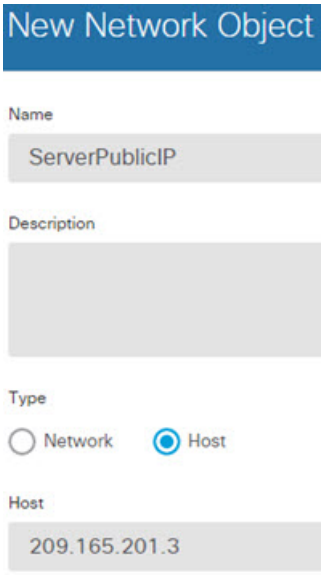


c) 点击**确定**。

步骤 4 为用于三台服务器的公共 IP 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，ServerPublicIP），选择**主机**，然后输入实际主机地址 209.165.201.3。



c) 点击**确定**。

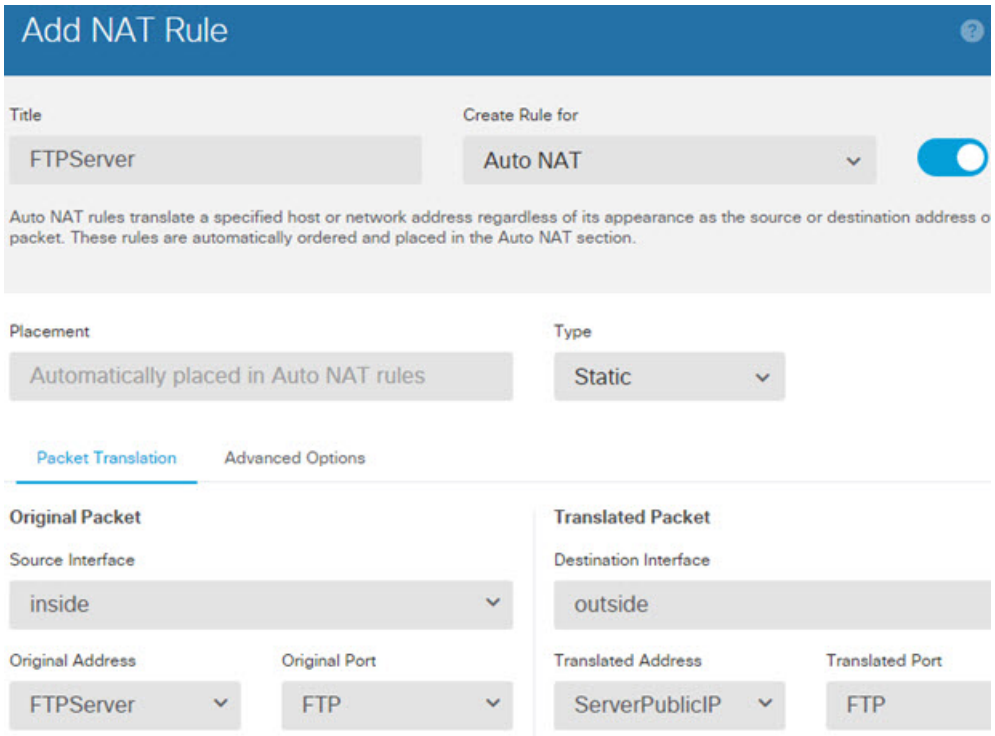
步骤 5 为 FTP 服务器配置具有端口转换的静态 NAT，并将 FTP 端口映射到其自身。

a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = FTPServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = FTPserver 网络对象。
- **转换后的地址** = ServerPublicIP 网络对象。
- **原始端口** = FTP 端口对象。
- **转换后的端口** = FTP 端口对象。



d) 点击**确定**。

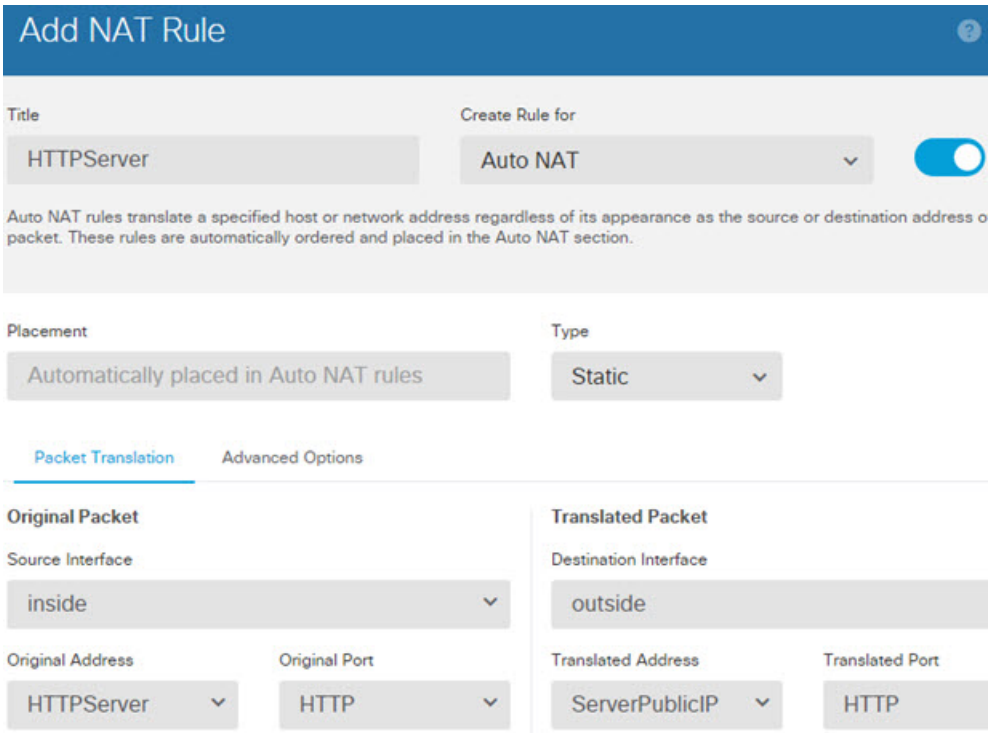
步骤 6 为 HTTP 服务器配置支持端口转换的静态 NAT，并将 HTTP 端口映射到其自身。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = HTTPServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 静态。

- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = HTTPserver 网络对象。
- **转换后的地址** = ServerPublicIP 网络对象。
- **原始端口** = HTTP 端口对象。
- **转换后的端口** = HTTP 端口对象。



c) 点击**确定**。

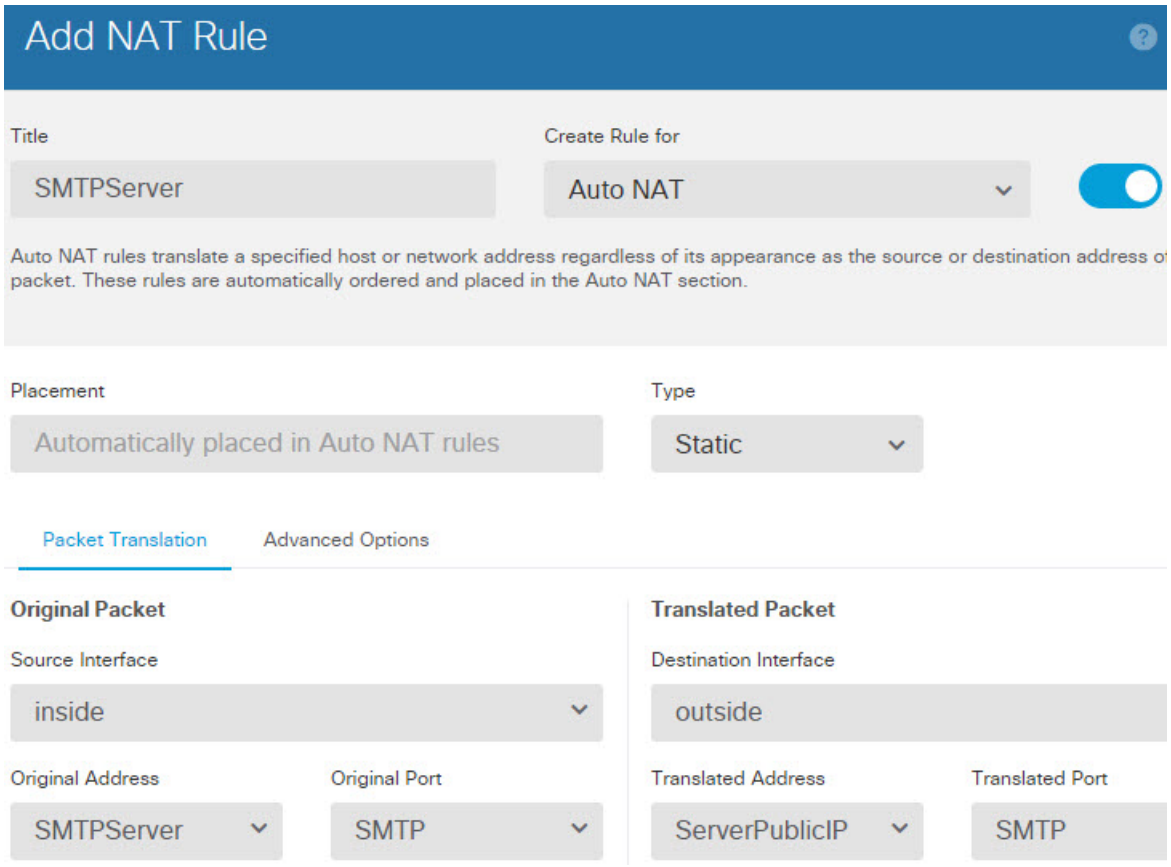
步骤 7 为 SMTP 服务器配置支持端口转换的静态 NAT，并将 SMTP 端口映射到其自身。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = SMTPServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = SMTPserver 网络对象。

- **转换后的地址** = ServerPublicIP 网络对象。
- **原始端口** = SMTP 端口对象。
- **转换后的端口** = SMTP 端口对象。



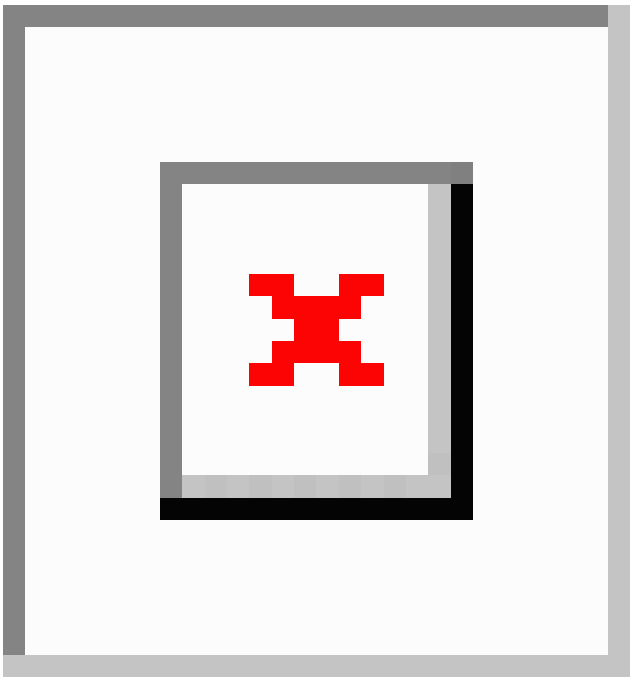
c) 点击**确定 (OK)**。

转换因目标而异（动态手动 PAT）

下图显示 10.1.2.0/24 网络上的一台主机正在访问两台不同的服务器。当主机访问位于 209.165.201.11 的服务器时，实际地址将转换为 209.165.202.129:*port*。当主机访问位于 209.165.200.225 的服务器时，实际地址将转换为 209.165.202.130:*port*。

注释 此示例假设内部接口是连接到交换机的标准路由接口，其中服务器连接到交换机。如果您的内部接口是网桥组接口 (BVI)，并且服务器连接到单独的网桥组成员接口，请选择对于相应规则，每个服务器连接的特定成员接口。例如，该规则可能以 inside1_2 和 inside1_3 而非 inside 作为源接口。

图 *49:* 具有不同目标地址的手动 *NAT*



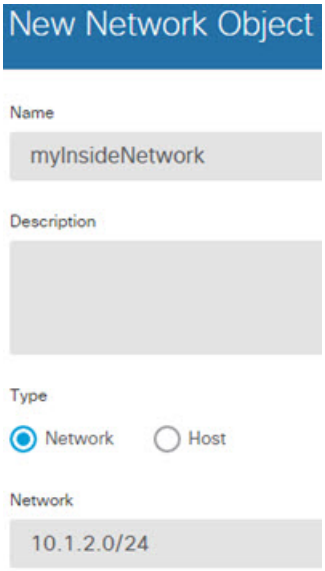
过程

步骤 1 为内部网络创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 为网络对象命名（例如，myInsideNetwork），选择**网络**，然后输入实际网络地址 10.1.2.0/24。

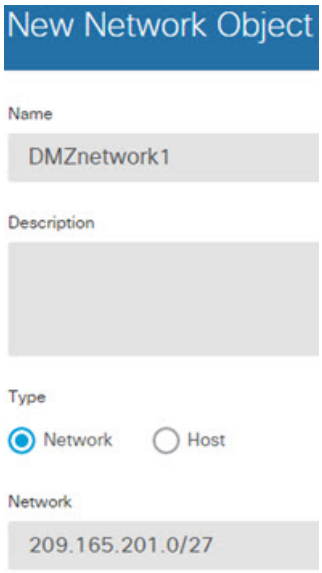


d) 点击**确定**。

步骤 2 为 DMZ 网络 1 创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，DMZnetwork1），选择**网络**，然后输入网络地址 209.165.201.0/27（子网掩码为 255.255.255.224）。

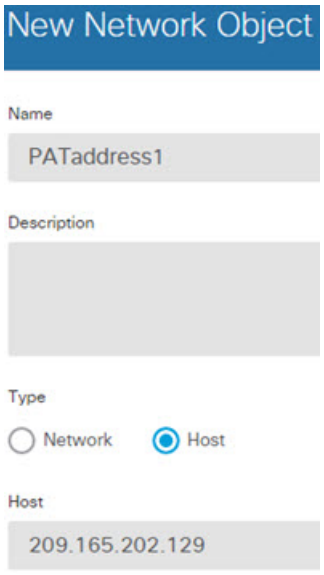


c) 点击**确定**。

步骤 3 为 DMZ 网络 1 的 PAT 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，PATaddress1），选择**主机**，然后输入主机地址 209.165.202.129。

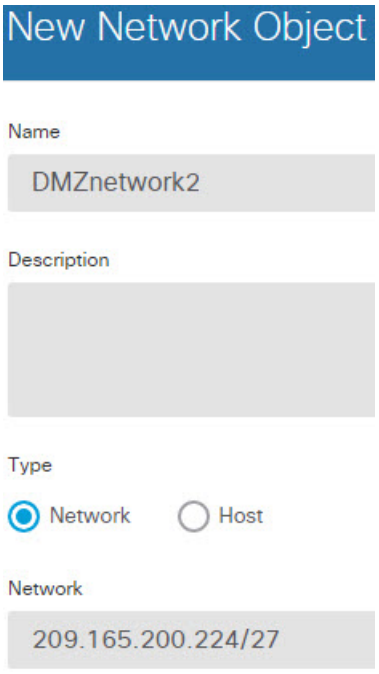


c) 点击**确定**。

步骤 4 为 DMZ 网络 2 创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，DMZnetwork2），选择**网络**，然后输入网络地址 209.165.200.224/27（子网掩码为 255.255.255.224）。

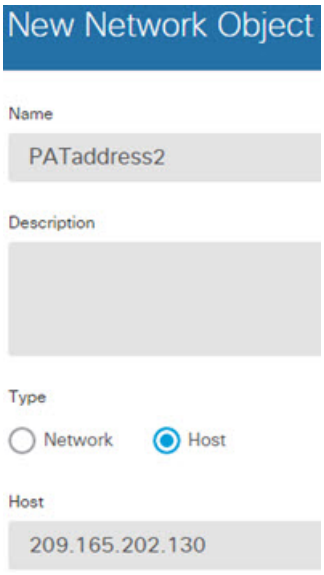


c) 点击**确定**。

步骤 5 为 DMZ 网络 2 的 PAT 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，PATaddress2），选择**主机**，然后输入主机地址 209.165.202.130。



c) 点击**确定**。

步骤 6 为 DMZ 网络 1 配置动态手动 PAT。

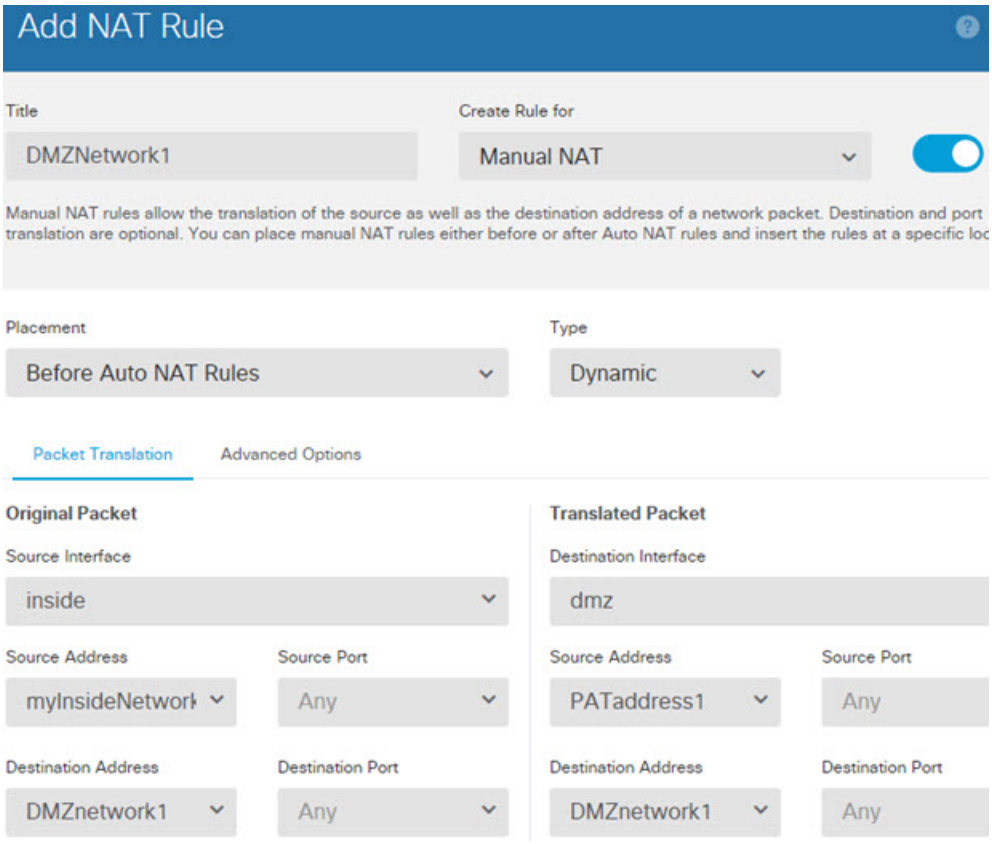
a) 依次选择**策略** > **NAT**。

b) 点击 **+** 按钮。

c) 配置以下属性：

- **标题** = DMZNetwork1（或您选择的其他名称）。
- **创建规则用于** = 手动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目标接口** = dmz。
- **原始源地址** = myInsideNetwork 网络对象。
- **转换后的源地址** = PATaddress1 网络对象。
- **原始目标地址** = DMZnetwork1 网络对象。
- **转换后的目标地址** = DMZnetwork1 网络对象。

  注释 由于您不需要转换目标地址，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。



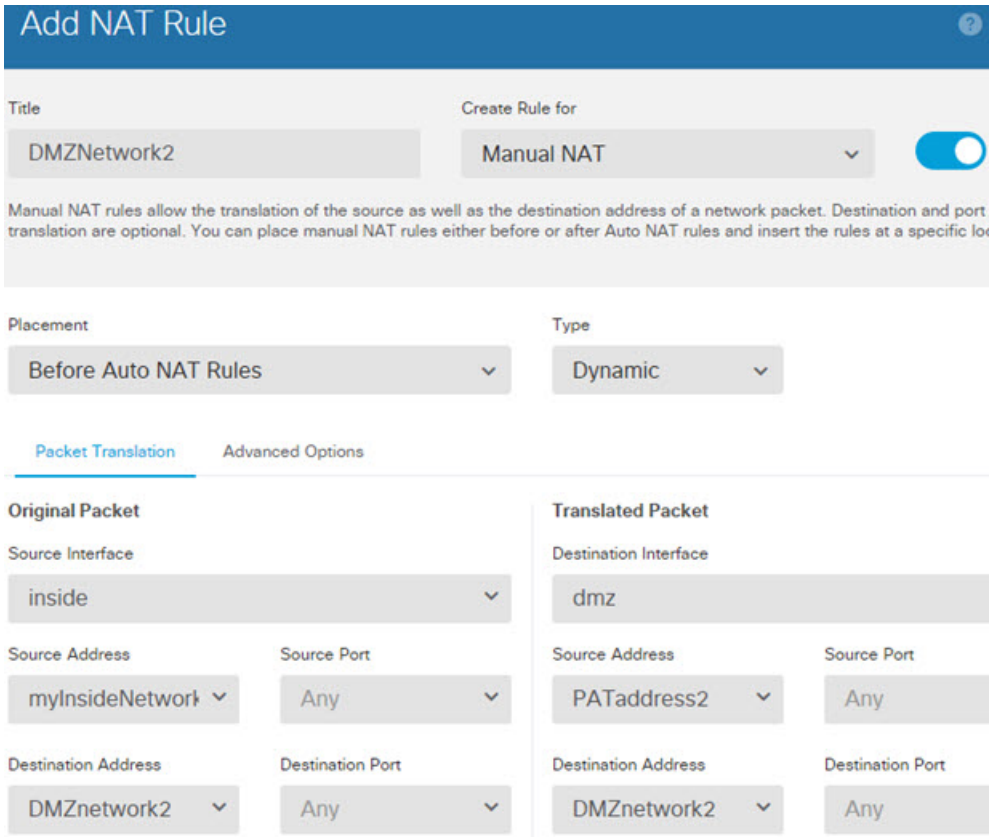
d) 点击**确定**。

步骤 7 为 DMZ 网络 2 配置动态手动 PAT。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = DMZNetwork2（或您选择的其他名称）。
- **创建规则用于** = 手动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目标接口** = dmz。
- **原始源地址** = myInsideNetwork 网络对象。
- **转换后的源地址** = PATaddress2 网络对象。
- **原始目标地址** = DMZnetwork2 网络对象。
- **转换后的目标地址** = DMZnetwork2 网络对象。



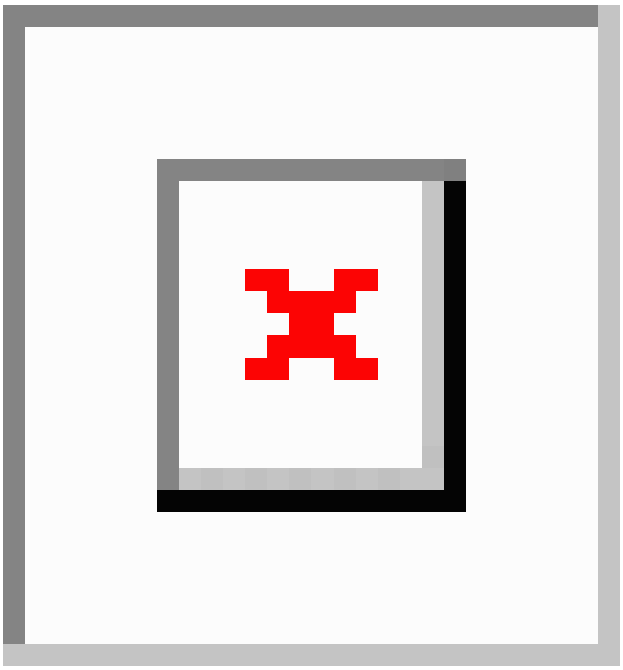
c) 点击**确定 (OK)**。

转换因目标地址和端口而异（动态手动 PAT）

下图显示源端口和目标端口的使用情况。10.1.2.0/24 网络上的主机同时因为网络服务和 Telnet 服务访问单个主机。当主机进行 Telnet 服务访问服务器时，实际地址将转换为 209.165.202.129:*port*。当主机进行网络服务访问相同服务器时，真实地址将转换为 209.165.202.130:*port*。

注释 此示例假设内部接口是连接到交换机的标准路由接口，其中服务器连接到交换机。如果内部接口是网桥组接口 (BVI) 而服务器连接到某个网桥组成员接口，请选择服务器连接到的具体成员接口。例如，该规则可能以 inside1_2 而非 inside 作为源接口。

图 *50:* 具有不同目标端口的手动 *NAT*



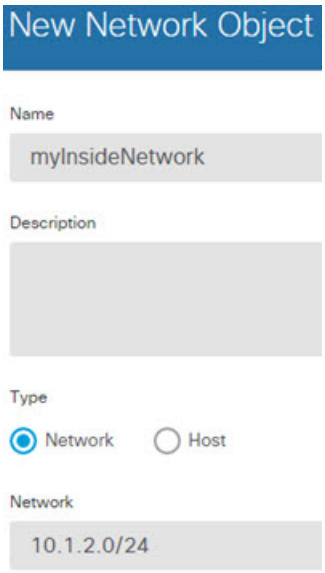
过程

步骤 1 为内部网络创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 为网络对象命名（例如，myInsideNetwork），选择**网络**，然后输入实际网络地址 10.1.2.0/24。

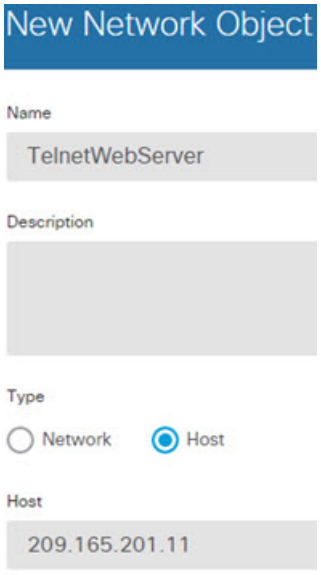


d) 点击**确定**。

步骤 2 为 Telnet/Web 服务器创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，TelnetWebServer），选择**主机**，然后输入实际主机地址 209.165.201.11。

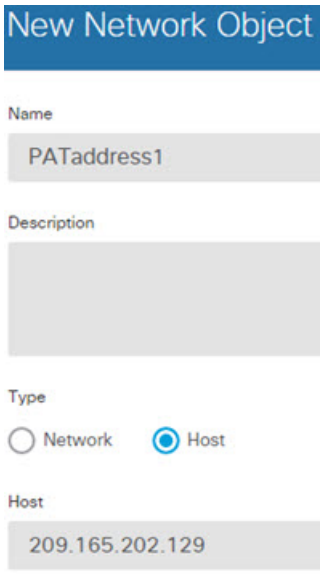


c) 点击**确定 (OK)**。

步骤 3 使用 Telnet 时为 PAT 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，PATaddress1），选择**主机**，然后输入主机地址 209.165.202.129。

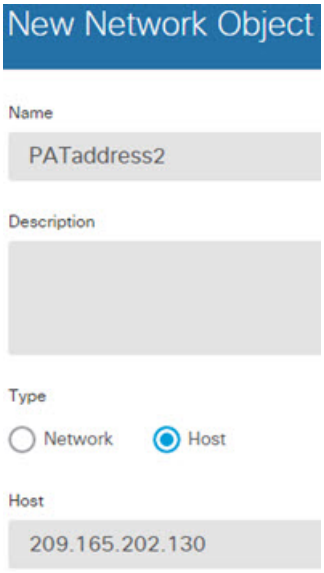


c) 点击**确定**。

步骤 4 使用 HTTP 时为 PAT 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，PATaddress2），选择**主机**，然后输入主机地址 209.165.202.130。



c) 点击**确定**。

步骤 5 为 Telnet 访问创建动态手动 PAT。

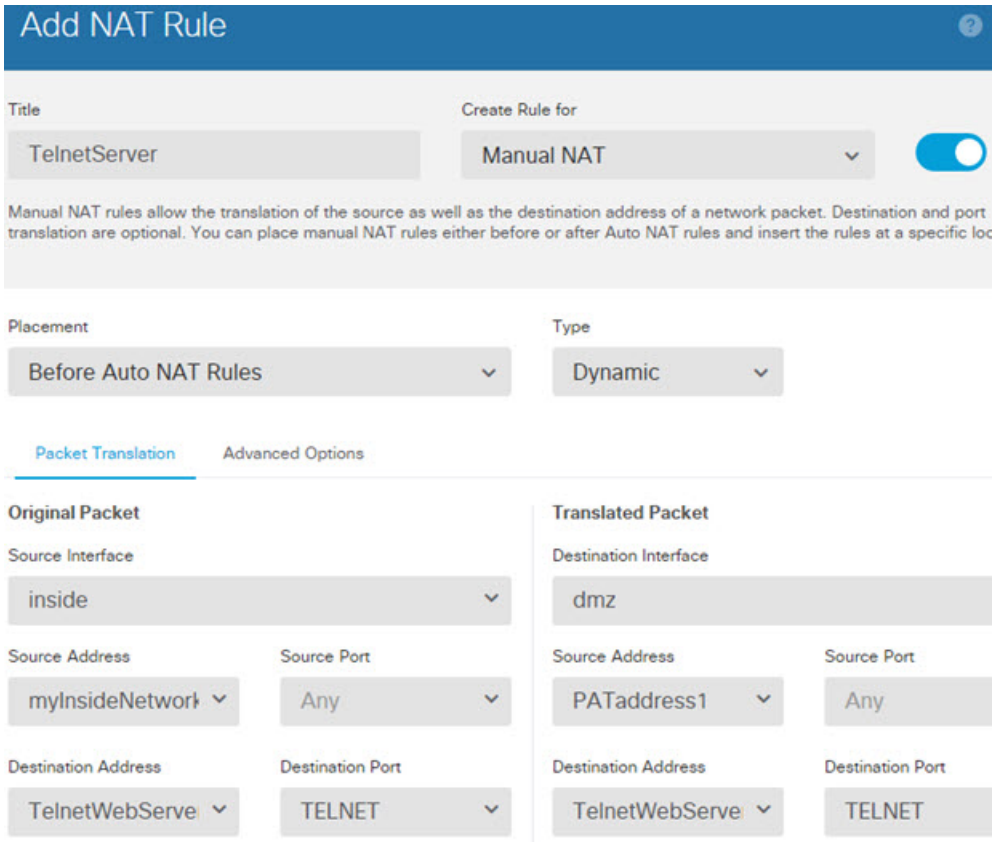
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = TelnetServer（或您选择的其他名称）。
- **创建规则用于** = 手动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目标接口** = dmz。
- **原始源地址** = myInsideNetwork 网络对象。
- **转换后的源地址** = PATaddress1 网络对象。
- **原始目标地址** = TelnetWebServer 网络对象。
- **转换后的目标地址** = TelnetWebServer 网络对象。
- **原始目标端口** = TELNET 端口对象。
- **转换后的目标端口** = TELNET 端口对象。

注释　由于您不需要转换目标地址或端口，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，以及为原始端口和转换后的端口指定相同的端口，从而为它们配置身份 NAT。



d) 点击**确定 (OK)**。

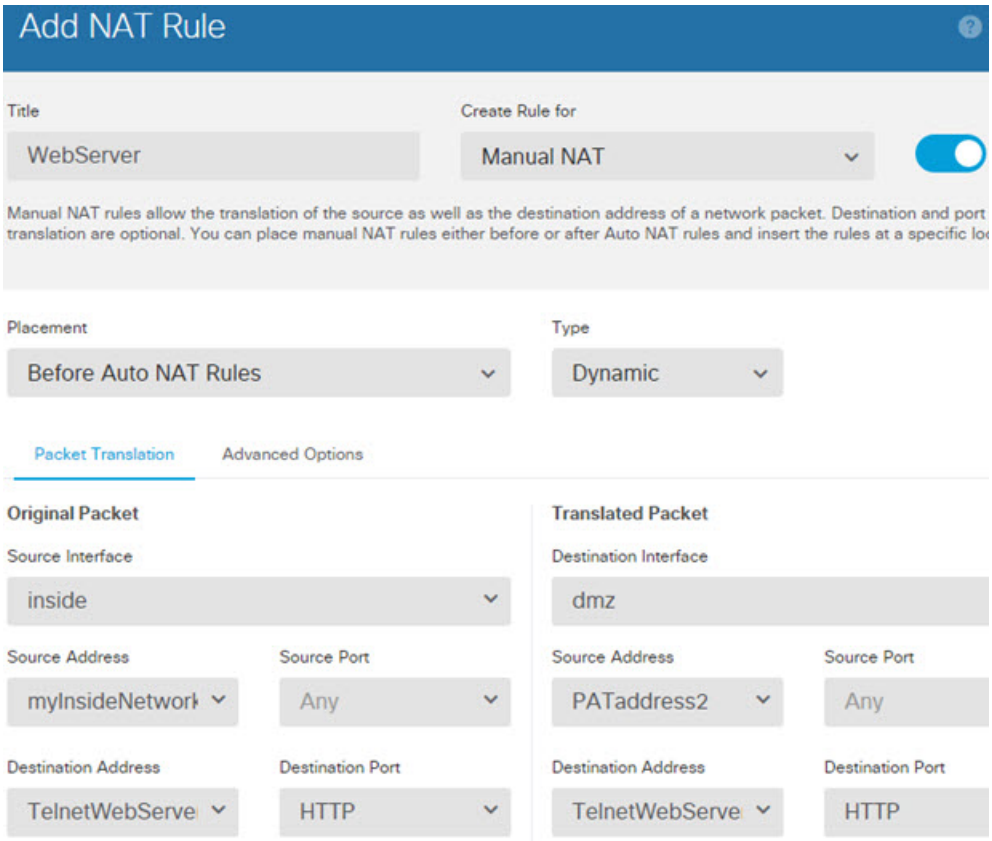
步骤 6　为 Web 访问创建动态手动 PAT。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = WebServer（或您选择的其他名称）。
- **创建规则用于** = 手动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目标接口** = dmz。
- **原始源地址** = myInsideNetwork 网络对象。
- **转换后的源地址** = PATaddress2 网络对象。
- **原始目标地址** = TelnetWebServer 网络对象。

- **转换后的目标地址** = TelnetWebServer 网络对象。
- **原始目标端口** = HTTP 端口对象。
- **转换后的目标端口** = HTTP 端口对象。



c) 点击**确定 (OK)**。

使用 NAT 重写 DNS 查询和响应

可能需要配置 威胁防御设备 以修改 DNS 应答，方法是用匹配 NAT 配置的地址替换应答中的地址。配置每条转换规则时，可以配置 DNS 修改。DNS 修改也称为“DNS Doctoring”。

此功能可以重写匹配 NAT 规则的 DNS 查询和应答中的地址（例如，适用于 IPv4 的 A 记录；适用于 IPv6 的 AAAA 记录；或者，适用于逆向 DNS 查询的 PTR 记录）。对于从映射接口穿越到任何其他接口的DNS应答，记录会从映射值被重写为实际值。相反，对于从任何接口穿越到映射接口的DNS应答，记录会从实际值被重写为映射值。此功能适用于 NAT44、NAT 66、NAT46 和 NAT64。

以下是需要在 NAT 规则上配置 DNS 重写的几种主要情况。

- 规则为 NAT64 或 NAT46，并且 DNS 服务器位于外部网络上。您需要进行 DNS 重写以实现 DNS A 记录（适用于 IPv4）和 AAAA 记录（适用于 IPv6）之间的转换。

- DNS 服务器在外部，客户端在内部，并且客户端使用的一些完全限定域名解析到其他内部主机。
- DNS服务器在内部并以专用IP地址进行响应，客户端在外部，并且客户端访问指向内部托管的服务器的完全限定域名。

DNS 重写限制

以下是 DNS 重写的某些限制：

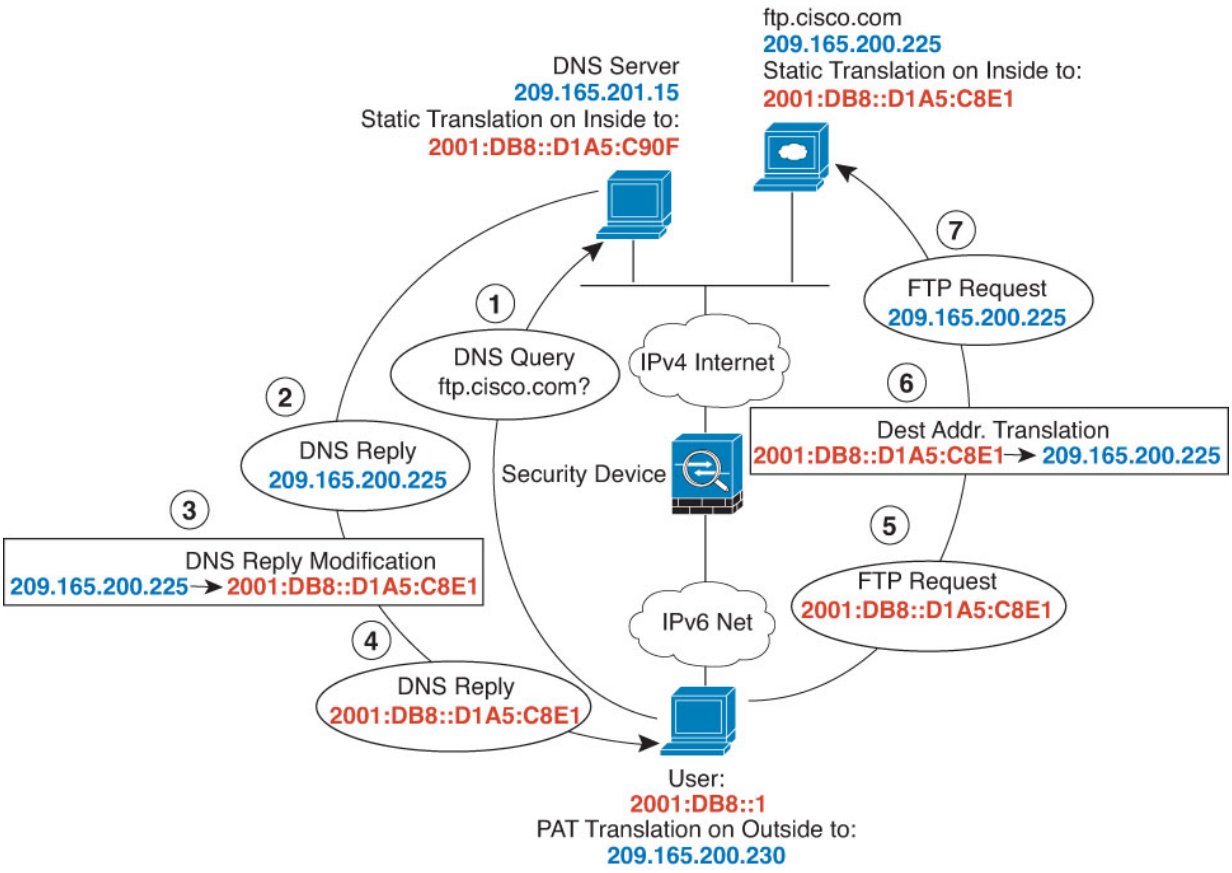
- DNS 重写不适用于 PAT，因为多条 PAT 规则适用于每个 A 或 AAAA 记录，而要使用的 PAT 规则不确定。
- 如果您配置了手动 NAT 规则，当指定了目的地址和源地址时，不能配置 DNS 修改。当流向 A 与 B 时，这类规则可能会有单个地址的不同转换。因此，将精确匹配 DNS 应答中的 IP 地址与正确的两次 NAT 规则相匹配；DNS 应答不包含有关哪个源地址/目标地址组合位于提示 DNS 请求的数据包中的信息。
- 实际上，DNS 重写在 xlate 条目而非 NAT 规则上完成。因此，如果没有面向动态规则的 xlate，则不能正确完成重写。静态 NAT 也会出现相同的问题。
- DNS 重写不会重写 DNS 动态更新消息（操作码为 5）。

以下主题提供了 NAT 规则中 DNS 重写的示例。

DNS 64 回复修改

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

由于您希望内部用户使用 ftp.cisco.com 的映射地址（2001:DB8::D1A5:C8E1，其中 D1A5:C8E1 是 209.165.200.225 的 IPv6 对应物），因此需要配置 DNS 回复修改以进行静态转换。本示例还包括面向 DNS 服务器的静态 NAT 转换和面向内部 IPv6 主机的 PAT 规则。



注释 此示例假定，内部接口不是网桥组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

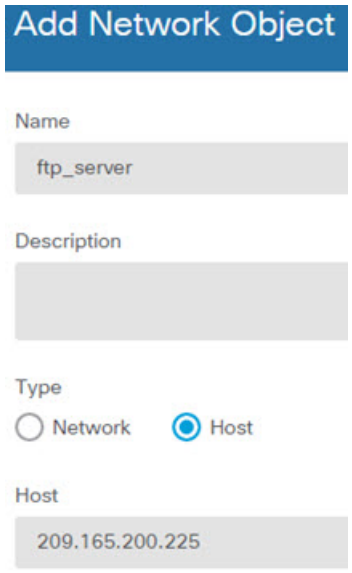
步骤 1 为 FTP 服务器、DNS 服务器、内部网络和 PAT 池创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义实际 FTP 服务器地址。

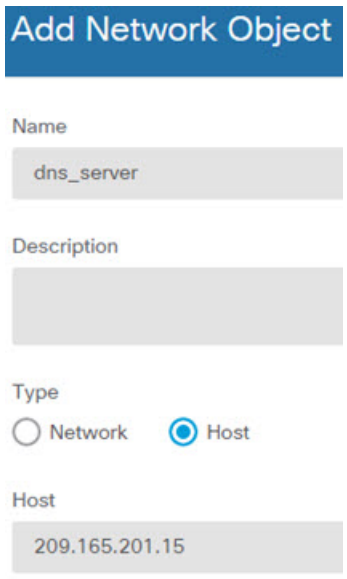
为网络对象命名（例如，ftp_server)，选择**主机**，然后输入实际主机 IP 地址 209.165.200.225。



d) 点击**确定**。

e) 点击 + 并定义 DNS 服务器的实际地址。

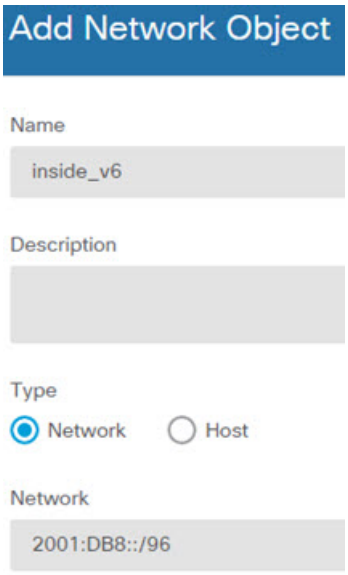
为网络对象命名（例如，dns_server)，选择**主机**，然后输入主机地址 209.165.201.15。



f) 点击**确定**。

g) 点击 + 并定义内部 IPv6 网络。

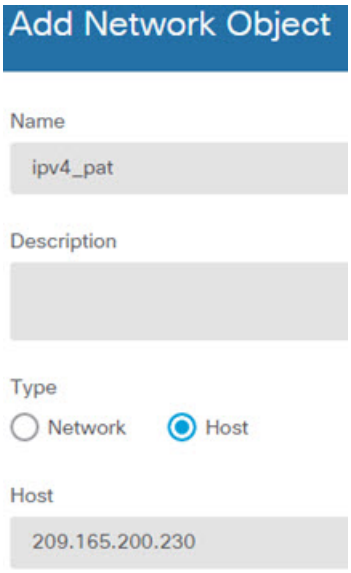
为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:DB8::/96。



h) 点击**确定**。

i) 点击 + 并为内部 IPv6 网络定义 IPv4 PAT 地址。

为网络对象命名（例如，ipv4_pat），选择**主机**，然后输入主机地址 209.165.200.230。



j) 点击**确定**。

步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

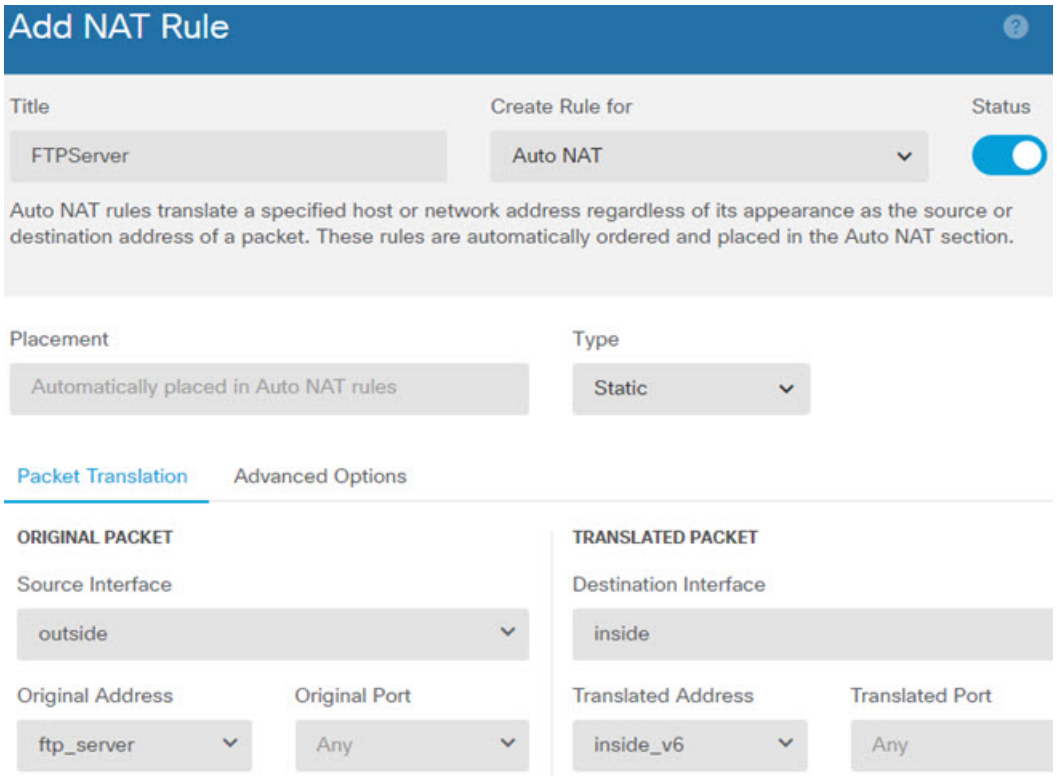
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = FTPServer（或您选择的其他名称）。

- **创建规则用于** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 外部。
- **目标接口** = 内部。
- **原始地址** = ftp_server 网络对象。
- **转换后的地址** = inside_v6 网络对象。由于在将 IPv4 转换为 IPv6 地址时使用 IPv4 嵌入地址方法，因此系统将 209.165.200.225 转换为 IPv6 对等的 D1A5:C8E1，并添加网络前缀以获取完整地址 2001:DB8::D1A5:C8E1。
- 在**高级选项**选项卡中，选择**转换与此规则匹配的 DNS 回复**。



d) 点击**确定**。

步骤 3 为 DNS 服务器配置静态 NAT 规则。

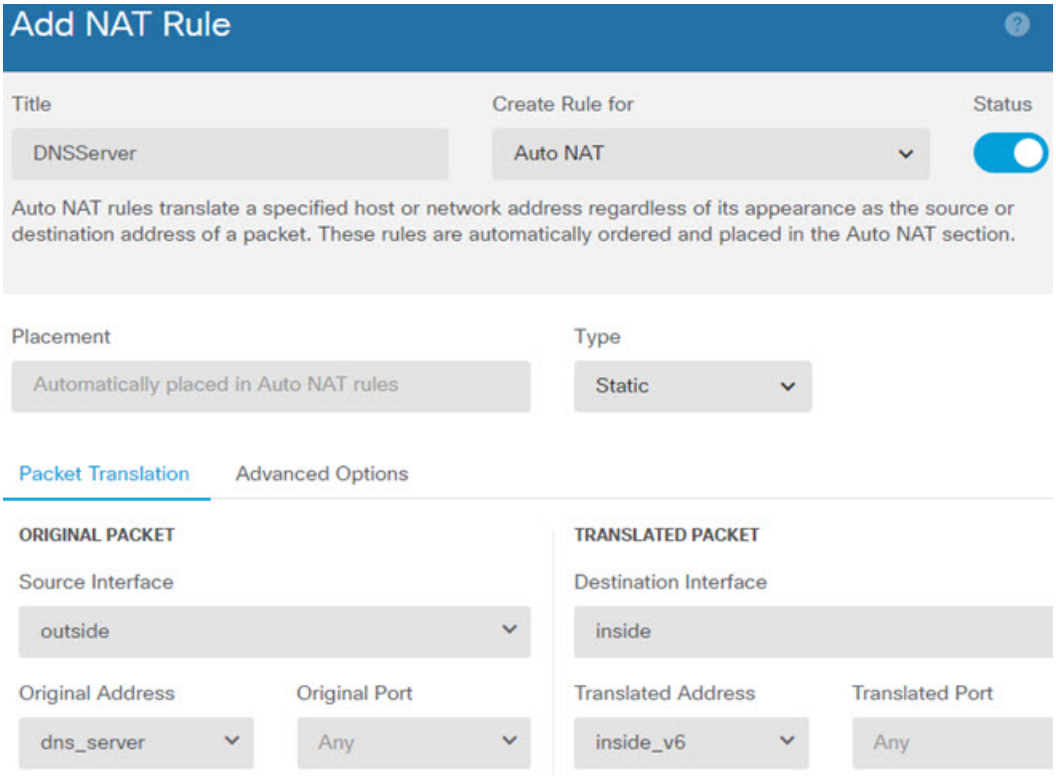
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = DNSServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。

- **类型** = 静态。
- **源接口** = 外部。
- **目标接口** = 内部。
- **原始地址** = dns_server 网络对象。
- **转换后的地址** = inside_v6 网络对象。由于在将 IPv4 转换为 IPv6 地址时使用 IPv4 嵌入地址方法，因此系统将 209.165.201.15 转换为 IPv6 对等的 D1A5:C90F，并添加网络前缀以获取完整地址 2001:DB8::D1A5:C90F。



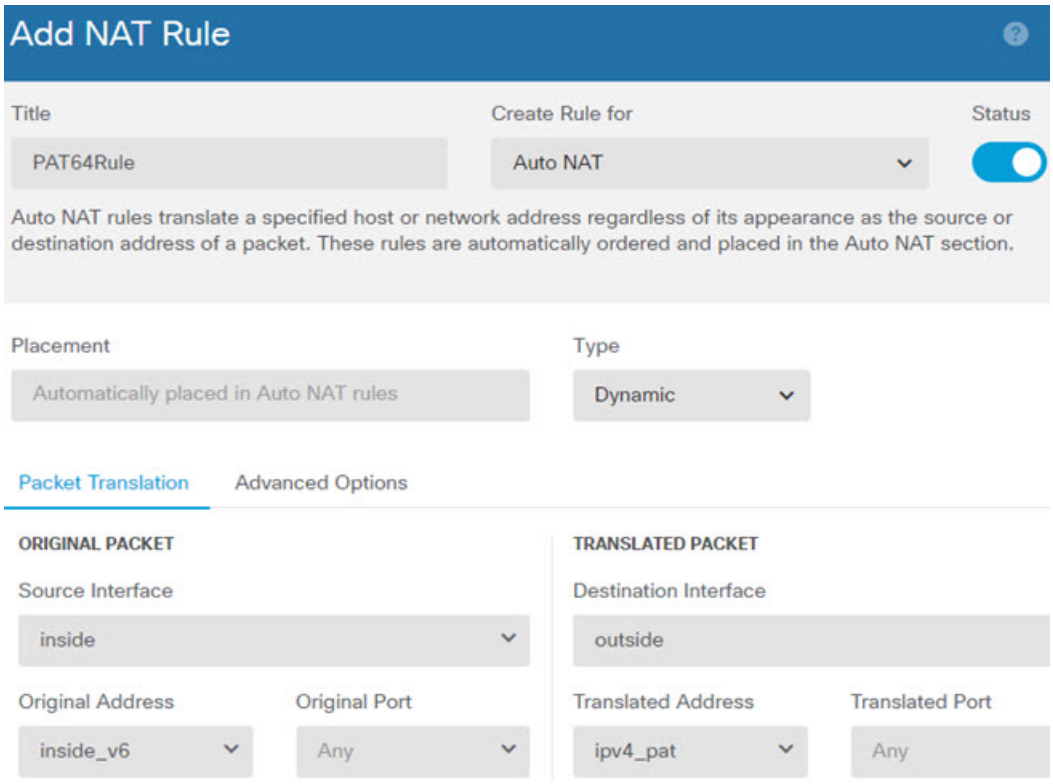
d) 点击**确定**。

步骤 4 为内部 IPv6 网络配置动态 PAT 规则。

a) 依次选择**策略** > **NAT**。
b) 点击 + 按钮。
c) 配置以下属性：

- **标题** = PAT64Rule（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 动态。
- **源接口** = 内部。

- 目标接口 = 外部。
- 原始地址 = inside_v6 网络对象。
- 转换后的地址 = ipv4_pat 网络对象。



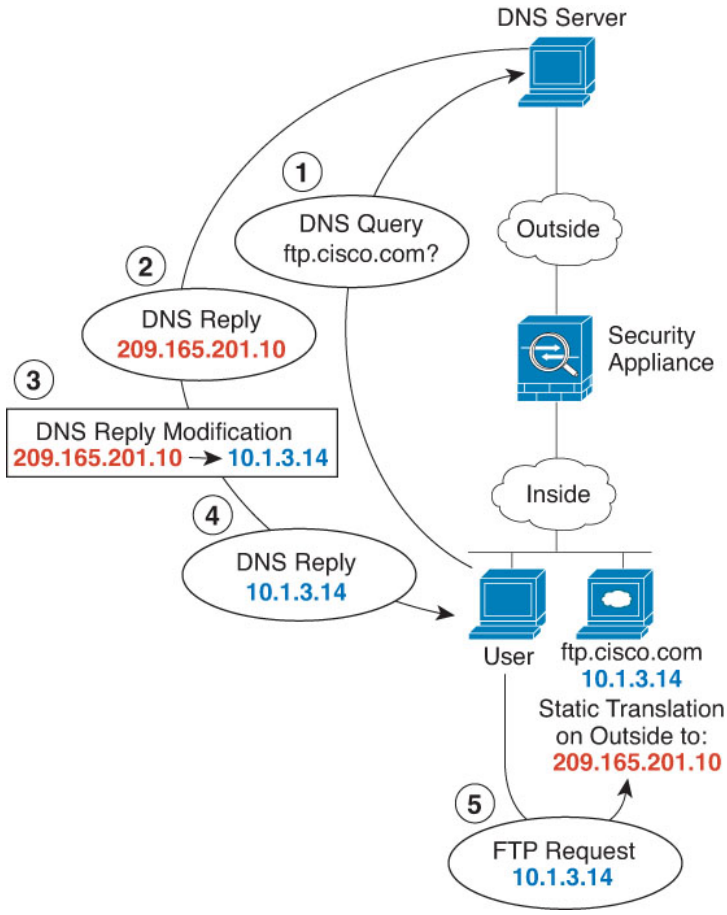
d) 点击确定 (OK)。

DNS 回复修改、外部接口上的 DNS 服务器

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

在这种情况下，您要在此静态规则上启用 DNS 回复修改，以便使用实际地址访问 ftp.cisco.com 的内部用户可以接收来自 DNS 服务器的实际地址，而不是映射地址。

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



注释 此示例假定，内部接口不是网桥组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

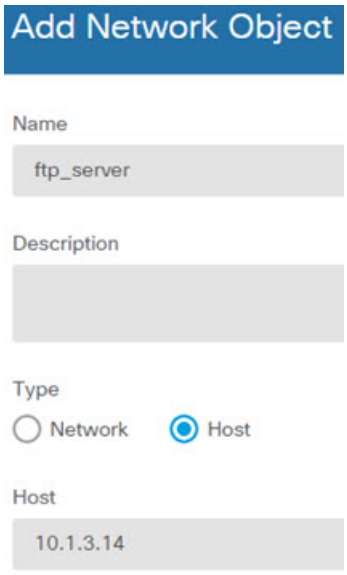
步骤 1 为 FTP 服务器创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义实际 FTP 服务器地址。

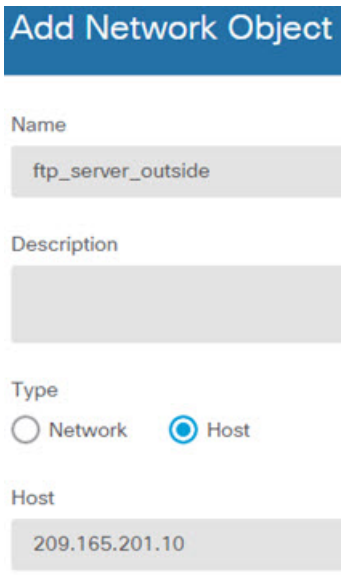
为网络对象命名（例如，ftp_server），选择**主机**，然后输入实际主机 IP 地址 10.1.3.14。



d) 点击**确定**。

e) 点击 **+**，然后定义 FTP 服务器的转换后的地址。

为网络对象命名（例如，ftp_server_outside），选择**主机**，然后输入主机地址 209.165.201.10。



步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

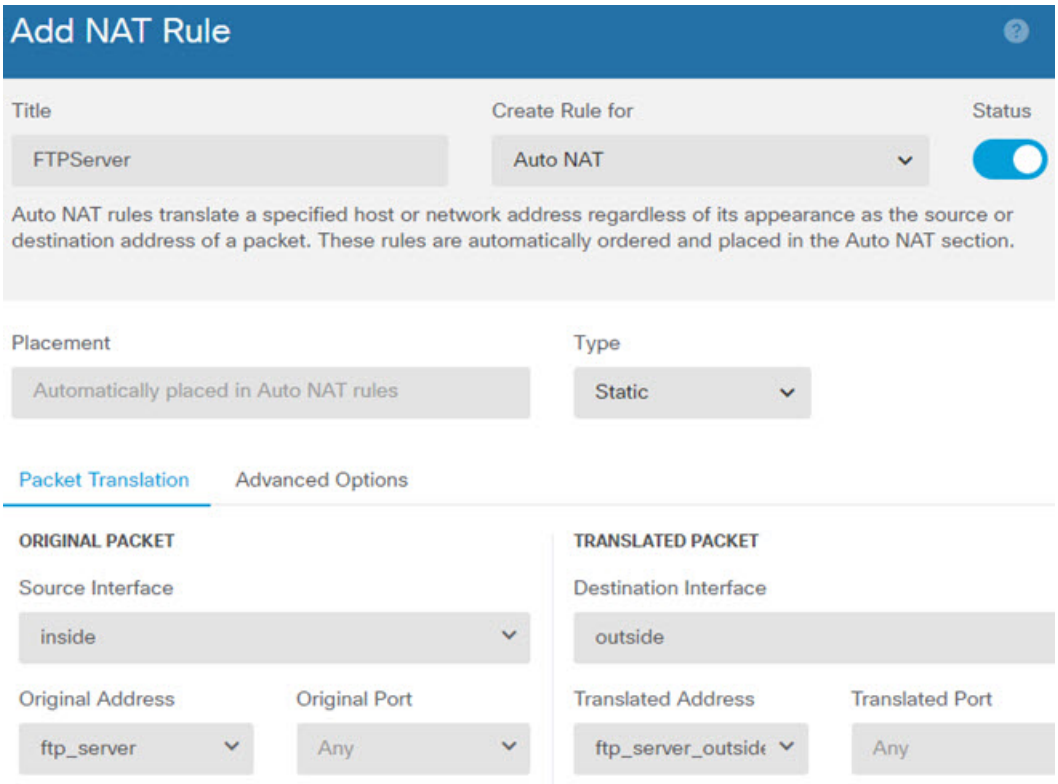
a) 依次选择**策略** > **NAT**。

b) 点击 **+** 按钮。

c) 配置以下属性：

- **标题** = FTPServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。

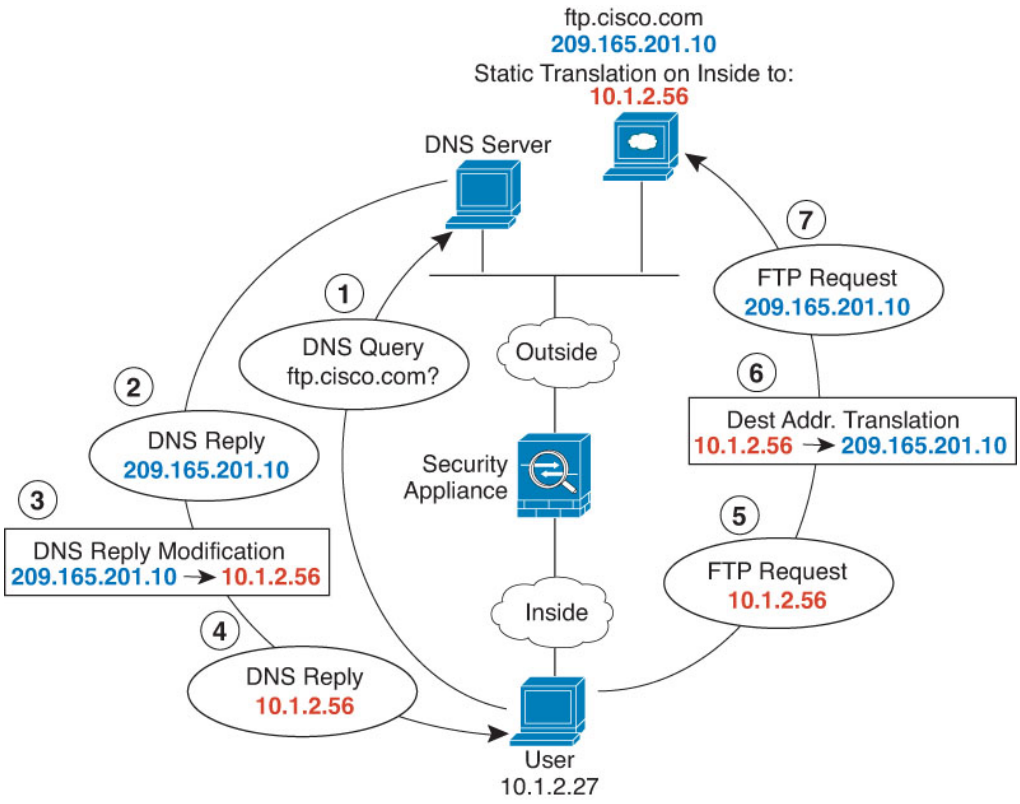
- **类型** = 静态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = ftp_server 网络对象。
- **转换后的地址** = ftp_server_outside 网络对象。
- 在**高级选项**选项卡中，选择**转换与此规则匹配的 DNS 回复**。



d) 点击**确定 (OK)**。

DNS 回复修改、主机网络上的 DNS 服务器

下图显示外部网络上的 FTP 服务器和 DNS 服务器。系统有面向外部服务器的静态转换。在这种情况下，当内部用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.20.10 作为响应。由于您希望内部用户使用 ftp.cisco.com 的映射地址 (10.1.2.56)，因此需要配置 DNS 回复修改以进行静态转换。



注释 此示例假定，内部接口不是网桥组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

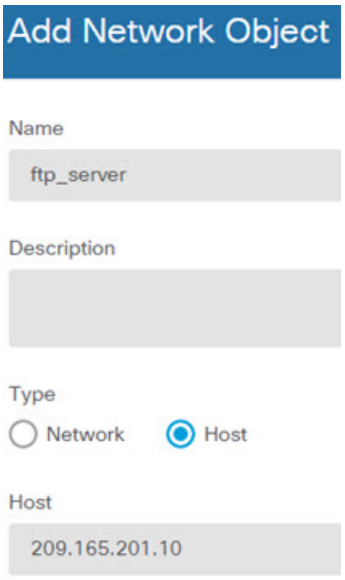
步骤 1 为 FTP 服务器创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义实际 FTP 服务器地址。

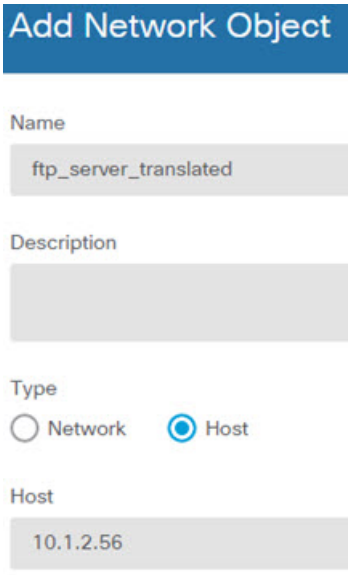
为网络对象命名（例如，ftp_server)，选择**主机**，然后输入实际主机 IP 地址 209.165.201.10.



d) 点击**确定**。

e) 点击 **+**，然后定义 FTP 服务器的转换后的地址。

为网络对象命名（例如，ftp_server_translated），选择**主机**，然后输入主机地址 10.1.2.56.



