适用于 Firepower 设备管理器（版本 6.2）的思科 Firepower 威胁防御配置指南

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

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

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

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

无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均按“原样”提供，并可能包含缺陷。思科和上面所提及的供应商拒绝所有明示或暗示保证，包括（但不限于）适销性、特定用途适用性和无侵权保证，或者因买卖或使用以及商业惯例所引发的保证。

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

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

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

目 录

第 1 章

使用入门

以下主题介绍如何开始配置 Firepower 威胁防御。

本指南适用对象

本指南介绍如何使用 Firepower 威胁防御 设备自带的、基于 Web 的 Firepower 设备管理器配置界面进行配置 Firepower 威胁防御。

通过Firepower设备管理器，可以配置小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，在此类网络中，无需使用高功率的多设备管理器来控制包含许多Firepower威胁防御 设备的大型网络。

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

您可以在以下设备上使用 Firepower 设备管理器。

表 *1*：*Firepower* 设备管理器支持的型号

设备型号	Firepower 威胁防御软件最低版本
ASA 5506-X、5506H-X、5506W-X、5508-X、5516-X	6.1
ASA 5512-X、5515-X、5525-X、5545-X、5555-X	6.1

Firepower 设备管理器/Firepower 威胁防御 6.2 版中的新增功能

发布时间：2017 年 1 月 23 日

下表列出了使用 Firepower 设备管理器进行配置时，Firepower 威胁防御 6.2 版中可用的新功能。

特性	说明
思科 Defense Orchestrator 云管理	您可以使用思科 Defense Orchestrator 基于云的门户来管理设备。依次选择**设备** > **系统设置** > **云管理**。有关思科 Defense Orchestrator 的详细信息，请参阅http://www.cisco.com/go/cdo。
拖放访问规则	您可以拖放访问规则，以在规则表中移动它们的位置。
Firepower 威胁防御软件升级	您可以通过 Firepower 设备管理器安装软件升级。依次选择**设备** > **更新**。
Firepower 威胁防御默认配置更改	对于新的或重新映像的设备，默认配置有一些重大更改，包括： • （ASA 5506-X、5506W-X、5506H-X。）除了第一个数据接口和 ASA 5506W-X 上的 Wi-Fi 接口，这些设备型号上的所有其他数据接口均构建为“内部”桥接组并启用。内部桥接组上有一个 DHCP 服务器。您可以将终端或交换机插入任何桥接接口，而终端将获取 192.168.1.0/24 网络中的地址。 • 内部接口 IP 地址现在为 192.168.1.1，并在接口上定义了 DHCP 服务器，地址池为 192.168.1.5 -192.168.1.254。 • 内部接口启用了 HTTPS 访问，因此可以通过默认地址 192.168.1.1 的内部接口打开 Firepower 设备管理器。对于 ASA 5506-X 型号，可以通过任意内部桥接组成员接口打开 Firepower 设备管理器。 • 管理端口为 192.168.45.0/24 网络托管 DHCP 服务器。您可以将工作站直接插入管理端口，获取 IP 地址，并打开 Firepower 设备管理器来配置设备。 • OpenDNS 公共 DNS 服务器现在是管理接口的默认 DNS 服务器。而在以前，并没有默认的 DNS 服务器。您可以在设备设置期间配置不同的 DNS 服务器。 • 管理 IP 地址的默认网关使用数据接口路由到互联网。因此，您不需要将管理物理接口连接到网络。

特性	说明
管理接口和访问更改	管理地址的运行原理及 Firepower 设备管理器的接入方式发生了一些变化： • 现在，您可以打开 HTTPS（用于 Firepower 设备管理器）和 SSH（用于 CLI）连接的数据接口。您不需要单独的管理网络或者将管理/诊断物理端口连接到内部网络，即可管理设备。依次选择**设备** > **系统设置** > **管理访问列表**。 • 系统可以通过外部接口的网关获取系统数据库更新。您不需要从管理接口或网络到互联网的显式路由。默认设置为通过数据接口使用内部路由。但是，如果您希望使用单独的管理网络，则可以设置特定的网关。依次选择**设备** > **系统设置** > **管理接口**。 • 您可以使用 Firepower 设备管理器配置管理接口，使它通过 DHCP 获取其 IP 地址。依次选择**设备** > **系统设置** > **管理接口**。 • 如果配置静态地址，可以在管理地址上配置DHCP服务器。依次选择**设备** > **系统设置** > **管理接口**。
其他用户界面更改	以下是一些值得注意的 Firepower 设备管理器用户界面更改。 • **设备**主菜单项目。在以前的版本中，此菜单项是您设备的主机名。此外，打开的页面称为“设备摘要”，而不是“设备控制面板”。 • 在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。 • **设备** > **系统设置** > **云首选项**现在称为**设备** > **系统设置** > **URL 过滤首选项**。 • **系统设置** > **DHCP 服务器**页面现安排在两个选项卡上，DHCP 服务器表与全局参数分离。
站点间 VPN 连接	您可以使用预共享密钥配置站点间虚拟专用网络 (VPN) 连接。可以配置 IKEv1 和 IKEv2 连接。

特性	说明
集成的路由与桥接支持。	集成路由和桥接提供了在桥接组和路由接口之间路由的功能。桥接组是 Firepower 威胁防御 设备用于桥接而非路由的一组接口。Firepower 威胁防御 设备不是真正的网桥，因为 Firepower 威胁防御 设备继续充当防火墙：接口之间实施访问控制，并且部署所有常用防火墙检查。 此功能可让您配置桥接组，并在桥接组之间以及桥接组和路由接口之间进行路由。桥接组使用桥接虚拟接口 (BVI) 作为桥接组的网关参与路由。如果 Firepower 威胁防御 设备上有额外的接口分配给桥接组，集成路由和桥接可为使用外部第 2 层交换机提供替代方案。BVI 可以是一个指定接口，可以与成员接口分开参与某些功能，例如 DHCP 服务器，您在桥接组成员接口上配置其他功能（如 NAT 和访问控制规则）。 选择**设备** > **接口**配置桥接组。

登录系统

连接 Firepower 威胁防御 设备的接口有两个：

Firepower 设备管理器 Web 界面

Firepower 设备管理器在网络浏览器中运行。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。另外，也可以使用它来代替 Firepower 设备管理器进行初始设置。

以下主题介绍如何登录这些界面和管理您的用户帐户。

登录 Firepower 设备管理器

使用Firepower设备管理器可配置、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 Firefox、Chrome、Safari 或 Internet Explorer 的当前版本。

开始之前

您只能使用 **admin** 用户名登录 Firepower 设备管理器。您无法为 Firepower 设备管理器访问创建其他用户。

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。如果已配置了 Ipv4 或 IPv6 地址或 DNS 名称，可以使用。

- 管理地址。默认情况下，这在管理/诊断接口上为 192.168.45.45。
- 您为 HTTPS 访问打开的数据接口的地址。默认情况下，“inside”接口允许 HTTPS 访问，因此您可以连接到默认的内部地址 192.168.1.1。在内部接口为桥接组的设备型号上，可以通过任何桥接组成员接口连接到此地址。

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 输入 **admin** 用户名和密码，然后点击**登录**。
默认管理员密码为 Admin123。

如果会话连续20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**。

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、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。
- 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，您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 261 页）。默认情况下，禁用 SSH 数据接口访问。使用 **admin** 用户名（默认密码为 Admin123）或其他 CLI 用户帐户登录。

登录后，如需了解CLI中可用的命令，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 上的 *Firepower* 威胁防御命令参考。

注释 您可以使用 **configure user add** 命令创建可登录 CLI 的用户帐户。但这些用户只能登录于 CLI，无法登录到 Firepower 设备管理器 Web 界面。

更改您的密码

密码应定期更改。以下步骤介绍了登录到 Firepower 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* 命令更改不同 CLI 用户的密码。

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。

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**。

为 Firepower 威胁防御创建 CLI 用户帐户

您可以在 Firepower 威胁防御设备上为 CLI 访问创建用户。这些帐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帐户。每个设备都有自己的一组唯一 CLI 帐户。

过程

步骤 1 使用具有配置权限的帐户登录设备 CLI。
管理员用户帐户具有所需的权限，但具有配置权限的任何帐户都可以执行操作。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** 命令可进入 Firepower 威胁防御 CLI。

步骤 2 创建用户帐户。
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帐户。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帐户的特性。
您可以使用以下命令更改默认帐户行为。

- **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。当您创建帐户时，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*

  设置在锁定帐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** 命令解锁帐户。新帐户的默认值为 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 根据需要管理用户帐户。
用户可能被锁定在帐户之外了，也可能您需要删除帐户或解决其他问题。使用以下命令管理系统中的用户帐户。

- **configure user access** *username* {**basic** | **config**}

  更改用户帐户的权限。

- **configure user delete** *username*

  删除指定的帐户。

- **configure user disable** *username*

  禁用指定的帐户，而不将其删除。用户无法登录，直到您启用该帐户为止。

- **configure user enable** *username*

  启用指定的帐户。

- **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帐户。

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，请参阅初始设置之前的默认配置，第 20 页。

过程

步骤 1 连接接口，第 9 页

步骤 2 完成初始配置，第 13 页
有关生成的配置的详细信息，请参阅进行初始设置之后的配置，第 21 页。

步骤 3 配置无线接入点 (ASA 5506W-X)，第 17 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。

的默认配置旨在让您将工作站直接连接到内部接口。对于内部接口为桥接组的设备型号，您可以连接到任意成员接口。或者，您也可以直接将工作站连接到管理端口。通过 DHCP 在正确的网络上获取地址。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或管理接口连接到具有活动 DHCP 服务器的网络。这将与已在内部端口和管理端口上运行的 DHCP 服务器冲突。如果要使用其他 DHCP 网络服务器，只需将工作站直接连接到管理端口，完成初始配置，然后禁用不需要的 DHCP 服务器。然后，您就可以将设备连接到网络。

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。

ASA 5506-X、5506W-X 和 5506H-X 的布线

图 *1*：*ASA 5506W-X*（有 *Wi-Fi*）、*5506-X*（无 *Wi-Fi*）

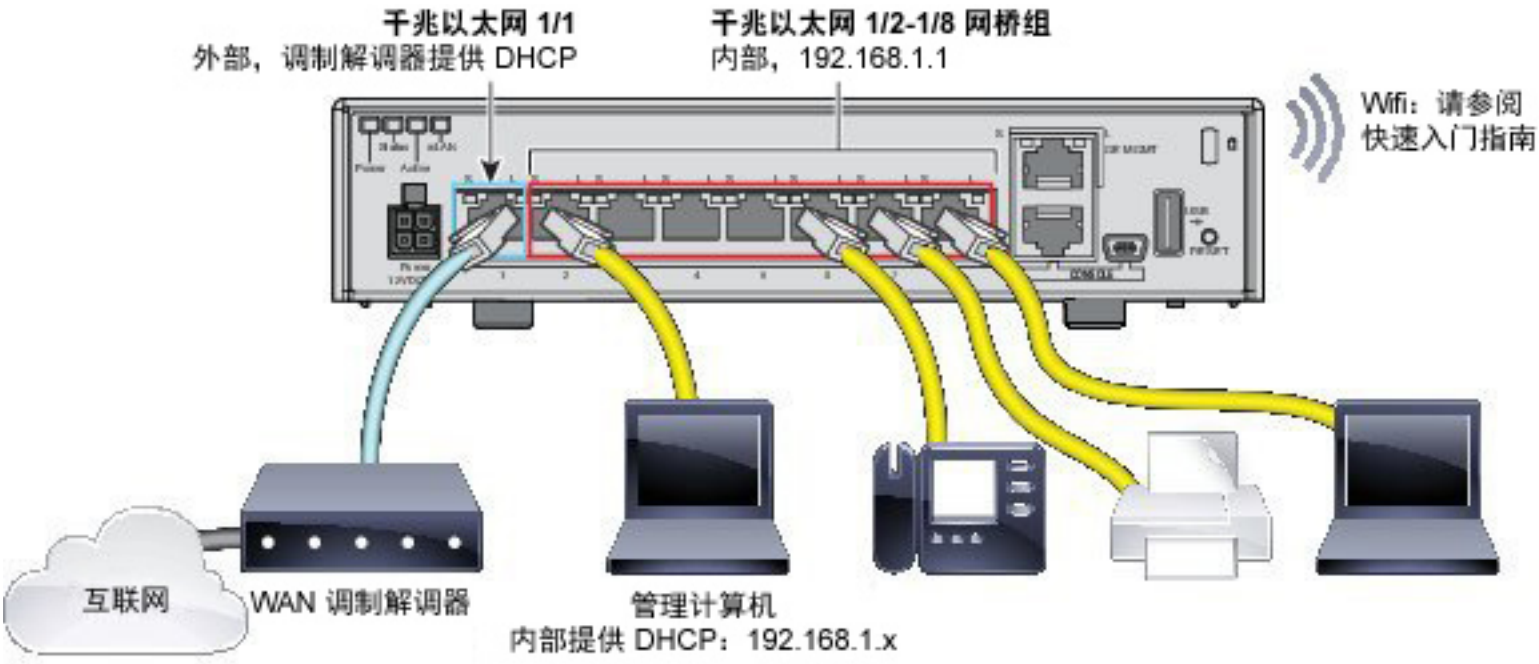
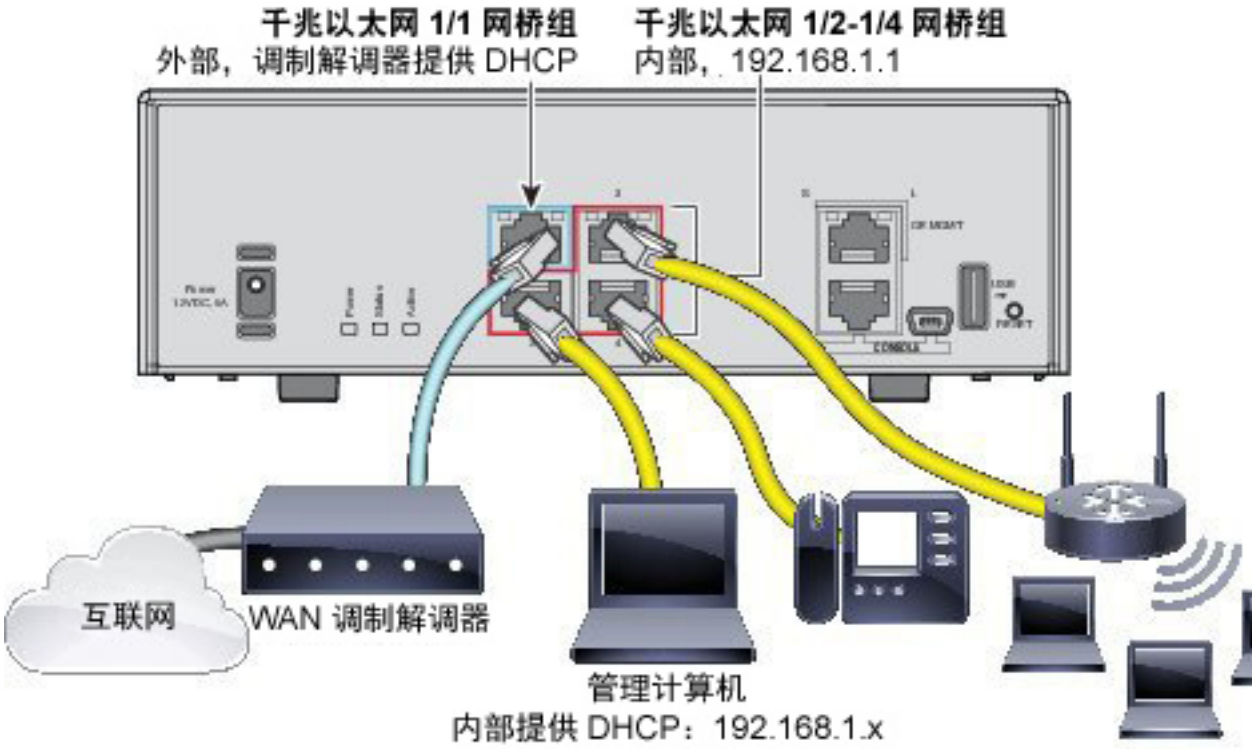


图 *2*：*ASA 5506H-X*

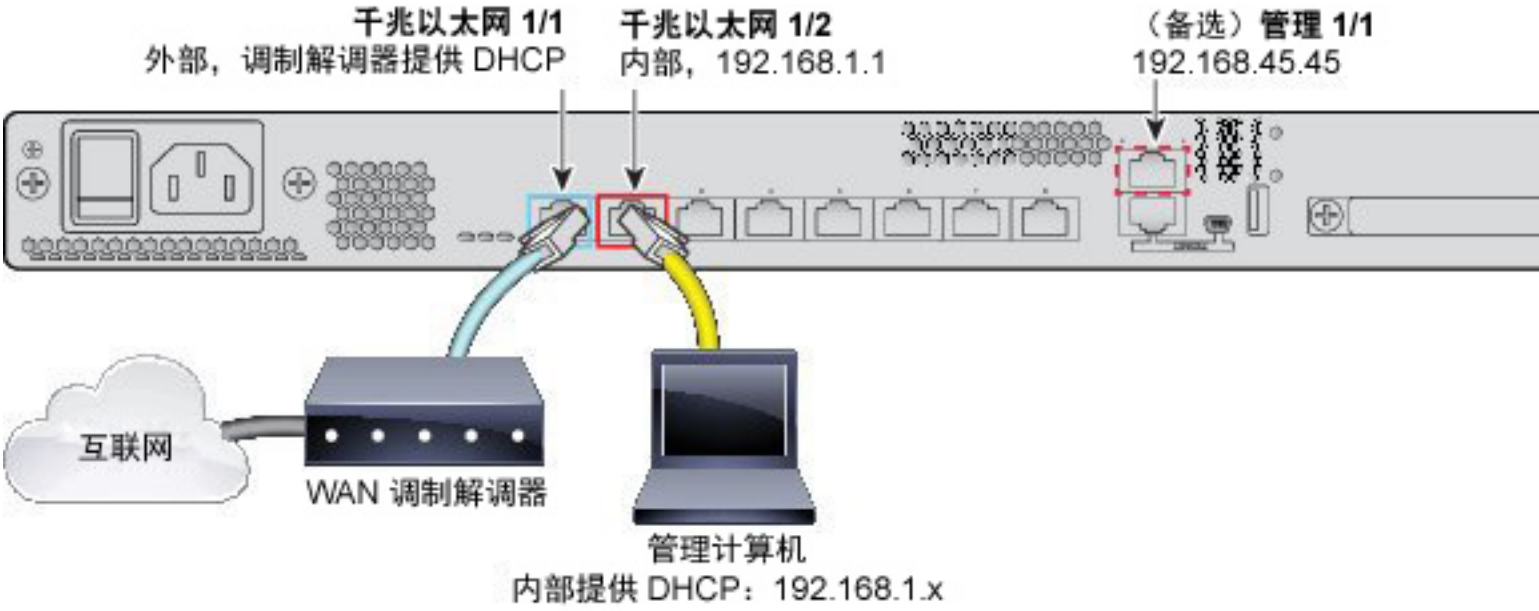


- 将 GigabitEthernet 1/1 连接到 ISP/WAN 调制解调器或其他外部设备。默认情况下，使用 DHCP 获取 IP 地址，但可以在初始配置期间设置静态地址。
- 将 GigabitEthernet 1/2（或另一个内部桥接组成员端口）连接到您的工作站，您将用它来配置设备。将工作站配置为通过 DHCP 获取 IP 地址。工作站将获得 192.168.1.0/24 网络中的地址。

注释 连接管理工作站还有几种其他选择。您也可以直接将其连接到管理端口。该工作站通过 192.168.45.0/24 网络上的 DHCP 获取地址。另一个方法是将工作站连接到一台交换机，并将该交换机连接到一个内部端口（例如GigabitEthernet1/2）。但是，您必须确保交换机的网络上没有正在运行 DHCP 服务器的其他设备，否则它会与在内部桥接组 192.168.1.1 上运行的设备冲突。

- 或者，将其他终端或交换机连接到内部桥接组中的其他端口。您最好是等到完成初始设备设置后再添加终端。如果添加交换机，请确保没有其他 DHCP 服务器在这些网络上运行，否则会与在内部桥接组上运行的 DHCP 服务器冲突。

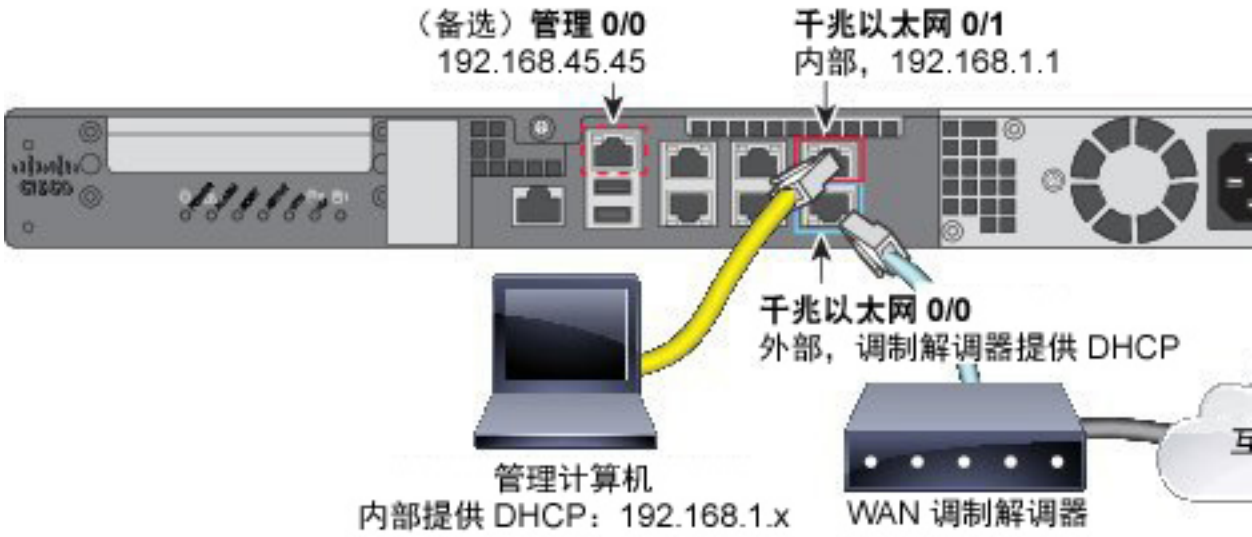
ASA 5508-X 和 5516-X 的布线



- 将 GigabitEthernet 1/1 连接到 ISP/WAN 调制解调器或其他外部设备。默认情况下，使用 DHCP 获取 IP 地址，但可以在初始配置期间设置静态地址。
- 将 GigabitEthernet 1/2 连接到您的工作站，即您将用来配置设备的工作站。将工作站配置为使用 DHCP 来获取 IP 地址。工作站将获得 192.168.1.0/24 网络中的地址。

注释 连接管理工作站还有几种其他选择。您也可以直接将其连接到管理端口。该工作站通过 192.168.45.0/24 网络上的 DHCP 获取地址。另一个方法是将工作站连接到交换机，并将该交换机连接到 GigabitEthernet1/2。但是，必须确保交换机的网络上没有其他设备正在运行 DHCP 服务器，因为它将与在内部接口 192.168.1.1 上运行的设备冲突。

ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X 的布线



- 将 GigabitEthernet 0/0 连接到 ISP/WAN 调制解调器或其他外部设备。默认情况下，使用 DHCP 获取 IP 地址，但可以在初始配置期间设置静态地址。
- 将 GigabitEthernet 0/1 连接到准备用于配置设备的工作站。将工作站配置为使用 DHCP 获取 IP 地址。工作站将获得 192.168.1.0/24 网络中的地址。

注释 连接管理工作站还有几种其他选择。您也可以直接将其连接到管理端口。工作站将通过 DHCP 获得 192.168.45.0/24 网络中的地址。另一个选择是仍将工作站连接到一台交换机，并将该交换机连接到 GigabitEthernet0/1。不过，必须确保该交换机的网络中没有其他设备运行 DHCP 服务器，否则就会与内部接口 192.168.1.1 上运行的 DHCP 服务器冲突。

完成初始配置

在首次登录 Firepower 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。

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 9 页和初始设置之前的默认配置，第 20 页）。

然后，将您的工作站连接到硬件型号的“内部”接口。对于内部接口是桥接组的型号，可以连接到任意桥接组成员接口，即除外部接口之外的任意数据端口。或者，您可以连接到管理/诊断物理接口。

管理/诊断物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/诊断接口连接到网络并配置单独的管理网关。

过程

步骤 1 登录 Firepower 设备管理器。

a) 假设您没有在 CLI 中进行初始配置，则在 **https://** *IP* 地址（其中地址为以下任意一个地址）打开 Firepower 设备管理器。

- 如果您已连接到内部接口，或具有默认内部桥接组的型号的一个内部桥接组数据接口：**https://192.168.1.1**。
- 如果连接到管理物理接口，则地址为：**https://192.168.45.45**。

b) 使用用户名 **admin** 和密码 **Admin123** 登录。

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。确保您的设置正确。如果您最终在与内部接口位于同一子网的外部接口上配置 IP 地址，并且连接到了内部地址上的 Firepower 设备管理器，那么当点击 **Next** 时，向导将会挂起，因为内部接口上的地址将被删除。要恢复，请参阅外部子网与内部子网冲突时怎么办（设置向导在第 1 步中挂起），第 15 页。

外部接口

- **配置 Ipv4 (Configure 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（请参阅初始设置之前的默认配置，第 20 页）。
- **配置 Ipv6 (Configure 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。

管理界面

- **DNS 服务器 (DNS Servers)** - 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。如果您编辑字段并想要恢复默认值，请点击**使用 OpenDNS** 以重新将合适的 IP 地址加载到字段。
- **防火墙主机名 (Firewall Hostname)** - 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 (Time Zone)** - 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，请点击链接登录您的智能软件管理器帐户，生成新的令牌，并将该令牌复制到编辑框。

要使用评估许可证，请选择**开始 90 天评估期，无需注册 (Start 90 day evaluation period without registration)**。若要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**组的链接。

步骤 6 点击**完成 (Finish)**。

接下来的操作

- 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 61 页。
- 如果这是新系统，则具有默认内部桥接组的设备型号上的其他接口可以用作内部桥接组的成员。您可以将终端直接连接到接口。对于具有单个默认物理接口的型号，可以将其他数据接口连接到不同的网络并配置接口。对于桥接组成员接口，您可以从桥接组移除它们并配置额外的唯一网络。有关配置接口的信息，请参阅如何添加子网，第 51 页和配置接口，第 97 页。
- 如果通过内部接口或桥接组成员接口管理设备，并且想通过内部接口打开 CLI 会话，请打开内部接口或 SSH 连接的桥接组。请参阅配置管理访问列表，第 261 页。
- 查看使用案例以了解如何使用产品。请参阅Firepower 威胁防御的使用案例，第 29 页。

外部子网与内部子网冲突时怎么办（设置向导在第 1 步中挂起）

如果通过内部接口连接到Firepower设备管理器，可能会发现，在第1步中（即配置外部接口一步）点击**Next**时，设置向导会挂起。请注意，通常情况下，完成此步骤需要花费一点时间，因此挂起意味着此过程将继续执行超过 10 分钟。如果刷新浏览器，您会看到已与 Firepower 设备管理器断开连接。（如果通过管理 IP 地址连接，该向导不会挂起，但您可能仍会遇到如下症状中所述的问题。）

发生这种情况最可能的原因是在同一子网上为外部和内部接口分配地址，这会导致内部接口丢失其配置。

默认配置包括内部接口上的静态地址以及 DHCP 服务器，以便您在完成设置向导后，设备可以立即投入工作，可以传递流量并支持连接的工作站。

但是，仅当您未在同一子网上为外部接口配置地址时，才可以使用默认的内部地址。这包括将通过DHCP提供地址的ISP设备连接到外部地址的情况。某些ISP为其内部接口（连接到您的外部接口）与 Firepower 威胁防御为其内部地址使用相同的 192.168.1.0/24 子网。

要解决此问题，您必须更改内部接口上的 IP 地址。

内部/外部子网冲突的症状

以下是在同一子网上为内部和外部接口分配地址的症状。

- 在设备设置向导运行期间，如果在第 1 步点击 Next，向导会挂起。请注意，通常情况下，完成此步骤需要花费一点时间，因此挂起意味着此过程将继续执行超过 10 分钟。
- 如果您连接到控制台端口，会在 CLI 中看到以下信息。如果尝试从 Firepower 设备管理器部署配置（无后续更改），也会看到此消息。

```
ERROR: Failed to apply IP address to interface GigabitEthernet1/1,
as the network overlaps with interface GigabitEthernet1/2.
Two interfaces cannot be in the same subnet.
```

- 如果完成设置，或者退出，则连接图会显示未与任何外部服务（例如网关、DNS 和 NTP 服务器以及智能许可）进行连接。在菜单中的 Deploy 图标还会显示需要部署。
- 从 CLI 中，**interface** 和 **dhcp** 配置在使用 **show running-config** 和 **show startup-config** 命令查看时对于内部和外部接口是不一致的。

过程

步骤 1 在设备设置期间，如果您连接到内部接口，则设置完成。

a) 通过插入管理接口重新连接到设备。如果需要，请释放并续订工作站的 DHCP 地址，以获得管理网络中的一个新地址 (192.168.45.0/24)。如果需要，请为您的工作站配置一个范围介于 192.168.45.1 和 192.168.45.44 之间的静态地址。

b) 通过 https://192.168.45.45 打开 Firepower 设备管理器。

c) 您应该会看到一条提示，要求您启动 90 天的评估许可证。选择此选项，然后点击 **Confirm**。

d) 依次选择 **Device** > **System Settings** > **NTP**，配置 NTP 服务器，然后点击 **Save**。如果默认服务器可以满足您的要求，可以跳过此步骤。

e) 从菜单右上方的用户图标下拉列表中选择 **Profile**，为设备选择时区，然后点击 **Save**。

f) 如果不想使用评估许可证，请依次选择 **Device** > **Smart License** > **View Configuration**，点击 **Request Register**，然后按照说明注册设备。请参阅注册设备，第 60 页。（此时您也可以启用所需的任何可选许可证。）

步骤 2 从内部接口删除 DHCP 服务器。

a) 依次选择 **Device** > **System Settings** > **DHCP Server**。

b) 点击 **DHCP 服务器**选项卡。

c) 将鼠标放置在内部接口行中的 **Actions** 列中，然后点击删除图标 ()。

步骤 3 更改内部接口上的地址。

a) 选择 **Device**。

b) 在 Interfaces 组中，点击指示了已启用接口数的链接（例如 **3 Enabled**）。

c) 将鼠标放置在内部接口中的 **Actions** 列中，然后点击编辑图标 ()。

d) 在 **IPv4 Address** 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。

e) 点击 **OK**。

步骤 4 （可选。）在内部地址上配置 DHCP 服务器。
如果为内部接口配置静态地址，则可以配置 DHCP 服务器来为连接至内部网络的工作站分配地址。这是典型设置。

a) 依次选择 **Device** > **System Settings** > **DHCP Server**。
b) 点击 **DHCP 服务器**选项卡。
c) 点击 +。
d) 选择此选项以启用该服务器并选择内部接口。
e) 对于地址池，请输入在与内部地址相同的子网上的一个范围。
例如，如果内部地址是 192.168.2.1/24，则可以使用 192.168.2.5-192.168.2.254。不要包括静态分配到该网络上的节点的地址。考虑保留该池外的几个地址，以便在需要时可以分配静态地址。

f) 点击 **OK**。

步骤 5 点击菜单中的**部署**按钮以部署更改。

步骤 6 点击**立即部署 (Deploy Now)**。
部署完成后，连接图对于外部服务应显示绿色。

配置无线接入点 (ASA 5506W-X)

ASA 5506W-X 包括集成到设备中的思科 Aironet 702i 无线接入点。该无线接入点默认处于禁用状态。连接到接入点的 Web 界面，以便可以启用无线电并配置 SSID 和安全设置。

接入点通过 GigabitEthernet1/9 接口进行内部连接。所有 Wi-Fi 客户端均属于该 GigabitEthernet1/9 网络。您的安全策略决定了 Wi-Fi 网络访问其他接口上任何网络的方式。接入点不含任何外部接口或交换机端口。

以下步骤介绍了如何配置接入点。该步骤假定您已完成了设备设置向导。如果您以手动方式配置设备，可能需要根据配置调整步骤。

有关详细信息，请参阅以下手册：

- 有关使用无线 LAN 控制器的详细信息，请参阅思科无线 LAN 控制器软件文档。
- 有关无线接入点硬件和软件的详细信息，请参阅思科 Aironet 700 系列文档。

开始之前

如果您无法连接到无线接入点，而 Firepower 威胁防御 设备使用的是建议的配置且未发现任何其他网络问题，您可能需要恢复无线接入点的默认配置。为此，您必须进入 Firepower 威胁防御 CLI（连接到控制台端口，或者配置 SSH 访问）。在 Firepower 威胁防御 CLI 中，输入以下命令。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password: <press enter, by default, the password is blank>
firepower# hw-module module wlan recover configuration
```

如果需要进一步对无线接入点进行故障排除，请使用 **session wlan console** 命令连接到无线接入点 CLI。

过程

步骤 1 配置并启用无线接口 GigabitEthernet1/9。

a) 点击**设备**，然后点击**接口**组中的链接以打开接口列表。

b) 点击 GigabitEthernet1/9 接口的编辑图标 ( )。

c) 配置以下选项。

- **接口名称 (Interface Name)** - 输入接口的名称，例如 **wifi**。
- **状态 (Status)** - 点击滑块可启用该接口。
- **IPv4 地址** - 选择**静态**作为地址类型，然后输入地址和子网掩码。例如 192.168.10.1/24。

d) 点击**保存 (Save)**。

步骤 2 将 Wi-Fi 接口添加到与内部接口相同的安全区。
设备设置向导将**内部**桥接组成员放在名为 **inside_zone** 的安全区。Wi-Fi 接口需要位于此安全区，以便您可访问无线接入点 Web 界面（通过默认的 Inside_Inside_Rule 访问规则实现）。

a) 点击菜单中的**对象**，然后从目录中选择**安全区**。

b) 点击 **inside_zone** 的编辑图标 ( )。

c) 点击**接口**下的 +，然后选择 **wifi** 接口。

步骤 3 验证是否存在允许 **inside_zone** 安全区中的接口之间的流量的访问控制规则。
设备设置向导将创建一项规则，允许流量从 **inside_zone** 流至 **outside_zone**，从而允许内部用户访问互联网。

该向导还创建一项规则，允许流量在 **inside_zone** 和 **inside_zone** 之间流动，以便内部主机可以互相访问。

通过将 **wifi** 接口添加到 **inside_zone**，Wi-Fi 用户也包含在这两个规则中，以便他们可以访问互联网和其他内部用户。

如果未完成向导，则这些规则可能不存在。由于默认操作是阻止所有流量，因此您必须创建这些规则。以下步骤说明了如何创建规则，以允许 **inside_zone** 安全区中的接口之间的流量。

a) 点击菜单中的**策略**。
b) 点击**访问控制**表上的 + 添加规则。
c) 在规则中必须配置以下选项。

- **标题 (Title)** - 为规则输入名称。例如 Inside_Inside。
- **操作 (Action)** - “允许”(Allow) 或“信任”(Trust)。
- **源/目的** > **源区** - 选择 inside_zone。
- **源/目的** > **目的区** - 选择 inside_zone。

d) 点击**确定 (OK)**。

步骤 4 在无线接口上配置 DHCP 服务器。
DHCP 服务器为连接到无线接入点的设备提供 IP 地址。另外，它还向无线接入点本身提供地址。

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。
d) 点击 DHCP 服务器表上方的 +。
e) 配置以下 DHCP 服务器属性。

- **启用 DHCP 服务器 (Enable DHCP Server)** - 点击滑块可启用 DHCP 服务器。
- **接口** - 选择 **wifi** 接口。
- **地址池 (Address Pool)** - 输入 DHCP 客户端的地址池。例如，如果对无线接口使用的是示例地址，则池是 192.168.10.2-192.168.10.254。该池必须与接口的 IP 地址位于同一子网中，并且池中不能包含接口地址或广播地址。

f) 点击**确定**。

步骤 5 点击菜单中的“部署”按钮，然后点击**立即部署**按钮，以部署对设备的更改。

请稍候，直到部署完成后再继续。

步骤 6 配置无线接入点。
无线接入点从为无线接口定义的 DHCP 池中获取其地址。它应获取池中的第一个地址。如果使用了示例地址，则地址为 192.168.10.2。（如果第一个地址不起作用，请尝试池中的下一个地址。）

a) 使用新的浏览器窗口访问无线接入点 IP 地址，例如 **http://192.168.10.2**。
此时将打开无线接入点的 Web 界面。

您必须位于内部网络或可转至该地址的网络，才能打开该地址。

b) 使用用户名 **cisco** 和密码 **Cisco** 进行登录。
c) 在左侧依次点击**简单设置** > **网络配置**。
d) 在**无线电配置**区域，针对**无线电 2.4Ghz** 和**无线电 5Ghz** 部分至少设置以下参数，然后针对每个部分点击**应用**。

- **SSID** - 服务集标识符。这是指无线网络的名称。用户在为其 Wi-Fi 连接选择无线网络时，会看到此名称。
- **Beacon 中的广播 SSID (Broadcast SSID in Beacon)** - 选择此选项。
- **通用管理模式：禁用**。
- **安全 (Security)** - 选择要使用的安全选项。

步骤 7 在无线接入点 Web 界面中，启用无线电。

a) 点击左侧的**摘要 (Summary)**，然后在**网络接口 (Network Interfaces)** 下的主页上点击 2.4 Ghz 无线电的链接。
b) 单击 **Settings**（设置）选项卡。
c) 对于 **Enable Radio** 设置，点击**启用 (Enable)** 单选按钮，然后点击页面底部的**应用 (Apply)**。
d) 针对 5 Ghz 无线电重复该过程。

初始设置之前的默认配置

在使用本地管理器（Firepower 设备管理器）初始配置 Firepower 威胁防御 设备之前，设备包括以下默认配置。

此配置假定您通过内部接口打开Firepower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。有关各个设备型号的默认内部和外部接口，请参阅下表。或者，您也可以将计算机插入管理/诊断物理接口，并通过DHCP获取地址。有关用于在浏览器中打开 Firepower 设备管理器的默认内部和管理 IP 地址，请参阅配置设置表。

默认配置设置

设置	默认	是否可在初始配置期间更改？
Admin 用户的密码。	Admin123	是。必须更改默认密码。
管理 IP 地址。	192.168.45.45	编号
管理网关。	设备上的数据接口。通常外部接口即是连通到互联网的路由。此网关仅适用于从设备传出的流量。	编号
管理接口上的 DHCP 服务器。	启用，使用地址池 192.168.45.46 - 192.168.45.254。	编号
管理接口的 DNS 服务器。	OpenDNS 公共 DNS 服务器，208.67.220.220 和 208.67.222.222。	是

设置	默认	是否可在初始配置期间更改？
内部接口 IP 地址。	192.168.1.1/24	编号
内部客户端的 DHCP 服务器。	在内部接口上运行，地址池为 192.168.1.5 - 192.168.1.254。	编号
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。	通过DHCP从互联网服务提供商 (ISP) 或上游路由器获取。	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。您必须从桥接组中删除一个接口，然后才能将其配置为非交换接口。

Firepower 威胁防御设备	外部接口	内部接口
ASA 5506-X ASA 5506H-X ASA 5506W-X	GigabitEthernet1/1	BVI1，其中包含除外部接口外的所有其他数据接口，对于 5506W-X，则是无线接口 GigabitEthernet1/9。
ASA 5508-X ASA 5516-X	GigabitEthernet1/1	GigabitEthernet1/2
ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	GigabitEthernet0/0	GigabitEthernet0/1

进行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明示选择的项目，或者它们是否基于您的其他选项而定义。请验证任何“默示”配置，如果它们不符合您的需求，对其进行编辑。

设置	配置	明示、默示或默认配置
Admin 用户的密码。	您输入的任何信息。	明示。
管理 IP 地址。	192.168.45.45	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。管理网关仅适用于来自设备的流量。	默认值。
管理接口上的 DHCP 服务器。	启用，使用地址池 192.168.45.46 - 192.168.45.254。	默认值。
管理接口的 DNS 服务器。	您输入的任何信息。	明示。
管理主机名。	**firepower** 或您输入的任何信息。	明示。
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。对于具有内部桥接组的型号，这涵盖了内部桥接组的所有成员接口。不允许 SSH 连接。允许 IPv4 和 IPv6 连接。	默示。
系统时间。	您所选的时区和 NTP 服务器。	明示。
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。	明示。
内部接口 IP 地址。	192.168.1.1/24	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 192.168.1.5 - 192.168.1.254。	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。	明示，但属于间接配置。

设置	配置	明示、默示或默认配置
数据接口配置。	（没有内部桥接组的型号。）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禁用。 （具有内部桥接组的型号。）除外部接口之外的所有数据接口（如 GigabitEthernet1/2）均启用，并且作为内部桥接组的一部分。您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。	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。请参阅初始设置之前的默认配置，第 20 页。 通过 DHCP 获取 IP 地址，或者是输入的静态地址(IPv4、IPv6 或两者)。	接口是默认值。 寻址为显式的。
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“任意”地址创建网络对象，即为 IPv4 创建 0.0.0.0/0，为 Ipv6 创建 ::/0。	默示。
安全区。	**inside_zone**，包含内部接口。对于具有内部桥接组的型号，该区域包含内部桥接组接口的所有成员。 **outside_zone**，包含外部接口。 （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）。	默示。
访问控制策略。	信任从 inside_zone 到 outside_zone 之间所有流量的规则。这样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。 对于具有内部桥接组的型号，第二个规则信任 inside_zone 中的接口之间的所有流量。这可在不进行检查的情况下，允许您的内部网络上的用户之间的所有流量。 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。	默示。

设置	配置	明示、默示或默认配置
NAT	（没有内部桥接组的型号。）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。 （具有内部桥接组的型号。）对于内部桥接组的每个成员，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。这些将显示在 NAT 规则表中，稍后您可以视需要进行编辑。 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。	默示。

配置基本信息

以下主题介绍配置设备的基本方法。

配置设备

首次登录 Firepower 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**。

过程

步骤 1 点击**设备**以访问**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 26 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。

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 (Interface)** - 除了管理接口外，至少应配置两个数据接口。请参阅接口，第 93 页。
- **路由 (Routing)** - 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 109 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，第 271 页。
- **系统设置 (System Settings)** - 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 261 页。
- **智能许可证 (Smart License)** - 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。请参阅给系统授权许可，第 57 页。
- **备份和恢复 (Backup and Restore)** - 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 275 页。
- **故障排除 (Troubleshoot)** - 在请求思科技术支持中心时生成故障排除文件。请参阅创建故障排除文件，第 286 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 239 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 25 页。

接下来的操作

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 (Objects)** 配置这些策略中所需的对象。

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。另外，由于某些更改需要检测引擎重新启动，重新启动期间会丢弃流量，因此请考虑在潜在中断造成的影响最低时部署更改。

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，使用 Firepower 设备管理器的 Firepower 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，请参阅重启检测引擎的配置更改，第 26 页。

过程

步骤 1 点击网页右上角的**部署更改**图标。
若有更改未部署，该图标将以圆点高亮显示。

此时将打开“部署摘要”(Deployment Summary) 页面。在部署启动并完成后，该窗口将显示先前部署的列表及更改摘要（“已修改对象”），以及每项部署的状态。

如果该图标未高亮显示，仍然可以点击它来查看先前部署作业的结果。

步骤 2 点击**立即部署 (Deploy Now)**。

重启检测引擎的配置更改

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

任何部署都会重启检测引擎。

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。

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**页面和**监控** > **系统**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“inside”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。如果没有名为“inside”的接口，则不会将任何端口标记为内部端口。
- 外部网络 - 仅对名为“outside”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**。另请参阅排除 NTP 故障，第 283 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。

过程

步骤 1 点击主菜单中的**任务列表**。

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**或**失败**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**可清空已结束的所有任务的列表。

第 2 章

Firepower 威胁防御的使用案例

以下主题主要介绍您可能希望用 Firepower 设备管理器通过 Firepower 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 Firepower 设备管理器的监控功能来分析网络流量。Firepower 设备管理器报告可帮助您解答以下问题：

- 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流量信息，包括策略、目标和安全区。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。

以下步骤介绍了如何设置Firepower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 通过此步骤无法了解用户所访问站点的网站类别和信誉，因此在 Web 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（例如金融服务），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 42 页。

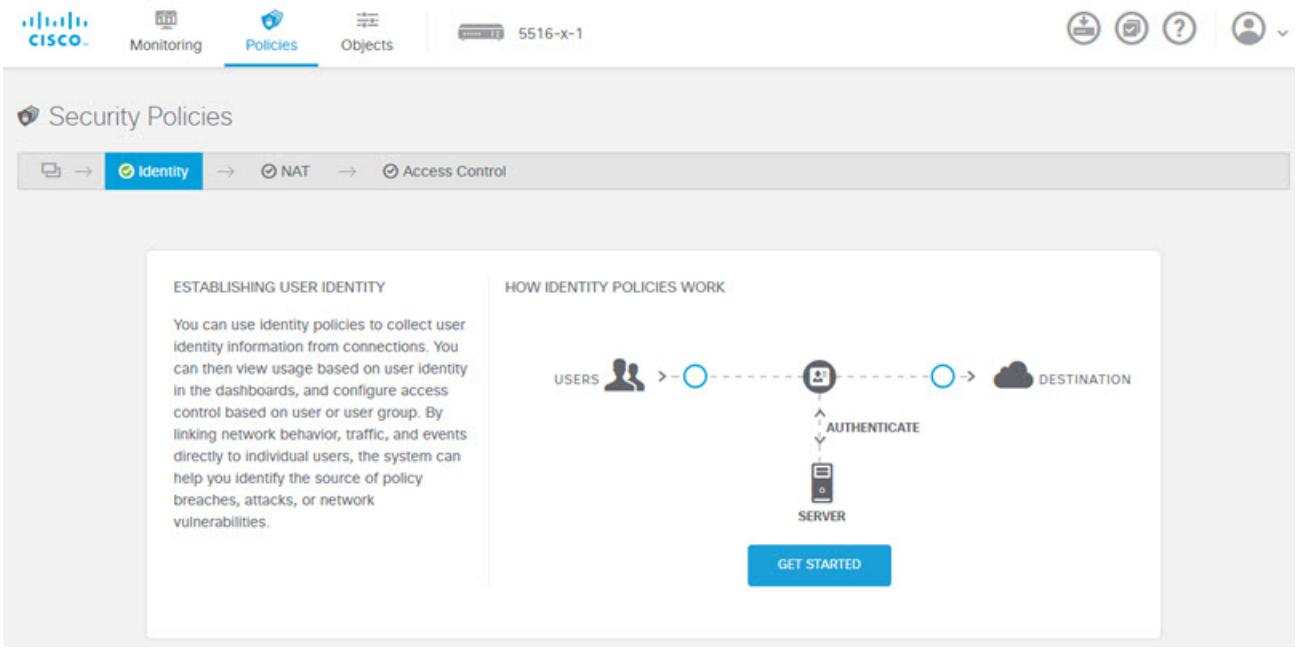
过程

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。

只有用户使用支持 HTTP 连接的 Web 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。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**开始**按钮，以启动配置所需元素的向导。

c) 标识您的 Active Directory 服务器。
填写以下信息。

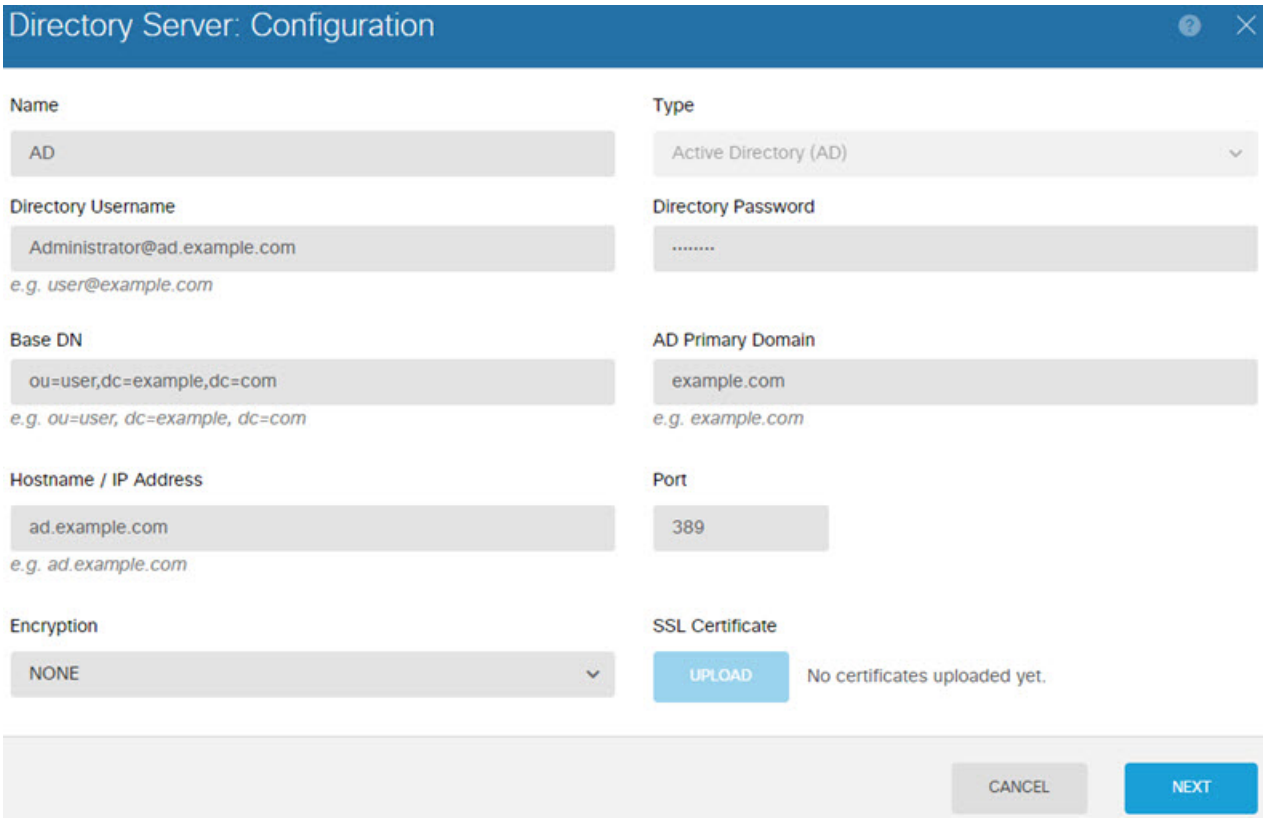
- **名称 (Name)** - 目录领域的名称。
- **类型 (Type)** - 目录服务器的类型。Active Directory 是唯一支持的类型，所以无法更改此字段。
- **目录用户名 (Directory Username)**、**目录密码 (Directory Password)** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。例如 admin@ad.example.com。
- **基准 DN (Base DN)** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如 dc=example,dc=com。有关查找基准 DN 的信息，请参阅确定目录基准标识名，第 117 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 (Hostname/IP Address)** - 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 (Port)** - 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 (None)**，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。

  LDAPS 需要基于 SSL 的 LDAP。使用端口 636。

- **SSL 证书 (SSL Certificate)** - 如果选择加密方法，请上传 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。



d) 点击**下一步 (Next)**。

e) 配置主动身份验证强制网络门户。
最简单的方法是按原样保留所有字段，然后点击**保存 (Save)**。您可以配置用于主动身份验证的默认端口，用户将获得一个自签名证书，他们需要该证书来获取信任，以便提供其用户名和密码。请告知用户此类预期会发生的事项，并且他们应接受该证书。

但是，最好是上传一个受他们的浏览器信任的证书。如果您有这样的证书，请填写以下字段以使用证书。

- **服务器证书 (Server Certificate)** - 在主动身份验证期间提供给用户的 CA 证书。该证书必须为 PEM 或 DER 格式的 X509 证书。粘贴证书，或点击**上传证书**并选择证书文件。在用户身份验证期间默认提供自签证书。
- **证书密钥 (Certificate Key)** - 服务器证书的密钥。粘贴密钥，或点击**上传密钥**并选择密钥文件。
- **端口 (Port)** - 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 1025-65535 的范围内。

f) 点击**保存 (Save)**。
安装向导随即完成。现在，创建一个身份规则以要求进行主动身份验证。

g) 点击**创建身份规则**按钮或 + 按钮。

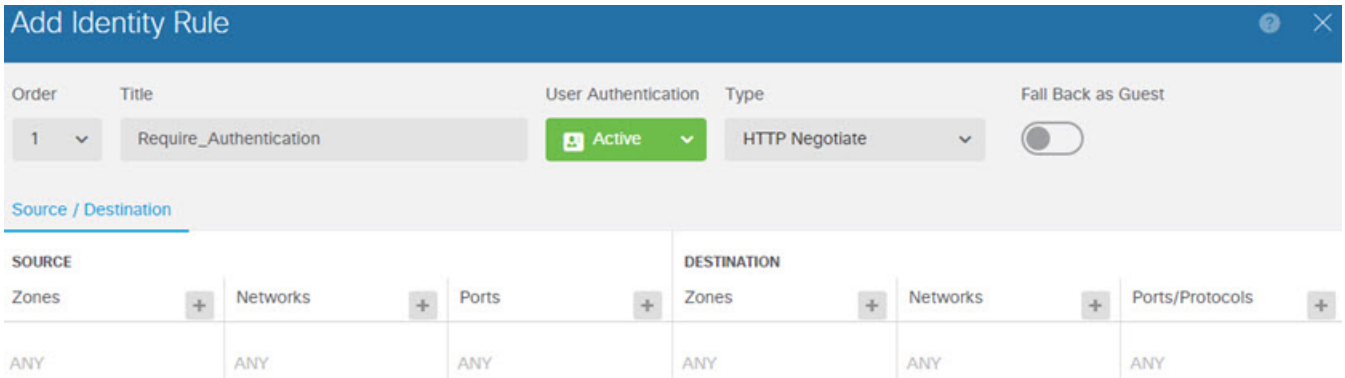
h) 填写身份规则属性。
假定您要求对每个人进行身份验证，可以使用以下设置：

- **名称 (Name)** - 您所选的任何信息，例如 Require_Authentication。
- **用户身份验证** - 应已选中**主动**；保持不变。
- **类型 (Type)** - 选择 **HTTP 协商 (HTTP Negotiate)**。这样则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 对于 HTTP Basic、HTTP Response Page 和 NTLM 身份验证方法，用户将使用该接口的 IP 地址重定向至强制网络门户。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。如果想要使用 HTTP Negotiate，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。 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。

- **源/目标 (Source/Destination)** - 让所有字段保留默认值“任意”(Any)。

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/目的条件匹配并不重要。有关身份策略属性的详细信息，请参阅配置身份规则，第 121 页。

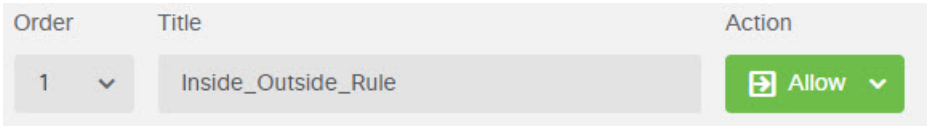


i) 点击**确定**以添加规则。
如果查看窗口的右上角，可以看到**部署**图标现在带有一个圆点，表示存在未部署的更改。在用户界面进行更改还不足以获取在设备上配置的更改，还必须部署更改。因此，您可以执行一组相关更改，然后再部署它们，这样就不会出现仅在设备上配置了部分更改的情况。在此步骤后面，将要部署更改。

步骤 2 将 Inside_Outside_Rule 访问控制规则上的操作更改为**允许 (Allow)**。
Inside_Outside_Rule 访问规则创建为信任规则。但由于不检测到受信任的流量，所以在匹配条件的流量不含应用或区域、IP 地址和端口之外的其他条件时，系统则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 （ASA 5506-X 型号。）还要考虑将 Inside_Inside_Rule 从“信任”更改为“允许”。此规则涵盖了内部接口之间的流量。

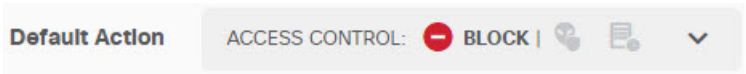
a) 点击**策略**页面上的**访问控制**。
b) 将鼠标悬停在 Inside_Outside_Rule 行右侧的**操作**单元格上将显示编辑和删除图标，然后点击编辑图标 () 以打开该规则。
c) 针对**操作**选择**允许**。



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。

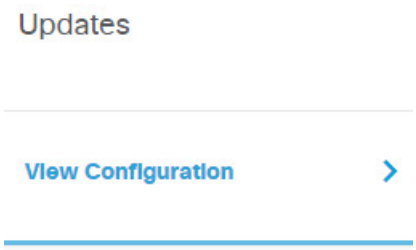
a) 点击访问控制策略页面底部默认操作的任意位置。



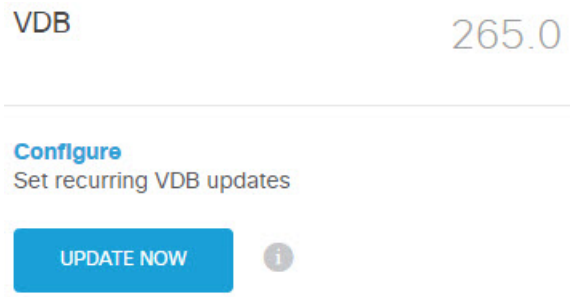
b) 选择**选择日志操作** > **连接开始和结束时**。
c) 点击**确定 (OK)**。

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**。

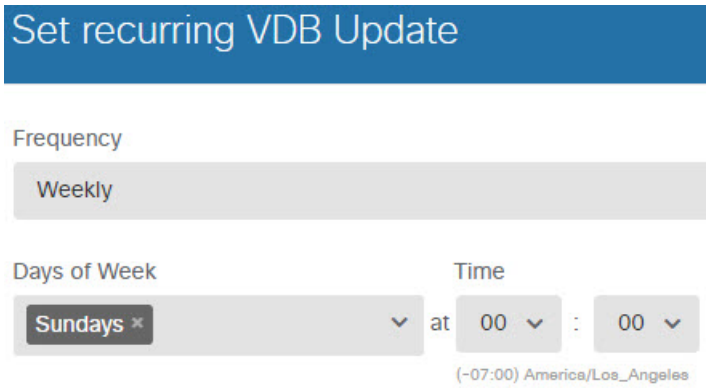


c) 点击 VDB 组中的**配置**。



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。

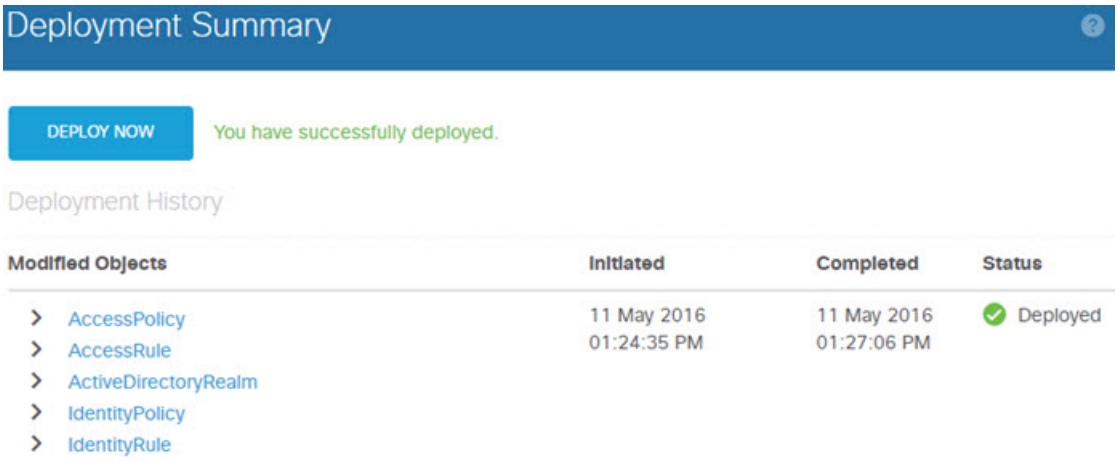


e) 点击**保存 (Save)**。

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，并等待部署完成。
部署摘要将指出，您已成功部署更改，而且作业的任务状态应为“已部署”(Deployed)。



接下来的操作

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 Web 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。

思科通过 Firepower 系统提供多种入侵策略。这些策略由思科 Talos 安全智能和研究小组设计，他们设定了入侵和预处理器规则的状态和高级设置。

过程

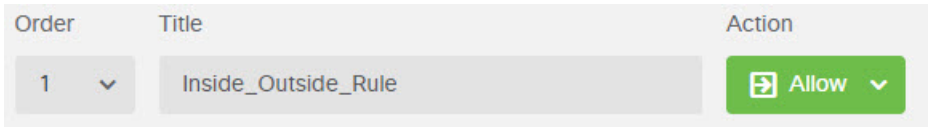
步骤 1 如果尚未启用**威胁**许可证，请启用该许可证。
只有启用威胁许可证，才能使用入侵策略。如果您当前使用的是评估许可证，将启用该许可证的评估版本。如果已注册设备，则必须购买所需的许可证，并将其添加到您在 Cisco.com 的智能软件管理器帐户。

a) 点击**设备**。
b) 点击“智能许可证”组中的**查看配置**。

c) 点击**威胁**组中的**启用**。
系统则会将该许可证注册到您的帐户，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“禁用”(Disable) 按钮。

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。对于 ASA 5506-X 型号，您可能还需要将其添加到 Inside_Inside_Rule。

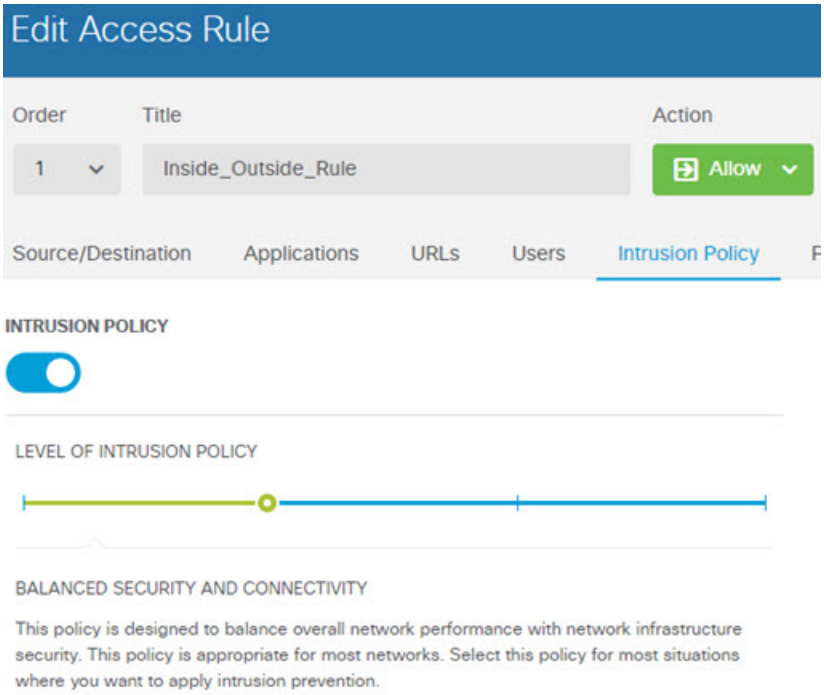
a) 在主菜单中点击**策略**。
确保系统显示**访问控制**策略。
b) 将鼠标悬停在 Inside_Outside_Rule 行右侧的**操作**单元格上将显示编辑和删除图标，然后点击编辑图标 ( ) 以打开该规则。
c) 如果尚未针对**操作**选择**允许**，请进行此选择。



d) 点击**入侵策略**选项卡。
e) 点击**入侵策略**旋钮以启用它，然后在滑块中选择入侵策略的级别。

策略将按安全性由低到高列出。对于大多数网络，合适的策略是**平衡安全性和连接**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**连接优先于安全性**以放宽策略。

如果您需要积极关注安全性，请尝试**安全性优先于连接**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。



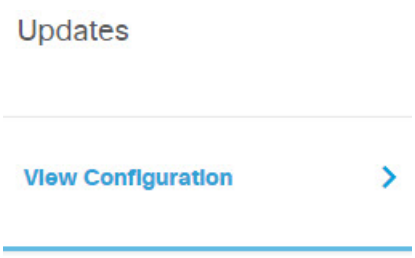
f) 点击**确定**以保存更改。

步骤 3 设置入侵规则数据库的更新计划。

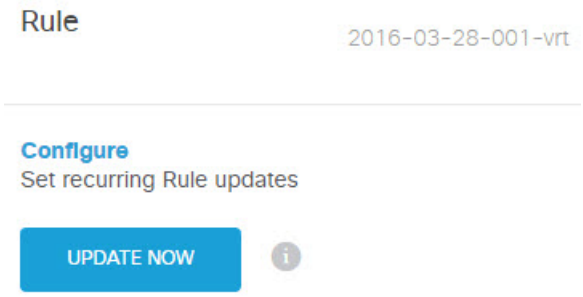
思科会定期发布入侵规则数据库更新，入侵策略使用入侵规则数据库来确定是否应丢弃连接。您应定期更新规则数据库。您可以手动下载更新，也可以设置定期更新计划。以下步骤介绍了如何设置计划。默认情况下，数据库更新处于禁用状态，所以您需要采取措施来获取更新的规则。

a) 点击**设备**。

b) 点击“更新”组中的**查看配置**。

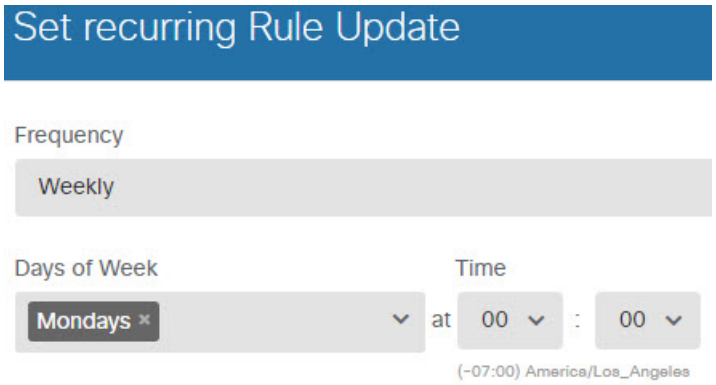


c) 点击“规则”组中的**配置**。



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 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，并等待部署完成。
部署摘要将指出，您已成功部署更改，而且作业的任务状态应为“已部署”(Deployed)。

接下来的操作

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。

如何阻止恶意软件

用户不断面临着从互联网站点或其他通信方法（例如邮件）获得恶意软件的风险。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。实际安全性意味着，逐个查看每个对象，而不只是初始请求。

使用文件策略，借助适用于 Firepower 的高级恶意软件保护（适用于 Firepower 的 AMP）检测恶意软件。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。

适用于 Firepower 的 AMP 使用 AMP 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 AMP 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 AMP 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 AMP 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**恶意软件**许可证，请启用该许可证。

只有启用恶意软件许可证，才能使用文件策略执行恶意软件控制。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 的智能软件管理器帐户。

a) 点击**设备**。

b) 点击“智能许可证”组中的**查看配置**。

c) 点击**恶意软件**组中的**启用**。

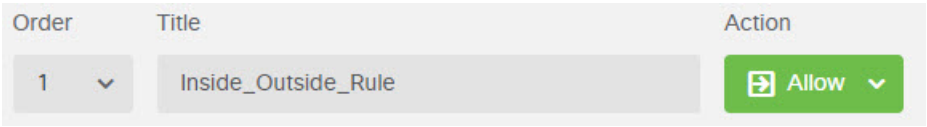
系统则会将该许可证注册到您的帐户，或激活相应的评估许可证。该组应指示许可证已启用，且按钮将改为“禁用”(Disable) 按钮。

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。对于 ASA 5506-X 型号，您可能还希望将其添加到 Inside_Inside_Rule。

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。

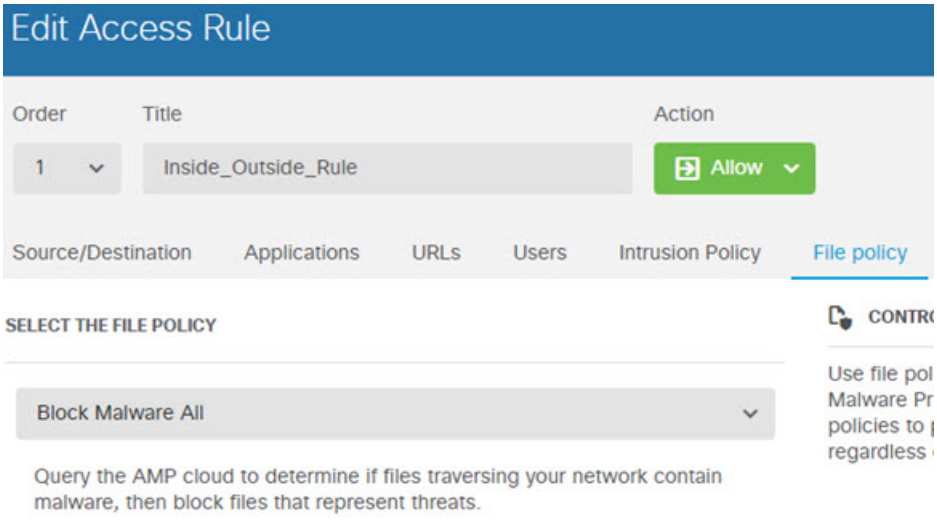


d) 点击**文件策略**选项卡。

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 (Block Malware All)** 或**全部执行云查找 (Cloud Lookup All)**，前者将丢弃被视为恶意软件的任何文件，后者将查询 AMP 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。

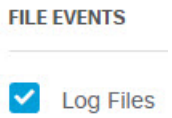
使用其他策略也可以阻止恶意软件。这些策略搭配文件控制，可阻止上传 Microsoft Office（或 Office）和 PDF 文档。也就是说，除了阻止恶意软件，这些策略还可阻止用户向其他网络发送这些类型的文件。如果它们符合您的需求，您可以选择这些策略。

对于本示例，请选择**阻止所有恶意软件 (Block Malware All)**。



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，并等待部署完成。
部署摘要将指出，您已成功部署更改，而且作业的任务状态应为“已部署”(Deployed)。

接下来的操作

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政策。可接受使用政策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 流量。

您可以使用URL过滤来定义访问策略的可接受使用政策。您可以基于各种类别（例如赌博）过滤，这样则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 Web 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。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。

以下步骤介绍了如何使用URL过滤实施可接受使用政策。在本例中，我们将阻止某些类别的任何信誉的站点、高风险社交网络站点和未分类站点 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 Web 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 的智能软件管理器帐户。

a) 点击**设备**。
b) 点击“智能许可证”组中的**查看配置**。

c) 点击 **URL 许可证**组中的**启用**。
系统则会将该许可证注册到您的帐户，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“禁用”(Disable) 按钮。

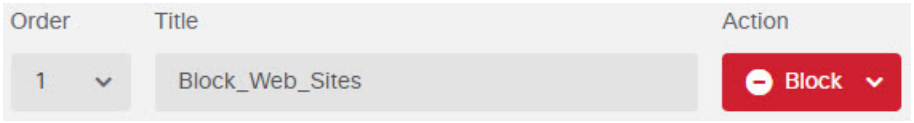
步骤 2 创建 URL 过滤访问控制规则。
您可能想要先查看用户访问的站点的类别，再实施阻止规则。对于这种情况，您可以创建一项规则，对可接受的类别（例如金融服务）执行“允许”(Allow) 操作。由于必须检测所有网络连接来确定 URL 是否属于此类别，所以即便是非金融服务站点，您也会收到相关的类别信息。

但是，可能存在您已知要阻止的网络类别。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。

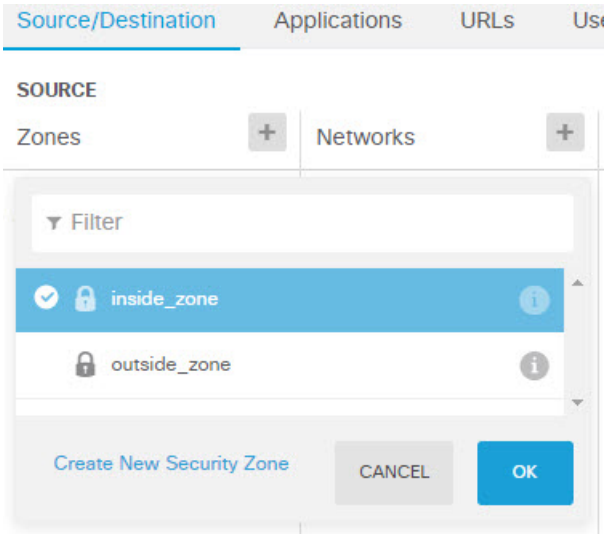
a) 在主菜单中点击**策略**。
确保系统显示**访问控制**策略。

b) 点击 + 添加新规则。
c) 配置顺序、标题和操作。

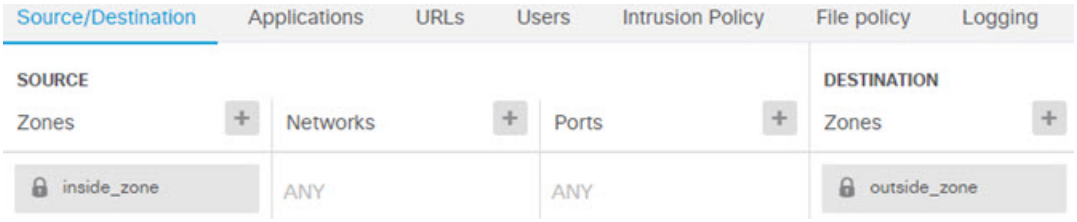
- **顺序 (Order)** - 默认将新规则添加到访问控制策略的末尾。但是，您必须将此规则放在符合相同源/目标及其他条件的任何规则之前（上方），否则该规则将无法获得匹配（一个连接仅匹配一个规则，即该规则是连接在表中匹配的第一个规则）。对于该规则，我们将使用与初始设备配置期间创建的 Inside_Outside_Rule 相同的源/目标。您可能也已经创建了其他规则。为了最大限度地提高访问控制效率，最好是尽早设置特定规则，以确保快速决定允许还是丢弃某个连接。对于此示例，请选择 **1** 作为规则顺序。
- **标题 (Title)** - 为该规则指定一个有意义的名称，例如 Block_Web_Sites。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



d) 在**源/目的**选项卡上，点击 + 以打开**源** > **区域**，然后选择 **inside_zone**，再在区域对话框中点击**确定**。
添加任何标准的方式与此相同。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。

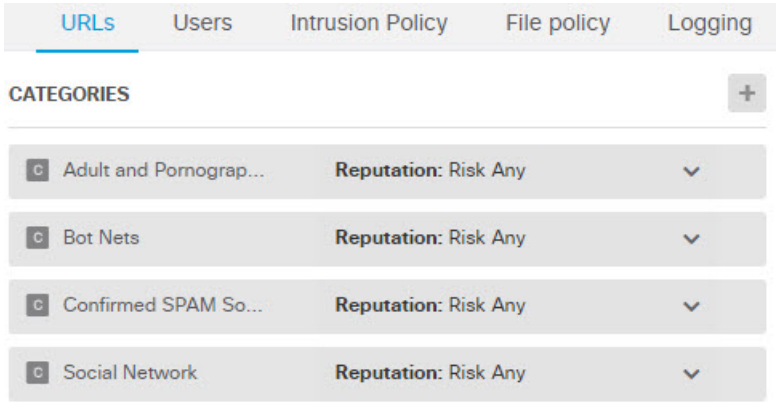


e) 按照相同的方法，为**目的** > **区域**选择 **outside_zone**。

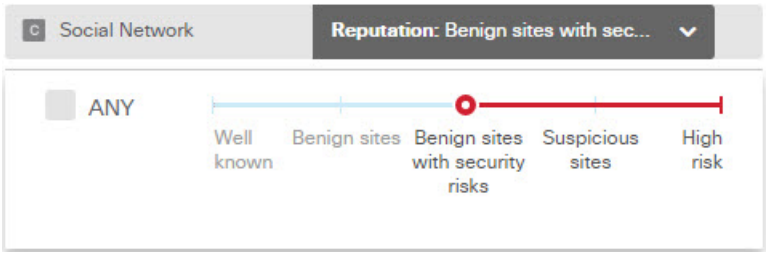


f) 点击 **URL** 选项卡。

g) 点击**类别**的 +，然后选择要完全或部分阻止的类别。
在本例中，选择“成人和色情”(Adult and Pornography)、“僵尸网络”(Bot Nets)、“确认的垃圾邮件源”(Confirmed SPAM Sources)和“社交网络”(Social Network)。您可能还希望阻止其他类别。



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**存在安全风险的良性站点**。点击远离滑块的位置将其关闭。

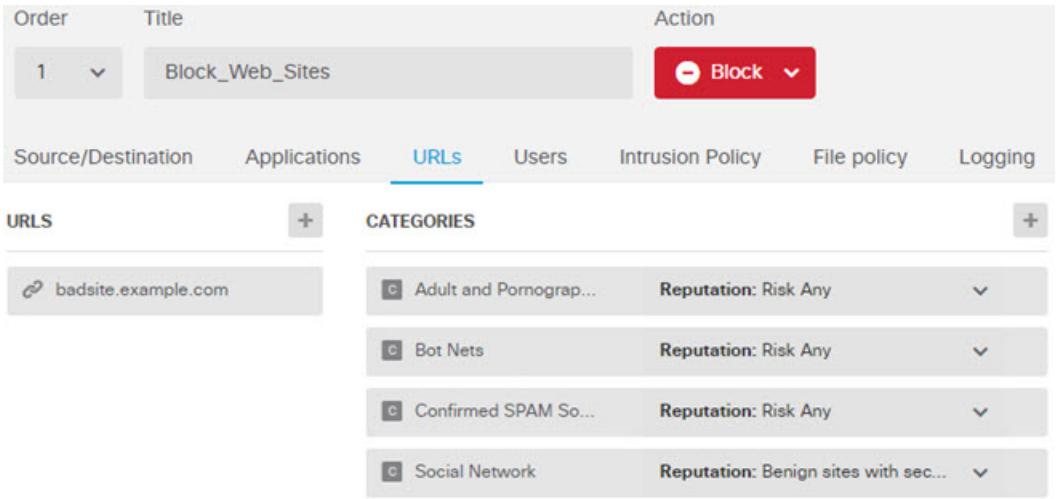


信誉滑块的左侧指示要允许的站点，右侧是要阻止的站点。在这种情况下，只会阻止信誉为“可疑站点”和属于“高风险”范围的社交网站。因此，您的用户应该能够访问风险较低的常用社交网站。

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**，然后依次点击**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。

另外，还可以选择将未分类的URL发送给思科进行分析。因此，如果用户连接至没有类别和信誉的新站点，思科可对其进行评估、分类、指定信誉，并将其加入此后的更新中。然后，后续访问该站点时，即可根据新信息允许或阻止该站点。

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) 选择**针对未知 URL 查询思科 CSI (Query Cisco CSI for Unknown URLs)**。
d) 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，并等待部署完成。
部署摘要将指出，您已成功部署更改，而且作业的任务状态应为“已部署”(Deployed)。

接下来的操作

这时，监控控制面板和事件应开始显示 Web 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。

如何控制应用使用情况

Web 已成为企业交付应用而普遍使用的平台，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。

Firepower 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关联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 29 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”(Applications) 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

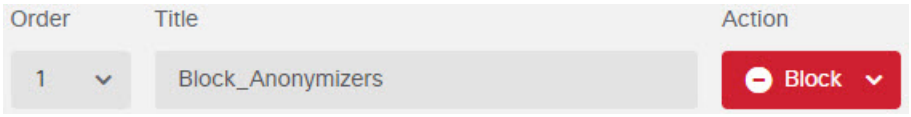
步骤 1 创建基于应用的访问控制规则。

a) 在主菜单中点击**策略**。
确保系统显示**访问控制**策略。

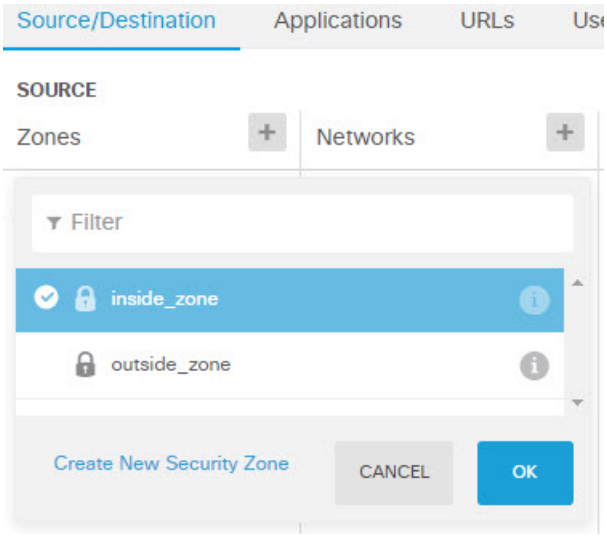
b) 点击 + 添加新规则。

c) 配置顺序、标题和操作。

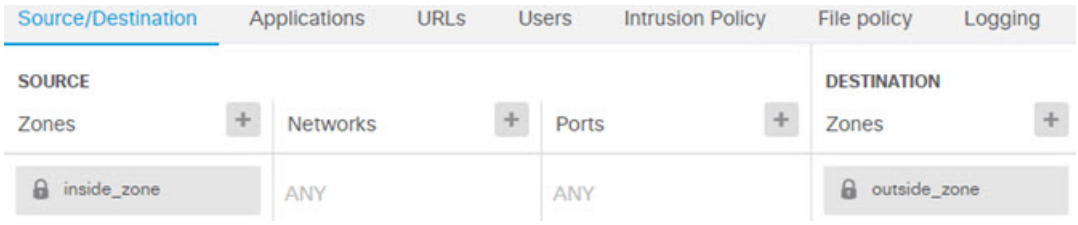
- **顺序 (Order)** - 默认将新规则添加到访问控制策略的末尾。但是，您必须将此规则放在符合相同源/目标及其他条件的任何规则之前（上方），否则该规则将无法获得匹配（一个连接仅匹配一个规则，即该规则是连接在表中匹配的第一个规则）。对于该规则，我们将使用与初始设备配置期间创建的 Inside_Outside_Rule 相同的源/目标。您可能也已经创建了其他规则。为了最大限度地提高访问控制效率，最好是尽早设置特定规则，以确保快速决定允许还是丢弃某个连接。对于此示例，请选择 **1** 作为规则顺序。
- **标题 (Title)** - 为该规则指定一个有意义的名称，例如 Block_Anonymizers。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



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



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



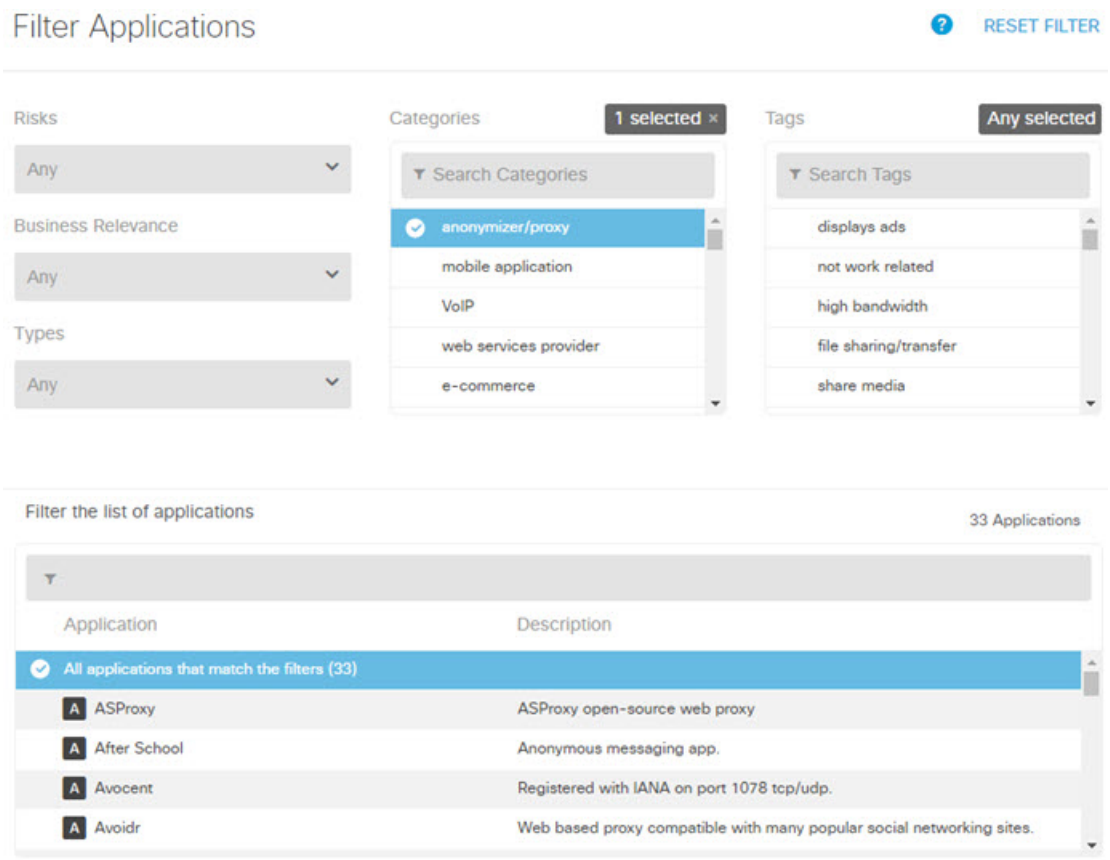
f) 点击 **Applications**（**应用**）选项卡。

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”(Application Filters) 列表中选择它们，但也可以直接在访问控制规则中指定标准，再选择将该标准另存为过滤器对象。除非为单个应用写入规则，否则使用“高级过滤器”(Advanced Filter) 对话框查找应用和构建适当的标准更方便。

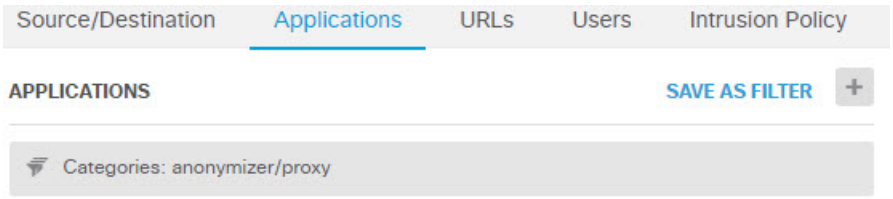
在选择标准时，对话框底部的“应用”(Application) 列表将准确显示符合标准的应用。您要编写的规则将应用到这些应用中。

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，在撰写本文时，Facebook 和 TFPT 则属于风险极高类别。而大多数组织不想阻止这些应用。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”(Categories) 列表中选择“匿名程序/代理”(anonymizers/proxies)。



h) 在“高级过滤器”对话框中点击**添加**。
“应用”(Applications) 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获取有关此规则阻止的所有连接的信息。

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，并等待部署完成。

部署摘要将指出，您已成功部署更改，而且作业的任务状态应为“已部署”(Deployed)。

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。

应用控制面板也将显示这些结果。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，则该应用可以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桥接组的一部分。如果它当前是桥接组成员，则必须首先将其从桥接组中删除，然后再执行此步骤。

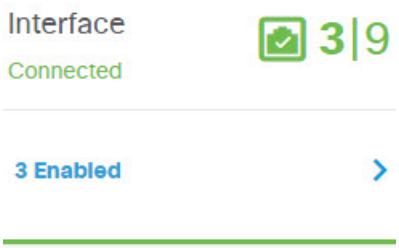
开始之前

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。

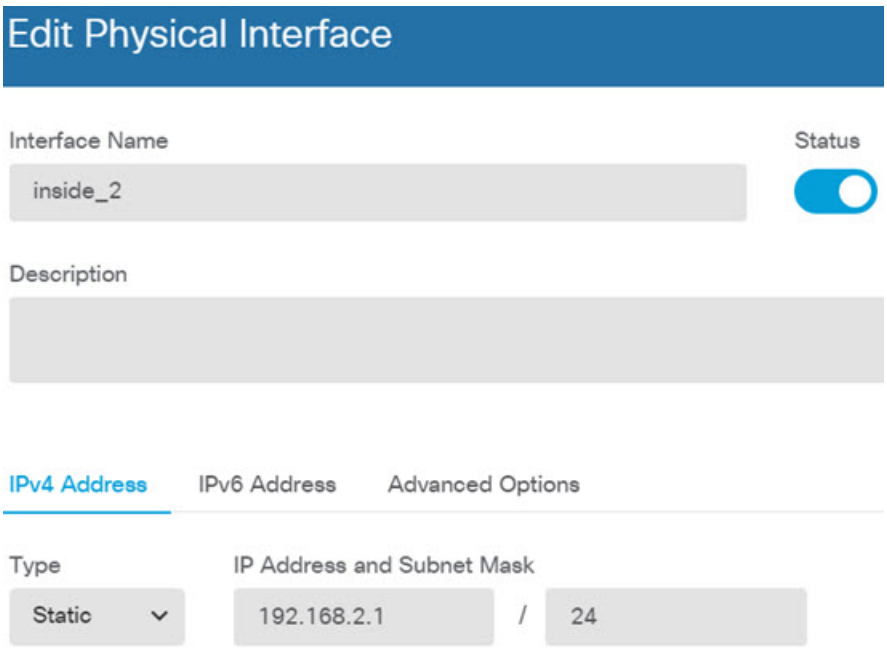
a) 点击**设备**。
b) 点击**接口**组中指示已启用接口数量的链接。
这里有设备上已启用接口数量相比总接口数量（视型号而异）的摘要。在本例中，启用了 9 个接口中的 3 个接口。



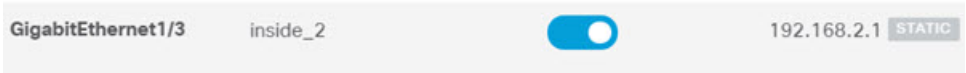
c) 将鼠标悬停在您连线的接口行右侧的**操作**单元格上方，然后点击编辑图标 ( )。

d) 配置基本接口属性。

- **名称 (Name)** - 接口的名称。在本例中为 **inside_2**。
- **状态 (Status)** - 点击状态旋钮可启用该接口。
- **IPv4 地址**选项卡 - 针对**类型**选择**静态**，然后输入 **192.168.2.1/24**。



e) 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**。

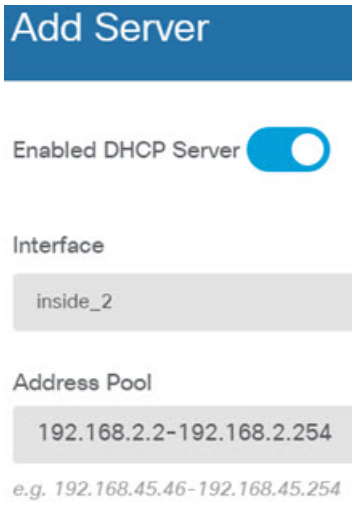
b) 点击**系统设置** > **DHCP 服务器**。

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 (Enable DHCP Server)** - 点击此旋钮可启用该服务器。
- **接口 (Interface)** - 选择您提供 DHCP 服务所基于的接口。在本例中，选择 inside_2。
- **地址池 (Address Pool)** - 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

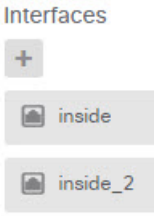
步骤 3 将该接口添加到内部安全区。
要在接口上编写策略，该接口必须属于安全区。您需要针对安全区编写策略。因此，您在区域中添加和删除接口时，会自动更改应用于接口的策略。

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。

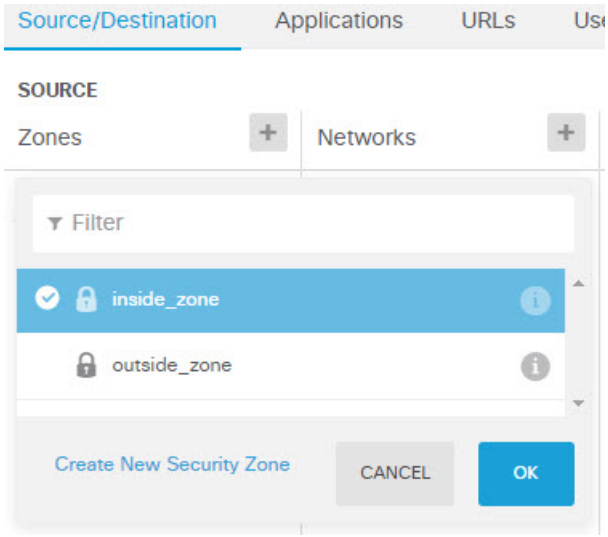
a) 在主菜单中点击**策略**。
确保系统显示**访问控制**策略。

b) 点击 + 添加新规则。

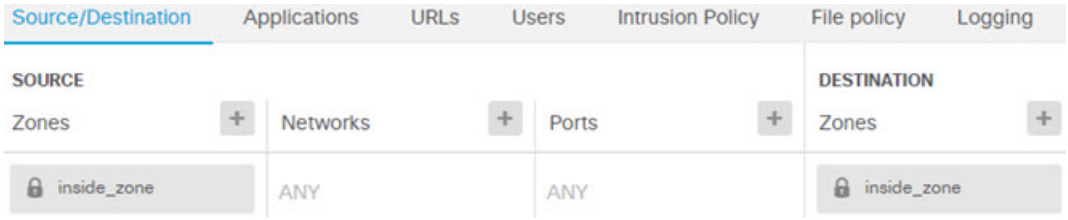
c) 配置顺序、标题和操作。

- **顺序 (Order)** - 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/目标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（一个连接仅匹配一个规则，即该规则是连接在表中匹配的第一个规则）。对于该规则，我们将使用唯一“源/目标”(Source/Destination) 标准，所以可以将该规则添加到列表的末尾。
- **标题 (Title)** - 为该规则指定一个有意义的名称，例如 Allow_Inside_Inside。
- **操作 (Action)** - 选择**允许 (Allow)**。

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



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“平衡安全性和连接”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 (Access Control)** - Inside_Outside_Rule 应允许新子网和外部网络之间的所有流量。如果您按照前面使用案例执行了操作，该策略则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 (Identity)** - 没有默认的身份策略。但是，如果您按照前面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，并等待部署完成。
部署摘要将指出，您已成功部署更改，而且作业的任务状态应为“已部署”(Deployed)。

接下来的操作

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。

第 3 章

给系统授权许可

以下主题介绍如何授权许可给 Firepower 威胁防御 设备。

Firepower 系统的智能许可

通过思科智能许可，您可以集中购买和管理许可证池。与产品授权密钥 (PAK) 许可证不同，智能许可证未绑定到特定序列号或许可证密钥。通过智能许可，您可以直观地评估许可证使用情况和需求。

此外，智能许可不会阻止您使用尚未购买的产品功能。只要注册到思科智能软件管理器，然后再购买一个许可证，立即就能使用该许可证。这样即可部署和使用某项功能，同时避免采购订单审批造成的延迟。

思科智能软件管理器

在为 Firepower 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，可以为组织创建一个主帐户。

默认情况下，许可证分配给主帐户下的默认虚拟帐户。作为帐户管理员，您可以创建其他虚拟帐户；例如，为区域、部门或子公司创建帐户。通过多个虚拟帐户，可帮助您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；只有该虚拟账户的设备可以使用分配给该帐户的许可证。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 Firepower 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 Firepower 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30天进行一次，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 Firepower 威胁防御 设备可用的许可证。

购买 Firepower 威胁防御 设备会自动附带基本许可证。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（自动包含）	永久	可选期限的许可证中未包括的所有功能。 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。
威胁	基于期限	**入侵检测和防御** - 入侵策略用于分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。 **文件控制** - 文件策略用于检测和选择性地阻止用户上传（发送）或下载（接收）特定类型的文件。通过面向 Firepower 的 AMP（需要恶意软件许可证），您可以检查和阻止包含恶意软件的文件。
恶意软件	基于期限	检查恶意软件的文件策略，将思科高级恶意软件保护 (AMP) 与适用于 Firepower 的 AMP（基于网络的高级恶意软件保护）和 AMP Threat Grid 结合使用。 文件策略可以检测和阻止通过网络传输的文件中的恶意软件。

许可证	持续时间	授予的功能
URL 过滤	基于期限	基于类别和信誉的 URL 过滤。 您可以对单个 URL 执行 URL 过滤，而不使用此许可证。

可选许可证过期或被禁用的影响

如果可选许可证过期，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帐户，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：

- **恶意软件许可证** - 系统会停止查询 AMP 云，还会停止确认从 AMP 云发送的追溯性事件。如果现有访问控制策略包括的文件策略会应用恶意软件检测，则无法重新部署现有访问控制策略。请注意，在禁用恶意软件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。
- **威胁** - 系统将不再应用入侵或文件控制策略。您无法重新部署需要该许可证的现有策略。
- **URL 过滤** - 带有 URL 类别条件的访问控制规则会立即停止过滤 URL，且系统不再会下载对 URL 数据的更新。如果现有访问控制策略包括的规则带有基于类别和信誉的 URL 条件，则不能重新部署现有的访问控制策略。

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。获许可的功能可继续工作，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。获许可的功能可继续工作，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、出口管制功能，并可获链接来打开思科智能软件管理器。出口控制的功能控制软件受国家安全、外交政策和反恐怖主义法律和法规约束。

以下步骤概述了如何管理系统的许可证。

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 60 页。

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 61 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 61 页
- 注销设备，第 62 页

注册设备

购买 Firepower 威胁防御 设备会自动附带基本许可证。基本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。

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 点击**申请注册**，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，然后登录您的帐户或创建一个新帐户（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”(Smart License Registration) 对话框的编辑框中。

d) 点击**申请注册 (Request Register)**。

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帐户中将其释放，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。

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。

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，您即可配置和部署该许可证控制的策略。
- **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。

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，则会最多运行 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**。

注销设备

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注销。注销后，您的虚拟帐户将释放与该设备关联的基本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。

注销设备后，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。

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**注销设备**。

步骤 3 如果确实要注销设备，请阅读警告并点击**注销**。

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。

在各个访问规则上启用以下类型的日志记录，可收集可选统计信息并生成事件。

- 连接日志记录 - 在连接结束时撰写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。
- 文件日志记录 - 只有启用文件日志记录，才能收集有关检测到的文件的信息。在访问规则中选择文件策略时将自动启用文件日志记录，但您可以禁用它。

除了您配置的日志记录外，系统会自动记录检测到禁止文件、恶意软件或入侵尝试的大多数连接（连接结束时）。默认操作处理的入侵事件例外。只有对默认操作启用连接日志记录，才能查看这些入侵事件。

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 Block 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。

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。

注释 流量相关控制面板中使用的数据从启用连接或文件日志记录的访问控制规则中收集。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 Web 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**，打开“控制面板”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 Web 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、连接使用的应用、匹配的入侵签名、所访问 URL 的 Web 类别和连接最常访问的目的。
- **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。
- **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 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，必须至少设置一个以 Web 类别为流量匹配标准的访问控制规则。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。
- **策略** - 显示网络流量匹配的排名靠前的访问规则。
- **传入区** - 显示流量进入设备所通过的排名靠前的安全区。
- **传出区** - 显示流量离开设备所通过的排名靠前的安全区。
- **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。
- **系统** - 显示总体系统视图，包括接口及其状态视图（将鼠标悬停在接口上可查看其 IP 地址）、总体系统吞吐量、系统事件摘要信息、CPU 使用情况、内存使用情况和磁盘使用情况。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”(System) 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。这些事件可帮助您解决用户的连接问题。

使用命令行监控更多统计信息

Firepower 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，您可以登录设备 CLI，获取控制面板上未涵盖的方面的其他信息（请参阅 登录命令行界面 (CLI)，第 5 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，包括诸如 **ping** 和 **traceroute** 之类的命令。大多数 **show** 命令随带 **clear** 命令，用于将统计信息重置为 0。

您可以在 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html 中的《*Firepower* 威胁防御的命令参考》中找到与这些命令相关的文档。

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访问规则中生成的事件。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。
- 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 □ 访问规则必须应用文件策略并启用文件日志记录。

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 67 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 68 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 70 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 69 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 (Filter)** 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。

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的统计信息。

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。只有在访问规则中启用连接日志记录，才可查看连接事件。

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。

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。适用于 Firepower 的 AMP 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。

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**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 70 页。

完成后，点击**确定**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运算符或值。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

对于连接事件，与访问控制规则相关联的操作或记录连接的默认操作：

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。

Block

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：

- 某个攻击程序被入侵策略阻止的连接。
- 某个文件被文件策略阻止的连接。

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。

Allowed Connection

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

连接中检测到的应用流量的业务相关性：Very High、High、Medium、Low 或 Very Low。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

展示了应用特征的标准，协助您了解应用功能。

Application Risk

连接中检测到的应用流量相关风险：Very High、High、Medium、Low 或 Very Low。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。

块类型

在访问控制规则中指定的与事件中的流量匹配的块类型：块或交互块。

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相关的业务相关性：Very High、High、Medium、Low 或 Very Low。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

展示了应用特征的标准，协助您了解应用功能。

客户端风险

连接中检测到的客户端流量相关风险：Very High、High、Medium、Low 或 Very Low。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。

Connection

内部产生的流量的唯一 ID。

Connection Blocktype Indicator

在访问控制规则中指定的与事件中的流量匹配的块类型：块或交互块。

Connection Bytes

连接的总字节量。

Connection Time

连接的开始时间。

Connection Timestamp

检测到连接的时间。

Denied Connection

系统是否已拒绝事件的流量通过。

Destination Country and Continent

接收主机的国家/地区和大洲。

目标 IP

接收主机的 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。

Direction

文件传输的方向。

处理结果

文件的处置：

恶意软件

表示 AMP 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。

清洁

表示 AMP 将文件归类为安全。

未知

表示系统查询了 AMP 云，但尚未指定文件处置；换句话说，AMP 云尚未对该文件分类。

不可用

表示系统无法查询 AMP 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 Detect Files 或 Block Files 规则处理了文件，系统不执行 AMP 云查找。

传出接口、传出安全区

连接离开设备所通过的接口和区域。

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）。

File Category

一般类别文件类型，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。

File Event Timestamp

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 **SHA256**

文件的 SHA-256 哈希值。

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，文件大小可以为空。

文件类型

文件类型，例如 HTML 或 MSEXE。

File/Malware Policy

与事件生成相关的文件策略。

Filelog Blocktype Indicator

在文件规则中指定的与事件中的流量匹配的块类型：块或交互块。

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 引用站点

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 Classification

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。

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。

Initiator Country and Continent

发起会话的主机的国家/地区和大洲。只有发起方的 IP 地址可路由，方可用。

发起方 IP

发起会话的主机 IP 地址（以及主机名，如果启用了 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设置为“丢弃并生成事件”(Drop and Generate Events)

入侵策略

启用了生成事件的规则的入侵策略。

IPS Blocktype Indicator

与事件中的流量匹配的入侵规则的操作。

最后数据包

查看会话的最后一个数据包的日期和时间。

MPLS 标签

与触发此入侵事件的数据包相关的多协议标签交换标签。

Malware Blocktype Indicator

在文件规则中指定的与事件中的流量匹配的块类型：块或交互块。

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。

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 标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

事件优先级由思科 Talos 安全智能和研究小组 (Talos) 确定：高、中或低。

协议

连接中使用的传输协议。

Reason

在以下几种情况，记录连接的原因：

Reason	说明
File Block	连接中包含系统禁止传输的文件或恶意软件文件。File Block 原因始终与 Block 操作匹配。
File Monitor	系统在连接中检测到特定类型的文件。
File Resume Allow	文件传输最初被 Block Files 或 Block Malware 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。
File Resume Block	Detect Files 或 Malware Cloud Lookup 文件规则最初允许文件传输。在部署阻止该文件的新访问控制策略后，将自动停止 HTTP 会话。
Intrusion Block	系统阻止或本可阻止在连接中检测到的攻击程序（违反入侵策略）。Intrusion Block 原因与用于阻止攻击程序的 Block 操作和用于本可阻止的攻击程序的 Allow 操作相匹配。
Intrusion Monitor	连接中检测到的攻击程序，为系统检测到，但并未阻止。当触发的入侵规则状态设置为“生成事件”(Generate Events) 时，会发生这种情况。

Receive Times

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。

Responder Country and Continent

响应会话的主机的国家/地区和大洲。只有响应方的 IP 地址可路由，方可用。

响应方 IP

会话响应方的主机 IP 地址（以及主机名，如果启用了 DNS 解析）。

签名

与事件的流量匹配的入侵规则的签名 ID。

Source Country and Continent

发送主机的国家/地区和大洲。只有源 IP 地址可路由，方可用。

源 IP

入侵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。

TCP Flags

在连接中检测到的 TCP 标志。

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）。

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。

User

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 App Business Relevance

与连接中检测到的 Web 应用流量相关的业务相关性：Very High、High、Medium、Low 或 Very Low。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 应用标签

展示了 Web 应用特征的标准，协助您了解 Web 应用功能。

Web App Risk

连接中检测到的 Web 应用流量相关风险：Very High、High、Medium、Low 或 Very Low。连接中检测的各类网络应用都有一个相关风险；该字段显示最高风险。

Web 应用程序

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

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标准。例如，网络对象定义主机和子网地址。

对象允许您定义标准，这样即可在不同策略中重用相同的标准。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

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
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 84 页。
地理定位	安全策略。	地理定位对象定义托管设备（流量的源或目标）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 87 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 242 页。

对象类型	主要用途	说明
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 245 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 81 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 82 页。
安全区	安全策略。	安全区是一组接口。区域将网络划分网段，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 83 页。
系统日志服务器	访问控制规则。 诊断日志记录。 SSL 解密规则。	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 88 页。
URL	访问控制规则。	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 86 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配置它们。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。

以下程序介绍了如何直接通过“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**链接即可。

过程

步骤 1 选择**对象**。
“对象”(Objects) 页面包含一个目录，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标准，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**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。
- 要编辑对象或组，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 输入对象的名称和描述（后者为可选项），并定义对象内容。

网络对象

选择对象**类型**：**网络**或**主机**。然后，输入主机或网络地址。您可以使用以下格式：

- IPv4 主机地址，例如 10.100.10.10。
- 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 主机地址，例如 2001:DB8::0DB8:800:200C:417A 或 2001:DB8:0:0:0DB8:800:200C:417A。
- IPv6 网络（包括前缀），例如 2001:DB8:0:CD30::/60。

网络组

点击 + 按钮，以选择要添加到组中的网络对象。另外，也可以创建新对象。

步骤 4 点击 **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标准，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。

- 要编辑对象或组，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 输入对象的名称和描述（后者为可选项），并定义对象内容。

端口对象

选择**协议 (Protocol)**，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 **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。如果内部接口为桥接组，则此区域包括所有桥接组成员接口，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。
- 要编辑对象，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 输入对象的名称和描述（后者为可选项）。

步骤 4 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 您不能将桥接组接口 (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 5 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关联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。

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”选项卡中添加应用条件后点击**另存为过滤器**链接来创建应用过滤器对象。

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。
- 要编辑对象，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 输入对象的名称和描述（后者为可选项）。

步骤 4 在**应用**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**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**。您可以重复该过程，以添加更多应用或过滤器。

注释 单个过滤器标准中的多个选项具有 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，显示更新中的应用列表仅显示符合标准的应用。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下使用应用的可能性，与娱乐相对，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。

标签

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。只能在未加密或已解密的流量中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。在计划将过滤器标准添加到规则中时，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 **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。使用这些对象可在访问控制策略中实施手动 URL 过滤。

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：

- 为了确定网络流量是否与URL条件相匹配，系统将执行简单的子字符串匹配。如果请求的URL与字符串的任意部分匹配，该 URL 将被视为匹配。因此，example.com 将与该网络中的任何主机匹配，例如 www.example.com 或 ads.example.com。另外，也与 badexample.com 匹配。
- 当使用包括 URL 条件的访问控制规则匹配网络流量时，系统会忽略加密协议（HTTP 和 HTTPS）。换句话说，如果阻止网站，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细化该规则。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用密钥中的主题公用名创建该对象。此外，系统会忽略在主题公用名中的子域，因此，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

注释 在配置定位于特定站点的 URL 对象之前，请仔细阅读访问控制章节中有关 URL 过滤的信息。URL 匹配的方式与您期望的方式不同，所以您很容易无意间结束阻止站点。例如，如果您尝试明确阻止游戏站点 ign.com，这也会阻止 verisign.com 和其他任何以“ign.”结尾的站点

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。
- 要编辑对象或组，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 输入对象的名称和描述（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 **OK**，保存更改。

配置地理位置对象

地理定位对象定义托管设备（流量的源或目标）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，使用地理定位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定位，而无需使用地理定位对象。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定位数据来过滤流量，思科强烈建议您定期更新地理定位数据库 (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**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。
- 要编辑对象，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 输入对象的名称和描述（后者为可选项）。

步骤 4 在**大洲/国家/地区**列表中，点击**添加** + 并选择要添加到该对象的大洲和国家/地区。选择大陆将会选择该大陆内的所有国家/地区。

步骤 5 点击 **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。如果您设置了系统日志服务器来执行日志收集和分析，请创建对象来定义它们，并在访问规则或诊断日志记录系统设置中使用这些对象。有关设置系统日志记录的信息，请参阅以下主题：

- 日志记录设置，第 142 页
- 配置诊断日志记录，第 263 页

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。
- 要编辑对象，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 配置系统日志服务器的属性：

- **设备接口**-选择用于连接系统日志服务器的接口。如果可以通过桥接组成员接口访问该服务器，请改而选择该桥接组接口 (BVI)。
- **IP 地址** - 输入系统日志服务器的 IP 地址。
- **端口** - 输入服务器用于接收系统日志消息的 UDP 端口。默认值为 514。

步骤 4 点击 **OK**，保存更改。

第 I 部分

基本操作

第 6 章

接口

以下主题介绍如何在 Firepower 威胁防御设备上配置接口。

关于 Firepower 威胁防御 接口

Firepower 威胁防御 设备包括数据接口和管理/诊断接口。以下主题介绍了通过 Firepower 设备管理器配置接口的局限性，以及其他接口管理概念。

接口配置的局限性

使用 Firepower 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 Firepower 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。
- 不支持仅 IPS 模式。不能将接口配置为内联、内联分流、被动或 ERSPAN 以执行仅 IPS 处理。仅 IPS 模式的接口将绕过许多防火墙检查，仅支持 IPS 安全策略。相比之下，防火墙模式接口需要对流量执行防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组和 TCP 规范化。另外，您还可以根据安全策略，选择配置该防火墙模式接口的 IPS 功能。
- 但无法配置 EtherChannel 或冗余接口。
- 无法为 IPv4 配置 PPPoE。如果将互联网接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，且 ISP 使用 PPPoE 为您提供 IP 地址，则您必须使用 Firepower 管理中心 来配置这些设置。
- 对于 ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X 而言，您可以安装可选的网络接口卡 (EPM)。仅在引导程序期间才会发现卡（即安装期间、在本地/远程管理之间切换时以及主要/次要版本[但不是补丁或修复补丁]升级期间）。对于 SFP 接口的卡而言，Firepower 设备管理器会将速度和双工设置为自动；但 SFP 接口不支持将速度和双工设置为自动。对于这些接口，请选

择合适的速度（例如 1000）或选择**默认**速度和双工模式。默认设置会告诉 Firepower 设备管理器无需配置选项，从而使它们保留默认设置（不清除任何现有配置）。请参阅 EPM 文档，以确定接口支持的最大速度。此外，您还可以为速度设置选择**不协商**（如果接口接受此选项），但请仅在确定接口支持此选项时再选择此项。

注释 如果出现错误并需要取消配置**不协商**，请将此选项设置为**自动**并进行部署。部署会失败。然后，可以将该选项设置为**默认**并重新部署，这样部署应会成功。

数据接口

您可以配置以下类型的接口：

路由

每个第 3 层路由接口（或子接口）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。

您可以分配静态地址，也可以从 DHCP 服务器获取静态地址。但是，如果 DHCP 服务器提供与设备上的静态定义接口相同的子网地址，系统会禁用 DHCP 接口。如果使用 DHCP 获取地址的接口停止传递流量，请检查该地址是否与设备上其他接口的子网重叠。

桥接

桥接组是 Firepower 威胁防御设备桥接而非路由的一组接口。桥接接口属于桥接组，且所有接口都在同一网络上。桥接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，桥接组成员接口上的流量不能离开桥接组。通常，您可以指定该接口，以便将成员接口路由到互联网。

在路由模式下，桥接组的一个用途是在 Firepower 威胁防御设备上使用额外接口，而不使用外部交换机。您可以将终端直接连接到桥接组成员接口。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。

可以在路由接口或 BVI 上同时配置 IPv4 和 IPv6 地址。请确保配置一条同时适用于 IPv4 和 IPv6 的默认路由。不能在桥接组成员接口上配置地址。

IPv6 编址

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。对于桥接组，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。本地链路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。在桥接组中，对 BVI 启用 IPv6 将为每个桥接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。

管理/诊断接口

标记为“管理”实际上有两个与其关联的单独接口。

- 管理虚拟接口 - 此 IP 地址用于系统通信。这是系统用于进行智能许可和检索数据库更新的地址。您可以打开它的管理会话（Firepower 设备管理器和 CLI）。您必须配置一个管理地址，该地址在**系统设置** > **管理界面**上定义。
- 诊断物理接口 - 此物理管理端口的实际名称为“诊断”。您可以使用此接口将系统日志消息发送到外部系统日志服务器。为诊断物理接口配置 IP 地址是可选项。配置该接口的唯一原因是您需要将它用于系统日志。此接口显示在**设备** > **接口**页面上，并可在此页面上进行配置。诊断物理接口只允许管理流量，而不允许穿越流量。

建议配置管理/诊断接口时，不要将物理端口连接到网络。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 Firepower 设备管理器（请参阅 配置管理访问列表，第 261 页）。

配置单独管理网络的建议

如果要使用单独管理网络，请将物理管理/诊断接口连接到交换机或路由器。

然后，进行以下配置：

- 依次选择**设备** > **系统设置** > **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。
- 仅当您打算通过该接口向系统日志服务器发送系统日志消息时，才需要为诊断接口配置地址（在**设备** > **接口**上）。否则，不要为诊断接口配置地址，因为不需要。您配置的任何 IP 地址必须与管理 IP 地址在同一子网上，并且不能在 DHCP 服务器池中。例如，默认配置使用

192.168.45.45 作为管理地址，192.168.45.46 至 192.168.45.254 作为 DHCP 池，因此您可以使用从 192.168.45.1 到 192.168.45.44 的任何地址配置诊断接口。

单独的管理网络的管理/诊断接口配置局限性

如果连接物理管理接口，请确保遵循以下限制：

- 如果需要一台位于管理网络中的 DHCP 服务器，请在管理接口上配置该服务器（**设备** > **系统设置** > **管理接口**）。不能在诊断（物理）接口上配置 DHCP 服务器。
- 如果管理网络中存在另一台 DHCP 服务器，请禁用该服务器或管理接口上运行的 DHCP 服务器。通常而言，一个给定子网中的 DHCP 服务器不应超过一台。
- 如果同时为管理接口和诊断接口配置地址，请确保其位于同一子网中。
- 您可以使用数据接口作为管理网关，即便为诊断接口配置了 IP 地址。但是，诊断接口不会使用该数据接口作为网关。如果需要从诊断接口通往其他网络的路径，则需要由位于管理网络中的另一台路由器来路由源于诊断 IP 地址的流量。如有必要，请为诊断接口配置静态路由（依次选择**设备** > **路由**）。

安全区域

可为每个接口分配一个安全区域。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。

对于桥接组，可将成员接口添加到区域，但不能添加桥接虚拟接口 (BVI)。

不能将诊断/管理接口包括在区域中。区域只适用于数据接口。

可在**对象**页面创建安全区域。

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。

关于 MTU

MTU 指定 Firepower 威胁防御设备 可在给定以太网接口上传输的最大帧负载大小。MTU 值是没有以太网报头、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

Firepower 威胁防御设备 支持路径 MTU 发现（如 RFC 1191 中定义），该功能允许两个主机之间网络路径中的所有设备协调 MTU，以便可以规范路径中的最低 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 Firepower 威胁防御设备 的内存有空间，即可接收大于配置的 MTU 的帧。

MTU 和巨帧

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：

- 匹配流量路径上的 MTU - 我们建议您将流量路径的所有 Firepower 威胁防御设备 接口及其他设备接口的 MTU 都设置为同一值。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨帧 - 巨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 最大可设置为 9198 字节，以容纳巨帧。

注释 加大MTU会为巨帧分配更多内存，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 ASA 5500-X 系列设备上将 MTU 增加到默认值 1500 以上，则必须重新启动系统。

配置接口

将电缆连接到接口接头时，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。如果该接口是桥接组的成员，此配置就已足够。对于非桥接组成员，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，可将一个物理接口划分成多个标记有不同 VLAN ID 的逻辑接口。

接口列表将显示可用的接口及其名称、地址和状态。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。使用桥接组接口上的开/关箭头可查看成员接口，这些成员接口也会显示于列表中。

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、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。

以下主题介绍如何配置接口。

配置物理接口

要使用物理接口，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，或者要将接口添加到桥接组，则无需配置 IP 寻址。

注释 您不能在桥接组成员接口上配置 IP 地址，但是可以根据需要修改高级设置。

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。
接口列表将显示可用的接口及其名称、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 要启用接口，请点击**状态** > **开**。
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 100 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。

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 **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。
- （可选。）**说明** - 说明最多为 200 个字符，单行，不能使用回车。

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：

- **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。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。

  注释 对于现有接口，如果为该接口配置的是DHCP服务器，则更改地址的功能将受到限制。新 IP 地址必须与 DHCP 地址池位于相同子网，但它不能在该池的范围内。如果需要配置位于不同子网的地址，请首先删除该 DHCP 服务器配置。请参阅配置 DHCP 服务器，第 264 页。

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明示 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 Firepower 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 编址，第 94 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。

- **抑制 RA** - 是否抑制路由器通告。Firepower 威胁防御设备 可参与路由器通告，以便相邻设备可动态获取默认路由器地址。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 Firepower 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。）配置高级接口选项，第 105 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，再编辑它们。

步骤 8 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。

注释 您不能在桥接组成员接口上配置 IP 地址，但是可以根据需要修改高级设置。

开始之前

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。

过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接。
接口列表将显示可用的接口及其名称、地址和状态。子接口组合在其物理接口下。

步骤 2 执行以下操作之一：

- 从齿轮下拉列表中选择**添加子接口**，以创建新的子接口。
- 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 要启用接口，请点击**状态** > **开**。

步骤 4 配置父接口、名称和描述：

- **父接口** - 选择要添加子接口的物理接口。创建子接口后，父接口则无法更改。
- **名称** - 子接口的名称，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。

- （可选。）**说明** - 说明最多为 200 个字符，单行，不能使用回车。

步骤 5 配置常规子接口特征：

- **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。
- **子接口 ID** - 以整数形式输入子接口 ID，介于 1 和 4294967295 之间。允许的子接口数因平台而异。创建子接口后，则无法更改该 ID。

步骤 6 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：

- **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。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。

  注释 对于现有接口，如果为该接口配置的是DHCP服务器，则更改地址的功能将受到限制。新 IP 地址必须与 DHCP 地址池位于相同子网，但它不能在该池的范围内。如果需要配置位于不同子网的地址，请首先删除该 DHCP 服务器配置。请参阅配置 DHCP 服务器，第 264 页。

步骤 7 （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明示 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 Firepower 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 编址，第 94 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。

- **抑制 RA** - 是否抑制路由器通告。Firepower 威胁防御设备 可参与路由器通告，以便相邻设备可动态获取默认路由器地址。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 Firepower 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 8　（可选。）配置高级接口选项，第 105 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，再编辑它们。

步骤 9　点击**确定 (OK)**。

配置桥接组

桥接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桥接组中所包含的接口。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桥接组成员。

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。

通常会在桥接组接口 (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。桥接组中的所有终端都必须具有与桥接组 IP 地址位于同一子网的 IP 地址。

注释　对于所有 ASA 5506-X 型号，在新版本 6.2+ 系统或重新映像的 6.2+ 系统上，设备随附预配置的桥接组 BVI1，名为**内部**，其中包括除**外部**接口外的所有数据接口。因此，设备已经预配置了一个端口用于连接到互联网或其他上游网络，而所有其他端口已启用并可用于直接连接终端。如果要将某个内部接口用于新的子网，必须先从 BVI1 删除所需接口。

开始之前

指定将成为桥接组成员的接口。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域中删除（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桥接组。

此外，还要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，而无需将其从桥接组删除。桥接组本身始终处于启用状态。

过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接。
接口列表将显示可用的接口及其名称、地址和状态。如果已有桥接组，此处将显示文件夹。点击开/关箭头可查看成员接口。成员接口也单独显示于列表中。

步骤 2 执行以下操作之一：

- 点击 BVI1 桥接组的编辑图标 ()。
- 从齿轮下拉列表中选择**添加桥接组接口**创建新组。

  注释 桥接组只能有一个。如果已经定义了一个桥接组，则应编辑该组而非尝试创建新组。如果需要创建新的桥接组，则必须先删除现有桥接组。

- 点击不再需要的桥接组的删除图标 ()。删除桥接组时，其成员将变成标准路由接口，并且所有 NAT 规则或安全区域成员身份保持不变。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桥接组，需要先删除 NAT 规则并将接口从所属安全区域中删除。

步骤 3 进行以下配置：

- **接口名称** - 桥接组的名称，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。

- （可选。）**说明** - 说明最多为 200 个字符，单行，不能使用回车。

步骤 4 编辑桥接组成员列表。
最多可向一个桥接组添加 64 个接口或子接口。

- 点击 + 添加接口。
- 将鼠标悬停在要删除的接口上方，然后点击右侧的 **x**。

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：

- **静态** - 如果希望分配固定的地址，请选择此选项。键入桥接组的 IP 地址和子网掩码。所有连接的终端都将位于此网络中。对于 ASA 5506-X 型号，BVI1“内部”网络的默认设置为 192.168.1.1/24（即 255.255.255.0）。确保该地址尚未在网络中使用。

  注释 对于现有桥接组，如果为该组配置了 DHCP 服务器，更改地址的功能将受到限制。新 IP 地址必须与 DHCP 地址池位于相同子网，但它不能在该池的范围内。如果需要配置位于不同子网的地址，请首先删除该 DHCP 服务器配置。请参阅配置 DHCP 服务器，第 264 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。桥接组通常不会使用此选项，但是您可以根据需要如此配置。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 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明示 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 编址，第 94 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。

- **抑制 RA** - 是否抑制路由器通告。Firepower 威胁防御设备 可参与路由器通告，以便相邻设备可动态获取默认路由器地址。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 Firepower 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。）配置高级接口选项，第 105 页。

请对桥接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桥接组接口。

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，再编辑它们。

步骤 8 点击**确定 (OK)**。

接下来的操作

- 确保已启用您打算使用的所有成员接口。
- 为桥接组配置 DHCP 服务器。请参阅配置 DHCP 服务器， 第 264 页。
- 将成员接口添加到相应的安全区域。请参阅配置安全区， 第 83 页。
- 确保各项策略（例如身份、NAT 和访问策略）可为桥接组和成员接口提供所需的服务。

配置高级接口选项

高级接口选项的默认设置适用于大多数网络。只有在需要解决网络问题时，再配置它们。

以下步骤假定已定义接口。另外，您还可以在初始编辑或创建接口时编辑这些设置。

对于桥接组，您可以在成员接口上配置大多数这些选项。除了 DAD 尝试，这些选项不可用于桥接虚拟接口 (BVI)。

过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接。
接口列表将显示可用的接口及其名称、地址和状态。

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**选项卡。

步骤 4 要将数据接口仅用于管理，请选择**仅管理 (Management Only)**。
仅管理接口不允许通过流量，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 5 将 **MTU**（最大传输单位）更改为所需的值。
默认 MTU 为 1500 字节。您可以指定介于 64 - 9198之间的值。如果通常在网络中使用巨帧，请设置一个较大的值。

注释 如果在 ASA 5500-X 系列设备 上将 MTU 提高到 1500 以上，则必须重新启动设备。登录 CLI 并使用 **reboot** 命令。

步骤 6 （仅限物理接口）。修改速度和双工设置。
默认设置为该接口与线路另一端的接口协商最佳双工和速度，但如有必要，您可以强制实施特定的双工或速度。在为 EPM 卡上的接口设置这些选项之前，请阅读接口配置的局限性， 第 93 页。

- **双工** - 选择**自动**、**半双工**、**全双工**或**默认**。当接口支持时，自动为默认值。

  选择**默认**表示 Firepower 设备管理器不应尝试配置设置。任何现有配置将保持不变。

- **速度** - 选择**自动**可使接口协商速度（默认值）或选取特定速度：**10** Mbps、**100** Mbps、**1000** Mbps。此外，您还可以选择以下特殊选项：

不协商 - 对于光纤接口，请将速度设置为 1000 Mbps，并且不协商链路参数。这是这些接口上配置的默认配置。

默认 - 表示 Firepower 设备管理器不应尝试配置设置。任何现有配置将保持不变。

步骤 7 修改 **IPv6 配置**设置。

- **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接本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。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 8 点击**确定 (OK)**。

监控接口

可在以下区域查看有关接口的一些基本信息：

- **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** > **入口区域**和**出口区域**。这些控制面板根据由接口组成的区域显示统计信息。您可以深入分析此信息以了解更多详情。
- **设备**。“连接图”显示接口状态。将鼠标悬停在端口上方可查看接口的 IP 地址以及接口状态和链路状态。使用此信息可帮助确定本应正常运行但却关闭的接口。

在 CLI 中监控接口

您还可以登录设备 CLI 并使用以下命令获取有关接口相关行为和统计信息的更多详细信息。

- **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。

第 7 章

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路由。

路由概述

以下主题介绍路由在 Firepower 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。

NAT 对路由选择的影响

Firepower 威胁防御 使用路由表和网络地址转换 (NAT) XLATE（转换）表来确定路由。为了处理目标 IP 转换的流量（即未转换流量），系统会搜索现有 XLATE 或静态转换来选择传出接口。

选择过程遵循以下步骤：

1. 如果已经存在目标 IP 转换 XLATE，则数据包的传出接口由 XLATE 表而非路由表来确定。
2. 如果不存在目标 IP 转换 XLATE，但是存在匹配的静态 NAT 转换，则传出接口由静态 NAT 规则确定，并且系统会创建 XLATE，而不使用路由表。
3. 如果不存在目标 IP 转换 XLATE，并且不存在匹配的静态转换，则不对数据包进行目标 IP 转换。系统通过查询路由以选择传出接口来处理此数据包，然后执行源 IP 转换（如有必要）。

   对于常规动态出站 NAT，将会使用路由表对初始传出数据包进行路由，然后创建 XLATE。仅使用现有 XLATE 转发传入返回数据包。对于静态 NAT，始终使用现有 XLATE 或静态转换规则来转发目标转换的传入数据包。

在选择传出接口之后，要另外执行路由查询，以找到属于所选传出接口的合适下一跳。如果路由表中没有明确属于所选接口的路由，则会丢弃数据包并生成 6 级系统日志消息 110001 (没有到主机的路由)，即使另外存在一条用于既定目标网络但属于不同传出接口的路由也是如此。如果找到属于所选传出接口的路由，则会将数据包转发到相应的下一跳。

路由表和路由选择

如果 NAT XLATE 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 的路由）。

如何制定转发决策

系统按如下制定转发决策：

- 如果目标不匹配路由表中的条目，则通过为默认路由指定的接口转发数据包。如果尚未配置默认路由，则会丢弃数据包。
- 如果目标匹配路由表中的单个条目，则通过与该路由关联的接口转发数据包。
- 如果目标匹配路由表中的多个条目，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 现有连接会继续使用已建立的界面，即使类似的某个新连接可能会因路由发生更改而导致不同的行为也会如此。

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地。

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 在**静态路由**页面中，执行以下某项操作：

- 要添加新路由，请点击 **+** > **添加静态路由**。
- 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 3 配置路由属性。

协议

选择路由是用于 **IPv4** 还是 **IPv6** 地址。

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。

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。

对于桥接组，您应为桥接组接口 (BVI)，而不是为成员接口，配置路由。

指标

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。

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。

步骤 4 点击**确定 (OK)**。

监控路由

要监控路由和进行故障排除，请登录设备 CLI 并使用以下命令。

- **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** 显示虚拟管理接口的配置，包括管理网关。通过虚拟接口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** 命令为虚拟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。

第 II 部分

安全策略

第 8 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，还可以根据用户名或用户组名称编写访问规则，从而基于用户授权选择性地允许或阻止对资源的访问。

注释 当系统检测到不同用户多次登录同一主机时，系统将假设某一时刻只有一个用户登录到了某给定主机，并且一个主机的当前用户是最后授权的用户登录。如果有多个用户通过远程会话登录，则服务器报告的最后用户即为该用户。

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。

对用户数量的限制

Firepower 设备管理器可以从目录服务器下载多达 2000 个用户的信息。

如果您的目录服务器上有2000多个用户帐户，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 2000 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 2000 个，则只能将下载的 2000 个名称与组成员身份进行匹配。

如果您有 2000 多个用户，请考虑使用 Firepower 管理中心（远程管理器）而非 Firepower 设备管理器。Firepower 管理中心支持的用户数量要多很多。

支持的目录服务器

可以将 Windows Server 2008 和 2012 上的 Microsoft Active Directory (AD) 与身份策略结合使用。

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
first name	givenname
last name	sn
email address	mail Userprincipalname（如果 mail 没有值）
department	department distinguishedname（如果 department 没有值）
telephone number	telephonenumber

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。您必须进入正确的基准，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

输入具有已知用户名（部分或完整）的 **dsquery user** 命令，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

输入具有已知组名称的 **dsquery group** 命令，以确定基准标识名。例如，以下命令使用组名称 Employees 返回标识名名称：