步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

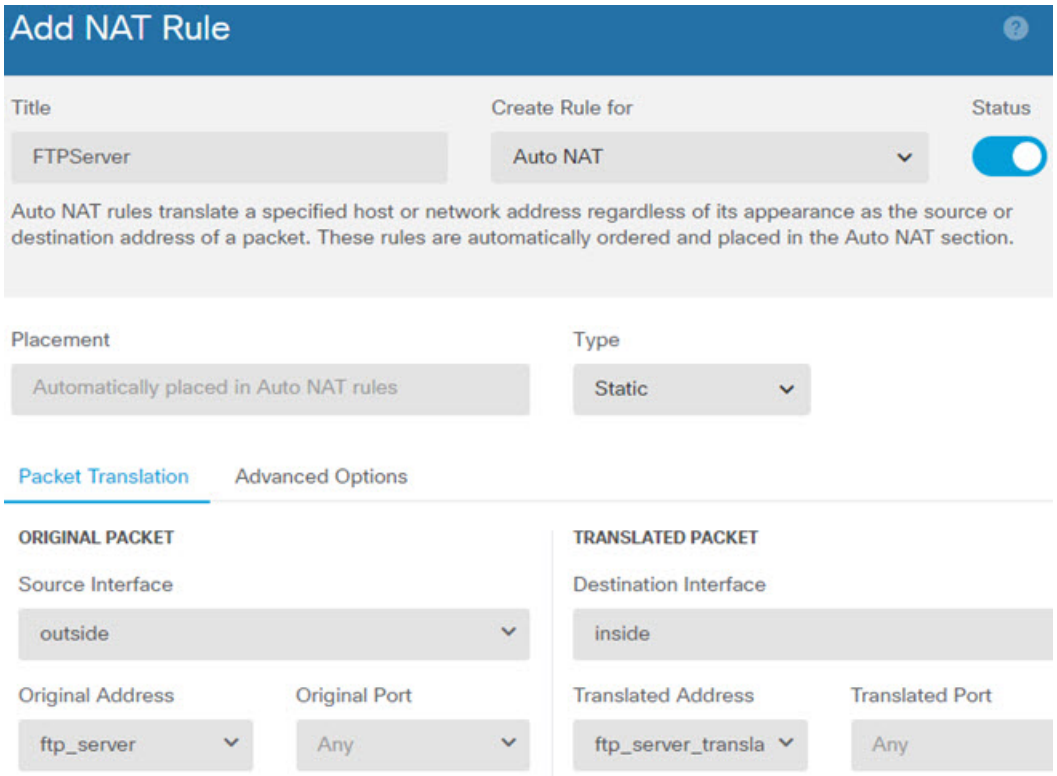
a) 依次选择**策略** > **NAT**。

b) 点击 **+** 按钮。

c) 配置以下属性：

- **标题** = FTPServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。

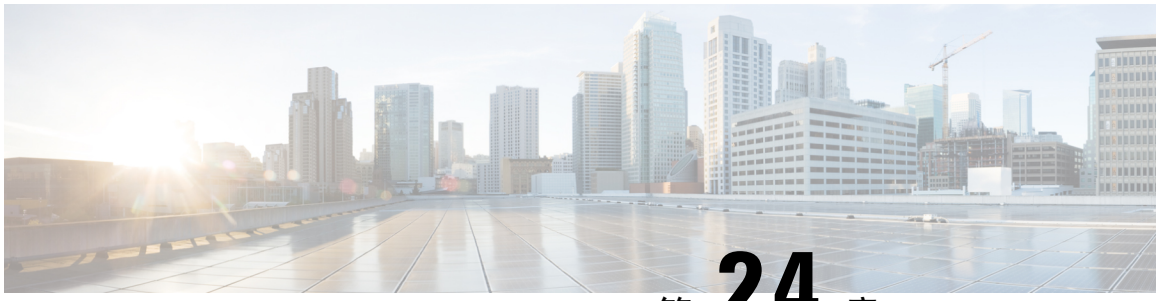
- **类型** = 静态。
- **源接口** = 外部。
- **目标接口** = 内部。
- **原始地址** = ftp_server 网络对象。
- **转换后的地址** = ftp_server_translated 网络对象。
- 在**高级选项**选项卡中，选择**转换与此规则匹配的 DNS 回复**。



d) 点击**确定 (OK)**。

第 VI 部分

虚拟专用网络 (VPN)



第 24 章

站点间 VPN

虚拟专用网络 (VPN) 是一种网络连接，通过诸如互联网或其他网络之类的公共资源在远程对等体之间建立安全隧道。VPN 使用隧道来封装正常 IP 数据包内的数据包，以在基于 IP 的网络上转发。它们使用加密来确保隐私和身份验证，以确保数据的完整性。

VPN 基础知识

借助隧道，可以使用互联网等公共TCP/IP网络在远程用户与企业专用网络之间创建安全连接。每个安全连接都称为一个隧道。

基于 IPSec 的 VPN 技术通过互联网安全关联和密钥管理协议（ISAKMP 或 IKE）以及 IPSec 隧道标准来建立和管理隧道。ISAKMP 和 IPSec 将完成以下操作：

- 协商隧道参数。
- 建立隧道。
- 验证用户和数据。
- 管理安全密钥。
- 加密和解密数据。
- 管理隧道中的数据传输。
- 作为隧道终端或路由器管理入站和出站数据传输。

VPN 中的设备可用作双向隧道终端。它可以从专用网络接收明文数据包，将其封装，创建隧道，然后发送到隧道的另一端，随后解封并发送到最终目标。它也会从公用网络接收封装数据包，将其解封，然后发送给其在专用网络上的最终目标。

建立站点间 VPN 连接之后，本地网关后的主机可通过安全 VPN 隧道连接至远程网关后的主机。一个连接由以下部分组成：这两个网关的 IP 地址和主机名、这两个网关后的子网，以及这两个网关用来进行相互身份验证的方法。

互联网密钥交换 (IKE)

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。

IKE 策略是一组算法，供两个对等体用于保护它们之间的 IKE 协商。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数保护后续 IKE 协商。对于 IKE 版本 1 (IKEv1)，IKE 策略包含单个算法集和模数组。与 IKEv1 不同，在 IKEv2 策略中，您可以选择多个算法和模数组，对等体可以在第 1 阶段协商期间从中进行选择。可创建单个 IKE 策略，尽管您可能需要不同的策略来向最需要的选项赋予更高优先级。对于站点间 VPN，您可以创建单个 IKE 策略。

要定义 IKE 策略，请指定：

- 唯一优先级（1 至 65,543，其中 1 为最高优先级）。
- 一种 IKE 协商加密方法，用于保护数据并确保隐私。
- 散列消息身份验证代码 (HMAC) 方法（在 IKEv2 中称为完整性算法），用于确保发送人身份，以及确保消息在传输过程中未被修改。
- 对于 IKEv2，使用单独的伪随机函数 (PRF) 作为派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法。这些选项与用于散列算法的选项相同。
- Diffie-Hellman 组，用于确定 encryption-key-determination 算法的强度。设备使用此算法派生加密密钥和散列密钥。
- 身份验证方法，用于确保对等体的身份。
- 在更换加密密钥前，设备可使用该加密密钥的时间限制。

当 IKE 协商开始时，发起协商的对等体将其启用的所有策略发送到远程对等体，然后远程对等体按优先级顺序搜索其自己的策略的匹配项。如果 IKE 策略具有相同的加密、散列（完整性和用于 IKEv2 的 PRF）、身份验证和 Diffie-Hellman 值，而且 SA 生命周期小于或等于发送的策略中的生命周期，则它们之间存在匹配。如果生命周期不同，则会应用较短的生命周期（来自远程对等体）。默认情况下，使用 DES 的简单 IKE 策略是唯一启用的策略。您可以启用更高优先级的其他 IKE 策略来协商更强的加密标准，但 DES 策略应确保成功协商。

VPN 连接应具有多高的安全性？

由于 VPN 隧道通常流经公共网络（最可能是互联网），因此您需要对连接进行加密以保护流量。可以使用 IKE 策略和 IPsec 提议定义要应用的加密和其他安全技术。

如果您的设备许可证允许应用较强的加密，则有大量的加密和散列算法以及Diffie-Hellman组供您选择。然而，通常情况下，应用于隧道的加密越强，系统性能越差。您要在安全性和性能之间实现平衡，在提供充分保护的同时不牺牲效率。

我们无法就选择哪些选项提供具体指导。如果您在大型公司或其他组织执行运营，可能已有需要满足的指定标准。如果没有，请花些时间研究各个选项。

下面的主题介绍了几个可用选项。

决定使用哪个加密算法

在决定用于 IKE 策略或 IPsec 提议的加密算法时，您的选择仅限于 VPN 中的设备所支持的算法。

对于 IKEv2，您可以配置多个加密算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

对于 IPsec 提议，该算法用于封装安全协议 (ESP)，该协议提供身份验证、加密和防重放服务。ESP 为 IP 协议类型 50。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀。

如果设备许可证符合强加密要求，可以从以下加密算法中选择。如果不符合强加密要求，则只能选择 DES。

注释 如果符合强加密要求，在从评估许可证升级到智能许可证之前，请检查并更新加密算法以实现更强的加密，从而使 VPN 配置正常工作。选择基于 AES 的算法。如果您使用支持强加密的账户注册，则不支持 DES。注册后，在删除对 DES 的所有使用之前，您无法部署更改。

- AES-GCM -（仅 IKEv2。）Galois/Counter 模式中的高级加密标准是提供机密性和数据源身份验证的分组加密操作模式，并且提供比 AES 更高的安全性。AES-GCM 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。GCM 是支持 NSA Suite B 所需的 AES 模式。NSA Suite B 是一套加密算法，设备必须支持这套算法才能满足密码强度的联邦标准。.
- AES - 高级加密标准是一种对称密码算法，提供比 DES 更高的安全性，在计算上比 3DES 更高效。AES 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。
- DES - 数据加密标准，使用 56 位密钥进行加密，是一种对称密钥块算法。如果您的许可证账户不符合导出控制要求，这将是您唯一的选择。
- Null、ESP-Null - 不使用加密。空加密算法提供不加密的身份验证。大多数平台都不支持这种加密算法。

决定使用哪些散列算法

在 IKE 策略中，散列算法创建消息摘要，用于确保消息的完整性。在 IKEv2 中，散列算法分成两个选项，一个用于完整性算法，一个用于伪随机函数 (PRF)。

在 IPsec 提议中，散列算法由封装安全协议 (ESP) 用于身份验证。在 IKEv2 IPsec 提议中，这称为完整性散列。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀，并且还有 -HMAC 后缀（代表“散列方法身份验证代码”）。

对于 IKEv2，您可以配置多个散列算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

您可以选择以下散列算法：

- SHA （安全散列算法）- 生成 160 位摘要的标准 SHA (SHA1)。

  以下 SHA-2 选项更加安全，可用于 IKEv2 配置。如果要实施 NSA Suite B 加密规范，请选择以下选项之一。

  - SHA256 - 指定具有 256 位摘要的安全散列算法 SHA 2。
  - SHA384 - 指定具有 384 位摘要的安全散列算法 SHA 2。
  - SHA512 - 指定具有 512 位摘要的安全散列算法 SHA 2。

- 空或无（NULL、ESP-NONE） -（仅限 IPsec 提议。）空散列算法；这通常仅用于测试目的。但是，如果选择 AES-GCM 选项之一作为加密算法，则应选择空完整性算法。即使选择非空选项，这些加密标准也会忽略完整性散列。

决定要使用的 Diffie-Hellman 模数组

您可以使用以下 Diffie-Hellman 密钥导出算法生成 IPsec 安全关联 (SA) 密钥。每组具有不同的长度模数。模数越大，安全性越高，但需要的处理时间更长。两个对等体上必须具有一个匹配的模数组。

如果选择 AES 加密，要支持 AES 所需的大型密钥长度，应使用 Diffie-Hellman (DH) 组 5 或更高组。IKEv1 策略不支持下面列出的所有组。

要实施 NSA Suite B 加密规范，请使用 IKEv2 并选择椭圆曲线 Diffie-Hellman (ECDH) 的一个选项：19、20 或 21。使用 2048 位模数的椭圆曲线选项和组较少遭受 Logjam 等攻击。

对于 IKEv2，您可以配置多个组。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

- 14 - Diffie-Hellman 组 14：2048 位模幂算法 (MODP) 组。被认为可以良好地保护 192 位密钥。
- 15 - Diffie-Hellman 组 15：3072 位 MODP 组。
- 16 - Diffie-hellman 组 16：4096 位 MODP 组。
- 19 - Diffie-Hellman 组 19：美国国家标准与技术研究所 (NIST) 256 位椭圆曲线取素数 (ECP) 组。
- 20 - Diffie-Hellman 组 20： NIST 384 位 ECP 组。
- 21 - Diffie-Hellman 组 21： NIST 521 位 ECP 组。
- 31 - Diffie-Hellman 组 31：椭圆曲线 25519 256 位 EC 组。

确定使用哪种身份验证方法

可以使用以下方法对站点间 VPN 连接中的对等体进行身份验证。

预共享密钥

预共享密钥是在连接中的每个对等体上配置的加密密钥字符串。这些密钥由 IKE 在身份验证阶段使用。对于 IKEv1，您必须在每个对等体上配置相同的预共享密钥。对于 IKEv2，您可以在每个对等体上配置唯一密钥。

与证书相比，预共享密钥的扩展性相对逊色。如果需要配置大量的站点间VPN连接，请使用证书而非预共享密钥。

证书

数字证书使用 RSA 密钥对为 IKE 密钥管理消息进行签名和加密。在配置站点间 VPN 连接的两端时，请选择本地设备的身份证书，以便远程对等体可以对本地对等体进行身份验证。

要使用证书方法，您需要执行以下操作：

1. 使用证书颁发机构 (CA) 注册本地对等体并获取设备身份证书。将证书上传到设备。有关详细信息，请参阅上传内部证书和内部 CA 证书，第 145 页。

   如果您也负责远程对等体，还需注册此对等体。虽然对这些对等体使用同一CA比较方便，但并非必须要这么做。

   无法使用自签证书来建立 VPN 连接。必须使用证书颁发机构来注册设备。

   如果使用 Windows 证书颁发机构 (CA) 创建用于站点间 VPN 终端的证书，则必须使用为应用策略扩展指定 IP 安全终端系统的证书。可以在证书“属性”对话框中的“扩展”选项卡上（在 Windows CA 服务器上）找到此内容。此扩展的默认值为“IP 安全 IKE 中间”，对于使用 设备管理器配置的站点间 VPN 不起作用。

2. 上传用于签署本地对等体身份证书的受信任 CA 证书。如果使用了中间 CA，请上传完整的证书链，包括根证书和中间证书。有关详细信息，请参阅上传受信任的 CA 证书，第 148 页。

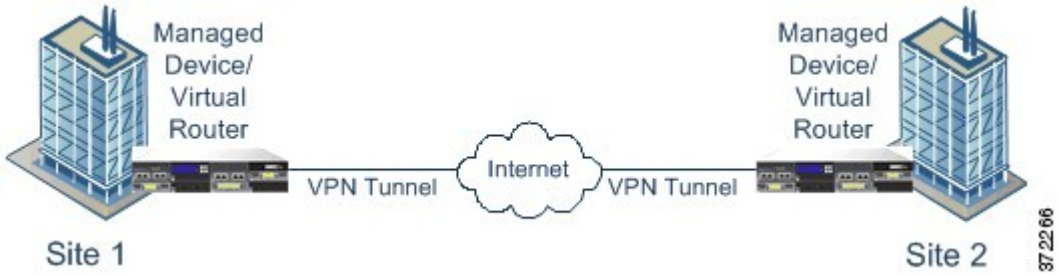
3. 如果使用了不同的 CA 注册远程对等体，还需上传用于签署远程对等体身份证书的受信任 CA 证书。从控制远程对等体的组织获取证书。如果他们使用了中间 CA，请上传完整的证书链，包括根证书和中间证书。

4. 在配置站点间 VPN 连接时，请选择证书方法，然后选择本地对等体的身份证书。连接的每一端会指定连接本地端的证书；您无需指定远程对等体的证书。

VPN 拓扑

只能使用 设备管理器来配置点对点 VPN 连接。虽然所有连接都是点对点的，但您可以通过定义设备参与的每个隧道，链接到更大的中心辐射型或网状 VPN。

下图显示了典型的点对点 VPN 拓扑。在点对点 VPN 拓扑中，两个终端彼此直接通信。将两个终端配置为对等体设备，任一台设备均可启动安全连接。



与动态寻址对等体建立站点间 VPN 连接

即使不知道对等体的 IP 地址，您也可以创建到此对等体的站点间 VPN 连接。此功能在以下情况下非常有用：

- 对等体使用 DHCP 获取它的地址时，您不能使用具有特定静态 IP 地址的远程终端。
- 设备在中心辐射型拓扑中充当控制中心，允许与其建立连接的远程对等体的数量不确定。

需要与动态寻址对等体 B 建立安全连接时，您需要确保连接端点 A 拥有静态 IP 地址。随后，在 A 上创建连接时，请指明对等体具有动态地址。但是，在对等体 B 上配置连接时，请确保输入 A 的 IP 地址作为远程对等地址。

当系统建立站点间 VPN 连接时，任何包含具有动态地址的对等体的连接都处于仅响应状态。换言之，必须由远程对等体发起连接。在远程对等体尝试建立连接时，设备会使用您在连接中定义的方法（预共享密钥或证书）验证连接。

由于只有在远程对等体发起连接之后才会建立VPN连接，因此在连接建立之前，系统会丢弃与允许流量通过 VPN 隧道的访问控制规则匹配的出站流量。这可确保数据不会在未采取适当加密和 VPN 保护措施的情况下离开您的网络。

虚拟隧道接口和基于路由的 VPN

传统上，您通过定义通过 VPN 隧道加密的特定本地和远程网络来配置站点间 VPN 连接。这些在 VPN 连接配置文件的加密映射中定义。这种类型的站点间 VPN 称为基于策略的 VPN。

或者，您还可以配置基于路由的站点间 VPN。在这种情况下，您可以创建虚拟隧道接口 (VTI)，即与特定物理接口（通常是外部接口）关联的虚拟接口。然后，使用带有静态和动态路由的路由表将所需流量定向到 VTI。通过 VTI（出口）路由的所有流量都通过您为 VTI 配置的 VPN 隧道进行加密。

因此，使用基于路由的站点间 VPN，只需更改路由表即可管理给定 VPN 连接中的受保护网络，而完全无需更改 VPN 连接配置文件。您无需跟踪远程网络并更新 VPN 连接配置文件，以考虑这些更改。这简化了云运营商和大型企业的 VPN 管理。

此外，您可以为 VTI 创建访问控制规则，以调整隧道中允许的流量类型。例如，您可以应用入侵检测以及 URL 和应用过滤。

配置基于路由的 VPN 的过程概述

简言之，设置基于路由的站点间 VPN 的过程包括以下步骤：

过程

步骤 1 为本地终端创建 IKEv1/2 策略和 IPsec 提议。

步骤 2 创建与面向远程对等体的物理接口关联的虚拟隧道接口 (VTI)。

步骤 3 创建使用 VTI、IKE 策略和 IPsec 提议的站点间 VPN 连接配置文件。

步骤 4 在远程对等体、远程 VTI 和指定此本地 VTI 作为远程终端的站点间 VPN 连接配置文件上创建与远程终端相同的 IKE 和 IPsec 提议（从远程对等体的角度来看）。

步骤 5 在两个对等体上创建路由和访问控制规则，以通过隧道发送相应流量。

确保每个终端上的路由和访问控制相互镜像，以允许流量在两个方向上流动。

静态路由具有以下一般特征：

- **接口** - 虚拟隧道接口 (VTI) 名称。
- **网络** - 定义受远程终端保护的远程网络的网络对象。
- **网关** - 定义 VPN 隧道的远程终端 IP 地址的网络对象。

虚拟隧道接口和基于路由的 VPN 准则

IPv6 准则

虚拟隧道接口仅支持 IPv4 地址。无法在 VTI 上配置 IPv6 地址。

其他准则

- 最多可以创建 1024 个 VTI。
- 不能在 VTI 基于路由的 VPN 上配置静态或动态反向路由注入。（只能使用 威胁防御 API 配置反向路由注入。）
- 选择 VTI 作为本地接口时，无法配置动态对等体地址。
- 选择 VTI 作为本地接口时，无法配置远程备份对等体。
- 不能为分配给自定义虚拟路由器的源接口创建 VTI。使用虚拟路由器时，只能在全局虚拟路由器中的接口上配置 VTI。
- 无论隧道中的数据流量如何，IKE 和 IPsec 安全关联都将不断重新生成密钥。这可确保 VTI 隧道始终处于活动状态。
- 不能在基于路由的连接配置文件上同时配置 IKEv1 和 IKEv2：必须仅配置一个 IKE 版本。

- 只要加密映射中配置的对等体地址与 VTI 的隧道目的地不同，就可以在同一个物理接口上使用不同的 VTI 和基于策略的（加密映射）配置。
- 在 VTI 上仅支持 BGP 路由协议。
- 如果系统终接 IOS IKEv2 VTI 客户端，请禁用 IOS 上的配置交换请求，因为系统无法为由 IOS VTI 客户端发起的会话检索 mode-CFG 属性。
- 基于路由的站点间 VPN 配置为双向，这意味着 VPN 隧道的任一终端都可以发起连接。创建连接配置文件后，您可以将此终端更改为唯一发起方 (INITIATE_ONLY) 或唯一响应方 (RESPOND_ONLY)。确保将远程终端修改为使用补充连接类型。要进行此更改，您必须转到 API Explorer 并使用 GET /devices/default/s2sconnectionprofiles 查找连接配置文件。然后，您可以将正文内容复制/粘贴到 PUT /devices/default/s2sconnectionprofiles/{objId} 方法中，更新 **connectionType** 以指定所需类型，并运行该方法。

IPsec 流分流

您可以将支持的设备型号配置为使用IPsec数据流分流。初始设置IPsec站点间VPN或远程访问VPN安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)，这应该会提高设备性能。

分流操作特别涉及入口上的预解密和解密处理，以及出口上的预加密和加密处理。系统软件处理内部流以应用安全策略。

默认情况下启用 IPsec 数据流分流，并应用于以下设备类型：

- Secure Firewall 3100

IPsec 流分流的限制

不分流以下 IPsec 流：

- IKEv1 隧道。仅 IKEv2 隧道将被分流。IKEv2 支持更强的密码。
- 配置了基于卷的密钥更新的流。
- 已配置压缩的流。
- 传输模式流。仅会分流隧道模式流。
- AH 格式。仅支持 ESP/NAT-T 格式。
- 已配置后分段的流。
- 防重放窗口大小不是 64 位且防重放的流不会被禁用。
- 已启用防火墙过滤器的流。

配置 IPsec 数据流分流

默认情况下，在支持该功能的硬件平台上启用 IPsec 数据流分流。要更改配置，请使用 FlexConfig 实施 **flow-offload-ipsec** 命令。有关命令的详细信息，请参阅 ASA 命令参考。

管理站点间 VPN

虚拟专用网络 (VPN) 是一种网络连接，通过诸如互联网或其他网络之类的公共资源在远程对等体之间建立安全隧道。VPN 使用隧道来封装正常 IP 数据包内的数据包，以在基于 IP 的网络上转发。它们使用加密来确保隐私和身份验证，以确保数据的完整性。

您可以与对等体设备创建VPN连接。所有连接都是点对点连接，但您可以通过配置所有相关连接，将设备连接到更大的中心辐射型或网格 VPN 中。

开始之前

以下事实控制可重新创建的站点间 VPN 连接的类型和数量：

- VPN 连接使用加密技术保护网络隐私。您可以使用的加密算法取决于您的基本许可证是否允许强加密。而控制这一点的，则是您在向思科智能许可证管理器注册时是否选择了允许在设备上使用出口控制功能的选项。如果您使用的是评估许可证，或者您没有启用出口控制功能，则无法使用强加密。
- 您最多可以创建 20 个唯一性 IPsec 配置文件。唯一性取决于 IKEv1/v2 提议和证书、连接类型、DH 组和 SA 生命周期的组合。您可以重复使用现有配置文件。因此，如果对所有站点间 VPN 连接使用相同的设置，则只有一个唯一性 IPsec 配置文件。一旦达到 20 个唯一性 IPsec 配置文件的限制，就无法创建新的站点间VPN连接，除非使用与现有连接配置文件相同的属性组合。

过程

步骤 1 点击**设备**，然后点击站点间 VPN 组中的**查看配置 (View Configuration)**。

此操作将打开“站点间 VPN”(Site-to-Site VPN) 页面，其中列出了您已配置的所有连接。

步骤 2 执行以下任一操作。

- 要创建新的站点间 VPN 连接，请点击 + 按钮。请参阅配置站点间 VPN 连接，第 622 页。

  如果尚无连接，也可以点击**创建站点间连接**按钮。

- 要编辑现有连接，请点击该连接的编辑图标 ( )。请参阅配置站点间 VPN 连接，第 622 页。
- 要将连接配置的摘要复制到剪贴板，请点击该连接的复制图标 ( )。您可以将此信息粘贴到文档中发送给远程设备的管理员，帮助完成连接另一端的配置。
- 要删除不再需要的连接，请点击该连接的删除图标 ( )。

配置站点间 VPN 连接

假定获得了远程设备所有者的合作与权限，您可以创建点对点VPN连接，将您的设备链接到另一台设备。虽然所有连接都是点对点的，但您可以通过定义设备参与的每个隧道，链接到更大的中心辐射型或网状 VPN。

开始之前

您可以为每个本地网络/远程网络组合创建单个 VPN 连接。但是，如果远程网络在每个连接配置文件中是唯一的，则可以为本地网络创建多个连接。

如果远程网络重叠，请务必先创建限制更严格的连接配置文件。系统将按照您创建连接配置文件的顺序创建隧道，而不是按其显示顺序（即字母顺序）创建隧道。

例如，如果您希望从192.16.0.0/16到10.91.0.0/16的一个隧道通向远程终端A，但希望隧道192.16.0.0/24通过远程终端 B 通向 10.0.0.0/8 的其余部分，则必须为 A 创建连接配置文件，然后再为 B 创建连接配置文件。

过程

步骤 1 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。

步骤 2 执行以下任一操作：

- 要创建新的站点间 VPN 连接，请点击 + 按钮。

  如果尚无连接，也可以点击**创建站点间连接**按钮。

- 要编辑现有连接，请点击该连接的编辑图标 ( )。

要删除不再需要的连接，请点击该连接的删除图标 ( )。

步骤 3 定义点对点 VPN 连接的终端。

- **连接配置文件名称** - 此连接的名称，最多 64 个字符，不含空格。例如，MainOffice。不能将 IP 地址用作名称。
- **类型** - 如何识别应通过 VPN 隧道发送的流量。选择以下一个选项：
  - **基于路由 (VTI)** - 您将使用路由表（主要是静态路由）定义应参与隧道的本地和远程网络。如果选择此选项，则必须选择虚拟隧道接口 (VTI) 作为本地 VPN 接入接口。您还必须为隧道的远程端使用静态 IP 地址。确保在创建 VPN 连接配置文件后为 VTI 配置适当的静态路由和访问控制规则。
  - **基于策略** - 您将直接在站点间 VPN 连接配置文件中指定本地和远程网络。这是定义哪些流量应受 VPN 隧道保护的经典方法。
- **本地站点** - 这些选项定义本地终端。

- **本地 VPN 访问接口** - 选择远程对等体可连接的接口。这通常是外部接口。该接口不能是网桥组的成员。如果为基于策略的连接配置备用对等体，请确保选择对等体可以连接的所有接口。对于基于路由的连接，只能选择一个接口。
- **本地网络** -（仅基于策略。）点击 + 并选择标识应参与 VPN 连接的本地网络的网络对象。这些网络上的用户将能够通过该连接访问远程网络。

  注释　您可以为这些网络使用 IPv4 或 IPv6 地址，但必须在连接的每一侧都具有匹配的地址类型。例如，本地 IPv4 网络的 VPN 连接必须至少有一个远程 IPv4 网络。您可以在单个连接的两端结合 IPv4 和 IPv6。终端受保护的网络不能重叠。

- **远程站点** - 这些选项定义远程终端。
  - **静态/动态** - 远程对等体的 IP 地址是以静态还是动态的方式定义的（例如，通过 DHCP 定义）。如果选择**静态**，请输入远程对等体的 IP 地址。如果选择**动态**，仅远程对等体可以发起此 VPN 连接。

    对于基于路由的 VPN，您可以仅选择**静态**。
  - **远程 IP 地址**（仅限于静态寻址。）- 输入将用于托管 VPN 连接的远程 VPN 对等体接口的 IP 地址。
  - **远程备用对等体** -（可选，仅基于策略的连接。）点击**添加对等体**为远程终端添加备用对等体。如果主终端不可用，系统会尝试与其中一个备用对等体重新建立VPN连接。您可以添加多个备用对等体。

    配置每个备用对等体时，您可以配置要用于该对等体的预共享密钥和证书。使用您为主远程对等体配置的相同技术。将这些设置留空可使用为连接配置文件配置的相同值。

    配置第一个备用对等体后，您可以通过点击**添加另一个对等体**来添加另一个对等体，或删除对等体，或点击**编辑**更改对等体的设置。

    如果备用对等体可通过主对等体之外的其他接口访问，请确保在**本地 VPN 访问接口**下选择所需接口。
  - **远程网络** -（仅基于策略。）点击 + 并选择标识应参与 VPN 连接的远程网络的网络对象。这些网络上的用户将能够通过连接访问本地网络。

步骤 4　点击**下一步**。

步骤 5　定义 VPN 的隐私配置。

注释　您的许可证决定您可以选择哪些加密协议。您必须符合强加密的条件，即满足导出管制条件，才能选择除最基本选项以外的任何其他选项。

- **IKE 版本 2**，**IKE 版本 1** - 选择在互联网密钥交换 (IKE) 协商期间使用的 IKE 版本。对于基于策略的连接，可以选择其中一项或两项；对于基于路由的连接，只能选择其中一项。当设备尝试与另一个对等体协商连接时，它使用您允许且该对等体接受的任何版本。如果这两个版本都允许，而对于最初选择的版本的协商不成功，则设备将自动回退到另一个版本。如果配置了 IKEv2，则系统将始终首先尝试它。两个对等体必须都支持 IKEv2 才能在协商中使用它。

- **IKE 策略** - 互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。这是一个全局策略：您启用的对象应用于所有 VPN。点击**编辑**以检查每个 IKE 版本当前全局启用的策略，并启用和创建新的策略。有关详细信息，请参阅配置全局 IKE 策略，第 626 页。
- **IPsec 提议** - IPsec 提议定义确保 IPsec 隧道中流量安全的安全协议和算法的组合。点击**编辑**并为每个 IKE 版本选择提议。选择要允许的所有提议。点击**设置默认值**以简单选择系统默认值，这根据您的出口合规性而有所不同。系统与对等体协商，从最强到最弱的提议，直到约定一个匹配项。有关详细信息，请参阅配置 IPsec 提议，第 630 页。
- **身份验证类型** - 您想要如何对 VPN 连接中的对等体进行身份验证，**预共享手动密钥**或**证书**中的任一种方法。您还需要根据您的选择填写以下字段。对于 IKEv1，您的选择必须与连接配置的 IKEv1 策略对象中选择的身份验证方式匹配。有关这些选项的详细信息，请参阅确定使用哪种身份验证方法，第 617 页。
  - （IKEv2）**本地预共享密钥，远程对等预共享密钥** - 此设备和远程设备上为 VPN 连接定义的密钥。这些密钥在 IKEv2 中可能不同。该密钥可以有 1 至 127 个字母数字字符。
  - （IKEv1）**预共享密钥** - 本地和远程设备上均定义的密钥。该密钥可以有 1 至 127 个字母数字字符。
  - **证书** - 本地对等体的设备身份证书。必须是通过证书颁发机构 (CA) 获取的证书；不能使用自签证书。如果尚未上传证书，请点击**创建新对象**链接。您还需要上传用于签署身份证书的根证书和所有中间受信任的 CA 证书。确保将上传的证书的**验证使用**设置为包括 **IPsec 客户端**。如果尚未上传这些证书，可以在完成向导后执行此操作。
- **IPsec 设置** - 安全关联的生存期。达到生存期后，系统会重新协商安全关联。当系统收到对等体发来的协商请求时，它会使用对等体提出的生存期值或本地配置的生存期值（取较小者）作为新安全关联的生存期。有两个生存期：“定时”生存期和“流量”生存期。只要到达这两个生存期之一（无论先到达哪一个），安全关联就会到期。
  - **生存期持续时间** - 安全关联在到期前可以存续的秒数。范围为 120 到 214783647 秒。全局默认值为 28,800 秒（8 小时）。
  - **生存期大小** - 使用特定安全关联的对等体之间在该安全关联到期前可通过的流量（以千字节为单位）。范围为 10 到 2147483647 千字节或留空。全局默认值为 4,608,000 千字节。将该字段留空可删除基于大小的限制，并使用持续时间作为唯一限制。
- **NAT 豁免** -（仅基于策略。）是否从本地 VPN 访问接口的 NAT 策略中豁免 VPN 流量。如果不想将 NAT 规则应用于本地网络，请选择托管本地网络的接口。此选项仅在本地网络驻留在单个路由接口（而非网桥组成员）后时有用。如果本地网络位于多个路由接口或一个或多个网桥组成员之后，则必须手动创建 NAT 豁免规则。有关手动创建所需规则的信息，请参阅使站点间 VPN 流量豁免 NAT，第 636 页。
- **完美前向保密的 Diffie-Hellman 组** - 是否使用完美前向保密 (PFS) 为每个加密交换生成和使用唯一会话密钥。唯一会话密钥可保护交换免于后续解密，即使整个交换已被记录且攻击者已经获得终端设备使用的预共享密钥或私钥。要启用完美前向保密，请选择在模数组列表中生成 PFS 会话密钥时使用的 Diffie-Hellman 密钥导出算法。如果同时启用 IKEv1 和 IKEv2，则选项仅限

于 IKEv1 支持的那些。有关选项的说明，请参阅 决定要使用的 Diffie-Hellman 模数组，第 616 页。

步骤 6 点击**下一步**。

步骤 7 查看摘要并点击**完成**。

摘要信息将复制到剪贴板。您可以将这些信息粘贴到文档中，并使用它来帮助您配置远程对等体，或将其发送到负责配置对等体的一方。

您必须执行一些附加步骤，才能允许 VPN 隧道中的流量，如允许流量通过站点间 VPN，第 626 页中所述。

部署配置后，登录到设备 CLI 并使用 **show ipsec sa** 命令确认终端是否建立了安全关联。请参阅验证站点间 VPN 连接，第 633 页。

配置虚拟隧道接口

您只能在基于路由的站点间VPN连接配置文件中使用虚拟隧道接口(VTI)。VTI与物理接口相关联，通过该物理接口与远程对等体建立 VPN 连接。使用虚拟接口，您可以简化站点间 VPN 连接并使用静态和动态路由控制流量，而无需在连接配置文件中为 VPN 指定本地和远程网络。

过程

步骤 1 点击**设备**，然后点击“接口”摘要中的链接，再点击**虚拟隧道接口**。

步骤 2 执行以下任一操作：

- 点击 **+** 或**创建虚拟隧道接口**以创建新接口。
- 点击现有接口的编辑图标 ( )。

如果不再需要某个子接口，请点击其删除图标 ( )。您必须先删除使用该接口的任何站点间连接配置文件，然后才能将其删除。

步骤 3 配置以下选项：

- **名称** - 接口的名称，最多 48 个字符。如果更改现有接口的名称，系统会在包含该接口的所有策略和对象中自动更改该接口。不得在名称中使用大写字母。
- **状态** - 将滑块点击为启用状态 。
- **说明** -（可选。）一行说明最多可包含 200 个字符（不包括回车符）。
- **隧道 ID** - 介于 0-10413 之间的编号。此编号附加到 Tunnel 一词后面，构成接口的硬件名称。您必须选择尚未用于其他 VTI 的编号。例如，输入 1 可创建接口 Tunnel1。

- **隧道源** - 选择与此 VTI 关联的接口。隧道源是虚拟隧道接口上定义的站点间 VPN 用于连接到远程终端的接口。选择可以访问远程终端的接口，例如外部接口。源接口可以是物理接口、子接口或 EtherChannel，并且必须具有名称。该接口不能是网桥虚拟接口 (BVI) 的成员。
- **IP 地址和子网掩码** - IPv4 地址和关联的子网掩码。例如，192.168.1.1/24 或 /255.255.255.0。此地址无需与隧道源接口的地址位于同一子网上。但是，如果在源接口上配置远程访问 (RA) VPN，则 VTI IP 地址不能处于为 RA VPN 配置的地址池中。

步骤 4 点击**确定 (OK)**。

允许流量通过站点间 VPN

可以使用以下方法之一来启用站点间 VPN 隧道中的流量。

- 配置 **sysopt connection permit-vpn** 命令，此命令会使匹配 VPN 连接的流量免受访问控制策略的限制。此命令的默认值是 **no sysopt connection permit-vpn**，这意味着 VPN 流量还必须获得访问控制策略的允许。

  由于外部用户无法在远程受保护网络中伪造 IP 地址，因此这是一种允许流量通过 VPN 的较为安全的方法。但它的缺点是，VPN 流量得不到检测，也就是说不会对流量应用入侵和文件保护、URL 过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映 VPN 连接。

  配置此命令的首选方法是创建远程访问 VPN 配置文件，其中您选择**为已解密的流量绕过访问控制策略**选项。如果您不想要配置 RA VPN，或您无法配置 RA VPN，则可以使用 FlexConfig 配置命令。

注释 此方法不适用于在虚拟隧道接口 (VTI) 上配置的基于路由的 VPN 连接。您必须始终为基于路由的 VPN 配置访问控制规则。

- 创建访问控制规则以允许来自远程网络的连接。此方法可确保对 VPN 流量进行检测，并将高级服务应用于连接。但它的缺点是，有可能造成外部用户伪造 IP 地址，进而获得访问　内部网络的权限。

配置全局 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

IKE 策略对象为这些协商定义 IKE 提议。您启用的对象是对等体协商 VPN 连接时使用的对象：不能为每个连接指定不同的 IKE 策略。每个对象的相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。如果协商无法找到两个对等体全都支持的策略，则不建立连接。

要定义全局 IKE 策略，需要为每个 IKE 版本选择启用哪些对象。如果预定义的对象不能满足您的要求，请创建新的策略来执行您的安全策略。

以下步骤说明如何通过“对象”(Objects) 页面配置全局策略。在编辑 VPN 连接时，您还可以点击 IKE 策略设置的**编辑**，来启用、禁用和创建策略。

注释 您最多可以启用 20 个 IKE 策略。

过程

步骤 1 从目录中选择**对象**，然后选择 **IKE 策略**。

IKEv1 和 IKEv2 的策略显示在不同列表中。

步骤 2 为每个 IKE 版本启用您希望允许的 IKE 策略。

a) 在对象表上方选择 **IKEv1** 或 **IKEv2**，以显示该版本的策略。

b) 点击**状态**开关以启用适当的对象并禁用不符合要求的对象。

如果您的一些安全要求没有反映在现有对象中，请定义新的对象以实施您的要求。有关详情，请参阅以下主题：

- 配置 IKEv1 策略，第 627 页
- 配置 IKEv2 策略，第 629 页

c) 验证相对优先级是否符合您的要求。

如果您需要更改策略的优先级，请进行编辑。如果策略为预定义的系统策略，则需要创建您自己的策略版本来更改优先级。

优先级是相对的，而非绝对的。例如，优先级 80 高于 160。如果 80 是您启用的最高优先级对象，则它将成为您的首选策略。但如果您随后启用了优先级为 25 的策略，那它将成为您的首选策略。

d) 如果同时使用两个 IKE 版本，使用另一个版本时，请重复相同的过程。

配置 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv1 策略有多个。如果哪个符合您的需求，只需点击**状态**开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在 VPN 连接中编辑 IKEv1 设置时，点击对象列表中所示的**创建新 IKE 策略**链接来创建 IKEv1 策略对象。

过程

步骤 1 从目录中选择**对象**，然后选择 **IKE 策略**。

步骤 2 选择对象表上方的 **IKEv1**，以显示 IKEv1 策略。

步骤 3 如果任何系统定义的策略符合您的要求，请点击**状态**旋钮以启用它们。

也可使用**状态**开关禁用不需要的策略。相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。

步骤 4 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 5 配置 IKEv1 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **名称** - 对象的名称，最多 128 个字符。
- **状态** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **身份验证 (Authentication)** - 在两个对等体之间使用的身份验证方法。有关详细信息，请参阅确定使用哪种身份验证方法，第 617 页。
  - **预共享密钥** - 使用在每个设备上定义的预共享密钥。在身份验证阶段，此类密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置对等体，则无法建立 IKE SA。
  - **证书 (Certificate)** - 使用对等体的设备身份证书来识别彼此。必须通过在证书颁发机构中注册每个对等体来获取这些证书。还须上传用于签署每个对等体的身份证书的受信任 CA 根证书和中间 CA 证书。对等体可以注册到相同或不同的 CA 中。对于任一对等体，都不能使用自签证书。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。有关选项的说明，请参阅决定使用哪个加密算法，第 615 页。

- **Diffie-Hellman 组 (Diffie-Hellman Group)** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。有关选项的说明，请参阅 决定要使用的 Diffie-Hellman 模数组，第 616 页。
- **散列** - 用于创建消息摘要的散列算法，以确保消息的完整性。有关选项的说明，请参阅决定使用哪些散列算法，第 615 页。
- **使用时间** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 6 点击**确定 (OK)**，保存更改。

配置 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击**状态**开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑 VPN 连接中的 IKEv2 设置时，点击对象列表中所示的**创建新 IKE 策略 (Create New IKE Policy)** 链接来创建 IKEv2 策略。

过程

步骤 1 从目录中选择**对象**，然后选择 **IKE 策略**。

步骤 2 选择对象表上方的 **IKEv2** 以显示 IKEv2 策略。

步骤 3 如果任何系统定义的策略符合您的要求，请点击**状态**旋钮以启用它们。

也可使用**状态**开关禁用不需要的策略。相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。

步骤 4 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 5 配置 IKEv2 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **名称** - 对象的名称，最多 128 个字符。
- **状态** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **加密 (Encryption)** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。选择要允许的所有算法，但不能在同一策略中同时包括混合模式 (AES-GCM) 和正常模式选项。（正常模式要求选择完整性散列，而混合模式禁止选择单独的完整性散列。) 系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪个加密算法，第 615 页。
- **Diffie-Hellman 组 (Diffie-Hellman Group)** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要允许的所有算法。系统与对等体协商，从最强到最弱组，直到达成匹配。有关选项的说明，请参阅决定要使用的 Diffie-Hellman 模数组，第 616 页。
- **完整性散列 (Integrity Hash)** - 用于创建消息摘要的散列算法的完整性部分，用于确保消息完整性。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。完整性散列不与 AES-GCM 加密选项一起使用。有关选项的说明，请参阅决定使用哪些散列算法，第 615 页。
- **伪随机函数 (PRF) 散列** - 散列算法中用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法，第 615 页。
- **使用时间** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 6 点击**确定 (OK)**，保存更改。

配置 IPsec 提议

IPsec 是设置 VPN 的最安全方法之一。IPsec 在 IP 数据包级别提供数据加密，提供一种基于标准的强大的安全解决方案。使用 IPsec，数据通过隧道在公共网络上传输。隧道是两个对等体之间安全的逻辑通信路径。进入 IPsec 隧道的流量由称为转换集的安全协议和算法组合保护。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体处相同的转换集。

根据 IKE 版本（IKEv1 或 IKEv2），存在不同的 IPsec 提议对象：

- 当创建 IKEv1 IPsec 提议时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在 VPN 中支持多个组合，请创建和选择多个 IKEv1 IPsec 提议对象。
- 当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

注释 我们建议对 IPsec 隧道使用加密和身份验证。

以下主题介绍如何为每个 IKE 版本配置 IPsec 提议。

为 IKEv1 配置 IPsec 提议

使用 IKEv1 IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

有几个预定义的 IKEv1 IPsec 提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv1 IPsec 设置时，点击对象列表中所示的**创建新 IPsec 提议**链接来创建 IKEv1 IPsec 提议对象。

过程

步骤 1 选择**对象**，然后从目录中选择 **IPsec 提议**。

步骤 2 选择对象表上方的 **IKEv1** 显示 IKEv1 IPsec 提议。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 配置 IKEv1 IPsec 提议属性。

- **名称** - 对象的名称，最多 128 个字符。
- **模式** - IPSec 隧道的运行模式。
  - **隧道**模式封装整个 IP 数据包。IPSec 报头被添加到原始 IP 报头和新的 IP 报头之间。这是默认值。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通

过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPSec。

- **传输**模式只封装 IP 数据包的上层协议。IPSec 报头被插入到 IP 报头和上层协议报头（例如 TCP）之间。传输模式要求源和目的主机都支持 IPSec，并且只有在隧道的目的对等体是 IP 数据包的最终目的时才可使用。通常只有在保护第 2 层或第 3 层隧道协议（例如 GRE、L2TP 和 DLSW）时，才会使用传输模式。

- **ESP 加密** - 此提议的封装安全协议 (ESP) 加密算法。有关选项的说明，请参阅决定使用哪个加密算法，第 615 页。
- **ESP 散列** - 要用于身份验证的散列或完整性算法。有关选项的说明，请参阅决定使用哪些散列算法，第 615 页。

步骤 5 点击**确定 (OK)**，保存更改。

为 IKEv2 配置 IPsec 提议

使用 IKEv2 IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

有几个预定义的 IKEv2 IPsec 提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv2 IPsec 设置时，点击对象列表中所示的**创建新 IPsec 提议**链接来创建 IKEv2 IPsec 提议对象。

过程

步骤 1 选择**对象**，然后从目录中选择 **IPsec 提议**。

步骤 2 选择对象表上方的 **IKEv2** 显示 IKEv2 IPsec 提议。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 配置 IKEv2 IPsec 提议属性。

- **名称** - 对象的名称，最多 128 个字符。
- **加密** - 此提议的封装安全协议 (ESP) 加密算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪个加密算法，第 615 页。

- **完整性散列 (Integrity Hash)** - 要用于身份验证的散列或完整性算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法，第 615 页。

  注释　如果选择其中一个 AES-GCM/GMAC 选项作为加密算法，则应该选择空完整性算法。即使您选择非空选项，这些加密标准也不会使用完整性散列算法。

步骤 5 点击**确定 (OK)**，保存更改。

验证站点间 VPN 连接

在配置站点间 VPN 连接并将该配置部署到设备后，请确认系统是否与远程设备建立了安全关联。

如果无法建立连接，请在设备 CLI 中使用 **ping interface** *interface_name remote_ip_address* 命令，以确保路径通过 VPN 接口连接到远程设备。如果没有连接通过配置的接口，可停用 **interface** *interface_name* 关键字并确定连接是否通过其他接口。您可能选错了用于连接的接口：必须选择面对远程设备的接口，而不是面对受保护网络的接口。

如果存在网络路径，请检查两个终端配置和支持的IKE版本和密钥，并根据需要调整VPN连接。确保没有访问控制规则或 NAT 规则会阻止连接。

过程

步骤 1 登录到设备 CLI，如登录命令行界面 (CLI)，第 7 页中所述。

步骤 2 使用 **show ipsec sa** 命令可确认是否建立了 IPsec 安全关联。

您应可看到设备（**本地地址**）与远程对等体 (**current_peer**) 之间建立了 VPN 连接。随着您通过该连接发送流量，数据包 (pkts) 计数应会而增加。访问列表应显示该连接的本地和远程网络。

例如，以下输出显示 IKEv2 连接。

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 69, #pkts encrypt: 69, #pkts digest: 69
      #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 69, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```

```
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/500, remote crypto endpt.: 192.168.4.6/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: CD22739C
      current inbound spi : 52D2F1E4

    inbound esp sas:
      spi: 0x52D2F1E4 (1389556196)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4285434/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xCD22739C (3441587100)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4055034/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

以下输出显示 IKEv1 连接。

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
      #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/0, remote crypto endpt.: 192.168.4.6/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 077D72C9
      current inbound spi : AC146DEC

    inbound esp sas:
```

```
      spi: 0xAC146DEC (2887020012)
         SA State: active
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
         slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (3914999/28567)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x000007FF
    outbound esp sas:
      spi: 0x077D72C9 (125661897)
         SA State: active
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
         slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (3914999/28567)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

步骤 3 使用 **show isakmp sa** 命令可验证 IKE 安全关联。

您可以使用不带 **sa** 关键字的命令（或改用 **stats** 关键字）查看 IKE 统计信息。

例如，以下输出显示 IKEv2 安全关联。

```
> show isakmp sa

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:15317, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local             Remote            Status   Role
592216161 192.168.2.15/500  192.168.4.6/500   READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/12 sec
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x52d2f1e4/0xcd22739c
```

以下输出显示 IKEv1 安全关联。

```
> show isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.4.6
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

```
There are no IKEv2 SAs
```

监控站点间 VPN

要对站点间 VPN 连接进行监控和故障排除，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。

- **show ipsec sa** 显示 VPN 会话（安全关联）。您可以使用 **clear ipsec sa counters** 命令重置这些统计信息。
- **show ipsec** *keyword* 显示的是 IPsec 运行数据和统计信息。输入 **show ipsec ?** 查看可用关键字。
- **show isakmp** 显示 ISAKMP 运行数据和统计信息。

站点间 VPN 示例

以下是配置站点间 VPN 的示例。

使站点间 VPN 流量豁免 NAT

当您在某个接口上定义了站点间 VPN 连接并且还对该接口实施了 NAT 规则时，可以选择使该 VPN 上的流量豁免 NAT 规则。如果 VPN 连接的远端可以处理您的内部地址，则可能要执行此操作。

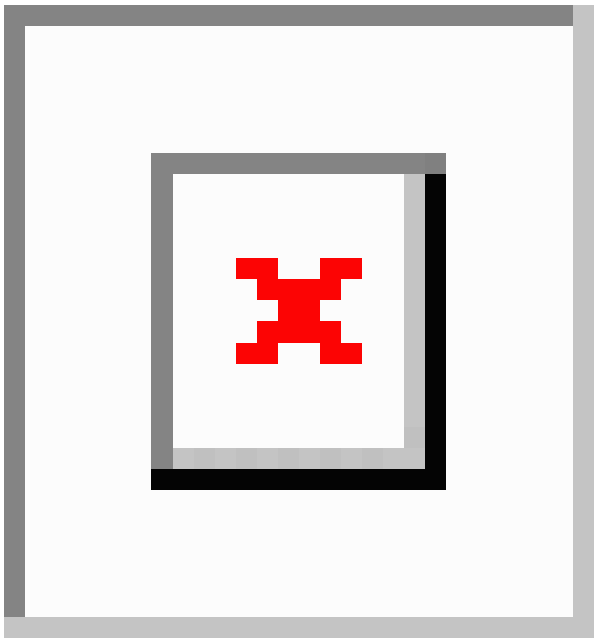
创建 VPN 连接时，可以选择 **NAT 豁免**选项自动创建 NAT 豁免规则。不过，此操作仅在通过单个路由接口（而非网桥组成员）连接本地受保护网络时才奏效。相反，如果该连接中的本地网络位于两个或多个路由接口之后或者一个或多个网桥组成员之后，则需要手动配置 NAT 豁免规则。

要使 VPN 流量豁免 NAT 规则，需要为目的是远程网络时的本地流量创建身份手动 NAT 规则。然后，将NAT应用于目的是其他网络（例如互联网）时的流量。如果本地网络有多个接口，请为每个接口分别创建规则。也可以考虑以下建议：

- 如果连接中有多个本地网络，请创建一个网络对象组用于容纳定义这些网络的对象。
- 如果 VPN 中同时包括 IPv4 和 IPv6 网络，请为其各创建一个单独的身份 NAT 规则。

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

图 *51:* 用于站点间 *VPN* 的接口 *PAT* 和身份 *NAT*



以下示例说明 Firewall1（博尔德办公室）的配置。该示例假定内部接口是网桥组，因此需要为每个成员接口编写规则。如果有一个或多个路由内部接口，其过程相同。

注释 此示例假定只包括 IPv4 网络。如果该 VPN 还包括 IPv6 网络，请为 IPv6 创建并行规则。请注意，由于无法实施 IPv6 接口 PAT，因此需要使用唯一 IPv6 地址创建主机对象用于 PAT。

过程

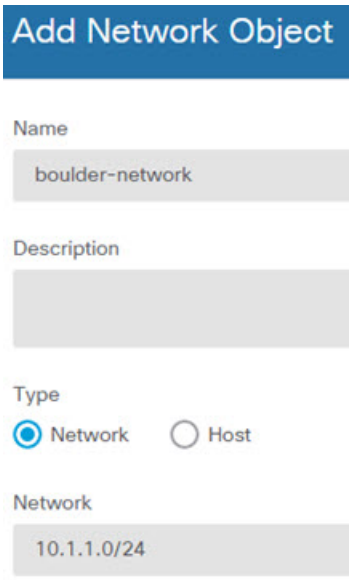
步骤 1 创建对象来定义各种网络。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 找到博尔德办公室内部网络。

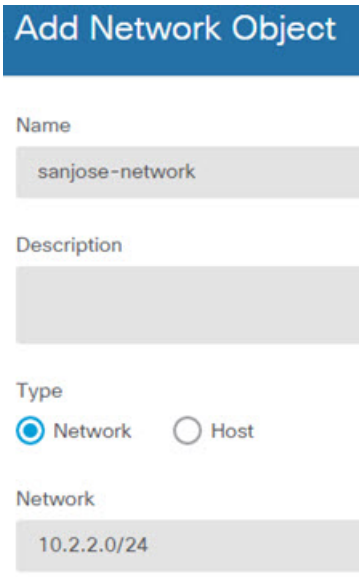
为网络对象命名（例如，boulder-network），选择**网络**，然后输入网络地址 10.1.1.0/24。



d) 点击**确定 (OK)**。

e) 点击 + 并定义内部圣荷西办公室网络。

为网络对象命名（例如，sanjose-network），选择**网络**，然后输入网络地址 10.2.2.0/24。



f) 点击**确定 (OK)**。

步骤 2 在Firewall1（博尔德办公室）上，为博尔德办公室网络配置经过VPN连接到圣荷西办公室时的手动身份 NAT。

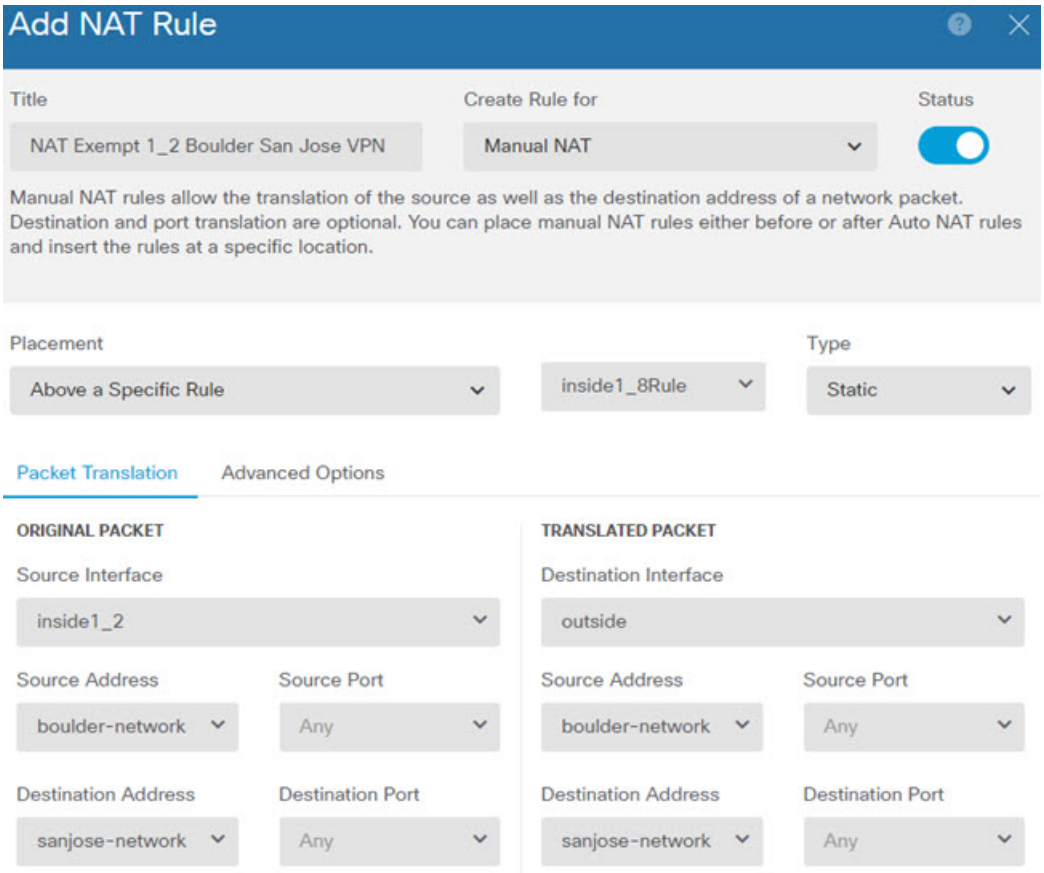
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = NAT Exempt 1_2 Boulder San Jose VPN（或您选择的其他名称）。
- **创建规则用于** = 手动 NAT。
- **位置** = **特定规则之上**，然后在“手动 NAT 在自动 NAT 之前”部分选择第一条规则。需要确保此规则在目标接口的任何常规接口 PAT 规则之前。否则，该规则可能不会应用于正确的流量。
- **类型** = 静态。
- **源接口** = inside1_2。
- **目标接口** = 外部。
- **原始源地址** = boulder-network 网络对象。
- **转换后的源地址** = boulder-network 网络对象。
- **原始目标地址** = sanjose-network 网络对象。
- **转换后的目标地址** = sanjose-network 网络对象。

  注释 由于您不需要转换目标地址，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。此规则为源和目标配置身份 NAT。



d) 在**高级**选项卡中，选择**不在目标接口上使用代理 ARP**。

e) 点击**确定 (OK)**。

f) 重复此过程，为每个其他内部接口创建相应规则。

步骤 3 在Firewall1（博尔德办公室）上，为内部博尔德办公室网络配置接入互联网时的手动动态接口 PAT。

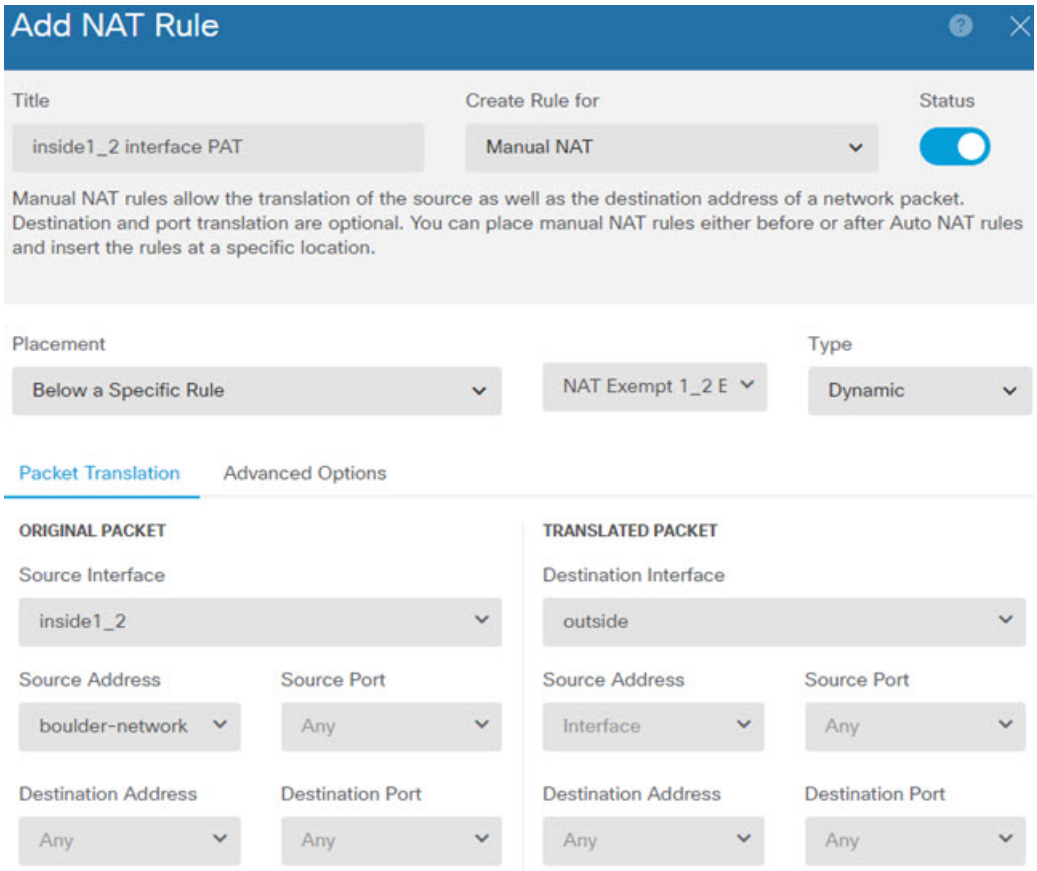
注释 内部接口可能已经配置了将所有 IPv4 流量包括在内的动态接口 PAT 规则，因为初始配置过程中会默认创建这些规则。不过，为完整起见，此处仍显示了这些配置。完成这些步骤之前，请检查是否已经存在将内部接口和网络包括在内的规则，如有则跳过此步骤。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = inside1_2 接口 PAT（或您选择的其他名称）。
- **创建规则用于** = 手动 NAT。
- **位置** = **特定规则之下**，然后在“手动 NAT 在自动 NAT 之前”部分选择您在上面为此接口创建的规则。由于此规则将应用于所有目标地址，使用 sanjose-network 作为目标的规则必须在此规则之前，否则 sanjose-network 规则永远没有匹配项。默认设置是将新的手动 NAT 规则放到“NAT 规则在自动 NAT 之前”部分的末尾，此设置也已足够。
- **类型** = 动态。

- **源接口** = inside1_2。
- **目标接口** = 外部。
- **原始源地址** = boulder-network 网络对象。
- **转换后的源地址** = **接口**。此选项配置使用目标接口的接口 PAT。
- **原始目标地址** = 任何。
- **转换后的目标地址** = 任何。



c) 点击**确定 (OK)**。

d) 重复此过程，为每个其他内部接口创建相应规则。

步骤 4 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

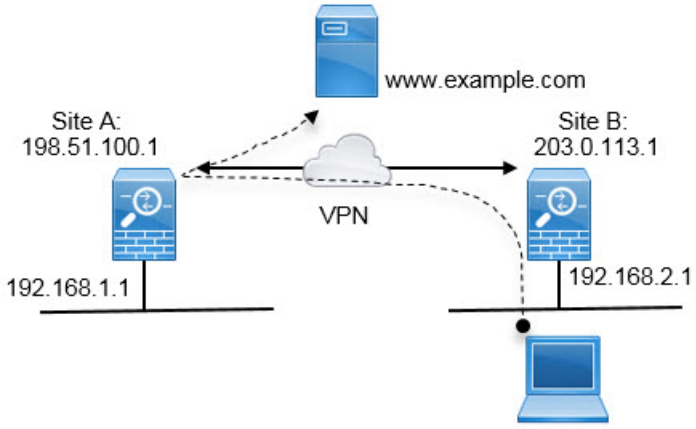
步骤 5 如果您也管理着 Firewall2（圣荷西办公室），您可以为该设备配置类似的规则。

- 当目标是 boulder-network 时，手动身份 NAT 规则将用于 sanjose-network。为 Firewall2 内部和外部网络创建新的接口对象。
- 当目标是“任何”时，手动动态接口 PAT 规则将用于 sanjose-network。

如何在外部接口上为外部站点间VPN用户提供互联网访问（发夹方法）

在站点间VPN中，您可能希望远程网络用户通过您的设备访问互联网。不过，这些远程用户进入设备所用的接口与访问互联网所用的接口（外部接口）相同，因此需要使互联网流量从外部接口退出。这种技术有时候称为发夹方法。

下图展示了一个示例。在 198.51.100.1（在主站点上，站点 A）与 203.0.113.1（远程站点，站点 B）之间配置了一个站点间 VPN 隧道。从网络内部的远程站点 192.168.2.0/24 流出的所有用户流量均通过此 VPN 隧道。因此，如果该网络上的用户想要访问互联网上的某个服务器（例如 www.example.com），连接会首先通过此 VPN 隧道，然后从 198.51.100.1 接口路由回到互联网。



以下程序介绍如何配置此服务。首先，需要配置 VPN 隧道的两个终端。

开始之前

此程序假定您使用了允许 VPN 流量的默认设置，使 VPN 流量受访问控制策略的限制。在运行配置中，这由 **no sysopt connection permit-vpn** 命令表示。如果您通过 FlexConfig或者通过在 RA VPN 连接配置文件中选择**为已解密的流量绕过访问控制策略**选项启用了 **sysopt connection permit-vpn**，则无需执行这些步骤来配置访问控制规则。

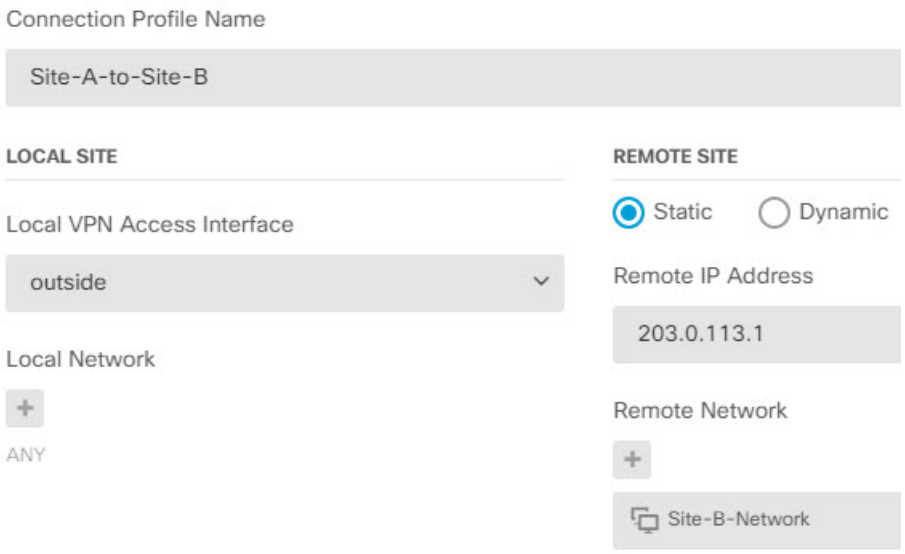
过程

步骤 1 （站点 A，主站点。）配置到远程站点 B 的站点间 VPN 连接。

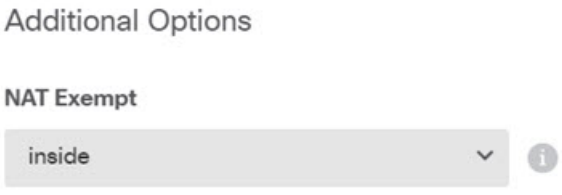
a) 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。

b) 点击 + 添加新连接。
c) 按如下所述定义终端，然后点击**下一步**：
   - **连接配置文件名称** - 为连接指定一个有意义的名称，例如 Site-A-to-Site-B。
   - **本地 VPN 接入接口** - 选择外部接口。
   - **本地网络** - 保留默认值“任何”。
   - **远程 IP 地址** - 输入远程对等体外部接口的 IP 地址。在本示例中，此地址为 203.0.113.1。
   - **远程网络** - 点击 +，然后选择定义远程对等体的受保护网络的网络对象。在本示例中，此对象为 192.168.2.0/24。可以点击**创建新网络**立即创建对象。

   下图展示了第一步操作对应的界面。



d) 定义隐私配置，然后点击**下一步**。
   - **IKE 策略** - IKE 设置对发夹方法没有影响。选择满足安全需求的 IKE 版本、策略和提议即可。请记下您输入的本地和远程预共享密钥：配置远程对等体时会用到这些信息。
   - **NAT 豁免** - 选择内部接口。



   - **完美前向保密的 Diffie-Hellman 组** - 此设置对发夹方法没有影响。可以根据需要配置此设置。

e) 点击**完成**。

连接摘要信息将会复制到剪贴板。您可以将这些信息粘贴到文本文件或其他文档，帮助您配置远程对等体。

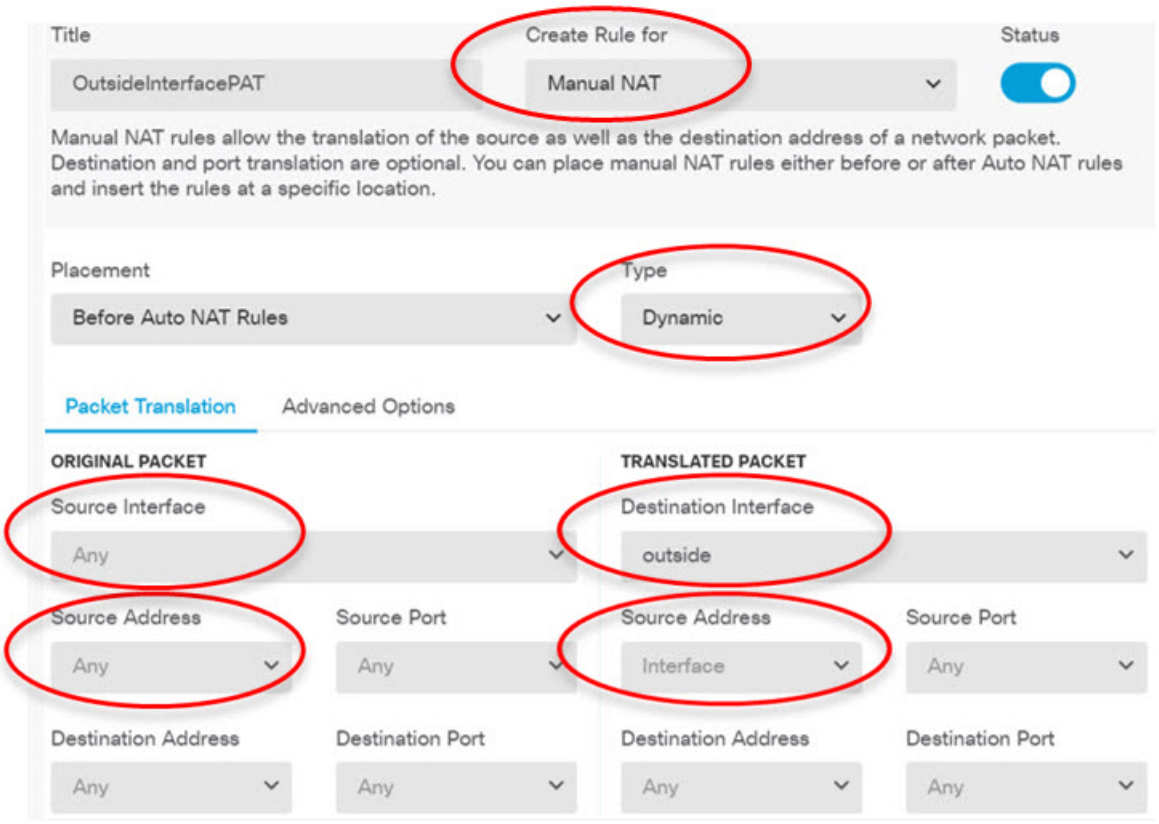
步骤 2 （站点 A，主站点。）将 NAT 规则配置为将外部接口发出的所有连接转换到外部 IP 地址上的端口（接口 PAT）。

完成初始设备配置后，系统将创建名为 InsideOutsideNatRule 的 NAT 规则。此规则将接口 PAT 应用于任意接口上通过外部接口流出设备的 IPv4 流量。由于外部接口包含在“任何”源接口中，因此，此规则已经存在，除非您对所需的规则进行编辑或将其删除。

以下程序介绍如何创建所需的规则。

a) 依次点击**策略** > **NAT**。
b) 执行以下操作之一：
   - 要编辑 InsideOutsideNatRule，请将鼠标指针悬停在**操作**列上，然后点击编辑图标 ()。
   - 要创建新规则，请点击 **+**。
c) 配置规则的以下属性：
   - **名称** - 为新规则输入一个有意义且不含空格的名称。例如，OutsideInterfacePAT。
   - **创建规则用于** - **手动 NAT**。
   - **位置** - **自动 NAT 规则之前**（默认）。
   - **类型** - **动态**。
   - **原始数据包** - 对于**源地址**，请选择“任何”或 any-ipv4。对于**源接口**，请确保选择“任何”（默认值）。对于所有其他“原始数据包”选项，请保留默认值“任何”。
   - **已转换的数据包** - 对于**目标接口**，请选择外部接口。对于**已转换的地址**，请选择**接口**。对于所有其他“已转换的数据包”选项，请保留默认值“任何”。

下图展示了选择“任何”作为源地址时的简单情况。



d) 点击**确定 (OK)**。

步骤 3 （站点 A，主站点。）配置访问控制规则，以允许访问站点 B 上的受保护网络。

仅仅创建 VPN 连接不会自动允许通过 VPN 上的流量。还需要确保您的访问控制策略允许流量通过远程网络。

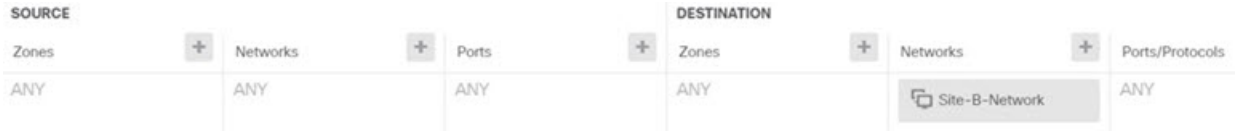
以下程序展示了如何添加远程网络专用的规则。是否需要其他规则取决于您现有的规则。

a) 依次点击**策略** > **访问控制**。

b) 点击 + 创建新规则。

c) 配置规则的以下属性：

- **顺序** - 在策略中选择一个位置，此位置应位于可能会匹配并阻止这些连接的任何其他规则之前。默认情况下，会将该规则添加到策略的末尾。如果稍后需要重新调整规则的位置，可以编辑此选项，也可以直接将规则拖放到表格中相应的位置。
- **名称** - 输入一个有意义且不含空格的名称。例如，Site-B-Network。
- **操作** - **允许**。如果不希望对此流量执行协议违规检测或入侵检测，可以选择“信任”。
- **源/目标**选项卡 - 对于**目标** > **网络**，请选择您在 VPN 连接配置文件中用于远程网络的同一对象。对于所有其他“源”和“目标”选项，请保留默认值“任何”。



- **应用**、**URL** 和**用户**选项卡 - 保留这些选项卡的默认设置，即不做任何选择。
- **入侵**、**文件**选项卡 -（可选）您可以选择入侵或文件策略，以进行威胁或恶意软件检测。
- **日志记录**选项卡 -（可选）您可以选择启用连接日志记录。

d) 点击**确定 (OK)**。

步骤 4 （站点 A，主站点。）确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。如果保持窗口打开，那么成功部署后，窗口中将指示没有待处理的更改。

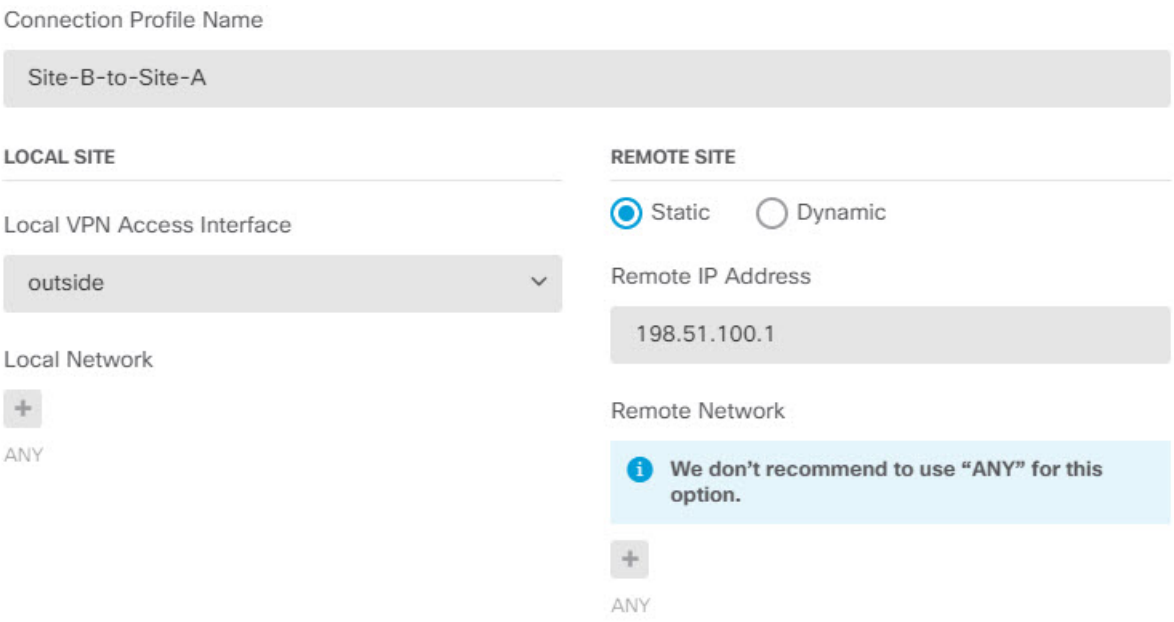
步骤 5 （站点 B，远程站点。）登录到远程站点设备，并配置到站点 A 的站点间 VPN 连接。

借助从站点 A 设备配置获取的连接摘要来配置连接的站点 B 端。

a) 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。
b) 点击 + 添加新连接。
c) 按如下所述定义终端，然后点击**下一步**：

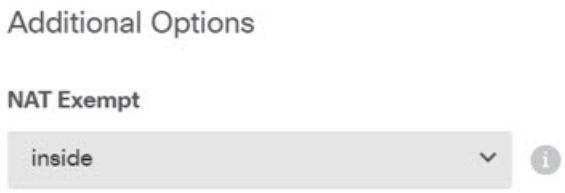
- **连接配置文件名称** - 为连接指定一个有意义的名称，例如，Site-B-to-Site-A。
- **本地 VPN 接入接口** - 选择外部接口。
- **本地网络** - 点击 +，然后选择定义本地受保护网络的网络对象。在本示例中，此对象为 192.168.2.0/24。可以点击**创建新网络**立即创建对象。
- **远程 IP 地址** - 输入主站点的外部接口的 IP 地址。在本示例中，此地址为 198.51.100.1。
- **远程网络** - 保留默认值“任何”。请忽略警告；此警告与本使用案例无关。

下图展示了第一步操作对应的界面。



d) 定义隐私配置，然后点击**下一步**。

- **IKE 策略** - IKE 设置对发夹方法没有影响。配置与 VPN 连接的站点 A 端相同或兼容的选项。必须正确配置预共享密钥：按照站点 A 设备上的配置交换本地和远程密钥（适用于 IKEv2）。对于 IKEv1，只有一个密钥，此密钥在两个对等体上必须相同。
- **NAT 豁免** - 选择内部接口。



- **完美前向保密的 Diffie-Hellman 组** - 此设置对发夹方法没有影响。匹配 VPN 连接的站点 A 端使用的设置。

e) 点击**完成**。

步骤 6 （站点 B，远程站点。）删除受保护网络的所有 NAT 规则，以便离开此站点的所有流量都必须流经 VPN 隧道。

由于站点 A 设备会执行地址转换，因此无需在此设备上执行 NAT。但还是请根据自己的具体情况具体分析。如果您有多个内部网络，而且不是所有这些网络都参与此 VPN 连接，则请勿删除这些网络所需的 NAT 规则。

a) 依次点击**策略** > **NAT**。

b) 执行以下操作之一：

- 要删除规则，请将鼠标指针悬停在“操作”列上，然后点击删除图标 ( )。

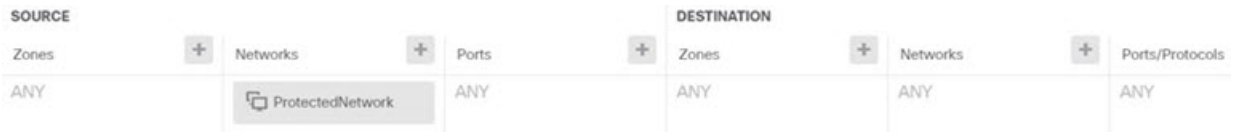
- 要编辑规则，使其不再应用于受保护的网络，请将鼠标指针悬停在“操作”列上，然后点击编辑图标 ()。

步骤 7 （站点 B，远程站点。）配置访问控制规则，以允许从受保护网络访问互联网。

以下示例允许受保护网络中的流量通过任何目标。您可以根据自己的具体要求调整此选项。也可以在此规则之前添加阻止规则，过滤掉不必要的流量。还有另外一种方法，就是在站点 A 设备上配置阻止规则。

a) 依次点击**策略** > **访问控制**。
b) 点击 + 创建新规则。
c) 配置规则的以下属性：

- **顺序** - 在策略中选择一个位置，此位置应位于可能会匹配并阻止这些连接的任何其他规则之前。默认情况下，会将该规则添加到策略的末尾。如果稍后需要重新调整规则的位置，可以编辑此选项，也可以直接将规则拖放到表格中相应的位置。
- **名称** - 输入一个有意义且不含空格的名称。例如，Protected-Network-to-Any。
- **操作** - **允许**。如果不希望对此流量执行协议违规检测或入侵检测，可以选择“信任”。
- **源/目标**选项卡 - 对于**源** > **网络**，请选择在 VPN 连接配置文件中用于本地网络的同一对象。对于所有其他“源”和“目标”选项，请保留默认值“任何”。



- **应用**、**URL** 和**用户**选项卡 - 保留这些选项卡的默认设置，即不做任何选择。
- **入侵**、**文件**选项卡 -（可选）您可以选择入侵或文件策略，以进行威胁或恶意软件检测。
- **日志记录**选项卡 -（可选）您可以选择启用连接日志记录。

d) 点击**确定 (OK)**。

步骤 8 （站点 B，远程站点。）确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮，并等待部署完成。

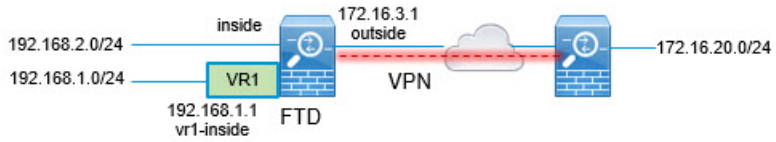
您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。如果保持窗口打开，那么成功部署后，窗口中将指示没有待处理的更改。

如何通过站点间 VPN 保护来自多个虚拟路由器的网络流量

如果在设备上配置多个虚拟路由器，则必须在全局虚拟路由器中配置站点间 VPN。不能在分配给自定义虚拟路由器的接口上配置站点间 VPN。

由于虚拟路由器的路由表是独立的，因此，如果需要通过站点间VPN来保护往返托管在自定义虚拟路由器内的网络的连接，必须创建静态路由。您还需要更新站点间VPN连接，以包括这些额外的网络。

请考虑以下示例。在这种情况下，站点间 VPN 在 172.16.3.1 的外部接口上定义。此 VPN 可以包括内部网络 192.168.2.0/24，而无需进行额外配置，因为内部接口也是全局虚拟路由器的一部分。但是，如果您需要为 192.168.1.0/24 网络（其为 VR1 虚拟路由器的一部分）提供站点间 VPN 服务，则必须配置双向静态路由，并将网络添加到站点间 VPN 配置中。



开始之前

此示例假设您已在本地网络 192.168.2.0/24 与外部网络 172.16.20.0/24 之间配置站点间 VPN，定义虚拟路由器，配置接口并将其分配给相应的虚拟路由器。

过程

步骤 1 配置从全局虚拟路由器到 VR1 的路由泄漏。

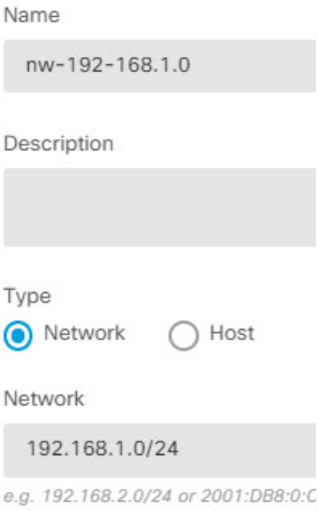
此路由允许受站点间 VPN 的外部（远程）终端保护的终端访问 VR1 虚拟路由器中的 192.168.1.0/24 网络。

a) 依次选择**设备** > **路由** > **查看配置**。

b) 点击全局虚拟路由器的查看图标 ( )。

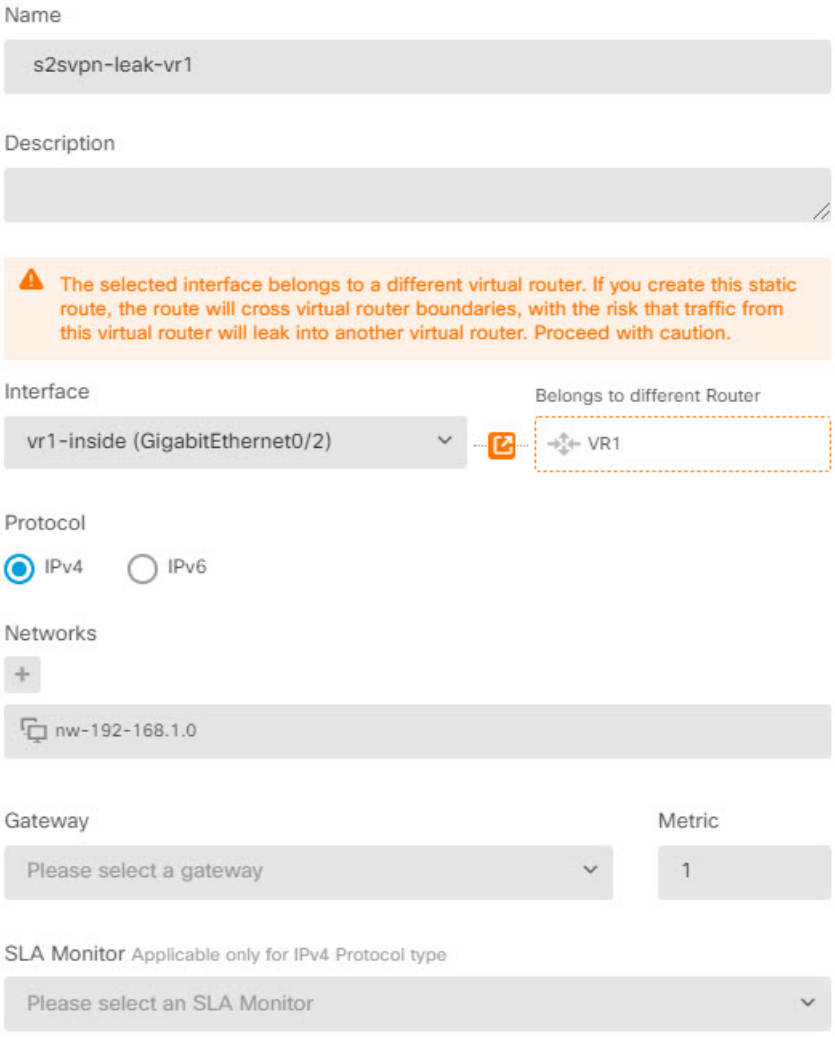
c) 在全局路由器的**静态路由**选项卡上，点击 **+** 并配置路由：

- **名称** - 可以使用任何名称，例如 **s2svpn-leak-vr1**。
- **接口** - 选择 **vr1-inside**。
- **协议** - 选择 **IPv4**。
- **网络** - 选择定义 192.168.1.0/24 网络的对象。如有需要，请点击**创建新网络**立即创建对象。



- **网关** - 将此项目留空。将路由泄漏到另一个虚拟路由器时，您不必选择网关地址。

对话框应如下所示：



d) 点击**确定**。

步骤 2 配置从 VR1 到全局虚拟路由器的路由泄漏。

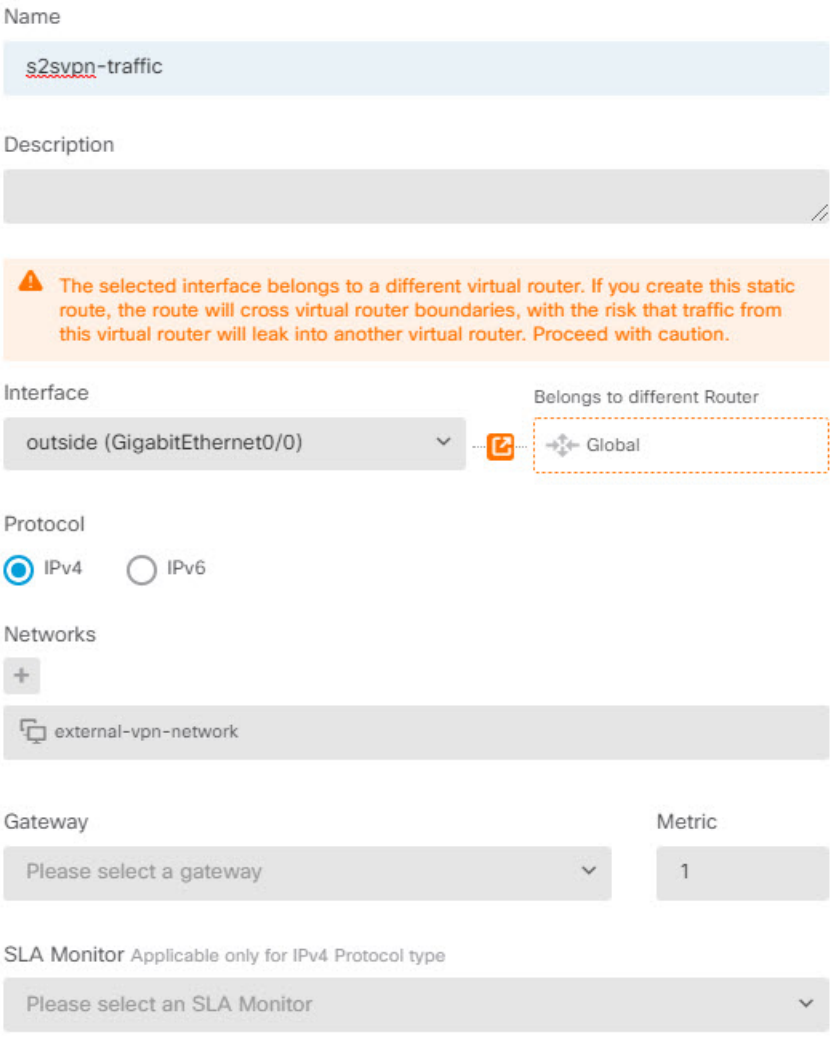
此路由允许 192.168.1.0/24 网络上的终端发起流经站点间 VPN 隧道的连接。在本示例中，远程终端正在保护 172.16.20.0/24 网络。

a) 从虚拟路由器下拉列表中选择 **VR1**，以切换至 VR1 配置。

b) 在 VR1 虚拟路由器的**静态路由**选项卡上，点击 **+** 并配置路由：

- **名称** - 可以使用任何名称，例如 **s2svpn-traffic**。
- **接口** - 选择 **outside**。
- **协议** - 选择 **IPv4**。
- **网络** - 选择为远程终端的受保护网络创建的对象，例如 **external-vpn-network**。
- **网关** - 将此项目留空。将路由泄漏到另一个虚拟路由器时，您不必选择网关地址。

对话框应如下所示：



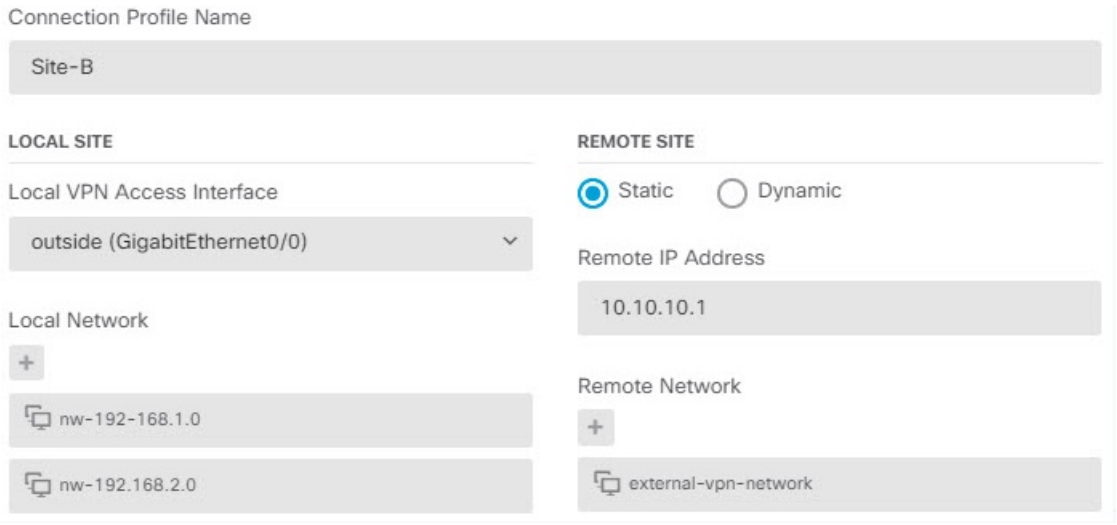
c) 点击**确定**。

步骤 3 将 192.168.1.0/24 网络添加到站点间 VPN 连接配置文件中。

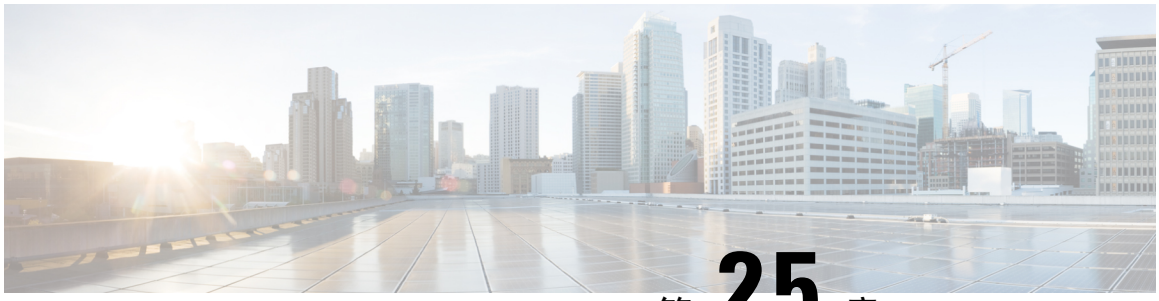
a) 依次选择**设备** > **站点间 VPN** > **查看配置**。

b) 点击连接配置文件的编辑图标 ( )。

c) 在向导的第一页上，点击**本地网络**下的 +，然后为 192.168.1.0/24 网络添加对象。


Connection Profile Name
Site-B
LOCAL SITE
Local VPN Access Interface
outside (GigabitEthernet0/0)
Local Network
nw-192-168.1.0
nw-192.168.2.0
REMOTE SITE
Static
Dynamic
Remote IP Address
10.10.10.1
Remote Network
external-vpn-network

d) 完成向导。



第 25 章

远程访问 VPN

远程访问虚拟专用网络 (VPN) 允许个人用户使用连接到互联网的计算机或其他受支持的 iOS 或 Android 设备，从远程位置连接到您的网络。这样，移动员工就可以从家庭网络或公共 Wi-Fi 网络进行连接。

以下主题介绍如何为您的网络配置远程访问 VPN。

远程访问 VPN 概述

您可以使用 设备管理器，配置通过 SSL 借助 Secure Client 软件实现的远程访问 VPN。

Secure Client 与 威胁防御 设备协商 SSL VPN 连接时，会使用传输层安全 (TLS) 或数据报传输层安全 (DTLS) 进行连接。DTLS 可避免与某些 SSL 连接关联的延迟和带宽问题，并可提高对于数据包延迟敏感的实时应用的性能。客户端与 威胁防御 设备协商要使用的 TLS/DTLS 版本。如果客户端支持 DTLS，则使用 DTLS。

各设备型号的最大并发 VPN 会话数量

根据设备型号，设备上允许的并发远程访问 VPN 会话数量有最大值限制。此限制用于确保系统性能不会降低到不可接受的水平。请使用这些限制进行容量规划。

设备型号	最大并发远程访问 VPN 会话数
Firepower 1010	75
Firepower 1120	150

设备型号	最大并发远程访问 VPN 会话数
Firepower 1140	400
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
Secure Firewall 3110	3000
Secure Firewall 3120	6000
Secure Firewall 3130	15,000
Secure Firewall 3140	20,000
Firepower 4100 系列，所有型号	10,000
Firepower 9300 设备，所有型号	20,000
Threat Defense Virtual：FTDv5	50
Threat Defense Virtual： FTDv10、FTDv20、FTDv30	250
Threat Defense Virtual：FTDv50	750
Threat Defense Virtual：FTDv100	10,000
ISA 3000	25

下载 Secure Client 软件

在配置远程访问 VPN 之前，必须将 Secure Client 软件下载到您的工作站。定义 VPN 时，您需要上传这些软件包。

您应该下载最新的 Secure Client 版本，以确保获得最新的功能、漏洞修复和安全补丁。请定期更新威胁防御设备上的软件包。

注释 可以为以下每个操作系统上传一个 Secure Client 软件包：Windows、Mac 和 Linux。无法为特定操作系统类型上传多个版本。

从 software.cisco.com 获取 Secure Client 软件包。您需要下载客户端的“完全安装软件包”版本。

用户如何安装 Secure Client 软件

要完成 VPN 连接，您的用户必须安装 Secure Client 软件。可以使用现有的软件分发方法直接安装该软件。或者，可以让用户直接从威胁防御设备安装 Secure Client 。

用户必须对其工作站具有管理员权限才能安装软件。

安装 Secure Client 后，如果您将新的 Secure Client 版本上传到系统，Secure Client 将在用户进行下一个VPN连接时检测到新版本。系统将自动提示用户下载并安装更新的客户端软件。这种自动化可为您和您的客户端简化软件分发。

如果您决定让用户一开始从 威胁防御设备安装软件，请告诉用户执行以下步骤。

注释 Android 和 iOS 用户应从相应的应用商店下载 Secure Client。

过程

步骤 1 使用 Web 浏览器，打开 **https://***ravpn-address*，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。

您在配置远程访问 VPN 时确定此接口。系统提示用户登录。

如果更改了远程访问 VPN 连接的端口，则用户必须在 URL 中包含该自定义端口。例如，如果将端口更改为 4443，则 URL 应为 https://ravpn.example.com:4443

步骤 2 登录到网站。

用户使用为远程访问 VPN 配置的目录服务器进行身份验证。登录成功后可继续操作。

如果登录成功，系统将确定用户是否已具有所需的 Secure Client版本。如果用户的计算机上没有 Secure Client ，或者客户端的版本较低，系统将自动开始安装 Secure Client 软件。

安装后，Secure Client 会完成远程访问 VPN 连接。

使用 RADIUS 和组策略控制用户权限和属性

您可以将用户授权属性（也称为用户权利或权限）应用于来自外部 RADIUS 服务器或 威胁防御设备上定义的组策略的 RA VPN 连接。如果 威胁防御 设备从与组策略上配置的属性冲突的外部 AAA 服务器接收属性，则来自 AAA 服务器的属性始终优先。

威胁防御设备按照以下顺序应用属性：

1. 外部 AAA 服务器上的用户属性 - 该服务器在用户身份验证或授权成功后返回这些属性。

2. 在 威胁防御设备上配置的组策略 - 如果 RADIUS 服务器为用户返回 RADIUS CLASS 属性 IETF-Class-25 (OU=group-policy) 值，威胁防御设备会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。
3. 连接配置文件分配的组策略 - 连接配置文件包含该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。连接至 威胁防御设备的所有用户最初都属于此组，这可以提供 AAA 服务器返回的用户属性或分配给用户的组策略中缺失的所有属性。

威胁防御设备支持供应商 ID 为 3076 的 RADIUS 属性。如果使用的 RADIUS 服务器没有定义这些属性，您必须手动定义它们。要定义属性，请使用属性名称或编号、类型、值和供应商代码 (3076)。

以下主题根据属性值是在 RADIUS 服务器中定义的还是由系统发送到 RADIUS 服务器的来介绍受支持的属性。

发送到 RADIUS 服务器的属性

RADIUS 属性 146 和 150 由 威胁防御 发送到 RADIUS 服务器，用于身份验证请求和授权请求。以下所有属性都是由 威胁防御设备发送到 RADIUS 服务器，用于记账开始请求、临时更新请求和停止请求。

表 *14:* 发送到 *RADIUS* 的属性 威胁防御

属性	属性编号	语法、类型	单值或多值	说明或值
客户端类型	150	整数	单值	连接到 VPN 的客户端类型： 2 = Secure Client SSL VPN
会话类型	151	整数	单值	连接类型： 1 = Secure Client SSL VPN
隧道组名称	146	字符串	单值	用于建立会话的连接配置文件名称，如 威胁防御设备上的定义。此名称可以包含 1-253 个字符。

从 RADIUS 服务器接收的属性

以下用户授权属性由 RADIUS 服务器发送到 威胁防御设备。

表 *15:* 发送到 威胁防御 的 *RADIUS* 属性

属性	属性编号	语法、类型	单值或多值	说明或值
Access-List-Inbound	86	字符串	单值	这两个访问列表属性都使用 威胁防御 设备上配置的 ACL 名称。使用 Smart CLI 扩展访问列表对象类型创建 ACL（依次选择**设备** > **高级配置** > **Smart CLI** > **对象**）。 此类 ACL 用于控制入站流量（流量进入 威胁防御设备）或出站流量（流量离开 威胁防御 设备）。
Access-List-Outbound	87	字符串	单值	

属性	属性编号	语法、类型	单值或多值	说明或值
Address-Pools	217	字符串	单值	威胁防御 设备上定义的网络对象名称，用于识别将作为地址池供客户端连接 RA VPN 时使用的子网。在**对象 (Objects)** 页面上定义网络对象。
Banner1	15	字符串	单值	用户登录时显示的横幅。
Banner2	36	字符串	单值	用户登录时显示的横幅的第二部分。横幅 2 附加到横幅 1。
Group-Policy	25	字符串	单值	要在连接中使用的组策略。必须在 RA VPN **组策略 (Group Policy)** 页面上创建组策略。您可以使用以下其中一种格式： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称；
Simultaneous-Logins	2	整数	单值	允许用户建立的独立并发连接的数量，0 - 2147483647。
VLAN	140	整数	单值	限制用户连接的 VLAN，0 - 4094。还必须在 威胁防御设备的子接口上配置此 VLAN。

双因素身份验证

可以为RA VPN配置双因素身份验证。配置了双因素身份验证时，用户必须提供用户名、静态密码，以及一个额外项，如RSA 令牌或Duo密码等。双因素身份验证不同于使用第二个身份验证源，双因素是在单个身份验证源中配置的，其与 RSA/Duo 服务器的关系绑定到主身份验证源。例外情况是 Duo LDAP，它将“Duo LDAP 服务器”配置为辅助身份验证源。

在双因素身份验证过程中，第一个因素是 RADIUS 或 AD 服务器，与之配合使用的第二个因素是推送到移动设备的 RSA 令牌和 Duo 密码，正是使用此令牌和密码来检测系统，

RSA 双因素身份验证

可以使用以下方法之一配置 RSA。有关 RSA 端配置的信息，请参阅 RSA 文档。

- 直接在 设备管理器 中将 RSA 服务器定义为 RADIUS 服务器，并将此服务器用作 RA VPN 中的主身份验证源。

  使用此方法时，用户必须使用 RSA RADIUS 服务器上配置的用户名进行身份验证，并使用一次性临时 RSA 令牌连接密码，用逗号分隔密码和令牌：密码,令牌。

  在此配置中，通常会使用单独的 RADIUS 服务器 （例如，Cisco ISE 提供的 RADIUS 服务器) 提供授权服务。将第二个 RADIUS 服务器配置为授权、配置或记账服务器。

- 将 RSA 服务器与支持直接集成的 RADIUS 或 AD 服务器集成，并配置 RA VPN，将非 RSA RADIUS 或 AD 服务器用作主要身份验证源。在这种情况下，RADIUS/AD 服务器使用 RSA-SDI 在客户端和 RSA 服务器之间代理和安排双因素身份验证。

  使用此方法时，用户必须使用非 RSA RADIUS 或 AD 服务器上配置的用户名进行身份验证，并使用一次性临时 RSA 令牌连接密码，用逗号分隔密码和令牌：密码,令牌。

  在此配置中，也会将第二个非 RSA RADIUS 服务器用作授权和记账（可选）服务器。

使用 RADIUS 的 Duo 双因素身份验证

可以将 Duo RADIUS 服务器配置为主要身份验证源。此方法使用 Duo RADIUS 身份验证代理。

有关配置 Duo 的详细步骤，请参阅 https://duo.com/docs/cisco-firepower。

然后，配置 Duo，以转发定向到代理服务器的身份验证请求，并将另一台 RADIUS 服务器或 AD 服务器用作第一个身份验证因素，将 Duo 云服务用作第二个因素。

使用此方法时，用户必须使用 Duo 身份验证代理和关联的 RADIUS/AD 服务器上配置的用户名，以及 RADIUS/AD 服务器中配置的用户名对应的密码进行身份验证，其后紧随以下其中一个 Duo 代码：

- *Duo-passcode*。例如，*my-password*,**12345**。
- **push**。例如，*my-password*,**push**。使用 **push** 告知 Duo 向用户应该已经安装并注册的 Duo 移动应用发送推送身份验证。
- **sms**。例如，*my-password*,**sms**。使用 **sms** 告知 Duo 向用户的移动设备发送包含新一批密码的 SMS 消息。使用 **sms** 时，用户的身份验证尝试将会失败。用户必须重新进行身份验证，并输入新密码作为辅助因素。
- **phone**。例如，*my-password*,**phone**。使用 **phone** 告知 Duo 执行电话回叫身份验证。

如果用户名/密码已经过验证，Duo 身份验证代理会联系 Duo 云服务，后者将核实该请求是来自有效配置的代理设备，然后按照指示将临时密码推送到用户的移动设备。当用户接受此密码时，Duo 会将会话标记为已验证，同时 RA VPN 成功创建。

使用 LDAP 的 Duo 双因素身份验证

可以将 Duo LDAP 服务器作为辅助身份验证源与作为主要源的 Microsoft Active Directory (AD) 或 RADIUS 服务器结合使用。使用 Duo LDAP 时，辅助身份验证使用 Duo 密码、推送通知或电话呼叫验证主要身份验证。

威胁防御设备使用通过端口 TCP/636 的 LDAPS 与 Duo LDAP 通信。

请注意，Duo LDAP 服务器仅提供身份验证服务，不提供身份服务。因此，如果将 Duo LDAP 作为主要身份验证源，则在任何控制面板中都将看不到与 RA VPN 连接关联的用户名，且将无法为这些用户编写访问控制规则。

使用此方法时，用户必须使用 RADIUS/AD 服务器和 Duo LDAP 服务器上配置的用户名进行身份验证。系统提示通过 Secure Client 登录时，用户应在主**密码**字段中提供 RADIUS/AD 密码，对于**辅助密码**，可以提供以下选项之一来使用 Duo 进行身份验证。有关详细信息，请参阅 https://guide.duo.com/anyconnect。

- *Duo* 密码 - 使用密码进行身份验证，密码将由 Duo Mobile 生成、通过 SMS 发送、由硬件令牌生成或由管理员提供。例如，1234567。
- **推送** - 如果已安装并激活 Duo Mobile 应用，请将登录请求推送至您的手机。查看请求并点击**批准**以登录。
- **电话** - 使用电话呼叫进行身份验证。
- **短信** - 以短信消息请求 Duo 密码。登录尝试失败。使用新密码重新登录。

有关使用 Duo LDAP 的详细说明和示例，请参阅如何使用 Duo LDAP 配置双因素身份验证，第 691 页。

远程访问 VPN 的许可要求

您的基本设备许可证必须满足出口要求，您才能配置远程访问 VPN。注册设备时，必须使用启用了出口控制功能的智能软件管理器账户。您也不能使用评估许可证配置该功能。

此外，您需要购买并启用远程访问 VPN 许可证，请选择以下任一项：Secure Client Advantage、Secure Client Premier 或 仅限 Secure Client VPN。即使这些许可证被设计为在与基于 ASA 软件的头端一起使用时允许不同的功能集，它们对于 威胁防御 设备都同等处理。

要启用许可证，请依次选择**设备** > **智能许可证** > **查看配置**，然后在远程访问 RA VPN 许可证组中选择正确的许可证。您需要在智能软件管理器账户中提供许可证。有关启用许可证的详细信息，请参阅启用或禁用可选许可证，第 87 页。

有关详细信息，请参阅《思科 *AnyConnect* 订购指南》http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf。另外，http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/datasheet-listing.html 中还提供了其他数据表。

远程访问 VPN 的准则和限制

配置 RA VPN 时，请时刻注意以下准则和限制。

- 对于同一个 TCP 端口，无法在同一接口上同时配置 设备管理器 访问（管理访问列表中的 HTTPS 访问）和远程访问 SSL VPN。例如，如果在外部接口上配置远程访问 SSL VPN，则也无法在端口 443 上打开 HTTPS 连接的外部接口。如果在同一接口上配置这两个功能，请确保至少更改其中一项服务的 HTTPS 端口，以避免冲突。
- RA VPN 外部接口是全局设置。不能在不同的接口上配置不同的连接配置文件。
- 无法在 NAT 规则的源地址和远程访问 VPN 地址池中使用重叠地址。
- 如果您使用 RADIUS 和 RSA 令牌配置双因素身份验证，则在大多数情况下，12 秒的默认身份验证超时太短，无法实现成功的身份验证。您可以通过创建自定义 Secure Client 配置文件并将其应用到 RA VPN 连接配置文件，来增加身份验证超时值，如 配置并上传客户端配置文件，第 663 页中所述。建议身份验证超时时间最短为 60 秒，以便用户有足够的时间进行身份验证并粘贴 RSA 令牌，以及进行令牌往返验证。

- 不直接支持对 RA VPN 前端发出命令（例如 **curl** ），并且可能不会产生所需的结果。例如，前端不响应 HTTP HEAD 请求。

配置远程访问 VPN

要为客户端启用远程访问 VPN，需要配置许多单独的项目。以下步骤程序介绍了端到端流程。

过程

步骤 1 配置许可证。

需要启用两个许可证：

- 注册设备时，必须使用启用了出口控制功能的智能软件管理器账户。基本许可证必须符合出口控制要求，然后才能配置远程访问 VPN。您也不能使用评估许可证配置该功能。有关注册设备的步骤程序，请参阅注册设备，第 85 页。
- 远程访问 VPN 许可证。有关详细信息，请参阅远程访问 VPN 的许可要求，第 661 页。要启用该许可证，请参阅启用或禁用可选许可证，第 87 页。

步骤 2 配置证书。

对客户端与设备之间的 SSL 连接进行身份验证需要使用证书。您可以将预定义的 DefaultInternalCertificate 用于 VPN，也可以自行创建证书。

如果对用于身份验证的目录领域使用加密连接，则必须上传受信任的 CA 证书。

有关证书及其上传方法的详细信息，请参阅配置证书，第 144 页。

步骤 3 （可选。）配置 TLS/SSL 设置。

默认情况下，系统将允许远程用户使用系统支持的任何 TLS 版本和加密密码连接到远程访问 VPN。但是，您可以限制允许使用的 TLS/DTLS 版本、密码和 Diffie-Hellman 组以执行更安全的连接。请参阅配置 TLS/SSL 密码设置，第 761 页。

步骤 4 （可选。）配置并上传客户端配置文件，第 663 页。

步骤 5 配置用于对远程用户进行身份验证的身份源。

您可以对允许登录远程访问 VPN 的用户账户使用以下源。或者，可以使用客户端证书进行身份验证，可单独使用，也可与身份源配合使用。

- Active Directory 身份领域 - 作为主要身份验证源。在 Active Directory AD 服务器中定义用户账户。请参阅配置 AD 身份领域，第 155 页。
- RADIUS 服务器组 - 充当主要或辅助身份验证源，并用于授权和记账。请参阅配置 RADIUS 服务器组，第 160 页。

- LocalIdentitySource（本地用户数据库）- 作为主要或回退源。您可以直接在设备上定义用户，不使用外部服务器。如果您使用本地数据库作为回退源，请确保您定义与外部服务器中定义的相同用户名/密码。请参阅配置本地用户，第 168 页。
- Duo LDAP 服务器 - 作为主要或辅助身份验证源。虽然您可以使用 Duo LDAP 服务器作为主要源，但这并不是常规配置。通常将其用作辅助源以便与主 Active Directory 或 RADIUS 服务器结合提供双因素身份验证。有关详细信息，请参阅如何使用 Duo LDAP 配置双因素身份验证，第 691 页。

步骤 6 （可选。）为 RA VPN 配置组策略，第 675 页

组策略定义用户相关的属性。可以配置组策略，根据组成员身份提供差异化的资源访问权限。或者，可以对所有连接使用默认策略。

步骤 7 配置 RA VPN 连接配置文件，第 668 页。

步骤 8 允许流量通过远程访问 VPN，第 666 页。

步骤 9 验证远程访问 VPN 配置，第 666 页。

如果在完成连接时遇到问题，请参阅远程访问 VPN 故障排除，第 681 页。

步骤 10 （可选。）启用身份策略并配置被动身份验证规则。

如果启用被动用户验证，通过远程访问VPN登录的用户将显示在控制面板上，他们也可以用作策略中的流量匹配条件。如果不启用被动身份验证，只有当远程访问 VPN 用户匹配主动身份验证策略时，这些用户才可用。必须启用身份策略以在控制面板中获取任何用户名信息，或将其用于流量匹配。

配置并上传客户端配置文件

Secure Client 配置文件随 Secure Client 软件一起下载到客户端。这些配置文件定义与客户端相关的诸多选项，例如启动时自动连接和自动重新连接，以及是否允许最终用户更改 Secure Client 首选项和高级设置中的选项。

如果在配置远程访问 VPN 连接时为外部接口配置完全限定主机名 (FQDN)，系统将为您创建一个客户端配置文件。此配置文件启用默认设置。只有在需要非默认行为时，才需要创建和上传客户端配置文件。请注意，客户端配置文件是可选的：如果您不上传， Secure Client 将对所有配置文件控制选项使用默认设置。

注释 必须将 威胁防御 设备的外部接口添加到 VPN 配置文件的服务器列表中，以便 Secure Client 在第一次连接时显示所有用户可控的设置。如果您不将地址或 FQDN 添加为配置文件中的主机条目，则系统不会向会话应用过滤器。例如，如果您创建了一个证书匹配，且证书与条件正确匹配，但您未将设备添加为该配置文件中的主机条目，那么证书匹配将被忽略。

您可以为 Secure Client 以及可以选择性地与 Secure Client 一起使用的各种模块（例如 AMP 启用程序）创建配置文件。虽然您可以为任何这些模块上传配置文件，但 设备管理器 仅支持创建 Secure Client 配置文件。但是，您可以通过 设备管理器上传任何类型的配置文件，然后使用 威胁防御 API（来自 API Explorer）更改对象的配置文件类型。配置文件页面显示所有类型的所有配置文件，但列表不指示配置文件类型。以下程序说明如何完成此任务。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。另外，您还可以在编辑配置文件属性时，点击对象列表中所示的**创建新的 Secure Client 配置文件 (Create New Secure Client Profile)** 链接来创建 Secure Client 配置文件对象。

开始之前

在上传客户端配置文件之前，必须先执行以下操作。

- 下载并安装独立版 Secure Client“配置文件编辑器 - Windows/独立版安装程序 (MSI)”。此安装文件仅适用于 Windows，文件名为 anyconnect-profileeditor-win-<version>-k9.msi，其中 <version> 是 Secure Client 版本（文件名可能会有所不同）。例如，anyconnect-profileeditor-win-4.3.04027-k9.msi。您还必须在安装配置文件编辑器之前安装 Java JRE 1.6（或更高版本）。从 software.cisco.com 获取 Secure Client 配置文件编辑器。请注意，此软件包包含所有配置文件编辑器，而不只是 VPN 客户端的一个配置文件编辑器。
- 使用配置文件编辑器创建所需的配置文件。您应在配置文件中指定外部接口的主机名或 IP 地址。有关详细信息，请参阅编辑器的在线帮助。

过程

步骤 1 选择**对象**，然后从目录中选择**Secure Client 配置文件 (Secure Client Profiles)**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。
- 要下载与对象关联的配置文件，请点击对象的下载图标 ( )。

要删除未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 为对象输入名称和（可选）说明。

如果要上传模块配置文件，请使用对象名称指示模块类型，以便更轻松地将其与 Secure Client 配置文件区分开来。

步骤 4 点击**上传**并选择使用配置文件编辑器创建的文件。

步骤 5 点击**打开**上传配置文件。

步骤 6 点击**确定**添加对象。

步骤 7 如果您创建的配置文件实际上是与 Secure Client 配置文件不同的类型，请完成以下步骤来更改对象的配置文件类型。

a) 点击“更多选项”按钮 (⋮) 并选择 **API Explorer**。

系统会在单独的选项卡或窗口中打开 API Explorer，具体取决于您的浏览器设置。

b) 打开 AnyConnectClientProfile 资源。

c) 选择 GET /object/anyconnectclientprofiles 方法，然后点击**试用！**按钮。

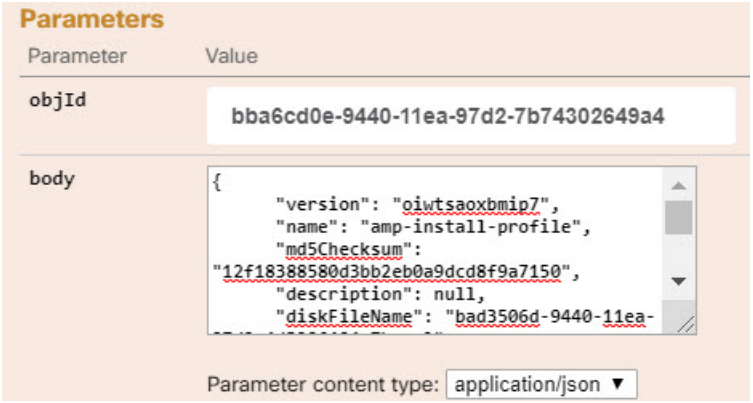
每个配置文件对象将如下所示。突出显示的属性是您需要更改的属性。

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile",
      "links": {
        "self": "https://10.89.5.38/api/fdm/v6/object/
anyconnectclientprofiles/bba6cd0e-9440-11ea-97d2-7b74302649a4"
      }
```

d) 在输出中找到您的对象，选择代码，按住 Ctrl 的同时点击将其复制到剪贴板。

e) 选择 PUT /object/anyconnectclientprofiles/{objId} 方法，并将内容粘贴到**正文**字段中。

f) 复制 **id** 值并将其粘贴到正文上方的 **objId** 编辑框中。您还可以在 “self” URL 的末尾找到对象 ID。



g) 在对象正文中，找到 **anyConnectModuleType** 字段，并将该值替换为您的配置文件类型的值。从 DART、FEEDBACK、WEB_SECURITY、ANY_CONNECT_CLIENT_PROFILE、AMP_ENABLER、NETWORK_ACCESS_MANAGER、NETWORK_VISIBILITY、START_BEFORE_LOGIN、ISE_POSTURE、UMBRELLA 中进行选择。

h) 再次在**正文**中，删除**链接**属性，在**类型**值后面添加逗号。

此对象正文应如下所示：

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
```

```
"diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
"anyConnectModuleType": "AMP_ENABLER",
"id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
"type": "anyconnectclientprofile"
}
```


i) 点击**试用！**按钮检查响应以验证对象是否已正确修改。您应获得响应代码200和回应更改的响应正文。您可以使用 GET 方法进一步验证结果。

允许流量通过远程访问 VPN

可以使用以下方法之一来启用远程访问 VPN 隧道中的流量。

- 配置 **sysopt connection permit-vpn** 命令，此命令会使匹配 VPN 连接的流量免受访问控制策略的限制。此命令的默认值是 **no sysopt connection permit-vpn**，这意味着 VPN 流量还必须获得访问控制策略的允许。

  外部用户无法在远程访问 VPN 地址池中伪造 IP 地址，因此这种允许 VPN 流量的方法较为安全。但它的缺点是，VPN流量得不到检测，也就是说不会对流量应用入侵和文件保护、URL过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映 VPN 连接。

  要配置此命令，请在 RA VPN 连接配置文件中选择**为已解密的流量绕过访问控制策略**选项。

- 创建访问控制规则以允许来自远程访问 VPN 地址池的连接。此方法可确保对 VPN 流量进行检测，并将高级服务应用于连接。但它的缺点是，有可能造成外部用户伪造IP地址，进而获得访问　内部网络的权限。

验证远程访问 VPN 配置

在配置远程访问 VPN 并将该配置部署到设备后，请确认是否可以进行远程连接。

如果遇到问题，请阅读故障排除主题以帮助查明和更正问题。请参阅远程访问 VPN 故障排除，第 681 页。

过程

步骤 1 在外部网络中，使用 Secure Client建立 VPN 连接。

使用 Web 浏览器，打开 **https://***ravpn-address*，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。如有必要，安装客户端软件并完成连接。请参阅用户如何安装 Secure Client 软件，第 657 页。

如果更改了远程访问 VPN 连接的端口，则必须在 URL 中包含该自定义端口。例如，如果将端口更改为 4443，则 URL 应为 https://ravpn.example.com:4443

如果配置了组 URL，也可尝试这些 URL。

步骤 2 登录到设备 CLI，如登录命令行界面 (CLI)，第 7 页中所述。 或者，打开 CLI 控制台。

步骤 3 使用 **show vpn-sessiondb** 命令查看有关当前 VPN 会话的摘要信息。

统计信息应显示您的活动 Secure Client 会话以及有关累积会话、峰值并发会话数量和非活动会话的信息。以下是该命令的输出示例。

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ----------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
--------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     50
Device Total VPN Capacity   :  10000
Device Load                 :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
Clientless                  :      0 :          1 :               1
AnyConnect-Parent           :      1 :         49 :               3
SSL-Tunnel                  :      1 :         46 :               3
DTLS-Tunnel                 :      1 :         46 :               3
--------------------------------------------------------------------------------
Totals                      :      3 :        142
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
IPv6 Usage Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
AnyConnect SSL/TLS/DTLS     :        :           :
  Tunneled IPv6             :      1 :         20 :           2
--------------------------------------------------------------------------------
```

步骤 4 使用 **show vpn-sessiondb anyconnect** 命令查看有关当前 VPN 会话的详细信息。

详细信息包括使用的加密方式、传输和接收的字节数及其他统计信息。如果使用VPN连接，随着您重新发出命令，您应可看到传输/接收的字节数会变化。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : priya                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
```

```
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                 Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy        Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                  Tunnel Zone  : 0
```

管理远程访问 VPN 配置

远程访问 VPN 连接配置文件定义了一些特征，这些特征允许外部用户使用 Secure Client与系统建立 VPN 连接。每个配置文件都定义了用于用户身份验证的 AAA 服务器和证书、分配用户 IP 地址的地址池，以及定义各种面向用户的属性的组策略。

如果需要为不同的用户组提供可变的服务，或者有不同的身份验证源，您将创建多个配置文件。例如，如果您的组织与使用不同身份验证服务器的组织合并，您可以为使用这些身份验证服务器的新组创建配置文件。

过程

步骤 1 点击**设备** > **远程访问 VPN** 组中的**查看配置**。

该组显示有关当前已配置多少连接配置文件和组策略的摘要信息。

步骤 2 点击目录中的**连接配置文件**（如果未将其选定）。

步骤 3 执行以下任一操作：

- 点击 + 按钮创建新的连接配置文件。有关详细说明，请参阅配置 RA VPN 连接配置文件，第 668 页。
- 点击查看按钮()，打开连接配置文件和连接说明的摘要。在摘要中，可以点击**编辑**以进行更改。
- 点击删除按钮 ()，删除不再需要的连接配置文件。
- 选择目录中的**组策略**，定义连接配置文件面向用户的属性。请参阅为 RA VPN 配置组策略，第 675 页。

配置 RA VPN 连接配置文件

您可以创建远程访问VPN连接配置文件，允许用户在外部网络（例如其家庭网络）上时连接到您的内部网络。创建单独的配置文件，以适应不同的身份验证方法。

开始之前

在配置远程访问 (RA) VPN 连接之前：

- 从 software.cisco.com 将所需的 Secure Client 软件包下载到您的工作站。
- 外部接口（作为远程访问 VPN 连接终端的外部接口）也不能具有允许相同端口上的 HTTPS 连接的管理访问列表。为管理访问配置其他端口（请参阅在数据接口上配置用于管理访问的HTTPS端口，第 729 页），或者为连接配置文件配置其他端口。这两项服务都默认使用 443，因此其中一项必须更改。

过程

步骤 1 点击**设备** > **远程访问 VPN** 组中的**查看配置**。

该组显示有关当前已配置多少连接配置文件和组策略的摘要信息。

步骤 2 点击目录中的**连接配置文件**（如果未将其选定）。

步骤 3 执行以下操作之一：

- 点击 + 按钮创建新的连接配置文件。
- 点击查看按钮()，打开连接配置文件和连接说明的摘要。在摘要中，可以点击**编辑**以进行更改。

步骤 4 配置基本连接属性。

- **连接配置文件名称** - 此连接的名称，最多 50 个字符，不能含空格。例如，MainOffice。不能将 IP 地址用作名称。

  注释 您在此输入的名称将是用户在 Secure Client 客户端的连接列表中看到的名称。选择一个对您的用户来说有意义的名称。

- **组别名**、**组 URL** - 别名包含特定连接配置文件的备用名称或URL。在连接到威胁防御 设备时，VPN 用户可以在连接列表中的 Secure Client 客户端中选择别名。连接配置文件名称会自动添加为组别名。别名最多可包含 31 个字符。

  您还可以配置组 URL 列表，在发起远程访问 VPN 连接时您的终端可以从该列表中进行选择。如果用户使用组 URL 进行连接，系统将自动使用与 URL 匹配的连接配置文件。此 URL 供尚未安装 Secure Client 客户端的客户使用。

  按需要添加组别名和 URL。在设备上定义的所有连接配置文件中，这些别名和 URL 必须是唯一的。组 URL 必须以 **https://** 开头。

  例如，您可能有别名承包商和组 URL https://ravpn.example.com/contractor。安装 Secure Client 客户端后，用户只需在连接的 Secure Client VPN 下拉列表中选择组别名。

步骤 5 配置主身份源和辅助身份源（可选）。

这些选项确定设备如何对远程用户进行身份验证，以启用远程访问VPN连接。最简单的方法是仅使用 AAA，然后选择 AD 领域或使用 LocalIdentitySource。根据**身份验证类型**，您可以使用以下方法：

- **仅 AAA** - 根据用户名和密码对用户进行身份验证和授权。有关详细信息，请参阅为连接配置文件配置 AAA，第 672 页。
- **仅客户端证书** - 根据客户端设备身份证书进行用户身份验证。有关详细信息，请参阅为连接配置文件配置证书身份验证，第 674 页。
- **AAA 和 ClientCertificate** - 同时使用用户名/密码和客户端设备身份证书。
- **SAML** - 在主身份验证时使用 SAML 服务器。使用 SAML 时，不能配置回退或辅助身份验证源。有关详细信息，请参阅为连接配置文件配置 AAA，第 672 页。

步骤 6 配置客户端的地址池。

地址池定义了远程客户端在建立 VPN 连接时，系统可以分配给它们的 IP 地址。有关详细信息，请参阅为 RA VPN 配置客户端寻址，第 675 页。

步骤 7 点击**下一步 (Next)**。

步骤 8 选择要用于此配置文件的**组策略**。

组策略在建立隧道后设置用户连接的条款。系统包含名为 DfltGrpPolicy 的默认组策略。您可以创建其他组策略，以提供您所需的服务。

选择组策略时，您会看到组特征的摘要。在摘要中，点击**编辑 (Edit)** 可进行更改。

如果您需要的组策略尚不存在，请在下拉列表中点击**创建新的组策略 (Create New Group Policy)**。

有关组策略的详细信息，请参阅为 RA VPN 配置组策略，第 675 页。

步骤 9 点击**下一步 (Next)**。

步骤 10 配置全局设置。

这些选项适用于每个连接配置文件。在创建第一个连接配置文件后，后续的每个配置文件都会预配置这些选项。如果您做出了更改，则每个已配置的连接配置文件都会更改。

- **设备身份证书** - 选择用于建立设备身份的内部证书。客户端必须接受此证书才能完成安全的VPN连接。如果您还没有证书，请点击下拉列表中的**创建新内部证书 (Create New Internal Certificate)**。您必须配置证书。
- **外部接口** - 用户在进行远程访问 VPN 连接时连接的接口。请选择您支持的设备与最终用户之间的任何接口，虽然这通常是外部（面向互联网的）接口。
- **外部接口的完全限定域名** - 接口的名称，例如 ravpn.example.com。如果指定名称，系统可以为您创建一个客户端配置文件。

  注释 您要确保 VPN 中和客户端使用的 DNS 服务器可以将此名称解析为外部接口的 IP 地址。将 FQDN 添加到相关 DNS 服务器。

- **端口** - 用于 RA VPN 连接的 TCP 端口。默认值为 443。如果需要在用于 RA VPN 的同一接口上连接到 设备管理器 ，则必须更改连接配置文件或 设备管理器的端口号。这两项服务都默认使用 443。请注意，如果更改远程访问 VPN 连接的端口，用户必须在 URL 中包含该端口号。
- **为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** -是否要让 VPN 流量受访问控制策略的限制。默认情况下已解密VPN流量受制于访问控制策略检查。启用**为已解密的流量绕过访问控制策略**选项会使流量绕过访问控制策略，但对于远程访问 VPN 而言，从 AAA 服务器下载的 VPN 过滤器 ACL 和授权 ACL 仍然适用于 VPN 流量。

  请注意，如果选择此选项，系统会配置 **sysopt connection permit-vpn** 命令，此为全局设置。这也会影响站点间VPN连接的行为。此外，就此选项而言，您无法为各连接配置文件采取不同的设置：此功能对所有的配置文件而言，要么都设为开启，要么都设为关闭。

  如果不选择此选项，外部用户可能会骗取远程访问 VPN 地址池中的 IP 地址，从而获取访问您网络的权限。这种情况可能会发生，因为您创建的访问控制规则需要允许地址池访问内部资源。如果您使用访问控制规则，请考虑使用用户说明来控制访问，而不是只使用源 IP 地址。

  选择此选项的弊端在于，VPN 流量将不会被检测，也就是说不会对流量应用入侵和文件保护、URL 过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映 VPN 连接。
- **NAT 豁免** - 启用 NAT 豁免，使进出远程访问 VPN 终端的流量免于执行 NAT 转换。如果不豁免 VPN 流量执行 NAT，请确保外部和内部接口的现有 NAT 规则不适用于 RA VPN 地址池。NAT 豁免规则是给定源/目标接口和网络组合的手动静态身份 NAT 规则，但它们不会反映在 NAT 策略中，它们是隐藏起来的。如果启用 NAT 豁免，还必须进行以下配置。

  请注意，这是一个全局选项；它会应用于所有连接配置文件。因此，请仅添加接口和内部网络，而不要替换它们，否则您将会改变已定义的所有其他连接配置文件的 NAT 豁免设置。

  - **内部接口** - 选择远程用户将要访问的内部网络的接口。所创建的 NAT 规则用于这些接口。
  - **内部网络** - 选择代表远程用户将访问的内部网络的网络对象。网络列表必须包含与您支持的地址池相同的 IP 类型。

- **Secure Client 软件包** - RA VPN 连接上将支持的 Secure Client 完整安装软件映像。对于每个软件包，文件名（包括扩展名）不能超过 60 个字符。可以为 Windows、Mac 和 Linux 终端上传单独的软件包。但是，无法为不同的连接配置文件配置不同的软件包。如果已为另一个配置文件配置软件包，则会预先选中此软件包。对此配置的更改将会应用于所有配置文件。

  从 software.cisco.com 下载该软件包。如果终端尚未安装正确的软件包，系统会提示用户在用户验证后下载并安装软件包。

步骤 11 点击**下一步**。

步骤 12 审核摘要。

首先，验证摘要是否正确。

然后，点击 **说明** 查看最终用户初步安装 Secure Client 软件需要做什么，并测试他们是否可以完成 VPN 连接。点击**复制 (Copy)** 将这些说明复制到剪贴板，然后分发给您的用户。

步骤 13 点击**完成 (Finish)**。

下一步做什么

确保 VPN 隧道中允许流量，如允许流量通过远程访问 VPN，第 666 页中所述。

为连接配置文件配置 AAA

身份验证、授权和记账(AAA)服务器使用用户名和密码来确认是否允许用户访问远程访问VPN。如果使用 RADIUS 服务器，则可以区分已验证用户的授权级别，从而提供对受保护资源的差异化访问权限。还可以使用 RADIUS 记账服务来跟踪使用情况。

在配置AAA时，您必须配置主身份源。辅助源和备用源是可选的。如果想要实施双重身份验证，请使用辅助源，例如，RSA 令牌或 DUO。

主身份源选项

- **用户身份验证的主身份源** - 用于对远程用户进行身份验证的主要身份源。必须在此源或可选的回退源中定义最终用户，才能完成 VPN 连接。选择以下一个选项：
  - Active Directory (AD) 身份领域。如果所需的领域尚不存在，请点击**创建新身份领域**。
  - RADIUS 服务器组。
  - LocalIdentitySource（本地用户数据库）- 您可以直接在设备上定义用户，而不使用外部服务器。
  - Duo LDAP 服务器。但是，这最好用作辅助身份验证源，以提供双因素身份验证，如如何使用 Duo LDAP 配置双因素身份验证，第 691 页中所述。如果将其用作主要源，则不会获取用户身份信息，而且在控制面板中也看不到用户信息，也不能编写基于用户的访问控制规则。
  - SAML 服务器。如果使用 SAML 服务器，则无法配置回退或辅助身份验证源。可以将RADIUS用作授权服务器，但必须配置RADIUS服务器，以便不需要身份验证。也就是说，在 SAML 对连接进行身份验证后，RADIUS 服务器将提供授权信息。
- **SAML 登录体验** - 如果选择 SAML 作为主身份验证源，您需要选择使用哪个客户端浏览器来完成 Web 身份验证：
  - **VPN 客户端嵌入式浏览器** - VPN 客户端使用其嵌入式浏览器进行 Web 身份验证，因此该身份验证仅适用于 VPN 连接。这是默认浏览器，无需进一步配置。
  - **默认操作系统浏览器** - VPN 客户端使用系统的默认浏览器进行 Web 身份验证。此选项可在您的 VPN 身份验证和其他企业登录之间启用单点登录 (SSO)。如果您想要支持无法在嵌入式浏览器中执行的 Web 身份验证方法（例如生物特征身份验证），也可选择此选项。

    您必须上传一个软件包，在浏览器中启用 Web 身份验证。从 software.cisco.com 获取软件包。请注意，所有使用 SAML 和默认操作系统浏览器的连接配置文件都使用您上传的数据； 这些数据包是全局的，而不是特定于连接配置文件的。

- **回退本地身份源** - 如果主要源是一个外部服务器，您可以选择 LocalIdentitySource 作为回退源，以防主服务器不可用。如果使用本地数据库作为回退源，请确保您定义的本地用户名/密码与外部服务器中的定义的用户名/密码相同。

高级选项 - 点击**高级**链接并配置以下选项：

- **删除选项** - 领域是管理域。启用以下选项将允许仅基于用户名进行身份验证。您可以启用这些选项的任意组合。但是，如果服务器无法分析分隔符，则必须选中这两个复选框。
  - **从用户名删除身份源服务器** - 在将用户名传递到 AAA 服务器之前，是否要从用户名删除身份源名称。例如，如果选择此选项且用户输入域\用户名作为用户名，则该域将从用户名中删除，并发送到 AAA 服务器进行身份验证。默认情况下，此选项处于取消选中状态。
  - **从用户名删除组** - 在将用户名传递到 AAA 服务器之前，是否要从用户名删除组名称。此选项适用于 username@domain 格式中给定的名称；此选项会剥离域和 @ 符号。默认情况下，此选项处于取消选中状态。
- **启用密码管理** - 是否允许用户在密码过期时更改密码。如果不选择此选项，当用户的密码过期时，Secure Client 将拒绝连接，用户必须前往 AAA 服务器更改密码。如果选择此选项，Secure Client 会在密码过期时提示用户更改密码，这对用户来说要方便得多。请选择以下其中一个选项。此外，请确保在 AAA 服务器上启用 MSCHAPv2。
  - **在密码过期前 x 天通知用户**（仅限 LDAP）- 从您指定的天数开始，警告用户密码即将过期。您可以将警告设置为 1-180 天，默认值为 14。
  - **在密码过期当天通知用户** - 不会警告用户，但在密码过期时仍会提示用户更改密码。即使您设置了警告期，RADIUS 用户也始终会出现此行为。

辅助身份源

- **用于用户授权的辅助身份源** - 可选的第二个身份源。如果用户成功使用主要源进行身份验证，则系统会提示其使用辅助源进行身份验证。可以选择 AD 领域、RADIUS 服务器组、Duo LDAP 服务器或本地身份源。
- **高级选项** - 点击**高级**链接并配置以下选项：
  - **辅助源的备用本地身份源** - 如果辅助源为外部服务器，您可以选择 LocalIdentitySource 作为备用源，以防辅助服务器不可用。如果使用本地数据库作为备用源，请确保您定义的本地用户名/密码与辅助外部服务器中定义的用户名/密码相同。
  - **使用主要用户名进行辅助登录** - 默认情况下，使用辅助身份源时，系统将提示输入辅助源的用户名和密码。如果选择此选项，系统将仅提示您输入辅助密码，并使用与主身份源相同的用户名来进行辅助源身份验证。如果您在主身份源和辅助身份源中配置了相同的用户名，请选择此选项。
  - **会话服务器用户名** - 身份验证成功后，用户名将显示在事件和统计控制面板中，用于确定基于用户或组的 SSL 解密和访问控制规则之间的匹配关系，并用于记账。由于使用了两个身份验证源，因此您需要告诉系统是使用主用户名还是辅助用户名作为用户身份。默认情况下，使用主用户名。

- **密码类型** - 如何获取辅助服务器的密码。仅当您选择 **AAA 和客户端证书**作为身份验证类型时，此字段才适用，并且对于证书选项，您选择**在用户登录窗口预填证书中的用户名**以及**在登录窗口隐藏用户名**。默认值为**提示**，这表明系统将提示用户输入密码。

  选择**主身份源密码**，自动使用用户在主服务器中进行身份验证时输入的密码。

  选择**公用密码**，为每个用户使用相同的密码，然后在**公用密码**字段中输入该密码。

其他选项

- **授权服务器** - 已配置为授权远程访问 VPN 用户的 RADIUS 服务器组。

  身份验证完成后，授权将控制对每个经过身份验证的用户都可用的服务和命令。授权通过组合一组描述用户被授权执行的操作、其实际功能和限制的属性来工作。如果您不使用授权，则单独的身份验证将为所有经过身份验证的用户提供相同的访问权限。有关配置 RADIUS 授权的信息，请参阅使用 RADIUS 和组策略控制用户权限和属性，第 657 页。

  请注意，如果系统从 RADIUS 服务器获取的授权属性与组策略中定义的属性重叠，则 RADIUS 属性将覆盖组策略属性。

- **记账服务器** -（可选。）用于为远程访问 VPN 会话记账的 RADIUS 服务器组。

  记账会跟踪用户正在访问的服务以及他们正在使用的网络资源量。威胁防御 设备向 RADIUS 服务器报告用户活动。记账信息包括每个会话的开始和停止时间、用户名、会话时通过设备的字节数、使用的服务以及每个会话的持续时间。然后，您可分析该数据，以进行网络管理、客户端计费或审核。您可以单独使用记账功能，也可以将其与身份验证和授权功能配合使用。

为连接配置文件配置证书身份验证

可以使用客户端设备安装的证书对远程访问VPN连接进行身份验证。使用证书身份验证时，请确保用于验证远程访问用户连接的受信任 CA 证书包括用于**验证使用**的 **SSL 客户端**选项。

使用客户端证书时，仍可以配置辅助身份源、备用源，以及授权和记账服务器。这些是AAA选项；有关详细信息，请参阅为连接配置文件配置 AAA，第 672 页。

以下是证书特定的属性。您可以为主身份源和辅助身份源单独配置这些属性。配置辅助源为可选操作。

- **从证书中获取的用户名** - 选择以下选项之一：
  - **映射特定字段** - 按照**主要字段**和**辅助字段**的顺序使用证书元素。默认值为 CN（公用名）和 OU（组织单位）。选择适用于您的组织的选项。这些字段组合在一起用于提供用户名，此名称用于事件和控制面板中，并出于匹配的目的，在 SSL 解密和访问控制规则中使用。
  - **使用完整 DN（可分辨名称）作为用户名** - 系统自动从 DN 字段派生出用户名。
- **高级选项 (Advanced options)** - 点击**高级 (Advanced)** 链接并配置以下选项：
  - **在用户登录窗口预填证书中的用户名** - 在提示用户进行身份验证时，是否在用户名字段填写检索到的用户名。

- **在登录窗口隐藏用户名** - 如果选择**预填充**选项，则可以隐藏用户名，这意味着用户无法编辑密码提示中的用户名。

为 RA VPN 配置客户端寻址

系统必须可以通过某种方法向连接到远程访问 VPN 的终端提供 IP 地址。这些地址可以由 AAA 服务器、DHCP 服务器、组策略中配置的 IP 地址池，或连接配置文件中配置的 IP 地址池提供。系统会按照以上顺序尝试使用这些资源，并在获取一个可用地址后停止尝试，然后将此地址分配给客户端。因此，您可以配置多个选项，以便在并发连接数异常多的情况下，可保障系统能获取地址。

使用下列一个或多个方法配置连接配置文件的地址池。

- **AAA 服务器**- 首先，在 威胁防御 设备上配置网络对象，用于指定地址池的子网。然后，在 RADIUS 服务器中，使用对象名称配置用户的地址池 (217) 属性。此外，还要在连接配置文件中指定用于身份验证的 RADIUS 服务器。
- **DHCP** - 首先，使用一个或多个 IPv4 地址范围为 RA VPN 配置 DHCP 服务器（您无法使用 DHCP 配置 IPv6 池）。然后，使用 DHCP 服务器的 IP 地址创建主机网络对象。随后，便可以在连接配置文件的 **DHCP 服务器 (DHCP Servers)**属性中选择此对象。您最多可以配置 10 个 DHCP 服务器。

  如果 DHCP 服务器有多个地址池，则可以在与连接配置文件关联的组策略中使用 **DHCP 作用域**属性，选择要使用的池。使用池的网络地址创建主机网络对象。例如，如果 DHCP 池包含 192.168.15.0/24 和 192.168.16.0/24，将 DHCP 范围设置为 192.168.16.0 可确保从 192.168.16.0/24 子网中选择地址。
- **本地 IP 地址池** - 首先，创建最多六个网络对象，用于指定子网。可以为 IPv4 和 IPv6 单独配置池。然后，在组策略或者连接配置文件的 **IPv4 地址池**和 **IPv6 地址池**选项中，选择这些对象。无需同时配置 IPv4 和 IPv6，只需配置您想要支持的地址方案即可。

  也不需要同时在组策略和连接配置文件中配置池。组策略会覆盖连接配置文件的设置，因此如果您在组策略中配置了池，则请将连接配置文件中的选项留空。

  请注意，系统按照您列出的顺序使用地址池。

为 RA VPN 配置组策略

组策略是针对远程访问 VPN 连接的一组面向用户的属性/值对。连接配置文件使用组策略，在建立隧道后设置用户连接的条款。通过组策略可将整组属性应用于用户或用户组，而不必为每个用户单独指定每个属性。

系统包含名为 DfltGrpPolicy 的默认组策略。您可以创建其他组策略，以提供您所需的服务。

过程

步骤 1 点击**设备** > **远程访问 VPN** 组中的**查看配置**。

该组显示有关当前已配置多少连接配置文件和组策略的摘要信息。

步骤 2 点击目录中的**组策略**。

步骤 3 执行以下任一操作：

- 点击 + 按钮，创建新组。有关组策略页面上的属性的说明，请参阅以下主题：
  - 常规属性，第 676 页
  - 会话设置属性，第 677 页
  - 地址分配属性，第 677 页
  - 分割隧道属性，第 678 页
  - Secure Client 属性，第 678 页
  - 流量过滤器属性，第 679 页
  - Windows 浏览器代理属性，第 680 页
- 点击编辑按钮 ( )，编辑现有组策略。
- 点击删除按钮 ( )，删除不再需要的组。当前，该组不能用于连接配置文件。

常规属性

组策略的常规属性定义组名称和一些其他基本设置。“名称”属性是唯一必需的属性。

- **名称** - 组策略的名称。此名称最多可包含 64 个字符，允许使用空格。
- **说明** - 组策略的说明。说明最多可以有 1,024 个字符。
- **DNS 服务器** - 选择定义连接到 VPN 时，DNS 服务器客户端应用于域名解析的 DNS 服务器组。如果所需的组尚不存在，请点击**创建 DNS 组 (Create DNS Group)** 并立即创建组。
- **横幅**- 登录时向用户显示的横幅文本或欢迎消息。默认无横幅。最多 496 字符。这种 Secure Client 支持部分 HTML。为确保向远程用户正确地显示横幅，请使用
 标记表示换行。
- **默认域** - RA VPN 中用户的默认域名。例如 example.com。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。
- **安全客户端配置文件** - 点击 + 并选择要用于该组的 Secure Client 配置文件。如果为外部接口（在连接配置文件中）配置的是完全限定域名，则系统将会为您创建默认配置文件。或者，您可上传您自己的客户端配置文件。使用独立的 Secure Client 配置文件编辑器创建这些配置文件，您可以从 software.cisco.com 下载和安装该编辑器。如果不选择客户端配置文件， Secure Client 将为所有选项使用默认值。此列表中的项目是 Secure Client 配置文件对象，而不是配置文件本身。您可以通过点击下拉列表中的**创建新的 Secure Client 配置文件 (Create New Secure Client Profile)**，创建（和上传）新配置文件。

  除了 Secure Client 配置文件，您还可以选择 Secure Client 模块配置文件，例如 AMP 启用程序。您可以为每个模块类型选择一个配置文件。

会话设置属性

组政策会话设置控制用户可以连接到 VPN 的时长和可以创建的独立连接的数量。

- **最长连接时间** - 在不注销和重新连接的情况下，允许用户持续连接到 VPN 的最大时间长度（以分钟为单位），范围为 1 到 4473924 或留空。默认值为无限（留空），但空闲超时仍适用。
- **连接时间警报间隔** - 如果您指定了最大连接时间，则警报间隔定义，在达到最长时间之前，向用户显示即将自动断开连接警告的时间。用户可以选择结束连接并重新连接，以重新启动计时器。默认值为 1 分钟。可以指定 1 到 30 分钟。
- **空闲时间** - VPN 连接在自动关闭之前可以闲置的时间长度（以分钟为单位），范围为 1 到 35791394。如果在此时间段内此连接上无通信活动，则系统会终止连接。默认值为 30 分钟。
- **空闲时间警报间隔** - 在达到空闲时间之前，向用户显示因闲置会话而即将自动断开连接的警报的时间。任何活动都会重置计时器。默认值为 1 分钟。可以指定 1 到 30 分钟。
- **每个用户的同时登录数** - 允许用户执行的最多同时登录数。默认值为 3。可以指定 1 到 2147483647 个连接。允许大量同时连接可能会危害安全性并影响性能。

地址分配属性

组策略的地址分配属性定义组的 IP 地址池。此处定义的地址池将覆盖使用此组的任何连接配置文件中定义的池。如果您希望使用连接配置文件中定义的池，请将这些设置留空。

- **IPv4 地址池、IPv6 地址池** - 这些选项定义远程终端的地址池。根据客户端用于建立 VPN 连接的 IP 版本，从这些池为客户端分配地址。选择一个网络对象，定义要支持的每个 IP 类型的子网。如果您不想支持该 IP 版本，则可以空着列表。例如，可以将 IPv4 池定义为 10.100.10.0/24。地址池不能与外部接口的 IP 地址位于同一子网。

  可以指定包含最多六个地址池的列表，用于本地地址分配。地址池的指定顺序非常重要。系统按照地址池出现的顺序分配这些地址池中的地址。

- **DHCP 范围** - 如果在连接配置文件中为地址池配置了 DHCP 服务器，DHCP 作用域会标识要用于此组的地址池的子网。DHCP 服务器的地址还必须来自此作用域标识的同一个子网。作用域允许您选择 DHCP 服务器中定义的部分地址池，用于此特定组。

  如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。

  要指定范围，请选择包含与所需池位于同一子网上但不在池内的可路由地址的网络对象。DHCP 服务器确定此 IP 地址所属的子网并从该地址池分配 IP 地址。

  建议尽可能将接口的 IP 地址用于路由目的。例如，如果池为 10.100.10.2-10.100.10.254，接口地址为 10.100.10.1/24，则使用 10.100.10.1 作为 DHCP 范围。请不要使用网络编号。如果对象尚不存在，请点击**创建新网络 (Create New Network)**。DHCP 仅可用于 IPv4 寻址。如果您选择的地址不是接口地址，可能需要为范围地址创建静态路由。

分割隧道属性

组策略的分割隧道属性定义系统如何处理用于内部网络的流量和流向外部的流量。分割隧道引导一些网络流量通过 VPN 隧道（加密），将剩下的网络流量引导至 VPN 隧道外部（未加密或以明文形式）。