```
C:\>dsquery group -name “Employees”
“CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com”
```

组基准标识名为 “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 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**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。

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。

如果您不想等到每天午夜更新，可以通过编辑目录服务器信息（依次选择**策略** > **身份**，然后点击**目录服务器**按钮）进行强制更新。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。

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，系统会提示您启动向导进行配置。点击**开始**启动向导。向导将指导您完成以下步骤：

a) 配置目录服务器，第 119 页
b) 配置主动身份验证强制网络门户，第 120 页

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。
- 要更改目录服务器配置，请点击**目录服务器**按钮（  ）。

- 要更改主动身份验证强制网络门户配置，请点击**主动身份验证**按钮（  ）。
- 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，请点击规则的编辑图标()。也可以选择在表中点击某编辑属性来编辑该属性。

  要删除不再需要的规则，请点击该规则的删除图标 ()。

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 121 页。

配置目录服务器

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。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的更新后的相关信息。

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 添加领域之后，即可通过点击**目录服务器**按钮，然后点击“目录服务器”对话框中的**测试**按钮来验证设置并测试连接。如果测试失败，请验证所有字段并确保管理 IP 地址与目录服务器之间存在网络路径。

过程

步骤 1 依次选择 **策略** > **身份**。

步骤 2 执行以下操作之一：

- 如果尚未配置目录或身份规则，请点击**开始**启动身份策略向导。系统首先会提示您配置目录服务器。
- 点击**目录服务器**按钮 ( ）。

步骤 3 填写有关目录服务器的以下信息：

- **名称 (Name)** - 目录领域的名称。
- **类型 (Type)** - 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 (Directory Username)**、**目录密码 (Directory Password)** - 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。例如 admin@ad.example.com。
- **基准 DN (Base 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 117 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 (Hostname/IP Address)** - 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 (Port)** - 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 (None)**，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。

  LDAPS 需要基于 SSL 的 LDAP。使用端口 636。

- **SSL 证书 (SSL Certificate)** - 如果选择加密方法，请上传 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 4 点击**下一步**（在向导中）或**保存**。

配置主动身份验证强制网络门户

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。如果不上传证书，系统会向用户提供自签名证书。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。

注释 对于 HTTP Basic、HTTP Response Page 和 NTLM 身份验证方法，用户将使用该接口的 IP 地址重定向至强制网络门户。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。如果想要使用 HTTP Negotiate，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。

开始之前

确保目录服务器、Firepower 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 执行以下操作之一：

- 如果使用**启动**向导，则在配置目录服务器后点击**下一步**。
- 点击**主动身份验证**按钮（  ）。

步骤 3 配置以下选项：

- **服务器证书 (Server Certificate)** - 在主动身份验证期间提供给用户的 CA 证书。该证书必须为 PEM 或 DER 格式的 X509 证书。粘贴证书，或点击**上传证书**并选择证书文件。在用户身份验证期间默认提供自签证书。
- **证书密钥 (Certificate Key)** - 服务器证书的密钥。粘贴密钥，或点击**上传密钥**并选择密钥文件。
- **端口 (Port)** - 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 1025-65535 的范围内。

步骤 4 点击**保存 (Save)**。

配置身份规则

身份规则将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”(No Authentication)。

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标。

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。

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 (Order)** 中，选择要将该规则插入有序规则列表的位置。
先匹配的规则先应用，所以您必须确保流量匹配标准较具体的规则显示在次之用来匹配流量的较通用标准的策略上方。

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 选择**用户身份验证 (User Authentication)** 类型。

- **主动** - 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 (No Authentication Required)**。

步骤 5 （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 (Type)**）。

- **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 124 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 对于 HTTP Basic、HTTP Response Page 和 NTLM 身份验证方法，用户将使用该接口的 IP 地址重定向至强制网络门户。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。如果想要使用 HTTP Negotiate，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。

步骤 6 （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 7 在**源/目的**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。

身份规则的源/目标标准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**。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 (Destination Zones)**。
- 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 (Source Zones)**。
- 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**，同时将目的区域留空。

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 IP 地址或地理位置的流量，请配置**源网络 (Source Networks)**。
- 要匹配流向 IP 地址或地理位置的流量，请配置**目标网络 (Destination Networks)**。
- 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的 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/地区或大陆控制流量的地理位置。选择大陆将会选择该大陆内的所有国家/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定位数据库 (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 (Source Ports)**。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 (Destination Ports/Protocols)**。
- 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 8 点击 **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 Firepower 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 Firepower 威胁防御 接口添加到“受信任站点”列表。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 Firepower 威胁防御 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，却可为终端用户提供方便。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挑战。

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 (Tools) > Internet 选项 (Internet Options)**。

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：

- **自动检测内联网 (Automatically detect intranet network)**。如果选择此选项，将禁用其他所有选项将。
- **包括绕过此代理的所有站点 (Include all sites that bypass the proxy)**。

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“Internet 选项”(Internet Options) 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 **OK**。

步骤 3 在“Internet 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Firepower 威胁防御接口绕过该代理。适当执行以下任一操作：

- 选择**为本地地址绕过代理服务器 (Bypass proxy server for local addresses)**。

- 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 以进行 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**。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部分，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** > **选项**，然后点击“选项”对话框中的**网络**选项卡来查找这些设置。点击“连接”组中的**设置**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。

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。

第 9 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标准的第一个规则。

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）。
- 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 请求的目标 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。
- 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，则可以对该流量应用 IPS 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。

应用程序过滤

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关联性、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，请参阅应用标准，第 138 页。

应用过滤有一些值得注意的限制，具体请参见对应用控制的限制，第 145 页。最显著的限制是加密流量。

如果应用使用加密（例如HTTPS连接），系统可能无法识别该应用。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。由于您无法使用Firepower设备管理器配置SSL 解密，因此这些应用的访问控制规则不起作用。例如，在撰写本文时，Dropbox 是有此标记的。因此，Dropbox 应用的访问规则会与 Dropbox 连接不匹配。

URL 过滤

URL 条件控制用户在您的网络中可访问的网站。此功能称为 *URL* 过滤。

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。
- 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。

以下主题提供了有关 URL 过滤的详细信息。

基于信誉的 URL 过滤

使用 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”(Auctions) 类别，而 monster.com 属于“职位搜索”(Job Search) 类别。一个 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“高风险”(High Risk)（第 1 级）到“知名”(Well known)（第 5 级）。

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 条件的规则。另外，您还必须启用与思科综合安全情报 (CSI) 的通信，以获得最新的威胁情报。

基于信誉的 URL 过滤的优势

URL 类别和信誉可帮助您快速配置 URL 过滤。例如，您可以使用访问规则阻止“滥用药物”(Abused Drugs) 类别中的高风险 URL。

使用类别和信誉数据可简化策略创建和管理。它可保证系统按预期控制网络流量。由于思科的威胁情报会不断更新有关新 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。例如，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。

一些系统调整方式的示例包括：

- 如果某个访问控制规则阻止所有游戏站点，则在新域注册并分类为“游戏”(Gaming) 时，系统可以自动阻止这些站点。
- 如果某个访问控制规则阻止所有恶意软件站点，而某个博客页面受到恶意软件感染，系统可以将来自该博客的 URL 重新分类为恶意软件，并阻止该站点。
- 如果访问控制规则阻止高风险社交网站，但有人在其简档页面发布的链接中包含指向恶意负载的链接，则系统可以将该页面的信誉从“良性站点”(Benign Sites) 更改为“高风险”(High Risk)，并阻止该网站。

手动 URL 过滤

在访问控制规则中，您可以通过手动过滤单个 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来阻止不适合于本组织的某个类别的网站。但是，如果该类别包含适合的网站，而您希望对它提供访问权限，则可以针对该站点创建手动“允许”(Allow) 规则，并将该规则放在适用于该类别的“阻止”(Block) 规则的前面。

在手动过滤特定 URL 时，请仔细考虑可能受影响的其他流量。为了确定网络流量是否与 URL 条件相匹配，系统将执行简单的子字符串匹配。如果请求的 URL 与字符串的任意部分匹配，该 URL 将被视为匹配。

例如，如果您允许到 example.com 的所有流量，用户可以浏览的 URL 将包括：

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

再例如，请考虑要明确阻止 ign.com（游戏站点）的情景。但是，子字符串匹配意味着阻止 ign.com 也会阻止 verisign.com，这可能并非您的意愿。

过滤 HTTPS 流量

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主题公用名称。

HTTPS 过滤与 HTTP 过滤不同，它不考虑主题公用名称内的子域。中手动过滤 HTTPS URL 时，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

按加密协议控制流量

系统在执行中的 URL 过滤时，不考虑加密协议（HTTP 与 HTTPS）。对于手动 URL 条件和基于信誉的 URL 条件均会发生此情况。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/

要配置仅与 HTTP 或 HTTPS 流量匹配的规则，请向该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（每个规则具有应用和 URL 条件）来允许对某个站点进行 HTTP 访问，同时禁止 HTTP 访问。

第一个规则允许 HTTPS 流量到达网站：

Action: Allow
Application: HTTPS
URL: example.com

第二个规则阻止对同一网站进行 HTTP 访问：

Action: Block
Application: HTTP
URL: example.com

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明示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定位，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。

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适用于 Firepower 的 AMP 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。

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)。

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标准的第一个规则。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标准。
- 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。

以下主题介绍如何配置策略。

配置默认操作

如果连接没有匹配的特定访问规则，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**，请在**入侵策略**下依次选择**启用策略** > **开**，然后选择一条入侵策略。
有关策略选项的说明，请查看入侵策略设置，第 141 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 142 页。

步骤 6 点击 **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标准的第一个规则。

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 (Order)** 中，选择要将该规则插入有序规则列表的位置。
先匹配的规则先应用，所以您必须确保流量匹配标准较具体的规则显示在次之用来匹配流量的较通用标准的策略上方。

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**标题 (Title)** 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，定义流量匹配标准：

- **源/目标** - 通过其传输流量的安全区域（接口）、IP 地址或该 IP 地址的国家/地区或大陆（地理位置）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、协议和端口。请参阅源/目的地条件，第 136 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。请参阅应用标准，第 138 页。
- **URL** - Web 请求的 URL 或 URL 类别。默认设置为任何 URL。请参阅URL 标准，第 139 页。
- **用户** - 用户或用户组。您的身份策略决定用户和群组信息是否可用于流量匹配。只有配置身份策略，才能使用此标准。请参阅用户条件，第 140 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**。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**。点击对象或元素的 **x**，可将其从策略中删除。

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，您可以使用单一规则对特定主机执行 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/目标和应用之间）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”(Allow) 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 IPS 入侵检测策略，可检测流量中是否存在入侵和漏洞。请参阅入侵策略设置，第 141 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 142 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 142 页。

步骤 9 点击**确定 (OK)**。

源/目的地条件

访问规则的“源/目标”(Source/Destination) 标准定义通过其传递流量的安全区（接口）、IP 地址或 IP 地址的国家/地区或大洲（地理位置）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、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。

您可以使用以下标准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 (Destination Zones)**。
- 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 (Source Zones)**。
- 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IPS检测，则应选择内部区域为**的目的地区域**，同时将源区域保留为空。要在规则中实施 IPS 过滤，则规则操作必须为**允许 (Allow)**，并且必须在该规则中选择入侵策略。

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 IP 地址或地理位置的流量，请配置**源网络 (Source Networks)**。
- 要匹配流向 IP 地址或地理位置的流量，请配置**目标网络 (Destination Networks)**。
- 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的 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/地区或大陆控制流量的地理位置。选择大陆将会选择该大陆内的所有国家/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，可以轻松地限制对特定国家/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定位数据来过滤流量，思科强烈建议您定期更新地理定位数据库 (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 (Source Ports)**。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 (Destination Ports/Protocols)**。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。

应用标准

访问规则的“应用”(Application) 标准定义 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。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关联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，但如果要创建复杂规则，使用对象可便于遵守每个标准 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。

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 单个过滤器标准中的多个选项具有 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，显示更新中的应用列表仅显示符合标准的应用。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下使用应用的可能性，与娱乐相对，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。

标签

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。只能在未加密或已解密的流量中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。在计划将过滤器标准添加到规则中时，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 标准

访问规则中的 URL 标准定义 Web 请求中使用的 URL 或请求的 URL 所属的类别。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。

URL 类别和信誉可供您快速创建访问控制规则的 URL 条件。例如，您可以阻止所有游戏站点或所有高风险社交网站。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 对象或群组，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**。

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。URL 匹配的方式与您期望的方式不同，所以您很容易无意间结束阻止站点。例如，如果您尝试明确阻止游戏站点 ign.com，这也会阻止 verisign.com 和其他任何以“ign.”结尾的站点

“类别”(Categories) 选项卡

点击 +，选择所需的类别，然后点击**确定 (OK)**。

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 **Suspicious sites**（第 2 级），则其还会自动阻止或监控 **High risk**（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 **Benign sites**（第 4 级），系统还会自动允许 **Well known**（第 5 级）站点。

用户条件

访问规则的“用户”(User) 标准定义 IP 连接的用户或用户组。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标准。

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 个用户或群组，所以选择群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以允许“工程”(Engineering) 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”(Engineering) 组即可。

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。

- **用户和组**选项卡 - 选择所需的用户或用户组。只有在目录服务器中配置了群组，才能使用群组。如果您选择了某个群组，规则将应用于该群组的所有成员，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。

注释 默认情况下，Active Directory 服务器会限制它们从辅助群组报告的用户数量。您必须自定义此限制，这样才能报告辅助群组的所有用户，并且可将他们用于使用用户条件的访问控制规则。Firepower 设备管理器的总体限制为 2000 个用户，因此如果您的目录有 2000 多个用户，则不会看到所有可能的用户名。

- **特殊实体**选项卡 - 从以下项目中选择：

  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”(Guest) 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。

入侵策略设置

思科通过 Firepower 系统提供多种入侵策略。这些策略由思科 Talos 安全智能和研究小组设计，他们设定了入侵和预处理器规则的状态和高级设置。您不能修改这些策略。

对于允许流量的访问控制规则，您可以选择以下任一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。

要启用入侵检测，请选择**入侵策略** > **开**，并使用滑块选择所需的策略。策略将按安全性由低到高列出。

- **连接优先于安全性** - 此策略适用于连接（即确保能够获取所有资源）优先于网络基础设施安全性的组织。此入侵策略启用的规则远远少于“安全性优先于连接”(Security over Connectivity) 策略中启用的规则。仅会启用阻止流量的最重要规则。如果要应用某些入侵保护，但对网络的安全性相当自信，可选择此策略。
- **平衡安全性和连接** - 此策略用于平衡整体网络性能和网络基础设施安全性。此策略适合大多数网络。对于要应用入侵防御的大多数情况，可选择此策略。
- **安全性优先于连接** - 此策略适用于网络基础设施安全性优先于用户便利性的组织。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。如果安全性至上或针对高风险流量，可选择此策略。
- **最大检测** - 此策略适用于网络基础设施安全性比在“安全性优先于连接”策略中还要重要、有可能产生更大运营影响的组织。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。如果选择此策略，请仔细评估是否要丢弃过多的合法流量。

文件策略设置

借助适用于Firepower的高级恶意软件保护（适用于Firepower的AMP），可使用文件策略检测恶意软件（或恶意软件）。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。

适用于 Firepower 的 AMP 使用 AMP 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AMP云并执行恶意软件查找。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 AMP 云中是否存在该文件的处置。可能的处置包括：

- 恶意软件 - AMP 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）将被标记为恶意软件。
- 安全 - AMP 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，存档文件将被标记为安全。
- 未知 - AMP 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，存档文件将被标记为未知。
- 不可用 - 系统无法通过查询AMP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 AMP 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 AMP 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。
- **阻止 Office 文档和 PDF 上传、阻止其他恶意软件** - 阻止用户上传 Microsoft Office 文档和 PDF。此外，查询 AMP 云以确定遍历网络的文件是否包含恶意软件，然后阻止存在威胁的文件。
- **阻止 Office 文档上传、阻止其他恶意软件** - 阻止用户上传 Microsoft Office 文档。此外，查询 AMP 云以确定遍历网络的文件是否包含恶意软件，然后阻止存在威胁的文件。

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。

您应该根据贵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”(Block) 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 (Block)**，原因为**入侵阻止 (Intrusion Block)**，即使执行入侵检测，也必须使用“允许”(Allow) 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 **Block**，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。

监控访问控制策略

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 64 页。

- **监控** > **策略**显示命中率最高的访问控制规则和相关统计信息。
- 可以在**网络概述**、**目的**、**入口区**和**出口区**控制面板找到常规统计信息。
- 可以在 **Web 类别**和**目的地**控制面板找到 URL 过滤结果。必须至少有一个 URL 过滤策略，才能在“Web 类别”控制面板中看到任何信息。
- 可以在**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**控制面板上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。

在 CLI 中监控访问控制策略

您还可以登录设备 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 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。

访问控制限制

以下主题介绍了访问控制策略的一些限制。

对应用控制的限制

应用识别的速度

在执行以下操作之前，系统无法执行应用控制：

- 客户端和服务器之间建立受监控连接，并且
- 系统识别会话中的应用

此识别应在 3 到 5 个数据包内发生，或者在 SSL 握手中的服务器证书交换（如果流量已加密）后发生。

如果早期流量与所有其他标准匹配，但应用识别未完成，系统将允许传递数据包，并允许建立连接（或允许 SSL 握手完成）。在系统完成其识别后，系统会对剩余的会话流量应用适当的操作。

对于访问控制，这些通过的数据包由访问控制策略的默认入侵策略（既不是默认操作入侵策略，也不是近乎匹配规则的入侵策略）检查。

已加密和已解密流量的应用控制

系统可识别和过滤已加密和已解密的流量：

- 加密流量 - 系统可以检测使用 StartTLS（包括 SMTP、PoP、FTP、Telnet 和 IMAP）加密的应用流量。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主题专有名称值来识别某些加密应用。这些应用附以 `SSL Protocol` 标记。只能在未加密或已解密的流量中检测到没有此标记的应用。
- 解密流量 - 系统还会将 `decrypted traffic` 标记分配给系统只能在解密流量中检测到（在加密或未加密流量中无法检测到）的应用。

处理无负载的应用流量数据包

在执行访问控制时，对于在识别应用的连接中没有负载的数据包，系统会应用默认策略操作。

处理推荐的应用流量

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）。

控制使用多个协议的应用流量 (Skype)

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。

对用户或组控制的限制

Firepower 设备管理器可以从目录服务器下载多达 2000 个用户的信息。

如果您的目录服务器上有2000多个用户帐户，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 2000 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 2000 个，则只能将下载的 2000 个名称与组成员身份进行匹配。

如果您有 2000 多个用户，请考虑使用 Firepower 管理中心（远程管理器）而非 Firepower 设备管理器。Firepower 管理中心支持的用户数量要多很多。

对 URL 过滤的限制

URL 识别的速度

在满足以下情况之前，系统无法过滤 URL：

- 客户端与服务器之间建立受监控连接
- 系统识别会话中的 HTTP 或 HTTPS 应用
- 系统识别所请求的 URL（对于加密会话，则为 ClientHello 消息或服务器证书中的 URL）

此识别应在 3 到 5 个数据包内发生，或者在 SSL 握手中的服务器证书交换（如果流量已加密）后发生。

如果早期流量与所有其他规则条件匹配，但识别未完成，系统将允许传递数据包，并允许建立连接（或允许 SSL 握手完成）。在系统完成其识别后，系统会对剩余的会话流量应用适当的规则操作。

对于访问控制，这些通过的数据包由访问控制策略的默认入侵策略（既不是默认操作入侵策略，也不是近乎匹配规则的入侵策略）检查。

手动 URL 过滤

在手动过滤特定 URL 时，请仔细考虑可能受影响的其他流量。为了确定网络流量是否与 URL 条件相匹配，系统将执行简单的子字符串匹配。如果请求的 URL 与字符串的任意部分匹配，该 URL 将被视为匹配。

针对已加密 Web 流量的 URL 过滤

在对加密的 Web 流量执行 URL 过滤时，系统将：

- 不考虑加密协议；如果规则包含 URL 条件，但不包含指定协议的应用条件，该规则将同时匹配 HTTPS 和 HTTP 流量。
- 根据用于加密流量的公共密钥中的主题公用名称匹配 HTTPS 流量，不考虑主题公用名称内的子域。

在 URL 中搜索查询参数

系统不使用 URL 中的搜索查询参数来匹配 URL 条件。例如，考虑这样一个场景：您阻止所有购物流量。在这种情况下，系统不会阻止使用网络搜索来搜索 amazon.com，但会阻止浏览至 amazon.com。

针对所选设备型号的内存限制

由于内存限制，某些设备型号会使用一系列较小、欠精细的类别和信誉执行大部分 URL 过滤。例如，如果父 URL 的子站点具有不同的 URL 类别和信誉，某些设备可能仅存储父 URL 的数据。对于这些设备处理的 Web 流量，系统可能会执行云查找来确定本地数据库中没有的站点的类别和信誉。