- **IPv4 分割隧道、IPv6 分割隧道** - 可以根据流量是使用 IPv4 寻址还是 IPv6 寻址来指定不同的选项，但每个流量的选项都相同。如果想要启用分割隧道，指定其中一个要求您选择网络对象的选项。
  - **允许所有流量通过隧道** - 不分割隧道。一旦用户建立 RA VPN 连接，用户的所有流量都会通过受保护隧道。这是默认值。这也被视为最安全的选项。
  - **允许指定流量通过隧道** - 选择定义目标网络和主机地址的网络对象。前往这些目标的所有流量都会通过受保护隧道。客户端会将前往其他目标的流量路由至隧道外部（例如，本地 Wi-Fi 或网络连接）。
  - **排除以下指定网络** - 选择定义目标网络或主机地址的网络对象。客户端将前往这些目标的所有流量路由至隧道外部的连接。前往其他目标的流量都会通过隧道。
- **分割 DNS** - 您可以配置系统通过安全连接发送某些 DNS 请求，同时允许客户端将其他 DNS 请求发送到客户端上配置的 DNS 服务器。您可以配置以下 DNS 行为：
  - **根据分割隧道策略发送 DNS 请求** - 使用此选项时，系统将按照与定义分割隧道选项相同的方式处理 DNS 请求。如果启用分割隧道，则会根据目标地址发送 DNS 请求。如果未启用分割隧道，所有 DNS 请求都会通过受保护的连接。
  - **始终通过隧道发送 DNS 请求** - 如果启用了分割隧道，但想要通过受保护连接将所有 DNS 请求发送到为该组定义的 DNS 服务器上，则可选择此选项。
  - **仅通过隧道发送指定的域** - 如果想要让受保护的 DNS 服务器仅解析特定域的地址，则可选择此选项。然后，指定这些域，用逗号分隔域名。例如，example.com, example1.com。如果想要让内部 DNS 服务器解析内部域的名称，同时让外部 DNS 服务器处理所有其他互联网流量，请使用此选项。

Secure Client 属性

组策略的 Secure Client 属性定义 Secure Client 客户端用于远程访问 VPN 连接的某些 SSL 和连接设置。

SSL 设置

- **启用数据报传输层安全 (DTLS)**-是否允许 Secure Client 使用两个同步隧道：SSL 隧道和 DTLS 隧道。使用 DTLS 可避免某些 SSL 连接带来的延迟和带宽问题，并可改进对数据包延迟敏感的实时应用的性能。如果不启用 DTLS，Secure Client 用户在建立 SSL VPN 连接时仅与 SSL 隧道连接。
- **DTLS 压缩** - 是否使用 LZS 为此组压缩数据报传输层安全 (DTLS) 连接。默认情况下会禁用 DTLS 压缩。

- **SSL 压缩** - 是否启用数据压缩，如启用，则设置要使用的数据压缩方法：**Deflate** 或 **LZS**。默认情况下会**禁用** SSL 压缩。数据压缩加快了传输速率，但也增加了每个用户会话的内存需求和 CPU 使用率。因此，SSL 压缩会降低设备的整体吞吐量。
- **SSL 重新生成密钥方法**、**SSL 重新生成密钥间隔** - 客户端能够为 VPN 连接重新生成密钥，重新协商加密密钥和初始化向量，从而提高连接的安全性。选择**无**可禁用重新生成密钥。要启用重新生成密钥，请选择**新隧道 (New Tunnel)**来创建新的隧道。（**现有隧道**选项导致的操作与**新隧道**的相同。）如果启用重新生成密钥，还需设置重新生成密钥间隔，默认间隔为 4 分钟。可以将间隔设置为 4 到 10080 分钟（1 周）。

连接设置

- **忽略 DF（不分片）位** - 是否忽略需要分片的数据包内的“不分片” (DF) 位。选择此选项会允许强制将已设置 DF 位的数据包分片，从而使这些数据包能够通过隧道。
- **客户端绕行协议** - 允许您配置安全网关管理 IPv4 流量（安全网关仅允许 IPv6 流量时）或管理 IPv6 流量（安全网关仅允许 IPv4 流量时）的方式。

  当 Secure Client 建立与头端的 VPN 连接时，头端可以为客户端分配 IPv4 和/或 IPv6 地址。如果头端对 Secure Client 连接仅分配一个 IPv4 地址或一个 IPv6 地址，则您可以配置 Client Bypass Protocol 以丢弃头端尚未分配 IP 地址（默认、已禁用、未检查）的网络流量，或允许该流量绕过头端并从客户端以未加密或“明文形式”发送（已启用、已检查）。

  例如，假设安全网关只将一个 IPv4 地址分配给 Secure Client 连接，且终端为双协议栈。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以明文形式发送 IPv6 流量。
- **MTU** - Secure Client 为 SSL VPN 连接建立的最大传输单位 (MTU) 大小。默认值为 1406 字节。范围为 576 至 1462 字节。
- **Secure Client 和 VPN 网关之间的保持连接消息** - 是否在对等体之间交换保持连接消息，以证明它们可用于在隧道中发送和接收数据。保持连接消息以设置的时间间隔传输。默认间隔为 20 秒，有效范围为 15 到 600 秒。
- **网关端 DPD 间隔**、**客户端 DPD 间隔** - 启用失效对等体检测 (DPD)，确保 VPN 网关或 VPN 客户端快速检测对等体不再响应的时间。您可以单独启用网关或客户端 DPD。发送 DPD 消息的默认间隔为 30 秒。时间间隔可以是 5 到 3600 秒。

流量过滤器属性

组策略的流量过滤器属性定义您想要对分配到该组的用户设置的限制。您可以使用这些属性（而非创建策略规则）根据主机或子网地址和协议或 VLAN 来限制 RA VPN 用户仅可访问特定资源。

默认情况下，RA VPN 用户不会受到组策略的限制，可以访问受保护网络上的任何目标。

- **访问列表过滤器** - 使用扩展的访问控制列表 (ACL) 限制访问权限。选择 Smart CLI 扩展 ACL 对象，或点击**创建扩展访问列表**并立即创建。

  扩展 ACL 允许您基于源地址、目标地址和协议（例如 IP 或 TCP）进行过滤。ACL 评估遵循自上而下、“先匹配的规则先应用”原则，因此，请确保特定规则放在一般规则之前。ACL 末尾

不包含隐式“deny any”语句，因此如果您只是想要拒绝对几个子网的访问，同时允许其他访问，请确保在 ACL 末尾加上“permit any”规则。VPN 过滤器仅适用于初始连接。它不适用于因应用检查操作而打开的辅助连接，例如 SIP 媒体连接。

由于您无法在编辑扩展的 ACL Smart CLI 对象时创建网络对象，因此您应在编辑组策略之前创建 ACL。否则，您可能需要先创建对象，然后再返回来创建网络对象，最后创建您需要的所有访问控制条目。要创建 ACL，请转至**设备** > **高级配置** > **Smart CLI** > **对象**，创建对象，并选择**扩展访问列表**作为对象类型。有关示例，请参阅如何通过组控制 RA VPN 访问，第 714 页。

- **限制 VPN 到 VLAN** - 也称为“VLAN 映射”，此属性指定该组策略应用到的会话的出口 VLAN 接口。系统将该组中的所有流量都转发到所选 VLAN。

  使用此属性向组策略分配 VLAN 以简化访问控制。向此属性赋值是在会话中使用 ACL 过滤流量的替代方法。确保您指定了在设备子接口上定义的 VLAN 编号。值的范围为 1 到 4094。

Windows 浏览器代理属性

组策略的 Windows 浏览器代理属性确定用户浏览器上定义的代理是否运行以及如何运行。

可以为 **VPN 会话期间浏览器代理**选择以下值之一：

- **终端设置无变化** - 允许用户配置（或不配置）浏览器代理或HTTP，并在已配置的情况下使用代理。
- **禁用浏览器代理** - 不使用为浏览器定义的代理（如有）。浏览器连接不会通过该代理。
- **自动检测设置** - 在客户端设备的浏览器中启用自动代理服务器检测。
- **使用自定义设置** - 定义所有客户端设备应对 HTTP 流量使用的代理。配置以下设置：
  - **代理服务器 IP 或主机名、端口** - 代理服务器的 IP 地址或主机名，以及代理服务器用于代理连接的端口。主机和端口总共不能超过 100 个字符。
  - **浏览器例外列表** - 与例外列表中的主机/端口的连接不通过代理。添加不应使用代理的所有目标的主机/端口值。例如，www.example.com port 80。点击**添加 (Add)** 链接以将项目添加到列表。点击垃圾桶图标可删除项目。整个代理例外列表（包括所有地址和端口）不能超过 255 个字符。

监控远程访问 VPN

要对远程访问 VPN 进行监控和故障排除，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。

- **show vpn-sessiondb** 显示有关 VPN 会话的信息。您可以使用 **clear vpn-sessiondb** 命令重置这些统计信息。
- **show webvpn** *keyword* 显示的是远程访问 VPN 配置相关信息，包括统计信息和安装的 AnyConnect 映像。输入 **show webvpn ?** 查看可用关键字。
- **show aaa-server** 可显示用于远程访问 VPN 的目录服务器的统计信息。

远程访问 VPN 故障排除

远程访问 VPN 连接问题可能源自客户端或 威胁防御设备配置。以下主题介绍您可能会遇到的主要故障排除问题。

SSL 连接问题故障排除

如果用户无法对外部 IP 地址进行初始非 Secure Client 连接以下载 Secure Client，请执行以下操作：

1. 如果为远程访问 VPN 连接配置文件配置了非默认端口，请确保用户在 URL 中包含该端口号。例如：https://ravpn.example.com:4443
2. 从客户端工作站，验证能否对外部接口的 IP 地址执行 ping 命令。如果不能，请确定从用户工作站到该地址无路由的原因。
3. 从客户端工作站，验证能否对外部接口（即远程访问 [RA] VPN 连接配置文件中定义的接口）的完全限定域名 (FQDN) 执行 ping 操作。如果能够 ping 通 IP 地址但 ping 不通 FQDN，则需要更新客户端和 RA VPN 连接配置文件使用的 DNS 服务器，添加该 FQDN 到 IP 地址的映射。
4. 验证用户是否接受外部接口提供的证书。用户应该永久接受该证书。
5. 检查 RA VPN 连接配置，并验证您是否选择了正确的外部接口。一个常见错误是选择了面向内部网络的内部接口，而不是面向 RA VPN 用户的外部接口。
6. 如果正确配置了 SSL 加密，请使用外部嗅探器来验证 TCP 三次握手是否成功。

Secure Client AnyConnect 下载和安装问题故障排除

如果用户可以与外部接口建立 SSL 连接，但无法下载和安装 Secure Client 软件包，请考虑以下方面：

- 确保您已上传客户端操作系统适用的 Secure Client 软件包。例如，如果用户的工作站运行的是 Linux，但您没有上传 Linux Secure Client 映像，就没有可安装的软件包。
- 对于 Windows 客户端，用户必须获有管理员权限才能安装软件。
- 对于 Windows 客户端，工作站必须启用 ActiveX 或安装 Java JRE 1.5 或更高版本，推荐使用 JRE 7。
- 对于 Safari 浏览器，必须启用 Java。
- 请尝试不同的浏览器，一种浏览器失败不意味着其他浏览器也会失败。

Secure Client 连接问题故障排除

如果用户能够连接到外部接口、下载并安装 Secure Client，然后却无法使用 Secure Client 完成连接，请考虑以下方面：

- 如果使用 DHCP 向客户端提供 IP 地址，并且客户端无法获取地址，请检查 NAT 规则。适用于 RA VPN 网络的任何 NAT 规则都应包括路由查找选项。路由查找可以帮助确保 DHCP 请求通过适当的接口发送到 DHCP 服务器。
- 如果身份验证失败，请检验用户输入的用户名和密码是否正确，该用户名在身份验证服务器中的定义是否正确。身份验证服务器还必须可以通过一个数据接口使用。

注释 如果身份验证服务器在外部网络，则需要配置与该外部网络的站点间 VPN 连接，并将远程访问 VPN 接口地址包括在 VPN 中。有关详细信息，请参阅如何通过远程访问 VPN 使用外部网络上的目录服务器，第 701 页。

- 如果在远程访问 (RA) VPN 连接配置文件中为外部接口配置了完全限定域名 (FQDN)，请验证能否从客户端设备 ping 通该 FQDN。如果能够 ping 通 IP 地址但 ping 不通 FQDN，则需要更新客户端和 RA VPN 连接配置文件使用的 DNS 服务器，添加该 FQDN 到 IP 地址的映射。如果使用的是为外部接口指定 FQDN 时生成的默认 Secure Client 配置文件，用户需要编辑服务器地址才能使用 IP 地址，直到 DNS 被更新。
- 验证用户是否接受外部接口提供的证书。用户应该永久接受该证书。
- 如果用户的 Secure Client 包括多个连接配置文件，请检验其选择的连接配置文件是否正确。
- 如果客户端似乎一切正常，请与 威胁防御设备建立 SSH 连接，并输入 **debug webvpn** 命令。检查尝试连接期间发出的消息。

RA VPN 流量问题故障排除

如果用户可以进行安全远程访问 (RA) VPN 连接，但无法发送和接收流量，请执行以下操作：

1. 使客户端断开连接，然后重新连接。有时此方法会消除问题。
2. 在 Secure Client中，请检查流量统计信息以确定发送和接收的数据包计数器是否在增加。如果接收的数据包计数保持为零，则 威胁防御设备未返回任何流量。这种情况下，威胁防御配置可能存在问题。常见问题包括：
   - 访问规则在阻止流量。检查访问控制策略是否包含阻止内部网络与 RA VPN 地址池之间传递流量的规则。如果您的默认操作是阻止流量，则可能需要创建一个显式“允许”规则。
   - VPN 过滤器会阻止流量。检查连接配置文件的组策略中配置的 ACL 流量过滤器或 VLAN 过滤器。您可能需要在 ACL 中进行调整或更改 VLAN，具体取决于您如何 （或是否）根据组策略过滤流量。
   - RA VPN 流量没有绕过 NAT 规则。确保为每个内部接口的 RA VPN 连接配置 NAT 豁免。或者，确保 NAT 规则不会阻止内部网络和接口与 RA VPN 地址池和外部接口之间的通信。
   - 路由配置错误。确保定义的所有路由有效并在正常工作。例如，如果您为外部接口定义了静态 IP 地址，请确保路由表包含默认路由（对于 0.0.0.0/0 和 ::/0）。

- 确保为 RA VPN 配置的 DNS 服务器和域名正确，并且客户端系统使用的是正确的 DNS 服务器和域名。验证 DNS 服务器是否可访问。
- 如果在 RA VPN 中启用分割隧道，请检查到指定内部网络的流量是否通过该隧道，而所有其他流量则绕过该隧道（以使 威胁防御设备看不到）。

3. 与 威胁防御设备建立 SSH 连接，并验证是否在为远程访问 VPN 发送和接收流量。使用以下命令。
   - **show webvpn anyconnect**
   - **show vpn-sessiondb**

远程访问 VPN 示例

以下是配置远程访问 VPN 的示例。

如何实施 RADIUS 授权更改

RADIUS 授权更改 (CoA)，也称为动态授权，为 威胁防御远程访问 VPN 提供终端安全。RA VPN 的一个主要挑战是保护　内部网络免遭受攻击终端感染，并在终端受病毒或恶意软件感染时，在终端上采取补救措施来保护终端。有必要在所有阶段（即，在 RA VPN 会话之前、过程中和之后）保护终端和内部网络。RADIUS CoA 功能有助于实现此目标。

如果使用思科身份服务引擎 (ISE) RADIUS 服务器，则可以配置授权更改策略实施。

ISE 授权更改功能提供一种机制，以在建立身份验证、授权和记账 (AAA) 会话后更改其属性。当 AAA 中的用户或用户组的策略发生更改时，ISE 会向 威胁防御 设备发送 CoA 消息，以重新初始化身份验证并应用新策略。不需要内联安全状态实施点 (IPEP) 来为与 威胁防御设备建立的每个 VPN 会话应用访问控制列表 (ACL)。

在 CoA 期间可以更改的属性包括重定向 URL、重定向 ACL 和安全组标记。

以下主题介绍 CoA 的运行方式和配置方法。

授权更改系统流程

Cisco ISE 拥有客户端安全状态代理，用于评估终端对条件的合规性，例如主机上安装的进程、文件、注册表项、防病毒保护、反间谍软件防护和防火墙软件。管理员可以限制网络访问权限直至终端合规，或者提高本地用户的权限，使其可以制定补救措施。ISE 终端安全评估可执行客户端评估。客户端从 ISE 获得终端安全评估要求策略、执行终端安全评估数据收集、将结果与策略进行比较，并将评估结果发送回 ISE。

以下是 威胁防御 设备、ISE 和 RA VPN 客户端之间的授权更改 (CoA) 处理流程。

1. 远程用户使用 Secure Client向 威胁防御 设备发起 RA VPN 会话。
2. 威胁防御 设备为此用户向 ISE 服务器发送 RADIUS 访问-请求消息。

3. 由于此时的客户端安全状态是未知的，因此ISE会将用户与为未知安全状态配置的授权策略进行匹配。此策略定义以下 cisco-av-pair 选项，ISE 将在 RADIUS 访问-接受响应中发送到 威胁防御 。

   - **url-redirect-acl=***acl_name*，其中 *acl_name* 是 威胁防御 设备上配置的扩展 ACL 的名称。此 ACL 定义哪些用户流量应重定向到 ISE 服务器，即 HTTP 流量。例如：

     ```
     url-redirect-acl=redirect
     ```

   - **url-redirect=***url*，其中，URL 是流量应重定向到的目标位置。例如：

     ```
     url-redirect=https://ise2.example.com:8443/guestportal/gateway?sessionId=xx&action=cpp
     ```

   您必须为数据接口配置 DNS，以便可以解析主机名。如果在连接配置文件的组策略中还配置流量过滤，请确保客户端池可以通过端口（在示例中为 TCP/8443）到达 ISE 服务器。

4. 威胁防御 设备发送 RADIUS 记账 - 请求开始数据包并接收来自 ISE 的响应。记账请求包含会话的所有详细信息，包括会话 ID、VPN 客户端的外部 IP 地址和 威胁防御 设备的 IP 地址。ISE 使用会话ID来识别会话。威胁防御 设备还会定期发送临时账户信息，其中最重要的属性是 威胁防御 设备分配给客户端的 IP 地址的 Framed-IP-Address 属性。

5. 在未知安全状态的情况下，威胁防御 设备会将流量从匹配重定向 ACL 的客户端重定向至重定向 URL。ISE 确定客户端是否具有所需的安全状态合规性模块，并在必要时提示用户安装。

6. 在客户端设备上安装代理后，代理会自动执行ISE终端安全评估策略中配置的检查。客户端直接与 ISE 通信。它向 ISE 发送终端安全评估报告，其中可以包含使用 SWISS 协议和 8905 TCP/UDP 端口进行的多个交换。

7. 当ISE收到代理发送的终端安全评估报告时，它会再次处理授权规则。这次，终端安全状态是已知的，会有另一个不同的规则与客户端会匹配。ISE 发送 RADIUS CoA 数据包，其中包括适用于兼容或不合规终端的可下载的 ACL (DACL)。例如，合规 DACL 可能允许所有访问，而不合规 DACL 会拒绝所有访问。DACL 内容由 ISE 管理员决定。

8. 威胁防御设备会删除重定向。如果没有缓存DACL，则必须发送访问-请求才可从ISE下载它们。此特定 DACL 与 VPN 会话关联；不会成为设备配置的一部分。

9. 当 RA VPN 用户再次尝试访问网页时，用户可以访问 威胁防御 设备上为此会话安装的 DACL 允许的资源。

注释 如果端点无法满足所有强制性要求，且需要手动采取补救措施时， Secure Client会打开一个补救窗口，显示需要操作的项目。补救窗口在后台运行，以保证网络活动更新不会弹出，引起干扰或中断。用户可以在 Secure Client 的 ISE 终端安全评估图块部分，点击**详细信息**，查看检测到的内容和您加入网络前所需的更新。

在 威胁防御 设备上配置授权更改

大多数授权更改策略是在 ISE 服务器中配置的。但是，您必须将 威胁防御 设备配置为正确连接到 ISE。以下程序介绍如何配置此配置的 威胁防御 端。

开始之前

如果在任何对象中使用了主机名，请确保配置可用于数据接口的DNS服务器，如为数据流量和管理流量配置 DNS，第 743 页中所述。通常，您仍然需要配置 DNS，才可获得功能齐全的系统。

过程

步骤 1 配置扩展的访问控制列表 (ACL)，用于将初始连接重定向到 ISE。

重定向 ACL 的目的是向 ISE 发送初始流量，以便 ISE 可以评估客户端安全状态。ACL 应向 ISE 发送 HTTPS 流量，而非已设定发往 ISE 的流量或被定向到域名解析 DNS 服务器的流量。重定向 ACL 的示例如下所示：

```
access-list redirect extended deny ip any host <ISE server IP>
access-list redirect extended deny ip any host <DNS server IP>
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
```

但是，请注意，ACL 包含隐式“deny any any”作为最后一个访问控制条目 (ACE)。在此示例中，与 TCP 端口 www（即端口 80）匹配的最后一个 ACE 将不会匹配与前 3 个 ACE 匹配的任何流量，因此这些 ACE 是冗余的。您只需使用最后一个 ACE 创建 ACL 即可获得相同的结果。

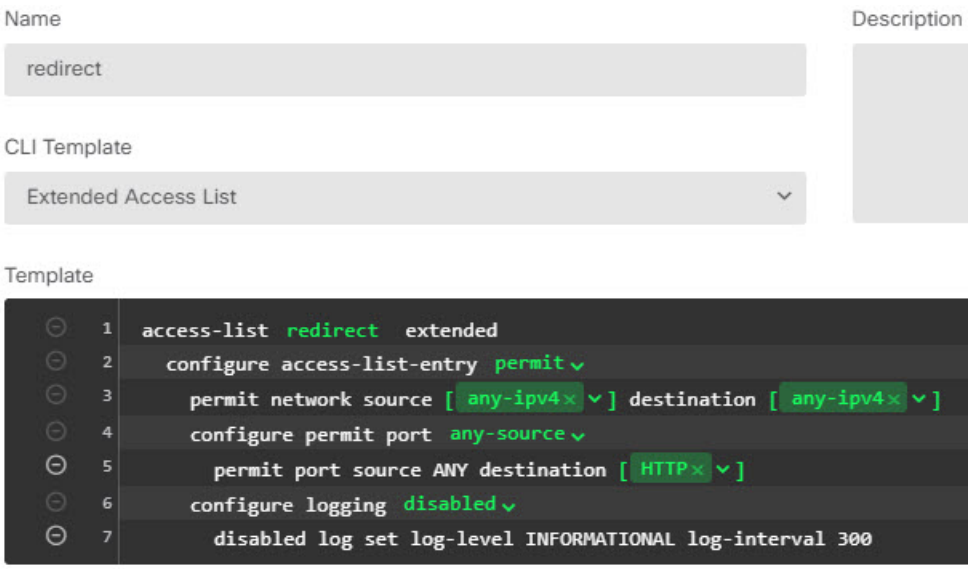
请注意，在重定向 ACL 中，允许和拒绝操作只会确定哪些流量与 ACL 匹配，系统会允许匹配的流量并拒绝不匹配的流量。实际上，系统并不会丢弃任何流量，被拒绝的流量只是未重定向至 ISE。

要创建重定向 ACL，您需要配置 Smart CLI 对象。

a) 选择**设备** > **高级配置** > **Smart CLI** > **对象**。
b) 点击 + 创建新对象。
c) 输入 ACL 的名称。例如，**重定向**。
d) 对于 **CLI 模板**，选择**扩展访问列表**。
e) 在**模板**正文中进行以下配置：

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = any-ipv4
- configure permit port = any-source
- destination-port = HTTP
- configure logging = disabled

ACE 应如下所示：



f) 点击**确定 (OK)**。

在下次部署更改时会配置此 ACL。无需在任何其他策略中使用此对象来强制部署。

注释 此 ACL 仅适用于 IPv4。如果您还想要支持 IPv6，除了要为源和目标网络选择 any-ipv6 外，只需再添加一个拥有所有相同属性的 ACE 即可。您还可以添加其他 ACE，以确保前往 ISE 或 DNS 服务器的流量未被重定向。您首先需要创建主机网络对象，以保留这些服务器的 IP 地址。

步骤 2 配置用于动态授权的 RADIUS 服务器组。

要启用授权更改（也称为动态授权），您必须在 RADIUS 服务器和服务器组对象中正确选择几个关键选项。以下步骤将重点介绍这些属性。有关这些对象的详细信息，请参阅RADIUS 服务器和组，第 158 页。

a) 依次选择**对象** > **身份源**。

b) 点击 **+** > **RADIUS 服务器**。

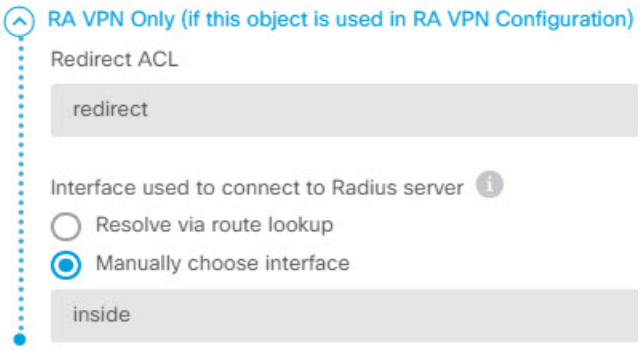
c) 输入服务器名称、ISE RADIUS 服务器的主机名/IP 地址、身份验证端口和服务器上配置的密钥。如果需要，可调整超时。这些选项不直接与动态授权相关。

d) 点击“仅 RA VPN”链接并配置以下选项：

- **重定向 ACL** - 选择您创建的用于重定向的扩展 ACL。在此示例中，ACL 命名为重定向。
- **用于连接 Radius 服务器的接口** - 选择**手动选择接口**，并选择通过其可以访问服务器的接口。您必须选择特定接口，以便系统可以正确启用接口上的 CoA 侦听程序。

  如果此服务器还用于 设备管理器 管理访问，则此接口将被忽略。系统始终通过管理 IP 地址对管理访问尝试进行身份验证。

以下示例展示了为内部接口配置的选项。



e) 点击**确定**保存服务器对象。

如果您设置了冗余，拥有多个相同的 ISE RADIUS 服务器，则请为每个服务器创建服务器对象。

f) 点击 **+** > **RADIUS 服务器组**。

g) 输入服务器组的名称，并根据需要调整空载时间和最大尝试次数。

h) 选择**动态授权**选项，如果 ISE 服务器配置为使用不同的端口，还需要更改端口号。端口 1700 用于侦听 CoA 数据包的默认端口。

i) 如果 RADIUS 服务器配置为使用 AD 服务器对用户进行身份验证，请选择**支持 RADIUS 服务器的领域**，指定与此RADIUS 服务器结合使用的 AD 服务器。如果尚不存在此领域，请点击列表底部的**创建新身份领域**立即配置。

j) 在 **RADIUS 服务器**下，点击 **+** 并选择您为 RA VPN 创建的服务器对象。

k) 点击**确定**保存服务器组对象。

步骤 3 依次选择**设备** > **RA VPN** > **连接配置文件**，并创建使用此 RADIUS 服务器组的连接配置文件。

使用**AAA 身份验证**（单独使用或与证书结合使用），并在**用户身份验证主身份源**、**授权**和**记账**选项中选择服务器组。

请根据组织的需要，配置所有其他选项。

注释 如果通过 VPN 网络访问 DNS 服务器，请编辑连接配置文件中使用的组策略，在分割隧道属性页面上配置**分割 DNS (Split DNS)** 选项。

在 ISE 中配置授权更改

大多数授权更改配置是在ISE服务器中完成的。ISE 具有安全状况评估代理，其在终端设备上运行，ISE 直接与要确定安全状况的设备进行通信。实质上，威胁防御设备会等待 ISE 发出指令，指示其如何处理给定的最终用户。

对配置安全状况评估策略的完整讨论不在本文档的范围之内。但是，以下程序介绍了一些基本配置。可以此为起点来配置 ISE。请注意，各版本中的具体命令路径、页面名称和属性名称可能会发生更改。您使用的 ISE 版本可能使用不同的术语或组织。

支持的最低 ISE 版本为 2.2 补丁 1。

开始之前

此程序假定您已在 ISE RADIUS 服务器中配置用户。

过程

步骤 1 依次选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **网络设备 (Network Devices)**，将 威胁防御 设备添加到“ISE 网络设备”(ISE Network Device) 清单，并配置 RADIUS 设置。

选择 **RADIUS 身份验证设置**，并配置与 威胁防御 RADIUS 服务器对象中配置的共享密钥相同的 **共享密钥** 。如果需要，可更改 **CoA 端口** 号，并确保在 威胁防御 RADIUS 服务器组对象中配置相同的端口。

步骤 2 依次选择**策略** > **策略元素** > **结果** > **授权** > **可下载的 ACL**。

创建 2 个可下载的 ACL (DACL)，一个供合规终端使用，另一个供不合规终端使用。

例如，您可能允许对合规终端 (permit ip any any) 的全部访问，同时拒绝对不合规终端 (deny ip any any) 的全部访问。您可以根据需要调整 DACL 的复杂程度，以根据用户的合规状态为其提供确切的访问权限。您将在授权配置文件中使用这些 DACL。

步骤 3 依次选择**策略** > **策略元素** > **结果** > **授权** > **授权配置文件**并配置所需的配置文件。

您需要适用于以下状态的配置文件。下文列出了每个配置文件至少应具备的属性。

- **未知** - 未知终端安全评估配置文件是默认的终端安全评估配置文件。在初次建立 RA VPN 连接时，每个终端都与此策略匹配。此规则的要点在于，要应用重定向 ACL 和 URL，且如果终端上未安装终端安全评估代理时，还需下载此代理。如果未安装代理或安装失败，终端可以保持与此配置文件关联。否则，在评估终端安全状况后，终端将移至合规或不合规的配置文件。

  至少应具备的属性包括：

  - **名称** - 例如，PRE_POSTURE。
  - **访问类型** - 选择 **ACCESS_ACCEPT**。
  - **常见任务**- 选择 **Web 重定向**（**CWA**、**MDM**、**NSP**、**CPP**），然后选择 **客户端调配**（**安全状况**），并输入您在 威胁防御 设备上配置的重定向 ACL 的名称。在**值**中，选择**客户端调配门户**（如果未选中此选项）。
  - **属性详细信息**应显示两个 cisco-av-pair 值，分别用于 url-redirect-acl 和 url-redirect。ISE 会将此数据发送到 威胁防御 设备，其会将此条件应用于 RA VPN 用户会话。

- **合规** - 终端安全评估完成后，如果终端符合为其配置的所有要求，则客户端被视为合规并可获取此配置文件。通常，您会给予此客户端完全访问权限。

  至少应具备的属性包括：

  - **名称** - 例如，FULL_ACCESS。
  - **访问类型** - 选择 **ACCESS_ACCEPT**。

- **常见任务** - 选择 **DACL 名称**，然后选择适用于合规用户的可下载 ACL，例如 PERMIT_ALL_TRAFFIC。ISE 会将此 ACL 发送到 威胁防御 设备，设备会将其应用于用户会话。此 DACL 将替换用于用户会话的初始重定向 ACL。

- **不合规** - 如果安全状况评估确定终端不符合所有要求，客户端可在一个倒计时时间内让终端符合规范，例如，通过安装所需的更新使终端符合规范。 Secure Client 通知用户合规性问题。在倒计时期间，终端始终处于未知合规状态。如果倒计时完毕后，终端仍不符合规范，则会话会被标记为不合规，并获得不合规配置文件。通常，您将阻止此终端的所有访问，或至少以某种方式限制访问权限。

  至少应具备的属性包括：

  - **名称** - 例如，Non_Compliant。
  - **访问类型** - 选择 **ACCESS_ACCEPT**。
  - **常见任务** - 选择 **DACL 名称**，然后选择适用于不合规用户的可下载 ACL，例如 DENY_ALL_TRAFFIC。ISE 会将此 ACL 发送到 威胁防御 设备，设备会将其应用于用户会话。此 DACL 将替换用于用户会话的初始重定向 ACL。

步骤 4 依次选择**策略** > **策略元素** > **结果** > **客户端调配** > **资源**并配置以下资源：

- **AnyConnect 软件包** - 从 software.cisco.com 下载的头端包文件。支持的客户端平台需要使用单独的软件包，因此您可能需要配置多个类型，例如 AnyConnectDesktopWindows。
- **ISE 安全状况配置文件**（**类型：AnyConnectProfile**）- 此配置文件定义合规性模块用于评估最终用户设备的设置。此文件还定义用户必须在多长时间内使不合规设备变为合规。
- **合规性模块软件包**（**类型：ComplianceModule**） - Secure Client 合规性模块文件是将推送到已安装的 AnyConnect 软件包，用于检查终端合规性的文件。使用**从思科站点添加资源**命令下载此文件。确保根据已配置的 Secure Client 软件包下载正确的模块，否则用户将会下载失败。您还可以在 ISEComplianceModule 文件夹中 Secure Client 列表内的 software.cisco.com 上找到这些文件。
- **AnyConnect 配置文件**（**类型：AnyConnectConfig**）- 这些 Secure Client 版本特定的设置定义要应用的 **AnyConnect 软件包**、**合规性模块**和 **ISE 安全状况**。由于每个操作系统都有各自适用的软件包，因此请为将支持的每个客户端操作系统（例如，Windows、MAC、Linux）创建单独的配置文件。

步骤 5 依次选择**策略** > **客户端调配**并配置客户端调配策略。

为需要实施 CoA 的每个操作系统创建新的规则，例如，使用 CoA_ClientProvisionWin 等名称。为规则选择适当的操作系统，并在**结果**中，选择您为操作系统创建的作为**代理**的 Secure Client 配置文件。

禁用已更换的默认操作系统特定的规则。

步骤 6 配置安全评估策略。

在此步骤中，您制定对组织有意义的终端安全评估要求。

- 依次选择**策略**>**策略元素**>**条件**>**终端安全评估**，并定义需要满足的基本安全评估条件。例如，您可能需要用户已安装特定应用。
- 依次选择**策略** > **策略元素** > **结果** > **终端安全评估** > **要求**，并定义终端的合规性模块要求。
- 依次选择**策略** > **终端安全评估** > **终端安全评估策略**，并配置适用于受支持操作系统的策略。

步骤 7 依次选择**策略** > **策略集** > **默认** > **授权策略**，并创建策略。

为每个合规条件添加规则。这些示例值是基于上一步骤中的示例。

- 未知，用于在安全评估前和安全评估中下载。
  - 名称 - 例如，PRE_POSTURE
  - 条件 -“Session-PostureStatus EQUALS Unknown”和“Radius-NAS-Port-Type EQUALS Virtual”
  - 配置文件 - 例如，PRE_POSTURE
- 合规，适用于符合安全评估要求的客户端。
  - 名称 - 例如，FULL_ACCESS
  - 条件 -“Session-PostureStatus EQUALS Compliant”和“Radius-NAS-Port-Type EQUALS Virtual”
  - 配置文件 - 例如，FULL_ACCESS
- 不合规，适用于不符合安全评估要求的客户端。
  - 名称 - 例如，NON-COMPLIANT
  - 条件 -“Session-PostureStatus EQUALS NonCompliant”和“Radius-NAS-Port-Type EQUALS Virtual”
  - 配置文件 - 例如，Non_Compliant

步骤 8 （可选。）依次选择**管理** > **设置** > **终端安全评估** > **重新评估**，并启用终端安全重新评估。

默认情况下，仅在连接时评估终端安全状况。您可以启用终端安全重新评估，以便定期检查已连接终端的安全状况。您可以设置重新评估间隔，以执行此操作的频率。

如果系统重新评估失败，您可以定义系统应如何做出响应。您可以允许用户继续操作（保持连接），将用户注销，或要求用户修复系统。

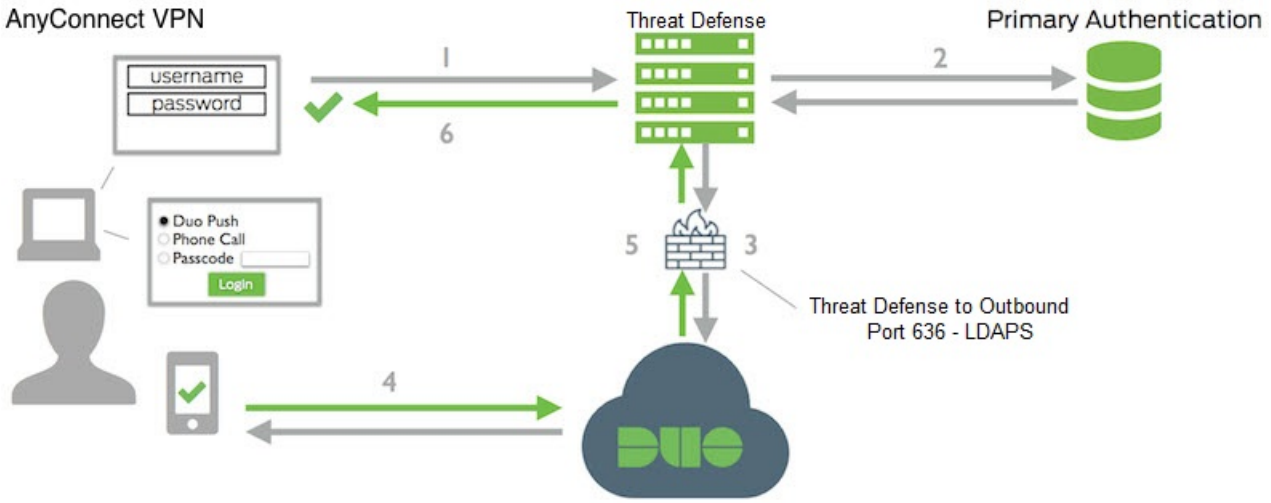
如何使用 Duo LDAP 配置双因素身份验证

可以将 Duo LDAP 服务器作为辅助身份验证源与作为主要源的 Microsoft Active Directory (AD) 或 RADIUS 服务器结合使用。使用 Duo LDAP 时，辅助身份验证使用 Duo 密码、推送通知或电话呼叫验证主要身份验证。

以下主题详细说明这种类型的高级配置。

Duo LDAP 辅助身份验证系统流程

下图显示的是 威胁防御 如何和 Duo 共同发挥作用，以使用 LDAP 提供双因素身份验证。



以下是系统流程的说明：

1. 用户对 威胁防御 设备进行远程访问 VPN 连接，并提供用户名和密码。
2. 威胁防御 使用主身份验证服务器（可能是 Active Directory 或 RADIUS）对此主要身份验证尝试进行身份验证。
3. 如果主身份验证正常工作， 威胁防御 会将辅助身份验证请求发送至 Duo LDAP 服务器。
4. 然后，通过推送通知、带密码的短信消息或电话呼叫单独对用户进行身份验证。用户必须成功完成此身份验证。
5. Duo 响应 威胁防御 设备，以指示用户是否已成功进行身份验证。
6. 如果辅助身份验证成功，则 威胁防御 设备会与用户的 Secure Client建立远程访问 VPN 连接。

配置 Duo LDAP 辅助身份验证

以下操作步骤介绍配置双因素身份验证的端到端过程，使用 Duo LDAP 作为辅助身份验证源，用于远程访问 VPN。请注意，必须拥有一个 Duo 账户，并从 Duo 获取一些信息，才能完成此配置。

过程

步骤 1 创建 Duo 账户并获取集成密钥、密钥和 API 主机名。

以下是对此过程的概述。有关详细信息，请参阅 Duo 网站 https://duo.com。

a) 注册 Duo 账户。
b) 登录到 Duo 管理面板并导航至**应用**，
c) 点击**保护应用**并在应用列表中找到思科 SSL VPN。点击**保护此应用**以获取您的集成密钥、密钥和 API 主机名。如需帮助，请参阅《Duo 入门指南》https://duo.com/docs/getting-started。

步骤 2 创建用于 Duo LDAP 服务器的 Duo LDAP 身份源。

必须使用 威胁防御 API 创建 Duo LDAP 对象，而不可使用 设备管理器创建该对象。可以使用 API Explorer 或编写自己的客户端应用来创建对象。以下步骤介绍如何使用 API Explorer 创建对象。

a) 请登录 设备管理器，点击“更多选项”按钮 ( )，然后选择 **API Explorer**。

系统会在单独的选项卡或窗口中打开 API Explorer，具体取决于您的浏览器设置。

b) （可选。）获取识别系统应用于连接至 Duo LDAP 服务器的接口所需的值。

如果不指定接口，系统将使用路由表。如有必要，可以创建用于Duo LDAP服务器的静态路由。或者，也可以指定要在Duo LDAP对象中使用的接口。如果要指定接口，请使用接口组中的各种 GET 方法获取所需值。可以使用物理接口、子接口、EtherChannel 接口或 VLAN 接口。例如，要获取物理接口的值，请使用 GET/devices/default/interfaces 方法并查找需要使用的接口的对象。需要从接口对象获得以下值：

- id
- type
- version
- name

c) 点击 **DuoLDAPIdentitySource** 标题以打开组。
d) 点击 **POST /object/duoldapidentitysources** 方法。
e) 在**参数**标题下，对于 **body** 元素，点击右侧**数据类型**列中的**示例值**显示框。此操作会将示例加载至正文值编辑框中。
f) 在**正文值**编辑框中，执行以下操作：

- 删除以下属性行：**version**、**id**。（这些属性是 PUT 调用而不是 POST 调用所需的属性。）
- 对于 **name**，请输入对象名称，例如，Duo-LDAP-server。
- 对于 **description**，要么输入对象的有意义说明以供参考，要么删除该属性行。
- 对于 **apiHostname**，请输入您从 Duo 账户中获取的 API 主机名。主机名应如下所示，X 替换为您的唯一值：API-XXXXXXXX.DUOSECURITY.COM。无需大写。

- 对于 **port**，请输入用于 LDAPS 的 TCP 端口。这应该是 636，除非 Duo 通知您使用不同端口。请注意，必须确保访问控制列表允许通过此端口流向 Duo LDAP 服务器的流量。
- 对于 **timeout**，请输入连接到 Duo 服务器所采用的超时时间（以秒为单位）。值可以是 1-300 秒。默认值为 120。要使用默认值，请输入 120 或删除该属性行。
- 对于 **integrationKey**，请输入从您的 Duo 账户获取的集成密钥。
- 对于 **secretKey**，输入从您的 Duo 账户获取的密钥。此密钥随后将被屏蔽。
- 对于 **interface**，请输入要用于连接到 Duo LDAP 服务器的接口的 ID、类型、版本和名称值，或删除用于定义接口属性的 6 行，包括尾部的右大括号。
- 对于 **type**，将值保留为 duoldapidentitysource。

例如，对象正文可能如下所示，其中系统会对 apiHostname 和 integrationKey 进行模糊处理，但会显示故意伪造的密钥：

```
{
  "name": "Duo-LDAP-server",
  "description": "Duo LDAP server for RA VPN",
  "apiHostname": "API-XXXXXXXX.DUOSECURITY.COM",
  "port": 636,
  "timeout": 120,
  "integrationKey": "XXXXXXXXXXXXXXXXXXXX",
  "secretKey": "123456789",
  "type": "duoldapidentitysource"
}
```

g) 点击**试用！**按钮。

系统将发出 **curl** 命令，以将对象发布至设备配置。系统将显示 curl 命令、响应正文和响应代码。如果创建的正文有效，则在**响应代码**字段中应该会看到 **200** 。

如果发生错误，请查看响应正文了解错误消息。可以更正正文值，然后重试。

h) 点击顶部菜单中的 **设备** ，返回至 设备管理器 。

i) 点击**对象**，然后点击目录中的**身份源**。

您的 Duo LDAP 对象应显示在列表中。如未显示，请返回 API Explorer，然后再次尝试创建对象。可以使用 GET 方法检查其是否确实已创建。

请注意，可以使用 设备管理器删除该对象，但不能对其进行编辑或查看其内容。必须使用 API 执行这些操作。相关方法显示在 **DuoLDAPIdentitySource** 组中。

步骤 3 将 Duo 网站的受信任 CA 证书上传至 设备管理器。

威胁防御 系统必须具有验证与 Duo LDAP 服务器的连接所需的证书。可以使用此程序获取并上传证书，该过程已通过 Google Chrome 浏览器完成。适用于您的浏览器的确切步骤可能有所不同。或者，也可以直接转至 https://www.digicert.com/digicert-root-certificates.htm 并下载证书，但以下程序是通用的，可以用其获取任何站点的根受信任 CA 证书。

a) 在浏览器中打开 https://duo.com。

b) 点击浏览器 URL 字段中的站点信息链接，然后点击**证书**链接。此操作将打开“证书信息”对话框。

c) 点击**证书路径**选项卡，并选择路径的根（顶部）级别。在本例中为 DigiCert。

d) 选择 DigiCert，然后点击**查看证书**。此操作将打开一个新的“证书”对话框，“常规”选项卡应指示其已发布给 DigiCert High Assurance EV 根 CA。这是需要上传至 设备管理器的根 CA 证书。

e) 点击**详细信息**选项卡，然后点击**复制到文件**按钮以启动证书下载向导。

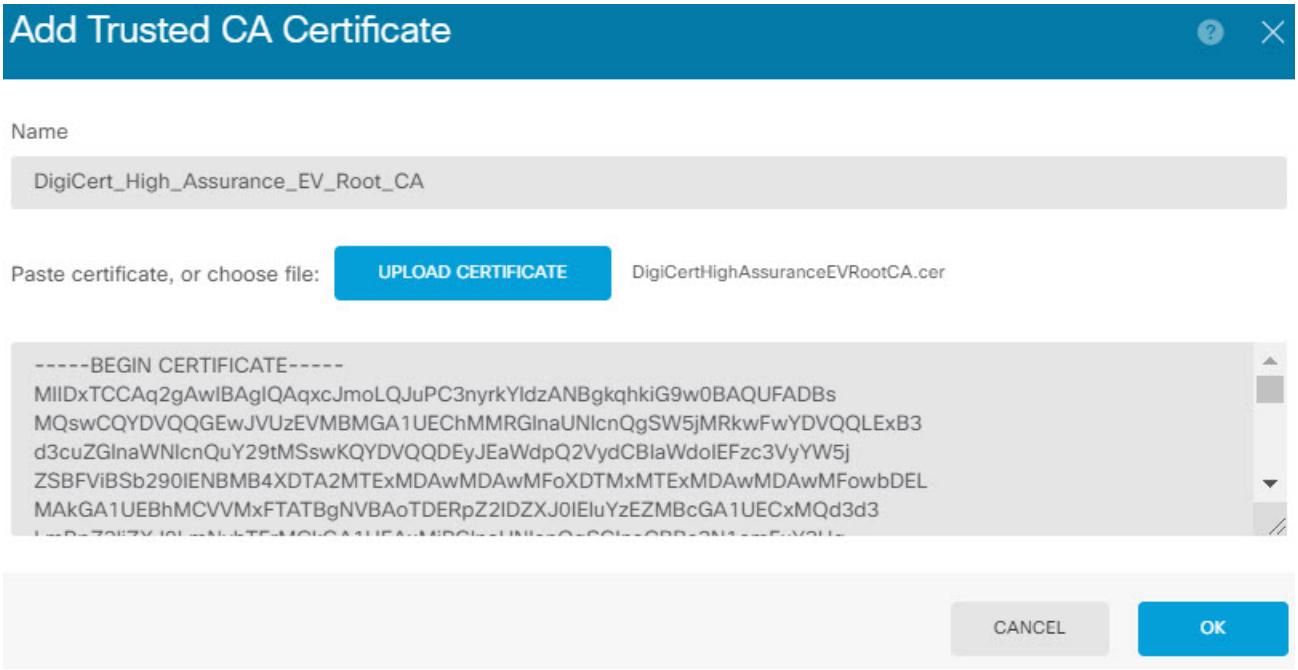
f) 使用该向导将证书下载至您的工作站。使用默认 DER 格式下载。

g) 在 设备管理器中，选择 **对象** > **证书**。

h) 依次点击 + > **添加受信任 CA 证书**。

i) 输入证书名称，例如，DigiCert_High_Assurance_EV_Root_CA。（不允许使用空格。）

j) 点击**上传证书**，然后选择下载的文件。



k) 点击**确定**。

步骤 4 使用 Secure Client 配置文件编辑器创建配置文件，将身份验证超时值指定为 60 秒或更长时间。

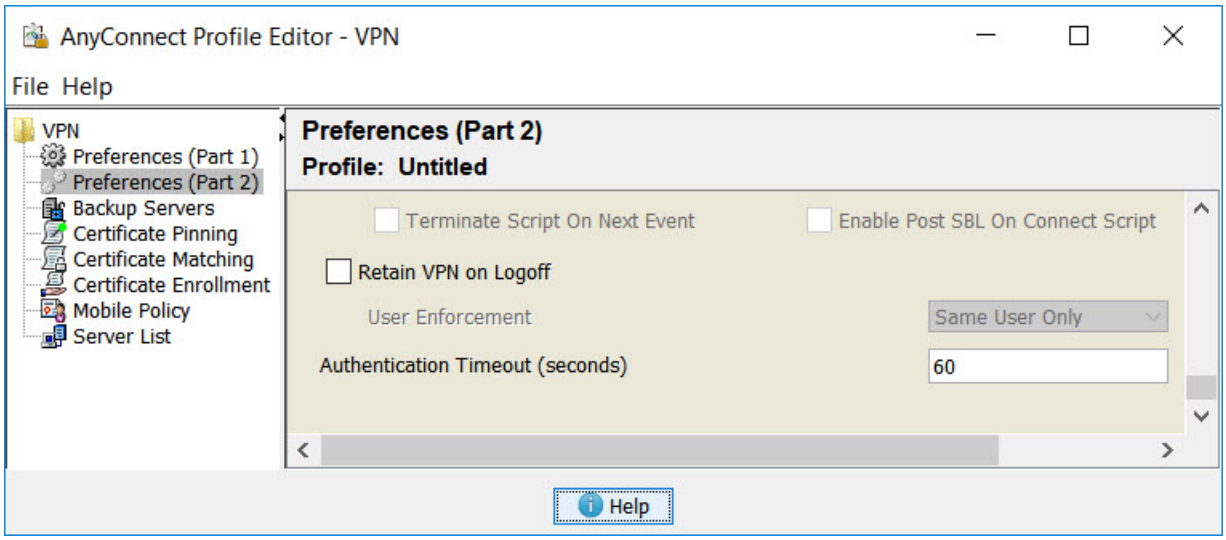
需要为用户提供额外的时间来获取 Duo 密码并完成辅助身份验证。我们建议将此时间设置为至少 60 秒。

有关创建并上传 Secure Client 配置文件的详细信息，请参阅配置并上传客户端配置文件，第 663 页。以下操作步骤介绍如何仅配置身份验证超时，然后将配置文件上传至 威胁防御。如果要更改其他设置，现在就可以进行更改。

a) 如果尚未执行此操作，请下载并安装 Secure Client 配置文件编辑器软件包。可以在思科软件中心 (software.cisco.com) 相应 Secure Client 版本文件夹内找到此软件包。

b) 打开 Secure Client **VPN 配置文件编辑器 (VPN Profile Editor)**。

c) 在目录中选择**首选项（第 2 部分）**，滚动至页面末尾，并将**身份验证超时**更改为 60（或更大值）。以下是来自 AnyConnect 4.7 VPN 配置文件编辑器的图像；先前或后续版本可能不同。



d) 选择**文件 (File)** > **保存 (Save)**，将配置文件 XML 文件保存至您的工作站，并使用适当名称（例如，duo-ldap-profile.xml）。

现在，可以关闭 VPN 配置文件编辑器应用。

e) 在 设备管理器 中，选择**对象 (Objects)** > **Secure Client 配置文件 (Secure Client Profiles)**。

f) 点击 + 创建新的配置文件对象。

g) 为对象输入**名称**。例如，Duo-LDAP-profile。

h) 点击**上传**，选择创建的 XML 文件。

i) 点击**确定**。

步骤 5 创建组策略，并在策略中选择 Secure Client 配置文件。

分配给用户的组策略控制连接的许多方面。以下操作步骤介绍如何将配置文件 XML 文件分配到组。有关可以使用组策略执行哪些操作的更多详细信息，请参阅为 RA VPN 配置组策略，第 675 页。

a) 在**设备 (Device)** > **远程访问 VPN (Remote Access VPN)** 中点击**查看配置 (View Configuration)**。

b) 选择目录中的**组策略**。

c) 编辑 DfltGrpPolicy，或者点击 + 并创建新的组策略。例如，如果您需要适用于所有用户的单个远程访问 VPN 连接配置文件，则宜编辑默认组策略。

d) 在“常规”(General) 页面上，配置以下属性：

- **名称** - 对于新的配置文件，请输入名称。例如，Duo-LDAP-group。
- **Secure Client 配置文件** - 点击 + 并选择创建的 Secure Client 配置文件对象。

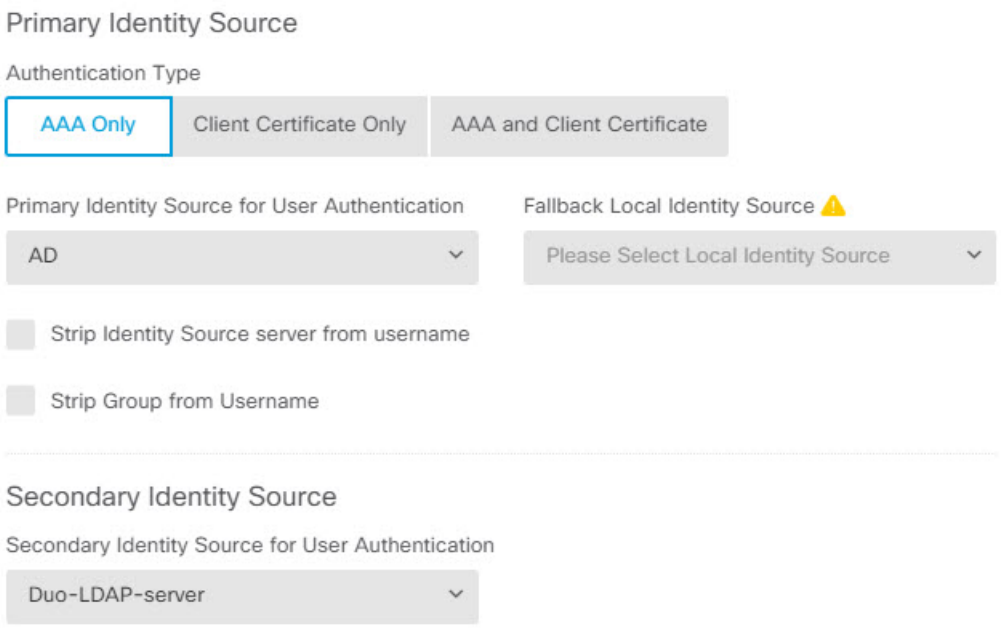
e) 点击**确定**保存组配置文件。

步骤 6 创建或编辑用于 Duo-LDAP 辅助身份验证的远程访问 VPN 连接配置文件。

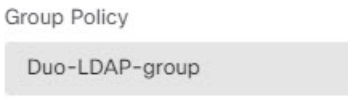
配置连接配置文件有很多步骤，详见配置 RA VPN 连接配置文件，第 668 页。以下操作过程仅介绍将 Duo-LDAP 启用为辅助身份验证源并应用 Secure Client 配置文件所需执行的密钥更改。对于新连接配置文件，必须配置其余必填字段。对于此操作过程，我们假设您正在编辑现有连接配置文件，而且您只需更改这两个设置。

a) 在 RA VPN 页面上，选择目录中的**连接配置文件 (Connection Profiles)**。
b) 编辑现有配置文件或创建新的配置文件。
c) 在主身份源下，配置以下内容：

- **身份验证类型** - 选择**仅 AAA** 或 **AAA 和客户端证书**。除非使用 AAA，否则无法配置双因素身份验证。
- **用于用户身份验证的主要身份源** - 选择主 Active Directory 或 RADIUS 服务器。请注意，可以选择一个 Duo-LDAP 身份源作为主要源。然而，Duo-LDAP 仅提供身份验证服务，而不提供身份服务，因此，如果将其作为主要身份验证源，则在任何控制面板中都将看不到与 RA VPN 连接关联的用户名，且将无法为这些用户编写访问控制规则。（如有需要，可将回退配置为本地身份源。）
- **辅助身份源** - 选择 Duo-LDAP 身份源。



d) 点击**下一步**。
e) 在“远程用户体验”(Remote User Experience) 页面上，选择您创建或编辑的**组策略 (Group Policy)**。



f) 点击此页面上的**下一步 (Next)** 和下一页上的“全局设置”(Global Settings)。
g) 点击**完成**，将更改保存至连接配置文件。

步骤 7 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

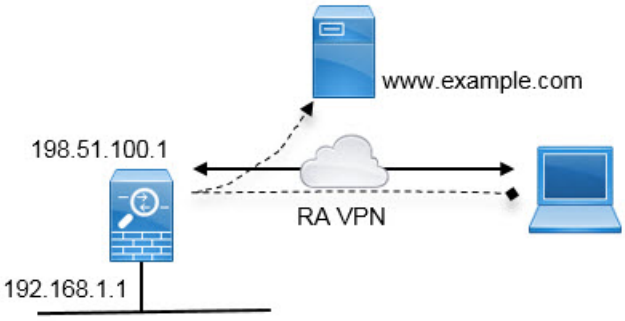
b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

如何在外部接口上为远程访问 VPN 用户提供互联网访问权限（发夹方法）

在远程访问VPN中，您可能希望远程网络用户通过您的设备访问互联网。不过，这些远程用户进入设备所用的接口与访问互联网所用的接口（外部接口）相同，因此需要使互联网流量从外部接口退出。这种技术有时候称为发夹方法。

下图展示了一个示例。外部接口 198.51.100.1 上配置了一个远程访问 VPN。您想要拆分远程用户的 VPN 隧道，以使退出的互联网流量重新回到外部接口，而流向内部网络的流量仍然流经设备。因此，如果远程用户想要访问互联网上的某个服务器（例如 www.example.com），连接会首先通过 VPN，然后从 198.51.100.1 接口路由回到互联网。



以下程序介绍如何配置此服务。

开始之前

此示例假定您已经注册设备、应用远程访问 VPN 许可证并上传 Secure Client 映像。同时还假定您已配置身份领域，并且此领域也用于身份策略。

过程

步骤 1 配置远程访问 VPN 连接。

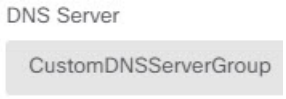
除连接配置文件外，配置还需要自定义的组策略。由于发夹为常见配置，且组策略中所需的设置通常是可用的，因此，在此示例中，我们将编辑默认组策略，而非创建新的组策略。您可以使用任一种方法。

a) 点击**设备** > **远程访问 VPN** 组中的**查看配置**。

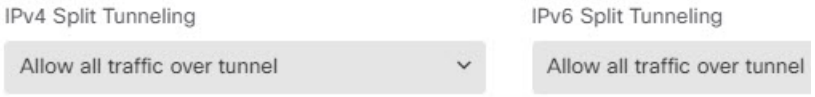
b) 点击目录中的**组策略**，然后点击 DfltGrpPolicy 对象的编辑图标 ( ) 。

c) 对默认组策略进行以下更改：

- 在 **DNS 服务器 (DNS Server)** 的**常规 (General)** 页面，选择定义服务器 VPN 终端在解析域名时应使用的 DNS 服务器组。



- 在**分割隧道 (Split Tunneling)** 页面上，为 **IPv4** 和 **IPv6 分割隧道 (IPv6 Split Tunneling)** 选择**允许所有流量通过隧道选项 (Allow all traffic over tunnel option)**。这是默认设置，因此它可能已正确配置。



注释 **此设置对启用发夹至关重要**。您希望所有流量都通过 VPN 网关，而分割隧道这种方法允许远程客户端直接访问 VPN 外部的本地或互联网站点。

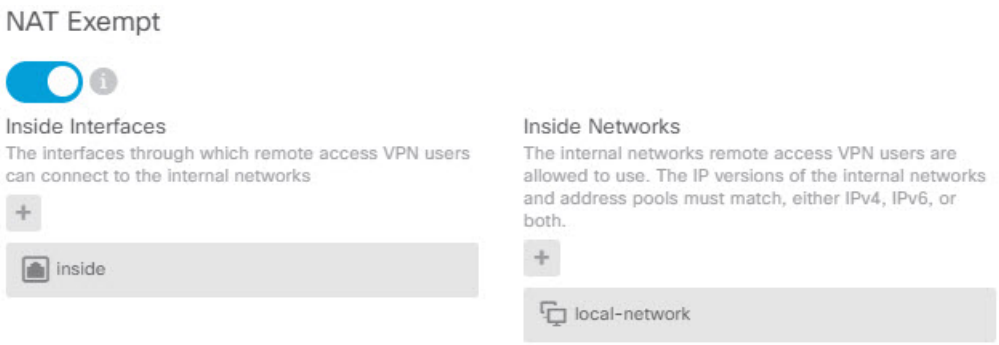
d) 点击**确定**，保存对默认组策略的更改。

e) 点击**连接配置文件**，编辑现有配置文件或创建新的配置文件。

f) 在连接配置文件中，就像配置任何其他 RA VPN 配置一样，按照向导程序操作并配置所有选项。但是，您必须正确配置以下选项才可启用发夹：

- 第 2 步中的**组策略**。选择需要为发夹自定义的组策略。

- 第 3 步中的 **NAT 豁免**。启用此功能。选择内部接口，然后选择定义内部网络的网络对象。在本示例中，该对象应指定 192.168.1.0/24。流向内部网络的 RA VPN 流量不会进行地址转换。但是，应用发夹方法的流量通过外部接口传出，因此这些流量仍会进行 NAT，因为 NAT 豁免仅适用于内部接口。请注意，如果您定义了其他连接配置文件，则需要将其添加到现有设置中，因为此配置适用于所有连接配置文件。



注释　**NAT 豁免**选项是另一个对发夹配置十分重要的设置。

g) （可选。）在**全局设置**步骤中，选择**为已解密流量绕过访问控制策略 (sysopt permit-vpn)** 选项。

选择此选项，则无需再配置访问控制规则以允许来自 RA VPN 地址池的流量通过。此选项可提供更好的安全性（外部用户无法骗取池中的地址），但会使得 RA VPN 流量不再会接受检查，包括 URL 过滤和入侵保护。请充分考虑此选项的优缺点再决定是否需要选择。

h) 查看远程访问 VPN 配置，然后点击**完成**。

步骤 2 将 NAT 规则配置为将外部接口发出的所有连接转换到外部 IP 地址上的端口（接口 PAT）。

完成初始设备配置后，系统将创建名为 InsideOutsideNatRule 的 NAT 规则。此规则将接口 PAT 应用于任意接口上通过外部接口流出设备的 IPv4 流量。由于外部接口包含在“任何”源接口中，因此，此规则已经存在，除非您对所需的规则进行编辑或将其删除。

以下程序介绍如何创建所需的规则。

a) 依次点击**策略** > **NAT**。

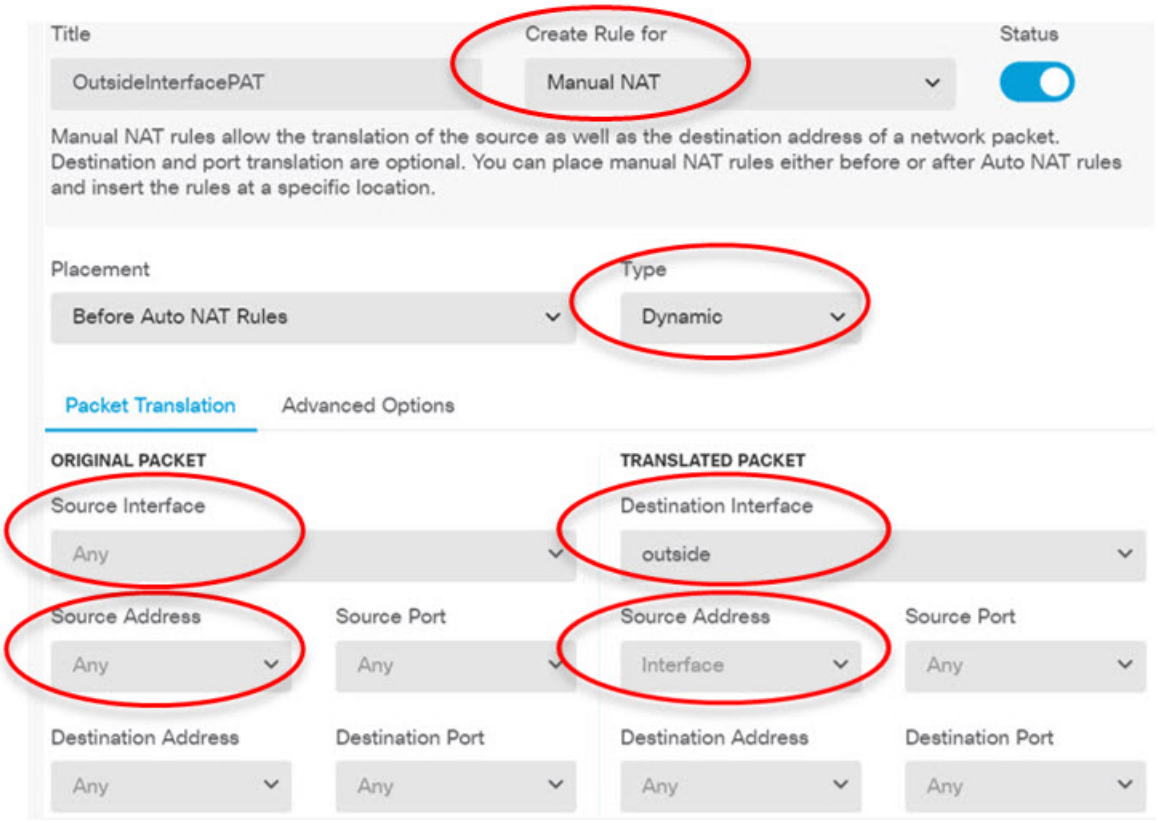
b) 执行以下操作之一：

- 要编辑 InsideOutsideNatRule，请将鼠标指针悬停在**操作**列上，然后点击编辑图标 ()。
- 要创建新规则，请点击 **+**。

c) 配置规则的以下属性：

- **名称** - 为新规则输入一个有意义且不含空格的名称。例如，OutsideInterfacePAT。
- **创建规则用于** - **手动 NAT**。
- **位置** - **自动 NAT 规则之前**（默认）。
- **类型** - **动态**。
- **原始数据包** - 对于**源地址**，请选择“任何”或 any-ipv4。对于**源接口**，请确保选择“任何”（默认值）。对于所有其他“原始数据包”选项，请保留默认值“任何”。
- **已转换的数据包** - 对于**目标接口**，请选择外部接口。对于**已转换的地址**，请选择**接口**。对于所有其他“已转换的数据包”选项，请保留默认值“任何”。

下图展示了选择“任何”作为源地址时的简单情况。



d) 点击**确定**。

步骤 3 （如果不在连接配置文件中配置**为已解密的流量绕过访问控制策略 (sysopt permit-vpn)**。）配置访问控制规则，以允许从远程访问 VPN 地址池进行访问。

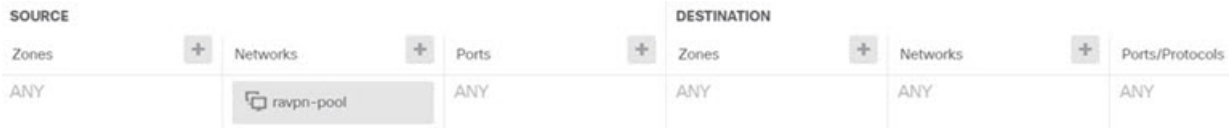
如果在连接配置文件中选择**为已解密的流量绕过访问控制策略 (sysopt permit-vpn)**，则来自 RA VPN 池地址的流量会绕过访问控制策略。您无法编写将应用于此流量的访问控制规则。仅当禁用此选项时，才需要编写规则。

在以下示例中，允许来自地址池的流量流至任何目标。您可以根据自己的具体要求调整此选项。也可以在此规则之前添加阻止规则，过滤掉不必要的流量。

a) 依次点击**策略** > **访问控制**。
b) 点击 + 创建新规则。
c) 配置规则的以下属性：

- **顺序** - 在策略中选择一个位置，此位置应位于可能会匹配并阻止这些连接的任何其他规则之前。默认情况下，会将该规则添加到策略的末尾。如果稍后需要重新调整规则的位置，可以编辑此选项，也可以直接将规则拖放到表格中相应的位置。
- **名称** - 输入一个有意义且不含空格的名称。例如，RAVPN-address-pool。
- **操作** - **允许**。如果不希望对此流量执行协议违规检测或入侵检测，可以选择“信任”。

- **源/目标**选项卡 - 对于**源** > **网络**，请选择在远程访问 VPN 连接配置文件中用于地址池的同一对象。对于所有其他“源”和“目标”选项，请保留默认值“任何”。



- **应用**、**URL** 和**用户**选项卡 - 保留这些选项卡的默认设置，即不做任何选择。
- **入侵**、**文件**选项卡 -（可选）您可以选择入侵或文件策略，以进行威胁或恶意软件检测。
- **日志记录**选项卡 -（可选）您可以选择启用连接日志记录。

d) 点击**确定 (OK)**。

步骤 4 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

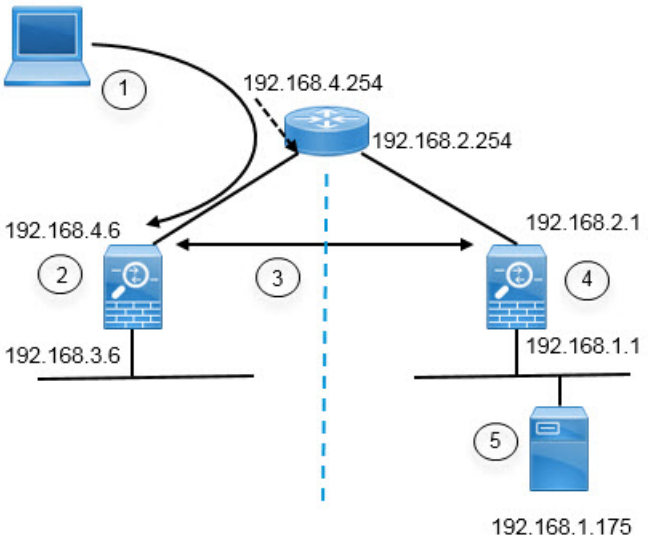
如何通过远程访问 VPN 使用外部网络上的目录服务器

您可以配置远程访问 VPN，以便移动员工和远程办公人员安全地连接到内部网络。此连接的安全性取决于您的目录服务器，该目录服务器对用户连接进行身份验证，以确保仅授权用户才能登录。

如果您的目录服务器位于外部网络而非内部网络上，则需要配置从外部接口到包含目录服务器的网络的站点间 VPN 连接。**站点间 VPN 配置有一个诀窍**：您必须将远程访问 VPN 设备的外部接口地址包括在站点间VPN连接的“内部”网络内，还必须将其包括在目录服务器所在设备的远程网络中。后续程序会对此加以说明。

注释 如果使用数据接口作为虚拟管理接口的网关，此配置还允许将目录用于身份策略。如果不使用数据接口作为管理网关，请确保存在从管理网络到参与站点间 VPN 连接的内部网络的路由。

此使用案例实施以下网络场景。



图中标注	说明
1	与 192.168.4.6 建立 VPN 连接的远程访问主机。客户端将在 172.18.1.0/24 地址池中获得一个地址。
2	站点 A，托管远程访问 VPN。
3	站点 A 和站点 B 威胁防御 设备的外部接口之间的站点间 VPN 隧道。
4	站点 B，托管目录服务器。
5	目录服务器，位于站点 B 的内部网络上。

开始之前

此使用案例假定您按照设备安装向导进行了正常的基准配置。具体包括：

- 有一条 Inside_Outside_Rule 访问控制规则，允许（或信任）从 inside_zone 到 outside_zone 的流量。
- inside_zone 和 outside_zone 安全区（分别）包含内部和外部接口。
- 有一个 InsideOutsideNATRule，对从内部接口到外部接口的所有流量执行接口 PAT。对于默认情况下使用内部网桥组的设备，可能存在多个接口 PAT 规则。
- 存在 0.0.0.0/0 的一条静态 IPv4 路由，指向外部接口。此示例假定您对外部接口使用静态 IP 地址，但也可以使用 DHCP 动态获取静态路由。在本示例中，我们假定采用以下静态路由：
  - 站点 A：外部接口，网关为 192.168.4.254。
  - 站点 B：外部接口，网关为 192.168.2.254。