低内存设备包括以下 ASA 型号：ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X 和 ASA5525-X。

第 10 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 和目标 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：

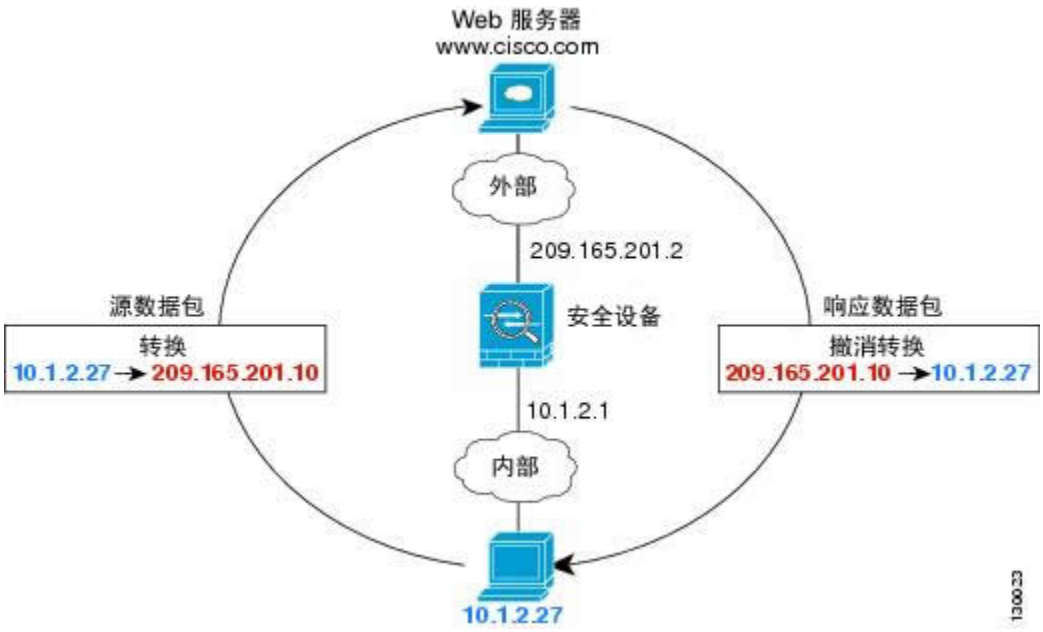
- 动态 NAT - 按先到先得的方式，将一组实际 IP 地址映射到一组映射 IP 地址（通常较小）。仅实际主机可以发起流量。请参阅动态 NAT，第 160 页。
- 动态端口地址转换 (PAT) - 使用 IP 地址的唯一源端口，将一组实际 IP 地址映射到单一 IP 地址。请参阅动态 PAT，第 165 页。

- 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 169 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，但又想免除一小部分地址时，可能就要这样配置 NAT。请参阅身份 NAT，第 178 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 *3*：*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，Firepower 威胁防御设备 接收数据包，因为 Firepower 威胁防御设备执行代理 ARP 以认领数据包。
3. 然后，Firepower 威胁防御设备 会将对映射地址 209.165.201.10 的转换改回为实际地址 10.1.2.27，再将其发送到主机。

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 规则来检查源和目的地 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/目标 A 应当有不同于源 A/目标 B 的转换。对于这种功能可以使用手动 NAT，由此可在单一规则中标识源地址和目标地址。

手动 NAT

手动NAT 允许您在单一规则中标识源地址和目标地址。同时指定源地址和目标地址，可以让您指定源 A/目标 A 可以有不同于源 A/目标 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，可以将它映射到其本身（身份 NAT），或者将它映射到不同的地址。目标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 - 确定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。可以为实际地址使用网络对象组意味着，手动 NAT 的扩展性更强。

- 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的。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以对源/目标组合实施特定转换。

  手动NAT - 单个规则同时转换源和目的。数据包仅匹配一条规则，且不再检查其他规则。即便未配置可选目标地址，一个匹配的数据包也仅会与一条手动 NAT 规则匹配。源和目

标绑在一起，使您可以根据源/目标组合实施不同的转换。例如，源 A/目标 A 可以有不同于源 A/目标 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 规则排序

自动 NAT 和手动 NAT规则存储在一个表中，该表分为三部分。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。

表 *3*：*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，所以必须确保特定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。
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，遵循以下排序指导原则：** **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：

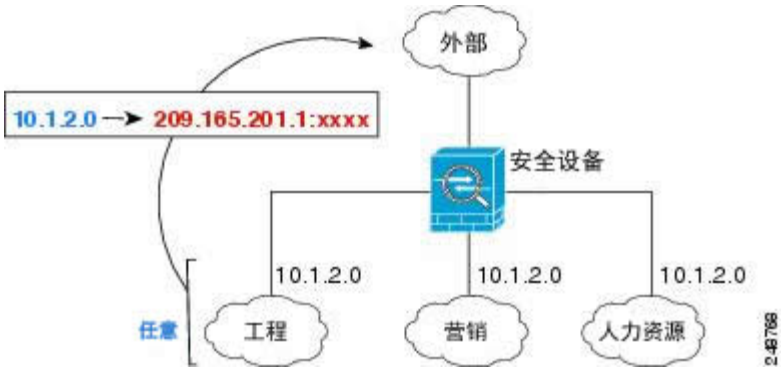
- 192.168.1.1/32（静态）
- 10.1.1.0/24（静态）
- 192.168.1.0/24（静态）
- 172.16.1.0/24（动态）（对象 abc）
- 172.16.1.0/24（动态）（对象 def）
- 192.168.1.0/24（动态）

NAT 接口

除了桥接组成员接口，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 4：指定任何接口



然而，“任何”接口的概念不适用于桥接组成员接口。当指定“任何”接口时，NAT 将排除所有桥接组成员接口。因此，要将NAT应用于桥接组成员，必须指定成员接口。这样可能导致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。

为 NAT 配置路由

Firepower 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的地。

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

如果使用与目的地（映射）接口在同一网络中的地址，Firepower 威胁防御设备 使用代理 ARP 应答任何对映射地址的ARP请求，从而拦截发往映射地址的流量。该解决方案简化了路由，因为Firepower威胁防御设备不必是任何附加网络的网关。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。上游路由器对于指向 Firepower 威胁防御设备的映射地址需要使用静态路由。

与实际地址相同的地址（身份 NAT）

用于身份 NAT 的默认行为已启用代理 ARP，匹配其他静态 NAT 规则。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，Firepower 威胁防御设备会对该地址执行代理 ARP，即使数据包实际并非发往 Firepower 威胁防御设备。（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 Firepower 威胁防御设备 ARP 响应，流量会被误发送到 Firepower 威胁防御设备。

NAT 指南

以下主题提供有关实施 NAT 的详细指导原则。

接口指导原则

标准路由物理接口或子接口都支持NAT

但是，在桥接组成员接口（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：

- 为桥接组的成员配置NAT时，需要指定成员接口。您不能为桥接组接口(BVI)本身配置NAT。
- 在桥接组成员接口之间执行 NAT 时，必须指定源接口和目的地接口。不能指定“任意”作为接口。
- 当目的地接口为桥接组成员接口时，不能配置接口 PAT，因为没有连接到该接口的 IP 地址。
- 当源接口和目的地接口是同一桥接组的成员时，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 指南

NAT 支持 IPv6，但有以下指导原则和限制。

- 对于标准路由模式接口，您还可以在 IPv4 和 IPv6 之间进行转换。
- 对于同一个桥接组的成员接口，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桥接组成员，另一个为标准路由接口的情况。
- 在同属一个桥接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桥接组成员，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 建议

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（手动 NAT 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（手动 NAT 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来允许它们。
- 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。当写入包括这些协议的 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、SMAP、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 *4*: *NAT* 支持的应用检测

应用	检测到的协议、端口	NAT 限制	创建的小孔
DCERPC	TCP/135	无 NAT64。	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。	是
H.323 H.225（呼叫信令） H.323 RAS	TCP/1720 UDP/1718 对于 RAS， UDP/1718-1719	无 NAT64。	是

应用	检测到的协议、端口	NAT 限制	创建的小孔
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
NetBIOS Name Server over IP	UDP/137、138（源端口）	无 NAT64。	否
RSH	TCP/514	无 PAT。 无 NAT64。	是
RTSP	TCP/554 （对于 HTTP 隐藏没有任何处理。）	无 NAT64。	是
SIP	TCP/5060 UDP/5060	无扩展 PAT。 无 NAT64 或 NAT46。	是
Skinny (SCCP)	TCP/2000	无 NAT64、NAT46 或 NAT66。	是
SQL*Net （版本 1、2）	TCP/1521	无 NAT64。	是
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。	是

其他 NAT 指南

- 对于作为桥接组成员的接口，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。
- （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。
- 如果更改 NAT 配置，而且在使用新 NAT 配置之前不想等待现有转换超时，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。

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** 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。
- （仅限手动 NAT。）在 NAT 规则中使用 **any** 作为源地址时，“any”流量（IPv4 与 IPv6）的定义取决于规则。只有数据包为 IPv6 到 IPv6 或 IPv4 到 IPv4 时，Firepower 威胁防御设备 才能对数据包执行 NAT；借助此先决条件，Firepower 威胁防御设备可确定 NAT 规则中的 **any** 的值。例如，如果配置从“any”到 IPv6 服务器的规则，且该服务器已从 IPv4 地址映射，则 **any** 指“任意 IPv6 流量”。如果配置从“any”到“any”的规则，并且将源映射至接口 IPv4 地址，则 **any** 指“任意 IPv4 流量”，因为映射的接口地址表明目标也是 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“any”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。

  故障切换接口 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。
- 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。

配置 NAT

网络地址转换可能非常复杂。我们建议您使规则尽可能保持简单，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 之前仔细规划至关重要。以下步骤提供了基本方法。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 决定所需的规则类型。
您可以创建动态 NAT、动态 PAT、静态 NAT 和身份 NAT 规则。有关概述，请参阅NAT 类型，第 150 页。

步骤 3 确定哪些规则应作为手动 NAT 或自动 NAT 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 151 页。

步骤 4 遵循以下部分中的说明创建规则。

- 动态 NAT，第 160 页
- 动态 PAT，第 165 页
- 静态 NAT，第 169 页
- 身份 NAT，第 178 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 ( )。
- 要删除规则，请点击规则的删除图标 ( )。

动态 NAT

以下主题介绍动态 NAT 以及如何配置动态 NAT。

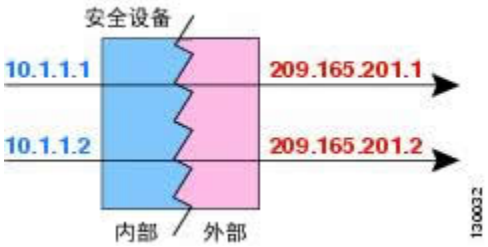
关于动态 NAT

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。

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 *5*：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 *6*：远程主机尝试向映射地址发起连接

动态 NAT 不足和优势

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。

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 (Title)** - 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：

- **Source Interface**、**Destination Interface** -（桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源 (Source)** 是实际接口，流量通过该接口进入设备。**目标 (Destination)** 是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（**任意 [Any]**）。
- **原始地址 (Original Address)** - 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 (Advanced Options)** 链接并选择所需的选项：

- **Translate DNS replies that match this rule** - 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 219 页。
- **Fallthrough to Interface PAT (Destination Interface)** - 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）。仅当您选择不是桥接组成员的目的地接口时，此选项才可用。

步骤 6 点击 **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；它们只能包含一种类型。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 (Original Source Address)** - 该地址可以是网络对象或组，而且它可以包含主机或子网。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。

如果您要在规则中为**原始目标地址 (Original Destination Address)** 和**转换后的目标地址 (Translated Destination Address)** 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：

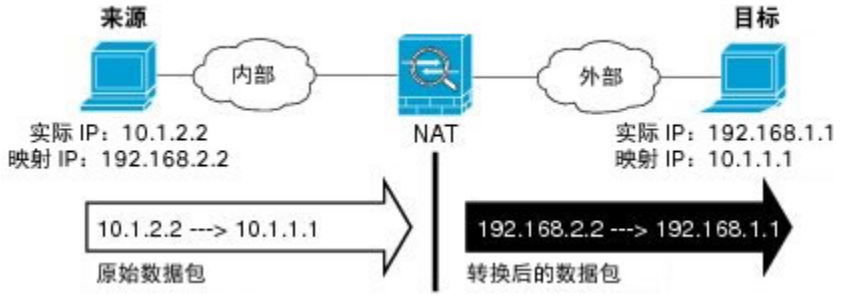
- **标题 (Title)** - 为规则输入名称。

- **创建规则用于 (Create Rule For)** - 选择**手动 NAT (Manual 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、目的地接口**—（桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源 (Source)** 是实际接口，流量通过该接口进入设备。**目标 (Destination)** 是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（**任意 [Any]**）。

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 (Original Source Address)** - 包含将要转换的地址的网络对象或组。
- **原始目标地址 (Original Destination Address)** -（可选。）包含目标地址的网络对象。如果将此留空，则无论目标为何都将应用源地址转换。如果指定目标地址，可以为该地址配置静态转换或只是为其使用身份 NAT。

  可以依次选择**接口 (Interface)** 以使原始目标基于源接口（不能为“任意”[Any]）。如果选择此选项，则还必须选择一个转换后的目标对象。要为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 (Translated Destination Address)** -（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 (Original Destination Address)** 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 (Original Destination Port)**，**转换后的目标端口 (Translated Destination Port)**。
动态 NAT 不支持端口转换，因此，请将**原始源端口 (Original Source Port)** 和**已转换源端口 (Translated Source Port)** 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 (Advanced Options)** 链接并选择所需的选项：

- **Translate DNS replies that match this rule** - 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 219 页。
- **Fallthrough to Interface PAT (Destination Interface)** - 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）。仅当您选择不是桥接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。

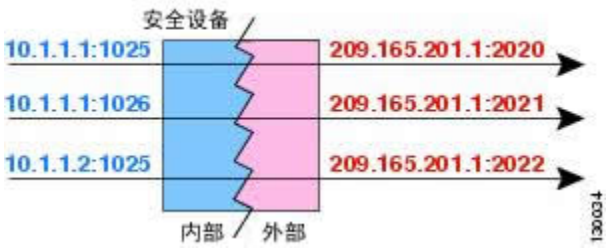
关于动态 PAT

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。如果可用，实际源端口号将用于映射端口。然而，如果实际端口不可用，将默认从与实际端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，低于 1024 的端口仅拥有很小的可用 PAT 池。

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 7：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。

动态 PAT 不足和优势

通过动态 PAT，可以使用单一映射地址，从而保存可路由地址。甚至可以使用 Firepower 威胁防御设备接口 IP 地址作为 PAT 地址。但是，不能将接口 PAT 用于接口上的 IPv6 地址。

当在同一桥接组中的接口之间转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于一个接口为桥接组成员，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 157 页。

动态 PAT 也可能会创建大量看似来自单一 IP 地址的连接，而且服务器可能会将这些流量解释为 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），而且它可以是主机或子网。
- **转换后的地址** - 可以通过以下选项指定 PAT 地址：

  目的接口 - 要使用目的接口 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 (Title)** - 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：

- **Source Interface**、**Destination Interface** -（桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源 (Source)** 是实际接口，流量通过该接口进入设备。**目标 (Destination)** 是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（**任意 [Any]**）。
- **原始地址 (Original Address)** - 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 (Interface)**。您还必须选择具体的目的接口，该接口不能是桥接组成员接口。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（目的 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）。仅当您选择不是桥接组成员的目的地接口时，此选项才可用。如果已将接口 PAT 配置为转换后的地址，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 **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；它们只能包含一种类型。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 (Original Source Address)** - 该地址可以是网络对象或组，而且它可以包含主机或子网。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：

  目的接口 - 要使用目的接口 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 (Original Destination Address)** 和**转换后的目标地址 (Translated Destination Address)** 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。）

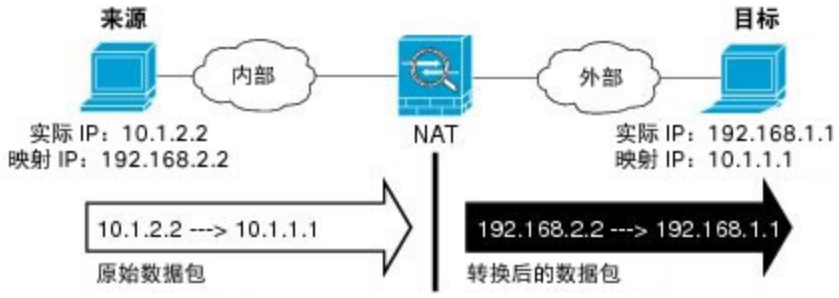
步骤 3 配置基本规则选项：

- **标题 (Title)** - 为规则输入名称。
- **创建规则用于 (Create Rule For)** - 选择**手动 NAT (Manual 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**、**目的地接口**—（桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源 (Source)** 是实际接口，流量通过该接口进入设备。**目标 (Destination)** 是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（**任意 [Any]**）。

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 (Original Source Address)** - 包含将要转换的地址的网络对象或组。

- **原始目标地址 (Original Destination Address)** -（可选。）包含目标地址的网络对象。如果将此留空，则无论目标为何都将应用源地址转换。如果指定目标地址，可以为该地址配置静态转换或只是为其使用身份 NAT。

  可以依次选择**接口 (Interface)**以使原始目标基于源接口（不能为“任意”[Any]）。如果选择此选项，则还必须选择一个转换后的目标对象。要为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 (Translated Source Address)** - 以下项之一：

  （接口 PAT。）要使用目标接口的 IPv4 地址，请选择**接口 (Interface)**。您还必须选择具体的目的接口，该接口不能是桥接组成员接口。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 (Translated Destination Address)** -（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 (Original Destination)** 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 (Original Destination Port)**，**转换后的目标端口 (Translated Destination Port)**。
动态NAT不支持端口转换，因此，请将**原始源端口 (Original Source Port)** 和**已转换源端口 (Translated Source Port)** 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（目的 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）。仅当您选择不是桥接组成员的目的地接口时，此选项才可用。如果已将接口 PAT 配置为转换后的地址，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。

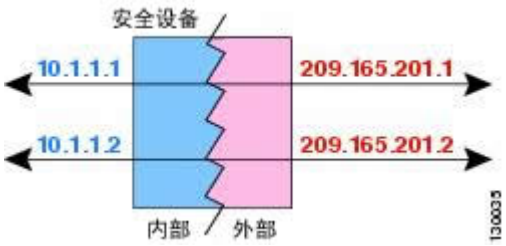
关于静态 NAT

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 *8*：静态 *NAT*



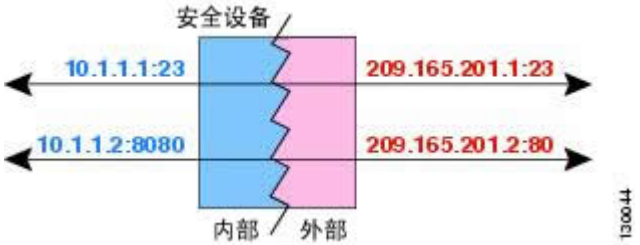
支持端口转换的静态 *NAT*

具有端口转换的静态 NAT 使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 *9*：支持端口转换的典型静态 *NAT* 场景



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。

下面是使用具有端口转换的静态 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*

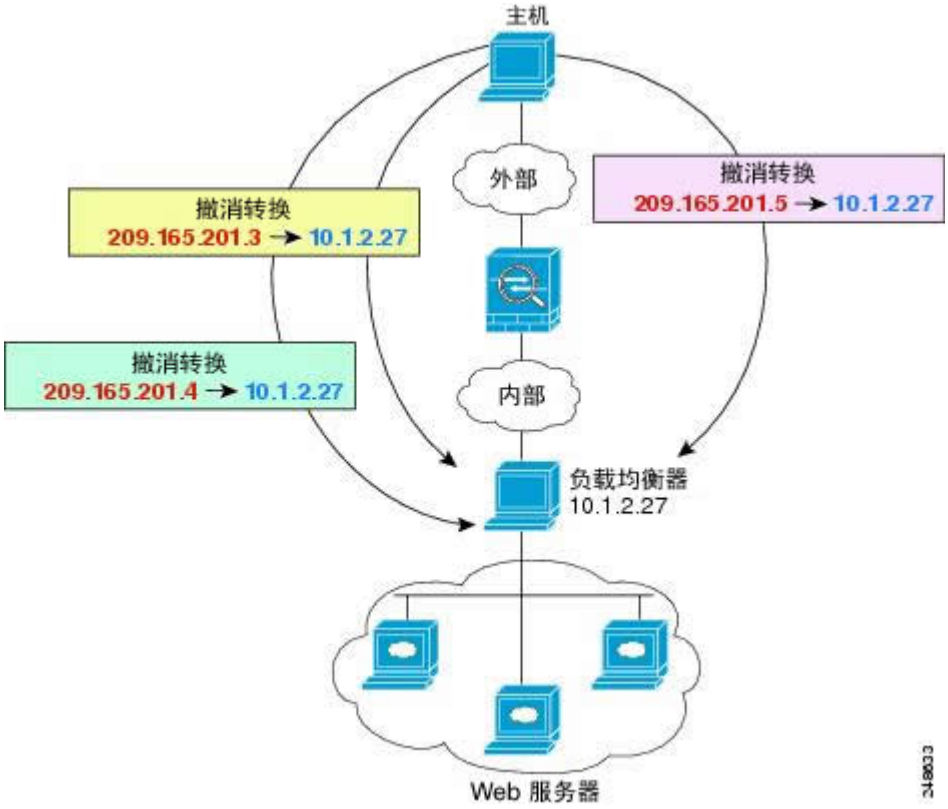
通常，配置带一对一映射的静态 NAT。然而，在某些情况下，可能要将单一实际地址配置到多个映射地址（一对多）。配置一对多静态 NAT 时，当实际主机发起流量时，它始终使用第一个映射地址。然而，对于发起到主机的流量，可以发起到任何映射地址的流量，并且不将它们转换为单一实际地址。

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 *10*: 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 *11*：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，等等，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 *12*：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 *13*：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 (Objects)** 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 (Original Address)** - 该地址必须是网络对象（而非组），而且它可以是主机或子网。
- **转换后的地址 (Translated Address)** - 您可以通过以下选项指定转换后的地址：

  目标接口 (Destination Interface) - 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 (Address) - 创建包含主机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 (Title)** - 为规则输入名称。
- **创建规则用于 (Create Rule For)** - 选择**自动 NAT (Auto NAT)**。
- **类型 (Type)** - 选择**静态 (Static)**。

步骤 4 配置以下数据包转换选项：

- **Source Interface**、**Destination Interface** -（桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源 (Source)** 是实际接口，流量通过该接口进入设备。**目标 (Destination)** 是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（**任意 [Any]**）。
- **原始地址 (Original Address)** - 包含您要转换的地址的网络对象。
- **转换后的地址 (Translated Address)** - 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 (Interface)**。您还必须选择具体的目的地接口，该接口不能是桥接组成员接口。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 (Original Port)**、**转换后的端口 (Translated Port)** - 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 (Advanced Options)** 链接并选择所需的选项：

- **转换与此规则匹配的 NDS 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 219 页。如果要执行端口转换，则此选项不可用。
- **不在目的接口上使用代理 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标的流量。该解决方案简化了路由，因为设备不必是任何附加网络的网关。如果需要，可以禁用代理 ARP，在此情况下您需要确保上游路由器中具有正确的路由。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 **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 (Objects)** 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；它们只能包含一种类型。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 (Original Source Address)** - 该地址可以是网络对象或组，而且它可以包含主机或子网。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 (Any)**。
- **转换后的源地址 (Translated Source Address)** - 可以通过以下选项指定转换后的地址：

  目标接口 (Destination Interface) - 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 (Address) - 创建包含主机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 (Original Destination Address)** 和**转换后的目标地址 (Translated Destination Address)** 配置静态转换，还可以为这些地址创建网络对象。如果希望配置仅具有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。）

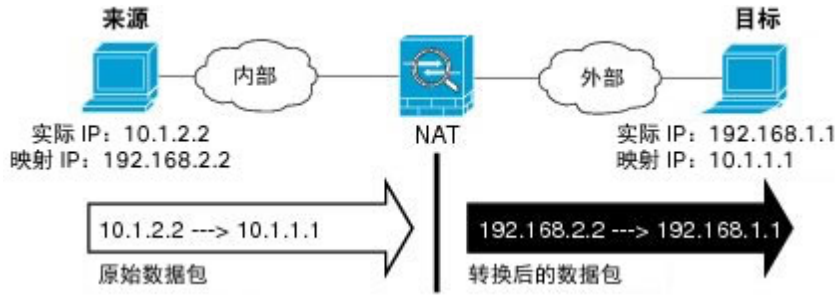
步骤 3 配置基本规则选项：

- **标题 (Title)** - 为规则输入名称。
- **创建规则用于 (Create Rule For)** - 选择**手动 NAT (Manual 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 (Type)** - 选择**静态 (Static)**。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**、**目的地接口**—（桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源 (Source)** 是实际接口，流量通过该接口进入设备。**目标 (Destination)** 是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（**任意 [Any]**）。

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 (Original Source Address)** - 包含将要转换的地址的网络对象或组。
- **原始目标地址 (Original Destination Address)** -（可选。）包含目标地址的网络对象。如果将此留空，则无论目标为何都将应用源地址转换。如果指定目标地址，可以为该地址配置静态转换或只是为其使用身份 NAT。

  可以依次选择**接口 (Interface)** 以使原始目标基于源接口（不能为“任意”[Any]）。如果选择此选项，则还必须选择一个转换后的目标对象。要为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 (Translated Source Address)** - 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 (Interface)**。您还必须选择具体的目的接口，该接口不能是桥接组成员接口。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 (Translated Destination Address)** -（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 (Original Destination)** 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标服务端口。

如果要配置具有端口转换的静态 NAT，可以为源和/或目标转换端口。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 (Original Source Port)**、**转换后的源端口 (Translated Source Port)** - 定义源地址的端口转换。

- **原始目标端口 (Original Destination Port)**、**转换后的目标端口 (Translated Destination Port)** - 定义目标地址的端口转换。

步骤 8 （可选。）点击**高级选项 (Advanced Options)** 链接并选择所需的选项：

- **转换与此规则匹配的 NDS 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 219 页。 如果要执行端口转换，则此选项不可用。
- **不在目的接口上使用代理 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标的流量。该解决方案简化了路由，因为设备不必是任何附加网络的网关。如果需要，可以禁用代理ARP，在此情况下您需要确保上游路由器中具有正确的路由。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。

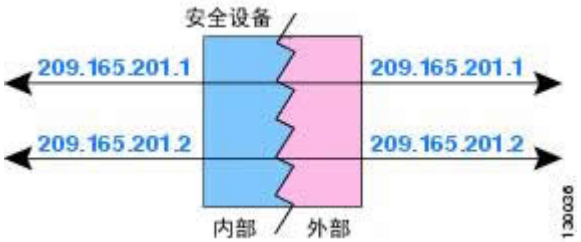
步骤 9 点击 **OK**。

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 *14*: 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 (Title)** - 为规则输入名称。
- **创建规则用于 (Create Rule For)** - 选择**自动 NAT (Auto NAT)**。
- **类型 (Type)** - 选择**静态 (Static)**。

步骤 4 配置以下数据包转换选项：

- **Source Interface**、**Destination Interface** -（桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源 (Source)** 是实际接口，流量通过该接口进入设备。**目标 (Destination)** 是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（**任意 [Any]**）。
- **原始地址 (Original Address)** - 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，您可以选择具有完全相同内容的其他对象。

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。
- **不在目的接口上使用代理 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标的流量。该解决方案简化了路由，因为设备不必是任何附加网络的网关。如果需要，可以禁用代理ARP，在此情况下您需要确保上游路由器中具有正确的路由。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 (Perform Route Lookup for Destination Interface)** - 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；它们只能包含一种类型。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 (Original Source Address)** - 该地址可以是网络对象或组，而且它可以包含主机或子网。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**任意**。
- **转换后的源地址** - 与原始源相同的对象。或者，您可以选择具有完全相同内容的其他对象。

如果您要在规则中为**原始目的地址**和**转换后的目的地址**配置静态转换，还可以为这些地址创建网络对象。如果希望配置仅具有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：

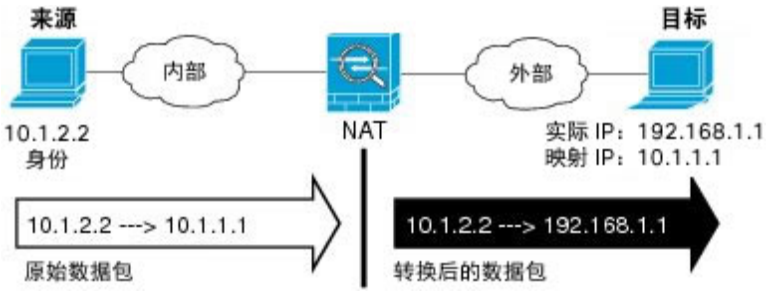
- **标题 (Title)** - 为规则输入名称。
- **创建规则用于 (Create Rule For)** - 选择**手动 NAT (Manual NAT)**。
- **规则位置** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。

- **类型 (Type)** - 选择**静态 (Static)**。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：

- **Source Interface**、**Destination Interface** -（桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源 (Source)** 是实际接口，流量通过该接口进入设备。**目标 (Destination)** 是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（**任意 [Any]**）。