过程

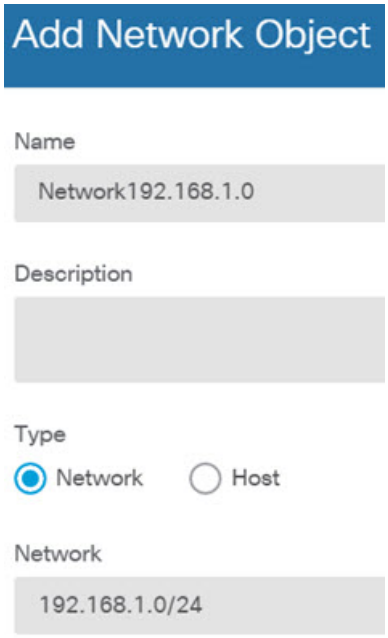
步骤 1 配置**站点 B**（托管目录服务器）上的站点间 VPN 连接。

a) 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。

b) 点击 + 按钮。

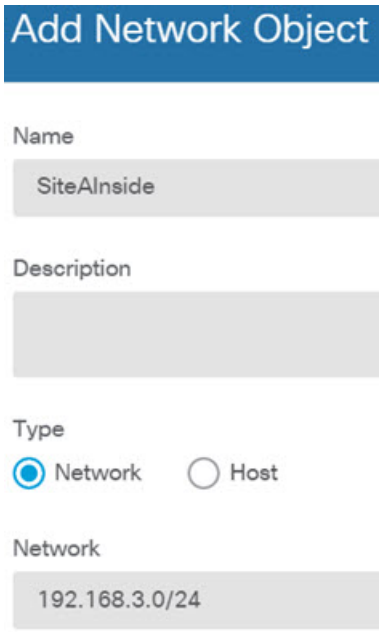
c) 为**终端设置**配置以下选项。

- **连接配置文件名称** - 输入名称，例如 SiteA（表示连接到站点 A）。
- **本地站点** - 这些选项定义本地终端。
  - **本地 VPN 访问接口** - 选择**外部**接口（图表中地址为 192.168.2.1 的那一个接口）。
  - **本地网络** - 点击 + 并选择标识应参与 VPN 连接的本地网络的网络对象。由于目录服务器在此网络上，因此可以参与站点间VPN。假定该对象尚不存在，点击**创建新网络**并为 192.168.1.0/24 网络配置对象。在保存对象后，在下拉列表中选择它并点击**确定**。

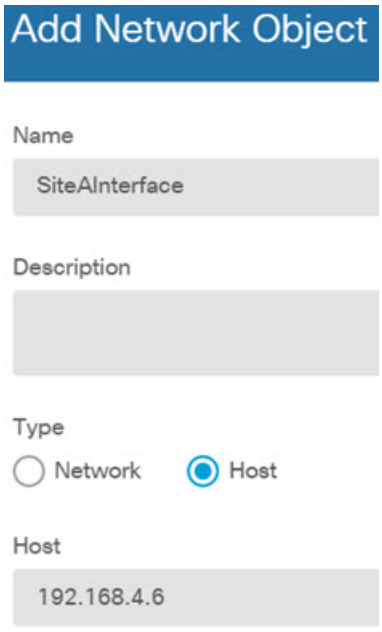


- **远程站点** - 这些选项定义远程终端。
  - **远程 IP 地址** - 输入 192.168.4.6，这是将托管 VPN 连接的远程 VPN 对等体接口的 IP 地址。
  - **远程网络** - 点击 + 并选择标识应参与 VPN 连接的远程网络的网络对象。点击**创建新网络**，配置以下对象，然后在列表中选择它们。

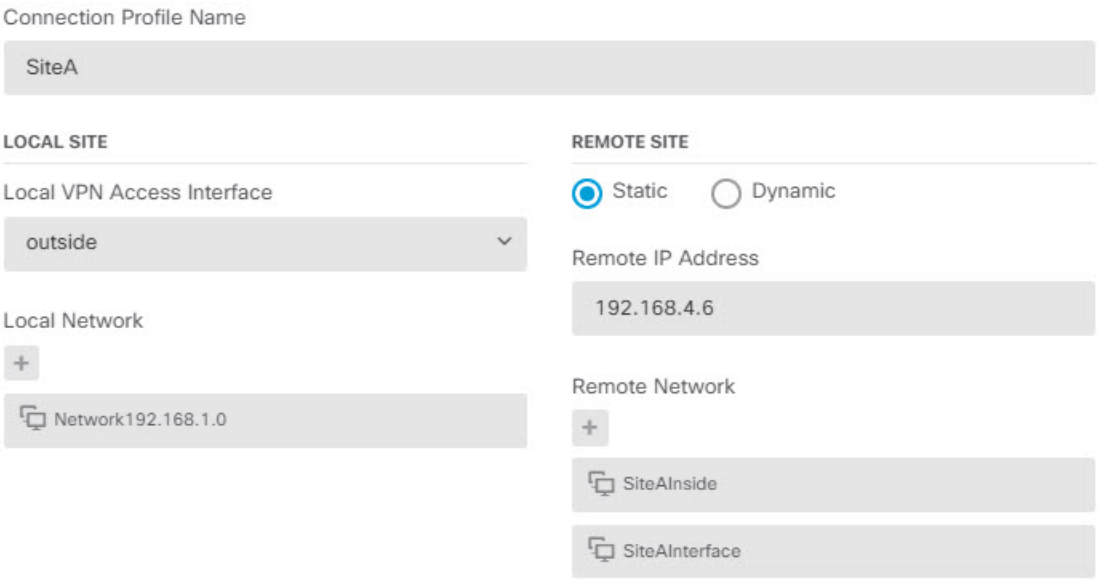
    1. SiteAInside，网络，192.168.3.0/24。



2. SiteAInterface，主机，192.168.4.6。这是关键：您必须将远程访问 **VPN** 连接点地址作为站点间 **VPN** 连接的远程网络的一部分，以便该接口上托管的 **RA VPN** 可以使用目录服务器。



完成后，终端设置应如下所示：



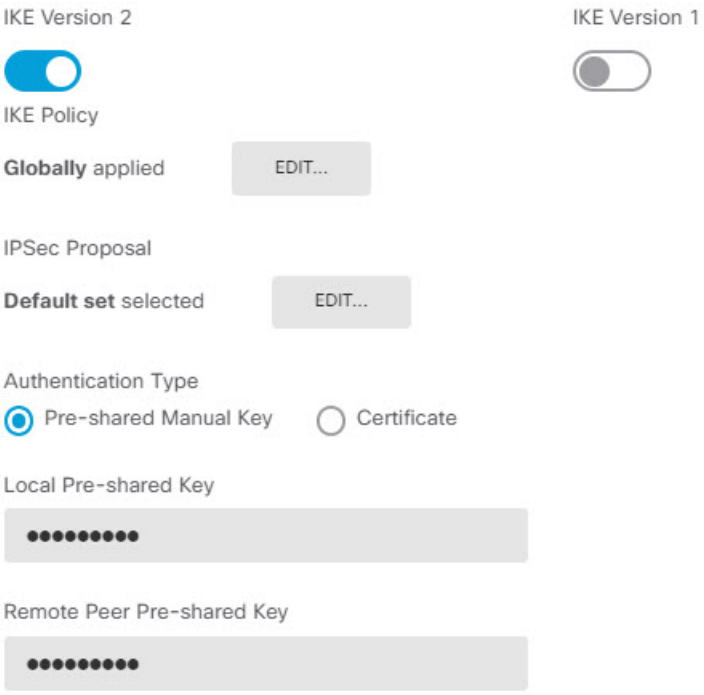
d) 点击**下一步**。

e) 定义 VPN 的隐私配置。

在本使用案例中，我们假定您符合出口控制功能的要求，允许使用强加密。调整这些示例设置以满足您的需求和许可证合规性。

- **IKE 版本 2**、**IKE 版本 1** - 保留默认设置，启用 **IKE 版本 2**，禁用 **IKE 版本 1**。
- **IKE 策略** - 点击**编辑**并启用 **AES-GCM-NULL-SHA** 和 **AES-SHA-SHA**，禁用 **DES-SHA-SHA**。
- **IPsec 提议** - 点击**编辑**。在“选择 IPSec 提议”对话框中，点击 **+**，然后点击**设置默认值**以选择默认 AES-GCM 提议。
- **本地预共享密钥**、**远程对等体预共享密钥** - 输入此设备和远程设备上为 VPN 连接定义的密钥。这些密钥在 IKEv2 中可能不同。该密钥可以有 1 至 127 个字母数字字符。**记住这些密钥，因为在站点 A 设备上创建站点间 VPN 连接时，必须配置相同的字符串**。

IKE 策略应如下所示：



f) 配置**其他选项**。

- **NAT 豁免** - 选择托管内部网络的接口，在本示例中为**内部**接口。通常，您不希望站点间 VPN 隧道中的流量转换其 IP 地址。此选项仅在本地网络驻留在单个路由接口（而非网桥组成员）后时有用。如果本地网络位于多个路由接口或一个或多个网桥组成员之后，则必须手动创建 NAT 豁免规则。有关手动创建所需规则的信息，请参阅使站点间 VPN 流量豁免 NAT，第 636 页。
- **完美前向保密的 Diffie-Hellman 组** - 选择**第 19 组**。此选项决定是否使用完美前向保密 (PFS) 为每个加密交换生成和使用唯一会话密钥。唯一会话密钥可保护交换免于后续解密，即使整个交换已被记录且攻击者已经获得终端设备使用的预共享密钥或私钥。有关选项的说明，请参阅决定要使用的 Diffie-Hellman 模数组，第 616 页。

该选项应如下所示：

g) 点击**下一步**。

h) 查看摘要并点击**完成**。

摘要信息将复制到剪贴板。您可以将这些信息粘贴到文档中，并使用它来帮助您配置远程对等体，或将其发送到负责配置对等体的一方。

i) 点击网页右上角的**部署更改**图标。

j) 点击**立即部署**按钮，并等待部署成功完成。

现在，站点 B 设备已准备好托管站点间 VPN 连接的一端。

步骤 2 注销**站点 B** 设备并登录**站点 A** 设备。

步骤 3 配置**站点 A**（托管远程访问 VPN）上的站点间 VPN 连接。

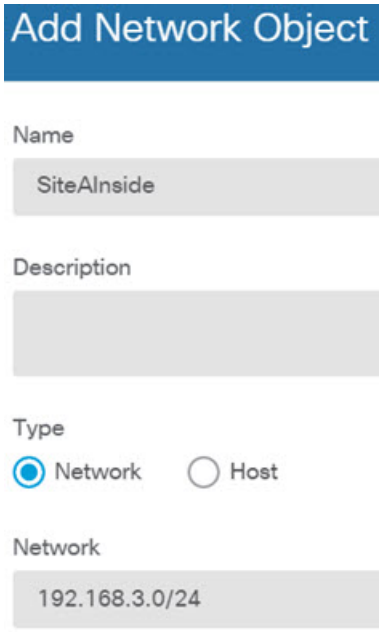
a) 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。

b) 点击 + 按钮。

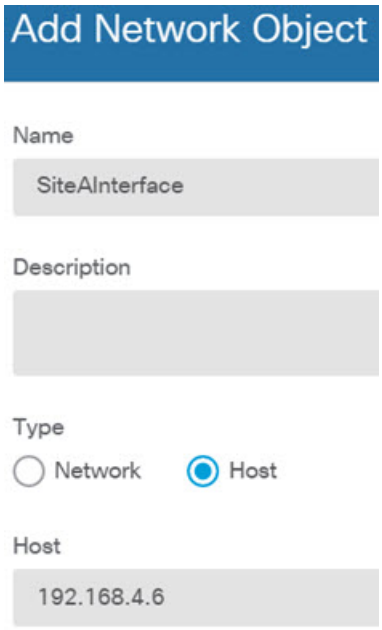
c) 为**终端设置**配置以下选项。

- **连接配置文件名称** - 输入名称，例如 SiteB（表示连接到站点 B）。
- **本地站点** - 这些选项定义本地终端。
  - **本地 VPN 接入接口** - 选择**外部**接口（图表中地址为 192.168.4.6 的那一个接口）。
  - **本地网络** - 点击 + 并选择标识应参与 VPN 连接的本地网络的网络对象。点击**创建新网络**，配置以下对象，然后在列表中选择它们。**注意，您已在站点 B 设备中创建相同的对象，但是您必须在站点 A 设备中重新创建它们。**

1. SiteAInside，网络，192.168.3.0/24。

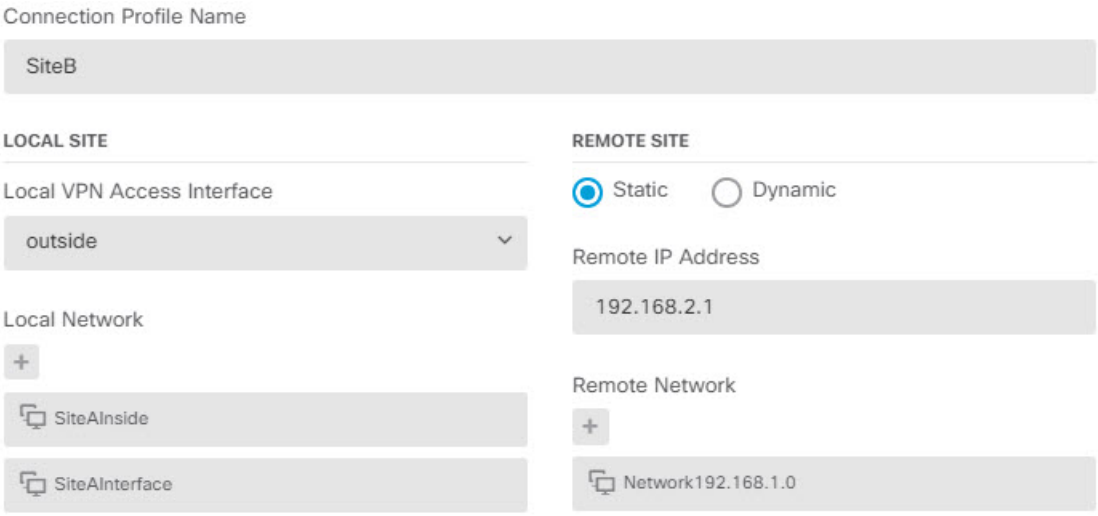


2. SiteAInterface，主机，192.168.4.6。**这是关键：您必须将远程访问 VPN 连接点地址作为站点间 VPN 连接的内部网络的一部分，以便该接口上托管的 RA VPN 可以使用远程网络上的目录服务器。**



- **远程站点** - 这些选项定义远程终端。
  - **远程 IP 地址** - 输入 192.168.2.1，这是将托管 VPN 连接的远程 VPN 对等体接口的 IP 地址。
  - **远程网络** - 点击 **+** 并选择标识应该参与 VPN 连接的远程网络的网络对象（包含目录服务器的 VPN 连接）。点击**创建新网络**并为 192.168.1.0/24 网络配置对象。在保存对象后，在下拉列表中选择它并点击**确定**。**注意，您已在站点 B 设备中创建相同的对象，但是您必须在站点 A 设备中重新创建它。**

完成后，终端设置应如下所示。请注意，与站点 B 设置相比，本地/远程网络是相反的。点对点连接的两端看起来应始终是这样的。

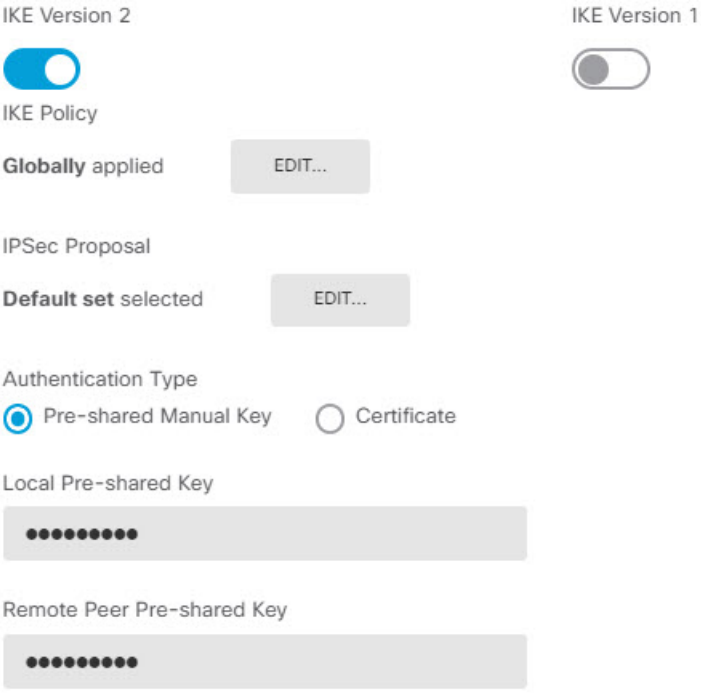


d) 点击**下一步**。

e) 定义 VPN 的隐私配置。

与站点 B 连接一样，配置相同的 IKE 版本、策略和 IPsec 提议，以及相同的预共享密钥，**但请确保调换本地和远程预共享密钥**。

IKE 策略应如下所示：



f) 配置**其他选项**。

- **NAT 豁免** - 选择托管内部网络的接口，在本示例中为**内部**接口。通常，您不希望站点间 VPN 隧道中的流量转换其 IP 地址。此选项仅在本地网络驻留在单个路由接口（而非网桥组成员）后时有用。如果本地网络位于多个路由接口或一个或多个网桥组成员之后，则必须手动创建 NAT 豁免规则。有关手动创建所需规则的信息，请参阅使站点间 VPN 流量豁免 NAT，第 636 页。
- **完美前向保密的 Diffie-Hellman 组** - 选择**第 19 组**。

该选项应如下所示：

g) 点击**下一步**。
h) 查看摘要并点击**完成**。
i) 点击网页右上角的**部署更改**图标。

j) 点击**立即部署**按钮，并等待部署成功完成。

现在，站点 A 设备已准备好托管站点间 VPN 连接的另一端。由于站点 B 已经配置了兼容设置，因此两台设备应该协商 VPN 连接。

您可以登录设备 CLI 并对目录服务器进行 ping 测试，从而确认连接。您也可以使用 **show ipsec sa** 命令查看会话信息。

步骤 4 在**站点 A** 上配置目录服务器。点击**测试**验证是否有连接。

a) 选择**对象**，然后从目录中选择**身份源**。
b) 点击 **+** > **AD**。
c) 配置基本领域属性。

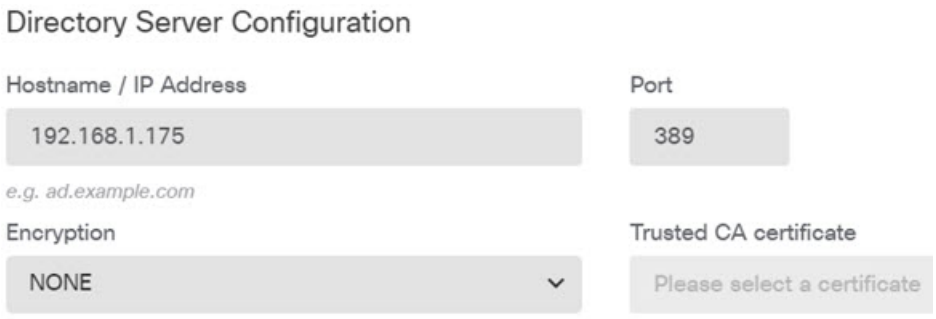
- **名称** - 目录领域的名称。例如，AD。
- **类型** - 目录服务器的类型。Active Directory 是唯一支持的类型，所以无法更改此字段。
- **目录用户名**、**目录密码** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

  注释 系统使用此信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=adminisntrator、cn=users、dc=example、dc=com。请注意，cn = users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

- **基准 DN** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如，cn=users,dc=example,dc=com。有关查找基准 DN 的信息，请参阅确定目录基准标识名，第 154 页。
- **AD 主域** - 设备应加入的 Active Directory 完全限定域名。例如 example.com。

d) 配置目录服务器属性。

- **主机名/IP 地址** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。在本例中，输入 192.168.1.175。
- **端口** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。在本例中，保留 389。
- **加密** - 使用加密连接下载用户和组信息。系统默认为**无**，也就是说以明文形式下载用户和组信息。对于 RA VPN，您可以使用 **LDAPS**，即基于 SSL 的 LDAP。如果选择此选项，则使用端口 636。RA VPN 不支持 STARTTLS。对于此示例，选择**无**。
- **受信任的 CA 证书** - 如果选择加密方法，请上传证书颁发机构 (CA) 证书以便在系统和目录服务器之间启用受信任的连接。如果要使用证书进行身份验证，则证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 192.168.1.175 作为 IP 地址，但证书中的地址为 ad.example.com，则连接会失败。



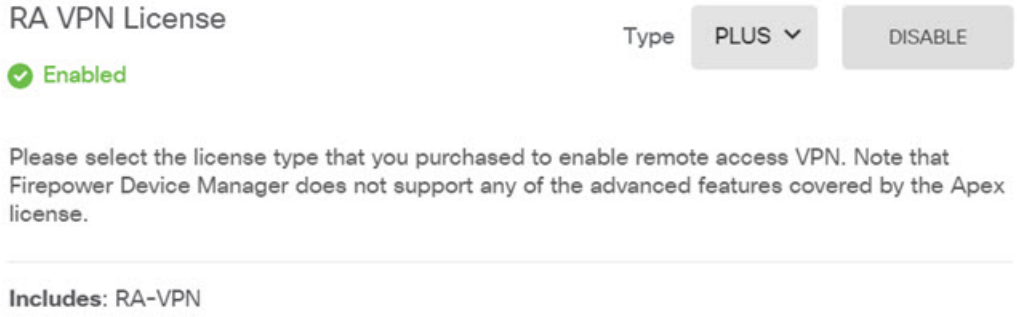
e) 点击**测试**按钮验证系统是否可以与服务器通信。

系统使用单独的进程访问服务器，因此您可能会收到错误通知，指出连接适用于一种用途而不适用于另一种用途，例如可用于身份策略，但不可用于远程访问 VPN。如果无法访问服务器，请确认 IP 地址和主机名正确、DNS 服务器具有该主机名的条目等。另外，验证站点间 VPN 连接是否正常工作，并且您在 VPN 中包含了站点 A 的外部接口地址，并且 NAT 不会转换目录服务器的流量。您可能还需要为服务器配置静态路由。

f) 点击**确定**。

步骤 5 依次点击**设备** > **智能许可证** > **查看配置**，然后启用 RA VPN 许可证。

启用 RA VPN 许可证时，请选择您购买的许可证类型：Plus、Apex（或两者）或仅 VPN。有关详细信息，请参阅远程访问 VPN 的许可要求，第 661 页。

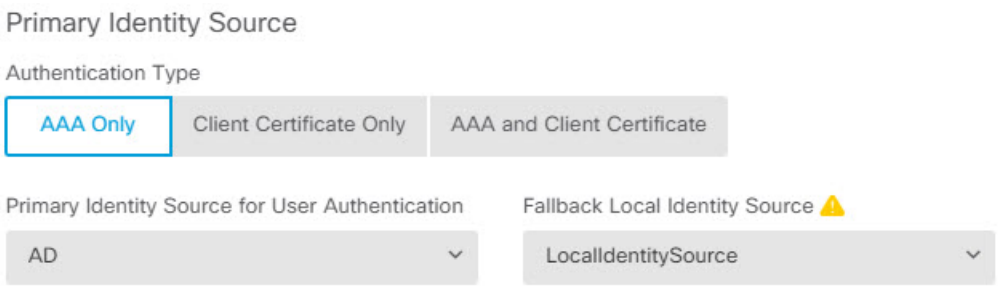


步骤 6 在站点 A 上配置远程访问 VPN。

a) 点击**设备** > **远程访问 VPN** 组中的**查看配置**。确保您位于**连接配置文件 (Connection Profiles)** 页面。

b) 创建或编辑连接配置文件。

c) 在向导的第一步中，设置配置文件名称，然后选择 AD 领域作为主身份验证源。或者，您可以选择本地数据库作为备用身份源。



d) 配置地址池。

对于本示例，点击 +，然后在 IPv4 地址池中选择**创建新的网络**，并为 172.18.1.0/24 网络创建一个对象，然后选择此对象。从该地址池中为客户端分配地址。将 IPv6 池留空。地址池不能与外部接口的 IP 地址位于同一子网。

该对象应如下所示：

该地址池规范应如下所示：

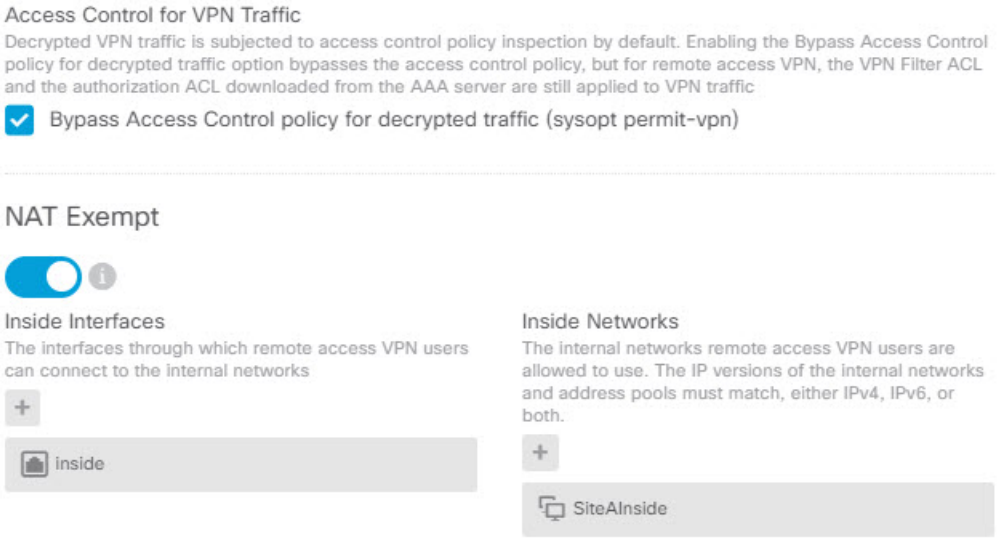
e) 点击**下一步**，然后选择适当的组策略。

选中您选择的策略的摘要信息。确保已配置 DNS 服务器。如果未配置，请立即编辑策略并配置 DNS。

f) 点击**下一步**，并在全局设置中，选择**为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** 选项，并配置 **NAT 豁免**选项。

对于 **NAT 豁免**，您需要配置以下选项。请注意，如果您定义了其他连接配置文件，则需要将其添加到现有设置中，因为此配置适用于所有连接配置文件。

- **内部接口** - 选择**内部**接口。这些是远程用户将要访问的内部网络的接口。所创建的 NAT 规则用于这些接口。
- **内部网络** - 选择 SiteAInside 网络对象。这些是代表远程用户将访问的内部网络的网络对象。



g) 上传适用于受支持平台的 Secure Client 软件包。

h) 点击**下一步**并验证设置。

首先，验证摘要是否正确。

然后，点击 **说明** 查看最终用户初步安装 Secure Client 软件需要做什么，并测试他们是否可以完成 VPN 连接。点击**复制**以将这些说明复制到剪贴板，然后将它们粘贴在文本文件或邮件中。

i) 点击**完成**。

步骤 7 点击网页右上角的**部署更改**图标。

步骤 8 点击**立即部署**按钮，并等待部署成功完成。

现在，站点 A 设备已准备好接受 RA VPN 连接。让外部用户安装 Secure Client 客户端并完成 VPN 连接。

您可以登录设备 CLI 并使用 **show vpn-sessiondb anyconnect** 命令查看会话信息，从而确认连接。

如何通过组控制 RA VPN 访问

您可以配置远程访问VPN连接配置文件，以根据组策略提供对内部资源的差异化访问权限。例如，如果您想要向员工提供不受限制的访问权限，但仅向承包商提供单个　内部网络的访问权限，则可以使用组策略来定义不同的 ACL，以适当地限制访问。

以下示例展示了如何为应只能访问 192.168.2.0/24 内部子网的承包商设置 RA VPN 连接。对于常规员工，您可以使用默认组策略，其中没有为VPN定义流量过滤器。如果您想要对这些用户设置限制，并应用按照以下方法构建的 ACL，则可以编辑默认组策略。

开始之前

此程序假定您已创建要用于承包商的身份源。此身份源可能不同于您用于常规员工的身份源。由于此身份源并非与限制访问严格相关，因此我们可以在本示例中忽略它。

此示例还假设“inside2”接口配置为托管 192.168.2.0/24 子网，其 IP 地址为 192.168.2.1（子网上的任何其他地址也是可接受的）。

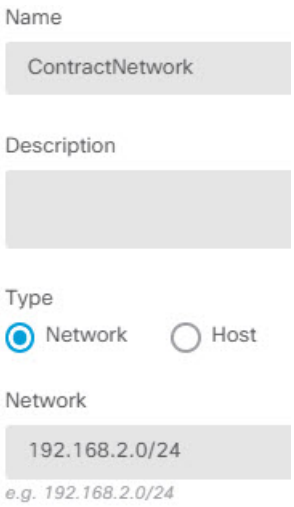
过程

步骤 1 配置扩展访问控制列表 (ACL)，以限制 RA VPN 流量。

您需要先配置定义目标 192.168.2.0/24 的网络对象，然后创建 Smart CLI 对象，定义此访问列表。由于 ACL 在末尾包含隐式拒绝语句，因此您需要仅允许对子网的访问，且定向至子网外部任何 IP 地址的流量将被拒绝。此示例仅适用于 IPv4；您还可以配置对象，来限制对特定子网的 IPv6 访问。只需创建网络对象并将基于 IPv6 的 ACE 添加到相同的 ACL。

a) 依次选择**对象** > **网络**，并创建所需的对象。

例如，将对象命名为 ContractNetwork。此对象应与以下所示类似：

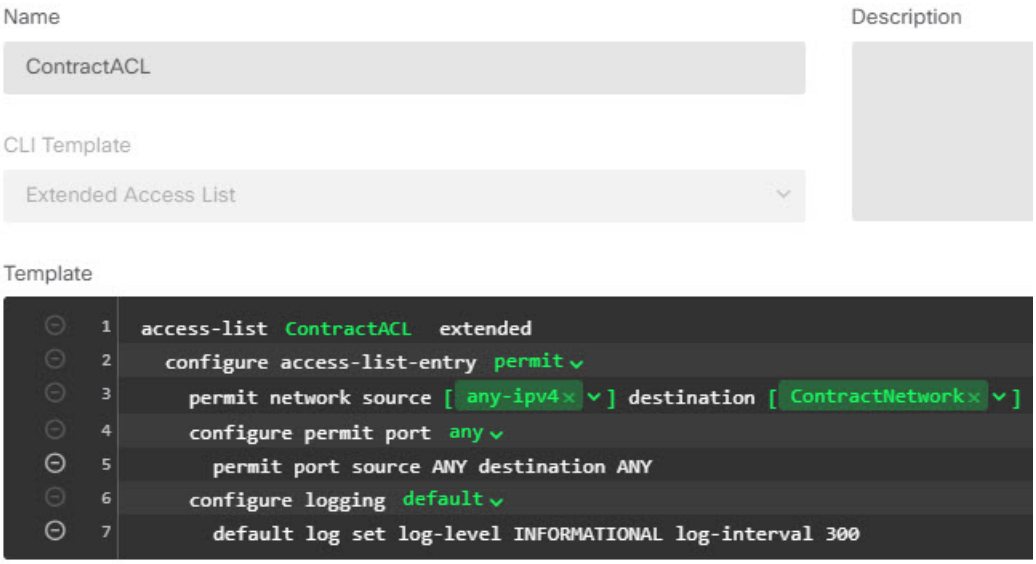


b) 选择**设备** > **高级配置** > **Smart CLI** > **对象**。
c) 点击 **+** 创建新对象。
d) 输入 ACL 的名称。例如，**ContractACL**。
e) 对于 **CLI 模板**，选择**扩展访问列表**。
f) 在**模板**正文中进行以下配置：

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = ContractNetwork object
- configure permit port = any

- configure logging = default

ACE 应如下所示：



g) 点击**确定 (OK)**。

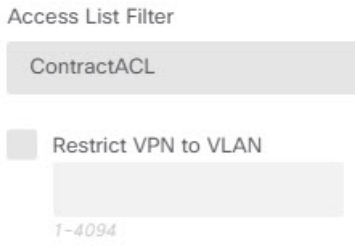
在下次部署更改时会配置此 ACL。无需在任何其他策略中使用此对象来强制部署。

步骤 2 创建使用此 ACL 的组策略。

您至少还需要为组策略配置DNS服务器。您可以根据需要配置其他选项。以下步骤重点介绍与此使用案例相关的一个设置。

a) 依次选择**设备** > **RA VPN** > **组策略**。
b) 点击+，创建新的组策略。
c) 在**常规 (General)**页面中，输入策略名称，例如 **ContractGroup**。
d) 点击目录中的**流量过滤器**。
e) 对于**访问列表过滤器**，选择 ContractACL 对象。

对于本示例，将 VLAN 选项留空。请注意，您也可以设置一个 VLAN 用于过滤，并为 VLAN 配置子接口。



f) 点击**确定**保存组策略。

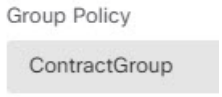
步骤 3 配置适用于承包商的连接配置文件。

a) 在 RA VPN 页面上，点击目录中的**连接配置文件 (Connection Profiles)**。
b) 点击 **+**，创建新的连接配置文件。
c) 完成向导的第 1 步，然后点击**下一步**。

输入配置文件的名称，例如，Contractors。

按照惯常做法配置其余选项。包括为承包商选择适当的身份验证源和定义地址池。

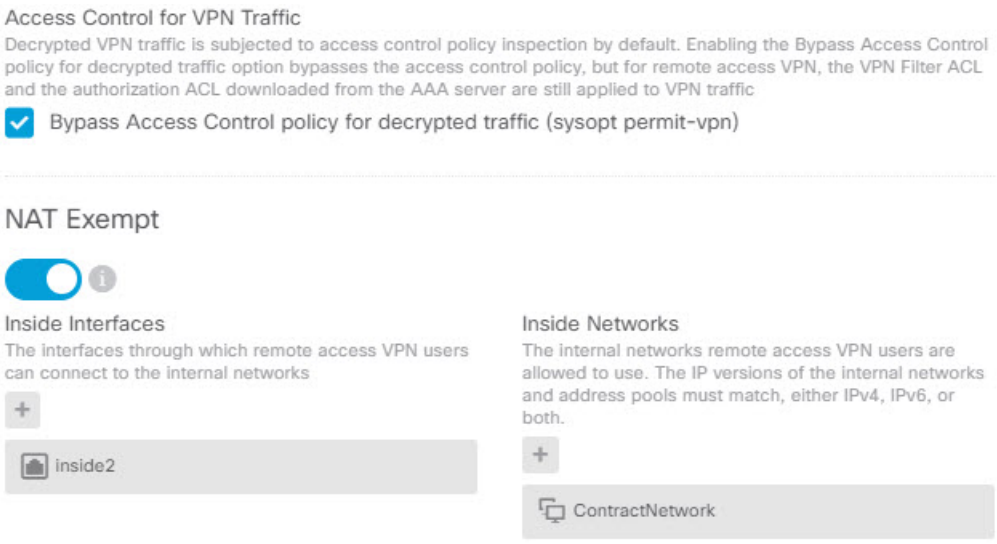
d) 选择为承包商配置的组策略，然后点击**下一步**。



e) 在全局设置中，选择**为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** 选项，并配置 **NAT 豁免**选项。

对于 **NAT 豁免**，您需要配置以下选项。请注意，如果您定义了其他连接配置文件，则需要将其添加到现有设置中，因为此配置适用于所有连接配置文件。

- **内部接口** - 选择 **inside2** 接口。这些是远程用户将要访问的内部网络的接口。所创建的 NAT 规则用于这些接口。
- **内部网络** - 选择 ContractNetwork 网络对象。这些是代表远程用户将访问的内部网络的网络对象。



f) 上传适用于受支持平台的 Secure Client 软件包。
g) 点击**下一步**并验证设置。

首先，验证摘要是否正确。

然后，点击 **说明** 查看最终用户初步安装 Secure Client 软件需要做什么，并测试他们是否可以完成 VPN 连接。点击**复制**以将这些说明复制到剪贴板，然后将它们粘贴在文本文件或邮件中。

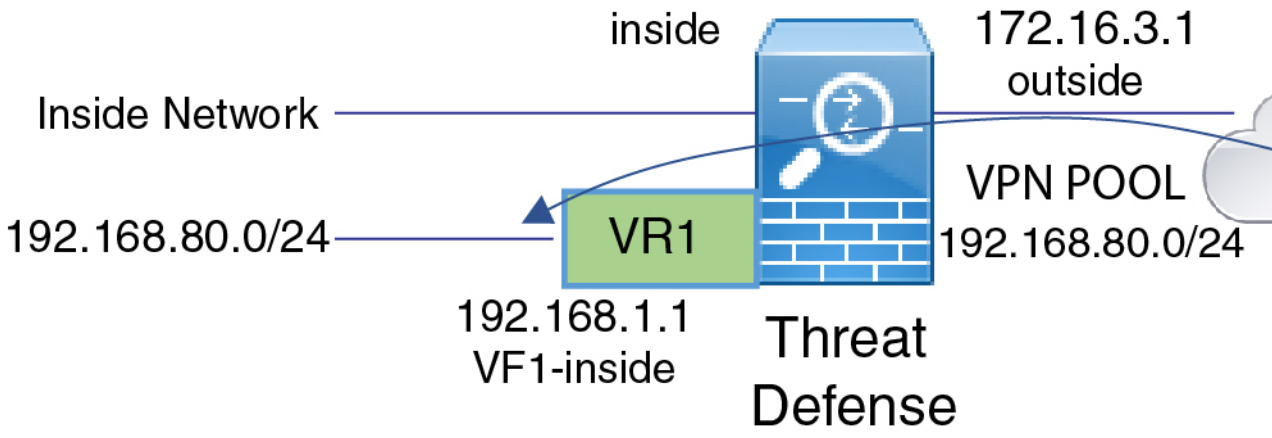
h) 点击**完成**。

如何对不同虚拟路由器中的内部网络进行 RA VPN 访问

如果在设备上配置多个虚拟路由器，则必须在全局虚拟路由器中配置 RA VPN。不能在分配给自定义虚拟路由器的接口上配置 RA VPN。

由于虚拟路由器的路由表是独立的，因此，如果RA VPN用户需要访问属于不同虚拟路由器的网络，则必须创建静态路由。

请考虑以下示例。在这种情况下，RA VPN 用户连接到地址为 172.16.3.1 的外部接口，并在 192.168.80.0/24 池中获得IP地址。此时，该用户可以访问连接到全局虚拟路由器的内部网络。但是，该用户无法访问属于虚拟路由器 VR1 的 192.168.1.0/24 网络。要允许 VR1 网络和 RA VPN 用户之间的流量传输，必须配置双向静态路由。



开始之前

此示例假设您已配置 RA VPN，定义虚拟路由器，配置接口并将其分配给相应的虚拟路由器。

过程

步骤 1 配置从全局虚拟路由器到 VR1 的路由泄漏。

此路由允许在 VPN 池中分配 IP 地址的 Secure Client访问 VR1 虚拟路由器中的 192.168.1.0/24 网络。

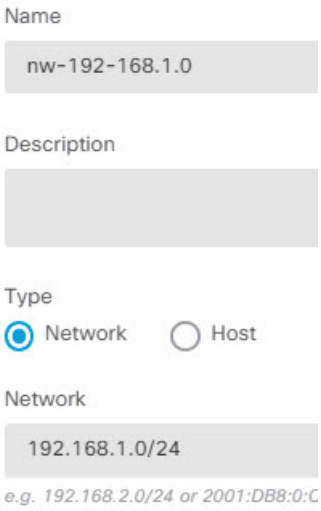
a) 依次选择**设备** > **路由** > **查看配置**。

b) 点击全局虚拟路由器的查看图标 ( )。

c) 在全局路由器的**静态路由**选项卡上，点击 + 并配置路由：

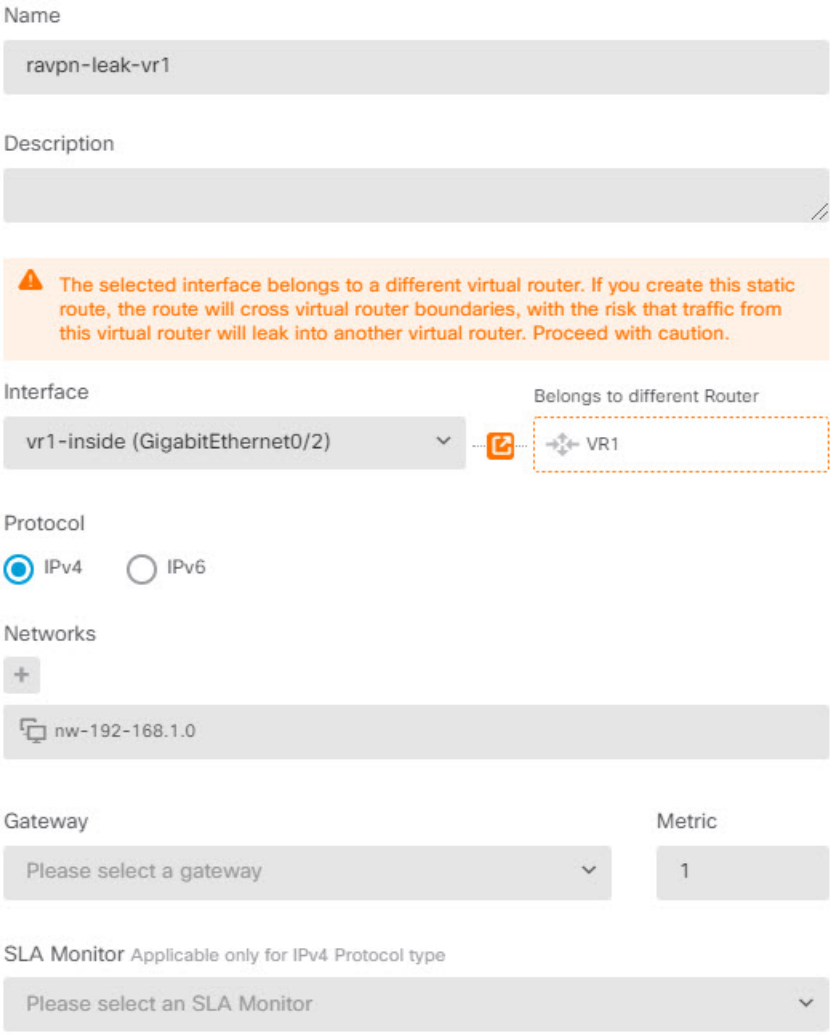
- **名称** - 可以使用任何名称，例如 **ravpn-leak-vr1**。
- **接口** - 选择 **vr1-inside**。

- **协议** - 选择 **IPv4**。
- **网络** - 选择定义 192.168.1.0/24 网络的对象。如有需要，请点击**创建新网络**立即创建对象。



- **网关** - 将此项目留空。将路由泄漏到另一个虚拟路由器时，您不必选择网关地址。

对话框应如下所示：



d) 点击**确定**。

步骤 2 配置从 VR1 到全局虚拟路由器的路由泄漏。

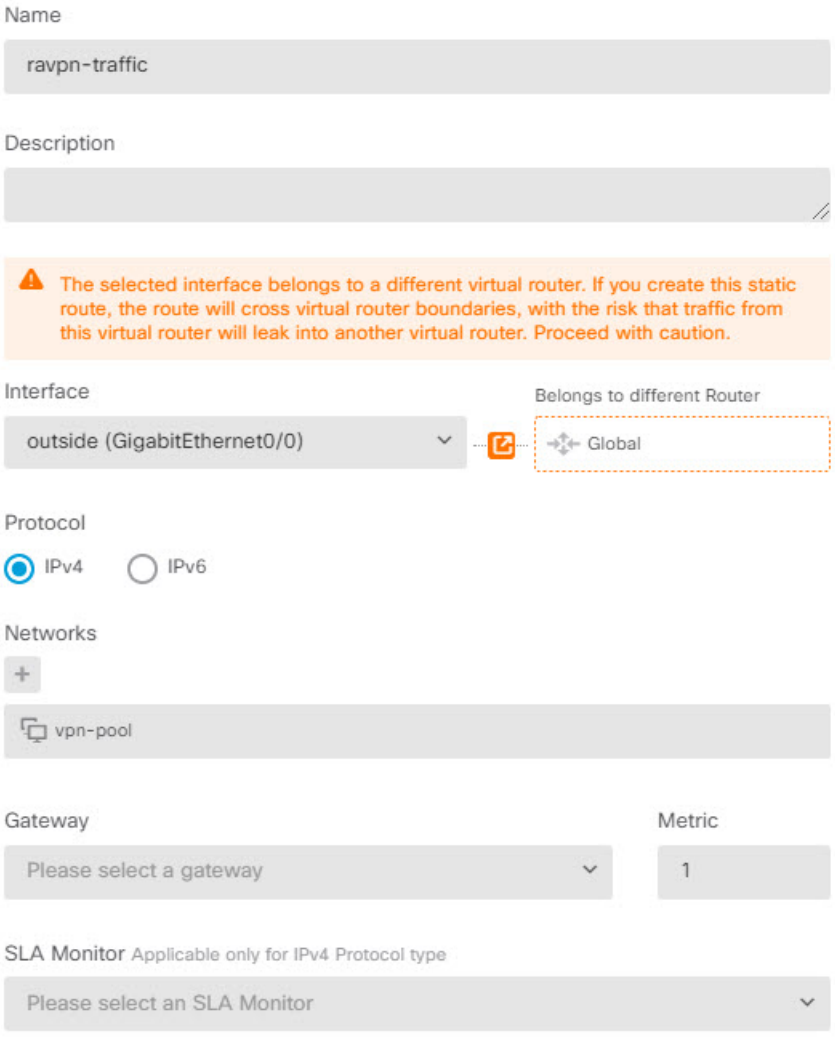
此路由允许 192.168.1.0/24 网络上的终端向在 VPN 池中分配 IP 地址的 Secure Client发起连接。

a) 从虚拟路由器下拉列表中选择 **VR1**，以切换至 VR1 配置。

b) 在 VR1 虚拟路由器的**静态路由**选项卡上，点击 **+** 并配置路由：

- **名称** - 可以使用任何名称，例如 **ravpn-traffic**。
- **接口** - 选择 **outside**。
- **协议** - 选择 **IPv4**。
- **网络** - 选择为 VPN 池创建的对象，例如 **vpn-pool**。
- **网关** - 将此项目留空。将路由泄漏到另一个虚拟路由器时，您不必选择网关地址。

对话框应如下所示：



c) 点击**确定 (OK)**。

下一步做什么

如果 RA VPN 地址池与自定义虚拟路由器中的 IP 地址之间存在重叠，则还必须对 IP 地址使用静态 NAT 规则，以启用正确的路由。但是，更简单的方法是，直接更改 RA VPN 地址池，使其不存在重叠。

如何自定义 Secure Client 图标和徽标

您可以在 Windows 和 Linux 客户端计算机上自定义 Secure Client 应用的图标和徽标。图标的名称是预定义的，并且对您上传的图像的文件类型和大小有特定限制。

虽然您在部署自己的可执行文件以自定义 GUI 时可以使用任何文件名，但本示例假设您只是在不部署完全自定义框架的情况下交换图标和徽标。

您可以替换许多图像，其文件名因平台而异。有关自定义选项、文件名、类型和大小的完整信息，请参阅 *Cisco* 安全客户端管理员指南中有关自定义和本地化 Secure Client 和安装程序的章节。例如，在以下位置可以找到 4.8 客户端的相应章节：

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/customize-localize-anyconnect.html

开始之前

在本示例中，我们将替换 Windows 客户端的以下图像。请注意，如果图像的大小与最大值不同，系统会自动将其调整为最大值，并在必要时扩展图像。

- app_logo.png

  此应用徽标图像是应用图标，最大大小为 128 x 128 像素。

- company_logo.png

  此公司徽标图像显示在托盘浮出控件左上角和“高级”对话框中。最大大小为 97 x 58 像素。

- company_logo_alt.png

  “关于”对话框右下角显示备用公司徽标图像。最大大小为 97 x 58 像素。

要上传这些文件，必须将其放置在 威胁防御 设备可以访问的服务器上。您可以使用 TFTP、FTP、HTTP、HTTPS 或 SCP 服务器。根据服务器设置的要求，从这些文件获取图像的 URL 可以包括路径和用户名/密码。此示例将使用 TFTP。

过程

步骤 1 将图像文件上传到充当 RA VPN 头端且应使用自定义图标和徽标的每个 威胁防御 设备。

a) 使用 SSH 客户端登录设备 CLI。

b) 在 CLI 中，输入 **system support diagnostic-cli** 命令以进入诊断 CLI 模式。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv1>
```

注释 阅读消息！您必须按 **Ctrl+a，然后按 d**，才能退出诊断 CLI 并返回正常的 威胁防御 CLI 模式。

c) 请注意命令提示符。普通 CLI 仅使用 >，而诊断 CLI 的用户执行模式使用主机名加 >。在本例中为 ftdv1>。您需要进入特权执行模式，该模式使用 **#** 作为结束字符，例如 ftdv1#。如果提示符已包含 **#**，请跳过此步骤。否则，请输入 enable 命令，并在密码提示时按 Enter 键，而不输入密码。

```
ftdv1> enable
Password:
ftdv1#
```

d) 使用 **copy** 命令将每个文件从托管服务器复制到 威胁防御 设备的 disk0。您可以将它们放在子目录中，例如 disk0:/anyconnect-images/。您可以使用 **mkdir** 命令创建新文件夹。

例如，如果 TFTP 服务器的 IP 地址为 10.7.0.80，并且您想要创建新目录，则命令将类似于以下内容。请注意，第一个示例后省略了对 **copy** 命令的响应。

```
ftdv1# mkdir disk0:anyconnect-images

Create directory filename [anyconnect-images]? yes

Created dir disk0:/anyconnect-images

ftdv1# copy /noconfirm tftp://10.7.0.80/app_logo.png
disk0:/anyconnect-images/app_logo.png

Accessing tftp://10.7.0.80/app_logo.png...!!!!!!
Writing file disk0:/anyconnect-images/app_logo.png...
!!!!!!
12288 bytes copied in 1.000 secs (12288 bytes/sec)

ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo.png
disk0:/anyconnect-images/company_logo.png
ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo_alt.png
disk0:/anyconnect-images/company_logo_alt.png
```

步骤 2 在诊断 CLI 中使用 **import webvpn** 命令指示 AnyConnect 在客户端计算机上安装 Secure Client 时下载这些图像。

import webvpn AnyConnect-customization type resource platform win name *filename* **disk0:/***directoryname/filename*

此命令适用于 Windows。对于 Linux，请根据您的客户端的需要，将 **win** 关键字替换为 **linux** 或 **linux-64**。

例如，要导入上一步中上传的文件，假设我们仍在诊断 CLI 中：