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。
- **原始目的地址** -（可选。）包含目标地址的网络对象。如果将此留空，则无论目标为何都将应用源地址转换。如果指定目标地址，可以为该地址配置静态转换或只是为其使用身份 NAT。

  您可以选择**接口**以使原始目的基于源接口（不能为“任意”）。如果选择此选项，则还必须选择一个转换后的目标对象。要为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，您可以选择具有完全相同内容的其他对象。
- **转换后的目的地址** -（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 (Original Destination Address)** 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标服务端口。
如果要配置具有端口转换的静态 NAT，可以为源和/或目标转换端口。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 (Original Source Port)**、**转换后的源端口 (Translated Source Port)** - 定义源地址的端口转换。
- **原始目标端口 (Original Destination Port)**、**转换后的目标端口 (Translated Destination Port)** - 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。
- **不在目的接口上使用代理 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标的流量。该解决方案简化了路由，因为设备不必是任何附加网络的网关。如果需要，可以禁用代理ARP，在此情况下您需要确保上游路由器中具有正确的路由。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。
- **对目的接口执行路由查找** - 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)**。

Firepower 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。

职位

为规则输入名称。名称不能包含空格。

创建规则用于 (Create Rule For)

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。

Type

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、目的地接口

（桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源 (Source)** 是实际接口，流量通过该接口进入设备。**目标 (Destination)** 是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（**任意 [Any]**）。

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），而且它可以是主机或子网。

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。
- **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 (Interface)**。您还必须选择具体的目的接口，该接口不能是桥接组成员接口。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。包含主机或子网的对象或组。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 (Interface)**。您还必须选择具体的目的地接口，该接口不能是桥接组成员接口。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，您可以选择具有完全相同内容的其他对象。

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、目的地接口

（桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源 (Source)** 是实际接口，流量通过该接口进入设备。**目标 (Destination)** 是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（**任意 [Any]**）。

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。
- **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 (Interface)**。您还必须选择具体的目的接口，该接口不能是桥接组成员接口。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。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 (Interface)**。您还必须选择具体的目的地接口，该接口不能是桥接组成员接口。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，您可以选择具有完全相同内容的其他对象。

原始目标地址 (Original Destination Address)

包含目标地址的网络对象。如果将此留空，则无论目标为何都将应用源地址转换。如果指定目标地址，可以为该地址配置静态转换或只是为其使用身份 NAT。

您可以选择**接口**以使原始目的基于源接口（不能为“任意”）。如果选择此选项，则还必须选择一个转换后的目标对象。要为目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目标端口选择适当的端口对象。

转换后的目标地址 (Translated Destination Address)

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 (Original Destination)**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）。

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 (Advanced)** 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 (Translate DNS replies that match this rule)

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 219 页。如果在静态 NAT 规则中进行端口转换，则此选项不可用。

跳转到接口 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）。仅当您选择不是桥接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 (Do not proxy ARP on Destination Interface)（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标的流量。该解决方案简化了路由，因为设备不必是任何附加网络的网关。如果需要，可以禁用代理ARP，在此情况下您需要确保上游路由器中具有正确的路由。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。

为目标接口执行路由查找 (Perform Route Lookup for Destination Interface)（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。由于指定了目标时无法在手动 NAT 规则中启用 DNS 重写，所以最好是创建两个自动 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 可在路由接口和桥接组成员接口上使用。

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。

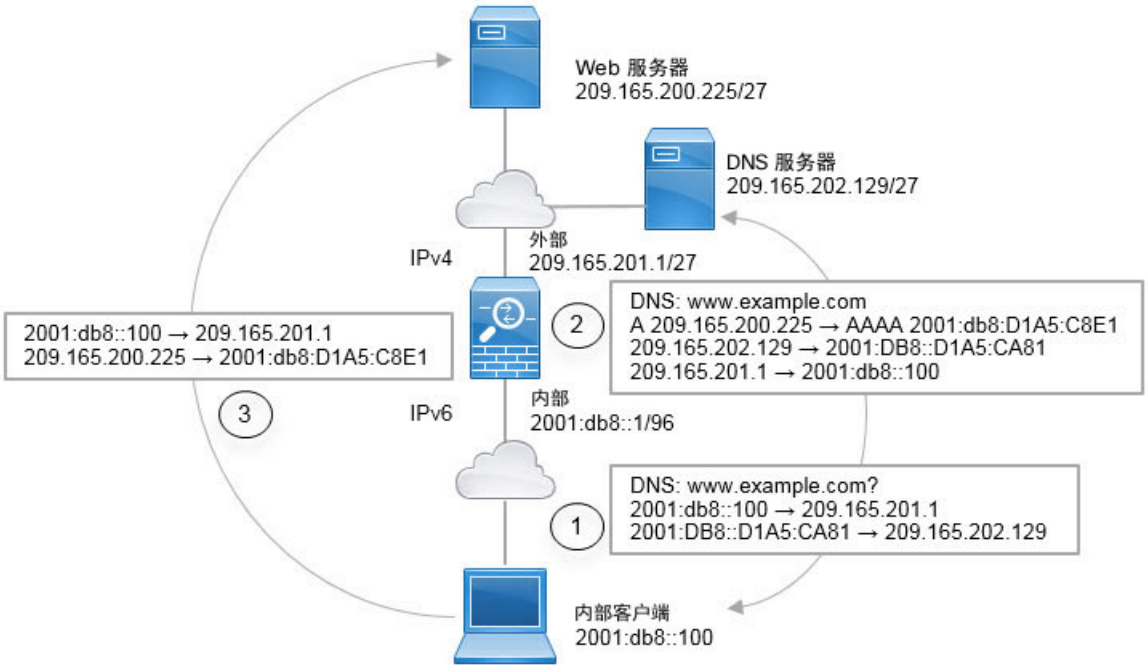
- NAT64 规则的 IPv4 地址池一般较小，通常可能没有足够的地址与 IPv6 客户端地址一对一映射。与动态或静态 NAT 相比，动态 PAT 可以更容易满足可能的大量 IPv6 客户端地址需要。

- 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，一个用于目的地 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。由于指定了目标时无法在手动 NAT 规则中启用 DNS 重写，所以最好是创建两个自动 NAT 规则。

NAT64/46 示例：内部 IPv6 网络与外部 IPv4 互联网

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的地址未转换：

- 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 请求中的源和目的如下转换：

- 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。）

以下步骤介绍了如何配置此示例。

注释 此示例假定，内部接口不是桥接组接口 (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。

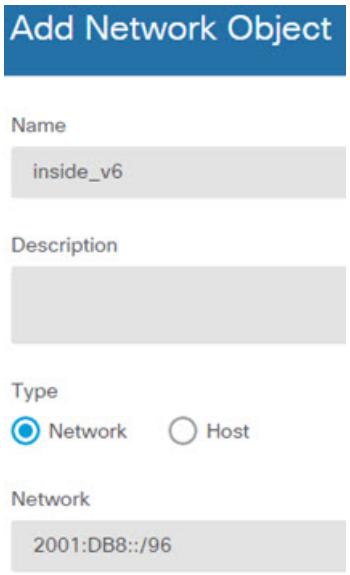
过程

步骤 1 创建定义内部 IPv6 网络和外部 IPv4 网络的网络对象。

a) 选择**对象 (Objects)**。

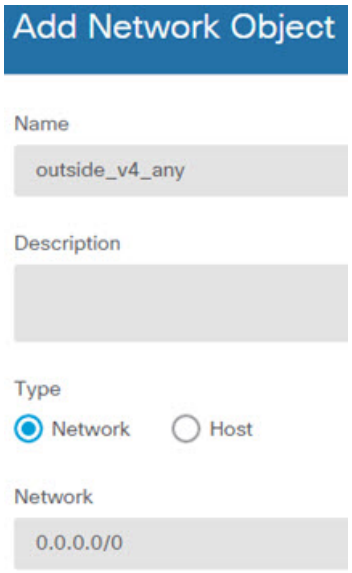
b) 从目录中选择**网络**，然后点击 +。

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) 依次点击**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。

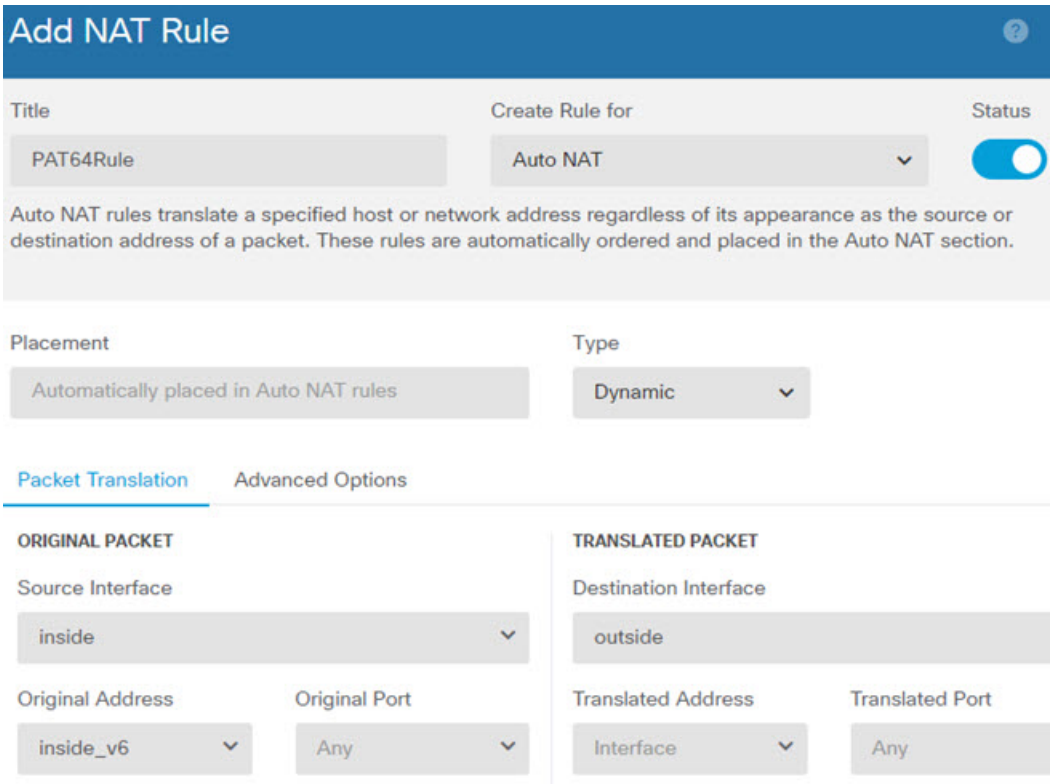
a) 依次选择 **策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = PAT64Rule（或您选择的其他名称）。

- **创建规则的对象** = 自动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目的接口** = 外部。
- **原始地址** = inside_v6 网络对象。
- **转换后的地址** = **接口**。此选项使用目的接口的 IPv4 地址作为 PAT 地址。



d) 点击**确定 (OK)**。
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。

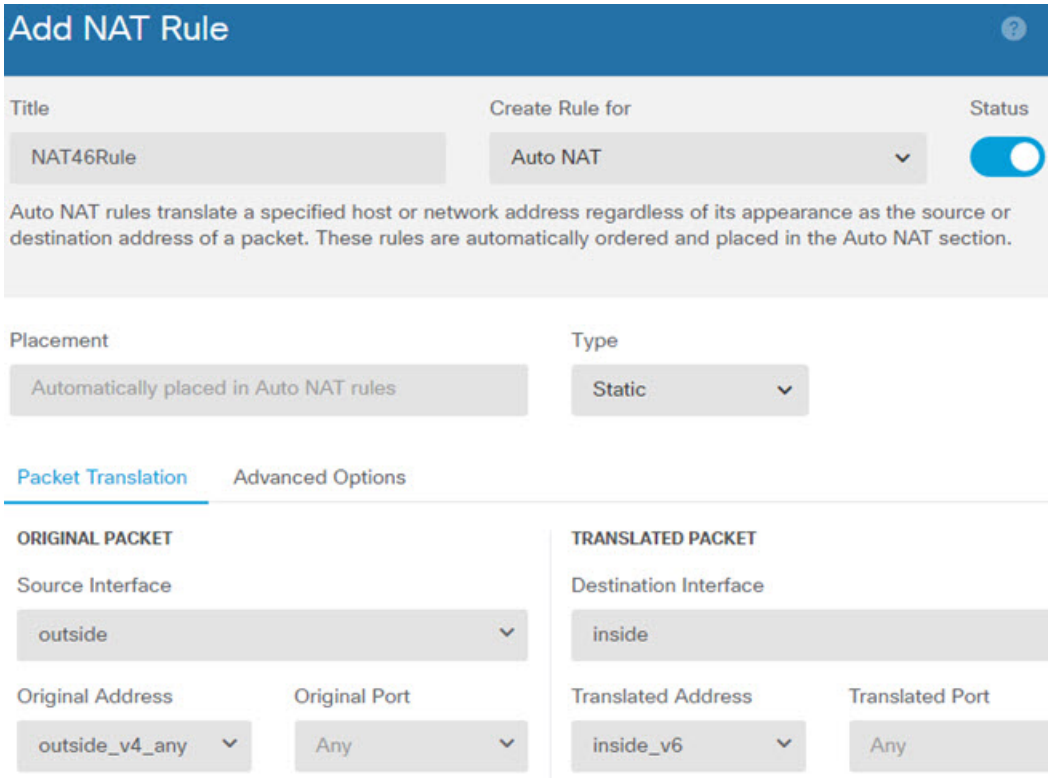
步骤 3 为外部 IPv4 网络配置静态 NAT46 规则。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = NAT46Rule（或您选择的其他名称）。
- **创建规则的对象** = 自动 NAT。
- **类型** = 静态。

- **源接口** = 外部。
- **目的接口** = 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 (OK)**。
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。

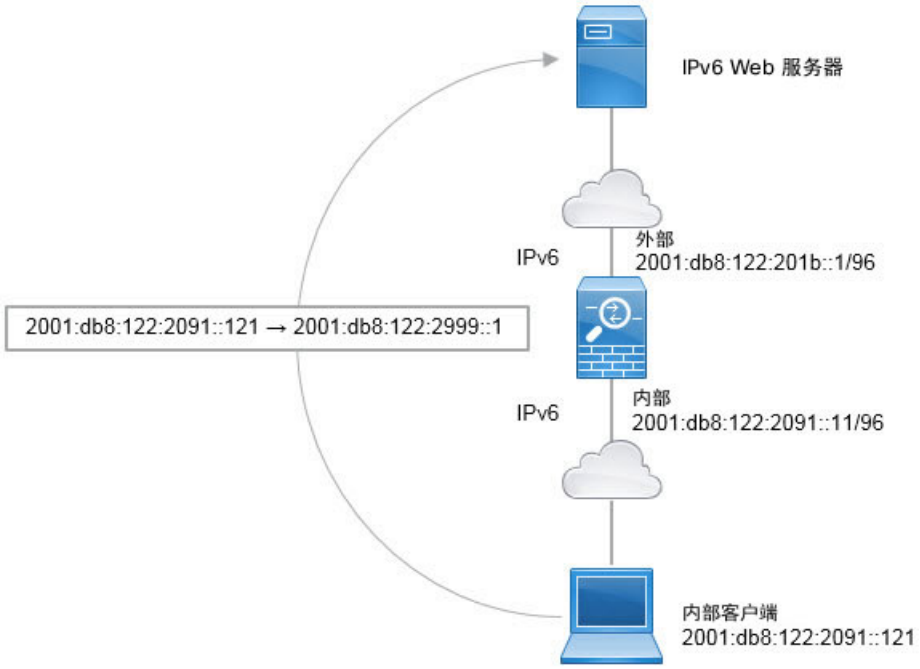
NAT66：将 IPv6 地址转换为不同的 IPv6 地址

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。不过，如果您不希望允许返回流量，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，内部接口不是桥接组接口 (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

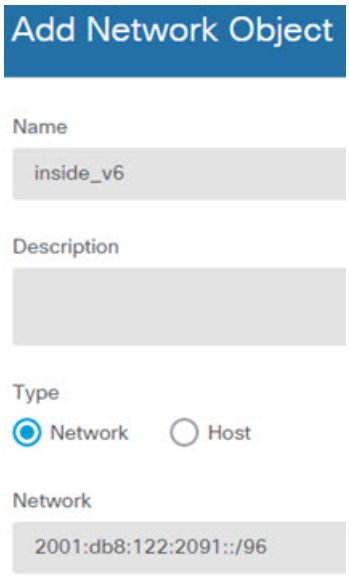
步骤 1 创建定义内部 IPv6 网络和外部 IPv6 NAT 网络的网络对象。

a) 选择**对象 (Objects)**。

b) 从目录中选择**网络**，然后点击 +。

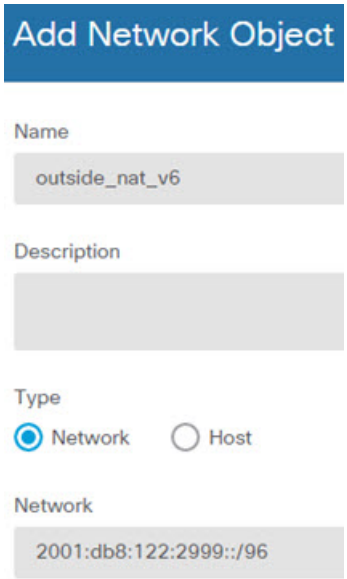
c) 定义内部 IPv6 网络。

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) 依次点击**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。

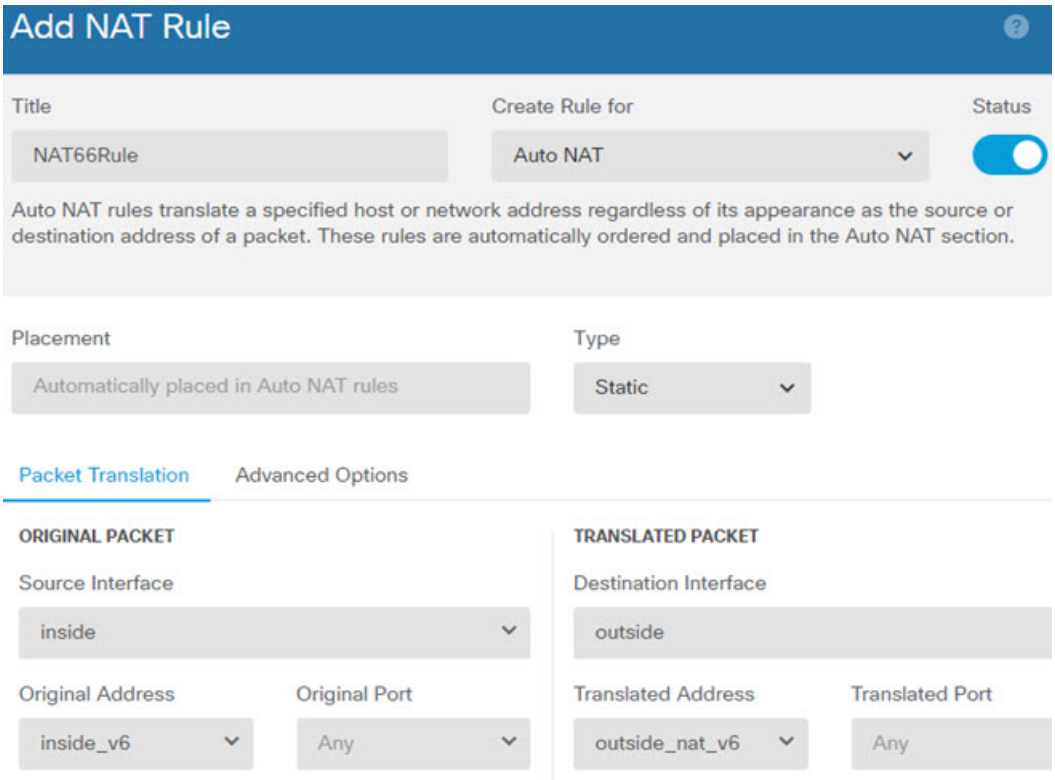
a) 依次选择 **策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = NAT66Rule（或您选择的其他名称）。

- **创建规则的对象** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 内部。
- **目的接口** = 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。

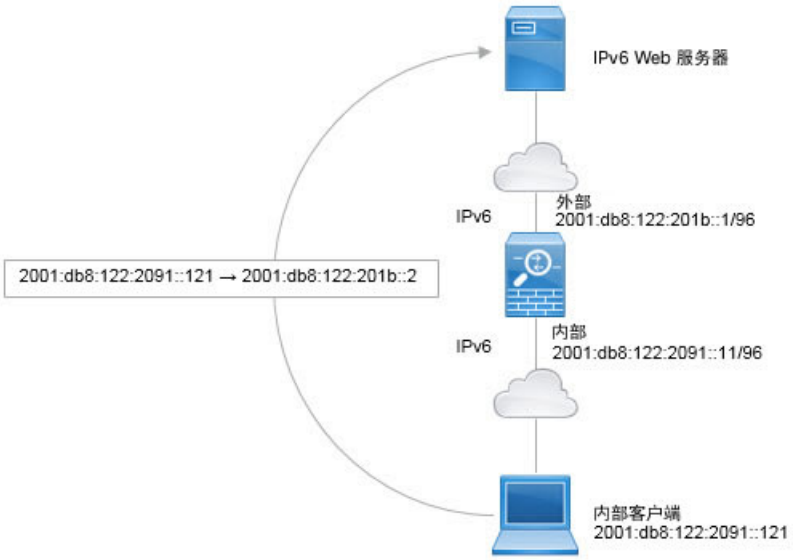


d) 点击**确定 (OK)**。
使用此规则，从内部接口上的 2001:db8:122:2091::/96 子网到外部接口的任何流量都会经静态 NAT66 转换为 2001:db8:122:2999::/96 网络上的地址。

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 Firepower 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，内部接口不是桥接组接口 (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

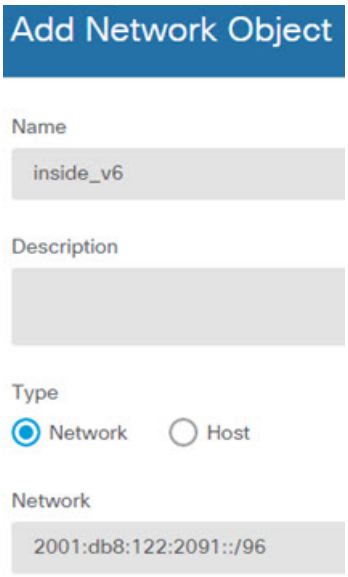
步骤 1 创建定义内部 IPv6 网络和 IPv6 PAT 地址的网络对象。

a) 选择**对象 (Objects)**。

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) 依次点击**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。

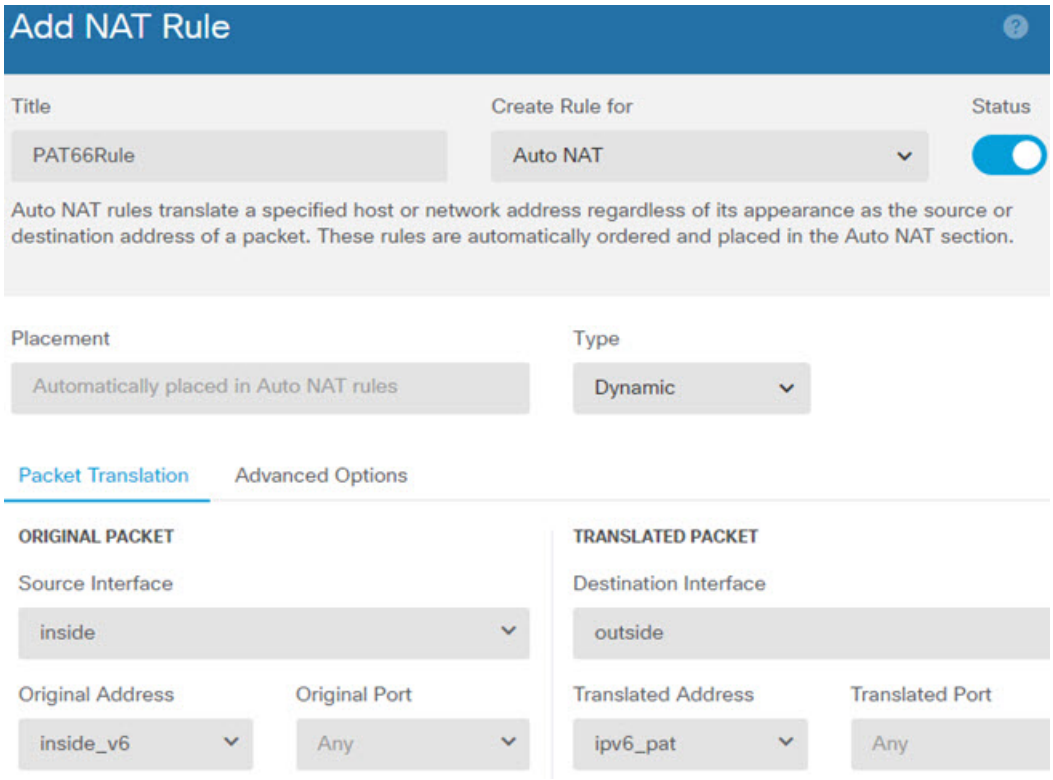
a) 依次选择 **策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = PAT66Rule（或您选择的其他名称）。

- **创建规则的对象** = 自动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目的接口** = 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 (OK)**。
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

要监控 NAT 连接并对其进行故障排除，请登录设备 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。

NAT 示例

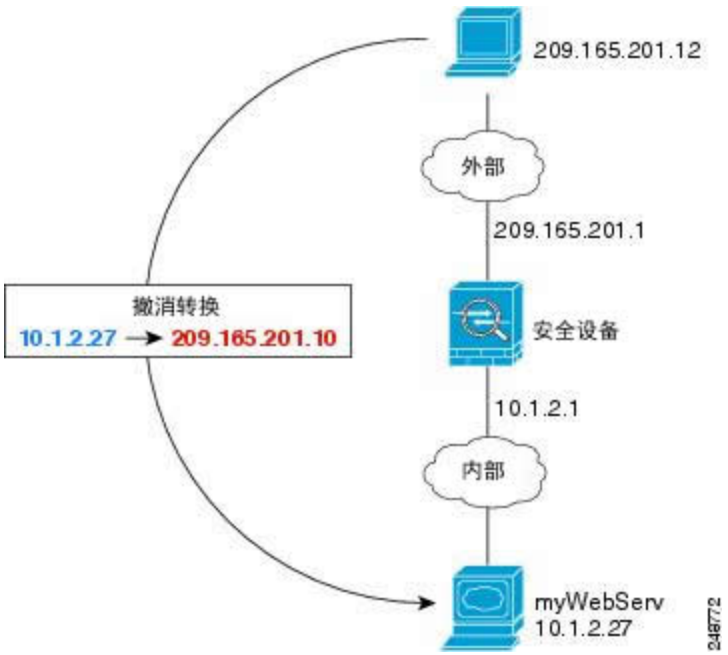
以下主题提供了在威胁防御设备上配置 NAT 的示例。

提供对内部 Web 服务器的访问（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，内部接口不是桥接组接口 (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桥接组成员接口，例如 inside1_3。

图 *15*: 面向内部 *Web* 服务器的静态 *NAT*



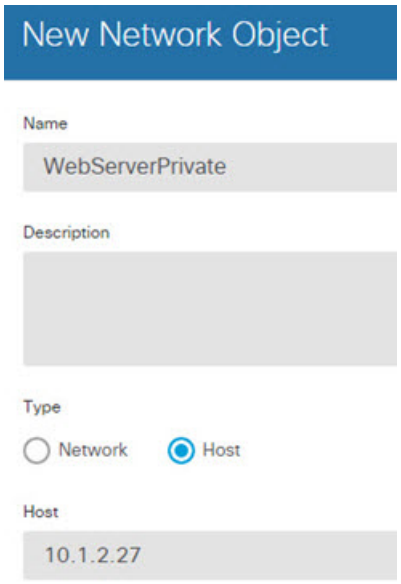
过程

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 (Objects)**。

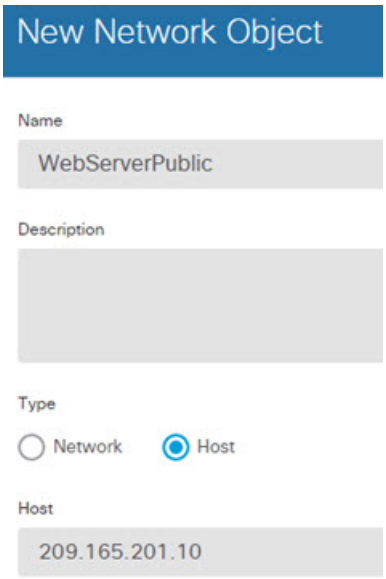
b) 从目录中选择**网络**，然后点击 +。

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 (Host)**，然后输入实际主机 IP 地址 10.1.2.27。



d) 依次点击**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 (Host)**，然后输入实际主机地址 209.165.201.10。



f) 依次点击**确定**。

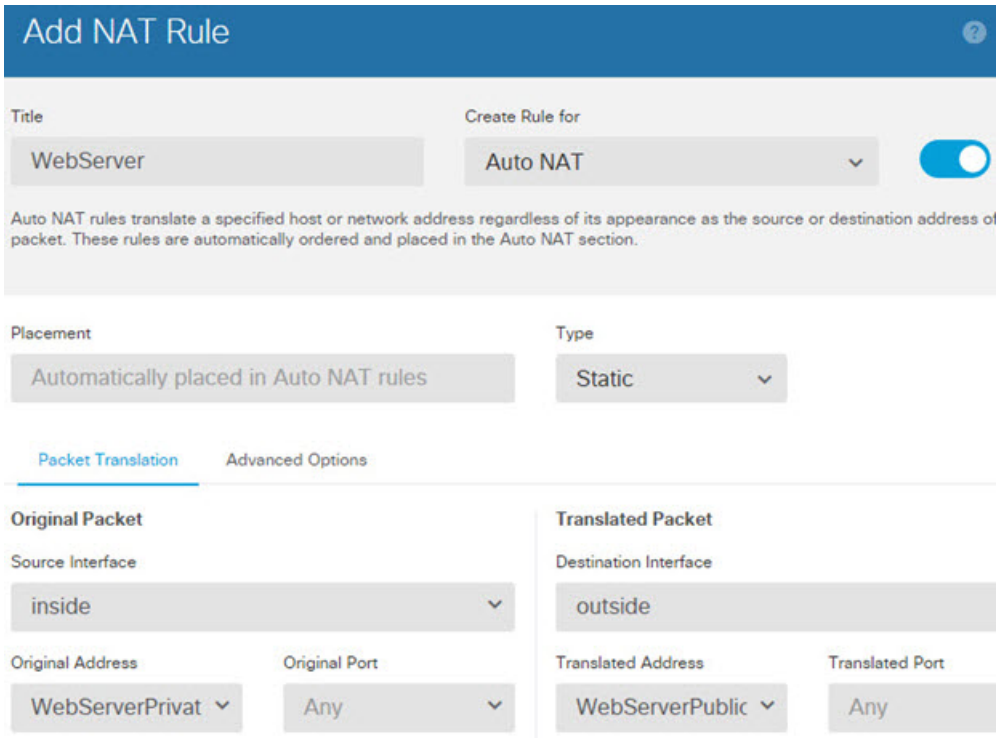
步骤 2 配置对象的静态 NAT。

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）。
- **创建规则的对象** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 内部。
- **目的接口** = 外部。
- **原始地址** = WebServerPrivate 网络对象。
- **转换后的地址** = WebServerPublic 网络对象。



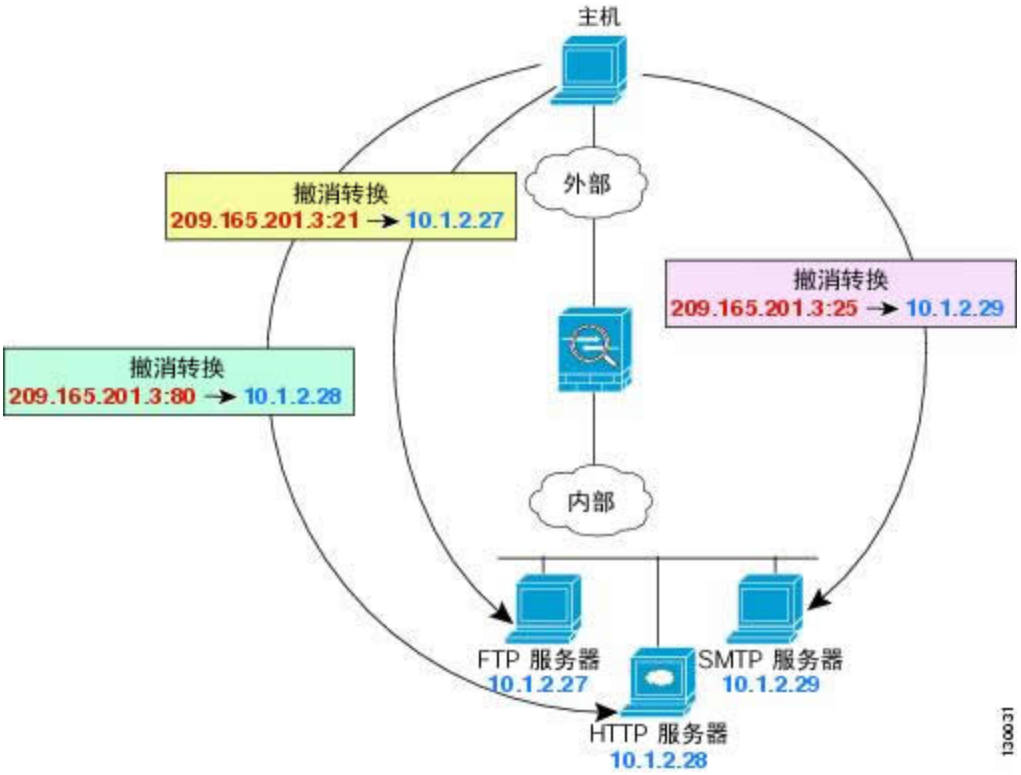
d) 点击**确定 (OK)**。

FTP、HTTP 和 SMTP 的单个地址 (Single Address for FTP, HTTP, and SMTP)（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桥接组接口 (BVI)，并且服务器连接到单独的桥接组成员接口，请选择每个服务器连接的用于相应规则的特定成员接口。例如，规则的源接口可能有 inside1_2、inside1_3 和 inside1_4，而不是 inside。

图 *16*: 支持端口转换的静态 *NAT*



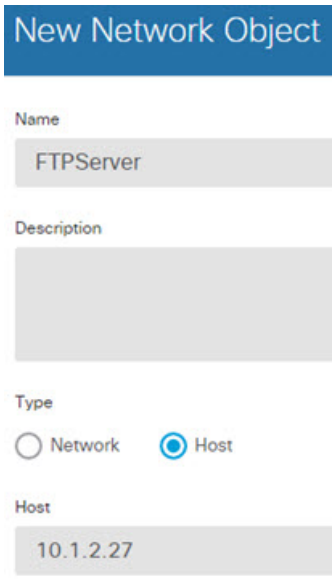
过程

步骤 1 为 FTP 服务器创建网络对象。

a) 选择**对象 (Objects)**。

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 (Host)**，然后输入 FTP 服务器的实际 IP 地址 10.1.2.27。

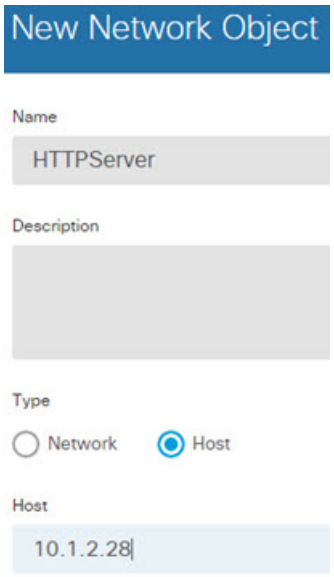


d) 点击**确定**。

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 (Host)**，然后输入实际主机地址 10.1.2.28。

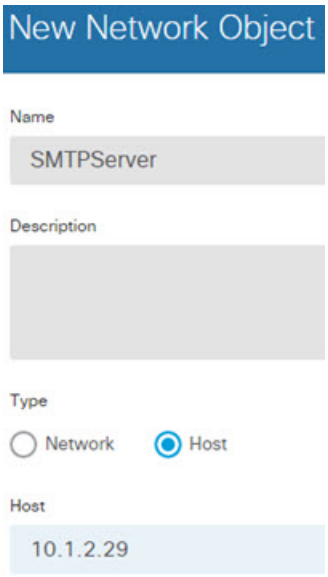


c) 点击**确定**。

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 (Host)**，然后输入实际主机地址 10.1.2.29。

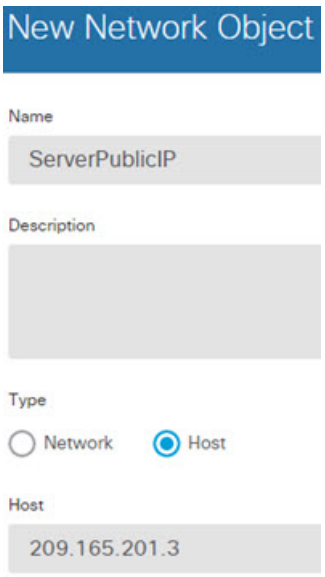


c) 点击**确定**。

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 (Host)**，然后输入实际主机地址 209.165.201.3。



c) 点击**确定**。

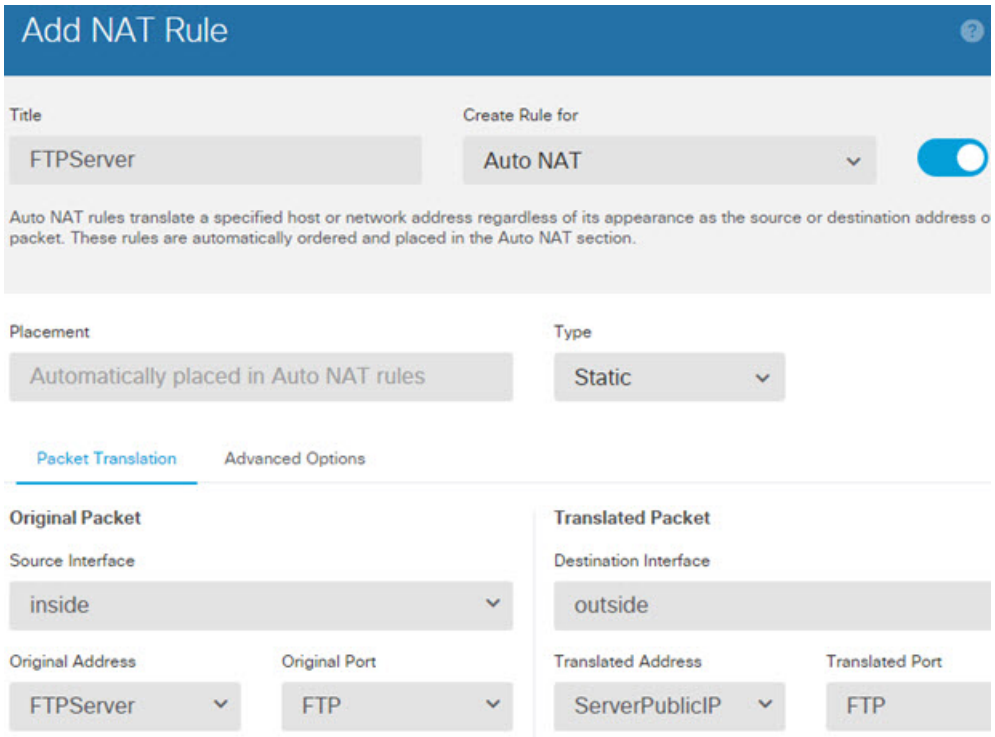
步骤 5 为 FTP 服务器配置具有端口转换的静态 NAT，并将 FTP 端口映射到其自身。

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）。
- **创建规则的对象** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 内部。
- **目的接口** = 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 (OK)**。

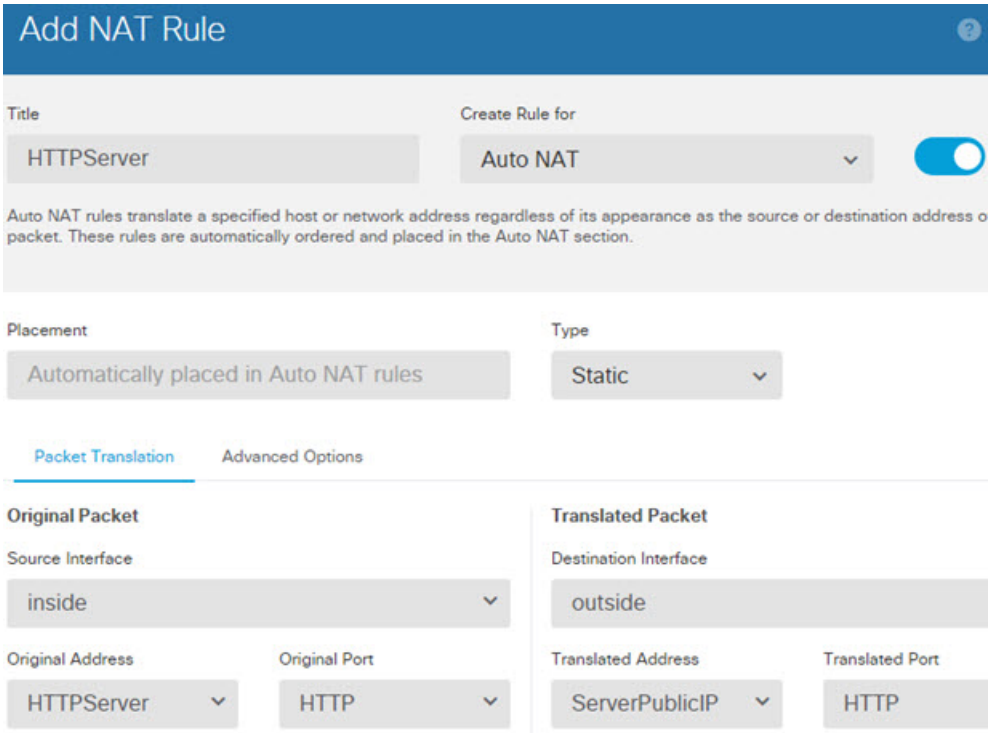
步骤 6 为 HTTP 服务器配置具有端口转换的静态 NAT，并将 HTTP 端口映射到其自身。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = HTTPServer（或您选择的其他名称）。
- **创建规则的对象** = 自动 NAT。

- **类型** = 静态。
- **源接口** = 内部。
- **目的接口** = 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 (OK)**。

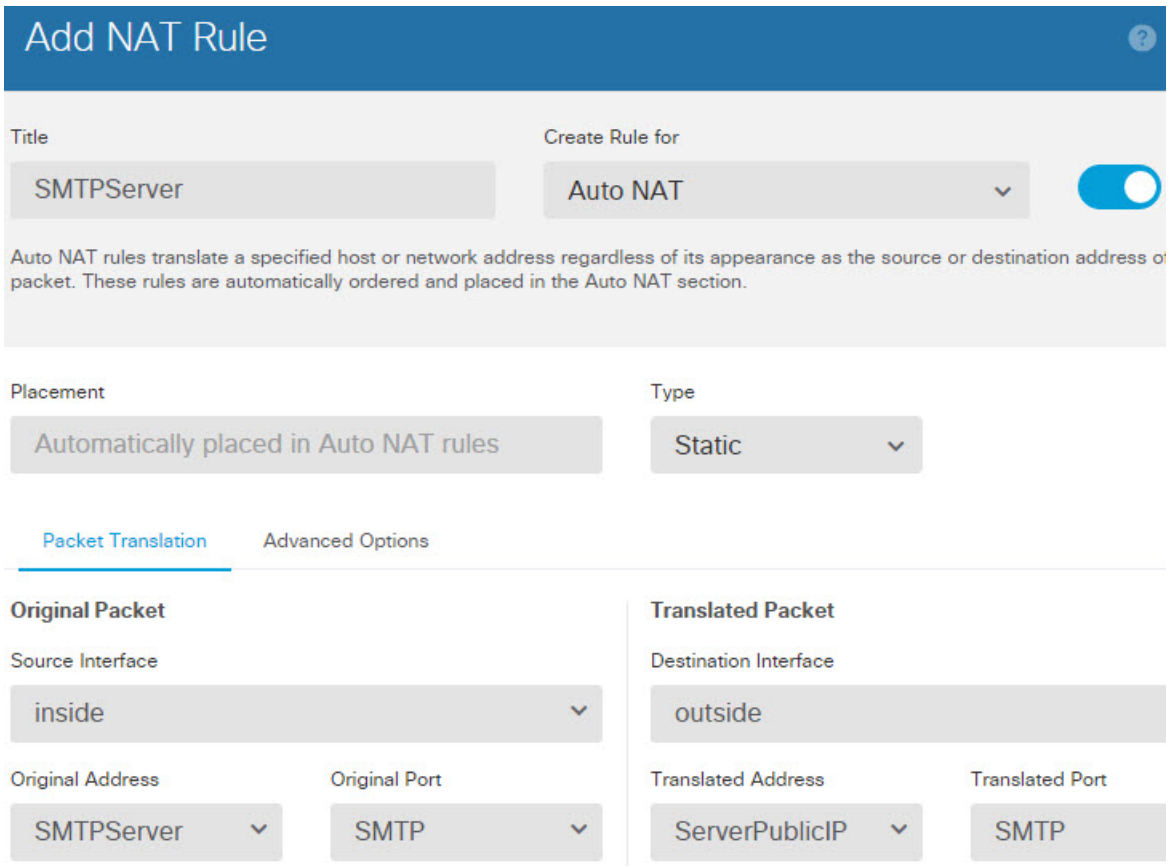
步骤 7 为 SMTP 服务器配置具有端口转换的静态 NAT，并将 SMTP 端口映射到其自身。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = SMTPServer（或您选择的其他名称）。
- **创建规则的对象** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 内部。
- **目的接口** = 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。



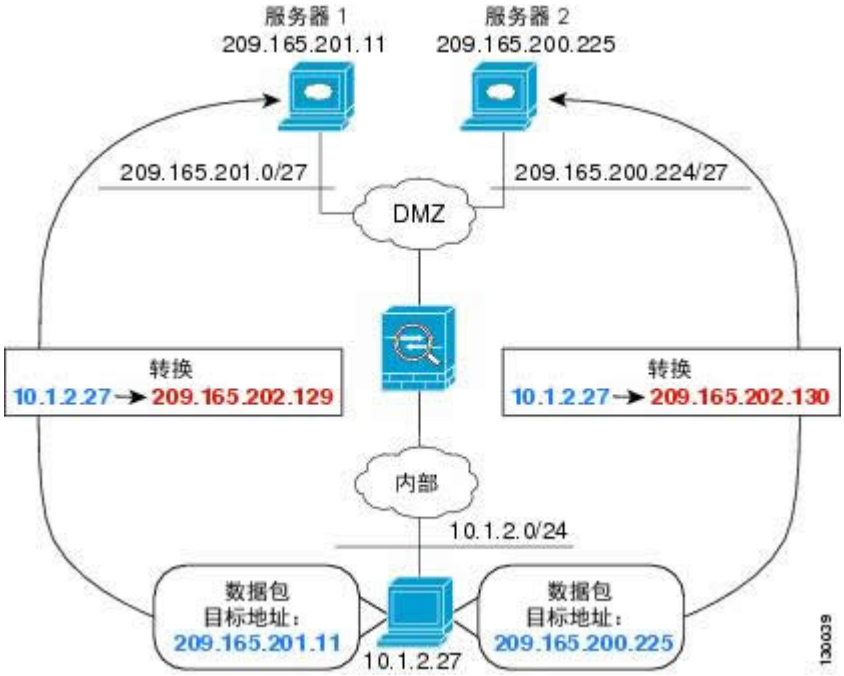
c) 点击**确定 (OK)**。

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:端口。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:端口。

注释 此示例假定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桥接组接口 (BVI)，并且服务器连接到单独的桥接组成员接口，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，对于源接口而言，规则可能有 inside1_2 和 inside1_3，而非 inside。

图 *17*: 具有不同目标地址的手动 *NAT*



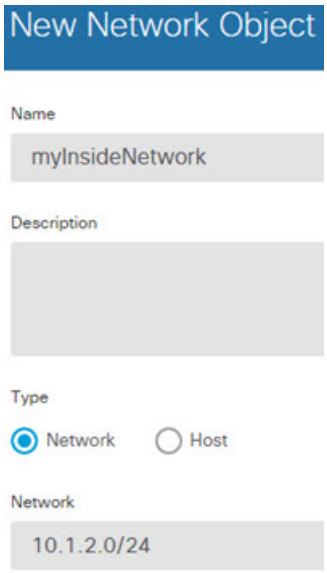
过程

步骤 1 为内部网络创建网络对象。

a) 选择**对象 (Objects)**。

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 (Network)**，然后输入实际网络地址 10.1.2.0/24。

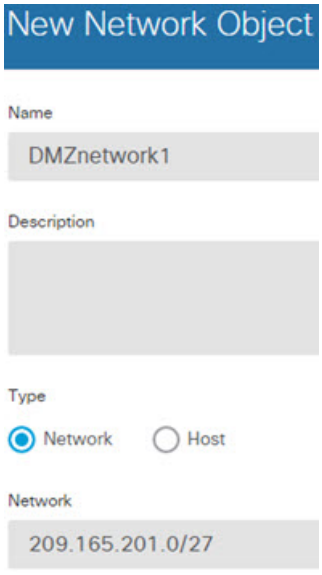


d) 依次点击**确定**。

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 (Network)**，然后输入网络地址 209.165.201.0/27（子网掩码为 255.255.255.224）。

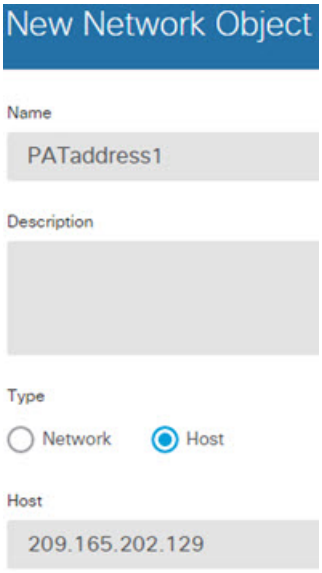


c) 依次点击**确定**。

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 (Host)**，然后输入实际主机地址 209.165.202.129。

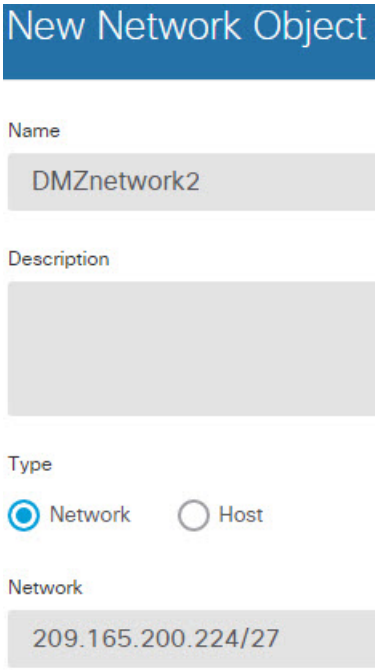


c) 依次点击**确定**。

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 (Network)**，然后输入网络地址 209.165.200.224/27（子网掩码为 255.255.255.224）。

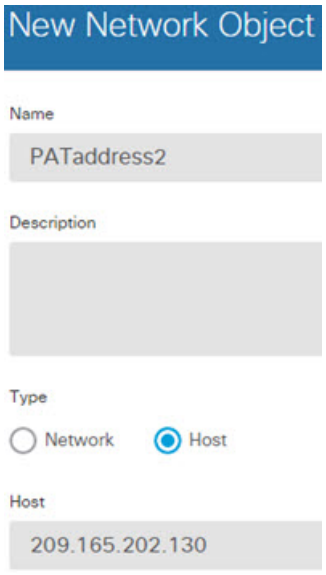


c) 依次点击**确定**。

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 (Host)**，然后输入实际主机地址 209.165.202.130。



c) 依次点击**确定**。

步骤 6 为 DMZ 网络 1 配置动态手动 PAT。

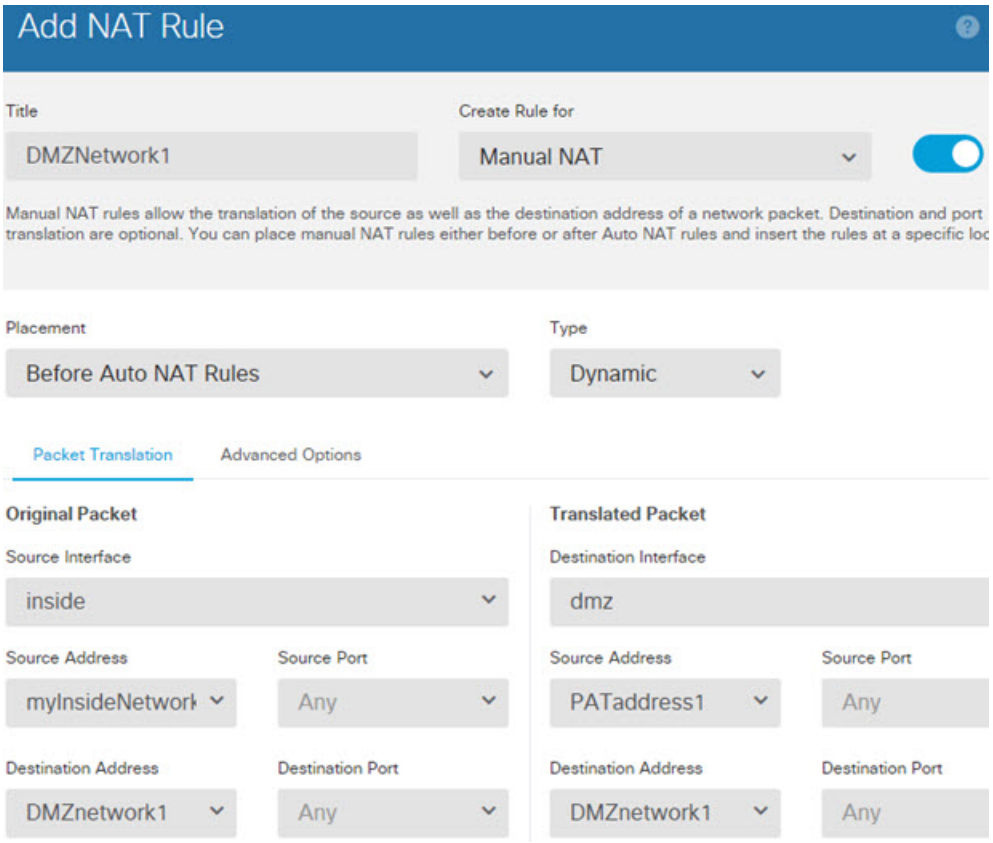
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = DMZNetwork1（或您选择的其他名称）。
- **创建规则的对象** = 手动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目的接口** = dmz。
- **原始源地址** = myInsideNetwork 网络对象。
- **转换后的源地址** = PATaddress1 网络对象。
- **原始目的地址** = DMZnetwork1 网络对象。
- **转换后的目的地址** = 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。



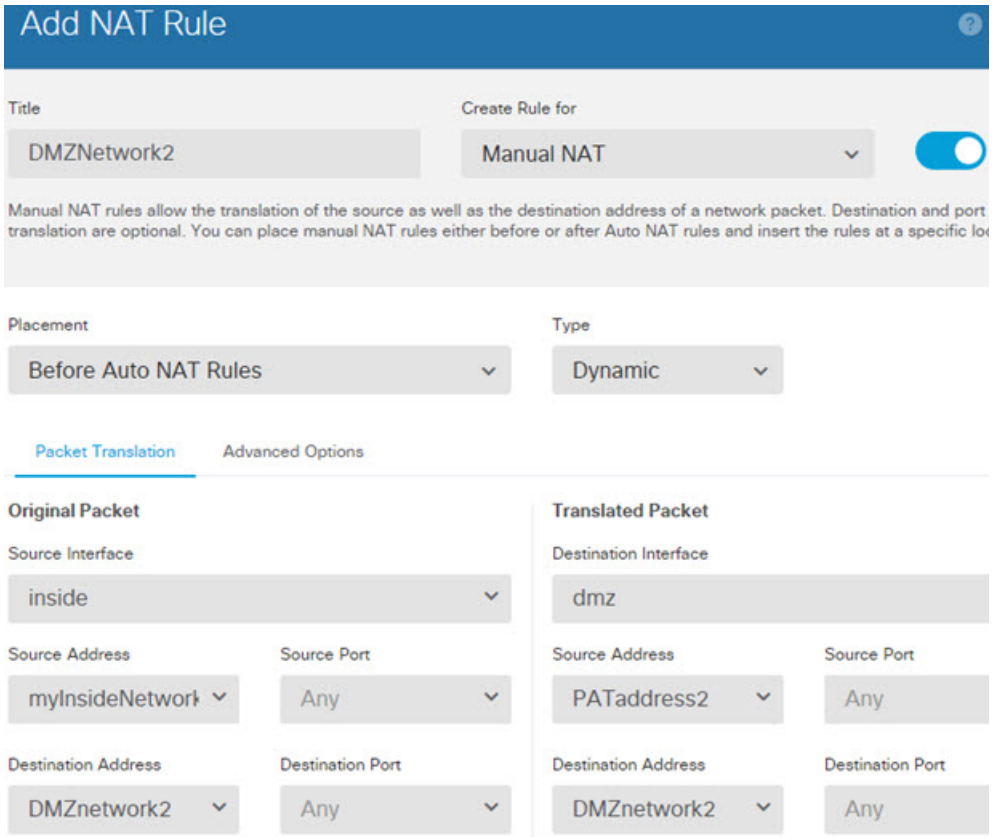
d) 点击**确定 (OK)**。

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）。
- **创建规则的对象** = 手动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目的接口** = dmz。
- **原始源地址** = myInsideNetwork 网络对象。
- **转换后的源地址** = PATaddress2 网络对象。
- **原始目的地址** = DMZnetwork2 网络对象。
- **转换后的目的地址** = DMZnetwork2 网络对象。



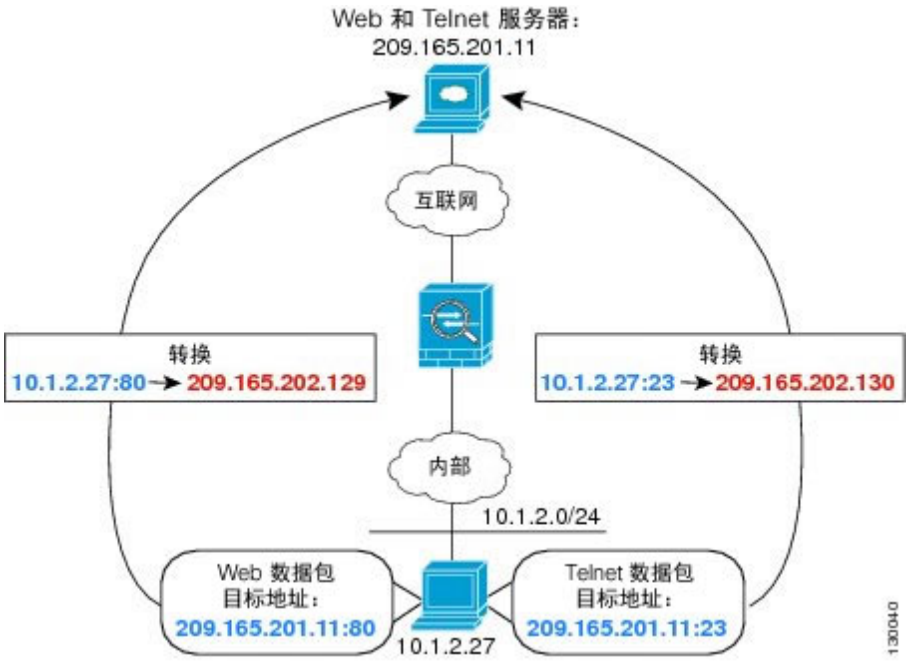
c) 点击**确定 (OK)**。

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。当主机因为 Telnet 服务访问服务器时，实际地址将转换为 209.165.202.129:*port*。当主机访问同一服务器以实现 Web 服务时，真实地址将转换为 209.165.202.130:*port*。

注释 此示例假定，内部接口是连接到一台交换机的标准路由接口，而服务器也连接到该交换机。如果内部接口是桥接组接口 (BVI) 而服务器连接到某个桥接组成员接口，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“内部”作为源接口。

图 *18*: 具有不同目标端口的手动 *NAT*



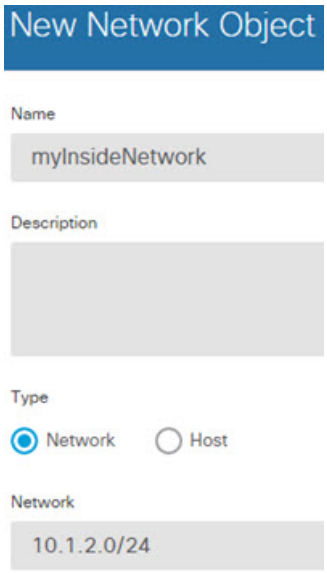
过程

步骤 1 为内部网络创建网络对象。

a) 选择**对象 (Objects)**。

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 (Network)**，然后输入实际网络地址 10.1.2.0/24。

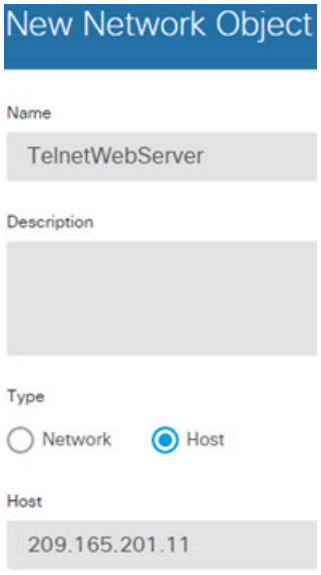


d) 点击**确定**。

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 (Host)**，然后输入实际主机地址 209.165.201.11。

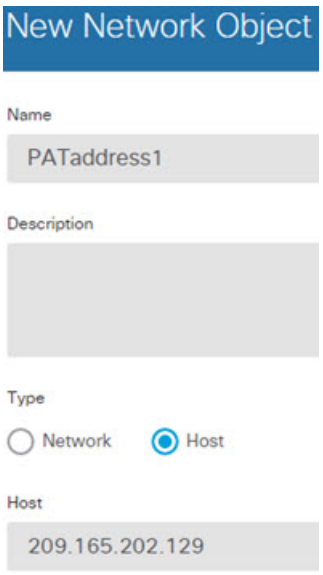


c) 点击**确定**。

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 (Host)**，然后输入实际主机地址 209.165.202.129。

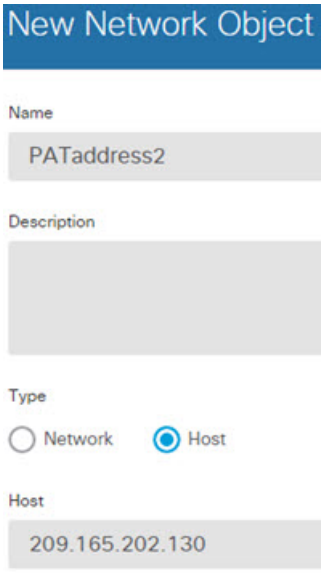


c) 点击**确定**。

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 (Host)**，然后输入实际主机地址 209.165.202.130。



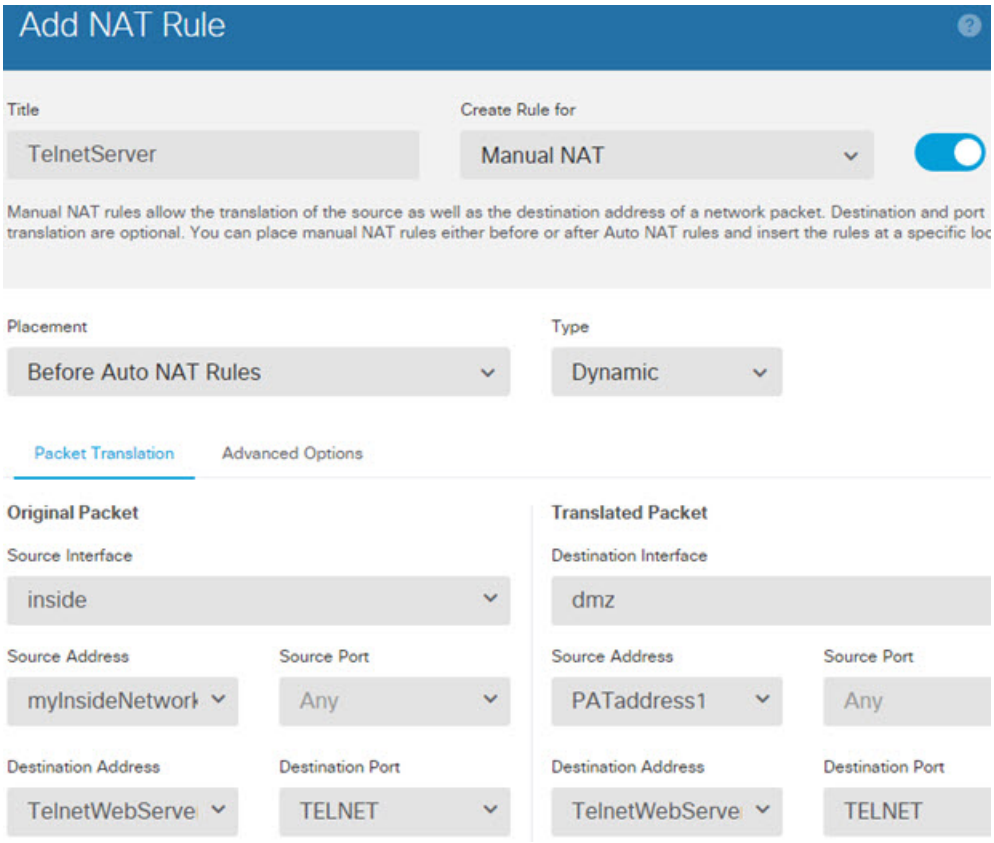
c) 点击**确定**。

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）。
- **创建规则的对象** = 手动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目的接口** = dmz。
- **原始源地址** = myInsideNetwork 网络对象。
- **转换后的源地址 (Translated Source Address)** = PATaddress1 网络对象。
- **原始目的地址** = TelnetWebServer 网络对象。
- **转换后的目的地址** = TelnetWebServer 网络对象。
- **原始目的端口** = TELNET 端口对象。
- **转换后的目的端口** = 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)**。

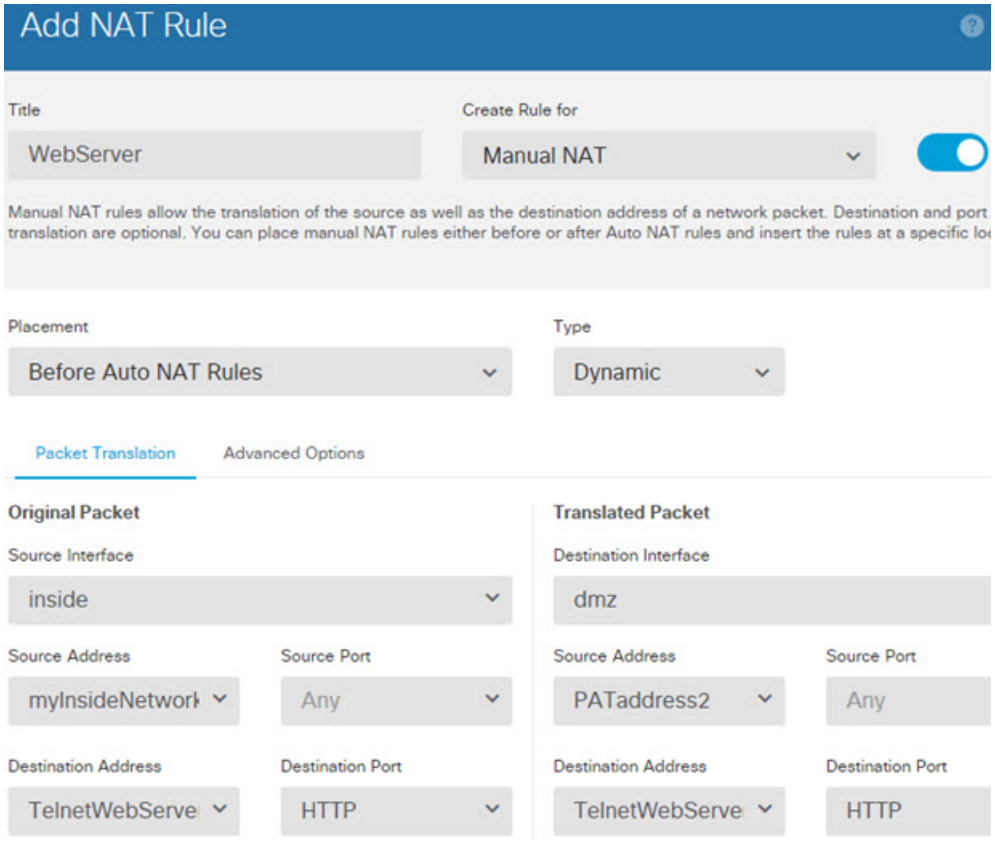
步骤 6 为 Web 访问创建动态手动 PAT。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = WebServer（或您选择的其他名称）。
- **创建规则的对象** = 手动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目的接口** = dmz。
- **原始源地址** = myInsideNetwork 网络对象。
- **转换后的源地址** = PATaddress2 网络对象。
- **原始目的地址** = TelnetWebServer 网络对象。
- **转换后的目的地址** = TelnetWebServer 网络对象。
- **原始目的端口** = HTTP 端口对象。

- 转换后的目的端口 = 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 Firepower 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。

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。

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：

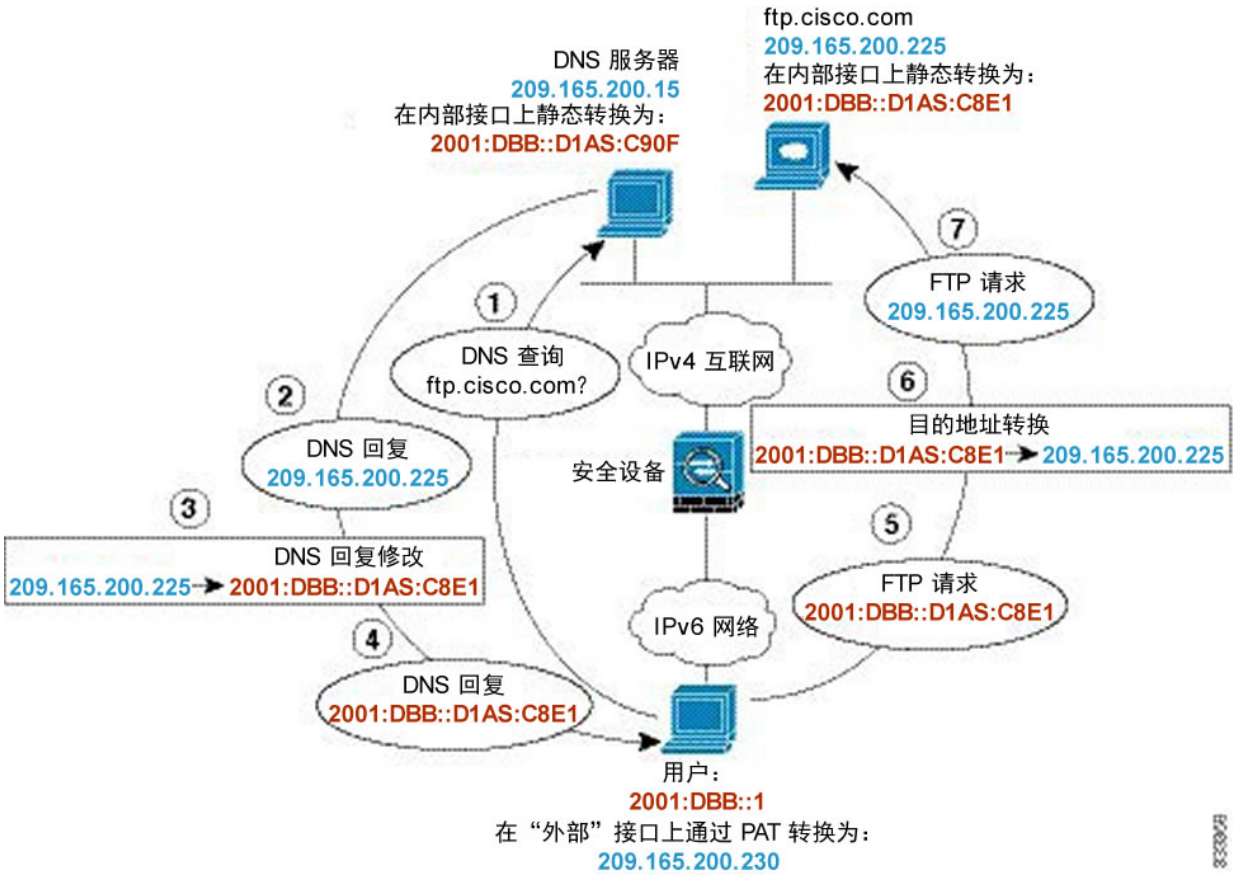
- DNS 重写不适用于 PAT，因为多条 PAT 规则适用于每个 A 或 AAAA 记录，而要使用的 PAT 规则不确定。
- 如果您配置了手动 NAT 规则，当指定了目的地址和源地址时，不能配置 DNS 修改。当流向 A 与 B 时，这类规则可能会有单个地址的不同转换。因此，Firepower 威胁防御设备 将精确匹配 DNS 应答中的 IP 地址与正确的两次 NAT 规则相匹配；DNS 应答不包含有关哪个源地址/目标地址组合位于提示 DNS 请求的数据包中的信息。
- 实际上，DNS 重写在 xlate 条目而非 NAT 规则上完成。因此，如果没有面向动态规则的 xlate，则不能正确完成重写。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，内部接口不是桥接组接口 (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。

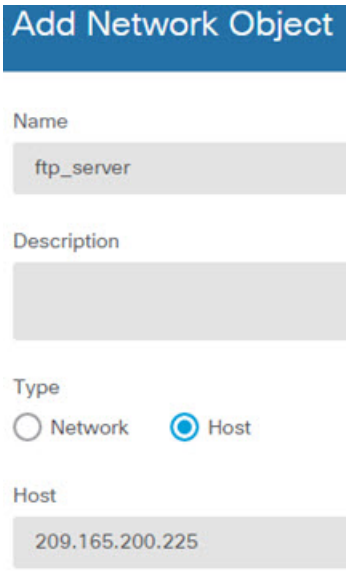
过程

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 (Objects)**。

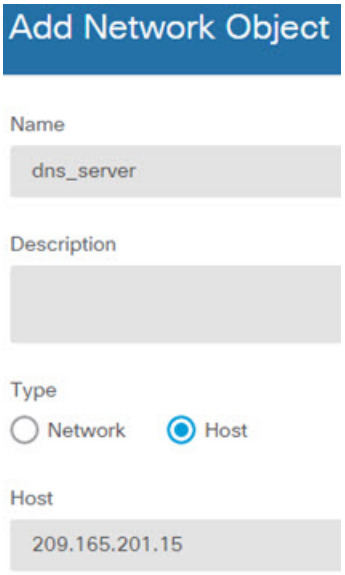
b) 从目录中选择**网络**，然后点击 +。

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。



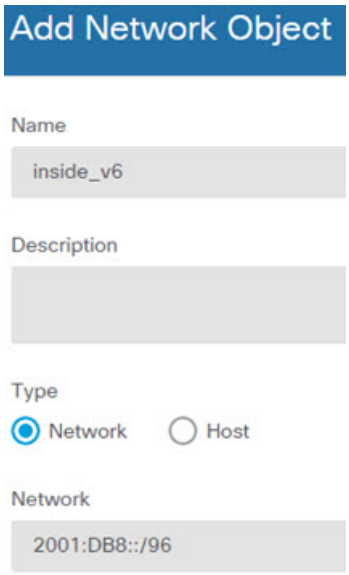
d) 点击**确定**。

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。



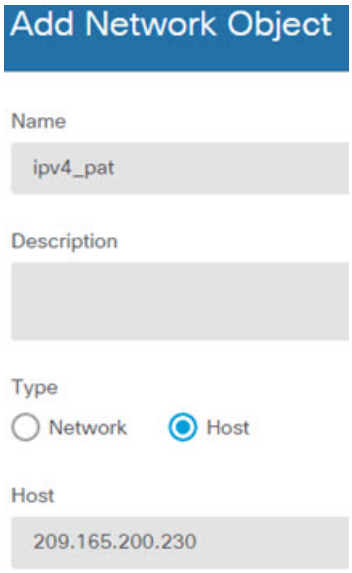
f) 点击**确定**。

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**。

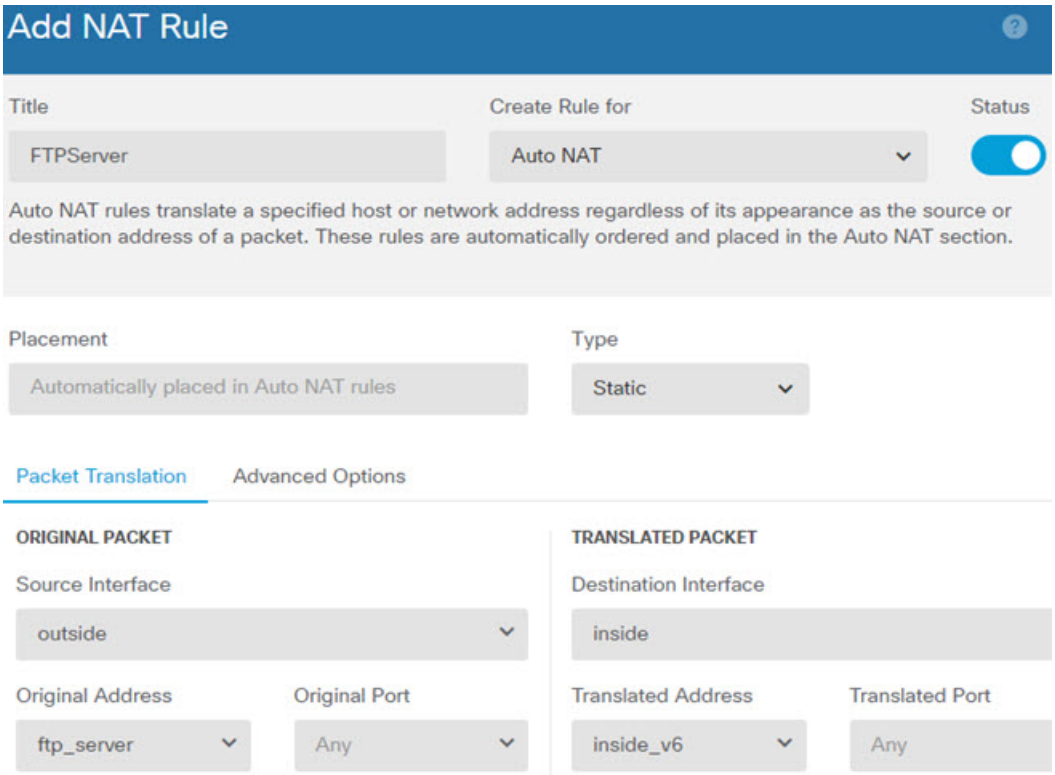
步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

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）。
- **创建规则的对象** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 外部。
- **目的接口** = 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**选项卡上，选择**转换与此规则匹配的 DNS 回复**。



d) 点击**确定 (OK)**。

步骤 3 为 DNS 服务器配置静态 NAT 规则。

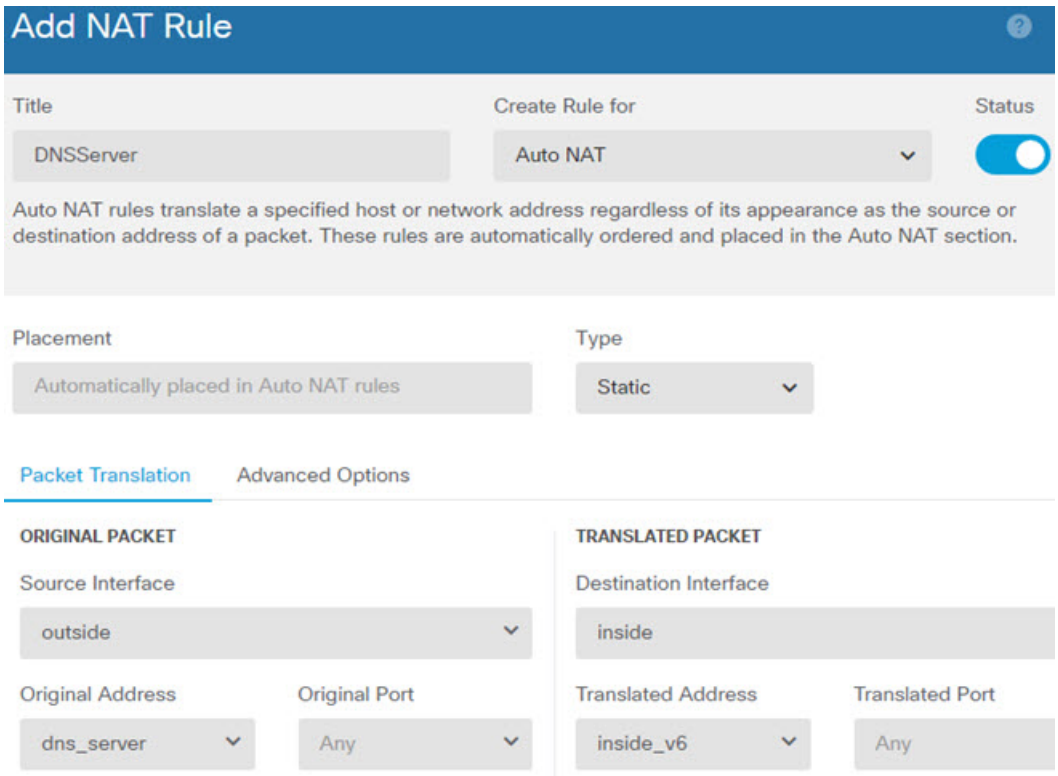
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = DNSServer（或您选择的其他名称）。

- **创建规则的对象** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 外部。
- **目的接口** = 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 (OK)**。

步骤 4 为内部 IPv6 网络配置动态 PAT 规则。

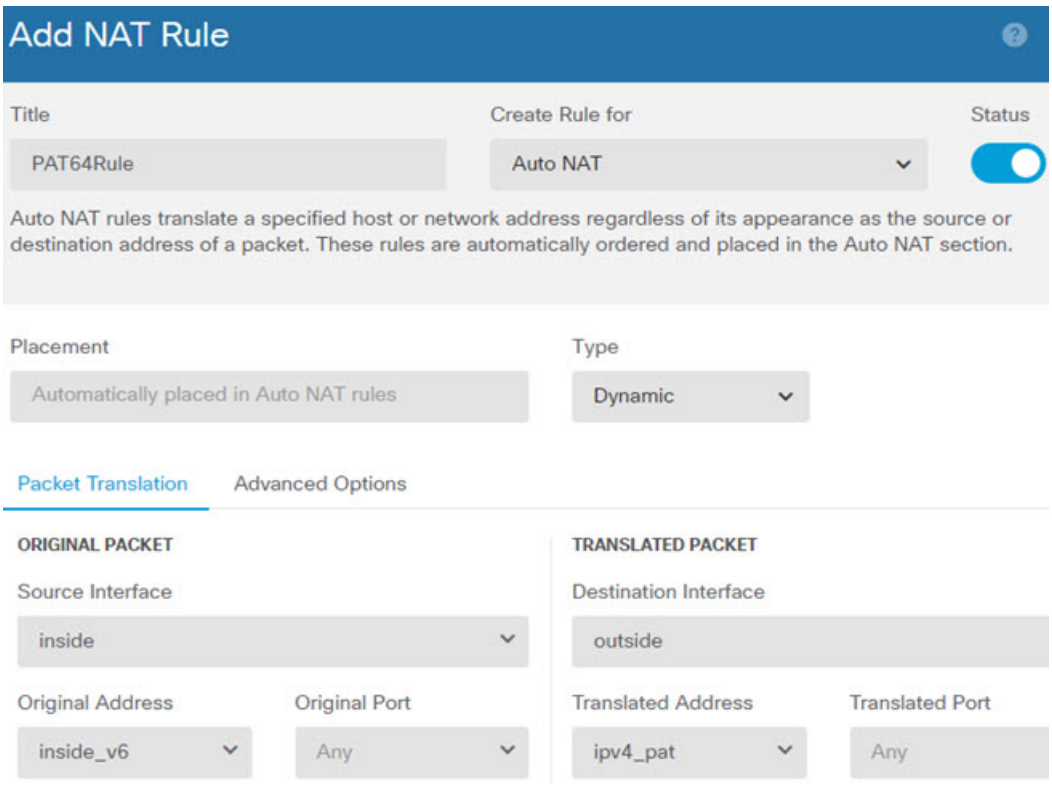
a) 依次选择 **策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = PAT64Rule（或您选择的其他名称）。
- **创建规则的对象** = 自动 NAT。
- **类型** = 动态。

- **源接口** = 内部。
- **目的接口** = 外部。
- **原始地址** = inside_v6 网络对象。
- **转换后的地址** = ipv4_pat 网络对象。



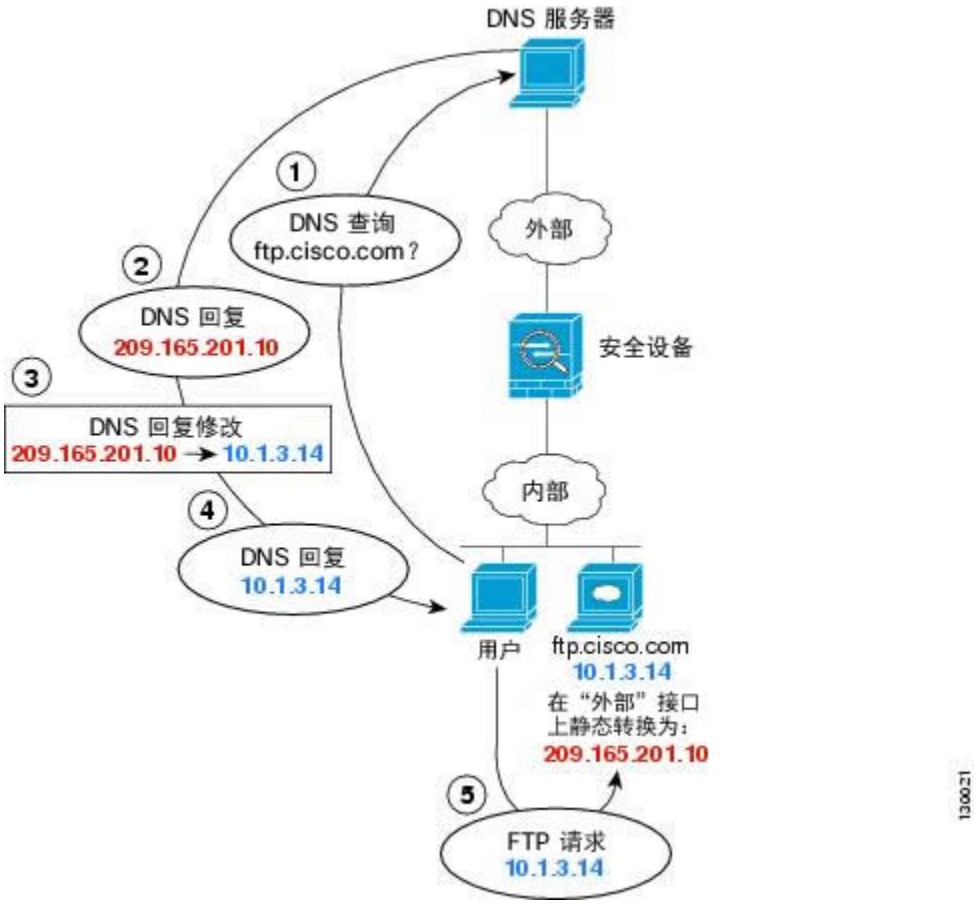
d) 点击**确定 (OK)**。

DNS 应答修改，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，要在此静态规则上启用 DNS 应答修改，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) 作为应答。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 应答修改，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，内部接口不是桥接组接口 (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

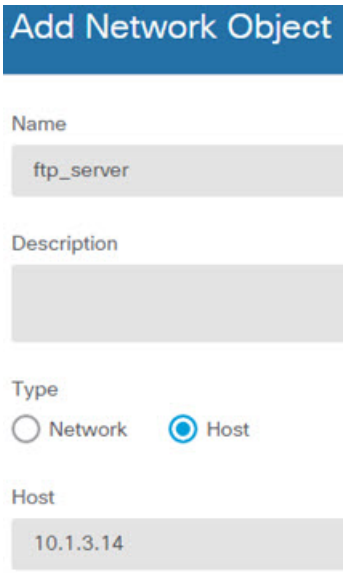
步骤 1 为 FTP 服务器创建网络对象。

a) 选择**对象 (Objects)**。

b) 从目录中选择**网络**，然后点击 +。

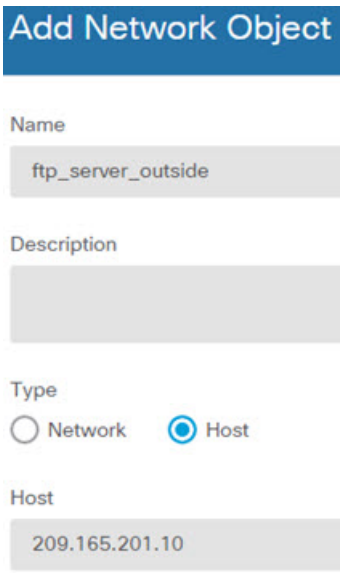
c) 定义实际 FTP 服务器地址。

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。

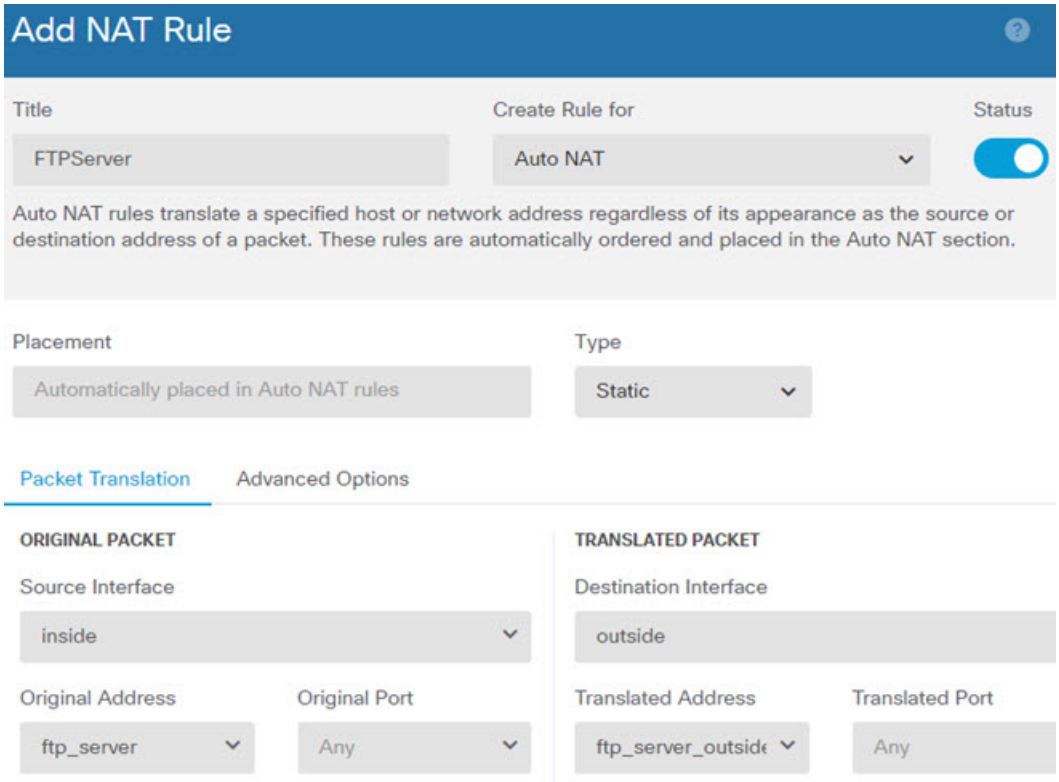
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = FTPServer（或您选择的其他名称）。

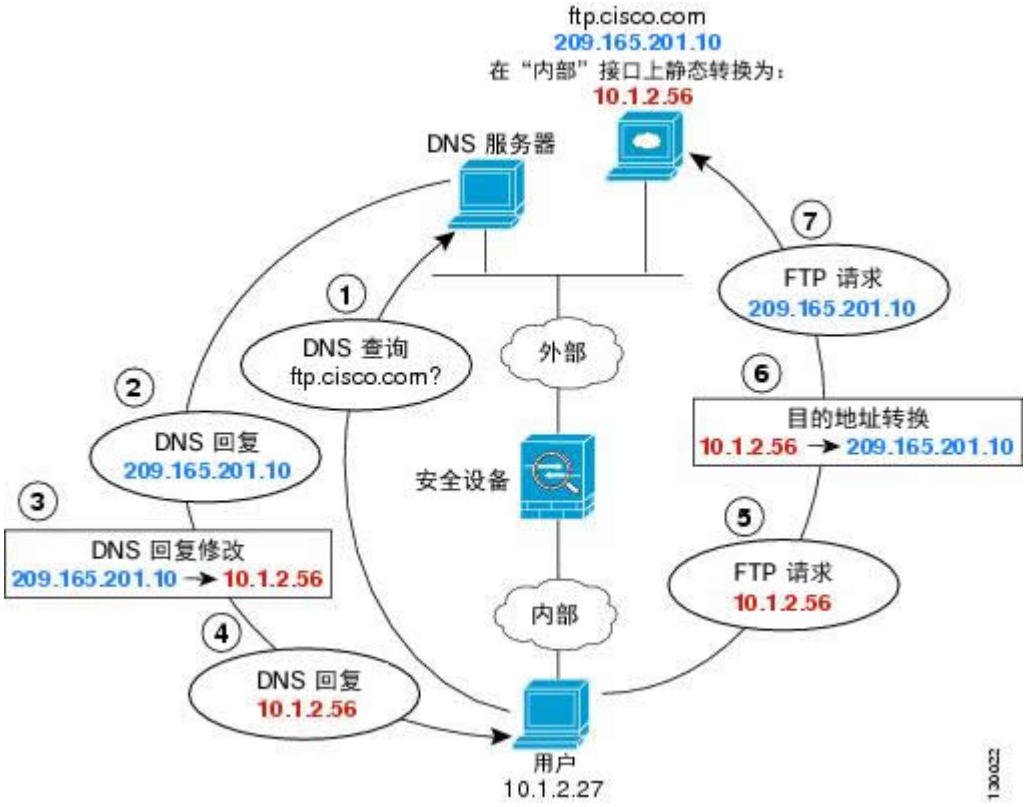
- **创建规则的对象** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 内部。
- **目的接口** = 外部。
- **原始地址** = ftp_server 网络对象。
- **转换后的地址** = ftp_server_outside 网络对象。
- 在**高级选项**选项卡上，选择**转换与此规则匹配的 DNS 回复**。



d) 点击**确定 (OK)**。

DNS 应答修改，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。因为您想让内部用户使用 ftp.cisco.com 的映射地址 (10.1.2.56)，需要配置 DNS 应答修改以进行静态转换。



注释 此示例假定，内部接口不是桥接组接口 (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

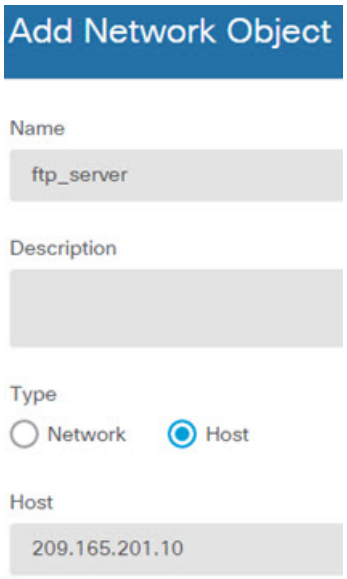
步骤 1 为 FTP 服务器创建网络对象。

a) 选择**对象 (Objects)**。

b) 从目录中选择**网络**，然后点击 +。

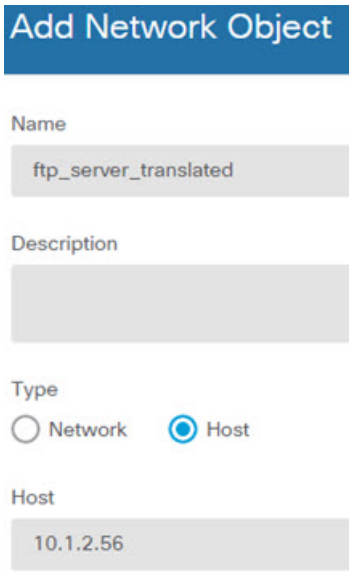
c) 定义实际 FTP 服务器地址。

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。

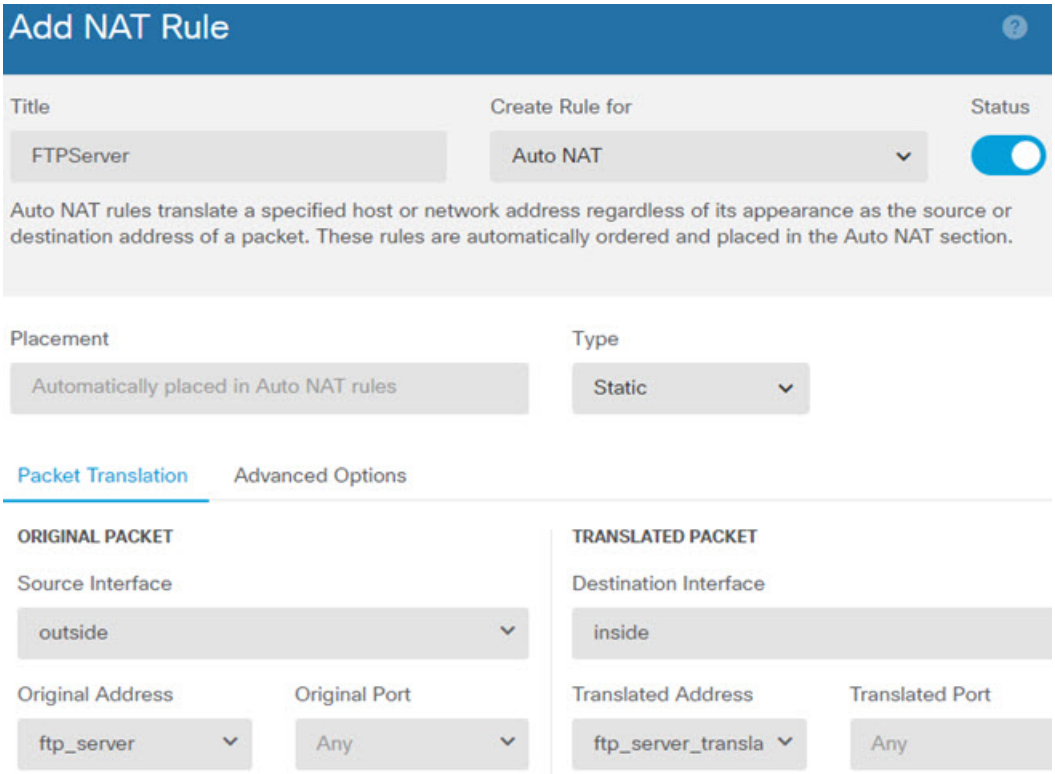
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = FTPServer（或您选择的其他名称）。

- **创建规则的对象** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 外部。
- **目的接口** = 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**选项卡上，选择**转换与此规则匹配的 DNS 回复**。



d) 点击**确定 (OK)**。

第 III 部分

虚拟专用网络 (VPN)

第 11 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的地。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。

在 Firepower 威胁防御中，系统在 VPN 流量通过访问控制策略前不会发送该流量。传入隧道数据包经过解码后才发送到 Snort 进程。传出数据包则由 Snort 处理后再加密。识别 VPN 隧道每个终端节点的受保护网络可以确定允许通过 Firepower 威胁防御设备并访问内部主机的流量。此外，在隧道关闭时，系统不向公共资源发送隧道流量。

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方案。

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 群，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。

注释 仅预共享密钥用于身份验证。

- 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。系统将按照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。

- 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-GMAC -（仅 IKEv2 IPsec 提议。）高级加密标准 Galois 消息身份验证代码是仅提供数据源身份验证的分组加密操作模式。它是 AES-GCM 的一个变体，允许在不加密数据的情况下进行数据身份验证。AES-GMAC 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。
- 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。
- 3DES - 三重 DES，使用 56 位密钥加密三次，比 DES 更加安全，因其使用不同密钥对每个数据块处理三次。不过，此算法比 DES 使用的系统资源更多且速度更慢。
- 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。此算法比 3DES 快且使用的系统资源更少，但安全性也较低。如果不需要很强的数据保密性，并且系统资源或速度存在问题，请选择 DES。
- 空 - 空加密算法提供不加密的身份验证。这通常仅用于测试目的。

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。系统将按照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 位的摘要。SHA 抗暴力攻击的能力高于 MD5。但是，它也会比 MD5 占用更多的资源。对于需要最高级别安全性的实施，请使用 SHA 散列算法。

  标准 SHA (SHA1) 生成 160 位摘要。

  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。

- MD5（消息摘要 5）- 生成 128 位的摘要。MD5 能使用更少的处理时间实现比 SHA 更快的整体性能，但 MD5 被认为安全性低于 SHA。
- 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/GMAC 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 策略仅允许组 1、2 和 5。

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。

- 1 - Diffie-Hellman 组 1：768 位模数。
- 2 - Diffie-Hellman 组 2：1024 位模数。
- 5 - Diffie-Hellman 组 5：1536 位模数。可以为 128 位密钥提供较好的保护。

- 14 - Diffie-Hellman 组 14：2048 位模数。可以为 192 位密钥提供较好的保护。
- 19 - Diffie-Hellman 组 19：256 位椭圆曲线。
- 20 - Diffie-Hellman 组 20：384 位椭圆曲线。
- 21 - Diffie-Hellman 组 21：521 位椭圆曲线。
- 24 - Diffie-Hellman 组 24：2048 位模数和 256 位素数阶子组。

VPN 拓扑

使用 Firepower 设备管理器仅可以配置点对点 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设备，任一台设备均可启动安全连接。

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。

注释 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，或者您没有启用受到出口管制的功能，则无法使用强加密。

过程

步骤 1 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。
此操作将打开“站点间 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 240 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 240 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。

注释 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。

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。

  如果还是没有连接，您还可以点击**创建站点间连接**按钮。

- 要编辑现有连接，请点击连接的编辑图标 ( )。

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。

- **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。该接口不能是桥接组的成员。

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。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。

  远程 IP 地址 - 输入将托管 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。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 (Next)**。

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，即满足出口管制条件，才能并只能选择最基本的选项。

- **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。根据需要选择一个或两个选项。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 242 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 245 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。

- **NAT 免除** - 是否从本地 VPN 访问接口的 NAT 策略中免除 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（而非桥接组成员）后时有用。如果本地网络位于多个路由接口或一个或多个桥接组成员之后，则必须手动创建 NAT 免除规则。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 248 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 238 页。

步骤 6 点击**下一步 (Next)**。

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。

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 254 页。

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方案。IKE 方案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”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。

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 243 页

• 配置 IKEv2 策略 ， 第 244 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 是一种促进基于 IPsec 的通信管理的密钥管理协议。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 IKEv1 策略有多个。如果哪个满足您的需要，只需点击**状态**开关启用它们。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，可点击**状态**开关启用它们。
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。
- 要编辑对象，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 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** - 在两个对等体之间使用的身份验证方法。选择预共享密钥。在身份验证阶段，预共享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。
- **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，请查看 决定使用哪个加密算法，第 237 页。
- **Diffie-Hellman 组** - 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，请查看 决定要使用的 Diffie-Hellman 模数组，第 238 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，请查看 决定使用哪些散列算法，第 238 页。
- **生命周期** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647。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。

步骤 6 点击 **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**旋钮便可启用它们。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**链接来创建 IKEv2 策略。

过程

步骤 1 选择**对象**，然后从目录中选择 **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。相对优先级确定系统首先尝试这些策略中的哪一个，数字越小，代表的优先级越高。

步骤 4 执行以下操作之一：

- 要创建对象，请点击 + 按钮。

- 要编辑对象，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 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** - 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 237 页。
- **Diffie-Hellman 组** - 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 238 页。
- **完整性散列** - 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 238 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。系统与对等体从最强算法到最弱算法进行协商，直到商定一种双方匹配的算法。有关选项的说明，请参阅决定使用哪些散列算法，第 238 页。
- **生命周期** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647。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。

步骤 6 点击 **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 方案对象：

- 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。
- 要编辑对象，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 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 237 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 238 页。

步骤 5 点击 **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。
- 要编辑对象，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 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。系统与对等体从最强算法到最弱算法进行协商，直到商定一种双方匹配的算法。有关选项的说明，请参阅决定使用哪个加密算法，第 237 页。
- **完整性散列** - 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。系统与对等体从最强算法到最弱算法进行协商，直到商定一种双方匹配的算法。有关选项的说明，请参阅决定使用哪些散列算法，第 238 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 **OK**，保存更改。

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（而非桥接组成员）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桥接组成员之后，则需要手动配置 NAT 豁免规则。

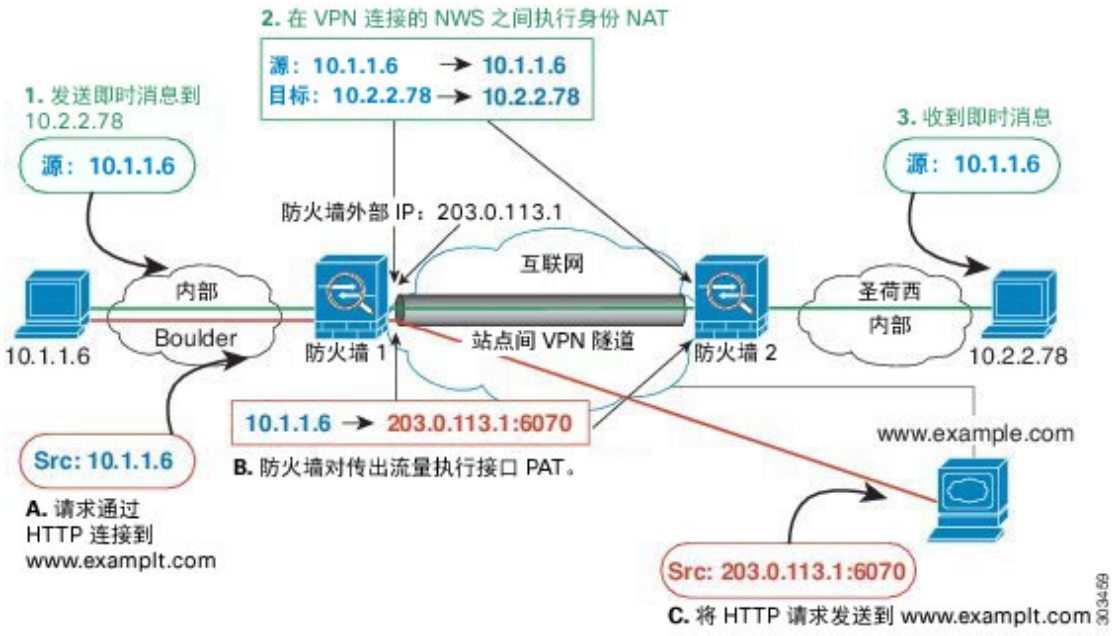
要使 VPN 流量豁免 NAT 规则，需要为目的是远程网络时的本地流量创建身份手动 NAT 规则。然后，将 NAT 应用于目的是其他网络（例如互联网）时的流量。如果本地网络有多个接口，请为每个接口分别创建规则。也可以考虑以下建议：

- 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 *19*：用于站点到站点 *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桥接组，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。

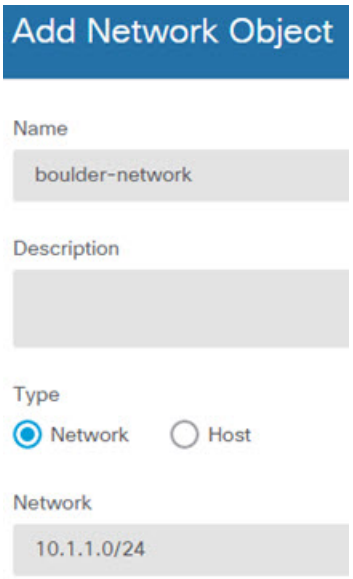
过程

步骤 1 创建对象来定义各种网络。

a) 选择**对象 (Objects)**。

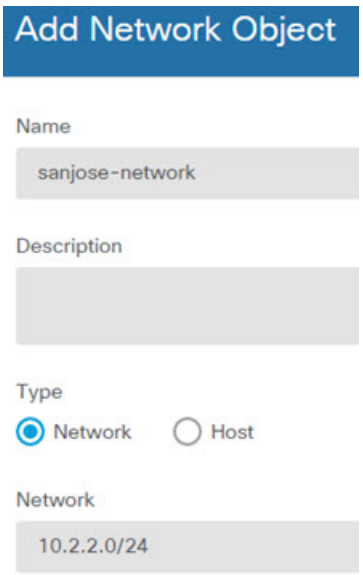
b) 从目录中选择**网络**，然后点击 +。

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。

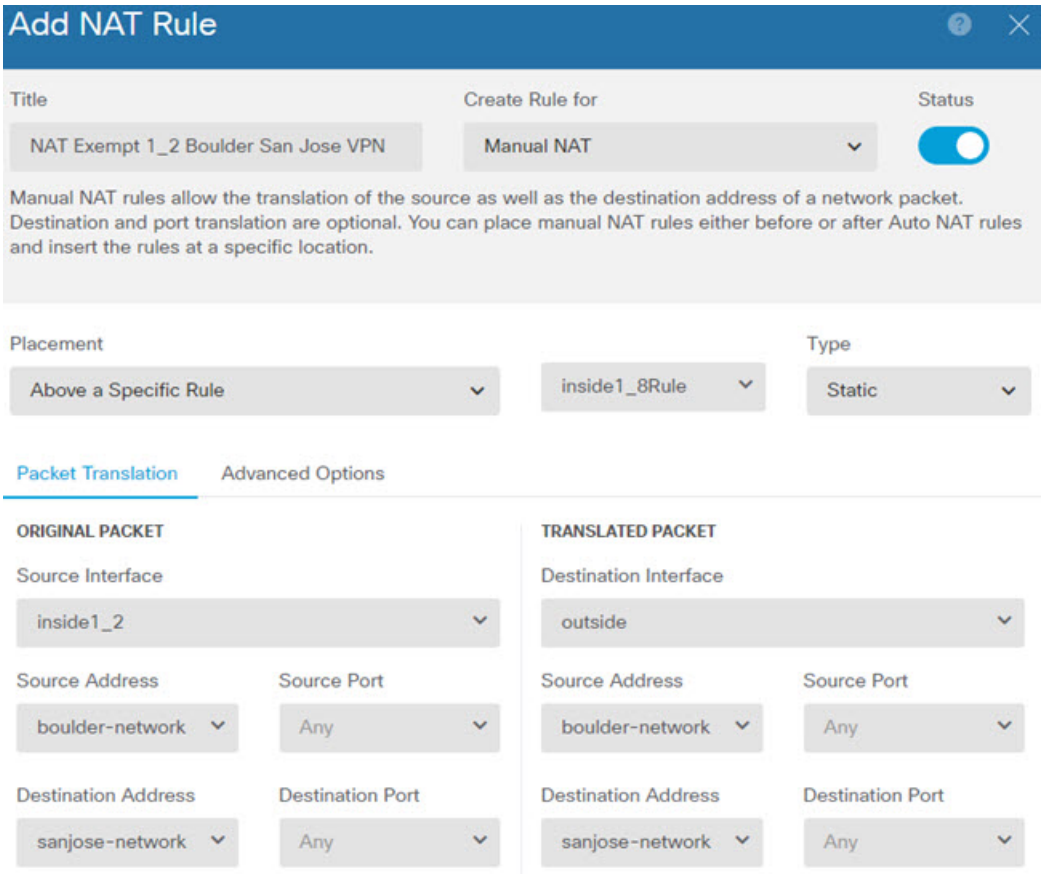
a) 依次选择**策略** > **NAT**。

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）。
- **创建规则的对象** = 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的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。
- **目的接口** = 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。
- **原始目的地址** = sanjose-network 网络对象。
- **转换后的目的地址** = 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。此规则为源和目的配置身份 NAT。



d) 在**高级**选项卡中，选择**不在目的接口上使用代理 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。

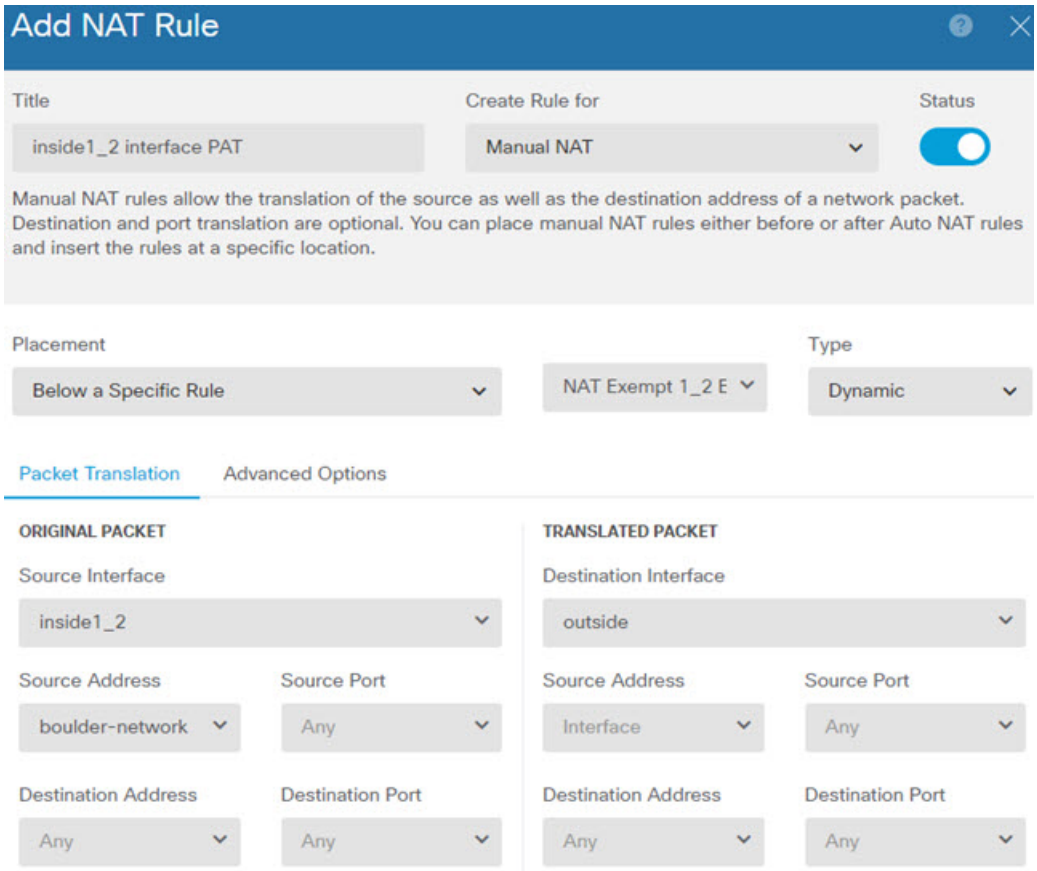
注释 内部接口可能已经配置了将所有 IPv4 流量包括在内的动态接口 PAT 规则，因为初始配置过程中会默认创建这些规则。不过，为完整起见，此处仍显示了这些配置。完成这些步骤之前，请检查是否已经存在将内部接口和网络包括在内的规则，如有则跳过此步骤。

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）。
- **创建规则的对象** = 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的地址，使用 sanjose-network 作为目的的规则必须在此规则之前，否则永远也不会匹配 sanjose-network 规则。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。
- **目的接口** = 外部。
- **原始源地址** = boulder-network 网络对象。
- **转换后的源地址** = **接口**。此选项配置使用目的接口的接口 PAT。
- **原始目的地址** = 任意。
- **转换后的目的地址** = 任意。



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 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。

- 当目的是 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。
- 当目的是“任意”时，手动动态接口 PAT 规则将用于 sanjose-network。

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 5 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**）与远程对等设备 (**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 进行监控和故障排除，请登录设备 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 IPsec 运行数据和统计信息。输入 **show ipsec ?** 可查看可用的关键字。
- **show isakmp** 显示 ISAKMP 运行数据和统计信息。

第 IV 部分

系统管理

第 12 章

系统设置

以下主题介绍如何配置在“系统设置”(System Settings) 页面一起分组的各种系统设置。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 Firepower 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，允许建立 Firepower 设备管理器连接或与 CLI 建立 SSH 连接。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”桥接组的设备型号，这意味着可以通过桥接组中的任意数据接口，与桥接组 IP 地址（默认值为 192.168.1.1）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“任意”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。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **管理访问列表**链接。
如果您已位于“系统设置”页面，只需点击目录中的**管理访问列表**

规则列表定义了允许哪些地址访问指定的端口：对于 Firepower 设备管理器（HTTPS Web 界面）而言，该端口为 443；对于 SSH CLI 而言，该端口为 22。

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 ()。

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。

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。

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。
- **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) 点击**确定 (OK)**。

配置诊断日志记录

诊断日志记录可为与连接不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。以下步骤介绍如何配置诊断消息的日志记录。

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”页面中，只需点击目录中的**日志记录设置**

步骤 2 点击**诊断日志设置** > **开**。
即使配置了本页的剩余字段，只要未开启此设置，也不会生成诊断日志消息。

步骤 3 针对您要查看诊断日志消息的每个位置，将滑块转至**开**的位置，然后选择一个最低严重性级别。
可以将日志消息记录到以下位置：

- **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。
- **系统日志** - 这些消息将发送到您指定的外部系统日志服务器。点击 **+**，选择系统日志服务器对象，然后在弹出对话框中点击**确定**。如果服务器对象尚不存在，请点击**添加系统日志服务器**创建对象。

步骤 4 点击**保存 (Save)**。

严重性级别

下表列出系统日志消息严重性级别。

表 *5*: 系统日志消息严重级别

级别号	严重性级别	说明
0	**emergencies**	系统不可用。
1	**alert**	需要立即采取措施。
2	**critical**	严重情况。
3	**error**	错误情况。
4	**warning**	警告情况。
5	**notification**	正常但重大的情况。

级别号	严重性级别	说明
6	**informational**	消息仅供参考。
7	**debugging**	消息仅供调试。

注释 Firepower 威胁防御不会生成严重性级别为零（紧急）的系统日志消息。

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。

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。

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。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **DHCP 服务器**链接。
如果已经位于“系统设置”页面中，只需点击目录中的 **DHCP 服务器**

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。
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** - 域名系统 (DNS) 服务器客户端应用于域名解析的地址。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 地址加载到字段中。

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，但要将其禁用，直到可以使用为止。
- **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。对于桥接组，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。

  您不能在诊断接口上配置 DHCP 服务器，而应在管理接口上配置，它位于**设备** > **系统设置** > **管理接口**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（从低到高）。IP 地址的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。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。

c) 点击 **OK**。

配置 DNS

域名系统 (DNS) 服务器用来将主机名解析到 IP 地址。这些服务器通过管理界面使用。DNS 服务器在初始系统设置期间配置，但您可以使用以下步骤对其进行更改。

此外您还可以在 CLI 中使用 **configure network dns servers** 和 **configure network dns searchdomains** 命令更改 DNS 配置。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **DNS 服务器**链接。
如果已经位于“系统设置”页面中，只需点击目录中的 **DNS 服务器**

步骤 2 在**主**、**辅助**、**第三 DNS IP 地址 (Primary, Secondary, Tertiary DNS IP address)** 中，按照首选项顺序输入最多三个 DNS 服务器的 IP 地址。
正常情况下，会使用主DNS服务器，除非联系不上它，在这种情况下，会尝试使用辅助服务器，最终尝试第三服务器。

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 地址加载到字段中。

步骤 3 在**域搜索名称 (Domain Search Name)** 中，输入网络的域名，例如 example.com。
此域将添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。

步骤 4 点击**保存 (Save)**。

配置管理接口

管理接口是连接到物理管理端口的虚拟接口。该物理端口名为诊断接口，可在“接口”页面上使用其他物理端口进行配置。

管理接口有两种用途：

- 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。

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 Firepower Device Manager 设置向导，管理地址和网关将保留默认值。

如果需要，可以通过 Firepower 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。

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。默认情况下，管理地址是静态的，而且 DHCP 服务器通常运行在端口。因此，您可以将设备直接连接到管理端口并为工作站获取 DHCP 地址。这种方法可以十分方便地连接和配置设备。

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 Firepower 设备管理器（或 CL）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。

过程

步骤 1 点击**设备**，然后依次点击**系统设置** > **管理接口**链接。
如果已经位于“系统设置”页面中，只需点击目录中的**管理接口**

步骤 2 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：

- **使用数据接口作为网关** - 如果没有单独的管理网络连接到物理管理接口，请选择此选项。流量根据路由表路由到互联网，通常经过外部接口。这是默认选项。
- **为管理接口使用独特网关** - 如果您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）。

步骤 3 配置管理地址、子网掩码或 IPv6 前缀，并根据需要配置 IPv4 和/或 IPv6 的网关。
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。

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。但是，如果使用数据接口作为网关，则不能使用 DHCP。在此情况下，必须使用静态地址。

步骤 4 （可选。）如果配置的是静态 IPv4 地址，请在该端口上配置 DHCP 服务器。
如果在管理端口上配置 DHCP 服务器，则直接连接的客户端或管理网络中的客户端可从 DHCP 池获取其地址。

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 5 点击**保存 (Save)**，阅读警告，然后点击**确定 (OK)**。

配置设备主机名

可以更改设备主机名。

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 Firepower 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**

步骤 2 输入新主机名。

步骤 3 点击**保存 (Save)**，阅读警告，然后点击**继续 (Proceed)**。

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对其进行更改。如果您无法连接到NTP，请参阅排除 NTP 故障，第 283 页。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **NTP** 链接。
如果已经位于“系统设置”页面中，只需点击目录中的 **NTP**

步骤 2 在 **NTP 服务器时间 (NTP Time Server)** 中，选择使用您自己的（手动）时间服务器还是思科的时间服务器。

- **默认 NTP 时间服务器** - 如果您选择此选项，则服务器列表会显示用于 NTP 的服务器名称。
- **手动输入** - 如果您选择此选项，则输入您要使用的 NTP 服务器的完全限定域名或 IP 地址。例如 ntp1.example.com 或 10.100.10.10。如果您有多个 NTP 服务器，请点击**添加另一个 NTP 时间服务器**并输入地址。

步骤 3 点击**保存 (Save)**。

为思科 CSI 配置URL 过滤首选项

系统使用思科综合安全情报 (CSI) 获取信誉、风险和威胁情报。

如果您有适用于 Firepower 的 URL 过滤和 AMP 所需的许可证（用于恶意软件文件策略），系统会自动启用这些功能并启用通信，以从思科 CSI 检索所需的信息。但是，您可以配置某些选项来控制通信。

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”页面中，只需依次点击目录中的**URL 过滤首选项**

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。
- **通过思科 CSI 查询未知 URL** - 对在本地 URL 过滤数据库中不含类别和信誉数据的 URL，是否通过思科 CSI 查询其更新的信息。如果查询在合理的时间限制内返回此信息，则在根据 URL 条件选择访问规则是使用。否则，URL 将匹配未分类的类别。

步骤 3 点击**保存 (Save)**。

配置云管理

可以使用思科 Defense Orchestrator 基于云的门户来管理设备。使用思科 Defense Orchestrator，您可以通过以下方法来进行设备管理：

- 下载初始配置 - 在此方法中，您从思科 Defense Orchestrator 下载初始设备配置，但之后使用 Firepower 设备管理器在本地配置设备。

  注释 使用 Firepower 设备管理器配置设备后，如果您决定要通过云管理设备，请确保在基于云的配置中复制本地更改。

- 通过云进行远程配置管理 - 在此方法中，您使用思科 Defense Orchestrator 创建和更新设备配置。使用此方法时，不要对配置进行本地更改，因为在每个云部署中，云中定义的配置将替换设备上的本地配置。如果进行了本地更改，请确保在基于云的配置中重复此配置以保存更改。

有关云管理原理的更多信息，请参阅思科 Defense Orchestrator 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

获取思科 Defense Orchestrator 的注册密钥。

此外，请确保设备有到互联网的路由。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **云管理**链接。
如果已经位于“系统设置”页面中，只需点击目录中的**云管理**

步骤 2 点击**开始**。

步骤 3 在**注册密匙**中粘贴密钥，然后点击**连接**。
注册请求将发送到云门户。如果密钥有效，并且有通往互联网的路由，则设备会成功注册到门户。然后，您便可以开始使用门户来管理设备了。

如果您决定不想再使用云管理，可以从齿轮图标下拉列表中选择**取消注册**。

第 13 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

系统使用多个数据库来提供高级服务。思科会对这些数据库提供更新，以便您的安全策略采用可用的最新信息。

系统数据库更新概述

Firepower 威胁防御使用以下数据库提供高级服务。

入侵规则

在发现新漏洞时，思科 Talos 安全智能和研究小组 (Talos) 将发布入侵规则更新，以便于您导入。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。

地理定位数据库 (GeoDB)

思科地理定位数据库 (GeoDB) 包含与可路由 IP 地址关联的地理数据（例如国家/地区、城市、坐标）和连接相关数据（例如互联网服务提供商、域名、连接类型）。

GeoDB 更新物理位置、连接类型等方面的更新信息，系统会将这些信息与所检测到的可路由 IP 地址相关联。您可以使用地理定位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定位信息收集），但更新执行时的确会占用系统资源。在计划更新时，请考虑到这一点。

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、客户端和应用程序指纹。Firepower 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 安全智能和研究小组 (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。

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。

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

为了避免对待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。

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 要手动更新数据库，请点击该数据库的**立即更新**部分。
在下载和应用更新后，系统会自动重新部署策略到设备，以便系统可使用更新的信息。

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 (Edit)**。
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。

c) 点击**保存 (Save)**。

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。

升级 Firepower 威胁防御软件

您可以在 Firepower 威胁防御软件升级可用时安装升级。以下程序假定您的系统已在运行 Firepower 威胁防御 6.2.0 版或更高版本，并且它们运行正常。

升级有三种：热修补、次要升级和主要升级。热修补升级可能不需要重新启动系统，而次要和主要版本升级则的确需要重新启动。如果需要重新启动，系统会在安装后自动重新启动。安装任何更新都可能造成流量中断，因此请在非工作时间进行安装。

使用此程序无法重新映像设备或从 ASA 软件迁移到 Firepower 威胁防御软件。

注释 如有任何等待完成的更改，请务必在安装更新前部署这些更改。此外，您还应该运行备份并下载备份副本。

开始之前

登录 Cisco.com，下载升级映像。

- 确保您获得适当的升级文件（文件类型为 .sh）。请勿下载系统软件包或引导映像。

- 确认您是否正在运行升级所需的基准映像。有关兼容性信息，请参阅《思科 *Firepower* 兼容性指南》，网址是：http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html。
- 阅读有关新版本的版本说明。您可以在 http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html 找到版本说明。

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 上传升级文件。

- 如果尚未上传升级文件，请点击**浏览**并选择该文件。
- 如果已有上传的文件，但要上传与之不同的文件，请点击**上传其他文件**链接。只能上传一个文件。如果上传新文件，它将取代旧文件。
- 要删除该文件，请点击删除图标 ( )。

步骤 3 点击**安装 (Install)** 开始安装过程。
图标旁的信息表示设备是否会在安装期间重新启动。您将从系统中自动注销。安装可能需要30分钟或更长时间。

请耐心等候，然后重新登录系统。“设备摘要”（或“系统监控”控制面板）应该显示新版本。

如果遇到问题，可以查看有关安装的日志。日志文件保存在/var/log/升级文件名称文件夹中，其中，文件夹的名称是不含内部版本号的升级文件名称。可以查看的最有用的日志文件是**main_upgrade_script.log**。请在设备 CLI 中使用 **system support view-logs** 命令查看该日志。如果安装失败且无法通过重新安装升级来解决问题，请联系思科技术支持服务。

步骤 4 （可选。）更新系统数据库。
如果没有为地理位置、规则和漏洞数据库 (VDB) 配置自动更新作业，现在正是对其进行更新的好时机。

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 Firepower 威胁防御软件。无法将运行 ASA 映像的设备升级为运行 Firepower 威胁防御映像的设备。

- 设备运行的是 6.1.0 版本之前的映像，而您要升级到 6.1 或更高版本的映像，并使用 Firepower 设备管理器配置设备。无法使用 Firepower 管理中心升级 6.1 版本之前的设备，然后再切换到本地管理。
- 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的编写的《重新映像思科 *ASA* 或 *Firepower* 威胁防御设备指南》或《*Firepower* 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。

只有两台设备的型号相同且运行相同版本的软件，才能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。

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**。
此时将打开“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 输入备份名称和描述（后者为可选项）。
如果决定以后再执行备份（而不是立即执行），可以改为点击**计划 (Schedule)**。

步骤 4 点击**立即备份 (Back Up Now)**。
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。

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的计划，请编辑该计划并点击**删除 (Remove)**。

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 输入备份名称和描述（后者为可选项）。

步骤 4 选择备份的日期和时间。

步骤 5 点击 **Schedule**（**安排**）。
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 (Remove)**。

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 输入备份名称和描述（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。系统将在每天的预定时间执行备份。
- **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（下午 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（下午 11 点）进行。

步骤 5 点击**保存 (Save)**。
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。

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

您可以根据需要恢复备份。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。这可以确保您对该地址所作的任何更改都得以保留，也让您有可能恢复位于不同网段中不同设备上的配置。

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**。
此时将打开“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。

恢复完成后，系统将重新启动。

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。系统还会重新部署策略。

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。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，您即可将该文件移到安全文件存储。
- 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**>**浏览文件**，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 10 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 - 要恢复备份副本，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。

重新启动系统

如果您认为系统运行不正确，而解决问题的其他操作均失败，您可以重新启动设备。您必须通过CLI重新启动设备；不能通过 Firepower 设备管理器重新启动设备。

过程

步骤 1 使用 SSH 客户端打开指向管理 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 输入 **reboot** 命令。

示例：