```
ftdv1# import webvpn AnyConnect-customization type resource platform win
name app_logo.png disk0:/anyconnect-images/app_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo.png disk0:/anyconnect-images/company_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png disk0:/anyconnect-images/company_logo_alt.png
```

步骤 3 确认配置：

- 要验证导入的文件，请在诊断 CLI 特权执行模式下使用 **show import webvpn AnyConnect-customization** 命令。
- 要验证图像是否已下载到客户端，这些图像应在用户运行客户端时显示。您还可以在 Windows 客户端上检查以下文件夹，其中 %PROGRAMFILES% 通常解析为 c:\Program Files。

  %PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res

下一步做什么

如果要恢复默认图像，请对自定义的每个图像使用 **revert webvpn** 命令（在诊断 CLI 特权执行模式下）。命令为：

revert webvpn AnyConnect-customization type resource platform win name *filename*

与 **import webvpn** 一样，如果您已自定义这些客户端平台，请将 **win** 替换为 **linux** 或 **linux-64**，并为导入的每个图像文件名单独发出该命令。例如：

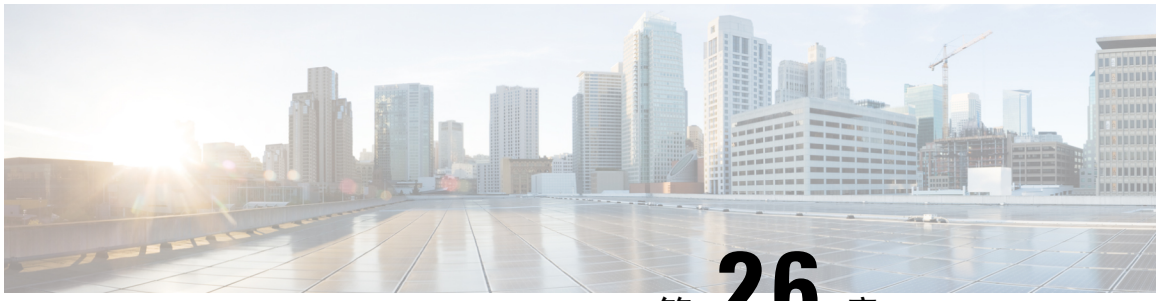
```
ftdv1# revert webvpn AnyConnect-customization type resource platform win
name app_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png
```

第 VII 部分

系统管理



第 26 章

系统设置

以下主题介绍如何配置一起划分到“系统设置”(System Settings) 页面的各种系统设置。这些设置涵盖整个系统功能。

配置管理访问

管理访问指能够登录到 威胁防御 设备进行配置和监控。您可以配置以下项目：

- AAA 用于确定要用于用户访问身份验证的身份源。您可以使用本地用户数据库或外部 AAA 服务器。有关管理用户管理的详细信息，请参阅管理 设备管理器 和 威胁防御 用户访问， 第 785 页。
- 针对管理接口和数据接口的访问控制。对于这些接口有单独的访问列表。您可以决定允许哪些 IP 地址访问 HTTPS（用于 设备管理器）和 SSH（用于 CLI）。请参阅配置管理访问列表， 第 728 页。

- 管理 Web 服务器证书，用户必须接受它们才能连接到 设备管理器。通过上传网络浏览器已信任的证书，可以避免用户被要求信任未知的证书。请参阅配置 威胁防御 Web 服务器证书，第 730 页。

配置管理访问列表

默认情况下，您可以从任何 IP 地址的管理地址访问设备的 设备管理器 Web 或 CLI 界面。系统访问仅受用户名/密码的保护。但是，您可以配置访问列表以仅允许来自特定 IP 地址或子网的连接，以进一步加强保护。

您还可以开放数据接口以允许 设备管理器 或 SSH 连接至 CLI。然后，无需使用管理地址即可管理设备。例如，您可以允许对外部接口进行管理访问，这样就能远程配置设备。用户名/密码可防止不希望看到的连接。默认情况下，对数据接口的 HTTPS 管理访问会在内部接口上启用而在外部接口上禁用。对于具有默认“内部”网桥组的 Firepower 1010 这意味着可以 设备管理器 通过网桥组中的任意数据接口与网桥组 IP 地址建立连接（默认值为 192.168。95.1）建立 Firepower 设备管理器连接。您可以只在进入设备所通过的接口上开放管理连接。

注意 如果只允许访问特定地址，那么您可能很容易将自己锁定在系统之外。如果删除对当前所用 IP 地址的访问，并且没有“任何”地址条目，则在部署策略时将丢失对系统的访问。如果决定配置访问列表，必须非常小心。

开始之前

不能在同一接口上为同一 TCP 端口同时配置 设备管理器 访问（HTTPS 访问）和远程访问 SSL VPN。例如，如果在外部接口上配置远程访问 SSL VPN，则也无法在端口 443 上打开 HTTPS 连接的外部接口。如果在同一接口上配置这两个功能，请确保至少更改其中一项服务的 HTTPS 端口，以避免冲突。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **管理访问**链接。

如果您已位于“系统设置”(System Settings) 页面，只需点击目录中的**管理访问 (Management Access)**。

您还可以在此页面上配置 AAA，允许外部 AAA 服务器中定义的用户进行管理访问。有关详细信息，请参阅管理 设备管理器 和 威胁防御 用户访问，第 785 页。

步骤 2 要为管理地址创建规则，请执行以下操作：

a) 选择**管理接口**选项卡。

规则列表定义允许访问专用端口的地址：443 用于 设备管理器 （HTTPS 网络接口），22 用于 SSH CLI。

规则不是一个有序列表。如果一个 IP 地址与请求的端口的任意规则匹配，则用户可以尝试登录设备。

注释 要删除规则，请点击该规则的垃圾桶图标()。如果删除了某个协议的所有规则，则没有人可以使用该协议访问该接口上的设备。

b) 点击 + 并填写以下选项：

- **协议** - 选择规则是用于 HTTPS（端口 443）还是 SSH（端口 22）。
- **IP 地址** - 选择定义应该能够访问系统的 IPv4 或 IPv6 网络或主机的网络对象。要指定“任何”地址，请选择 **any-ipv4** (0.0.0.0/0) 和 **any-ipv6** (::/0)。

c) 点击**确定 (OK)**。

步骤 3 要为数据接口创建规则，请执行以下操作：

a) 选择**数据接口**选项卡。

规则列表定义允许访问接口上专用端口的地址：443 用于 设备管理器（HTTPS 网络接口），22 用于 SSH CLI。

规则不是一个有序列表。如果一个 IP 地址与请求的端口的任意规则匹配，则用户可以尝试登录设备。

注释 要删除规则，请点击该规则的垃圾桶图标()。如果删除了某个协议的所有规则，则没有人可以使用该协议访问该接口上的设备。

b) 点击 + 并填写以下选项：

- **接口** - 选择要在其上允许管理访问的接口。
- **协议** - 选择规则是用于 HTTPS（端口 443）、SSH（端口 22）还是二者。不能为远程访问 VPN 连接配置文件中使用的外部接口配置 HTTPS 规则。
- **允许的网络** - 选择定义应该能够访问系统的 IPv4 或 IPv6 网络或主机的网络对象。要指定“任何”地址，请选择 **any-ipv4** (0.0.0.0/0) 和 **any-ipv6** (::/0)。

c) （可选。）如果要更改 HTTPS 数据端口编号，请点击相应编号并输入新端口。请参阅在数据接口上配置用于管理访问的 HTTPS 端口，第 729 页。

d) 点击**确定 (OK)**。

在数据接口上配置用于管理访问的 HTTPS 端口

默认情况下，出于管理目的进行的设备访问（对于 设备管理器 或威胁防御 API）会通过端口 TCP/443 进行。您可以更改数据接口的管理访问端口。

如果更改端口，用户必须在 URL 中包含自定义端口才能访问系统。例如，如果数据接口是 ftd.example.com，并且您将端口更改为 4443，则用户必须将 URL 修改为 https://ftd.example.com:4443。

所有数据接口将使用同一端口。不得为每个接口配置不同的端口。

注释 不得更改管理接口的管理访问端口。管理接口始终使用端口 443。

过程

步骤 1 点击**设备 (Device)**，然后依次点击**系统设置 (System Settings)** > **管理访问 (Management Access)** 链接。

如果您已位于“系统设置”(System Settings) 页面，只需点击目录中的**管理访问 (Management Access)**。

步骤 2 点击**数据接口 (Data Interfaces)** 选项卡。

步骤 3 点击 **HTTPS 数据端口 (HTTPS Data Port)** 号。

步骤 4 在“数据接口设置”对话框中，将 **HTTPS 数据端口**更改为要使用的端口。

不得指定以下端口号：

- 22，该端口号用于 SSH 连接。
- 用于远程访问 VPN 的端口（如果您已为允许用于管理访问的任何接口配置了该端口）。远程访问 VPN 默认使用端口 443，但您可以为其配置自定义端口。
- 在身份策略中该端口用于主动身份验证，默认为 885。

步骤 5 点击**确定 (OK)**。

配置 威胁防御 Web 服务器证书

当您登录到 Web 界面时，系统将使用数字证书来确保使用 HTTPS 的流量安全。默认证书不受您的浏览器信任，所以您会看到不受信任的颁发机构警告，并询问您是否要信任该证书。虽然用户可以将该证书保存到受信任的根证书存储区，但您也可以上传已配置为受浏览器信任的新证书。

过程

步骤 1 点击**设备**，然后依次点击**系统设置** > **管理访问**链接。

如果您已位于“系统设置”(System Settings) 页面，只需点击目录中的**管理访问 (Management Access)**。

步骤 2 点击**管理 Web 服务器 (Management Web Server)** 选项卡。

步骤 3 在 **Web 服务器证书**中，选择要用于保护 设备管理器HTTPS 连接的内部证书.

如果尚未上传或创建证书，请点击列表底部的**新建内部证书 (Create New Internal Certificate)** 链接立即创建。

默认值为预定义的 DefaultWebserverCertificate 对象。

步骤 4 如果证书不是自签名证书，请将完全信任链中的所有中间证书和根证书添加到**受信任链**列表。

您最多可以向链中添加 10 个证书。点击 **+** 添加各个中间证书，最后添加根证书。点击**保存 (Save)**（然后在警告您 Web 服务器将重启的对话框中点击**继续 (Proceed)**）时，如果证书丢失，您将收到一条错误消息，其中包含链中缺少的下一个证书的通用名称。如果添加不在链中的证书，您也会收到错误消息。仔细检查消息，确定需要添加或删除的证书。

点击 **+** 后，点击**创建新的受信任 CA 证书 (Create New Trusted CA Certificate)**，即可在此处上传证书。

步骤 5 点击**保存 (Save)**。

更改将立即应用，且系统会重新启动 Web 服务器。您无需部署配置。

请等待几分钟，在重启完成后，刷新浏览器。

配置系统日志记录设置

您可以为 威胁防御设备启用系统日志记录（系统日志）。日志记录信息可以帮助您发现并隔离网络或设备配置问题。您可以为诊断日志记录和连接相关的日志记录（包括访问控制、入侵防御和文件及恶意软件日志记录）启用系统日志。

诊断日志记录可以为与连接不相关的事件（包括与设备和系统健康状况以及网络配置相关的事件）提供系统日志消息。可以在各个访问控制规则内配置连接日志记录。

诊断日志记录可为在数据平面上运行的功能（即在 CLI 配置中定义的功能，可以使用 **show running-config** 命令查看这些功能）生成消息。这包括诸如路由、VPN、数据接口、DHCP 服务器、NAT 等功能。

有关这些消息的信息，请参阅 https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html中的 *Cisco* 威胁防御系统日志消息 。

以下主题介绍如何配置发送到各个输出位置的诊断和文件/恶意软件消息的日志记录。

严重性级别

下表列出系统日志消息严重性级别。

表 *16:* 系统日志消息严重级别

级别号	严重性级别	说明
0	应急	系统不可用。
1	警报	需要立即采取措施。
2	严重	严重情况。
3	错误	错误情况。

级别号	严重性级别	说明
4	**警告**	警告情况。
5	**通知**	正常但重大的情况。
6	**信息性**	消息仅供参考。
7	**调试**	消息仅供调试。 调试问题时，仅临时记录此级别的日志。此日志级别可能会生成太多消息，从而影响系统性能。

注释 ASA 和 威胁防御 不会生成严重性级别为零 (emergencies) 的系统日志消息。

配置系统将日志记录发送到远程系统日志服务器

您可以配置系统将系统日志消息发送到外部系统日志服务器。这是系统日志记录的最佳选项。通过使用外部服务器，您可以提供更多空间来暂存消息，并使用服务器的功能来查看、分析和存档消息。

此外，如果您在访问控制规则中对流量应用了文件策略，来控制文件访问或恶意软件，或同时控制两者，则您可以配置系统将文件事件消息发送到外部系统日志服务器。如果您未配置系统日志服务器，则仅可在 设备管理器 事件查看器中查看事件。

以下步骤介绍了如何为诊断（数据）日志记录和文件/恶意软件日志记录启用系统日志。您还可以为以下事件配置外部日志记录：

- 连接事件，通过在单个访问控制规则、SSL 解密规则或安全智能策略设置上选择系统日志服务器。
- 入侵事件，通过在入侵策略设置中选择系统日志服务器。

开始之前

仅当您应用需要 IPS 和 恶意软件防御许可证的文件或恶意软件策略时，文件/恶意软件事件的系统日志设置才具有相关性。

此外，您必须确保在应用这些策略的访问控制规则上选择了**文件事件** > **日志文件**选项。否则，系统不会生成任何事件，既不会为系统日志，也不会为事件查看器生成事件。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **日志记录设置**链接。

如果已经位于“系统设置”(System Settings) 页面中，只需点击目录中的**日志记录设置 (Logging Settings)**

步骤 2 在**远程服务器**下，将**数据日志记录**滑块调为**启用**，以为诊断数据平面生成的消息启用将日志记录发送到外部系统日志服务器。然后，配置以下选项：

- **系统日志服务器** - 点击 + 并选择一个或多个系统日志服务器对象，然后点击**确定**。如果对象不存在，请点击**添加系统日志服务器**链接，并立即创建对象。有关详细信息，请参阅配置系统日志服务器，第 138 页。
- **过滤 FXOS 机箱系统日志的严重性级别** - 对于使用 FXOS 的特定设备型号，基础 FXOS 平台生成的系统日志消息的严重性级别。仅当其与您的设备相关时，系统才会显示此选项。选择严重性级别。此级别或更高级别的消息会发送到系统日志服务器。
- **消息过滤**- 选择以下选项之一来控制为 威胁防御 操作系统生成的消息。
  - **用于过滤所有事件的严重性级别** - 选择严重性级别。此级别或更高级别的消息会发送到系统日志服务器。
  - **自定义日志记录过滤器** - 如果想要执行其他消息过滤，以便仅获得您感兴趣的消息，请选择事件列表过滤器，定义您想要生成的消息。如果尚不存在过滤器，请点击**创建新的事件列表过滤器**，然后创建过滤器。有关详细信息，请参阅配置事件列表过滤器，第 734 页。

步骤 3 将**文件/恶意软件**滑块调为**启用**，以为文件和恶意软件事件启用将日志记录发送到外部系统日志服务器。然后，配置文件/恶意软件日志记录的选项：

- **系统日志服务器** - 选择系统日志服务器对象。如果对象不存在，请点击**添加系统日志服务器**链接，并立即创建对象。
- **日志严重性级别** - 选择应分配给文件/恶意软件事件的严重性级别。由于生成的所有文件/恶意软件事件都具有相同的严重性，因此不会执行任何过滤；无论选择哪种级别，您都会看到所有事件。这将是消息严重性字段中显示的级别（即，FTD-x-<message_ID> 中的 x）。文件事件的消息 ID 为 430004，恶意软件事件则为 430005。

步骤 4 点击**保存 (Save)**。

配置系统将日志记录保存到内部缓冲区

您可以配置系统将系统日志消息保存到内部日志缓冲区。可在 CLI 或 CLI 控制台中使用 **show logging** 命令查看缓冲区的内容。

新消息将附加到缓冲区的末端。当缓冲区填充满时，系统将清除缓冲区并继续向其添加消息。当日志缓冲区已满时，系统将删除最早的消息，以释放缓冲区空间供新消息使用。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **日志记录设置**链接。

如果已经位于“系统设置”(System Settings) 页面中，只需点击目录中的**日志记录设置 (Logging Settings)**

步骤 2 将**内部缓冲区**滑块调为**启用**，以将缓冲区设为日志记录目标。

步骤 3 配置内部缓冲区日志记录的选项：

- **用于过滤所有事件的严重性级别** - 选择严重性级别。此级别或更高级别的消息会发送到内部缓冲区。
- **自定义日志记录过滤器** -（可选。）如果想要执行其他消息过滤，以便仅获得您感兴趣的消息，请选择事件列表过滤器，定义您想要生成的消息。如果尚不存在过滤器，请点击**创建新的事件列表过滤器**，然后创建过滤器。有关详细信息，请参阅配置事件列表过滤器，第 734 页。
- **缓冲区大小** - 用于保存系统日志消息的内部缓冲区的大小。当缓冲区填满时，它将被覆盖。默认值为 4096 字节。范围为 4096 到 52428800。

步骤 4 点击**保存 (Save)**。

配置系统将日志记录发送到控制台

您可以配置系统将消息发送到控制台。当在控制台端口上登录 CLI 时会显示这些消息。使用 **show console-output** 命令也可以在其他界面（包括管理地址）的 SSH 会话中看到这些日志。此外，从主 CLI 中输入 **system support diagnostic-cli** 即可在诊断 CLI 中实时看到这些消息。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **日志记录设置**链接。

如果已经位于“系统设置”(System Settings) 页面中，只需点击目录中的**日志记录设置 (Logging Settings)**

步骤 2 将**控制台过滤器**滑块调为**启用**，以将控制台设为日志记录目标。

步骤 3 选择**严重性**级别。此级别或更高级别的消息会发送到控制台。

步骤 4 点击**保存 (Save)**。

配置事件列表过滤器

事件列表过滤器是自定义过滤器，可以将其应用于日志记录目标，以控制将哪些消息发送到该目标。通常，只根据严重性来过滤目标消息，但可以使用事件列表根据事件类、严重性和消息标识符 (ID) 组合进一步控制要发送的消息。

仅当只按照严重性级别过滤消息不足以达到您的目的时，才会使用过滤器。

以下步骤介绍如何在**对象 (Objects)** 页面创建过滤器。在配置可以使用过滤器的日志记录目标时，您还可以创建过滤器。

过程

步骤 1 选择**对象**，然后从目录中选择**事件列表过滤器**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置过滤器属性：

- **名称** - 过滤器对象的名称。
- **说明** - 对象的可选说明。
- **严重性和日志类** - 如果想要按消息类别进行过滤，请点击**+**，然后为类别过滤器选择一个严重性级别，并点击**确定**。然后，点击严重性级别内的下拉箭头，在此严重性级别上选择一个或多个类别进行过滤，并点击**确定**。

  仅当指定类别的消息的严重性级别处于或高于此级别时，系统才会发送其系统日志消息。您可以为每个严重性级别最多添加一行。

  如果对给定严重性级别上的所有类别进行过滤，请将严重性列表留空，并且在启用日志记录目标时，为此目标选择全局严重性级别。
- **系统日志范围/消息 ID** - 如果想要按系统日志消息 ID 过滤，请输入您要为其生成消息的单个消息 ID 或 ID 号码范围。使用连字符分隔开始 ID 号和结束 ID 号，例如 100000-200000。ID 是 6 位数号码。有关特定消息 ID 和相关消息，请参阅 https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html中的 *Cisco Firepower Threat Defense* 系统日志消息 。

步骤 4 点击**保存**。

您现在可以在自定义过滤选项中选择此对象，用于允许此对象的日志记录目标。转至**设备** > **系统设置** > **日志记录设置**。

配置 DHCP

DHCP 服务器可为 DHCP 客户端提供网络配置参数，例如 IP 地址。您可以在接口上配置 DHCP 服务器，以便为连接网络中的 DHCP 客户端提供配置参数，也可以在接口上启用 DHCP 中继，以便将请求转发到在网络中的另一台设备上运行的外部 DHCP 服务器。

这两个功能只能二选其一：您可以配置其中一个功能或另一个功能，但不能同时配置这两个功能。

配置 DHCP 服务器

DHCP 服务器可为 DHCP 客户端提供网络配置参数，例如 IP 地址。您可以在接口上配置 DHCP 服务器，为连接的网络上的 DHCP 客户端提供配置参数。

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。DHCP 服务器不支持 BOOTP 请求。

注释 不要在已经有 DHCP 服务器运行的网络上配置 DHCP 服务器。这两个服务器将发生冲突，结果不可预测。

开始之前

DHCP 客户端必须与启用了服务器的接口位于同一网络内。即服务器和客户端之间不能有干预路由器，但可以有交换机。

如果您必须支持多个网络，但不想在每个接口上配置 DHCP 服务器，您可以配置 DHCP 中继，将 DHCP 请求从一个网络转发到位于不同网络上的 DHCP 服务器。在这种情况下，DHCP 服务器必须位于网络中的不同设备上：不能在同一设备的一个接口上配置 DHCP 服务器，而在另一个接口上配置 DHCP 中继。使用 DHCP 中继时，请确保为 DHCP 服务器将管理的每个网络地址空间配置地址池。

要配置 DHCP 中继，请参阅配置 DHCP 中继，第 737 页。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **DHCP 服务器/中继**链接。

如果已经位于“系统设置”(System Settings) 页面中，只需点击目录中的 **DHCP** > **DHCP 服务器 (DHCP Server)**。

该页有两个选项卡。一开始，**配置**选项卡显示全局参数。

DHCP 服务器选项卡显示已在其上配置 DHCP 服务器的接口、服务器启用情况以及服务器的地址池。

步骤 2 在**配置**选项卡上，配置自动配置和全局设置。

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。通常，如果您是在使用 DHCP 获取地址，则会使用自动配置，但您可以选择通过 DHCP 获取其地址的任何接口。如果无法使用自动配置，可以手动定义所需的选项。

a) 如果要使用自动配置，请点击**启用自动配置** > **开**（滑块应位于右侧），然后在**源接口**中选择正在通过 DHCP 获取其地址的接口。

如果要配置虚拟路由器，则只能在全局虚拟路由器中的接口上使用 DHCP 服务器自动配置。为用户定义的虚拟路由器分配的接口不支持自动配置功能。

b) 如果不启用自动配置，或者如果要覆盖任何一个自动配置的设置，请配置以下全局选项。这些设置将发送到托管 DHCP 服务器的所有接口上的 DHCP 客户端。

- **主 WINS IP 地址**、**辅助 WINS IP 地址** - Windows Internet Name Service (WINS) 服务器客户端应该用于 NetBIOS 域名解析的地址。
- **主 DNS IP 地址**、**辅助 DNS IP 地址** - 客户端应该用于域名解析的域名系统 (DNS) 服务器的地址。如果要配置 OpenDNS 公共 DNS 服务器，请点击**使用 OpenDNS**。点击该按钮会将正确的 IP 地址载入字段中。

c) 点击**保存 (Save)**。

步骤 3 点击 **DHCP 服务器**选项卡并配置服务器。

a) 执行以下操作之一：

- 要为尚未列出的接口配置 DHCP 服务器，请点击 **+**。
- 要编辑现有的 DHCP 服务器，请点击该服务器的编辑图标 ( )。

要删除服务器，请点击该服务器的垃圾桶图标 ( )。

b) 配置服务器属性：

- **启用 DHCP 服务器** - 是否启用服务器。您可以配置服务器，但在做好准备开始使用之前，要一直将其禁用。
- **接口** - 选择您为客户端提供 DHCP 地址的接口。接口必须拥有静态 IP 地址；如果要在接口上运行 DHCP 服务器，则不能使用 DHCP 获取接口。对于网桥组，在网桥虚拟接口 (BVI) 上（而不是成员接口上）配置 DHCP 服务器，并且服务器在所有成员接口上运行。

  您不能在此屏幕中的管理接口上配置 DHCP 服务器，而应在上配置，它位于**设备 (Device)** > **接口 (Interfaces)** 页面。
- **地址池** - 允许服务器为请求地址的客户端提供的 IP 地址的范围（最低至最高）。指定该池的开始和结束地址，用连字符隔开。例如 10.100.10.12-10.100.10.250。

  该 IP 地址范围必须与所选接口位于同一子网上，并且不能包括接口本身的 IP 地址、广播地址或子网地址。

  威胁防御 设备上地址池的大小不得超过每个池 256 个地址。如果地址池范围大于 253 个地址，则 威胁防御 接口的网络掩码不能为 C 类地址（例如 255.255.255.0）且需要成为更大的地址，例如 255.255.254.0。

c) 点击**确定 (OK)**。

配置 DHCP 中继

您可以配置 DHCP 中继代理以向一个或多个 DHCP 服务器转发接口上收到的 DHCP 请求。

DHCP 客户端使用 UDP 广播发送其初始 DHCPDISCOVER 消息，因为它们没有与其所连接网络有关的信息。如果客户端位于不包含服务器的网段，则通常 UDP 广播不会由 威胁防御 设备进行转发，因为它不转发广播流量。DHCP 中继代理允许您配置接收广播的威胁防御设备的接口，以将 DHCP 请求转发到可通过另一个接口使用的 DHCP 服务器。

因此，子网中不托管 DHCP 服务器的客户端仍然可以从位于不同子网中的 DHCP 服务器获取 IP 地址租用。

开始之前

- 为要添加的每个子网配置具有地址池的 DHCP 服务器。例如，如果您在具有 192.168.1.1/24 地址的接口上启用 DHCP 中继客户端，要支持 192.168.1.0/24 网络上的客户端，DHCP 服务器必须能够提供 192.168.1.0/24 子网上的 IP 地址，例如 192.168.1.2-192.168.1.254。
- 为每个 DHCP 服务器创建主机网络对象，指定服务器的 IP 地址。
- 确保已删除或已禁用 **DHCP** > **DHCP 服务器 (DHCP Servers)** 页面上的所有服务器。如果在接口上启用了 DHCP 中继，则您不能在任何接口上托管 DHCP 服务器，即使它们是不同的接口。
- 接口限制 - 接口必须具有用于服务器或代理的名称。此外：
  - 接口不能是路由 ECMP 流量区域的成员。
  - 接口无法使用 DHCP 获取其地址。
  - 您可以在物理接口、子接口、VLAN 接口和 EtherChannel（但不是它们的成员）上配置 DHCP 服务器和 DHCP 中继。
  - 您还可以在虚拟隧道接口 (VTI) 上配置 DHCP 中继服务器。
  - 这两项服务都不支持管理接口，也不支持网桥组及其成员。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **DHCP 服务器/中继**链接，然后点击目录中的 **DHCP** > **DHCP 中继**。

如果您已经在“系统设置”(System Settings) 页面中，只需点击目录中的 **DHCP** > **DHCP 中继 (DHCP Relay)**。

步骤 2 （可选。）根据需要调整 **IPv4 中继超时**和 **IPv6 中继超时**设置。

这些超时设置用于设置给定 IP 版本的 DHCP 中继地址协商所允许的秒数。默认值为 60 秒（1 分钟），但您可以设置介于 1-3600 秒的其他超时值。如果子网和 DHCP 服务器之间存在明显延迟，则可能需要更长的超时时间。

步骤 3 配置 **DHCP 中继服务器**。

DHCP 中继服务器是网络中应为 DHCP 中继请求提供服务的 DHCP 服务器。这些 DHCP 服务器与您正在配置的设备位于网络中的不同设备上。

a) 点击 **+**，选择具有 DHCP 服务器 IP 地址的主机网络对象，然后点击**确定 (OK)**。

如果该对象尚不存在，请点击**创建新网络**并立即创建。如果您不想再使用已添加的 DHCP 服务器，请点击该服务器条目右侧的 **X** 将其删除。

b) 点击您添加的 DHCP 服务器条目，然后选择可以访问 DHCP 服务器的接口。

步骤 4 配置 DHCP 中继代理。

DHCP 中继代理在接口上运行。它们将来自其网段中客户端的 DHCP 请求转发到 DHCP 服务器，然后将响应返回给客户端。

a) 点击 **+**，选择应运行 DHCP 中继代理的接口，然后点击**确定 (OK)**。

如果您不想再在接口上运行 DHCP 中继代理，请点击该服务器条目右侧的 **X** 将其删除。或者，您可以只禁用所有 DHCP 中继服务，而不从表中删除接口。

b) 点击您添加的接口条目，选择您希望代理提供的 DHCP 服务，然后点击**确定 (OK)**。

- **启用 IPv4** - 将 IPv4 地址请求转发到 DHCP 服务器。如果不选择此选项，则会忽略任何 IPv4 地址请求，并且客户端无法获取 IPv4 地址。
- **设置路由** （仅限 IPv4）- 将从 DHCP 服务器发送的数据包中的第一个默认路由器地址更改为运行 DHCP 中继代理的 威胁防御 设备接口的地址。通过此操作，客户端可以将其默认路由设置为指向 威胁防御设备，即使 DHCP 服务器指定了另一个路由器也如此。如果数据包内无默认路由器选项，DHCP 中继代理会添加一个包含接口地址的选项。
- **启用 IPv6** - 将 IPv6 地址请求转发到 DHCP 服务器。如果不选择此选项，则会忽略任何 IPv6 地址请求，并且客户端无法获取 IPv6 地址。

步骤 5 点击**保存 (Save)**。

配置动态 DNS

您可以将系统配置为使用 Web 更新方法将动态域名系统 (DDNS) 更改发送到动态 DNS 服务。这些服务随后会更新 DNS 服务器，以使用与完全限定域名 (FQDN) 关联的新 IP 地址。因此，当用户尝试使用主机名访问系统时，DNS 会将该名称解析为正确的 IP 地址。

使用 DDNS 有助于确保为系统中的接口定义的 FQDN 始终解析为正确的 IP 地址。当您将接口配置为使用 DHCP 获取地址时，这一点尤其重要。但使用它获取静态 IP 地址以确保 DNS 服务器具有正确的地址也是有价值的，并且在更改静态地址时可以很容易更新。

您可以将 DDNS 配置为使用一组选定的 DDNS 服务提供商，或者使用自定义选项将更新定向到支持 Web 更新的任何其他 DDNS 提供商。您为接口指定的 FQDN 应注册到这些服务提供商。

注释 您可以使用 设备管理器 仅配置 Web 更新 DDNS。您不能配置 DDNS 来实现 IETF RFC 2136 中定义的方法。

开始之前

系统必须拥有信任的 CA 证书，以验证提供商的证书，否则 DDNS 连接将不会成功。您可以从服务提供商的站点下载证书。请确保上传并部署适当的证书。还要确保您将上传的证书的**验证使用**设置为包括 **SSL 服务器**。请参阅上传受信任的 CA 证书，第 148 页。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **DDNS 服务**链接。

如果已经位于“系统设置”页面中，只需点击目录中的 **DDNS 服务 (DDNS Service)**。

该页面显示 DDNS 更新方法的列表，包括服务提供商、接口、接口的完全限定域名 (FQDN)，以及 DNS 服务器因 FQDN IP 地址更改而更新的频率。您可以点击条目的**显示状态**链接来检查其是否正常工作。

步骤 2 执行以下操作之一：

- 要创建新的动态 DNS 更新方法，请点击 **+** 或**创建 DDNS 服务**按钮。
- 要编辑现有的动态 DNS 更新方法，请点击该方法的编辑图标 ()。

要删除方法，请点击该方法的垃圾桶图标 ()。

步骤 3 配置动态 DNS 服务属性：

- **名称** - 服务的名称。
- **Web 类型更新** - 根据您的 DDNS 服务提供商的支持情况选择要更新的地址类型。默认更新**所有地址**（IPv4 和 IPv6）。您可以更新 **IPv4 地址**、**IPv4 和一个 IPv6 地址**、**一个 IPv6 地址**、**所有 IPv6 地址**。

  对于 IPv6 地址，请注意以下几项：

  - 仅更新全局地址。从不更新本地链路地址。
  - 由于 设备管理器 允许您为每个接口配置一个 IPv6 地址，因此在实践中，只会更新一个 IPv6 地址。

- **服务提供商** - 选择将接收和处理动态 DNS 更新的服务提供商。您可以使用以下服务提供商。
  - **No-IP** - No-IP DDNS 服务提供商，https://www.noip.com/。
  - **动态 DNS** - Oracle Dynamic DNS 服务提供商，https://account.dyn.com/。
  - **Google** - Google Domains 服务提供商，https://domains.google.com。
  - **自定义 URL** - 任何其他 DDNS 服务提供商。您将需要在 **Web URL** 字段中输入选定提供商所需的 URL（包括用户名和密码）。DDNS 服务应遵守 https://help.dyn.com/remote-access-api/ 中所述的标准。

- **用户名、密码**（非自定义 URL 方法）- 发送动态 DNS 更新时要使用的在服务提供商平台上定义的用户名和密码。

  注意：

  - 用户名不能包含空格，也不能包含 @ 和 : 字符，因为它们会被作为分隔符。
  - 密码不能包含空格或 @ 字符，因为它会被作为分隔符。第一个 : 之后和 @ 之前的任何 : 字符都被视为密码的一部分。

- **Web URL**（自定义 URL 方法）- 如果您选择自定义 URL 作为服务提供商，请输入您的动态 DNS 服务的 URL。URL 必须采用以下格式，限制为 511 个字符：

  http(s)://username:password@provider-domain/xyz?hostname=<h>&myip=<a>

  https://username:password@domain-provider/xyz?hostname=%3Ch%3E&myip=%3Ca%3E

- **接口和完全限定域名** - 选择此服务提供商中要更新 DNS 记录的接口，然后输入每个接口的完全限定域名。例如，interface.example.com。接口受到以下限制：

  - 您只能选择指定的物理接口和子接口。
  - 您不能选择以下类型的接口：管理、BVI/EtherChannel 或其成员、VLAN、虚拟隧道接口 (VTI)。
  - 只能在一个 DDNS 更新方法中选择给定的接口。您可以选择应在同一 DDNS 更新对象中使用服务提供商的所有接口。

- **更新间隔** - 发送动态 DNS 更新的频率。默认值为**更改时**，只要接口的 IP 地址更改就发送更新。或者，您可以选择**每小时**、**每天**或**每月**。在每天和每月的设置中，还可以配置在每天的什么时间和每月的哪一天发送更新。

步骤 4 点击**确定 (OK)**。

配置 DNS

域名系统 (DNS) 服务器用来将主机名解析到 IP 地址。DNS 服务器的配置在初始系统设置期间执行，并且这些服务器将应用于数据和管理接口。您可以在设置完成后对其进行更改，并对数据和管理接口使用单独的一组服务器。

至少，必须要为管理接口配置 DNS。如果您想要使用基于 FQDN 的访问控制规则，或想要在 CLI 命令（如 **ping**）中使用主机名，那么还必须要为数据接口配置 DNS。

DNS 的配置分两步完成：配置 DNS 组，然后在接口上配置 DNS。

以下主题更详细地介绍了这一过程。

配置 DNS 组

DNS 组定义 DNS 服务器列表和某些相关联的属性。您可以在管理和数据接口上单独配置 DNS。需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 www.example.com。

完成设备设置向导后，您将有一个或两个系统定义的以下 DNS 组：

- CiscoUmbrellaDNSServerGroup - 此组包括思科 Umbrella 所搭配 DNS 服务器的 IP 地址。如果您在初始设置期间选择了这些服务器，此组便是系统定义的唯一组。您无法更改此组中的名称或服务器列表，但您可以编辑其他属性。
- CustomDNSServerGroup - 如果您不在设备设置期间选择 Umbrella 服务器，系统将使用您的服务器列表创建此组。您可以编辑此组中的任何属性。

过程

步骤 1 选择**对象**，然后从目录中选择 **DNS 组**。

步骤 2 执行以下操作之一：

- 要创建组，请点击**添加组** ( ) 按钮。
- 要编辑组，请点击该组的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置以下属性：

- **名称** - DNS 服务器组的名称。保留 DefaultDNS 名称：不能使用该名称。
- **DNS IP 地址** - 输入 DNS 服务器的 IP 地址。点击**添加另一个 DNS IP 地址**配置多个服务器。如果您想要删除服务器地址，请点击该地址的删除图标 ( )。

  列表采用优先顺序：始终使用列表中的第一个服务器，只有当从前面的服务器收不到响应时，才使用后面的服务器。您最多可以配置 6 个服务器。但是，仅数据接口上支持 6 个服务器。管理接口仅使用前面的 3 个服务器。
- **域搜索名称** - 为您的网络输入域名，例如 example.com。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。名称必须不能超过 63 个字符以使用数据接口组。
- **重试次数** - 系统接收不到响应时，重试 DNS 服务器列表的次数，介于 0 和 10 次之间。默认值为 2。此设置仅适用于数据接口上使用的 DNS 组。
- **超时** - 尝试下一个 DNS 服务器之前要等待的秒数，介于 1 和 30 秒之间。默认值为 2 秒。每次系统重试服务器列表，此超时将加倍。此设置仅适用于数据接口上使用的 DNS 组。

步骤 4 点击**确定 (OK)**。

为数据流量和管理流量配置 DNS

域名系统 (DNS) 服务器用来将主机名解析到 IP 地址。有两种适用于不同类型流量的 DNS 服务器设置：数据流量和特殊管理流量。数据流量包括使用需要进行 DNS 查找的 FQDN 的任何服务，例如访问控制规则和远程接入 VPN。特殊管理流量包括管理接口上发出的流量，例如智能许可和数据库更新。

如果使用 CLI 安装向导，则在初始系统配置期间，配置管理 DNS 服务器。还可以在 设备管理器 安装向导中设置数据和管理 DNS 服务器。可使用以下过程更改 DNS 服务器默认设置。

您还可以在 CLI 中使用 **configure network dns servers** 和 **configure network dns searchdomains** 命令更改 DNS 配置。如果数据和管理接口使用相同的 DNS 组，组将更新，且所做的更改也会在下一个部署中应用到数据接口。

为了确定 DNS 服务器通信的正确接口， 威胁防御 使用路由查找，但使用哪种路由表取决于您启用 DNS 的接口。有关详细信息，请参阅下面的接口设置。

如果您无法进行 DNS 解析，请参阅：

- 常规 DNS 问题故障排除， 第 744 页
- 为管理接口排除 DNS 故障， 第 798 页

开始之前

- 确保已创建 DNS 服务器组。有关说明，请参阅配置 DNS 组， 第 742 页。
- 确保 威胁防御 设备具有适当的静态路由或动态路由来访问 DNS 服务器。

过程

步骤 1 点击**设备 (Device)**，然后点击**系统设置 (System Settings)** > **DNS 服务器 (DNS Server)** 链接。

如果已经位于**系统设置 (System Settings)** 页面中，则点击目录中的 **DNS 服务器 (DNS Server)**。

步骤 2 为**数据接口**配置 DNS。

a) 在所有接口或特定接口上启用 DNS 查找。这些选择还会影响所使用的路由表。

请注意，在接口上启用 DNS 查找与指定用于查找的源接口不同。设备始终使用路由查询来确定源接口。

- **任何**（不选择任何接口）- 在所有接口。设备 仅检查数据路由表。
- 已选择接口，但未选择管理接口或管理专用接口 - 在指定接口上启用 DNS 查找。设备仅检查数据路由表。
- 已选择接口，并且选择了管理接口或管理专用接口 - 在指定接口上启用 DNS 查找。设备检查数据路由表，如果未找到路由，则回退到管理专用路由表。
- 仅选择了管理接口或管理专用接口 - 在管理或管理专用接口上启用 DNS 查找。设备仅检查管理专用路由表。

b) 选择定义在数据接口上使用的服务器的 **DNS 组**。如果组尚不存在，请点击**创建新的 DNS 组 (Create New DNS Group)** 立即创建组。如果您想要阻止在数据接口上进行查找，请选择**无**。

c) （可选。）如果在访问控制规则中使用 FQDN 网络对象，配置 **FQDN DNS 设置**。

仅解析 FQDN 对象时使用这些选项，任何其他类型的 DNS 解析都将忽略这些选项。

- **轮询时间** - 将 FQDN 网络对象解析为 IP 地址的轮询周期，以分钟为单位。仅在访问控制策略中使用 FQDN 对象时，解析这些对象。计时器决定两次解析之间的最长时间；DNS 条目的生存时间 (TTL) 值也用于确定更新 IP 地址解析的时间，因此，解析单个 FQDN 的频率可能大于轮询周期。默认设置为 240（4 个小时）。范围为 1 至 65535 分钟。
- **过期** - DNS 条目过期（即，超出从 DNS 服务器获得的 TTL）后，从 DNS 查找表中删除该条目前等待的分钟数。删除条目要求重新编译表，使频繁删除能够增加设备上的处理负载。因为某些 DNS 条目可以有非常短的 TTL（短至 3 秒），所以您能够使用此设置实际上延长 TTL。默认设置为 1 分钟（即，TTL 过去后 1 分钟，会删除条目）。范围为 1 至 65535 分钟。

d) 点击**保存 (Save)**。您还必须部署配置，将更改应用到设备。

步骤 3 为**管理接口**配置 DNS。

a) 选择定义在管理接口上使用的服务器的 **DNS 组**。如果组尚不存在，请点击**创建新的 DNS 组 (Create New DNS Group)** 立即创建组。

b) 点击**保存 (Save)**。必须部署更改以更新管理 DNS 服务器。

常规 DNS 问题故障排除

必须为管理和数据接口单独配置DNS服务器。某些功能通过这两类接口中的其中一类接口，而不是这两类接口，解析域名。有时，给定的功能将使用不同的解析方法，具体取决于您如何使用该功能。

例如，**ping** *hostname* 和 **ping interface** *interface_name hostname* 命令使用数据接口 DNS 服务器解析域名，而 **ping system** *hostname* 命令使用管理接口 DNS 服务器。这使您可以通过特定接口和路由表测试连接。

排除主机名查找问题时，请记住这一点。

有关排除管理接口 DNS 故障的信息，另请参阅为管理接口排除 DNS 故障，第 798 页。

未发生域名解析

如果根本没有发生域名解析，可参照以下故障排除提示。

- 验证您是否已为管理和数据接口均配置 DNS 服务器。对于数据接口，对接口使用“任何”设置。仅当您不想在某些接口上允许 DNS 时，才明确指定接口。
- 您无法通过管理接口或管理专用接口访问DNS服务器。如果要使用管理接口，请确保该接口是选择的唯一接口。

- 执行 ping 操作，以验证是否可访问每个 DNS 服务器的 IP 地址。使用 **system** 和 **interface** 关键字测试特定接口。如果 ping 操作不成功，请检查您的静态路由和网关。您可能需要为服务器添加静态路由。
- 如果 ping 操作成功，但域名解析失败，请检查访问控制规则。验证您是否允许连接服务器的接口的 DNS 流量 (UDP/53)。此流量也可能被系统和 DNS 服务器之间的设备阻止，因此您可能需要使用不同的 DNS 服务器。
- 如果 ping 操作成功、路由充足，并且访问控制规则不是症结所在，请考虑 DNS 服务器是否存在 FQDN 映射。您可能需要使用不同的服务器。

域名解析错误

如果进行了域名解析，但名称的IP地址不是最新地址，可能存在缓存问题。此问题仅影响基于数据接口的功能，例如访问控制规则中使用的 FQDN 网络对象。

系统有从前期查找中获得的DNS信息的本地缓存。需要新的查询时，系统首先在本地缓存中查找。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 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。

每个查找都有一个生存时间值，该值由DNS服务器定义并自动从缓存到期。此外，系统会为访问控制规则中使用的 FQDN 定期刷新该值。至少，系统会按照轮询时间间隔（默认情况下，每 4 小时一次）刷新，不过可根据该条目的生存时间值，增加刷新频率。

使用 **show dns-hosts** 和 **show dns** 命令检查本地缓存。如果 FQDN 的 IP 地址错误，可以使用 **dns update** [**host** *hostname*] 命令强制系统刷新信息。如果在使用此命令时没有指定主机，系统会刷新所有主机名。

可以使用 **clear dns** [**host** *fqdn*] 和 **clear dns-hosts cache** 命令删除缓存的信息。

配置设备主机名

可以更改设备主机名。

您还可以在 CLI 中使用 **configure network hostname** 命令更改主机名。

⚠

注意 如果更改连接到系统所用的主机名，由于这些更改会立即应用，因此您将丢失对 设备管理器 的访问。您需要重新连接到设备。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **主机名**链接。

如果已经位于“系统设置”页面中，只需点击目录中的**主机名 (Hostname)**

步骤 2 输入新主机名。

步骤 3 点击**保存**。

主机名更改随后立即应用到某些系统进程。但是，您必须部署更改以完成更新，以便所有系统进程都使用相同的名称。

配置网络时间协议 (NTP)

必须配置网络时间协议 (NTP) 服务器才能在系统上定义时间。NTP 服务器在初始系统设置期间配置，但您可以使用以下步骤程序对其进行更改。如果您无法连接到 NTP，请参阅 NTP 故障排除，第 797 页。

威胁防御 设备支持 NTPv4。

注释 对于 Firepower 4100/9300，请勿通过 设备管理器设置 NTP。在 FXOS 中配置 NTP。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **时间服务**链接。

如果已经在“系统设置”(System Settings) 页面中，则只需点击目录中的**时间服务 (Time Services)** 即可。

步骤 2 在 **NTP 时间服务器**中，选择使用您自己的时间服务器还是思科时间服务器。

- **默认 NTP 时间服务器** - 如果选择此选项，服务器列表会显示用于 NTP 的服务器名称。
- **用户定义的 NTP 服务器** - 如果选择此选项，则输入您要使用的 NTP 服务器的完全限定域名或 IPv4 或 IPv6 地址。例如 ntp1.example.com 或 10.100.10.10。最多可以添加 3 个 NTP 服务器。

步骤 3 点击**保存 (Save)**。

配置精确时间协议 (ISA 3000)

精确时间协议 (PTP) 是一种时间同步协议，用于在基于数据包的网络中同步各种设备的时钟。这些设备时钟通常具有不同的精度和稳定性。该协议专为工业联网测量和控制系统设计，而且最适合用于分布式系统，因为其需要极少的带宽和处理开销。

PTP 系统是一个分布式联网系统，包含 PTP 设备和非 PTP 设备的组合。PTP 设备包含常见的时钟、边界时钟和透明时钟。非 PTP 设备包含网络交换机、路由器和其他基础设施设备。

可以将 威胁防御 设备配置为透明时钟。 威胁防御 设备不会将其时钟与 PTP 时钟同步。 威胁防御 设备将使用 PTP 默认配置文件，如 PTP 时钟上所定义。

配置 PTP 设备时，需要为要一起运行的设备定义一个域编号。因此，可以配置多个 PTP 域，然后将每个非 PTP 设备配置为特定域使用 PTP 时钟。

开始之前

确定设备应使用的 PTP 时钟上配置的域编号。另外，确定系统可通过哪些接口到达域中的 PTP 时钟。

以下是 PTP 配置准备：

- 此功能在思科 ISA 3000 设备上不可用。
- 思科 PTP 仅支持组播 PTP 消息。
- PTP 仅可用于 IPv4 网络，不可用于 IPv6 网络。
- 物理以太网数据接口支持 PTP 配置，无论是路由组还是网桥组成员。管理接口、子接口、Etherchannel 接口、桥接虚拟接口 (BVI) 或任何其他虚拟接口均不支持此版本。
- 假如父接口上具有适当的 PTP 配置，则支持 VLAN 子接口上的 PTP 流。
- 必须确保允许 PTP 数据包通过设备。PTP 流量由 UDP 目标端口 319 和 320 以及目标 IP 地址 224.0.1.129 标识，因此允许此流量的任何访问控制规则均应有效。
- 当PTP数据包在路由接口之间传输时，您必须启用多路广播路由，并且每个接口应加入224.0.1.129 IGMP 多路组播组。当 PTP 数据包在同一网桥组中的接口之间流动时，您无需启用组播路由和配置 IGMP 组。

过程

步骤 1 验证面向 PTP 时钟的接口的配置。

默认配置将所有接口置于同一个网桥组中，但可以从网桥组中删除接口。必须确定接口是路由组成员还是网桥组成员，因为对于组播 IGMP 组而言这两种成员必须进行不同的配置。

以下操作步骤介绍如何确定哪些接口是网桥组成员。检查您为 PTP 配置的接口是否为网桥组成员。

a) 点击**设备** > **接口**中的**查看所有接口**。
b) 在列表中查找相应接口，并选中“模式”列。如果是 BridgeGroupMember，则意味着属于网桥组；否则应该属于路由组。

步骤 2 点击**设备**，然后点击**系统设置** > **时间服务**链接。

如果已经在**系统设置 (System Settings)** 页面中，则只需点击目录中的**时间服务 (Time Services)** 即可。

步骤 3 配置 PTP 设置：

- **域编号** - 在网络中的 PTP 设备上配置的域编号，范围为0-255。在其他域中接收的数据包将像正常组播数据包一样处理，不会进行任何 PTP 处理。

- **时钟模式**-选择 **EndToEndTransparent**。您只能将设备作为 PTP 透明时钟运行。

  或者，也可以选择**转发**，但这在本质上与不配置 PTP 时的情况相同。域编号将被忽略。PTP 数据包基于组播流量的路由表通过设备。这是默认的 PTP 配置。

- **接口** - 选择可由系统用于连接至网络中的 PTP 时钟的所有接口。仅在这些接口上启用 PTP。

步骤 4 点击**保存**。

步骤 5 如果您选择的任何接口是路由接口（即它们不是网桥组成员），则需要使用 FlexConfig 启用组播路由，并将路由接口加入正确的 IGMP 组。

如果所有选定的接口都是网桥组成员，则不用完成此步骤。如果您尝试在网桥组成员上配置IGMP，则会出现部署故障。

a) 在**设备** > **高级配置**中点击**查看配置**。
b) 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。
c) 创建启用组播路由和为路由接口配置 IGMP 加入所需的对象。

以下将是对象的基本模板。在本示例中，GigabitEthernet1/2 是您在其中启用 PTP 的一个路由接口。根据需要更改接口硬件名称，并且如果您有多个路由接口，请对每个其他接口重复**interface** 和 **igmp** 命令。

igmp 命令将会加入 224.0.1.129 IGMP 组。无论网络地址如何，这都是所有接口的正确 IP 地址。

```
multicast-routing
interface GigabitEthernet1/2
 igmp join-group 224.0.1.129
```

取消模板如下所示：

```
no multicast-routing
interface GigabitEthernet1/2
 no igmp join-group 224.0.1.129
```

d) 点击目录中的 **FlexConfig 策略**，将此对象添加到 FlexConfig 策略中，然后点击**保存**。

验证预览内容是否会显示您对象中的预期命令。

下一步做什么

在部署更改后，您可以验证 PTP 设置。在 设备管理器 CLI 控制台或 SSH 或控制台会话中，发出各种 **show ptp** 命令。例如，如果仅为 GigabitEthernet1/2 配置了用于域 10 的 PTP，则输出内容可能如下所示：

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
```

```
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 4
  PTP version: 2
  Port state: Disabled
```

配置管理连接的 HTTP 代理

如果系统和互联网之间没有直接连接，可以为管理接口设置 HTTP 代理。然后，系统将该代理用于所有管理连接，包括与 设备管理器 的连接以及为下载数据库更新而从系统到思科建立的连接。

您还可以使用 **configure network http-proxy** 命令在 威胁防御 CLI 中配置 HTTP 代理。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **HTTP 代理**链接。

如果已经位于**系统设置 (System Settings)** 页面中，只需点击目录中的 **HTTP 代理 (HTTP Proxy)**

步骤 2 点击此切换启用代理，然后配置代理设置：

- **HTTP 代理** - 代理服务器的 IP 地址。
- **端口** - 配置为侦听 HTTP 连接的代理服务器端口号。
- **使用代理身份验证** - 如果服务器配置为需要对代理连接进行身份验证，请选择此选项。如果选择此选项，还需输入可登录代理服务器的账户的**用户名**和**密码**。

步骤 3 点击**保存**，然后确认进行更改。

所做更改会立即应用。不需要部署作业。

由于您要更改系统完成管理连接的方式，因此将失去与 设备管理器的连接。请等待几分钟以完成更改，然后刷新浏览器窗口并重新登录。

配置云服务

您可以注册云服务，以便使用各种基于云的应用，例如 CDO、Cisco 威胁响应和 Cisco Success Network。

在云中注册后，该页面将显示注册状态和租用类型，以及注册设备所使用的账户名称。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **云服务**链接。

如果已经位于**系统设置 (System Settings)** 页面，只需点击目录中的**云服务 (Cloud Services)**。

如果您的设备未注册，此页面会显示注册思科云的注册方法。注册云后，您将能够启用或禁用单个云服务。

步骤 2 要注册思科云（在评估模式下或从云服务取消注册后），请选择以下选项之一：

- **安全/CDO 账户** - 您可以使用以下方法之一：
  - **通过 Cisco 防御协调器自动注册租用** （仅限 Firepower 1000、2100、Secure Firewall 3100）。您可以使用自动注册而不是获取注册密钥。首先，转到CDO，使用设备的序列号添加设备。然后，在 设备管理器中，选中此复选框并启动注册。从设备机箱或装箱单上获取序列号。对于FXOS，您可以进入FXOS CLI并使用 **show chassis detail** 命令检索标记为“Serial (SN)”的正确序列号。请注意， 威胁防御 命令 **show serial-number** 提供不同的序列号，不建议用于 CDO 注册。 此方法适用于 CDO 中的云交付 管理中心 以及 CDO 中的传统设备管理器模式。

    注释 传统设备管理器模式仅适用于已经使用该模式管理 威胁防御 的现有用户。

  - 登录 CDO 或其他安全账户并生成注册密钥。然后返回此页面，选择**云服务区域 (Cloud Services Region)**并粘贴**注册密钥 (Registration Key)**。 此方法仅适用于 CDO 中的传统设备管理器模式。有关 CDO 中的云交付管理中心，请参阅从 设备管理器 切换到 管理中心 或 CDO ，第 755 页。

    注释 传统设备管理器模式仅适用于已经使用该模式管理 威胁防御 的现有用户。

    此时您还可以启用**思科防御协调器**和 **Cisco Success Network**。默认情况下，这些功能处于启用状态。

- **智能许可证**-（仅当您不使用 CDO时。）点击链接转到“智能许可”(Smart Licensing) 页面并注册 CSSM。注册 CSSM 后，设备也会注册云服务。

注释　如果您已从云服务中取消注册，则注册智能许可证可能需要一些额外步骤。在这种情况下，请选择**云服务区域 (Cloud Services Region)**，然后点击**注册 (Register)**。阅读披露内容并点击**接受 (Accept)**。

步骤 3 注册云服务后，您可以根据需要启用或禁用功能。请参阅以下主题：

- 启用或禁用 CDO（传统设备管理器模式），第 751 页
- 连接到 Cisco Success Network，第 752 页
- 将事件发送至思科云，第 752 页
- 取消注册云服务，第 753 页

启用或禁用 CDO（传统设备管理器模式）

注释　本部分仅适用于 CDO 中的传统设备管理器模式，而不适用于云交付的管理中心。

如果您从CDO中使用注册密钥注册了云服务（如配置云服务，第750页中推荐），则设备已向CDO注册。此后，您可以根据需要禁用或重新启用连接。

如果使用智能许可将设备注册到云服务，则在启用 CDO 时会出现问题：设备不会显示在 CDO 清单中。强烈建议您先从云服务取消注册设备；从齿轮 (⚙) 下拉列表中选择**取消注册云服务**。取消注册后，从 CDO 获取注册令牌，然后使用该令牌和您的安全账户重新注册，如配置云服务，第 750 页中所述。

有关云管理原理的更多信息，请参阅 CDO 门户 (http://www.cisco.com/go/cdo) 或咨询您的经销商或合作伙伴。

开始之前

如果您想要配置高可用性，则必须注册您要在高可用性组中使用的两台设备。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **云服务**链接。

如果已经位于“系统设置”(System Settings) 页面，只需点击目录中的**云服务 (Cloud Services)**。

步骤 2 点击 CDO 功能的 **启用/禁用** 按钮，根据需要更改设置。

连接到 Cisco Success Network

注册设备时，需决定是否启用与 Cisco Success Network 之间的连接。请参阅注册设备，第 85 页。

通过启用 Cisco Success Network，可以向思科提供使用信息和统计信息，这对思科为您提供技术支持至关重要。通过此信息，思科还可以改进产品，并使您获悉未使用的可用功能，以便您能够在网络中将产品的价值最大化。

启用连接时，设备将与思科云建立安全连接，以确保设备可以参与思科提供的其他服务（例如技术支持服务、云管理和监控服务）。您的设备将随时建立并维护此安全连接。有关从云完全断开连接的信息，请参阅取消注册云服务，第 753 页。

注册设备后，可以更改 Cisco Success Network 设置。

注释 系统向思科发送数据时，任务列表会显示一项遥测作业。

开始之前

要启用 Cisco Success Network，必须向云注册设备。要注册设备，请使用 Cisco 智能软件管理器（在“智能许可”(Smart Licensing) 页面上）注册该设备，在注册过程中选择“Cisco Success Network”选项，或者通过输入注册密钥使用 CDO 进行注册（仅限 CDO 中的传统设备管理器模式）。

注释 如果您在高可用性组的主用设备上启用 Cisco Success Network，也会在备用设备上启用该连接。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **云服务**链接。

如果已经位于“系统设置”(System Settings) 页面，只需点击目录中的**云服务 (Cloud Services)**。

步骤 2 点击 Cisco Success Network 功能的**启用**/**禁用**控件，可以根据需要更改设置。

可以点击**样本数据**链接，查看发送给思科的信息类型。

启用该连接时，请阅读披露的信息并点击**接受**。

将事件发送至思科云

可以将事件发送至思科云服务器。各种思科云服务均可从这里访问事件。然后，可以使用这些云应用来分析事件并评估设备可能遇到的威胁。

云工具确定是否使用您发送的事件。请查阅工具的文档，或检查事件数据，以确保您不会将未使用的事件发送到云（这会浪费带宽和存储空间）。请记住，这些工具从同一来源提取事件，因此您的选择应反映您使用的所有工具，而不仅仅是限制性最强的工具。例如：

- CDO 中的安全分析和日志记录工具可以利用所有连接事件。
- 威胁响应仅使用高优先级连接事件，因此无需将所有连接事件都发送到云端。此外，它将仅使用安全智能高优先级事件。

开始之前

必须先向云服务注册设备，然后才能启用此服务。

在美国地区通过 https://visibility.amp.cisco.com/，在欧盟地区通过 https://visibility.eu.amp.cisco.com，以及在 APJC 地区通过 https://visibility.apjc.amp.cisco.com 可以连接至威胁响应。您可以在 YouTube 上观看视频 (http://cs.co/CTRvideos)，了解此应用的使用方法和优点。有关详细信息，请参阅 https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html 处提供的 *Cisco Secure Firewall Threat Defense* 和 *SecureX* 威胁响应集成指南。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **云服务**链接。

如果已经位于“系统设置”(System Settings) 页面，只需点击目录中的**云服务 (Cloud Services)**。

步骤 2 点击用于**将事件发送至思科云**选项的**启用/禁用**控件，可以根据需要更改设置。

步骤 3 当您启用该服务时，系统会提示您选择要发送到云的事件。稍后，您可以点击所选事件列表旁边的**编辑**以更改这些选项。选择要发送的事件类型并点击**确定**。

- **文件/恶意软件** - 适用于在任何访问控制规则中应用的任何文件策略。
- **入侵** - 适用于在任何访问控制规则中应用的任何入侵策略。
- **连接** - 适用于已启用日志记录的访问控制规则。选择此选项后，您还可以选择发送所有连接事件，或者只发送高优先级连接事件。高优先级连接事件是指与触发入侵、文件或恶意软件事件的连接相关，或与匹配安全智能阻止策略的连接相关。

取消注册云服务

如果不想再使用任何云服务，则可以从云中取消注册设备。您可能希望在从服务中删除设备或以其他方式处理设备时取消注册。如果需要更改云服务区域，请先取消注册，然后在重新注册时选择新区域。

使用此程序从云中取消注册不会影响智能许可注册。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **云服务**链接。

如果已经位于“系统设置”(System Settings) 页面，只需点击目录中的**云服务 (Cloud Services)**。

步骤 2 从齿轮 (⚙) 下拉列表中选择**取消注册云服务**。

步骤 3 阅读警告并点击**取消注册**。

已启用的任何云服务都将自动禁用，并且您将无法再启用这些服务。但现在会显示注册云的控件，您可以重新注册。

启用或禁用网络分析

启用网络分析可根据页面点击量向思科提供匿名产品使用情况信息。这类信息包括查看的页面、在页面上花费的时间、浏览器版本、产品版本、设备主机名等。此信息可帮助思科确定功能使用模式，帮助思科改进产品。所有使用情况数据均为匿名数据，且不会传输敏感数据。

默认启用网络分析。

过程

步骤 1 点击**设备 (Device)**，然后点击**系统设置 (System Settings)** > **网络分析 (Web Analytics)** 链接。

如果已经位于“系统设置”页面中，只需点击目录中的**网络分析 (Web Analytics)**。

步骤 2 点击**网络分析 (Web Analytics)** 功能的**启用/禁用 (Enable/Disable)** 控件，根据需要更改设置。

配置 URL 过滤首选项

系统从思科综合安全情报(CSI) (思科 Talos 情报小组 (Talos)) 获取 URL 类别和信誉数据库。这些首选项控制数据库更新和系统如何处理类别或信誉未知的 URL。必须启用 URL 过滤许可证，才能设置这些首选项。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **URL 过滤首选项**链接。

如果已经位于“系统设置”(System Settings) 页面中，只需依次点击目录中的 **URL 过滤首选项 (URL Filtering Preferences)**

步骤 2 配置以下选项：

- **启用自动更新** - 允许系统自动检查和下载更新的 URL 数据，这些数据中包括类别和信誉信息。系统每30分钟检查一次更新，不过数据通常每天更新一次。默认会启用更新。如果取消选中该选项，并且在使用类别和信誉过滤，请定期启用该功能以获得新的 URL 数据。
- **URL 查询源**- 要获取 URL 的类别和信誉的查询源。
  - **Local Database Only**- 仅在本地 URL 过滤数据库中查找类别和信誉。如果没有匹配项，URL 将被取消分类，没有信誉。此方法可能会受到限制，特别是在存储有限的低端系统上，因此 URL 过滤数据库较小。
  - **本地数据库和 Cisco 云**- 这是推荐的选项。如果本地数据库中没有匹配项，则会查询思科云以获取更新的类别/信誉信息。如果及时收到响应，则将其用于匹配目的。否则，如果没有匹配项，URL 将被取消分类，没有信誉。
  - **仅 Cisco 云**- 始终向 Cisco 云查询类别和信誉信息。请勿使用本地 URL 数据库。
- **URL 生存时间**（选择**对未知 URL 查询 Cisco CSI** 时可用）- 特定 URL 的类别和信誉查找值的缓存时间。生存时间到期时，下一个 URL 访问尝试将导致新的类别/信誉查找。更短的时间会产生更准确的 URL 过滤，较长的时间会给未知 URL 带来更好的表现。您可以将 TTL 设置为 2、4、8、12、24 或 48 小时、一周或从不（默认）。

步骤 3 您可以根据需要**检查 URL 的类别**。

您可以检查特定 URL 的类别和信誉。在**待检查的 URL** 框中输入 URL，然后点击**前往**。系统会将您转至外部网站以查看结果。如果您对分类持有不同意见，请点击**提交 URL 类别争议**链接，将您的想法反馈给我们。

步骤 4 点击**保存 (Save)**。

从 设备管理器 切换到 管理中心 或 CDO

如果要从 设备管理器进行切换，您可以将 威胁防御 设备配置连接到 管理中心 或 CDO 进行管理

注释 CDO 可以使用云交付的管理中心来管理 威胁防御 设备。CDO 中的简化设备管理器功能仅适用于已经在此模式下管理 威胁防御 的现有用户。此程序仅适用于云交付的管理中心。

当您使用 设备管理器执行 管理中心/CDO 设置时， 在您切换到 管理中心/CDO 进行管理时，除管理接口和管理器访问设置外，会保留在 设备管理器 中完成的 所有 接口配置。请注意，不会保留其他默认配置设置，例如访问控制策略或安全区。使用 威胁防御CLI 为 管理中心/CDO执行初始设置时，仅保留管理接口和管理器访问设置（例如，不保留默认的内部接口配置）。

切换到 管理中心/CDO后，您将无法再使用 设备管理器 管理 威胁防御 设备。

开始之前

如果防火墙已配置为高可用性，您必须首先使用 设备管理器 （如果可能）或 **configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

过程

步骤 1 如果您将防火墙注册到思科智能软件管理器，则必须在切换管理器之前取消注册防火墙。请参阅取消注册设备，第 88 页。

取消注册防火墙会释放基本许可证和所有功能许可证。如果不取消注册防火墙，这些许可证将保持分配给思科智能软件管理器中的防火墙。

步骤 2 （可能需要）配置管理接口。请参阅配置管理接口，第 234 页。

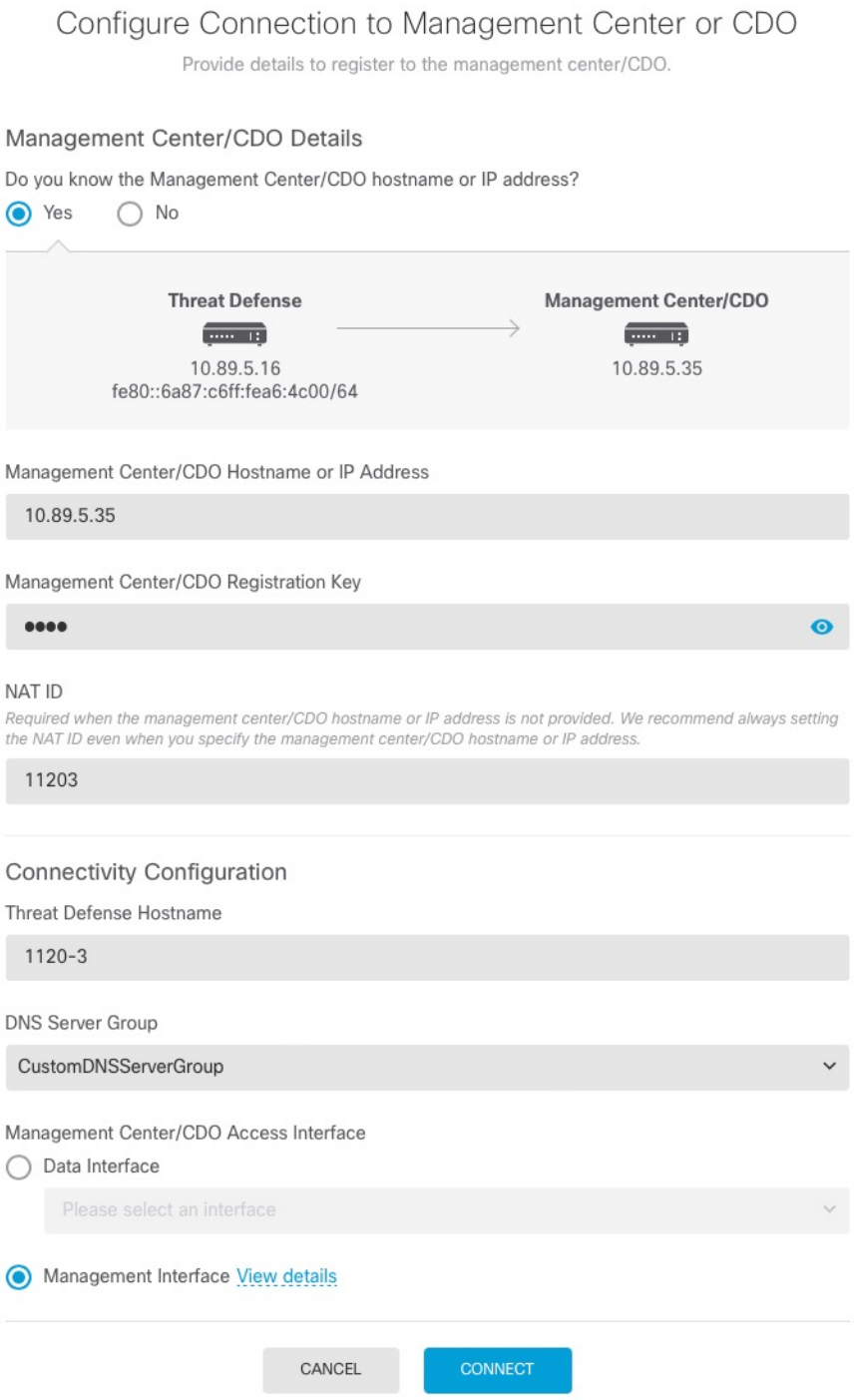
您可能需要更改管理接口配置，即使您打算使用数据接口访问管理器。如果您使用 设备管理器 连接的管理接口，则必须重新连接到 设备管理器 。

- 用于管理器访问的数据接口 - 管理接口必须将网关设置为数据接口。默认情况下，管理接口从 DHCP 接收 IP 地址和网关。如果您没有从 DHCP 接收到网关（例如，您没有将此接口连接到网络），则网关将默认为数据接口，并且您无需进行任何配置。如果您从 DHCP 接收到了网关，则需要使用静态 IP 地址配置此接口，并将该网关设置为数据接口。
- 用于管理器访问的管理接口 - 如果您要配置静态 IP 地址，请确保另将默认网关设置为唯一网关，而不是数据接口。如果您使用 DHCP，则无需进行任何配置，前提是您已成功从 DHCP 获取网关。

步骤 3 选择 **设备** > **系统设置** > **集中管理**，然后点击 **继续** 设置 管理中心/CDO 管理。

步骤 4 配置 **管理中心/CDO 详细信息**。

图 *52:* 管理中心/*CDO* 详细信息



a) 对于 **是否知道管理中心/CDO 主机名或 IP 地址**，如果您可以使用 IP 地址或主机名访问 管理中心/CDO，请点击 **是**，如果 管理中心/CDO 位于 NAT 之后或没有公共 IP 地址或主机名，请点击 **否**。

必须至少有一个设备（ 管理中心/CDO 或 威胁防御 设备）具有可访问的 IP 地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。

b) 如果您选择 **是**，则输入 **管理中心/CDO 主机名/IP 地址**。

c) 指定 **管理中心/CDO 注册密钥**。

此密钥是您选择的一次性注册密钥，注册威胁防御设备时也要在 管理中心/CDO上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 可用于将多台设备注册到 管理中心/CDO。

d) 指定 **NAT ID**。

此 ID 是您选择的唯一一次性字符串，您还需要在 管理中心/CDO上指定它。如果仅在其中一台设备上指定 IP 地址，则此字段必填；但建议您即使在知道两台设备的 IP 地址时，仍指定 NAT ID。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能 用于将任何其他设备注册到 管理中心/CDO。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。

步骤 5 配置**连接配置**。

a) 指定 **FTD 主机名**。

如果您使用数据接口进行 **管理中心/CDO 访问接口** 访问，则此 FQDN 将用于此接口。

b) 指定 **DNS 服务器组**。

选择现有组或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

如果要为 **管理中心/CDO 访问接口**选择数据接口，则此设置会设置 数据 接口 DNS 服务器。您使用安装向导设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。您可能会选择用于管理的相同 DNS 服务器组，因为管理和数据流量都通过外部接口到达 DNS 服务器。

在 管理中心/CDO上，数据接口 DNS 服务器在您分配给此 威胁防御 的平台设置策略中配置。当您将威胁防御设备添加到管理中心/CDO时，本地设置将保留，并且 DNS 服务器 不会 添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的 威胁防御 设备，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使 管理中心/CDO 和 威胁防御 设备同步。

此外，仅当在初始注册时发现 DNS 服务器， 管理中心/CDO 才会保留本地 DNS 服务器。

如果要为 **管理中心/CDO 访问接口**选择管理接口，则此设置会配置管理 DNS 服务器。

c) 对于 **管理中心/CDO 访问接口**，请选择任何已配置的接口。

将威胁防御设备注册到管理中心/CDO后，您可以将该管理器接口更改为管理接口或另一数据接口。

步骤 6 （可选） 如果您选择了数据接口，并且该接口不是外部接口，那么请添加默认路由。

您将看到一条消息，要求您检查是否有通过接口的默认路由。如果您选择了外部接口，那么您已经在安装向导中配置了此路由。如果您选择了其他接口，那么需要在连接到管理中心/CDO之前手动配置默认路由。 有关配置静态路由的更多信息，请参阅 配置静态路由，第 309 页 。

如果您选择了管理接口，那么需要先将网关配置为唯一网关，然后才能在此屏幕上继续操作。请参阅配置管理接口，第 234 页。

步骤 7 （可选） 如果您选择了数据接口，请点击**添加动态 DNS (DDNS) 方法**。

如果 IP 地址发生变化，DDNS 确保 管理中心/CDO 可接通完全限定域名 (FQDN) 的 威胁防御 设备。参阅**设备** > **系统设置** > **DDNS 服务**配置动态 DNS。

如果您在将威胁防御设备添加到管理中心/CDO之前配置 DDNS，则威胁防御设备会自动为 Cisco 受信任根 CA 捆绑包中的所有主要 CA 添加证书，以便威胁防御设备可以验证用于 HTTPS 连接的 DDNS 服务器证书。 威胁防御支持任何使用 DynDNS 远程 API 规范的 DDNS 服务器 (https://help.dyn.com/remote-access-api/)。

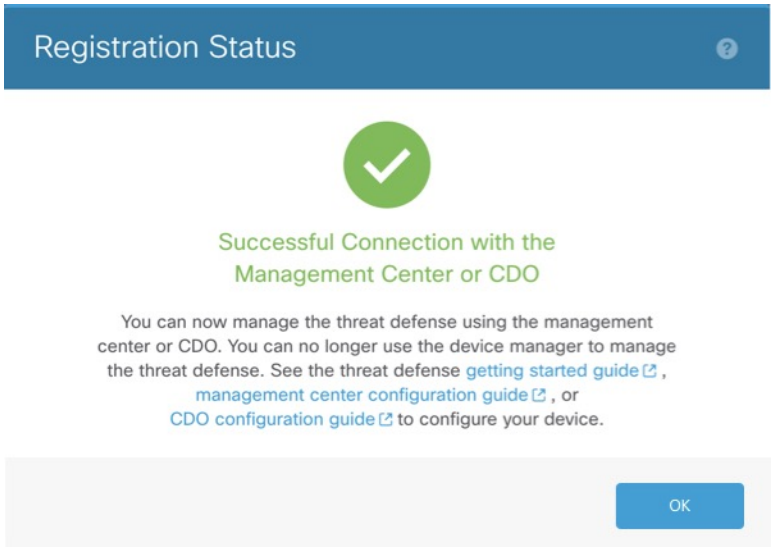
使用管理接口访问管理器时，不支持 DDNS。

步骤 8 点击**连接 (Connect)**。**注册状态** 对话框显示切换到 管理中心/CDO的当前状态。在 **保存管理中心/CDO 注册设置** 步骤后，转到管理中心/CDO，并添加防火墙。

如果要取消切换到 管理中心/CDO，请点击 **取消注册**。否则，请在 **保存管理中心/CDO 注册设置** 步骤之后关闭 设备管理器 浏览器窗口。如果这样做，该过程将暂停，并且只有在您重新连接到 设备管理器时才会恢复。

如果您在 **保存管理中心/CDO 注册设置** 步骤后保持连接到 设备管理器 ，您最终将看到 **与管理中心的成功连接或 CDO** 对话框。您将断开与 设备管理器的连接。

图 *53:* 成功连接



从 管理中心 或 CDO 切换到 设备管理器

您可以将当前由本地部署或云交付的管理中心管理的威胁防御设备配置为使用设备管理器设备。

您可以从管理中心切换到设备管理器，而无需重新安装软件。在从管理中心切换到设备管理器之前，请确认设备管理器 满足您的所有配置要求。如果要从 设备管理器 切换到 管理中心，请参阅 从 设备管理器 切换到 管理中心 或 CDO ， 第 755 页。

⚠

注意 切换到 设备管理器 会清除设备配置，并会使系统恢复默认配置。但是，管理 IP 地址和主机名保留不变。

过程

步骤 1 在 管理中心 中，从**设备 (Devices)** > **设备管理 (Device Management)** 页面删除防火墙。

步骤 2 使用 SSH 或控制台端口连接到 威胁防御 CLI。如果使用 SSH，请打开与 **管理 IP 地址**的连接，并使用 **admin** 用户名（或具有管理员权限的任何其他用户）登录 威胁防御 CLI。

控制台端口默认为 FXOS CLI。使用 **connect ftd** 命令连接到 威胁防御 CLI。SSH 会话直接连接到 威胁防御 CLI。

如果无法连接到管理 IP 地址，请执行以下操作之一：

- 确保管理物理端口连接到正常运行的网络。
- 确保为管理网络配置了管理 IP 地址和网关。使用 **configure network ipv4/ipv6 manual** 命令。

步骤 3 验证您当前处于远程管理模式之下。

show managers

示例：

```
> show managers
Type                       : Manager
Host                       : 10.89.5.35
Display name               : 10.89.5.35
Identifier                 : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration               : Completed
```

步骤 4 删除远程管理器，进入无管理器模式。

configure manager delete *uuid*

无法直接从远程管理转至本地管理。 如果定义了多个管理器，则需要指定标识符（也称为 UUID；请参阅 **show managers** 命令）。单独删除每个管理器条目。

示例：

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

步骤 5 配置本地管理器。

configure manager local

现在，您可以使用 Web 浏览器在 **https://***management-IP-address* 位置打开本地管理器。

示例：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

配置 TLS/SSL 密码设置

SSL 密码设置控制允许使用哪些 TLS 版本和加密密码套件来建立与设备的 TLS/SSL 连接。具体而言，这些设置控制在建立远程访问 VPN 连接时允许客户端使用的密码。

通常，您配置的密码套件应具有多个可用的加密密码套件。系统将确定客户端和威胁防御设备都支持的最高 TLS 版本，然后选择两者都支持且与该 TLS 版本兼容的密码套件。系统将选择两个终端都支持的最强 TLS 版本和密码套件，以确保在您允许的密码中建立最安全的连接。

开始之前

默认情况下，系统使用 DefaultSSLCipher 对象定义允许的密码套件。此对象中包含的密码取决于您的智能许可证账户是否启用了出口控制功能。此默认对象设置较低的安全级别，以确保尽可能多的客户端可以完成连接。还有默认的 Diffie-Hellman 组。仅当默认项不满足您的需求时，才需要配置这些设置。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **SSL 设置**链接。

步骤 2 配置以下选项：

- **密码** - 选择定义允许的 TLS 版本和加密算法的 SSL 密码对象。DefaultSSLCipher 对象设置的安全级别较低。将此对象替换为 CiscoRecommendedCipher 或您自己的自定义密码对象，以实施更

高的要求。理想的情况是，创建一个对象，其中包括所有且仅包括您希望允许的 TLS 版本和密码。

如果需要立即创建对象，请点击列表底部的**创建新密码**。

- **临时 Diffie-Hellman 组** - 用于临时加密算法的 DH 组。有关 DH 组的说明，请参阅 决定要使用的 Diffie-Hellman 模数组，第 616 页。默认值为 14。
- **椭圆曲线 DH 组** - 用于椭圆曲线加密算法的 DH 组。默认值为 19。

步骤 3 点击**保存 (Save)**。

配置 TLS/SSL 密码对象

SSL 密码对象定义在建立与 威胁防御 设备的 SSL 连接时可以使用的安全级别、TLS/DTLS 协议版本和加密算法的组合。在**设备** > **系统设置** > **SSL 设置**中使用这些对象为与设备建立 SSL 连接的用户定义安全要求。

您可以选择的 TLS 版本和密码由您的智能许可证账户控制。如果满足出口合规性要求，则可以选择选任意组合选项。如果您的许可证不符合出口要求，则只能使用最低安全选项 TLSv1.0 和 DES-CDC-SHA。评估模式被视为不合规模式，因此在许可系统之前，您的选项会受到限制。

系统中包括多个预定义对象。仅当预定义对象不符合安全要求时，才需要创建新对象。这些对象为：

- DefaultSSLCipher - 这是一个安全级别较低的组。它是 SSL 设置中使用的默认设置，用于确保尽可能多的客户端可以完成与系统的连接。它包括系统支持的所有协议版本和密码。
- CiscoRecommendedCipher - 这是一个安全级别较高的组，仅包括最安全的密码和 TLS 版本。此组具有最高的安全性，但您需要确保您的客户端可以使用匹配的密码。由于密码不匹配问题，某些客户端无法完成连接的可能性更大。

过程

步骤 1 选择**对象**，然后从目录中选择 **SSL 密码**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 输入对象的**名称**和说明（后者为可选项）。

步骤 4 配置以下选项：

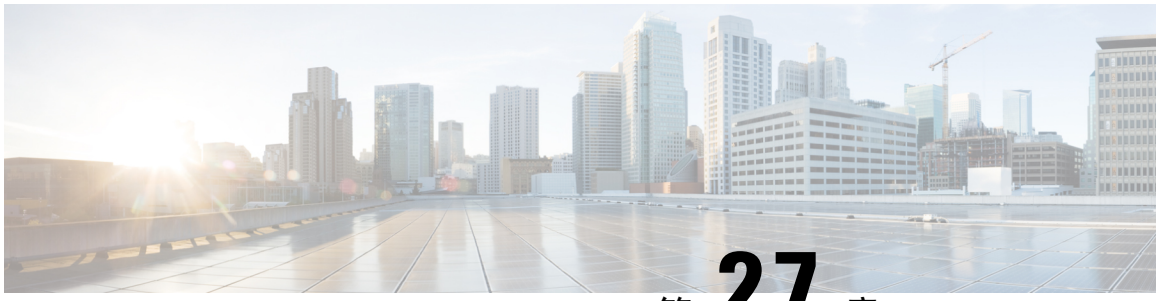
- **安全级别** - 对象的相对安全级别。请注意，如果在选择安全级别后编辑协议版本或密码套件列表，则对象提供的实际安全级别可能与选择的安全级别不匹配。选择以下其中一个选项：

- **全部** - 在对象中包括从低安全性到高安全性的所有 TLS 级别和密码套件。
- **低** - 包括所有 TLS 版本和密码，允许用户使用安全性最低的密码完成连接。对于非出口合规许可证，这包括 TLSv1.0 和 DES-CBC-SHA。
- **中** - 包括所有 TLS 版本，但会删除一些相对不安全的密码。此选项与“低”/“全部”选项之间的差异极小。不能将此选项用于非出口合规许可证。
- **高** - 仅允许最新的 DTLS 和 TLS 版本，以及适用于这些版本的密码。此选项将连接限制为当前可用的最安全密码。不能将此选项用于非出口合规许可证。
- **自定义** - 想要单独选择 TLS 版本和密码时选择此选项。您选择的选项将决定您是定义高安全加密设置还是低安全加密设置。虽然自定义对象没有默认设置，但如果您在选择自定义之前选择了另一个级别，则为方便起见，之前显示的选项将保持选中状态。

- **协议版本**- 允许客户端在与 威胁防御 设备建立 TLS/SSL 连接时使用的 TLS/DTLS 版本。对于自定义对象，请选择要支持的版本。对于其他安全级别，最好不要编辑列表，但您可以根据需要添加或删除版本。
- **适用的密码套件** - 客户端可以使用的加密算法。点击 **+** 可添加新套件；点击某个套件上的 **x** 可将其删除。

  您选择的协议版本控制此列表中可用的套件。如果更改协议版本，系统将标记不再适用于所选版本的所选套件：您必须删除这些版本或重新添加所需的协议版本。

步骤 5 点击**确定 (OK)**。



第 27 章

系统管理

以下主题介绍如何执行系统管理任务，例如更新系统数据库及备份和恢复系统。

安装软件更新

您可以安装系统数据库和系统软件的更新。以下主题介绍如何安装这些更新。

更新系统数据库和源

系统使用许多个数据库和安全智能源来提供高级服务。思科会对这些数据库和源提供更新，以便您的安全策略采用可用的最新信息。

系统数据库和源更新概述

威胁防御 使用以下数据库 和源 提供高级服务。

入侵规则

随着新的漏洞被发现，思科 Talos 情报小组 (Talos) 会发布入侵规则更新，您可以导入更新的规则。这些更新会影响入侵规则、预处理器规则和使用这些规则的策略。

入侵规则更新提供全新和更新的入侵规则及预处理器规则、现有规则的修改状态和修改的默认入侵策略设置。另外，规则更新还可能删除规则，提供新规则类别和默认变量，并修改默认变量值。

要使入侵规则更新所做的更改生效，必须重新部署配置。

入侵规则更新可能很大，所以请在网络使用量低的环境下更新重要规则。在慢速网络中，更新尝试可能会失败，您将需要重试。

地理位置数据库 (GeoDB)

Cisco 地理位置数据库 (GeoDB) 是一个与可路由的 IP 地址关联的地理数据数据库（例如国家、城市、坐标）。

GeoDB 更新提供物理位置的更新信息，系统会将这些信息与所检测到的可路由 IP 地址相关联。您可以使用地理位置数据作为访问控制规则的条件。

更新 GeoDB 所需的时间取决于您的设备；安装通常需要 30-40 分钟。虽然 GeoDB 更新不会中断任何其他系统功能（包括正在进行的地理位置信息收集），但更新执行时的确会占用系统资源。制定更新计划时需要考虑这一点。

漏洞数据库 (VDB)

思科漏洞数据库 (VDB) 包含主机可能易受感染的已知漏洞，以及操作系统、客户端和应用指纹。防火墙系统可将指纹与漏洞关联，帮助您确定某个特定主机是否会增加网络受攻击的风险。思科 Talos 情报小组 (Talos) 定期发布 VDB 更新。

更新漏洞映射所需的时间取决于网络映射中的主机数量。您可能希望在系统使用量低的期间安排更新，以尽可能地降低对任何系统停机的影响。一般说来，将网络中的主机数除以 1000，即可估算出执行更新所需的大致时间（分钟）。

在更新 VDB 后必须部署配置，才能使更新的应用检测器和操作系统指纹生效。

思科 Talos 情报小组 (Talos) 安全智能源

Talos 提供对安全智能策略中使用的定期更新智能源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。这些源包含已知威胁的地址和 URL。当系统更新源时，不必重新部署。新列表可用于评估后续连接。

URL 类别/信誉数据库

系统从思科综合安全智能 (CSI) 获取 URL 类别和信誉数据库。如果您配置过滤类别和信誉的 URL 过滤访问控制规则，请求的 URL 将根据数据库进行匹配。您可以在 **系统设置** > **URL 过滤首选项**上配置数据库更新和某些其他 URL 过滤首选项。您不能通过管理其他系统数据库更新的方式管理 URL 类别/信誉数据库更新。

更新系统数据库

您可以在方便之时，手动检索和执行系统数据库更新。从思科支持站点可检索更新。因此，系统的管理地址必须可连接互联网。

或者，您可以从互联网中自行检索更新软件包，然后从您的工作站上传这些更新软件包。此方法主要用于气隙网络，在其中没有用于从 Cisco 检索更新的互联网路径。从下载系统软件升级的相同文件夹中下载 software.cisco.com 的更新。

注释 在 2022 年 5 月，我们将 GeoDB 拆分为两个包：一个将 IP 地址映射到国家/地区/大洲的国家/地区代码包，以及一个包含与可路由 IP 地址相关的上下文数据的 IP 包。 设备管理器 没有，也从未使用过 IP 数据包中的信息。此拆分可在本地托管 威胁防御 部署中节省大量磁盘空间。如果您自己从 Cisco 获取 GeoDB，请确保获取国家/地区代码软件包，该软件包与旧的一体化软件包具有相同的文件名：Cisco_GEODB_Update-*date-build*。

另外，您还可以设置计划来定期检索和应用数据库更新。由于这些更新可能很大，所以请将它们安排在网络活动少的时间进行更新。

注释 在更新数据库时，您可能会发现用户界面响应操作的速度迟缓。

开始之前

为了避免对进行的更改造成任何潜在影响，请先将配置部署到设备，再手动更新这些数据库。

请注意，VDB 和 URL 类别更新可删除应用或类别。您需要更新使用这些已弃用项目的任何访问控制或 SSL 解密规则，然后才能部署更改。

过程

步骤 1 点击**设备**，然后点击“更新”摘要中的**查看配置**。

此时将打开“更新”(Updates) 页面。该页面上的信息显示每个数据库的当前版本，以及每个数据库的最后更新日期和时间。

步骤 2 要手动更新某数据库，请点击该数据库的相关部分中的以下其中一个选项：

- **从云进行更新**- 使 设备管理器 从 Cisco 检索更新软件包。这是最简单、最可靠的方法，但必须有一个到互联网的路径才能使用它。
- （**向下箭头**）>**选项**- 从您的工作站或连接到工作站的驱动器中选择更新包。该选项将是以下选项之一：
  - **选择文件** - 选择 VDB 或地理位置包。
  - **更新至更高版本** - 选择比当前安装的版本更高的入侵规则包。
  - **降级到更低版本** - 选择比当前安装的版本更低的入侵规则包。

规则和VDB更新需要部署配置，使其处于活动状态。当您从云端更新时，系统会询问是否要立即部署；点击**是**。如果点击**否**，请记住尽早启动部署作业。

如果上传自己的文件，则必须手动部署更改。

注释　手动上传入侵规则包时，请确保为您的 Snort 版本上传正确类型的包：为 Snort 2 上传 SRU；为 Snort 3 上传 LSP。您可以上传非活动 Snort 版本的包，但除非您切换版本，否则系统不会激活此包。有关切换 Snort 版本的信息，请参阅在 Snort 2 和 Snort 3 之间切换，第 504 页。

步骤 3　（可选）要设置定期数据库更新计划，请执行以下操作：

a) 点击所需数据库的**配置**链接部分。如果已有计划，请点击**编辑**。

数据库的更新计划是独立的。您必须单独定义计划。

b) 设置更新开始时间：

- 更新频率（每日、每周或每月）。
- 对于每周或每月更新，希望在星期几或每月几日执行更新。
- 希望开始更新的时间。 您指定的时间已根据夏令时调整，因此当您所在地区的时间被调整时，它会向前或向后移动一小时。如果您想要在全年确保此时间准确无误，您必须在时间被更改时编辑计划。

c) 对于规则或 VDB 更新，如果希望系统在更新数据库时部署配置，请选中**自动部署更新**复选框。

更新在完成部署之前无效。自动部署还将部署尚未部署的任何其他配置更改。

d) 点击**保存**。

注释　如果要删除定期更新计划，请点击**编辑**链接打开计划对话框，然后点击**删除**按钮。

更新思科安全智能源

思科 Talos 情报小组 (Talos) 提供对定期更新的安全智能源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。当系统更新源时，不必重新部署。新列表可用于评估后续连接。

如果要对系统从互联网更新源的时间进行严格控制，可以禁用该源的自动更新。但是，自动更新可确保获取最新的相关数据。

过程

步骤 1　点击**设备 (Device)**，然后点击“更新”(Updates) 摘要中的**查看配置 (Save)**。

此时将打开“更新”页面。页面上的信息显示**安全智能源**的当前版本以及其上次更新日期和时间。

步骤 2　要手动更新源，请点击**安全智能源 (Security Intelligence Feeds)** 组中的**立即更新 (Update Now)**。

如果您在高可用性组中的一台设备上手动更新源，也需要在另一台设备上手动进行此更新，以确保一致性。

步骤 3　（可选。）要配置定期更新频率，请执行以下操作：

a) 点击“思科源”(Cisco Feeds) 部分中的**配置 (Configure)** 链接。如果已有计划，请点击**编辑 (Edit)**。
b) 选择所需的频率。

   默认值为**每小时**。您还可以设置**每日**更新（指定具体时间）或**每周**更新（选择星期几和具体时间）。 您指定的时间已根据夏令时调整，因此当您所在地区的时间被调整时，它会向前或向后移动一小时。如果您想要在全年确保此时间准确无误，您必须在时间被更改时编辑计划。

   点击**删除 (Delete)** 阻止自动更新。

c) 点击**确定 (OK)**。

升级 威胁防御

使用此程序可升级 独立 威胁防御 设备。如果您需要更新 FXOS，请先执行此操作。 要升级高可用性威胁防御，请参阅升级 高可用性 威胁防御 ，第 212 页。

注意 升级时会丢弃流量。即使系统显示为非活动或无响应，也不要在升级过程中手动重新启动或关闭；您可以将系统置于不可用状态并要求重新映像。您可以手动取消失败或正在进行的主要和维护升级，并重试失败的升级。如果问题持续存在，请联系 思科 TAC。

有关升级过程中可能遇到的这些问题和其他问题的详细信息，请参阅威胁防御升级故障排除，第 773 页。

开始之前

完成预升级核对表。确保部署中保持正常运行，并且能够成功通信。

提示 升级前核对表包括规划（首先阅读Cisco Secure Firewall Threat Defense 版本说明）、备份、获取升级包以及执行相关升级（例如 Firepower 4100/9300 的 FXOS）。它还包括必要的配置更改检查、 就绪性检查、磁盘空间检查，以及运行和计划任务的检查。对于详细的升级说明，包括升级前的检查清单，请参阅适用于您的版本的《适用于设备管理器的 Cisco Secure Firewall Threat Defense 升级指南》。