```
> reboot
```

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。

用于测试连接的 Ping 命令

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。您可以登录到设备 CLI 来使用 ping 命令。

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，系统必须能够通过虚拟管理接口到达思科许可证服务器，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）。

以下是 ping 网络地址的主要选项。

通过虚拟管理接口 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*

指定主机的 IP 地址。如果您仅知道 FQDN，可使用 **nslookup** *fqdn-name* 命令来确定 IP 地址。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，可使用 **pinginterface** *if_name* 命令。您还可以使用此命令指定诊断接口，但不能指定虚拟管理接口。

pinginterface *if_name host*

指定主机的 IP 地址。如果您仅知道 FQDN，可使用 **nslookup** *fqdn-name* 命令来确定 IP 地址。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。如果您仅知道 FQDN，可使用 **nslookup** *fqdn-name* 命令来确定 IP 地址。

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的地发送 UDP 数据包或者向目的地发送 ICMPv6 回应。通往目的地沿途的路由器以 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。您可以登录设备 CLI 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。

输出符号	说明
!P	ICMP 协议不可达。
!A	管理性禁止 ICMP。
?	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 目的

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 目的

指定主机的 IP 地址。如果您仅知道 FQDN，可使用 **nslookup** *fqdn-name* 命令来确定 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。

排除 NTP 故障

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 **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 **Device** > **System Settings** > **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 **Device** > **System Settings** > **Management Interface** 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 **Device** > **Routing** 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，Firepower 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。

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“‘ntpq -pn’的结果”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 服务器前的 + 表示 它是一个潜在的候补者。此处的星号 * 表示当前的 时间源对等体。

NTP 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，然后由时钟的选择 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 Firepower 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。

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 *Firepower* 威胁防御的命令参考（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** 命令。

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
seshat
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，将一起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。

在本地和远程管理之间切换

您可以使用本地 Firepower 设备管理器（直接托管在设备上）配置和管理自己的设备，也可以使用 Firepower 管理中心 多设备管理器进行远程配置和管理。如果要配置不受 Firepower 设备管理器支持的功能，或需要 Firepower 管理中心提供的效能和分析功能，您可能要使用远程管理器。

另外，若要在透明防火墙模式下运行设备，也必须使用 Firepower 管理中心。

您可以在本地和远程管理之间切换，而无需重新安装软件。在从远程管理切换至本地管理之前，请确认 Firepower 设备管理器满足您的所有配置要求。

注意 切换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。

开始之前

如果已注册了设备，特别是如果启用了任何功能许可证，则必须通过Firepower设备管理器取消注册设备，然后才能切换到远程管理。取消注册设备会释放基本许可证和所有功能许可证。如果不取消注册设备，这些许可证将保持分配给思科智能软件管理器中的设备。请参阅注销设备，第 62 页。

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 Firepower 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 Firepower 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 要从本地管理切换为远程管理，请执行以下操作：

a) 验证您当前处于本地管理模式之下。