过程

步骤 1 选择**设备 (Device)**，然后点击“更新”(Updates) 面板中的**查看配置 (View Configuration)** 。
“系统升级”(System Upgrade) 面板将显示当前运行的软件版本和您已上传的任何升级包。

步骤 2 上传升级包。

您只能上传一个软件包。如果上传新的软件包，它将替换旧的软件包。请确保您拥有适合您的目标版本和设备型号的软件包。点击**浏览 (Browse)** 或**替换文件 (Replace File)** 以开始上传。

上传完成后，系统将显示确认对话框。在点击**确定 (OK)** 之前，可以选择**立即运行升级 (Run Upgrade Immediately)** 以选择回滚选项并立即升级。如果您现在升级，请务必完成尽可能多的升级前核对表（请参阅下一步）。

步骤 3 执行最终的升级前检查，包括就绪性检查。

重新查看预升级核对表。确保您已完成所有相关任务，尤其是最终检查。 如果不手动运行就绪性检查，它将在您启动升级时运行。如果就绪检查失败，则会取消升级。有关详细信息，请参阅运行 威胁防御的升级就绪性检查 ，第 770 页。

步骤 4 点击 **立即升级** 以开始安装过程。

a) 选择回滚选项。

您可以**升级失败时，系统将自动取消升级并回滚至上一版本**。启用此选项后，设备会在主要或维护升级失败时自动返回到升级前的状态。如果您希望能够手动取消或重试失败的升级，请禁用此选项。

b) 点击**继续 (Continue)** 升级并重新启动设备。

您将自动注销并转到状态页面，您可以在其中监控升级，直到设备重新启动。该页面包含用于取消正在进行中的安装的选项。如果禁用了自动回滚并且升级失败，则可以手动取消或重试升级。

升级时会丢弃流量。 仅对于 ISA 3000，如果您为电源故障配置了硬件旁路，则在升级期间流量会被丢弃，但在设备完成其升级后重新启动时会通过而不进行检查。

步骤 5 尽可能重新登录并验证升级是否成功。

设备摘要页面显示当前运行的软件版本。

步骤 6 完成升级后的任务。

a) 更新系统数据库。如果没有为入侵规则、VDB 和 GeoDB 配置自动更新，请立即进行更新。
b) 完成发行说明中所述的其他任何升级后配置更改。
c) 部署。

运行 威胁防御的升级就绪性检查

在系统安装升级之前，它会运行就绪性检查，以确保升级对系统有效，并会检查有时会阻止成功升级的其他项目。如果就绪性检查失败，您应在再次尝试安装之前修复问题。如果检查失败，下次尝试安装时系统会提示您，并且您可以选择是否强制安装。

您还可以在启动升级之前手动运行就绪性检查，如本程序所述。

开始之前

上传要检查的升级软件包。

过程

步骤 1 选择**设备**，然后点击“更新”摘要中的**查看配置**。

系统升级部分将显示当前运行的软件版本和您已上传的任何更新。

步骤 2 查看**就绪性检查**部分。

- 如果尚未执行升级检查，请点击**运行升级就绪性检查**链接。此区域会显示检查进度。完成此过程大约需要 20 秒。
- 如果已执行升级检查，则此部分会指示检查是成功还是失败。对于失败的检查，请点击**查看详细信息**以查看有关就绪性检查的详细信息。修复问题后，再次运行检查。

步骤 3 如果就绪性检查失败，您应在安装升级之前解决问题。详细信息包括有关如何解决指示问题的帮助。对于失败的脚本，请点击**显示恢复消息**链接以查看信息。

以下是一些典型问题：

- FXOS 版本不兼容 - 在单独安装 FXOS 升级的系统（例如 Firepower 4100/9300）中，升级软件包可能需要与当前运行的 威胁防御 软件版本不同的最低 FXOS 版本。在这种情况下，您必须先升级 FXOS，然后才能升级 威胁防御 软件。
- 不受支持的设备型号 - 无法在此设备上安装升级软件包。您可能上传了错误的软件包，或者设备是旧型号，在新的 威胁防御 软件版本中不再受支持。请检查设备兼容性并上传支持的软件包（如果有）。
- 磁盘空间不足 - 如果可用空间不足，请尝试删除不需要的文件，例如系统备份。仅删除已创建的文件。

监控威胁防御升级

当您开始升级 威胁防御 时，系统会自动将您注销并转到状态页面，您可以在其中监控总体升级进度。该页面包含用于取消正在进行中的安装的选项。如果禁用了自动回滚并且升级失败，则该页面允许您手动取消或重试升级。

您还可以通过 SSH 连接到设备并使用 CLI： **show upgrade status**。添加 **continuous** 关键字可在创建日志条目时查看日志条目，添加**detail** 可查看详细信息。添加这两个关键字来获取持续的详细信息。

升级完成后，当设备重新启动时，您将失去对状态页面和 CLI 的访问权限。

取消中 或重试中 威胁防御 升级

使用升级状态页面或 CLI 以手动取消失败或正在进行的主要和维护升级，并重试失败的升级：

- 升级状态页面：点击**取消升级 (Cancel Upgrade)** 可取消正在进行的升级。如果升级失败，您可以点击**取消升级 (Cancel Upgrade)** 以停止作业并返回到升级前的设备状态，也可以点击**继续 (Continue)** 以重试升级。
- CLI：使用 **upgrade cancel** 以取消正在进行的升级。如果升级失败，您可以使用 **upgrade cancel** 以停止作业并返回到升级前的设备状态，也可以使用 **upgrade retry** 以重试升级。

注释 默认情况下，在升级失败时 威胁防御 自动将其恢复到升级前的状态（“自动取消”）。要能够手动取消或重试失败的 升级，请在启动升级时禁用自动取消选项。在高可用性部署中，自动取消会单独应用于每个设备。也就是说，如果一台设备上的升级失败，则仅恢复该设备。

修补程序不支持“取消”和“重试”。有关恢复成功升级的信息，请参阅恢复中 威胁防御，第 772 页。

恢复中 威胁防御

如果主要或维护升级成功但系统未按预期运行，则可以进行恢复。恢复 威胁防御 可将软件恢复到上次主要或维护升级前的状态；无法保留升级后配置更改。修补后恢复必然也会删除修补程序。请注意，您无法恢复单个修补程序或修补程序。

以下程序介绍如何从 设备管理器恢复。如果您无法进入 设备管理器，可以使用 **upgrade revert** 命令从 SSH 会话中的 威胁防御 命令行恢复。您可以使用该 **show upgrade revert-info** 命令查看系统将恢复到哪个版本。

开始之前

如果设备属于高可用性对，则必须恢复这两台设备。理想情况下，同时在两台设备上启动恢复，以便恢复配置，而不会出现故障转移问题。打开与两台设备的会话，并验证每台设备都可以恢复，然后启动恢复过程。请注意，在恢复期间流量将中断，因此请尽可能在非工作时间执行此操作。

对于 Firepower 4100/9300 机箱，主要 威胁防御 版本具有特别限定和推荐的配套 FXOS 版本。这意味着在恢复 威胁防御 软件后，您可能正在运行非推荐版本的 FXOS（太新）。尽管新版本的 FXOS 与旧版 威胁防御 版本向后兼容，但我们会对推荐的组合执行增强测试。您无法降级 FXOS，因此，如果您发现自己需要执行降级，并且想要运行推荐的组合，则需要重新映像设备。

过程

步骤 1 选择**设备**，然后点击**更新**摘要中的**查看配置**。

步骤 2 在**系统升级**部分中，点击**恢复升级**链接。

系统将显示确认对话框，其中显示当前版本以及系统将恢复到的版本。如果没有可恢复的可用版本，则不会显示**恢复升级**链接。

步骤 3 如果您熟悉目标版本（并且有一个目标版本可用），请点击**恢复**。

恢复后，必须向智能软件管理器重新注册设备。

威胁防御升级故障排除

当您升级任何设备时，无论是独立设备还是高可用性对，都可能发生这些问题。要解决特定于高可用性升级的问题，请参阅 高可用性 威胁防御升级故障排除，第 214 页。

升级包错误。

要查找升级包正确的型号，请在 思科支持和下载站点上选择或搜索您的型号，然后浏览至相应版本的软件下载页面。列出了可用的升级包以及安装包、修补程序和其他适用的下载。升级包文件名反映平台、软件包类型（升级、补丁、修补程序）、软件版本和内部版本。

从 6.2.1 及更高版本进行升级包经过签名，并在 .sh.REL.tar 中终止。请勿解压已签名的升级包。请勿通过邮件来重命名升级包或传送它们。

升级期间根本无法访问设备。

设备在升级期间或在升级失败时停止传输流量。升级之前，请确保来自您所在位置的流量不必遍历设备本身即可访问设备的管理界面。

设备在升级期间显示为非活动状态或无响应。

您可以手动取消正在进行的主要和维护升级；请参阅 取消中 或重试中 威胁防御 升级，第 771 页。如果设备无响应，或者如果您无法取消升级，请联系思科 TAC。

注意 即使系统显示为非活动状态，也不要在升级过程中手动重新启动或关闭。您可以将系统置于不可用状态并要求重新映像。

升级成功，但系统未按预期运行。

首先，确保缓存的信息得到刷新。不要简单地刷新浏览器窗口以重新登录。相反，请从URL中删除任何“额外”路径并重新连接到主页；例如，http://threat-defense.example.com/。

如果问题仍然存在并需要返回到较早的主要或维护版本，则可以恢复；请参阅 恢复中 威胁防御，第 772 页。如果无法恢复，则必须重新映像。

升级失败。

启动主要或维护升级时，请使用 **升级失败自动取消...**（自动取消）选项，用于选择升级失败时的操作，如下所示：

- 自动取消已启用（默认）：如果升级失败，则升级会取消，并且设备会自动恢复到升级前的状态。请更正所有问题，然后重试。
- 自动取消已禁用：如果升级失败，设备将保持原样。请更正问题并立即重试，或手动取消升级并稍后重试。

有关详细信息，请参阅取消中 或重试中 威胁防御 升级 ，第 771 页。如果无法重试或取消，或者问题持续存在，请联系思科 TAC。

重新映像设备

重新映像设备包括擦除设备配置和安装新软件映像。重新映像是为了通过出厂默认配置实现安全安装。

在以下情况下，您可以重新映像设备：

- 要将系统从 ASA 软件转换为 威胁防御软件。无法将运行 ASA 映像的设备升级为运行 威胁防御映像的设备。
- 设备无法正常工作，而修复配置的所有尝试均失败。

有关如何重新映像设备的信息，请参阅针对您的设备型号编写的 重新映像 *Cisco ASA* 或威胁防御设备 或 威胁防御快速入门 指南。如需查阅上述指南，请访问 http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html。

备份和恢复系统

您可以备份系统配置，这样在配置因后续配置错误或物理故障而受损时即可恢复设备。

仅当两台设备的型号相同且运行相同版本的软件（包括内部版本号，而不仅仅是相同的发布版）时，才可将备份恢复到替换设备上。请勿使用备份和恢复过程在设备之间复制配置。备份文件包含唯一标识设备的信息，所以不能按此方式进行共享。

注释 备份不包括管理 IP 地址配置。因此，恢复备份文件时，不会从备份副本中替换管理地址。这可以确保保存对地址所做的任何更改，并且还可以在其他网段的其他设备上恢复配置。备份也不包括许可或云注册信息，因此系统将保留恢复时存在的所有许可证或云注册状态。

备份仅包括配置，而不是系统软件。如果需要完全重新映像设备，您需要重新安装软件，然后才能上传备份和恢复配置。

在备份期间将锁定配置数据库。在备份期间不能更改配置，但可以查看策略、控制面板等。在恢复期间，系统完全不可用。

“备份和恢复”(Backup and Restore) 页面的表格将列出系统中可用的所有现有备份副本，包括备份的文件名、创建日期和时间及文件大小。备份类型（手动、预定或周期性）以您指示系统创建该备份副本的方式为基础。

提示 备份副本在系统中创建。您必须手动下载备份副本，并将它们存储到安全服务器上，以确保拥有执行灾难恢复所需的备份副本。系统在设备上最多保留 3 个备份副本。新备份将替换最早的备份。

以下主题介绍如何管理备份和恢复操作。

立即备份系统

您可以根据需要随时开始备份。

过程

步骤 1 点击**设备**，然后点击“备份和恢复”摘要中的**查看配置**。

点击后随即会打开“备份和恢复”(Backup and Restore) 页面。表格中将列出系统中可用的所有现有备份副本。

步骤 2 依次点击**手动备份** > **立即备份**。

步骤 3 输入备份名称和说明（后者为可选项）。

如果决定以后再进行备份（而不是立即进行），可以改为点击**计划**。

步骤 4 （可选。）选择**加密文件**选项以加密备份文件。

如果选择该选项，则必须输入恢复备份文件所需的**密码**（并**确认密码**）。

步骤 5 （仅限于 ISA 3000）选择**备份文件的位置**。

您可以在**本地硬盘**或 **SD 卡**上创建备份。使用 SD 卡的好处是，您可以使用卡将配置恢复到替换设备。

步骤 6 点击**立即备份**。

系统将开始备份过程。备份完成后，备份文件将显示在表格中。然后，您即可将备份副本下载到系统并存储到其他位置（如需）。

初始化备份后，即可离开“备份和恢复”(Backup and Restore) 页面。但是，系统可能会非常缓慢，您应考虑暂停您的工作以让备份完成。

此外，系统将在部分或所有备份期间获取配置数据库上的锁，这可能会阻止您在备份过程的持续时间内进行更改。

在预定时间备份系统

您可以设置预定备份，以便在将来的某个特定日期和时间备份系统。预定备份是一次性事件。如果要创建备份计划以定期创建备份，请配置周期性备份，而不是预定备份。

注释 如果要删除将来备份计划，请编辑该计划并点击**删除**。

过程

步骤 1 点击**设备**，然后点击“备份和恢复”摘要中的**查看配置**。

步骤 2 依次点击**预定备份** > **计划备份**。

如果您已经有计划备份，请点击**预定备份** > **编辑**。

步骤 3 输入备份名称和说明（后者为可选项）。

步骤 4 选择备份的日期和时间。

步骤 5 （可选。）选择**加密文件**选项以加密备份文件。

如果选择该选项，则必须输入恢复备份文件所需的**密码**（并**确认密码**）。

步骤 6 （仅限于 ISA 3000）选择**备份文件的位置**。

您可以在**本地硬盘**或 **SD 卡**上创建备份。使用 SD 卡的好处是，您可以使用卡将配置恢复到替换设备。

步骤 7 点击**计划**。

当选择的日期和时间到达时，系统将执行备份。完成后，备份将在备份表格中列出。

设置周期性备份计划

您可以设置周期性备份来定期备份系统。例如，您可以在每个周五的午夜执行备份。周期性备份计划有助于确保您始终拥有一组最近的备份。

注释 如果要删除周期性计划，请编辑该计划并点击**删除**。

过程

步骤 1 点击**设备**，然后点击“备份和恢复”摘要中的**查看配置**。

步骤 2 依次点击**周期性备份** > **配置**。

如果您已配置周期性备份，请依次点击**周期性备份** > **编辑**。

步骤 3 输入备份名称和说明（后者为可选项）。

步骤 4 选择**频率**和相关计划：

- **每日** - 选择一天的时间。系统每天在预定时间执行备份。
- **每周** - 选择星期几和当日的时间。系统将在您所选的每天的预定时间执行备份。例如，您可将备份安排在每个星期一、星期三和星期五的 23:00（晚上 11 点）进行。

- **每月** - 选择每月的日期和当日的时间。系统将在您所选的每天的预定时间执行备份。例如，您可将备份安排在每月一 (1) 日、十五 (15) 日和二十八 (28) 日的 23:00（晚上 11 点）进行。

您指定的时间已根据夏令时调整，因此当您所在地区的时间被调整时，它会向前或向后移动一小时。如果您想要在全年确保此时间准确无误，您必须在时间被更改时编辑计划。

步骤 5 （可选。）选择**加密文件**选项以加密备份文件。

如果选择该选项，则必须输入恢复备份文件所需的**密码**（并**确认密码**）。

步骤 6 （仅限于 ISA 3000）选择**备份文件的位置**。

您可以在**本地硬盘**或 **SD 卡**上创建备份。使用 SD 卡的好处是，您可以使用卡将配置恢复到替换设备。

步骤 7 点击**保存**。

到所选日期及时间时，系统执行备份。完成后，备份将在备份表格中列出。

周期性计划将持续执行备份，直到您更改或删除该计划为止。

恢复备份

只要设备运行的软件版本（包括内部版本号）与备份时相同，即可根据需要还原备份。只有两台设备的型号相同且运行相同版本的软件（包括内部版本号），才能将备份恢复到替换设备上。

不过，当设备属于高可用性对的一部分时，您无法恢复备份。您必须首先从**设备 (Device)** > **高可用性 (High Availability)** 页面中断高可用性，然后才能恢复备份。如果备份包括高可用性配置，设备将重新加入高可用性组。不要在两台设备上恢复相同备份，因为这两台设备都会变成活动状态。相反，您要在想要首先恢复活动状态的设备上恢复备份，然后在另一台设备上恢复等效备份。

如果设备中没有要恢复的备份副本，必须先上传该备份，才能进行恢复。

在恢复期间，系统完全不可用。

注释 备份不包括管理 IP 地址配置。因此，恢复备份文件时，不会从备份副本中替换管理地址。这可以确保保存对地址所做的任何更改，并且还可以在其他网段的其他设备上恢复配置。备份也不包括许可或云注册信息，因此系统将保留恢复时存在的所有许可证或云注册状态。

开始之前

如果要在其他系统上恢复备份，例如，在更换设备时，最佳做法是先注册设备并启用备份文件中配置的功能所需的所有可选许可证。备份文件不包含许可证或云服务信息，因此系统将保留在恢复之前所做的所有许可证更改或云注册。

过程

步骤 1 点击**设备**，然后点击“备份和恢复”摘要中的**查看配置**。

点击后随即会打开“备份和恢复”(Backup and Restore) 页面。表格中将列出系统中可用的所有现有备份副本。

步骤 2 如果可用的备份列表中没有要恢复的备份副本，请依次点击**上传** > **浏览**，并上传该备份副本。

步骤 3 点击该文件的恢复图标 ( )。

您需要确认恢复。默认情况下，恢复后系统将删除备份副本，但您可以事先选择**恢复后不删除备份**以保留备份副本，然后再继续进行恢复。

如果备份文件已加密，则必须输入打开文件和解密所需的**密码**。

恢复完成后，系统会重新启动。

注释 系统重新启动后，会自动检查漏洞数据库 (VDB)、地理位置和规则数据库更新，并根据需要进行下载。由于这些更新可能很大，因此初始尝试可能会失败。请检查任务列表，如果下载失败，请手动下载更新，如更新系统数据库，第 766 页中所述。系统还会重新部署策略。在更新成功之前，任何后续部署都将失败。

步骤 4 如有必要，请依次点击**设备** > **智能许可证** > **查看配置**，重新注册该设备，并重新启用所需的可选许可证。

备份不包括许可证或云注册信息。因此，如果将备份恢复到新系统（例如，在更换设备时），并且系统处于评估模式，则需要注册该设备并启用所需的所有许可证。如果在恢复之前注册设备并启用许可证，则无需进行其他更改。

如果您只是将以前的备份恢复到同一系统，则无需对许可证或云注册进行任何更改。但是，请验证是否已启用所需的所有可选许可证，因为备份可能包括需要在创建备份后禁用的许可证的功能。

更换 ISA 3000 设备

您可以移除 ISA 3000 的 SD 卡，将其插入另一台 ISA 3000 设备。如果您在 SD 卡上创建系统备份，可以使用此功能轻松更换设备。只需取出故障设备的 SD 卡，并插入新的设备。然后即可通过备份进行恢复。

要确保您有必要的备份，请配置备份作业以在 SD 卡上创建备份。

管理备份文件

在创建新备份时，备份文件将列在“备份和恢复”(Backup and Restore) 页面。备份副本不会无限期保留：当设备上的磁盘空间使用率达到最大阈值时，系统将删除较早的备份副本以便为较新的备份腾出空间。此外，当您安装除热修复以外的任何升级时，所有备份文件都会被删除。因此，您应定期管理备份文件，确保保存最希望保留的特定备份。

您可以执行以下操作来管理备份副本：

- 将文件下载到安全存储 - 要将备份文件下载到您的工作站，请点击该文件的下载图标 ( )。然后，您就可以将该文件移到安全文件存储了。
- 将备份文件上传到系统 - 如果要恢复设备中不再可用的备份副本，请依次点击**上传 (Upload)** > **浏览文件 (Browse File)**，并从工作站上传文件。然后即可执行恢复。

注释 可以重命名上传的文件，以便与原始文件名匹配。此外，如果系统中的备份副本已超过 3 个，系统将删除最早的备份副本，以便为上传的文件腾出空间。无法上传使用较早的软件版本创建的文件。

- 恢复备份 - 要恢复备份，请点击该文件的恢复图标 ( )。系统在恢复期间不可用，恢复完成后将重新启动。在系统正常运行后，您需要部署配置。
- 删除备份文件 - 如果不再需要某个特定备份，请点击该文件的删除图标 ( )。您需要确认删除。删除后，则无法恢复备份文件。

审核与变更管理

您可以查看有关系统事件以及用户已执行操作的状态信息。此信息可以帮助您审核系统，并确保正确地管理系统。

依次点击**设备 (Device)** > **设备管理 (Device Administration)** > **审核日志 (Audit Log)** 可以查看审核日志。此外，您可以通过点击右上角的**任务列表 (Task List)** 或**部署 (Deployment)** 图标按钮查找系统管理信息。

以下主题介绍系统审核和变更管理的一些主要概念和任务。

审核事件

审核日志可包括以下类型的事件：

自定义源更新事件，自定义源更新失败

这些事件表示已成功完成或失败的自定义安全智能源更新。详细信息包括更新开始者，以及有关正在更新的源的信息。

自定义规则文件导入摘要事件

这些事件表明您导入了包含一个或多个自定义入侵规则的文件。事件中包括已添加、已更新和已删除规则数的摘要，以及显示有关已导入规则的详细信息的差异视图。

部署已完成，部署失败：作业名称或实体名称

这些事件表示部署作业已成功完成或失败。详细信息包括作业发起人以及与作业实体相关的信息。失败的作业包括与失败相关的错误消息。

详细信息还包括一个**差异视图**选项卡，其中显示了作业执行过程中部署到设备的更改。这里汇总了已部署实体的所有实体更改事件。

要过滤这些事件，只需点击**部署历史记录**预定义过滤器。请注意，这些事件的事件类型是部署事件，您无法仅过滤已完成或失败的事件。

事件名称包括用户定义的作业名称（如果进行了配置）或“用户（用户名）触发的部署”。其中还包括，在运行设备设置向导期间发生的“设备设置自动部署”和“设备设置自动部署（最后一步）”作业。

实体已创建、实体已更新、实体已删除：实体名称（实体类型）

这些事件表示对识别的实体或对象进行了更改。实体详细信息包括实施更改的人员以及实体名称、类型和ID。您可以过滤这些项目。详细信息还包括一个**差异视图**选项卡，其中显示了应用于对象的更改。

HA 操作事件

这些事件与有关高可用性配置的操作有关，它们可以是您发起的操作，也可以是系统发起的操作。HA 操作事件的类型为事件，但事件名称是以下项之一：

- **HA 已暂停** - 有意暂停系统上的 HA。
- **HA 已恢复** - 有意恢复系统上的 HA。
- **HA 已重置** - 有意重置系统上的 HA。
- **HA故障转移：设备切换模式** - 有意切换模式，或系统由于运行状况指标违规而进行了故障转移。此消息表明，主用对等体变为了备用设备，或备用对等体变为了主用设备。

高可用性同步已完成

主用设备的配置已与备用设备同步。事件包括与同步版本相比之前版本的更改信息。

已扫描接口列表

此事件表示您已扫描接口清单中的更改。

已放弃等待完成的更改

此事件表示已删除所有待完成的更改。此事件与先前的“部署已完成”事件之间由“实体已创建”、“实体已更新”以及“实体已删除”事件指明的所有更改均已删除，并且受影响对象的状态恢复到上一次部署的版本。

规则更新事件

运行 Snort 3 时，来自 LSPUpdateServer 实体的此事件显示在下载和安装新入侵规则包时添加、删除或更改的入侵规则相关详细信息。事件限制为 100 条规则，因此，如果添加、删除或更改的规则超过 100 条，则事件将无法提供完整的信息。对于 Snort 2 更新，系统不会显示此事件。

任务已开始，任务已完成，任务失败

任务事件表示系统或用户发起的作业的开始和结束。这两个事件将会整合到任务列表中的一个任务中，您可以通过点击右上角的**任务列表**按钮进行查看。

任务包括部署作业以及手动或计划的数据库更新等操作。任务列表中的任何项目都将与审核日志中的两个任务事件对应，指示任务开始、成功完成或失败。

用户已登录、用户已注销：用户名

这些事件显示用户登录和注销设备管理器的时间和源IP地址。主动注销和因空闲时间超时而自动注销都会引发“用户已注销”事件。

这些事件无关于与设备建立连接的 RA VPN 用户。它们也不包含登录/注销设备 CLI。

查看和分析审核日志

审核日志包括有关系统发起和用户发起事件的相关信息，例如，部署作业、数据库更新和登录/注销设备管理器。

有关日志中可以显示的事件类型的说明，请参阅审核事件，第 779 页。

过程

步骤 1 点击**设备**，然后点击**设备管理** > **查看配置**链接。

步骤 2 点击目录中的**审核日志**（如果未将其选定）。

事件将按照日期分组，一天内的事件按时间分组，日期/时间最新的事件排在列表顶部。最初，所有事件都处于折叠状态，只能看到时间、事件名称、发起事件的用户以及该用户的源 IP 地址。如果用户和 IP 地址为“系统”，这意味着事件是由设备自身发起的。

可以执行以下操作：

- 点击事件名称旁边的 >，可打开事件并查看详细信息。再次点击该图标可关闭事件。很多事件具有一系列简单的事件属性，例如，事件类型、用户名、源 IP 地址等。但实体和部署事件包含两个选项卡：
  - **摘要**显示基本事件属性。
  - **差异视图**显示现有的“已部署”配置与事件过程中所发生变更的对比信息。如果是部署作业，此视图可能会很长，需要滚动鼠标才能完整查看。它将汇总部署作业过程中实体事件变更的所有差异。
- 从过滤器字段右侧的下拉列表中选择不同的时间范围。默认是查看过去 2 周的事件，但您可以更改范围，查看过去 24 小时、7 天、1 个月或 6 个月的事件。点击**自定义 (Custom)** 可通过输入开始和结束日期与时间指定具体范围。
- 点击日志中的任意链接，为该条目添加搜索过滤器。列表会更新，仅显示包含该条目的事件。您也可以点击**过滤器 (Filter)** 框，直接构建过滤器。此外，还可以点击过滤器框下方的预定义过滤器，加载相关的过滤条件。有关过滤事件的详细信息，请参阅过滤审核日志，第 782 页。

- 重新加载浏览器页面将会刷新日志，以显示最新事件。

过滤审核日志

您可以对审核日志应用过滤器，将视图显示范围缩小到仅显示特定类型的消息。过滤器中的每个元素都是一个准确、完全的匹配。例如，“User = admin”仅显示名为 **admin** 的用户发起的事件。

您可以单独或组合使用以下方法来构建过滤器：每次添加过滤器元素时，列表都会自动更新。

点击预定义过滤器

过滤器字段下方是预定义的过滤器。点击链接即可加载过滤器。系统将要求您进行确认。如果您已应用过滤器，该过滤器会被替换，也不会添加该过滤器。

点击高亮显示的条目

要构建过滤器，最简单的方法是点击日志表或事件详细信息中包含作为过滤标准的值的条目。点击条目后，**过滤器**字段将替换为该值和元素组合的格式设置正确的元素。但是，使用此方法要求现有的事件列表中包含所需的值。

如果可以为条目添加过滤器元素，当您将鼠标指针悬停在该条目上时，该条目会标有下划线，并显示命令**点击添加到过滤器**。

选择原子元素

此外，您还可以通过以下方法创建过滤器：点击**过滤器**字段，从下拉列表中选择所需的原子元素，在等号后面键入匹配值，然后按 Enter 键。您可以过滤以下元素。请注意，对于每种类型的事件而言，并非所有元素都是相关的。

- **事件类型** - 事件类型通常与事件名称（不含实体名称或用户等变量限定符）相同，但并非总是这样。部署事件的事件类型是“部署事件”。有关事件类型的说明，请参阅审核事件，第 779 页。
- **用户** - 发起事件的用户的名称。系统用户采用字母全部大写的形式：SYSTEM。
- **源 IP** - 用户发起事件的源 IP 地址。系统发起事件的源 IP 地址是 SYSTEM。
- **实体 ID** - 实体或对象的 UUID，这是一种比较长且不可读的字符串，例如 8e7021b4-2e1e-11e8-9e5d-0fc002c5f931。通常，要使用此过滤器，您需要点击事件详细信息中的实体 ID，或使用 REST API 通过相关 GET 调用检索所需的 ID。
- **实体名称** - 实体或对象的名称。对于用户创建的实体，实体名称通常是您为对象指定的名称，例如，将网络对象命名为 InsideNetwork。对于系统生成的实体或（在某些情况下）用户定义的实体，实体名称是预定义但可识别的名称，例如，将没有明确命名的部署作业命名为“User (admin) Triggered Deployment”。
- **实体类型** - 实体或对象的类型。这些是预定义但可识别的名称，例如 Network Object。您可以通过查看相关对象模型的“type”值，在 API Explorer 中查找实体类型。API 类型通常采用字母全部小写形式，且不含空格。如果您完全按照模型中所示输入类型，则按 Enter 键

时，字符串会变成可读性更强的格式。这两种输入方式都可以接受。要打开 API Explorer，点击更多选项按钮 (⋮) 并选择 **API Explorer**。

复杂审核日志过滤器的规则

在构建包含多个原子元素的复杂过滤器时，请记住以下规则：

- 相同类型的元素在该类型的所有值之间具有 OR 关系。例如，包括“User = admin”和“User = SYSTEM”将会匹配由任一用户发起的事件。
- 不同类型的元素之间为 AND 关系。例如，包括“Event Type = Entity Updated”和“User = SYSTEM”仅会显示由系统而非活动用户更新实体的事件。
- 您不能使用通配符、正则表达式、部分匹配或简单的文本字符串匹配。

检查部署和实体更改历史记录

部署和实体事件在事件详细信息中包括**差异视图**选项卡。此选项卡以彩色显示旧配置与更改之间的对比情况。

- 对于部署作业，此对比为部署之前设备上运行的配置与实际所部署更改之间的对比。
- 对于实体事件，这些是对之前版本的对象所做的配置更改。之前的版本可能是实际设备使用的版本，也可能是对象尚未部署的变化。

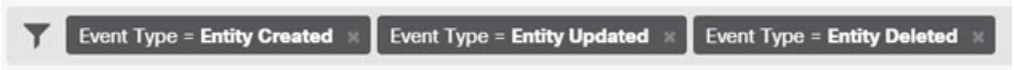
过程

步骤 1 点击**设备**，然后点击**设备管理** > **查看配置**链接。

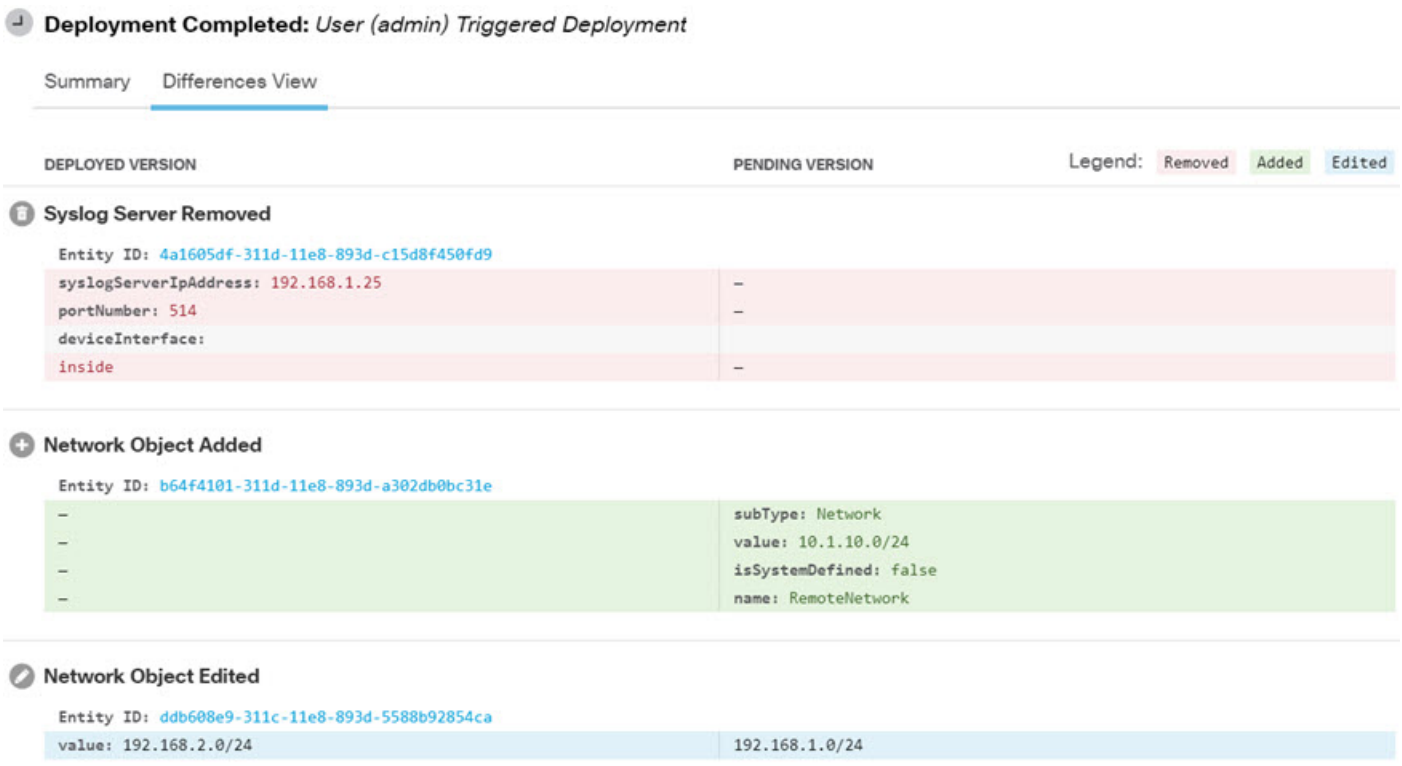
步骤 2 点击目录中的**审核日志**（如果未将其选定）。

步骤 3 （可选。）过滤消息：

- 部署事件 - 点击过滤器框下的**部署历史记录**预定义过滤器。
- 实体更改事件 - 使用事件类型元素为您感兴趣的更改类型手动创建过滤器。要查看所有实体更改，请选择实体已创建、实体已更新和实体已删除这三种规格。过滤器应如下所示：



步骤 4 打开事件，然后点击**差异视图**选项卡。



所做的更改会使用颜色编码，标题指示对象的类型以及对象是被添加（创建）、移除（删除）还是编辑（更新）。编辑的对象仅显示已更改或从该对象删除的属性。在部署作业中，每个更改的实体都有单独的标题。标题表明对象的实体类型。

放弃所有待处理更改

如果您对一套尚未部署的配置更改不满意，您可以放弃所有待处理的更改。此操作使所有功能均恢复到设备上存在的状态。之后，您可以再重新开始部署配置更改。

过程

步骤 1 点击网页右上角的**部署更改 (Deploy Changes)** 图标。

如存在待处理的更改，系统会用圆点高亮显示。

步骤 2 依次点击**更多选项 (More Options)** > **全部放弃 (Discard All)**。

步骤 3 点击确认对话框中的**确定 (OK)**。

系统将放弃更改，操作完成后您会看到一条表示没有待处理更改的消息。系统会在审核日志中添加“已放弃待处理的更改”事件。

导出设备配置

可以 JSON 格式导出一份当前部署的配置。可以使用该文件进行归档或备案。密码和密钥等所有敏感数据均被屏蔽。

无法将文件导入此设备或其他设备。此功能不会取代系统备份。

必须至少完成一个成功的部署作业，才能下载配置。

过程

步骤 1 选择**设备 (Device)**，然后点击**设备管理 (Device Administration)** 组中的**查看配置 (View Configuration)**。

步骤 2 点击目录中的**下载配置 (Download Configuration)**。

步骤 3 点击**获取设备配置 (Get Device Configuration)** 启动创建文件的作业。

如果您之前创建了一个文件，您将看到一个下载按钮和一条含文件创建日期的**文件可供下载**消息。

生成文件可能需要几分钟的时间，具体取决于配置的大小。检查任务列表或审核日志，或者定期返回到此页面，直到导出配置作业完成并生成文件。

步骤 4 生成文件后，返回到此页面并点击**下载配置文件 (Download the Configuration File)** 按钮 () 将文件保存到工作站。

管理 设备管理器 和 威胁防御 用户访问

您可以为登录到威胁防御的用户配置外部身份验证和授权源（HTTPS 访问）。您可以将外部服务器与本地用户数据库和系统定义的 **admin** 用户结合使用，或不使用后两者。请注意，您无法创建用于设备管理器 访问的额外本地用户帐户。

虽然您可以有多个可以更改配置的外部 设备管理器用户帐户，但用户不跟踪这些更改。当一个用户部署更改时，所有用户做出的更改均被部署。没有任何锁定：即，多个用户可能会尝试在同一时间更新同一对象，这将导致只有一个用户能够成功保存更改。您也无法基于用户丢弃更改。

您可以有 5 个并发用户会话。如果第六个用户登录，开始时间最早的用户会话会自动注销。还有空闲超时，非活动用户空闲 20 分钟后注销。

您还可以为对 威胁防御 CLI 的 SSH 访问配置外部身份验证和授权。在使用外部源之前，总是会检查本地数据库，以便您可以创建其他本地用户，实现故障保护访问。请勿在本地源和外部源中重复创建用户。除 **admin** 用户之外，CLI 和 设备管理器 用户之间没有任何交叉：用户帐户是完全独立的。

注释 使用外部服务器时，您可以通过设置单独的 AAA 服务器组，或在仅允许用户访问特定 威胁防御 设备 IP 地址的 AAA 服务器中创建身份验证/授权策略，来控制用户对您部分设备的访问。

以下主题介绍如何配置和管理 设备管理器 用户访问和 CLI 用户访问。

为设备管理器 (HTTPS) 用户配置外部授权 (AAA)

您可以从外部 AAA 服务器提供对 设备管理器 的 HTTPS 访问权限。通过启用 AAA 身份验证和授权，您可以提供不同级别的访问权限，使并非每个用户都通过本地 **admin** 账户登录。

这些外部用户还有权访问 威胁防御API 和 API Explorer。

您可以通过在 AAA 服务器中设置管理用户的授权来提供基于角色的访问控制 (RBAC)。级别因服务器类型而异。用户登录 设备管理器后，页面右上角将显示用户名和角色：管理员、读写用户或只读用户。在 RADIUS 服务器上正确设置账户后，您可以使用此程序启用账户，以进行管理访问。

SAML 用户授权

在配置 SAML 服务器身份源时，标识包含授权级别的字段。您可以配置具有以下类型的授权访问的外部用户：管理员、审核管理员、加密管理员、读写用户、只读用户。请参阅 配置 SAML 服务器，第 165 页。

RADIUS 用户授权

要提供基于角色的访问控制 (RBAC)，请更新 RADIUS 服务器上的用户账户以定义 **cisco-av-pair** 属性（注意这是在 ISE 中，而在 Free RADIUS 中该属性拼写为 Cisco-AVPair；请检查系统的拼写是否正确）。必须在用户账户上正确定义此属性，否则系统会拒绝用户访问 设备管理器。以下是受支持的 **cisco-av-pair** 属性值：

- **fdm.userrole.authority.admin** 提供完全管理员访问权限。这些用户可以执行本地 **admin** 用户可以执行的所有操作。
- **fdm.userrole.authority.rw** 提供读写访问权限。这些用户可以执行只读用户可以执行的任何操作，还可以编辑和部署配置。唯一的限制是无法执行关键系统操作，包括安装升级、创建和恢复备份、查看审核日志以及中止 设备管理器 用户的会话。
- **fdm.userrole.authority.ro** 提供只读访问权限。这些用户可以查看控制面板和配置，但无法进行任何更改。如果用户尝试进行更改，会显示错误消息，指明权限不足。

过程

步骤 1 点击**设备**，然后依次点击**系统设置** > **管理访问**链接。

如果您已位于“系统设置”(System Settings) 页面，只需点击目录中的**管理访问 (Management Access)**。

步骤 2 点击 **AAA 配置**选项卡（如果未将其选定）。

步骤 3 配置 **HTTPS 连接**选项：

- **管理/REST API 的服务器组**-选择您想要用作主要身份验证源的RADIUS或SAML服务器组（用于外部身份验货/授权）或本地用户数据库 (LocalIdentitySource)。

  如果尚不存在服务器组，点击链接立即创建服务器组。对于 RADIUS，您还需要为每个服务器创建 RADIUS 服务器对象，将这些对象添加到组（定义服务器组时可以执行此操作）。有关 RADIUS 的详细信息，请参阅 RADIUS 服务器和组，第 158 页。 有关 SAML 的信息，请参阅 配置 SAML 服务器，第 165 页。

- **使用本地身份源进行身份验证** （仅限 RADIUS）- 如果您选择外部 RADIUS 服务器组，可以指定如何使用包含本地 **admin** 用户账户的本地身份源。选择以下一个选项：
  - **在外部服务器之前** - 系统首先对照本地源检查用户名和密码。
  - **在外部服务器之后** - 仅当外部源不可用或在外部来源中找不到用户账户时，才检查本地源。
  - **从不** -（不推荐。）从不使用本地源，因此不能以 admin 用户身份登录。

    注意 如果您选择 **从不**，将无法使用 **管理员** 账户登录 设备管理器 。如果 AAA 服务器不可用，或者未在 AAA 服务器中配置账户，您将被锁定在系统外面。

注释 使用 SAML 时，**LOCAL 身份验证** 不适用。使用 SAML，您始终可以通过输入本地用户名和密码使用本地数据库登录，因为您必须明确点击 **单点登录 (SSO)** 链接才能输入SAML凭证。

步骤 4 点击**保存 (Save)**。

配置 威胁防御 CLI (SSH) 用户外部授权 (AAA)

您可以从外部 RADIUS 服务器提供对 威胁防御 CLI 的 SSH 访问权限。通过启用 RADIUS 身份验证和授权，您可以从单个身份验证源提供不同级别的访问权限，而无需在每台设备上定义单独的本地用户账户。

这些 SSH 外部用户**不**具备访问 威胁防御 API 和 API Explorer 的权限。用于定义 SSH 授权的机制不同于 HTTPS 访问权限所需的机制。但是，您可以配置同时符合 SSH 和 HTTPS 授权条件的 RADIUS 用户，以便指定用户可以通过两种协议访问系统。

要为 SSH 访问权限提供基于角色的访问控制 (RBAC)，请更新 RADIUS 服务器上的用户账户，以定义 **Service-Type** 属性。必须在用户账户上定义此属性，否则系统会拒绝用户对设备的 SSH 访问。以下是受支持的 **Service-Type** 属性值：

- **管理 (6)** 提供对 CLI 的 **config** 访问授权。这些用户可以在 CLI 中使用所有命令。
- **NAS 提示 (7)** 或除级别 6 以外的任何级别 - 提供 CLI 的**基本**访问授权。这些用户可以使用只读命令（例如 **show** 命令），用于监控和故障排除。

在 RADIUS 服务器上正确设置账户后，您可以使用此程序启用账户，以进行 SSH 管理访问。

注释 请勿在本地源和外部源中重复创建用户。如果创建了重复的用户名，请确保它们具有相同的授权权限。当本地用户账户的授权权限不同时，您无法使用外部版本用户账户的密码登录；您仅可使用本地密码登录。如果权限相同，假定密码不同，则您使用的密码将确定您是登录到外部用户还是本地用户中。即使先检查本地数据库，如果本地数据库中存在用户名但密码不正确，还是会检查外部服务器，如果外部源的密码正确，则登录成功。

开始之前

请告知外部定义的用户以下操作，使他们合理设置预期：

- 外部用户首次登录时，威胁防御 会创建所需的结构，但不能同时创建用户会话。用户只需再次进行身份验证，即可启动会话。用户将看到与以下消息类似的消息：“已识别新的外部用户名。请重新登录以启动会话。”
- 同样地，如果自上次登录以来，Service-Type 中定义的用户授权发生了更改，则用户将需要重新进行身份验证。用户将看到与以下消息类似的消息：“您的授权权限已更改。请重新登录以启动会话。”

过程

步骤 1 点击**设备**，然后依次点击**系统设置** > **管理访问**链接。

如果您已位于“系统设置”(System Settings) 页面，只需点击目录中的**管理访问 (Management Access)**。

步骤 2 点击 **AAA 配置**选项卡（如果未将其选定）。

步骤 3 配置 **SSH 连接**选项：

- **服务器组** - 选择您想要用作主要身份验证源的 RADIUS 服务器组或本地用户数据库 (LocalIdentitySource)。必须选择要使用外部授权的 RADIUS 服务器组。

  如果尚不存在服务器组，点击**创建新 RADIUS 服务器组**链接立即创建服务器组。您还需要为每个服务器创建 RADIUS 服务器对象，将这些对象添加到组（定义服务器组时可以执行此操作）。有关 RADIUS 的详细信息，请参阅 RADIUS 服务器和组，第 158 页。

  请注意，SSH 连接仅使用组中的前 2 个服务器。如果使用的组中包含 3 个或更多的服务器，系统永远不会尝试其余的服务器。此外，系统也不会使用**空载时间**和**最大失败尝试次数**组属性。

- **使用本地身份源进行身份验证** - 如果您选择外部服务器组，则可以指定如何使用本地身份源。对于 SSH 访问，系统始终会在检查外部服务器之前检查本地数据库。

步骤 4 点击**保存 (Save)**。

管理设备管理器用户会话

依次选择**监控** > **会话**，查看当前登录到 设备管理器的用户的列表。列表会显示当前会话每个用户登录的持续时间。

如果相同的用户名出现多次，则表示用户从不同的源地址打开会话。系统根据用户名和源地址单独跟踪会话，而且每个会话具有唯一时间戳。

系统允许 5 个并发用户会话。如果第六个用户登录，开始时间最早的当前会话会自动注销。此外，非活动状态长达 20 分钟的空闲用户会被自动注销。

如果 设备管理器 用户输入错误的密码且连续 3 次尝试登录失败，则该用户的账户将锁定 5 分钟。用户必须待锁定时间结束后方可尝试重新登录。无法解锁 设备管理器用户账户，也无法调整重试计数或锁定超时。（请注意，对于 SSH 用户，可以调整这些设置并解锁账户。）

如果有必要，您可以通过点击会话的删除图标 () 终止用户会话。如果您删除您自己的会话，您也会被注销。结束会话没有锁定时段：用户可以立即重新登录。

启用备用 HA 设备上的外部用户设备管理器访问权限

如果为设备管理器用户配置了外部授权，则这些用户可以登录到高可用性对的主用和备用设备。但是，与登录主用设备相比，首次成功登录备用设备还需要执行一些额外操作。

外部用户首次登录到主用设备后，系统会创建一个对象，定义用户和用户的访问权限。随后，管理员或读写用户必须在主用设备上，为要在备用设备上显示的用户对象部署配置。

只有在部署和后续配置同步成功完成之后，外部用户才可登录到备用设备。

管理员和读写用户在登录到主用设备后可以部署更改。但是，只读用户无法部署配置，且必须请求拥有适当权限的用户部署配置。

为威胁防御 CLI 创建本地用户账户

可以在威胁防御设备上为CLI访问创建用户。这些账户不允许访问管理应用，仅允许访问CLI。CLI对于故障排除和监控非常有用。

您不能一次性在多个设备上创建本地用户账户。每个设备都有自己的一组唯一本地用户 CLI 账户。

过程

步骤 1 使用具有配置权限的账户登录设备 CLI。

管理员用户账户具有所需的权限，但具有配置权限的任何账户都可以执行操作。您可以使用 SSH 会话或控制台端口。

对于某些设备型号，控制台端口会带您进入 FXOS CLI。使用 **connect ftd** 命令进入 威胁防御 CLI。

步骤 2 创建用户账户。

configure user add *username* {**basic** | **config**}

您可以使用以下权限级别定义用户：

- **config** - 提供用户配置访问权限。此级别将赋予用户完整管理员权限，让其可以输入所有配置命令。
- **basic** - 提供用户基本访问权限。此级别不允许用户输入配置命令。

示例：

以下示例将添加一个名为 joecool 且具有配置访问权限的用户账号。在您键入密码时，密码不会显示。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

注释 告知用户他们可以使用 **configure password** 命令更改密码。

步骤 3 （可选。）根据安全要求调整该账户的特性。

您可以使用以下命令更改默认账户行为。

- **configure user aging** *username max_days warn_days*

  设置用户密码的到期日。指定密码最大有效天数，以及密码到期前向用户发出密码即将到期警告的天数。两个值均介于 1 到 9999 之间，但是警告天数必须小于最大天数。当您创建账户时，密码没有到期日。

- **configure user forcereset** *username*

  强制用户下次登录时更改密码。

- **configure user maxfailedlogins** *username number*

  设置在锁定账户之前您允许的最大连续失败登录次数，该值介于 1 至 9999 之间。使用 **configure user unlock** 命令解锁账户。新账户的默认值为 5 次连续失败登录。

- **configure user minpasswdlen** *username number*

  设置最小密码长度，此值介于 1 至 127 之间。

- **configure user strengthcheck** *username* {**enable** | **disable**}

  启用或禁用密码强度检查，此检查要求用户在更改密码时要满足特定的密码条件。如果用户密码到期或使用了 **configure user forcereset** 命令，则此要求会在用户下次登录时自动启用。

步骤 4 根据需要管理用户账户。

用户可能被锁定在账户之外了，也可能您需要删除账户或解决其他问题。使用以下命令管理系统中的用户账户。

- **configure user access** *username* {**basic** | **config**}

  更改用户账户的权限。

- **configure user delete** *username*

  删除指定的账户。

- **configure user disable** *username*

  禁用指定的账户，而不将其删除。用户无法登录，直到您启用该账户为止。

- **configure user enable** *username*

  启用指定的账户。

- **configure user password** *username*

  更改指定用户的密码。通常情况下，用户应使用 **configure password** 命令更改自己的密码。

- **configure user unlock** *username*

  解锁因超出最大连续失败登录尝试次数而被锁定的用户账户。

重启或关闭系统

如有必要，可以重新启动或关闭系统。

除了以下操作过程，还可以使用 **reboot** 或 **shutdown** 命令通过 SSH 会话或 设备管理器 CLI 控制台执行这些任务。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **重新启动/关闭** > 链路。

如果已经位于“系统设置”页面中，只需点击目录中的**重新启动/关闭 (Reboot/Shutdown)**

步骤 2 点击执行所需功能的按钮。

- **重新启动** - 如果认为系统运行不正确，而其他方法均无法解决问题，则可以重新启动设备。此外，可能有几个操作过程要求重新启动设备以重新加载系统软件。
- **关闭** - 关闭系统，以控制方式关闭电源。例如，如果想要从网络中删除设备（例如，为了更换设备），请使用“关闭”按钮。关闭设备后，可以用硬件开/关按钮重新打开设备。

步骤 3 等待操作完成。

如果您与防火墙建立了控制台连接，请在防火墙关闭时留意系统提示。您将看到以下提示：

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

对于 ISA 3000，完成关闭后，系统 LED 将熄灭。至少等待 10 秒，然后再断开电源。

重新启动或关闭系统时，无法在 设备管理器 或 CLI 中执行其他操作。

重新启动期间，设备管理器页面应在重新启动完成后刷新，并将您带至登录页面。如果在重新启动完成之前尝试刷新页面，则 Web 浏览器可能会基于该时间点的 设备管理器 Web 服务器运行状态返回 503 或 404 错误。

如果关闭设备，系统最终将无法响应，您将收到404错误。这是正常结果，因为您完全关闭了系统。

系统故障排除

以下主题介绍一些系统级故障排除任务和功能。有关对特定功能（如访问控制）进行故障排除的信息，请参阅相应功能的章节。

Ping 地址以测试连接

ping 是一种简单命令，可用于确定特定地址是否处于活动状态以及是否会做出响应。这意味着基本连接正常工作。然而，在设备上运行的其他策略可能会阻止特定类型的流量成功通过设备。您可通过打开 CLI 控制台或登录设备 CLI 来使用 **ping** 。

注释 由于系统有多个接口，您可以控制用于 ping 地址的接口。必须确保使用正确的命令，以便测试重要的连接。例如，系统必须能够通过管理接口访问思科许可证服务器，因此您必须使用 **ping system** 命令测试连接。如果使用 **ping**，则测试的是能否通过数据接口访问地址，这可能不会得到相同的结果。

正常 ping 使用 ICMP 数据包测试连接。如果您的网络禁止 ICMP，可以换用 TCP ping（仅用于数据接口 ping）。

您可以对 IP 地址或完全限定主机名 (FQDN) 执行 ping。要对 FQDN 执行 ping，为管理接口或数据接口配置的 DNS 服务器必须成功返回 IP 地址。必须为管理接口和数据接口分别配置 DNS 服务器。如果没有为特定接口配置 DNS 服务器，请使用 **dig** 命令查找给定 FQDN 的 IP 地址。

以下是 ping 网络地址的主要选项。

通过管理接口 ping 地址

使用 **ping system** 命令。

ping system *host*

主机可以是 IP 地址或完全限定域名 (FQDN)，例如 www.example.com。不同于通过数据接口进行 ping 操作，系统 ping 没有默认计数。ping 操作会持续执行，直到您使用 Ctrl+c 将其停止。例如：

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

使用路由表，通过数据接口 ping 地址

使用 **ping** 命令。测试的是系统一般能否找出通往主机的路由。因为这是系统正常路由流量的方式，所以您通常需要对此进行测试。

ping *host*

例如：

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

注释 您可以指定超时、重复计数、数据包大小甚至发送时所用的数据模式。在 CLI 中使用帮助指示符 ? 查看可用的选项。

通过特定数据接口 ping 地址

如果要通过特定数据接口测试连接性，可使用 **ping interface** *if_name* 命令。

ping interface *if_name host*

例如：

```
> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

使用 TCP ping，通过数据接口 ping 地址

使用 **ping tcp** 命令。TCP ping 发送 SYN 数据包，如果目标发送了 SYN-ACK 数据包，则认为 ping 取得了成功。

ping tcp [**interface** *if_name*] *host port*

您必须指定主机和 TCP 端口。

您可以选择指定接口，即 ping 的源接口，而不是用于发送 ping 的接口。此类 ping 通常使用路由表。

TCP ping 发送 SYN 数据包，如果目标发送了 SYN-ACK 数据包，则认为 ping 取得了成功。例如：

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

注释 您还可以指定 TCP ping 的超时、重复计数和源地址。在 CLI 中使用帮助指示符？查看可用的选项。

跟踪主机路由

如果您向某个IP地址发送流量时遇到问题，可以跟踪主机路由以确定网络路径是否有问题。traceroute 的工作方式是从无效端口向目标发送 UDP 数据包或者向目标发送 ICMPv6 回应。通往目标沿途的路由器以 ICMP Time Exceeded 消息响应，并向 traceroute 报告该错误。每个节点会收到三个数据包，因此对于每个节点，您有三次机会获得信息性结果。您可通过打开 CLI 控制台或登录设备 CLI 来使用 **traceroute** 。

注释 通过数据接口 (**traceroute**) 或通过虚拟管理接口 (**traceroute system**) 跟踪路由有单独的命令。请务必使用正确的命令。

下表说明了输出中显示的每个数据包的可能结果。

输出符号	说明
*	在超时期限内未收到对探测的响应。
nn msec	各节点指定探测数的往返时间（以毫秒为单位）。
!N.	无法访问 ICMP 网络。
!H	无法访问 ICMP 主机。
!P	ICMP 协议不可达。
!A	管理性禁止 ICMP。

输出符号	说明
?	未知 ICMP 错误。

通过虚拟管理接口跟踪路由

使用 **traceroute system** 命令。

traceroute system *destination*

主机可以是 IPv4/IPv6 地址或完全限定域名 (FQDN)，例如 www.example.com。例如：

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

通过数据接口跟踪路由

使用 **traceroute** 命令。

traceroute *destination*

如果为数据接口配置 DNS 服务器，主机可以是 IPv4/IPv6 地址或完全限定域名 (FQDN)，例如 www.example.com。如果没有为特定接口配置 DNS 服务器，请使用 **dig** 命令查找给定 FQDN 的 IP 地址。例如：

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

注释 您可以指定超时、生存时间、每个节点的数据包数量，乃至要用作 traceroute 源的 IP 地址或接口。在 CLI 中使用帮助指示符 ? 查看可用的选项。

使设备显示在跟踪路由上

默认情况下，威胁防御不会在跟踪路由上显示为跃点。要使其显示，您需要递减通过设备的数据包上的生存时间，并增加对 ICMP 不可达消息的速率限制。要实现此目的，您必须创建配置所需的服务策略规则和其他选项的 FlexConfig 对象。

有关服务策略和流量类别的详细讨论，请参阅《思科 *ASA* 系列防火墙配置指南》，网址为 https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html。

注释 如果减少生存时间，系统会丢弃 TTL 为 1 的数据包，但会为会话打开一个连接，前提是假设该连接可能包含具有更大 TTL 的数据包。请注意，某些数据包（例如 OSPF hello 数据包）发送时 TTL = 1，因此减去生存时间可能会导致意外后果。定义流量类时，请注意这些事项。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。

步骤 3 创建减小 TTL 的对象。

a) 点击 + 按钮以创建新的对象。

b) 为对象输入名称。例如，**Decrement_TTL**。

c) 在**模板**编辑器中，输入以下命令，包括缩进。

```
icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  set connection decrement-ttl
```

d) 在**取消模板**编辑器中，输入撤消此配置所需的命令。

正如要让命令启用模板需要添加父命令以进入正确的子模式那样，您也需要在取消模板中添加这些命令。

取消模板将在您从 FlexConfig 策略删除此对象（部署成功后删除）时，以及不成功的部署期间应用（将配置重置为之前的状态）。

因此，在本示例中，取消模板为：

```
no icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  no set connection decrement-ttl
```

e) 点击**确定**保存对象。

步骤 4 将对象添加到 FlexConfig 策略中。

仅部署在 FlexConfig 策略中选择的对象。

a) 点击目录中的 **FlexConfig 策略**。
b) 在组列表中点击 **+**。
c) 选择 Decrement_TTL 对象，然后点击**确定**。

系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。

d) 点击**保存**。

您现在可以部署策略。

NTP 故障排除

系统靠时间准确一致来正常运行，并确保事件和其他数据点得到准确处理。您必须配置至少一个（最好是三个）网络时间协议 (NTP) 服务器来确保系统始终能获得可靠的时间信息。

设备摘要连接图（在主菜单中点击**设备 (Device)**）显示至 NTP 服务器的连接状态。如果状态为黄色或橙色，说明与配置的服务器存在连接问题。如果连接问题仍然存在（不仅仅是一个临时问题），请尝试以下操作。

- 首先，确保在**设备** > **系统设置** > **NTP** 上配置至少三个 NTP 服务器。尽管不要求配置至少三个 NTP 服务器，但这样做可以大大提高可靠性。
- 确保管理接口 IP 地址（在**设备** > **系统设置** > **管理接口**中定义）与 NTP 服务器之间存在网络路径。
  - 当管理接口网关是数据接口时，如果默认路由不充足，则可以在**设备** > **路由**上配置到 NTP 服务器的静态路由。
  - 如果设置了显式管理接口网关，请登录设备 CLI，并使用 **ping system** 命令测试与每个 NTP 服务器之间是否存在网络路径。
- 登录设备 CLI，并使用以下命令检查 NTP 服务器的状态。
  - **show ntp**- 此命令显示 NTP 服务器的基本信息及其可用性。但是， 设备管理器 中的连接状态使用其他信息指示其状态，所以此命令的显示以及连接状态图的显示可能存在不一致的地方。还可从 CLI 控制台发出此命令。
  - **system support ntp** - 此命令包括 **show ntp** 的输出以及标准 NTP 命令 **ntpq**（该命令记录在 NTP 协议中）的输出。如果需要确认 NTP 同步，请使用此命令。

    查找“Results of ‘ntpq -pn’ ”部分。例如，您可能会看到类似如下的内容：

```
Results of 'ntpq -pn'
remote                  : +216.229.0.50
refid                   : 129.7.1.66
st                      : 2
t                       : u
when                    : 704
poll                    : 1024
```

```
reach                   : 377
delay                   : 90.455
offset                  : 2.954
jitter                  : 2.473
```

在本例中，NTP 服务器地址前的 + 表示作为潜在候选者。此处的星号 * 表示当前的时间源对等体。

NTP 后台守护程序 (NTPD) 使用每个对等体中的八个示例的滑动窗口，并选出一个示例，然后根据时钟选择确定正确的报时器和错误的断续器。然后，NTPD 会确定往返距离（候补者的偏移不得超过往返延迟的一半）。如果连接延迟、丢包或服务器问题导致一个或全部候补者被拒绝，则同步中会出现较长的延迟。而且，该调整很长一段时间后才会完成：时钟偏移和振荡器错误必须通过时钟训练算法解决，这可能会需要数小时的时间。

注释 如果 refid 是 .LOCL.，则表明对等体是一个未经训练的本地时钟，也即它只使用其本地时钟来设置时间。如果所选的对等体是 .LOCL.，则 设备管理器 始终将 NTP 连接标为黄色（未同步）。如果还有更好的证书，NTP 通常不会选择 .LOCL. 证书，这就是应配置至少三个服务器的原因所在。

为管理接口排除 DNS 故障

必须配置至少一个DNS服务器供管理接口使用。需要使用该服务器来云连接到智能许可、数据库更新（如 GeoDB、规则和 VDB）等服务，和处理其他需要域名解析的任何活动。

配置 DNS 服务器非常简单。只需在初始配置设备时输入所用 DNS 服务器的 IP 地址。随后可在**设备 (Device)** > **系统设置 (System Settings)** > **DNS 服务器 (DNS Server)** 页面进行更改。

但是，由于网络连接问题或 DNS 服务器本身的问题，系统可能会无法解析完全限定域名 (FQDN)。如果您发现系统无法使用您的DNS服务器，请考虑以下操作来识别和解决问题。另请参阅常规DNS问题故障排除，第 744 页。

过程

步骤 1 确定是否存在问题。

a) 使用 SSH 登录设备 CLI。

b) 输入 **ping system www.cisco.com**。如果您获得类似于下文的“未知主机”消息，系统将无法解析域名。如果 ping 操作成功，问题得到解决：DNS 正常工作。（按 Ctrl+C 可停止 ping 命令。）

```
> ping system www.cisco.com
ping: unknown host www.cisco.com
```

注释 务必在 **ping** 命令中添加 **system** 关键字。**system** 关键字通过管理 IP 地址执行 ping 操作，该接口也是使用管理DNS服务器的唯一接口。访问 www.cisco.com 也是一个不错的选择，因为您需要到该服务器的路由以获得智能许可和更新。

步骤 2 验证管理接口的配置。

a) 依次点击**设备 (Device)** > **接口 (Interfaces)**，编辑管理接口，并验证以下内容。如果您进行更改，点击**保存**后会立即应用所做的更改。如果您更改管理地址，需要重新连接并重新登录。

- 管理网络的网关IP地址是正确的。如果您使用数据接口作为网关，后续步骤将验证该配置。
- 如果您不使用数据接口作为网关，请验证管理 IP 地址/子网掩码和网关 IP 地址位于同一子网。

b) 依次点击**设备 (Device)** > **系统设置 (System Settings)** > **DNS 服务器 (DNS Server)**，并验证是否正确配置 DNS 服务器。

如果您在网络边缘部署设备，运营商可能会对您可以使用的 DNS 服务器提出特定要求。

c) 如果您使用数据接口作为网关，确认您具有所需的路由。

您需要为 0.0.0.0 提供默认路由。如果 DNS 服务器不能使用默认路由的网关，您可能需要额外的路由。这种情况基本分为两类：

- 如果您使用 DHCP 获取外部接口的地址且选择 **使用 DHCP 获取默认路由 (Obtain Default Route using DHCP)** 选项，默认路由在 设备管理器中不可见。从 SSH 输入 **show route** 验证是否存在适用于0.0.0.0的路由。由于这是外部接口的默认配置，您可能会遇到这样的情况。（请转至 **设备** > **接口** 查看外部接口的配置。）
- 如果您在外部接口上使用静态 IP 地址或不从 DHCP 获取默认路由，则打开**设备** > **路由**。验证已为默认路由使用正确的网关。

如果无法通过默认路由访问 DNS 服务器，则必须在**路由页**为其定义静态路由。请注意，不应为直连网络（即直接连接到系统任何数据接口的网络）添加路由，因为系统可以自动路由到这些网络。

此外，验证没有静态路由将发往服务器的流量错误引导至不正确的接口。

d) 如果部署按钮指示存在未部署的更改，请现在部署这些更改并等待部署完成。

e) 重新测试 **ping system www.cisco.com**。如果问题仍然存在，继续执行下一步。

步骤 3 在 SSH 会话中，输入 **dig www.cisco.com**。

- 如果 **dig** 指示可获取 DNS 服务器的响应，但服务器找不到名称，这意味着，DNS 已正确配置，但所用的 DNS 服务器没有适用于 FQDN 的地址。此错误由 NXDOMAIN 状态指示。响应应类似于以下内容：

```
> dig www.cisco.com

; <<>> DiG 9.11.4 <<>> www.cisco.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 43246
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 78b1c6b2b3ef5b689fc2f65260db9e9b36a7d9fefb301943 (good)
;; QUESTION SECTION:
;www.cisco.com.                 IN      A

;; AUTHORITY SECTION:
.                       3600    IN      SOA     a.root-servers.net.
nstld.verisign-grs.com. 2021062901 1800 900 604800 86400

;; Query time: 13 msec
;; SERVER: 10.163.47.11#53(10.163.47.11)
;; WHEN: Tue Jun 29 22:28:43 UTC 2021
;; MSG SIZE  rcvd: 145
```

解决方案：在这种情况下，您需要配置不同的DNS服务器，或获取已更新的服务器，使其能够解析需要解析的 FQDN。联系您的网络管理员或 ISP，获取可用于您网络的 DNS 服务器的 IP 地址。

- 如果命令超时，系统将无法访问DNS服务器，或所有DNS服务器目前均有故障，无法响应（不太可能出现这种情况）。继续进行下一步。

步骤 4 使用 **traceroute system** *DNS_server_ip_address* 命令追踪到 DNS 服务器的路由。

例如，如果 DNS 服务器为 10.100.10.1，请输入：

```
> traceroute system 10.100.10.1
```

下文是可能出现的结果：

- 跟踪路由完成并到达 DNS 服务器。在这种情况下，实际上存在通向 DNS 服务器的路由，且系统可以访问该服务器。因此，没有任何路由问题。但是，由于某种原因，到此服务器的DNS请求没有获得响应。

  解决方案：可能是因为沿该路径的路由器或防火墙丢弃 UDP/53 流量，这是用于 DNS 的端口。您可以沿其他网络路径尝试连接DNS服务器。这种问题比较棘手，因为您需要确定哪个节点阻止流量，并联系系统管理员才能更改访问规则。

- 跟踪路由连一个节点都无法访问，其响应如下所示：

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
(and so forth)
```

  解决方案：在这种情况下，系统存在路由问题。尝试为网关IP地址执行 **ping system**。按照之前步骤中的介绍重新验证管理接口的配置，确保您已配置所需的网关和路由。

- 跟踪路由可以通过几个节点，之后便不再能够解析路由，其响应如下所示：

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.475 ms  0.532 ms  0.542 ms
```

```
2  10.88.127.1 (10.88.127.1)  0.803 ms  1.434 ms  1.443 ms
3  site04-lab-gw1.example.com (10.89.128.25)  1.390 ms  1.399 ms  1.435 ms
4  * * *
5  * * *
6  * * *
```

解决方案：这种情况下，路由在最后一个节点出现问题。您可能需要联系系统管理员，以在该节点安装正确的路由。但是，如果有意地在该节点不设置通往DNS服务器的路由，您需要更改网关，或创建自己的静态路由， 使其指向可以将流量路由到 DNS 服务器的路由器。

分析 CPU 和内存使用情况

要查看有关CPU和内存使用情况的系统级信息，请依次选择**监控**>**系统**，然后查找CPU和“内存”条形图。这些图表显示通过 CLI 使用 **show cpu system** 和 **show memory system** 命令收集的信息。

如果打开 CLI 控制台或登录 CLI，还可以使用这些命令的其他版本查看其他信息。通常，只有当使用情况存在长时间持续的问题时，或者奉思科技术支持中心 (TAC) 之命，才会查看此信息。其中许多详细信息比较复杂，需要 TAC 加以解释。

以下是您可以检查的一些要点。您可以在Cisco Firepower Threat Defense 命令参考（网址为 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html）中找到有关这些命令的更多详细信息。

- **show cpu** 显示数据平面 CPU 使用情况。
- **show cpu core** 分别显示每个 CPU 核心的使用情况。
- **show cpu detailed** 显示其他每个核心及总数据平面的 CPU 使用情况。
- **show memory** 显示数据平面内存使用情况。

注释 某些关键字（上文未提及）需要先使用 **cpu** 或 **memory** 命令设置分析或其他功能。这些功能只能奉 TAC 之命使用。

查看日志

系统会记录各种操作的信息。您可以使用 **system support view-files** 命令打开系统日志。请在配合思科技术支持中心 (TAC) 解决问题时使用此命令，以便他们帮助您解释输出内容并选择要查看的相应日志。

该命令将显示一个菜单供您选择日志。请使用以下命令在向导中导航：

- 要更改为子目录，请键入该目录的名称并按 Enter 键。
- 要选择欲查看的文件，请在提示符后输入**s**。然后系统将提示您输入文件名。请键入完整名称，并注意区分大小写。文件列表会显示日志的大小，您最好考虑一下再打开非常大的日志。

- 看到 --More-- 时，按空格键可查看下一页日志条目；按 Enter 键仅查看下一个日志条目。到达日志末尾后，即会转到主菜单。--More-- 行会显示日志的大小和已查看部分的大小。**如果不想翻阅完整个日志，请使用 Ctrl+C 关闭日志并退出命令。**
- 键入 **b** 返回菜单结构的上一级。

如果要保持日志打开以便及时看到添加的新消息，请使用 **tail-logs** 命令而非 **system support view-files**。

以下示例显示如何查看 cisco/audit.log 文件，该文件用于跟踪系统登录尝试。文件列表首先在顶部列出目录，然后列出当前目录下的文件。

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>


([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

============================
Directory: /ngfw/var/log/cisco
-----------files------------
2017-02-13 22:44:42.394907 | 472        | audit.log
2017-02-13 23:40:30.858198 | 903615     | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0          | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338    | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338    | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218    | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848      | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160    | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login successful,

2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,
```

```
2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked account.,


<remaining log truncated>
```

创建故障排除文件

在提交问题报告时，思科技术支持中心 (TAC) 人员可能要求您提交系统日志消息。这些信息可帮助他们诊断问题。您无需提交诊断文件，除非要求您这样做。

以下步骤程序介绍了如何创建和下载诊断文件。

过程

步骤 1 点击**设备**。

步骤 2 在**故障排除**下，点击**请求创建文件**或**重新请求创建文件**（如果您之前已创建一份文件）。

系统将开始生成诊断文件。您可以转至其他页面，再返回此处检查状态。当该文件准备就绪后，会显示文件创建日期和时间及下载按钮。

步骤 3 当该文件准备就绪后，请点击下载按钮。

系统将使用浏览器的标准下载方法，将该文件下载到您的工作站。

不常见的管理任务

以下主题介绍您即便执行，也不会经常执行的操作。所有这些操作都可能清除您的设备配置。在进行这些更改之前，请确保设备当前没有向生产网络提供重要服务。

更改防火墙模式

威胁防御 防火墙可在路由模式或透明模式下运行。路由模式防火墙是指路由的跳跃，可作为连接到任一屏蔽子网的主机的默认网关。另一方面，透明防火墙是第 2 层防火墙，其作用相当于“网络嵌入式”或“隐形防火墙”，不会被视为路由器跳跃至相连设备。

本地 设备管理器仅支持路由模式。不过，如果需要在透明模式下运行该设备，则可以更改防火墙模式，开始使用 管理中心管理设备。相反，您可以将透明模式设备转换为路由模式，然后选择使用本地管理器对其进行配置（也可以使用 管理中心管理路由模式设备）。

无论执行本地还是远程管理，都必须使用设备 CLI 更改模式。

以下步骤程序介绍了使用本地管理器或计划使用本地管理器时如何更改模式。

注意 更改防火墙模式会清除设备配置，并会使系统恢复默认配置。但是，管理 IP 地址和主机名保留不变。

开始之前

如果要转换为透明模式，请先安装 管理中心 ，再更改防火墙模式。

如果启用了任何功能许可证，您必须首先在设备管理器中禁用它们，然后才能删除本地管理器和切换为远程管理。否则，这些许可证将仍旧分配给思科智能软件管理器中的设备。请参阅启用或禁用可选许可证，第 87 页。

如果设备已配置为高可用性，您必须首先使用设备管理器（如果可能）或 **configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

过程

步骤 1 使用 SSH 客户端打开与**管理 IP 地址**的连接，使用具有配置 CLI 访问权限的用户名登录设备 CLI。例如 **admin** 用户名。

连接到管理 IP 地址时，请务必执行此过程。使用 设备管理器时，您可以选择通过数据接口上的 IP 地址管理设备。但是，必须使用“管理”物理端口和管理 IP 地址来远程管理设备。

如果无法连接到管理 IP 地址，请解决以下问题：

- 确保管理物理端口连接到正常运行的网络。
- 确保为管理网络配置了管理 IP 地址和网关。在 设备管理器中，在**设备** > **系统设置** > **管理接口**上配置地址和网关。（在 CLI 中，使用 **configure network ipv4/ipv6 manual** 命令。）

  注释 确保使用外部网关作为管理 IP 地址。使用远程管理器时，不能将数据接口用作网关。

步骤 2 要从路由模式更改为透明模式，并且使用远程管理：

a) 禁用本地管理，并进入无管理器模式。

若有活动管理器，则无法更改防火墙模式。使用 **configure manager delete** 命令可删除管理器。

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

b) 将防火墙模式更改为透明。

configure firewall transparent

示例：

```
> configure firewall transparent
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

c) 配置远程管理器

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*]

其中：

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} 指定管理此设备的 管理中心 的 DNS 主机名或 IP 地址（IPv4 或 IPv6）。如果 管理中心无法直接寻址，请使用 **DONTRESOLVE**。如果使用 **DONTRESOLVE**，则需要使用 *nat_id*。
- *regkey* 是向 管理中心注册设备所需的唯一字母数字注册密钥。
- *nat_id* 是在管理中心与设备之间的注册流程中使用的可选字母数字字符串。如果主机名设置为 DONTRESOLVE，此项为必填项。

例如，要在 192.168.0.123 处使用该管理器，注册密钥为 **secret**，请输入以下信息：

```
> configure manager add 192.168.0.123 secret
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                      : 192.168.0.123
Registration Key          : ****
Registration              : pending
RPC Status                :
```

d) 登录 管理中心并添加设备。

有关详细信息，请参阅 管理中心在线帮助。

步骤 3 要从透明模式更改为路由模式并转换为本地管理，请执行以下操作：

a) 从 管理中心 注销设备。

b) 访问 威胁防御 设备 CLI，首选使用控制台端口。

由于更改模式会清除配置，管理 IP 地址将恢复为默认值，所以更改模式后，您可能会丢失与管理 IP 地址的 SSH 连接。

c) 将防火墙模式更改为路由。

configure firewall routed

示例：

```
> configure firewall routed
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

d) 启用本地管理器。

configure manager local

例如：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

现在，您可以使用 Web 浏览器在 **https://***management-IP-address* 位置打开本地管理器。

重置配置

如果要重新开始，您可以将系统配置重置为出厂默认设置。虽然无法直接重置配置，但删除和添加管理器可清除配置。

如果您计划擦除配置，然后恢复备份，请确保您已下载要恢复的备份副本。重置系统后，您需要上传备份副本，然后才能执行恢复。

开始之前

如果启用了任何功能许可证，必须首先在 设备管理器 中禁用它们，然后才能删除本地管理器。否则，这些许可证将仍旧分配给思科智能软件管理器中的设备。请参阅启用或禁用可选许可证，第87页。

如果设备已配置为高可用性，您必须首先使用 设备管理器（如果可能）或**configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

过程

步骤 1 使用 SSH 客户端打开与管理 IP 地址的连接，使用具有配置 CLI 访问权限的用户名登录设备 CLI。例如 **admin** 用户名。

步骤 2 使用 **configure manager delete** 命令可删除管理器。

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
```

```
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

步骤 3 配置本地管理器。

configure manager local

例如：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

现在，您可以使用Web浏览器在**https://***management-IP-address*位置打开本地管理器。清除配置后，系统会提示您完成设备安装向导。

Cisco Secure Firewall 3100上的热插拔 SSD

如果您有两个SSD，它们会在您启动时形成RAID。防火墙启动时，您可以在CLI上执行以下任务：威胁防御

- 热插拔其中一个 SSD - 如果 SSD 出现故障，您可以更换它。请注意，如果您只有一个 SSD，则无法在防火墙开启时将其删除。
- 删除一个 SSD - 如果您有两个 SSD，可以删除一个。
- 添加第二个 SSD - 如果您有一个 SSD，可以添加第二个 SSD 并形成 RAID。

⚠

注意 请勿在未使用此程序从 RAID 中移除 SSD 的情况下将其移除。可能会导致数据丢失。

过程

步骤 1 删除其中一个 SSD。

a) 从 RAID 中删除 SSD。

configure raid remove-secure local-disk {**1** | **2**}

remove-secure 关键字将从 RAID 中删除 SSD，禁用自加密磁盘功能，并对 SSD 执行安全擦除。如果您只想从 RAID 中删除 SSD 并保持数据不变，可以使用 **remove** 关键字。

示例：

```
> configure raid remove-secure local-disk 2
```

b) 监控 RAID 状态，直到 SSD 不再显示在清单中。

show raid

从 RAID 中删除 SSD 后， **可操作性** 和 **驱动器状态** 将显示为 **降级**。第二个驱动器将不再列为成员磁盘。

示例：

```
> show raid
Virtual Drive
ID:                          1
Size (MB):                   858306
Operability:                 operable
Presence:                    equipped
Lifecycle:                   available
Drive State:                 optimal
Type:                        raid
Level:                       raid1
Max Disks:                   2
Meta Version:                1.0
Array State:                 active
Sync Action:                 idle
Sync Completed:              unknown
Degraded:                    0
Sync Speed:                  none

RAID member Disk:
Device Name:                 nvme0n1
Disk State:                  in-sync
Disk Slot:                   1
Read Errors:                 0
Recovery Start:              none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                 nvme1n1
Disk State:                  in-sync
Disk Slot:                   2
Read Errors:                 0
Recovery Start:              none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                          1
Size (MB):                   858306
Operability:                 degraded
Presence:                    equipped
Lifecycle:                   available
Drive State:                 degraded
Type:                        raid
Level:                       raid1
Max Disks:                   2
Meta Version:                1.0
Array State:                 active
```

```
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) 从机箱中取出 SSD。

步骤 2 添加 SSD。

a) 将 SSD 物理添加到空插槽。

b) 将 SSD 添加到 RAID。

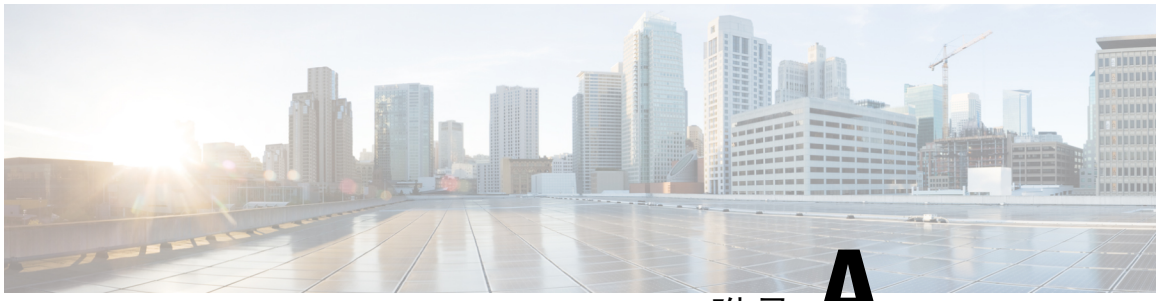
configure raid add local-disk {**1** | **2**}

将新 SSD 同步到 RAID 可能需要几个小时，在此期间防火墙完全正常运行。您甚至可以重新启动，同步将在启动后继续。使用 **show raid** 命令显示状态。

如果您安装的 SSD 以前在另一个系统上使用过，并且仍处于锁定状态，请输入以下命令：

configure raid add local-disk {**1** | **2**} *psid*

Psid 印在SSD背面的标签上。或者，您可以重新启动系统，SSD将被重新格式化并添加到RAID。



附录 A

高级配置

某些设备功能可使用 ASA 配置命令进行配置。虽然 设备管理器 可以配置很多基于命令的功能，但它并非支持所有功能。如果需要使用 设备管理器本不支持的一些 ASA 功能，可以使用 Smart CLI 或 FlexConfig 手动配置这些功能。

以下主题详细说明这种类型的高级配置。

关于 Smart CLI 和 FlexConfig

威胁防御使用ASA配置命令实现一些功能，但不是所有功能。没有唯一的一组 威胁防御 配置命令。

您可以借助以下方法使用 CLI 配置功能：

- **Smart CLI** -（首选方法。）Smart CLI 模板为用于特定功能的预定义模板，提供相应功能所需的所有命令，您只需选择变量值即可。系统会验证您的选择，以促进您正确配置具体功能。如果您所需的功能有对应的 Smart CLI 模板，则必须使用此方法。
- **FlexConfig** - FlexConfig 策略是 FlexConfig 对象的集合。FlexConfig 对象的形式比 Smart CLI 模板更自由，且系统不执行 CLI、变量或数据验证。您必须了解 ASA 配置命令，并按照 ASA 配置指南创建有效的命令序列。

Smart CLI 和 FlexConfig 的意义在于允许您配置不直接通过 设备管理器 策略和设置支持的功能。

注意 思科强烈声明，只建议具有较强 ASA 背景且自承风险的高级用户使用 Smart CLI 和 FlexConfig。您可以配置不受禁止的任何命令。通过 Smart CLI 和 FlexConfig 启用功能可能会导致配置的其他功能出现意想不到的结果。

您可以联系思科技术支持中心获取有关您已配置的 Smart CLI 和 FlexConfig 对象的支持。思科技术支持中心不代表任何客户设计或编写自定义配置。思科不保证正确的操作或与其他 威胁防御功能的互通性。Smart CLI 和 FlexConfig 功能可能随时被摒弃。为获得充分保证的功能支持，您必须等待 设备管理器 支持。如有疑问，请勿使用 Smart CLI 或 FlexConfig。

以下主题更详细地解释这些功能。

Smart CLI 和 FlexConfig 的建议用法

FlexConfig 有两大主要推荐用途：

- 您正在从 ASA 迁移至 威胁防御，并且存在您正在使用（且需要继续使用）的 设备管理器 不直接支持的兼容功能。在这种情况下，请在 ASA 上使用 **show running-config** 命令来查看功能配置，并创建实现功能的 FlexConfig 对象。通过比较两个设备上的 **show running-config** 输入予以验证。
- 您正在使用 威胁防御，但有一个设置或功能需要配置，例如思科技术援助中心告诉您特定的设置应解决您遇到的特定问题。对于复杂功能，请使用实验室设备测试 FlexConfig，并验证您是否将得到预期行为。

尝试重新创建ASA配置前，请先确定是否可在标准策略中配置等效功能。例如，访问控制策略包括 ASA 使用单独功能实现的入侵检测和预防、HTTP 和其他类型的协议检查、URL 过滤、应用过滤和访问控制。由于许多功能并未使用 CLI 命令予以配置，因此，您不会看到各策略均显示在 **show running-config** 输出内。

注释 在任何时候，请记住 ASA 和 威胁防御之间不存在一对一重叠关系。请勿尝试在 威胁防御 设备上完全重新创建 ASA 配置。您必须仔细测试使用 FlexConfig 配置的各项功能。

Smart CLI 和 FlexConfig 对象中的 CLI 命令

威胁防御 使用 ASA 配置命令配置某些功能。虽然并非所有 ASA 功能都与 威胁防御兼容，但有一些功能可以在 威胁防御 上使用，但不能在 设备管理器 策略中进行配置。您可以使用 Smart CLI 和 FlexConfig 对象指定配置这些功能所需的 CLI。

如果决定使用Smart CLI或FlexConfig手动配置功能，则需负责根据正确语法了解和执行这些命令。FlexConfig 不验证 CLI 命令语法。有关正确语法和配置 CLI 命令的更多信息，请使用以下 ASA 文档作为参考：

- ASA CLI 配置指南介绍了如何配置功能。指南位于：http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html
- ASA 命令参考提供按命令名称排序的附加信息。参考位于：http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html

以下主题介绍了有关配置命令的更多信息。

软件升级如何影响 FlexConfig 策略

每个新版本的 威胁防御 软件都添加了对配置 设备管理器中功能的支持。有时，这些新功能可能与您先前已使用 FlexConfig 配置的功能重叠。

升级后，您需要检查 FlexConfig 策略和对象。如果任何策略和对象包含因 设备管理器 或 Smart CLI 中添加的支持而被禁用的命令，则对象列表中的图标和相关消息会指出这一问题。请抽出时间重新进行配置。参考禁用命令列表，以帮助确定现在应在何处配置这些命令。

系统不会阻止您部署更改，尽管连接到FlexConfig策略的FlexConfig对象包含新禁用的命令。但是，您将无法创建新的 Smart CLI 对象，直到解决 FlexConfig 策略中提及的所有问题。

从 FlexConfig 策略中删除有问题的对象即可，因为限制仅适用于您主动部署到设备配置的对象。因此，您可以删除这些对象，创建相应的 Smart CLI 或集成 设备管理器 配置时再使用这些对象作参考。新配置达到要求后，删除对象即可。如果删除的对象包含一些未禁用的元素，您可以编辑这些对象以删除不受支持的命令，然后将对象重新连接到 FlexConfig 策略。

确定 ASA 软件版本和当前 CLI 配置

由于系统使用 ASA 软件命令配置某些功能，因此需要确定在 威胁防御设备上运行的软件中使用的当前 ASA 版本。此版本号指示用于指导配置功能的 ASA CLI 配置指南。此外，您还应检查当前基于 CLI 的配置，并将其与要实施的 ASA 配置进行比较。

注意，任何 ASA 配置都与 威胁防御 配置有着显著的差异。许多 威胁防御 策略都是在 CLI 之外配置的，因此查看这些命令看不到配置。请勿尝试在 ASA 和 威胁防御 配置之间创建一对一的对应关系。

要查看此信息，请在 设备管理器 中打开 CLI 控制台，或与设备管理接口建立 SSH 连接，然后发出以下命令：

- **show version system** 并查找思科自适应安全设备软件版本号。
- **show running-config** 查看当前的 CLI 配置。
- **show running-config all** 包括当前 CLI 配置中的所有默认命令。

禁止的 CLI 命令

Smart CLI 和 FlexConfig 的用途是配置在 ASA 设备上可用但无法使用 设备管理器在 威胁防御 设备上配置的功能。

因此，您无法配置在 设备管理器中具有等同功能的 ASA 功能。下表列出的是一些禁止的命令区。该列表包含许多进入配置模式的父命令。禁止父命令包括禁止子命令。还包括命令的 **no** 版本及其相关的 **clear** 命令。

FlexConfig 对象编辑器可防止将这些命令纳入对象中。此列表不适用于 Smart CLI 模板，因为这些模板仅包含可有效配置的命令。

禁止的 CLI 命令	备注
aaa	使用**对象** > **身份源**。
aaa-server	使用**对象** > **身份源**。
access-list	部分阻止。 • 可以创建 **ethertype** 访问列表。 • 不能创建 **extended** 和 **standard** 访问列表。使用 Smart CLI 扩展访问列表或标准访问列表对象创建这些 ACL。然后，可以在按对象名称引用 ACL 且支持 FlexConfig 的命令中使用，例如带扩展 ACL 的 **match access-list** 用于服务策略流量类别。 • 无法创建 **advanced** 访问列表，系统将该访问列表与 **access-group** 命令一起使用。请使用**策略** > **访问控制**来配置访问规则。 • 不能创建 **webtype** 访问列表。
anyconnect-custom-data	使用**设备 (Device)** > **远程访问 VPN (Remote Access VPN)** 来配置 Secure Client。
asdm	此功能不适用于 威胁防御 系统。
as-path	创建 Smart CLI AS 路径对象，并将其用于 Smart CLI BGP 对象，以配置自治系统路径过滤器。
attribute	-
auth-prompt	此功能不适用于 威胁防御 系统。
boot	—
call-home	—
captive-portal	使用**策略** > **身份**配置用于主动身份验证的强制网络门户。
clear	—
client-update	—
clock	使用**设备** > **系统设置** > **NTP** 来配置系统时间。
cluster	—
command-alias	—

禁止的 **CLI** 命令	备注
community-list	创建 Smart CLI 扩展社区列表或标准社区列表对象，并将其用于 Smart CLI BGP 对象，以配置社区列表过滤器。
compression	—
configure	—
crypto	在**对象 (Objects)** 页面上，使用**证书 (Certificates)**、**IKE 策略 (IKE Policies)** 和 **IPSec 提议 (IPSec Proposals)**。
ddns	使用**设备** > **系统设置** > **DDNS 服务**配置动态 DNS。
dhcp-client	—
dhcpd	依次选择**设备** > **系统设置** > **DHCP 服务器**。 但是，允许使用 **dhcpd option** 命令。
dhcprelay	请改用 威胁防御 API 中的 dhcprelayservices 资源。
dns	使用**对象** > **DNS 组**配置 DNS 组，并使用**设备** > **系统设置** > **DNS 服务器**分配这些组。
dns-group	使用**对象** > **DNS 组**配置 DNS 组，并使用**设备** > **系统设置** > **DNS 服务器**分配这些组。
domain-name	使用**对象** > **DNS 组**配置 DNS 组，并使用**设备** > **系统设置** > **DNS 服务器**分配这些组。
dynamic-access-policy-config **dynamic-access-policy-record**	—
enable	—
event	—
failover	—
fips	—
firewall	设备管理器 仅支持路由防火墙模式。
hostname	依次选择**设备** > **系统设置** > **主机名**。
hpm	此功能不适用于 威胁防御 系统。
http	依次访问**设备** > **系统设置** > **管理访问**，使用**数据接口**选项卡。
inline-set	—

禁止的 CLI 命令	备注
interface 用于 BVI、管理、以太网、千兆以太网和子接口。	部分阻止。 在**设备 (Device)** > **接口 (Interfaces)** 页面上，配置物理接口、子接口和网桥虚拟接口。然后，可使用 FlexConfig 配置其他选项。 但对于这些接口类型，禁止如下 **interface** 模式命令。 **cts** **ip address** **ip address dhcp** **ipv6 address** **ipv6 enable** **ipv6 nd dad** **ipv6 nd suppress-ra** **mode** **nameif** **security-level** **shutdown** **zone-member**
适用于 **vni**、**redundant**、**tunnel** 的 **interface**	在 **设备 (Device)** > **接口 (Interfaces)** 页面上配置接口。设备管理器不支持这些类型的接口。
ip audit	此功能不适用于威胁防御 系统。而应使用访问控制规则应用入侵策略。
ip-client	要将系统配置为使用数据接口作为管理网关，请使用**设备** > **系统设置** > **管理接口**。
ip local pool	使用**设备** > **远程访问 VPN**，配置地址池。
ipsec	—
ipv6	创建 Smart CLI IPv6 前缀列表对象，并将其用于 Smart CLI BGP 对象，以配置 IPv6 前缀列表过滤。
ipv6-vpn-addr-assign	使用**设备** > **远程访问 VPN**，配置地址池。
isakmp	使用**设备** > **站点间 VPN**。
jumbo-frame	如果将任何接口的 MTU 增至超出默认值 1500，系统将自动启用巨型帧支持。
ldap	—
license-server	使用**设备** > **智能许可证**。

禁止的 **CLI** 命令	备注
logging	使用**对象** > **系统日志服务器**和**设备** > **系统设置** > **日志记录设置**。 但是，您可以在 FlexConfig 中配置 **logging history** 命令。
management-access	—
migrate	使用**设备** > **远程访问 VPN** 和**设备** > **站点间 VPN** 来启用 IKEv2 支持。
mode	设备管理器 仅支持单情景模式。
mount	—
mtu	在**设备** > **接口**上配置各接口的 MTU。
nat	使用**策略** > **NAT**。
ngips	—
ntp	使用**设备** > **系统设置** > **NTP**
object-group network **object network**	使用**对象** > **网络**。 无法在 FlexConfig 中创建网络对象或组，但可使用在模板内的对象管理器中定义的网络对象和组作为变量。
object service |natorigsvc **object service |natmappedsvc**	通常允许 **object service** 命令，但无法编辑名为 |natorigsvc 或 |natmappedsvc 的内部对象。在这些名称中，竖线是有意使用的，是限制对象名称的首个字符。
passwd **password**	—
password-policy	—
policy-list	创建 Smart CLI 策略列表对象，并将其用于 Smart CLI BGP 对象，以配置策略列表。
policy-map 子命令	不能在策略映射中配置以下命令。 **priority** **police** **match tunnel-group**
prefix-list	创建 Smart CLI IPv4 前缀列表对象，并将其用于 Smart CLI OSPF 或 BGP 对象，以配置 IPv4 前缀列表过滤。
priority-queue	—
privilege	—

禁止的 CLI 命令	备注
reload	不能安排重新加载。系统不使用 **reload** 命令重启系统，它使用的是 **reboot** 命令。
rest-api	此功能不适用于 威胁防御 系统。始终安装并启用 REST API。
route	使用**设备** > **路由**配置静态路由。
route-map	创建 Smart CLI 路由映射对象，并将其用于 Smart CLI OSPF 或 BGP 对象，以配置路由映射。
router bgp	使用适用于 BGP 的 Smart CLI 模板。
router eigrp	使用适用于 EIGRP 的 Smart CLI 模板。
router ospf	使用适用于 OSPF 的 Smart CLI 模板。
scansafe	此功能不适用于 威胁防御 系统。请在访问控制规则中配置 URL 过滤。
setup	此功能不适用于 威胁防御 系统。
sla	—
snmp-server	使用 FTP API SNMP 资源配置 SNMP。
ssh	依次访问**设备** > **系统设置** > **管理访问**，使用**数据接口**选项卡。
ssl	使用**设备** > **系统设置** > **SSL 设置**。
telnet	威胁防御 不支持 Telnet 连接。使用 SSH 而不是 Telnet 访问设备 CLI。
time-range	—
tunnel-group	使用**设备** > **远程访问 VPN** 和**设备** > **站点间 VPN**。
tunnel-group-map	使用**设备** > **远程访问 VPN** 和**设备** > **站点间 VPN**。
user-identity	使用**策略** > **身份**。
username	要创建 CLI 用户，请打开 SSL 或设备控制台会话并使用 **configure user** 命令。
vpdn	—
vpn	—
vpn-addr-assign	—
vpnclient	—

禁止的 CLI 命令	备注
vpn-sessiondb	—
vpnsetup	—
webvpn	—
zone	—
zonelabs-integrity	此功能不适用于 威胁防御 系统。

Smart CLI 模板

下表介绍的是基于该功能的 Smart CLI 模板。

注释 您还可以使用 Smart CLI 模板配置 OSPF 和 BGP。但是，可通过**设备 (Devices)** > **路由 (Routing)** 页面而不是“高级配置”(Advanced Configuration) 页面使用这些模板。

功能	模板	说明
对象：AS 路径	ASPath	创建用于路由协议对象的 ASPath 对象。
对象：访问列表	扩展访问列表 标准访问列表	创建用于路由对象的扩展或标准 ACL。您也可以从 FlexConfig 对象（用于配置使用 ACL 的允许命令）按名称引用这些对象。
对象：社区列表	扩展社区列表 标准社区列表	创建用于路由对象的扩展或标准社区列表。
对象：前缀列表	IPV4 前缀列表 IPV6 前缀列表	创建用于路由对象的 IPv4 或 IPv6 前缀列表。
对象：策略列表	策略列表	创建用于路由对象的策略列表。
对象：路由映射	路由映射	创建用于路由对象的路由映射。

Smart CLI 和 FlexConfig 的准则和限制

通过 Smart CLI 或 FlexConfig 配置功能时，请牢记以下几点。

- FlexConfig 对象中定义的命令应在通过 设备管理器（包括 Smart CLI）定义的功能的所有命令之后进行部署。这样您就可以确保，在向设备发出这些命令前，配置好相应的对象和接口等。如果需要在 Smart CLI 模板中使用 FlexConfig 已部署的项目，请先创建和部署 FlexConfig，再创建

和部署 Smart CLI 模板。例如，如果要使用 OSPF Smart CLI 模板重新分配 EIGRP 路由，请先使用 FlexConfig 配置 EIGRP，然后创建 OSPF Smart CLI 模板。

- 如果要删除通过 FlexConfig 配置的功能或功能的一部分，但 Smart CLI 模板引用该功能，则首先必须删除 Smart CLI 模板中使用该功能的命令。然后，部署配置，以便 Smart-CLI 配置功能不再引用它。然后，您可以从 FlexConfig 中删除该功能，并重新部署配置，最终完全清除该配置。

配置 Smart CLI 对象

Smart CLI 对象定义了无法在 设备管理器中配置的功能。Smart CLI 对象为功能配置提供了一定程度的指导。对于给定的功能（模板），所有可能的命令均已预先加载且已验证所输入的变量。因此，尽管仍然使用 CLI 命令进行功能配置，但 Smart CLI 对象并不像 FlexConfig 对象一样具有自由的形式。

虽然 Smart CLI 模板确实提供了一定程度的指导，但仍然需要阅读 ASA 配置指南和命令参考，了解命令的用法，从而选择可以在您的网络环境下正确运行的值。最好已有可作为配置基础使用的 ASA 配置，只需在 Smart CLI 对象中构建相同的命令序列。

Smart CLI 对象根据功能区进行分组。

注释 所定义的所有 Smart CLI 对象都将被部署。与 FlexConfig 不同的是，无法创建多个 Smart CLI 对象，然后再从中选择要部署的对象。只需为要配置的功能创建 Smart CLI 对象。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中点击 **Smart CLI** 下的相应功能区。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 输入对象的名称和说明（后者为可选项）。

步骤 5 为要配置的功能选择 **CLI 模板**。

系统会将命令模板加载到**模板**窗口中。最初，系统只显示模板所需的命令。这些命令表示模板所需的最低配置。

步骤 6 填写变量并根据需要在模板中添加命令。

最好使用 ASA 或 威胁防御 设备（由 管理中心负责管理）的现有配置。有了相应配置，只需确保模板符合配置要求，即可更改适合网络中该特定设备位置的变量（例如 IP 地址和接口名称）。

以下是填写模板的一些提示：

- 要选择变量值，请点击变量，然后键入适当的值或从列表中选择（在有枚举值的情况下）。将鼠标移动到需要键入的变量上，显示该选项的有效值（例如数字范围）。在某些情况下，系统会提供建议值。

  例如，在 OSPF 模板中，所需的命令 **router ospf** *process-id* 在鼠标悬停于其上时显示“进程 ID (1-65535)”，点击 *process-id* 时，该字段会高亮显示。只需键入所需的数字即可。

- 选择变量选项时，如果有其他可能的命令可以配置该选项，则会自动显示并根据需要禁用或启用。注意这些附加命令。

- 使用模板上方的**显示/隐藏禁用**链接控制视图。系统不会配置禁用的命令，但您必须显示这些命令才能进行配置。要查看完整模板，请点击模板上方的**显示已禁用**链接。如只查看将要配置的命令，请点击表上方的**隐藏禁用**链接。

- 要清除上次保存对象之后的所有编辑内容，请点击模板上方的**重置**链接。

- 要启用可选命令，请点击行号左侧的 +按钮。

- 要禁用可选命令，请点击行号左侧的 - 按钮。如果已编辑该行，则不会删除编辑内容。

- 要复制命令，请点击“选项”**...** 按钮，然后选择**复制**。只有在多次输入命令有效时，才允许复制命令。

- 要删除复制命令，请点击选项 **...** 按钮，然后选择**删除**。无法删除作为基本模板组成部分的命令。

步骤 7 点击**确定 (OK)**。

配置 FlexConfig 策略

FlexConfig 策略只是希望部署到设备配置中的 FlexConfig 对象列表。系统仅部署该策略中包含的对象，所有其他对象均只进行定义而不使用。

FlexConfig 对象中定义的命令应在通过 设备管理器（包括 Smart CLI）定义的功能的所有命令之后进行部署。这样您就可以确保，在向设备发出这些命令前，配置好相应的对象和接口等。如果需要在 Smart CLI 模板中使用 FlexConfig 已部署的项目，请先创建和部署 FlexConfig，再创建和部署 Smart CLI 模板。例如，如果要使用 OSPF Smart CLI 模板重新分配 EIGRP 路由，请先使用 FlexConfig 配置 EIGRP，然后创建 OSPF Smart CLI 模板。

注释 如有用于功能的 Smart CLI 模板，则不可使用 FlexConfig 进行配置。必须使用 Smart CLI 对象。

开始之前

创建 FlexConfig 对象。请参阅以下主题：

- 配置 FlexConfig 对象， 第 822 页
- 在 FlexConfig 对象中创建变量， 第 824 页
- 配置密钥对象， 第 831 页

过程

步骤 1 在**设备 (Device)** > **高级配置 (Advanced Configuration)**中点击**查看配置 (View Configuration)**。

步骤 2 在“高级配置”(Advanced Configuration) 目录中依次点击 **FlexConfig** > **FlexConfig 策略 (FlexConfig Policy)**。

步骤 3 管理**组列表**中的对象列表。

- 要添加对象，请点击 + 按钮。如果对象尚不存在，请点击**创建新的 FlexConfig 对象 (Create New FlexConfig Object)** 来定义。
- 要删除对象，请点击对象条目右侧的 **X** 按钮。

注释 建议使每个对象都完全独立，而不依赖于任何其他 FlexConfig 对象中定义的配置。这样可以确保在不影响其他对象的情况下添加或删除对象。

步骤 4 在**预览**窗格中评估建议的命令。

可以点击**展开 (Expand)** 按钮（随后点击**折叠 (Collapse)**）加宽显示画面，以便更清晰地查看长命令。

预览将评估变量并生成将要发布的确切命令。请确保这些命令正确且有效。您必须确保这些命令不会导致错误或配置不当，否则会使设备无法使用。

注意 系统不验证命令。可以部署无效甚至可能有破坏性的命令。在部署更改之前，请仔细检查预览。

步骤 5 点击**保存 (Save)**。

下一步做什么

编辑 FlexConfig 策略后，仔细检查下一部署的结果。如果出现错误，请更正对象中的 CLI。请参阅 FlexConfig 策略故障排除， 第 832 页。

配置 FlexConfig 对象

对于无法使用 设备管理器进行配置的特定功能，FlexConfig 对象包含配置这类功能所需的 ASA 命令。您必须确保输入正确的命令序列，且无拼写错误。系统不验证 FlexConfig 对象的内容。

建议为要配置的每个常规功能创建单独的对象。例如，如要定义 banner 并配置 RIP 路由协议，请使用 2 个单独的对象。如果以单独的对象隔离各个功能，则可以更轻松地选择要部署的对象，而且更易于进行故障排除。

注释 请勿包括 **enable** 和 **configure terminal** 命令。系统将自动进入配置命令的正确模式。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 输入对象的名称和说明（后者为可选项）。

步骤 5 在**变量**部分，创建要在对象正文中使用的所有变量。

唯一必须创建的变量是指向 设备管理器中所定义对象的变量，具体而言即网络、端口和密钥变量类型，或指向指定接口的接口变量。对于其他变量类型，只需将值输入到对象正文中。

有关创建和使用变量的详细信息，请参阅在 FlexConfig 对象中创建变量，第 824 页。

步骤 6 在**模板**部分，键入配置该功能所需的 ASA 命令。

必须按正确的顺序输入命令，以便配置该功能。使用 ASA CLI 配置指南，了解如何输入命令。最好拥有 ASA 或其他 威胁防御 设备提供的经过预先测试的配置文件，以便用作参考。

此外，还可以使用 Mustache 表示法来引用和处理变量。有关详细信息，请参阅引用 FlexConfig 变量和检索值，第 826 页。

以下是创建对象正文的一些提示：

- 要添加行，请将光标放在行尾然后按 Enter 键。
- 要使用变量，请在双括号 {{*variable_name*}} 中键入变量名称。对于引用对象的变量，必须包括要检索其值的属性：{{*variable_name.attribute*}}。可用属性因对象类型而异。有关完整信息，请参阅变量引用：{{variable}} 或 {{{variable}}}，第 826 页。
- 要使用 Smart CLI 对象，请键入对象的名称。如果需要引用 Smart CLI 中配置的路由进程，请输入进程标识符。请参阅在 FlexConfig 对象中引用 Smart CLI 对象，第 830 页。
- 点击模板正文上方的**展开/折叠**链接，放大或缩小正文。
- 点击**重置**链接，清除自上次保存对象之后所做的任何更改。

步骤 7 在**取消模板**部分，输入删除或反向对象正文中已配置命令所需的命令

“取消”部分非常重要，有两个用途：

- 它简化了部署。在重新部署正文中的命令之前，系统将使用这些命令先清除或取消配置。这将确保一个干净的部署环境。
- 如果您决定通过从 FlexConfig 策略中删除对象的方式来删除该功能，系统将使用这些命令从设备中删除命令。

如果不提供在对象正文中取消或反向 CLI 所需的命令，则部署操作可能需要清除整个设备配置并重新部署所有策略，而不仅仅是对象中的命令。这将使部署时间更长，并且将造成流量中断。确保拥有撤消对象正文中所定义配置所需的所有命令，而且只有这些命令。虽然在模板中否定命令通常是命令的 **no** 或 **clear** 形式，如果真实关闭已启用的功能，“否定”命令实际上是命令的肯定形式，也即启用功能的形式。

使用ASA配置指南和命令参考确定相应的命令。有时，可以使用单个命令撤消配置。例如，在配置 RIP 的对象中，单个 **no router rip** 命令即可删除整个 **router rip** 配置，包括子命令。

同样，如果输入多个 **banner login** 命令创建多行横幅，则单个 **no banner login** 命令将取消整个登录横幅。

如果模板创建多个嵌套对象，取消模板需要按照反向顺序删除对象，即首先删除对象引用，然后再删除对象。例如，如果您先创建一个ACL，接着在流量类中引用该ACL，随后在策略映射中引用流量类，最后使用服务策略启用策略映射，那么取消模板必须依次删除服务策略、策略映射、流量类以及 ACL 来撤消配置。

步骤 8 点击**确定**。

下一步做什么

仅创建一个 FlexConfig 对象不足以完成部署。必须将该对象添加到 FlexConfig 策略中。仅 FlexConfig 策略中的对象可进行部署。这样可细化 FlexConfig 对象并为特殊用途做一些准备，而不会自动部署这些对象。请参阅配置 FlexConfig 策略，第 821 页。

在 FlexConfig 对象中创建变量

FlexConfig 对象中使用的变量在该对象中进行定义。没有单独的变量列表。因此，无法定义某个变量，然后在单独的 FlexConfig 对象中使用该变量。

变量提供以下主要好处：

- 可以指向使用 设备管理器定义的对象。这包括网络、端口和密钥对象。
- 可以隔离可能会随对象正文变化的值。因此，如果需要更改值，只需编辑变量，而无需编辑对象正文。如果需要在多个命令行中引用对象，这会特别有用。

此程序说明向 FlexConfig 对象中添加变量的过程。

过程

步骤 1 从**设备** > **高级配置页**中编辑或创建 FlexConfig 对象。

请参阅配置 FlexConfig 对象，第 822 页。

步骤 2 在**变量**部分执行下列操作之一：

- 要添加变量，请点击 + 按钮（如果尚未定义变量，请点击**添加变量 (Add Variable)**）。
- 要编辑变量，请点击该变量的编辑图标 ( )。

要删除变量，请点击该变量的垃圾桶 ( ) 图标。确保从模板正文中删除变量的任何引用。

步骤 3 输入变量的名称和说明（后者为可选项）。

步骤 4 选择变量的数据**类型**，然后输入或选择相应值。

可以创建以下类型的变量。选择满足使用变量的命令数据要求的类型。

- **字符串** - 文本字符串。例如，主机名、用户名等。
- **数字** - 整数。不要使用逗号、小数、符号（如负号 -）或十六进制表示法。对于非整数数字，请使用字符串变量。
- **布尔值** - 逻辑真/假。选择真或假。
- **网络** -“对象”(Objects) 页面上定义的网络对象或组。选择网络对象或组。
- **端口** -“对象”(Objects) 页面上定义的 TCP 或 UDP 端口对象。选择端口对象。无法为其他协议选择组或对象。
- **接口** -“设备”(Device) >“接口”(Interfaces) 页面上定义的指定接口。选择接口。无法选择没有名称的接口。
- **IP** - 不带网络掩码或前缀长度的单个 IPv4 或 IPv6 IP 地址。
- **密钥** - 为 FlexConfig 定义的密钥对象。选择对象。有关创建密钥对象的详细信息，请参阅配置密钥对象，第 831 页。

步骤 5 在“变量”(Variable) 对话框中点击**添加 (Add)** 或**保存 (Add Variable)**。

此时，可以在FlexConfig对象正文中使用该变量。引用变量的方式根据变量类型的不同而有所不同。有关如何使用这些变量的详细信息，请参阅下列主题：

- 变量引用：{{variable}} 或 {{{variable}}}，第 826 页
- 部分 {{#key}} {{/key}} 和反向部分 {{^key}} {{/key}}，第 828 页

步骤 6 在“FlexConfig 对象”(FlexConfig Object) 对话框中点击**确定 (OK)**。

引用 FlexConfig 变量和检索值

FlexConfig 将 Mustache 作为模板语言，但支持仅限于以下各节中介绍的功能。使用这些功能引用变量、检索其值并予以处理。

变量引用：{{variable}} 或 {{{variable}}}

要引用在 FlexConfig 对象中定义的变量，请使用以下表示法：

{{*variable_name*}}

或：

{{{*variable_name*}}}

这足以用于为单值的简单变量，其中包括如下类型的变量：**数字**、**字符串**、**布尔值**和 **IP**。如果变量包含特殊字符（如 &），请使用三重大括号 。或者，您可以始终对所有变量使用三重大括号。

但是，对于指向在配置数据库中建模为对象的元素的变量，必须使用点符号并纳入要检索的对象属性的名称。可通过检查相关对象类型的 API Explorer 中的模型查找这些属性名称。必须借助以下表示法使用以下类型的变量：**密钥**、**网络**、**端口**和**接口**。

{{*variable_name.attribute*}}

例如，要从名为 net-object1 的网络变量（指向网络对象，而不是网络组）检索地址，可使用：

{{net-object1.value}}

如果想要从对象内的对象中检索属性值，则需使用一系列带点符号的属性向下钻取所需值。例如，将接口的 IP 地址建模为名为 ipv4 和 ipv6 的接口对象子接口。因此，要检索名为 int-inside（指向内部接口）的接口变量的 IPv4 地址和子网掩码，可以使用：

{{int-inside.ipv4.ipAddress.ipAddress}} {{int-inside.ipv4.ipAddress.netmask}}

注释 要打开 API Explorer，点击更多选项按钮 (⋮) 并选择 **API Explorer**。

下表列出的是变量类型、引用方式、API 模型名称及最可能使用的引用（对于对象）。

变量类型	参考模型	说明

布尔值
（简单变量）
	变量：
	{{*variable_name*}}
	部分：
	`{{#variable_name}}`
	`commands`
	`{{/variable_name}}`
	反向部分：
	`{{^variable_name}}`
	`commands`
	`{{/variable_name}}`
		逻辑 true/false。布尔变量的主要用途是用于部分或反向部分。可以编辑布尔变量值打开或关闭一部分命令，例如，如果需要定期或在特殊情况下启用某项功能。
		一些对象在其模型中也具有布尔属性，可用于提供可选的部分处理。

接口
（对象变量：API 模型是 Interface）
	变量：
	{{*variable_name.attribute*}}
	部分：
	`{{#variable_name.attribute}}`
	`commands`
	`{{/variable_name.attribute}}`
	反向部分：
	`{{^variable_name.attribute}}`
	`commands`
	`{{/variable_name.attribute}}`
		在“设备”(Device)>“接口”(Interfaces) 页面上定义命名的接口。无法指向未命名接口。
		接口模型中有各种可用属性。此外，接口模型包括子对象，例如 IP 地址子对象。
		以下是您可能觉得有用的一些主要属性：
		• *variable_name*.**name** 返回接口的逻辑名称。
		• *variable_name*。**hardwareName** 返回接口端口名称，如 GigabitEthernet1/8。
		• *variable_name*.**managementOnly** 是一个布尔值。TRUE 表示该接口被定义为仅限于管理。FALSE 表示该接口用于流经设备的流量。可以将此选项用作部分密钥。
		• *variable_name*.**ipv4.ipAddress.ipAddress** 返回接口的 IPv4 地址。
		• *variable_name*.**ipv4.ipAddress.netmask** 返回接口的 IPv4 地址的子网掩码。

IP （简单变量）	**变量：** {{*variable_name*}}	单个 IPv4 或 IPv6 IP 地址，无网络掩码或前缀长度。

变量类型	参考模型	说明
网络 （对象变量：API 模型是 NetworkObject）	**变量（网络对象）：** {{*variable_name*.*attribute*}} **部分（组对象）：** {{#*variable_name*.**networkObjects**}} commands referring to one of {{**value**}} {{**name**}} {{/*variable_name*.**networkObjects**}}	“对象”(Objects) 页面上定义的网络对象或组。可使用部分处理网络组。 以下是可能对您有用的主要属性： • {{*variable_name*.**name**}} 返回网络对象或组名称。 • {{*variable_name*.**value**}} 返回网络对象（而非网络组）的 IP 地址内容。确保将具有正确类型内容的网络对象用于给定命令，例如使用主机地址而不是子网掩码地址。 • {{*variable_name*.**groups**}} 返回网络组中包含的网络对象的列表。仅与指向网络组的变量结合使用，并在部分标记上使用以反复处理组内容。使用 {{**value**}} 或 {{**name**}} 依次检索各网络对象的内容。
数字 （简单变量）	**变量：** {{*variable_name*}}	整数。不要使用逗号、小数、符号（如负号 -）或十六进制表示法。对于非整数数字，请使用字符串变量。
端口 （对象变量：API 模型是 PortObject、tcpports 或 udpports）	**变量：** {{*variable_name*.*attribute*}}	在“对象”(Objects) 页面定义的 TCP 或 UDP 端口对象。必须为端口对象，而不是端口组。 以下是可能对您有用的主要属性： • {{*variable_name*.**port**}} 返回端口号。协议不包括在内。 • {{*variable_name*.**name**}} 返回端口对象名称。
密钥 （对象变量：API 模型是 Secret）	**变量：** {{*variable_name*.**password**}} 或： {{{*variable_name*.**password**}}}	为 FlexConfig 定义的密钥对象。 应该进行的唯一引用是返回加密字符串的 **password** 属性。 如果密码包含特殊字符（如 &），请使用三重大括号。
字符串 （简单变量）	**变量：** {{*variable_name*}}	文本字符串。例如，主机名、用户名等。

部分 {{#key}}{{/key}} 和反向部分 {{^key}}{{/key}}

部分或反向部分是部分开始和结束标记之间的命令块，将密钥作为处理条件。部分的处理方式取决于它是常规部分还是反向部分：

- 如果密钥为空或具有非空内容，则处理常规部分（或简称为部分）。如果密钥为FALSE或对象无内容，则该部分中的命令不予配置。该部分被绕过了。

  以下是常规部分的语法。

```
{{#key}}
one or more commands
{{/key}}
```

- 反向部分即部分的反面。如果密钥为FALSE或对象无内容，则处理反向部分。如果密钥为TRUE或对象具有内容，则绕过反向部分。

  以下是反向部分的语法。唯一的区别是插入符号替换散列标记。

```
{{^key}}
one or more commands
{{/key}}
```

以下主题介绍部分和反向部分的主要用途。

如何处理多值变量

多值变量处理的一个主要示例是指向网络组的网络变量。由于该组包含多个对象（在 **objects** 属性下），可迭代地遍历网络组中的值以使用不同值多次配置相同命令。

虽然对象组定义了对象属性中包含的网络对象，但这些对象并不包括所包含对象的内容。相反，您可以使用 **networkObjects** 属性获取所包含对象的内容。

例如，如果主机为 192.168.10.0、192.168.20.0 和 192.168.30.0 的网络组名称为 net-group，则可使用以下方法为各 RIP 路由地址配置网络命令。请注意，仅使用网络对象的 **value** 属性，因为在本部分开始时使用 **net-group.networkObjects** 意味着将从成员对象中获取该“value”属性。（对于 FlexConfig 对象中的“value”属性，不需要创建单独的变量。）

```
router rip
{{#net-group.networkObjects}}
 network {{value}}
{{/net-group.networkObjects}}
```

系统将该部分结构转换为：

```
router rip
   network 192.168.10.0
   network 192.168.20.0
   network 192.168.30.0
```

如何基于布尔值或空对象执行可选处理

注释 此主题中的示例仅作说明用途。例如，从版本 6.7 开始，不能使用 FlexConfig 配置 SNMP，而必须改用 威胁防御 API SNMP 资源。

如果相应部分开始标记中的变量内容为TRUE，或对象不为空，则处理该部分。如果布尔值为FALSE或空（例如空对象），则绕过该部分。

这里主要用于布尔值。例如，您可以创建布尔变量，并将命令置于变量所覆盖的节中。然后，如果需要启用或禁用 FlexConfig 对象中的一部分命令，则只需更改布尔变量的值，无需从代码中删除这些行。这使得启用或禁用功能很容易。

例如，如果使用 FlexConfig 启用 SNMP，则可能希望能够关闭 SNMP 陷阱。您可以创建名为 enable-traps 的布尔变量，且最初将其设为 TRUE。然后，如果需要关闭陷阱，只需编辑变量、将其更改为 FALSE、保存该对象，然后重新部署配置。命令序列可能如下所示：

```
snmp-server enable
snmp-server host inside 192.168.1.5
snmp-server community clearTextString
{{#enable-traps}}
snmp-server enable traps all
{{/enable-traps}}
```

还可根据对象内的布尔值执行此类处理。例如，您可以在接口上配置某些特性之前检查该接口是否仅限于管理。在下例中，int-inside 是指向名为 inside 的接口的接口变量。仅当并未将接口设为仅限于管理时，FlexConfig 才可在该接口上配置 EIGRP 相关接口选项。可使用反向部分，以便仅在布尔值为 FALSE 时才配置命令。

```
router eigrp 2
 network 192.168.1.0 255.255.255.0
{{^int-inside.managementOnly}}
interface {{int-inside.hardwareName}}
 hello interval eigrp 2 60
 delay 200
{{/int-inside.managementOnly}}
```

在 FlexConfig 对象中引用 Smart CLI 对象

创建 FlexConfig 对象时，您可以使用变量指向可以在 设备管理器中配置的对象。例如，您可以创建指向接口元素或网络对象的变量。

但是，不能以相同的方式指向 Smart CLI 对象。

相反，如果您创建需要在 FlexConfig 策略中使用的 Smart CLI 对象，只需在适当的位置输入 Smart CLI 对象的名称。

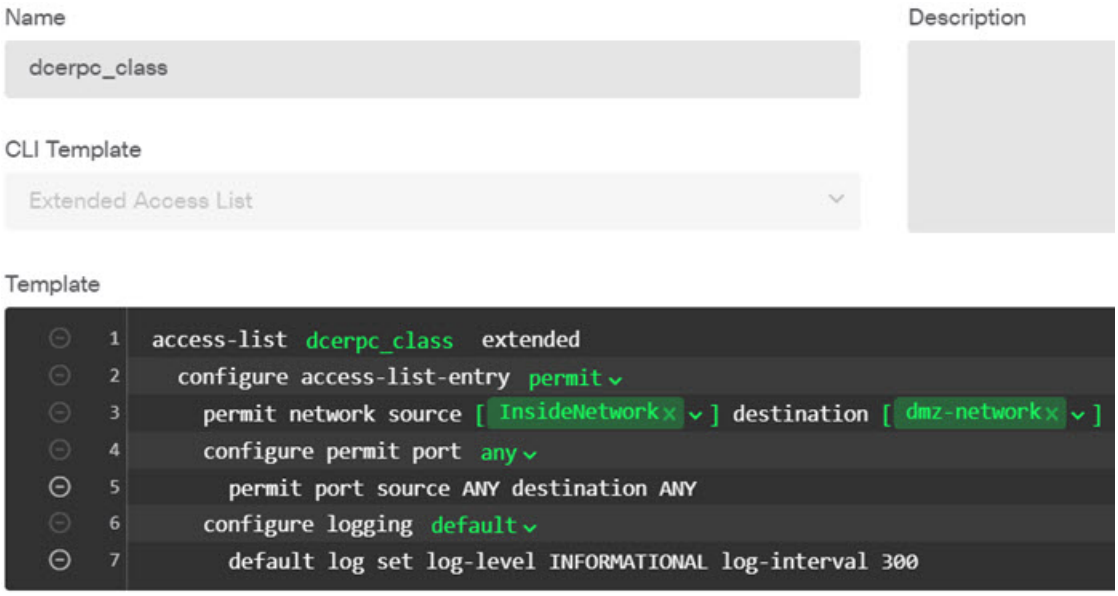
例如，配置协议检测时，您可能想将扩展访问列表用作流量类。由于扩展访问列表具有 Smart CLI 对象，您需要使用 Smart CLI 对象来创建 ACL：不能在 FlexConfig 对象中使用 **access-list** 命令。

例如，如果您要在网络 192.168.1.0/24 和 192.168.2.0/24 之间全局启用 DCERPC 检测，应执行以下操作。

过程

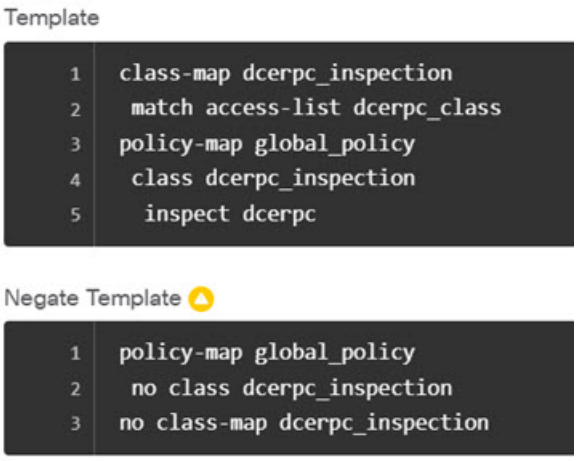
步骤 1 为两个网络创建单独的网络对象。例如，InsideNetwork 和 dmz-network。

步骤 2 在 Smart CLI 扩展访问列表对象中使用这些对象。



步骤 3 创建按名称指向 Smart CLI 对象的 FlexConfig 对象。

例如，如果为对象命名“dcerpc_class”，FlexConfig 对象应如下所示。请注意，在取消模板中，不对通过 Smart CLI 对象创建的访问列表求反，因为该对象实际上并非通过 FlexConfig 创建。



步骤 4 将对象添加到 FlexConfig 策略中。

配置密钥对象

密钥对象的重点在于隐藏密码或敏感字符串。如果不希望冒险让人看到 FlexConfig 对象或 Smart CLI 模板中使用的字符串，请为该字符串创建一个密钥对象。

过程

步骤 1 选择**对象**，然后从目录中选择**密钥**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 输入对象的名称和说明（后者为可选项）。

步骤 4 在**密码**字段和**确认密码**字段中输入密码或其他密钥字符串。

键入时系统会隐藏文本。

步骤 5 点击**确定**。

下一步做什么

- 如果是一个新对象，要在 FlexConfig 中使用该对象，请编辑 FlexConfig 对象，创建一个密钥类型变量，再选择该对象。然后，引用对象正文中的变量。有关详细信息，请参阅在 FlexConfig 对象中创建变量，第 824 页。
- 如要编辑作为 FlexConfig 策略一部分在 FlexConfig 对象中使用的现有对象，则需要部署配置，以使用新字符串更新设备。
- 在 Smart CLI 模板中，如果命令需要密钥，则在编辑相关属性时将会看到这些对象的列表。选择用于此用途的正确密钥。

FlexConfig 策略故障排除

编辑 FlexConfig 策略后，仔细检查下一部署的结果。如果您在“待处理更改”对话框中收到“上次部署失败”消息，请点击**查看详细信息**链接。链接将转至审核日志，您可以在其中找到失败的部署作业。打开作业，查找特定错误消息。

如果由于 FlexConfig 问题部署失败，则详细信息将提及带有错误命令的 FlexConfig 对象，并显示失败的命令。使用此信息更正对象并再次尝试部署。对象名称是一个链接，点击打开对象的编辑对话框。

例如，您可能需要配置最大 TCP 段大小 (TCP MSS)。您可以使用 **sysopt connection tcpmss** 命令控制此设置。通过 设备管理器配置时，此选项的 威胁防御 默认值为 0，而 ASA 默认值为 1380。

ASA 默认值是在使用 1500 默认 MTU 的接口上运行 IPv4 VPN 时的最佳处理。系统需要 120 个字节用于 VPN 报头。对于 IPv6，系统需要 140 个字节。 威胁防御 默认值为 0，仅允许终端协商 MSS，这是正常流量的理想设置，尤其是在设备接口上使用不同 MTU（包括超过 1500 的 MTU）的情况

下。由于 TCP MSS 是一个全局设置而不是根据接口，所以仅当流量中很大一部分通过 VPN，且获得过多分段时，才可对其进行更改。在这种情况下，可将 TCP MSS 设为 MTU - 120（适用于 IPv4）或 MTU - 140（适用于 IPv6），并将同一 MTU 用于所有接口。请注意，即使您明确设置了 MSS，如果 TLS/SSL 解密或服务器发现等组件需要某个特定 MSS，它也会根据接口 MTU 设置该 MSS 并忽略您设置的 MSS。

为了说明这个问题，现在假设需要将 TCP MSS 设为 3 个字节。该命令需要取 48 个字节作为最小值，因此，您会得到类似于以下内容的部署错误：

错误由这些元素组成：

1. 部署错误消息，其中包括导致错误的 FlexConfig 对象的名称。对象名称链接到编辑对话框，以便可快速打开对象更正错误。这是消息的第一句。
2. 以“ERROR：”开头的文本是从设备返回的消息。在键入错误命令但不格式化 SSH 客户端的情况下，ASA 就会做出这种响应。在本例中，错误消息是 “ERROR：[3] 小于 RFC 791 允许的最小 MSS 值 48”。以“Config Error”开头的文本会提及生成错误消息的特定行。
3. 黑色文本是实际导致错误的 FlexConfig 对象行。必须修复此行。在本例中，如果尝试在 MTU 1500 接口上（常见情况）容纳 IPv4 VPN 流量，则应将 3 改为 1380。

   修复本例时，可保持打开 CLI 控制台并使用 **show running-config all sysopt** 查看所有 **sysopt** 命令设置。多数 **sysopt** 命令均具有适用于多数用途的默认设置，因此，不会出现在运行配置中。**all** 关键字包括输出中的这些默认设置。

FlexConfig 示例

以下主题介绍使用 FlexConfig 配置功能的一些示例。

如何启用和禁用默认全局检测

某些协议在用户数据包中嵌入 IP 寻址信息，或在动态分配的端口上打开辅助信道。这些协议需要系统执行深度数据包检测，以便应用 NAT，并允许辅助信道。默认情况下，系统上启用了几个常见检测引擎，但您可能需要根据您的网络启用其他检测引擎或禁用默认检测。

要查看当前已启用的检测列表，请在 CLI 控制台或 SSH 会话中使用 **show running-config policy-map** 命令。以下是此命令在尚未更改检测配置的系统上运行的情况。在此输出中，输出末尾的 **inspect** 命令列表显示启用了哪些协议检测。上述命令在 inspection_default 流量类上启用这些检测（这是常规协议以及被检查协议的端口号，如果适用）。此类是 global_policy 策略映射的一部分，该映射使用未在输出中显示的服务策略命令将这些检测应用到所有接口。例如，在通过设备的所有 ICMP 流量上执行 ICMP 检查。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
!
```

注释 有关每个检测的详细讨论，请参阅《思科*ASA*系列防火墙配置指南》，网址为 https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html。

以下过程介绍如何启用或禁用此全局应用默认检测类中的检测。为便于解释，在本例中：

- 启用 PPTP（点对点隧道协议）。此协议用于在终端之间创建点对点连接。
- 禁用 SIP（会话发起协议）。通常仅当检测引发网络问题时，才会禁用 SIP。但是，如果禁用 SIP，必须确保访问控制策略允许 SIP 流量 (UDP/TCP 5060) 和任何动态分配的端口，而且，您无需为 SIP 连接提供 NAT 支持。通过标准页面而不是 FlexConfig 相应地调整访问控制和 NAT 策略。

开始之前

良好的规划可帮助您有效地使用 FlexConfig。在本示例中，我们要更改两个不同的不相关检测，尽管我们在同一流量类中进行更改。如果您需要更改这些策略，很可能需要单独执行此操作。

因此，我们建议在本示例中为每项检测创建单独的 FlexConfig 对象。通过这种方式，您可以轻松更改一项检测的设置，无需更改另一项检测的设置，也无需编辑 FlexConfig 对象。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。

步骤 3 创建要启用 PPTP 检测的对象。

a) 点击 **+** 按钮以创建新的对象。

b) 为对象输入名称。例如，**Enable_PPTP_Global_Inspection**。

c) 在**模板**编辑器中，输入以下命令，包括缩进。

```
policy-map global_policy
 class inspection_default
  inspect pptp
```

d) 在**取消模板**编辑器中，输入撤消此配置所需的命令。

正如要让命令启用模板需要添加父命令以进入正确的子模式那样，您也需要在取消模板中添加这些命令。

取消模板将在您从FlexConfig策略删除此对象（部署成功后删除）时，以及不成功的部署期间应用（将配置重置为之前的状态）。

因此，在本示例中，取消模板为：

```
policy-map global_policy
 class inspection_default
  no inspect pptp
```

该对象应如下所示：

高级配置

注释 由于 inspection_default 类启用了其他检测命令，您不想取消整个类。同样，global_policy 策略映射包括这些其他检测，而您也不想否定策略映射。

e) 点击**确定**保存对象。

步骤 4 创建要禁用 SIP 检查的对象。

a) 点击 + 按钮以创建新的对象。

b) 为对象输入名称。例如，**Disable_SIP_Global_Inspection**。

c) 在**模板**编辑器中，输入以下命令，包括缩进。

```
policy-map global_policy
 class inspection_default
  no inspect sip
```

d) 在**取消模板**编辑器中，输入撤消此配置所需的命令。

禁用“no”命令的“否定”命令是启用功能的命令。因此，“取消”模板不仅仅是禁用某项功能的命令，它是“肯定”模板中所执行任何命令的反向命令。取消模板的实质是撤消所做的更改。

因此，在本示例中，取消模板为：

```
policy-map global_policy
 class inspection_default
```

```
inspect sip
```

该对象应如下所示：

e) 点击**确定**保存对象。

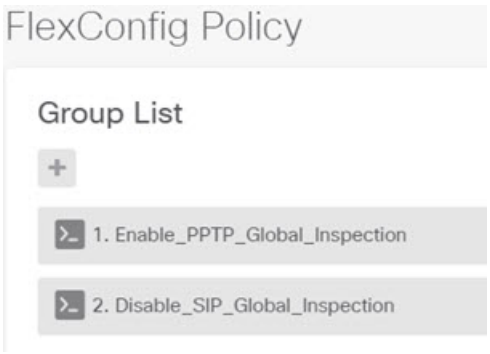
步骤 5 将对象添加到 FlexConfig 策略中。

仅创建对象远远不够。仅当您将对象添加到FlexConfig策略（并保存所做的更改）时，才部署对象。这样，您可以在对象上试验（可部分完成），不必担心会在未完成的作业上失败。您可以通过添加和删除对象轻松打开或关闭功能：无需每次都重新创建对象。

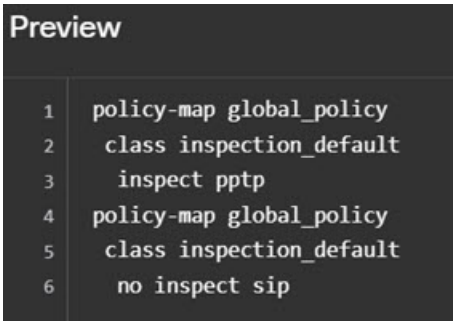
a) 点击目录中的 **FlexConfig 策略**。
b) 在组列表中点击 **+**。
c) 选择 Enable_PPTP_Global_Inspection 和 Disable_SIP_Global_Inspection 对象，然后点击**确定**。

组列表应如下所示：

高级配置



系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。



d) 点击**保存**。

您现在可以部署策略。

步骤 6 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 7 在 CLI 控制台或 SSH 会话中，使用 **show running-config policy-map** 命令并验证运行配置是否具有正确的更改。

请注意，在以下输出中，**inspect pptp** 已添加到 inspection_default 类的底部，而 **inspect sip** 在类中不再存在。这表示已成功部署 FlexConfig 对象中定义的更改。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
```

```
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
!
```

如何撤消 FlexConfig 更改

如果您在 FlexConfig 对象中输入正确的取消模板，删除使用该对象所做的更改非常简单。只需从 FlexConfig 策略中删除该对象，下一个部署时，系统即可使用取消模板撤消所做的更改。

您不需要创建新对象来撤消所做的更改。

以下示例展示如何重新启用全局 SIP 检测。该示例将恢复如何启用和禁用默认全局检测，第 833 页中所述的更改，此部分已禁用 SIP 检测。

开始之前

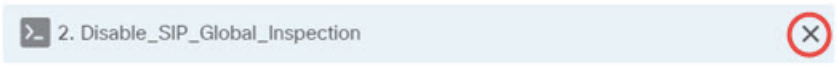
验证 FlexConfig 对象是否具有正确的取消模板。如果没有，请编辑对象更正取消模板。

过程

步骤 1 在**设备 (Device)** > **高级配置 (Advanced Configuration)**中点击**查看配置 (View Configuration)**。

步骤 2 在“高级配置”(Advanced Configuration) 目录中依次点击 **FlexConfig** > **FlexConfig 策略 (FlexConfig Policy)**。

步骤 3 点击 FlexConfig 策略中 **Disable_SIP_Global_Inspection** 对象条目右侧的 **X**，将其从策略中删除。



预览中将删除该对象中的命令。取消命令不会添加到预览，而是在后台执行。

步骤 4 点击**保存 (Save)**。

步骤 5 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 6 在 CLI 控制台或 SSH 会话中，使用 **show running-config policy-map** 命令并验证运行配置是否具有正确的更改。

请注意，在以下输出中，**inspect sip** 已添加到 inspection_default 类的底部。这表示已成功部署 FlexConfig 对象中定义的更改。（顺序在此类中不重要，因此， **inspect sip** 在末尾，而不在其原始位置并不重要。)

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
  inspect sip
!
```

如何启用唯一流量类检测

在本示例中，我们将对特定接口上两个终端之间的流量启用 PPTP 检测。此检测仅面向两者之间配置点到点隧道的终端。

启用 2 个终端之间 PPTP 检测所需的 CLI 涉及以下要素：

1. 源和目标设置为终端主机 IP 地址的 ACL。
2. 引用此 ACL 的流量类。
3. 包含流量类，并在该流量类上启用 PPTP 检测的策略映射。

4. 将策略映射应用到所需接口的服务策略。此步骤实际上是激活策略并启用检测的操作。

注释 有关与检测相关的服务策略的详细讨论，请参阅《思科 *ASA* 系列防火墙配置指南》，网址为：https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。

步骤 3 点击 + 按钮以创建新的对象。

步骤 4 为对象输入名称。例如，**Enable_PPTP_Inspection_on_Interface**。

步骤 5 为内部接口添加一个变量。

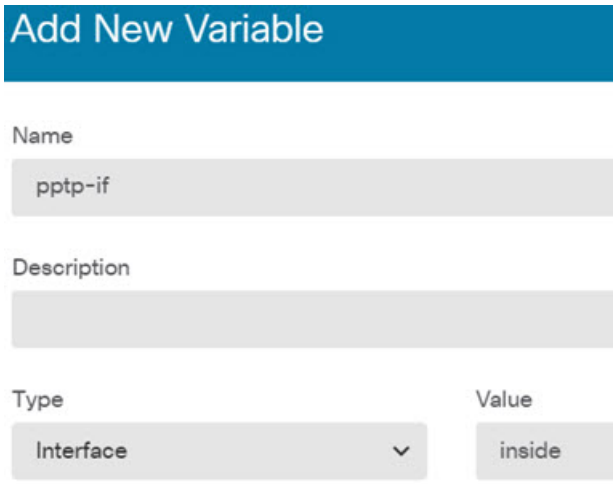
a) 点击变量列表上方的 +。

b) 输入变量的名称，例如 **pptp-if**。

c) 对于**类型**，请选择**接口**。

d) 对于**值**，请选择**内部**接口。

对话框应如下所示：



e) 点击**添加**。

步骤 6 在**模板**编辑器中，输入以下命令，包括缩进。

```
access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
class-map MATCH_CMAP
 match access-list MATCH_ACL
policy-map PPTP_POLICY
 class MATCH_CMAP
```

```
  inspect pptp
service-policy PPTP_POLICY interface {{pptp-if.name}}
```

请注意，要使用 变量，请在双括号中键入变量名称。此外，您还需要使用圆点表示法来选择您想要检索的属性，因为定义接口的对象具有许多属性。由于接口名称保存在“name”属性中，输入 **{{pptp-if.name}}** 将为接口检索分配给变量的名称属性的值。如果您需要更改执行 PPTP 检测的接口，只需选择变量定义中的其他接口。

步骤 7 在**取消模板**编辑器中，输入撤消此配置所需的命令。

对于本示例中，我们将假设类映射、策略映射和服务策略仅用于应用 PPTP 检测目的。因此，在取消模板中，我们想要删除所有这些要素。

但是，如果您将 PPTP 检测实际添加到接口上的现有服务策略，不需要对策略映射或服务策略求反。您可以从策略映射对类求反，或仅在策略映射的类中关闭检测。您需要清楚了解您在其他 FlexConfig 对象中实施的策略，确保取消模板不会产生意外的后果。

删除嵌套项目时，您需要按照与项目创建顺序相反的顺序执行删除。因此，您需要先删除服务策略，最后再删除访问列表。否则，您将尝试删除正在使用的对象，而系统将返回错误，不允许您执行此操作。

```
no service-policy PPTP_POLICY interface {{pptp-if.name}}
no policy-map PPTP_POLICY
no class-map MATCH_CMAP
no access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
```

该对象应如下所示：

高级配置

Name

Enable_PPTP_Inspection_on_Interface

Description

Variables

NAME	TYPE	VALUE	DESCRIPTION	ACTIONS
pptp-if	Interface	inside		

Template Expand Reset

```
1  access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
2  class-map MATCH_CMAP
3   match access-list MATCH_ACL
4  policy-map PPTP_POLICY
5   class MATCH_CMAP
6    inspect pptp
7  service-policy PPTP_POLICY interface {{pptp-if.name}}
```

Negate Template Expand Reset

```
1  no service-policy PPTP_POLICY interface {{pptp-if.name}}
2  no policy-map PPTP_POLICY
3  no class-map MATCH_CMAP
4  no access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
```

步骤 8 点击**确定**保存对象。

步骤 9 将对象添加到 FlexConfig 策略中。

a) 点击目录中的 **FlexConfig 策略**。

b) 在组列表中点击 **+**。

c) 选择 **Enable_PPTP_Inspection_on_Interface** 对象，然后点击**确定**。

组列表应如下所示：

FlexConfig Policy

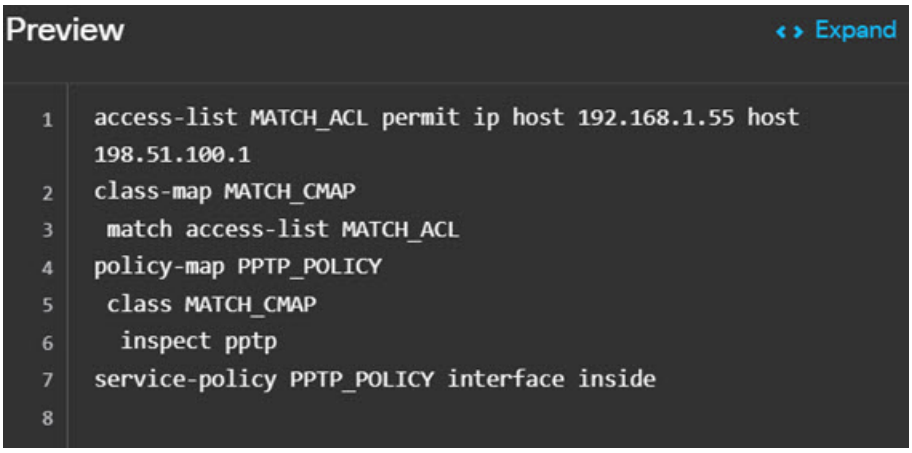
Group List

Drag and drop to reorder

1. Enable_PPTP_Inspection_on_Interface

高级配置

系统应随即使用模板中的命令更新预览。验证您是否看到下图所示的预期命令。请注意，接口变量在预览中解析为名称“inside”。需要特别注意变量：如果在预览中解析不正确，它们将不能正确部署。编辑 FlexConfig 对象，直到可以在预览中获得正确的变量转换。



d) 点击**保存**。

您现在可以部署策略。

步骤 10 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 11 在 CLI 控制台或 SSH 会话中，使用 **show running-config** 命令的变体并验证运行配置是否具有正确的更改。

您可以输入 **show running-config** 检查整个 CLI 配置，也可以使用以下命令验证此配置的每个部分：

- **show running-config access-list MATCH_ACL** 验证 ACL。
- **show running-config class** 验证类映射。此命令将显示所有类映射。
- **show running-config policy-map PPTP_POLICY** 验证类和策略映射配置。
- **show running-config service-policy** 验证应用于接口的策略映射。这将显示所有服务策略。

以下输出显示该序列命令，您可以看到配置已正确应用。

```
> show running-config access-list MATCH_ACL
access-list MATCH_ACL extended permit ip host 192.168.1.55 host 198.51.100.1

> show running-config class
!
class-map MATCH_CMAP
```

```
 match access-list MATCH_ACL
class-map inspection_default
 match default-inspection-traffic
!

> show running-config policy-map PPTP_POLICY
!
policy-map PPTP_POLICY
 class MATCH_CMAP
  inspect pptp
!
> show running-config service-policy
service-policy global_policy global
service-policy PPTP_POLICY interface inside
```

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。