```
> show managers
Managed locally.
```

b) 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 Firepower 管理中心的 DNS 主机名或 IP 地址（IPv4 或 IPv6）。如果 Firepower 管理中心不是直接可寻址的，请使用 **DONTRESOLVE**。如果使用 **DONTRESOLVE**，则需要使用 *nat_id*。
- *regkey* 是向 Firepower 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 Firepower 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
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before switching to remote management.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue  [yes/no] yes
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                :
```

注释 在执行注册期间，您可以使用 **configure manager delete** 删除该注册，然后使用 **configure manager local** 返回本地管理。

c) 登录 Firepower 管理中心并添加设备。
有关详细信息，请参见 Firepower 管理中心在线帮助。

步骤 3 要从远程管理切换为本地管理，请执行以下操作：

a) 验证您当前处于远程管理模式之下。

```
> show managers
Host                      : 192.168.0.123
Registration Key          : ****
Registration              : pending
RPC Status                :
```

b) 删除远程管理器，进入无管理器模式。
无法直接从远程管理转至本地管理。使用 **configure manager delete** 命令可删除管理器。

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

c) 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。

更改防火墙模式

Firepower 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 Firepower 设备管理器仅支持路由模式。不过，如果您需要在透明模式下运行该设备，可以更改防火墙模式，开始使用 Firepower 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 Firepower 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 Firepower 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 Firepower 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 61 页。

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 Firepower 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 Firepower 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 firewalltransparent

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 Firepower 管理中心的 DNS 主机名或 IP 地址（IPv4 或 IPv6）。如果 Firepower 管理中心不是直接可寻址的，请使用 **DONTRESOLVE**。如果使用 **DONTRESOLVE**，则需要使用 *nat_id*。
- *regkey* 是向 Firepower 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 Firepower 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 Firepower 管理中心并添加设备。
有关详细信息，请参见 Firepower 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 Firepower 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 firewallrouted

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Firepower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 61 页。

过程

步骤 1 使用SSH客户端打开指向管理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
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.
```

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。